Testing Classical Properties from Quantum Data

Matthias C. Caro
University of Warwick, Coventry, UK
Freie Universität Berlin, Germany

Preksha Naik
California Institute of Technology, Pasadena, CA, USA

Joseph Slote
California Institute of Technology, Pasadena, CA, USA

Abstract

Many properties of Boolean functions can be tested far more efficiently than the function itself can be learned. However, this dramatic advantage often disappears when testers are limited to random samples of f instead of adaptively chosen queries to f. In this work we investigate the *quantum* version of this restriction: quantum algorithms that test properties of a Boolean function f solely from copies of either the function state $|f\rangle \propto \sum_x |x, f(x)\rangle$ or the phase state $|(-1)^f\rangle \propto \sum_x (-1)^{f(x)} |x\rangle$.

Quantum advantage in testing from data. For monotonicity, symmetry, and triangle-freeness, we show passive quantum testers are unboundedly or super-polynomially better than their classical passive testing counterparts. They are competitive with classic *query*-based testers in each case.

Inadequacy of Fourier sampling. Our new testers use techniques beyond quantum Fourier sampling, and it turns out this is necessary: we show a certain class of bent functions can be tested from $\mathcal{O}(1)$ function states but has a sample complexity lower bound of $2^{\Omega(n)}$ for any tester relying exclusively on Fourier and classical samples.

Classical queries vs. quantum data. Our passive quantum testers are competitive with classical *query*-based testers, but this isn't universal: we exhibit a testing problem that can be solved from $\mathcal{O}(1)$ classical queries but requires $\Omega(2^{n/2})$ function state copies. The FORRELATION problem provides a separation of the same magnitude in the opposite direction, so we conclude that quantum data and classical queries are "maximally incomparable" resources for testing.

Towards lower bounds. We also begin the study of *lower bounds* for testing from quantum data. For quantum monotonicity testing, we prove that the ensembles of [58, 24], which give exponential lower bounds for classical sample-based testing, do not yield any nontrivial lower bounds for testing from quantum data. New insights specific to quantum data will be required for proving copy complexity lower bounds for testing in this model.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases Quantum Property Testing, Quantum Data, Boolean Functions

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.34

Related Version *Full Version*: `https://arxiv.org/abs/2411.12730` [37]

Funding Part of this work was completed while JS was visiting the Simons Institute for the Theory of Computing, supported by DOE QSA grant #FP00010905.
Matthias C. Caro: MCC was partially supported by a DAAD PRIME fellowship and by the BMBF (QPIC-1).
Joseph Slote: JS is funded by Chris Umans' Simons Foundation Investigator Grant.

Acknowledgements We thank Srinivasan Arunachalam, Fernando Jeronimo, Kyle Gulshen, Jiaqing Jiang, John Bostanci, Yeongwoo Hwang, Shivam Nadimpali, John Preskill, Akshar Ramkumar, Abdulrahman Sahmoud, Mehdi Soleimanifar, and Thomas Vidick for discussions. Moreover, we thank Nathan Harms for suggesting we look at monotonicity and discussions on classical bounds for related problems. We thank Fermi Ma for helpful discussions that provided inspiration for Theorem 12. We

are grateful to Francisco Escudero Gutiérrez for pointing us to the Fourier-analytic characterization of monotonicity which allowed us to improve a previous passive quantum monotonicity tester. Finally, we thank the anonymous STOC 2025 reviewers for helpful feedback.

1 Introduction

In property testing we consider a subset $\mathcal{P}$ of the set of all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ and aim to find fast algorithms for deciding (with high probability) whether an unknown function f has property $\mathcal{P}$ or is ε-far from having property $\mathcal{P}$; that is, we wish to decide between

$$\text{Case } (i) \quad f \in \mathcal{P} \qquad \text{or} \qquad \text{Case } (ii) \quad \min_{g \in \mathcal{P}} \|f - g\|_1 \geq \varepsilon \,,$$

promised one of these is the case. Here $\|f-g\|_1 = \Pr_{x \sim \{0,1\}^n}[f(x) \neq g(x)]$ is the L^1 distance. Property testing began in the context of program checking [30, 87], where it was shown that only $\mathcal{O}(1)$ queries to f are needed to determine (with high probability) whether f is linear or is $\Theta(1)$-far from linear – which compares very favorably to the $\Omega(n)$ query lower bound for *learning* linear functions. The extreme query efficiency of property testing algorithms soon after played a critical role in interactive proofs and PCP theorems [8, 7, 50]. Since then property testing has developed into a rich landscape of access models, complexity regimes, and separations [51, 86, 85, 93, 57].

One of the promises of this broad view of property testing, identified very early on [59], is its potential in data analysis and machine learning: one could run inexpensive property testing algorithms to guide the choice of which long-running learning algorithm to use. But there is an unfortunate catch: the dramatic complexity advantage of testing over learning typically disappears in the natural access model for data analysis and machine learning, where fresh queries to f cannot be made and only a limited dataset $\{(x_j, f(x_j)\}_j$ of random samples from f is available. This setting is known as *passive* or *sample-based testing* [59].

Indeed, many results in passive testing are lower bounds that grow with n, unlike the algorithms available in query-based testing: compare among the "Classical" columns in Table 1. In fact, Blais and Yoshida [27] showed that if a Boolean property can be tested from $\mathcal{O}(1)$ random samples, then the property is of a rather restricted kind.[1]

▶ Remark 1. This is not to say that the classical passive testing model is *uninteresting*; there are many exciting positive results for the model, falling under the umbrella of *sublinear* algorithms. For example, the line of work [53, 60, 48] showed that the existence of certain constant-query testers implies sample-based algorithms with sublinear dependence on n. But passive testers still cannot compete with query-based testing for many important problems, as the lower bounds in Table 1 attest.

How could we recover large testing speedups in the context of passive testing from data? In the present work we advocate for quantum computing (and "quantum datasets") as an answer. Viewed from the right perspective, early results in quantum complexity theory actually demonstrate that quantum data – in the form *quantum examples*, that is, copies of the *function state* $|f\rangle := 2^{-n/2} \sum_x |x, f(x)\rangle$ – can sometimes suffice for highly efficient property testing. For example, the Bernstein-Vazirani algorithm, usually understood as an $\mathcal{O}(1)$ quantum *query* algorithm, really only needs $\mathcal{O}(1)$ *function states* to test for linearity [19]

[1] In particular, such a property is only a function of the conditional expected values $\mathbb{E}_x[f(x)|x \in S_j]$ of f for sets S_j forming a constant-cardinality partition of the hypercube, $S_1 \sqcup \cdots \sqcup S_{\mathcal{O}(1)} = \{0,1\}^n$.

Table 1 Upper and lower bounds for testing and learning in various access models. All bounds are given for (a sufficiently small) constant $\varepsilon > 0$. Bounds that are given without a reference follow trivially from other bounds in the table.

	Quantum		Classical		
Property	Examples	Queries	Samples	Queries	Learning (from queries)
k-Juntas	$\mathcal{O}(k)$ [13]	$\widetilde{\mathcal{O}}(\sqrt{k})$ [6]	$\Omega(2^{k/2} + k \log n)$ [4]	$\widetilde{\Theta}(k)$ [25, 47]	$\Omega(2^k + k \log n)$ [4]
Linearity	$\Theta(1)$ [19]	$\mathcal{O}(1)$	$n + \Theta(1)$ [4]	$\Theta(1)$ [30]	$n + \Theta(1)$ [4]
$\mathbb{F}_2$ degree-d	$\mathcal{O}(n^{d-1})$ [10]	$\mathcal{O}(2^d)$	$\Theta(n^d)$ [4]	$\Theta(2^d)$ [5, 21]	$\Theta(n^d)$ [4]
Monotonicity	$\tilde{\mathcal{O}}(n^2)$ [Theorem 9]	$\widetilde{\mathcal{O}}(n^{1/4})$ [18]	$2^{\Omega(\sqrt{n})}$ [24]	$\widetilde{\mathcal{O}}(\sqrt{n})$ [74]	$2^{\Omega(\sqrt{n})}$ [29]
Symmetry	$\mathcal{O}(1)$ [37]	$\mathcal{O}(1)$	$\Theta(n^{1/4})$ [4]	$\mathcal{O}(1)$ [26]	$\Theta(n^{1/2})$ [4]
Triangle-freeness	$\mathcal{O}(1)$ [37]	$\mathcal{O}(1)$	$\Omega(2^{n/3})$ [37]	$\mathcal{O}(1)$ [26]	–

(vs. $\Omega(n)$ classical samples), and the quantum k-junta tester of Atıcı and Servedio [13] also requires only $\mathcal{O}(k)$ quantum examples (*c.f.* the lower bound of $\Omega(2^{k/2} + k \log n)$ classical samples). The present work seeks to establish *passive quantum testing* as a fundamental model of property testing by making progress on the question:

What is the extent of quantum advantage in testing classical properties from data?

Before this work it was not fully clear whether quantum data in the form of quantum examples can lead to testing speedups beyond linearity and k-junta-like properties (such as low Fourier degree): both the Bernstein–Vazirani algorithm and the Atıcı–Servedio junta tester rely only on *quantum Fourier sampling* [19], a quantum subroutine which, given copies of $|f\rangle$, returns the label $S \subseteq [n]$ of a Fourier character with probability $\widehat{f}(S)^2$. Despite the success of quantum Fourier sampling, its utility is restricted to properties that are "plainly legible" from the Fourier spectrum.[2]

In this work we expand the list of properties with efficient passive quantum testers, including one which provably requires a non-Fourier sampling approach. We also compare the power of quantum data to that of classical queries, finding that they are (essentially) maximally incomparable as resources for testing. Finally, we begin a study of lower bounds for testing monotonicity from quantum data by showing that the ensembles leading to exponential lower bounds for classical sample-based testing yield no nontrivial lower bounds for quantum data-based testing. In the remainder of the introduction we explore each of these points in greater detail.

[2] As an example of a property *not* detectable from the Fourier spectrum, consider the task of testing if f is a quadratic $\mathbb{F}_2$ polynomial. It is well-known (see, *e.g.*, [65, Claim 2.4]) that degree-2 $\mathbb{F}_2$ polynomials can have Fourier coefficients with uniformly exponentially-small magnitudes, so Fourier sampling is not directly useful for this task. Our Theorem 3 below serves as another example.

▶ Remark 2 (Where might quantum data appear?). While from the perspective of complexity theory quantum data leads to a natural counterpart to classical passive testing, and demonstrates a "data-based" quantum advantage, the reader may still feel it is not entirely natural from a practical or "physical" standpoint. To the contrary, we contend that quantum data may be a useful component of emerging quantum technologies. We briefly list some scenarios where quantum data may be a natural object.

- Suppose a researcher has time-limited query access to a data-generating process, but does not yet know what questions about the process she will eventually ask. She may prefer to store data in quantum memory rather than classical, to broaden the range of questions that can be answered *post hoc*.
- In high-latency and bandwidth-limited scenarios, back-and-forth (adaptive, query-based) interaction is not feasible, for example in space exploration. If a space probe departing Earth shared some entanglement with a ground station, it could later in its journey encode observations into quantum data and teleport the resulting states back to Earth. In such a scenario, the advantages of quantum data could lead to significant speedups in research and analysis.
- Rather than sharing the source code for a program f, a company may prefer to share a quantum data encoding of it as a form of copy protection – provided the function state is sufficient for the intended application.

1.1 Quantum advantage in testing from data: an emerging theme

Our first contribution is to expand the list of properties exhibiting quantum advantage in testing from data. Our algorithms work by finding new quantum ways to exploit insights from prior work in classical testing. See Section 2 for proofs.

Symmetry testing. A Boolean function is *symmetric* if $f(x) = f(y)$ when x is a permutation of y. We show that projecting $|f\rangle$ onto the symmetric subspace yields an $\mathcal{O}(1)$-copy quantum test. For comparison, classical passive symmetry testing requires $\Omega(n^{1/4})$ samples [4].

Monotonicity testing. A Boolean function f is *monotone* if $f(x) \leq f(y)$ when $x \prec y$ in the standard partial order $\prec$ on the hypercube. Monotonicity has been of central importance in the classical property testing literature [58, 18, 74]. We give a quantum algorithm that tests monotonicity with $\widetilde{\mathcal{O}}(n^2)$ copies of $|f\rangle$, in comparison to the lower bound of $2^{\Omega(\sqrt{n})}$ samples for classical passive testing [24].

The algorithm appeals to a characterization of monotonicity in terms of the Fourier spectrum of f. In particular, let ε be the L^1 distance between a Boolean function f and the set of all monotone functions. Then we may relate ε to the Fourier spectrum of f via

$$2\varepsilon \;\leq\; \mathbf{I}[f] - \textstyle\sum_i \widehat{f}(\{i\}) \;\leq\; 4\varepsilon n\,.$$

Here $\mathbf{I}[f]$ is the total influence of f and is equal to the expected size of a subset $S \subseteq [n]$ sampled according to the Fourier distribution of f. $\mathbf{I}[f]$ can thus be easily estimated with Fourier sampling, and the Fourier coefficients $\widehat{f}(\{i\})$ estimated with classical samples. The bounds above follow from a reinterpretation of the "pair tester" characterization of monotonicity [58], which was not originally Fourier-based.

Triangle-freeness. A Boolean function f is *triangle-free* if there are no x, y such that $(x, y, x+y)$ form a *triangle*: $f(x) = f(y) = f(x+y) = 1$. We give a passive quantum triangle-freeness tester that uses only $\mathcal{O}(1)$ copies of $|f\rangle$. This is to be contrasted with the $\Omega(2^{n/3})$ samples required classically.[3]

It is known that to test triangle-freeness, it suffices to estimate the probability that $(x, y, x+y)$ forms a triangle for uniformly random x, y [54, 66]. Our test estimates this probability by repeating the following subroutine. First, measuring copies of $|f\rangle$ in the computational basis allows us to find a uniformly random $y \in f^{-1}(1)$. Then by measuring the output register of copies of $|f\rangle$, we obtain copies of the entire 1-preimage state

$$\left|f^{-1}(1)\right\rangle \propto \sum_{x\in\{0,1\}^n,\, f(x)=1} |x\rangle \ .$$

Applying the unitary transformation $U_y |x\rangle = |x+y\rangle$ then allows us to transform copies of $\left|f^{-1}(1)\right\rangle$ into copies of

$$|f^{-1}(1)+y\rangle \propto \sum_{x\in\{0,1\}^n,\, f(x+y)=1} |x\rangle \ .$$

The overlap $|\langle f^{-1}(1)|f^{-1}(1)+y\rangle| = \Pr_{x\sim\{0,1\}^n}[f(x) = f(x+y) = 1]$ can now be estimated with a SWAP test [32].

1.2 Fourier sampling does not suffice

Given that Fourier sampling is sufficient to test linearity [19], k-juntas [13, 6], and (as shown above) monotonicity, one might wonder whether Fourier sampling is "all that quantum data is good for" in the context of property testing Boolean functions. To the contrary, we exhibit a property for which a Fourier sampling-based approach requires exponentially more data than the optimal passive quantum tester.

▶ **Theorem 3.** *There is a property $\mathcal{P}$ of Boolean functions on $2n$ bits such that:*

- **(i)** *There is no algorithm for testing $\mathcal{P}$ that uses $2^{o(n)}$ classical samples and any number of Fourier samples.*
- **(ii)** *There is an efficient quantum algorithm for testing $\mathcal{P}$ from $\mathcal{O}(1)$ copies of $|f\rangle$.*

Theorem 3 is proved in Section 3 as Theorems 10 and 11. The property $\mathcal{P}$ is the *Maiorana-McFarland (MM)* class of bent functions, which take the form $f(x, y) = \langle x, y\rangle + h(x)$ for h any n-bit Boolean function (see *e.g.,* [34] for more).

To prove (i), we show the set F_{yes} of MM functions are indistinguishable from the set F_{no} of their "duals," defined by replacing $h(x)$ with $h(y)$. To separate these two classes of functions, we can condition on the set of $h(x)$ having low bias. And, we note that a uniformly random $h(x)$ is low bias with high probability (via Chernoff). Every function in both these sets is *bent* – *i.e.*, all Fourier coefficients have equal magnitude – so Fourier samples cannot help. It thus suffices to lower bound the number of classical samples needed to solve the distinguishing problem. For any number of samples less than 2^{cn}, except in the very unlikely event that there is a collision among the sampled points $\{(x^{(i)}, y^{(i)})\}_i$, the distribution of values $f(x^{(i)}, y^{(i)})$ will look uniformly random, regardless of whether f is sampled uniformly from F_{yes} or F_{no} – and so distinguishing is impossible.

[3] This lower bound, the proof of which we outline in [37, Appendix A.2], arises from the requirement of seeing a linearly dependent triple $(x, y, x+y)$ among the sampled inputs.

As for item (*ii*), the passive quantum tester for this property first applies the unitary U defined by $|x, y, b\rangle \mapsto |x, y, b \oplus \langle x, y\rangle\rangle$ to $|f\rangle$. If f is a MM function, the result should be h, a function depending only on the first n variables, while if $|f\rangle$ is far from MM functions, it will have noticeable dependence on coordinates $n+1, \ldots, 2n$. This dependence can be measured by Fourier-sampling the transformed state.

1.3 Comparing access models

Quantum data is always at least as good as classical samples, and from Table 1 we see that for a growing list of properties, testing from quantum data is competitive with testing from classical *queries*. In fact, quantum data can be vastly more powerful than classical queries for testing. An extremal example of this is the Forrelation problem, which can be tested from $\mathcal{O}(1)$ function state copies but requires $\Omega(2^{n/2})$ classical queries [2].

Conversely, one may wonder to what extent classical queries may outperform quantum data for property testing. An answer is not obvious. Although classical queries enable direct access to $f(x)$ at any point x of the algorithm's choosing – a powerful advantage over quantum data – it is not clear whether this can lead to a separation for property testing. Recall that for a property testing problem, *yes* and *no* instances must be $\Omega(1)$-far in L^1 distance. So to create a hard property for quantum data-based testers, one must find two sets of functions which pairwise differ on a *constant fraction* of the locations in their truth tables, yet still remain hard to distinguish by a quantum algorithm operating on copies of their function states.

We succeed in "hiding" these large differences and identify a testing problem for which classical queries have a dramatic advantage over quantum data.

▶ **Theorem 4.** *There is a testing task (3-fold intersection detection) that can be accomplished with $\mathcal{O}(1)$ classical queries but requires $\Omega(2^{n/2})$ copies for quantum testing from data.*

Combined with the Forrelation separation of [2], Theorem 4 entails that quantum data and classical queries are (essentially) maximally incomparable. See Figure 1 for a full picture of resource inequalities for testing.

Theorem 4 is proved in Section 4 as Theorem 12. Given a function $f : \{0,1,2\} \times \{0,1\}^n \to \{0,1\}$ that indicates three subsets of the hypercube $A, B, C \subseteq \{0,1\}^n$, the 3-fold intersection detection task is to determine if the fractional 3-fold intersection $|A \cap B \cap C|/2^n$ is 0 or $\Omega(1)$-far from 0.

This property is readily tested from queries by computing the probability $x \in A \wedge x \in B \wedge x \in C$ for uniformly-random x. To prove the quantum passive testing lower bound, we show the indistinguishability of two ensembles of function states encoding set triples

$$\big\{(A,B,C)\big\}_{A,B,C \overset{\text{iid}}{\sim} \mathcal{P}\{0,1\}^n} \qquad \text{vs.} \qquad \big\{(A,B,A\Delta B)\big\}_{A,B \overset{\text{iid}}{\sim} \mathcal{P}\{0,1\}^n}.$$

Here Δ denotes symmetric difference, $\mathcal{P}$ denotes the power set, and the samples are uniform. Note the first ensemble has mutual intersection of $\Omega(1)$ density with high probability, while the ensemble always has zero intersection. To obtain the lower bound, the main observation is that the t-copy versions of the two associated function state ensembles are *equal* when projected onto the so-called *distinct subspace* (*i.e.,* the subspace spanned by basis states for which the t input registers are distinct). This projection moves the state ensembles at most $\mathcal{O}(t/2^{n/2})$ in trace distance, so we conclude that for any $t = o(2^{n/2})$, the two ensembles cannot be distinguished using t function state copies.

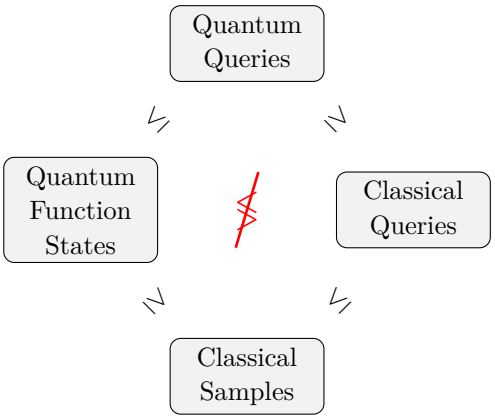

Figure 1 Property testing resource inequalities. The figure illustrates the connections between four different data access models in property testing, namely classical/quantum example/query access. Here, "resource A $\geq$ resource B" means that access to resource B can be simulated from access to resource A without any overhead. (For example, a single classical query can be used to simulate a single classical sample.) As a consequence of Theorem 4 and [19, 91, 2], the only two among these access models that are not trivially comparable are in fact very incomparable.

While 3-fold intersection detection is provably difficult from function state copies, its 2-fold counterpart is quantumly easy. For example, we can perform SWAP tests between function state copies. Rather surprisingly, we find that 2-fold intersection detection can even be achieved by a quantum algorithm using unentangled measurements applied to each copy of the quantum state independently. Namely, in [37, Section 4.2], we provide a quantum Fourier sampling-based approach to 2-fold intersection detection.

1.4 A challenge: lower bounds for quantum monotonicity testing

We also begin the project of finding lower bounds for the passive quantum testing model. Our main contribution is to establish lower bounds for monotonicity as an important first open problem. In particular, we show the ensembles that entail strong lower bounds for classical passive testing are wholly inadequate for quantum passive testing.

▶ **Theorem 5.** *The ensembles in Goldreich et al. [58] and Black [24] can be distinguished by a quantum algorithm with $\mathcal{O}(1/\varepsilon)$ copies of the corresponding function states.*

This theorem says that the best lower bound such ensembles could imply for quantum passive testing is $\Omega(1/\varepsilon)$. But that is no better than the lower bound that exists generically for every (non-trivial) property.[4] To see that $\Omega(1/\varepsilon)$ holds generically, it suffices to consider only two functions, f_{yes} and f_{no}, that are exactly ε-far apart. This is equivalent to $\langle f_{\text{yes}}|f_{\text{no}}\rangle = 1-\varepsilon$, so the trace distance between $|f_{\text{yes}}\rangle^{\otimes t}$ and $|f_{\text{no}}\rangle^{\otimes t}$ is $\sqrt{1-(1-\varepsilon)^{2t}} \leq \sqrt{2t\varepsilon}$. Therefore, distinguishing between f_{yes} and f_{no} with success probability $\geq 2/3$ requires $t \geq \Omega(1/\varepsilon)$ copies of the respective function state. Note that this straightforward lower bound separates quantum samples from quantum queries in the regime $\varepsilon = \mathcal{O}(n^{-3/2})$ because of the $\widetilde{\mathcal{O}}(n^{1/4}/\varepsilon^{1/2})$ quantum query upper bound for monotonicity testing proved in [18].

[4] A classical query complexity lower bound of $\Omega(1/\varepsilon)$ also holds for testing any non-trivial property [52].

We prove Theorem 5 via a combinatorial analysis of the spectrum of the matrix

$$A := \mathop{\mathbb{E}}_{\psi\sim E_0} \psi^{\otimes t} - \mathop{\mathbb{E}}_{\phi\sim E_1} \phi^{\otimes t},$$

where E_0 and E_1 are the "yes" and "no" ensembles from [58] (or, later, from [24]). As neither of our ensembles is close to Haar-random, we cannot directly draw on the rich recent literature on quantum pseudorandomness [73, 31, 56, 72, 80, 39, 88, 79]. Instead, we notice that our function state is unitarily equivalent to a phase state for a closely-related Boolean function. An intricate index rearrangement reveals A to be block-diagonal, with each block interpretable as the adjacency matrix for a complete bipartite graph. We then determine the spectrum of each block, with eigenvalues and their multiplicities given as functions of certain combinatorial quantities. Exponential generating function techniques lead to explicit formulas for these quantities, and finally the asymptotics can be understood by taking a probabilistic perspective on the counting formulas. Concentration arguments finish the proof and allow us to conclude that $\|A\|_1 \geq \Omega(1)$ (and thus the two ensembles are distinguishable) as soon as $t = \Omega(\varepsilon^{-1})$. This argument is presented in detail in Section 5.

A final remark for this section: for certain regimes of ε, the $\Omega(1/\varepsilon)$ lower bound on the number of function state copies already separates passive quantum testing from quantum query-based testing. For example, (adaptive) quantum query complexity upper bounds of $\tilde{\mathcal{O}}(n^{1/4}/\varepsilon^{1/2})$ for monotonicity testing [18] and of $\tilde{\mathcal{O}}((k/\varepsilon)^{1/2})$ for k-junta testing [6] are known. However, to the best of our knowledge, the "correct" ε-scaling for quantum property testing of classical functions is far from understood; prior works such as [13, 33, 38, 2, 6, 81] seem to establish quantum query complexity lower bounds only for constant ε.

1.5 Outlook and future directions

Here we lay out some directions for future work.

More and improved bounds for passive quantum property testing. We have established upper bounds for passive quantum testing of monotonicity, symmetry, and triangle-freeness from function states. These three properties together with linearity testing [19] and junta testing [13, 6] already demonstrate the power of quantum data for testing a variety of quite different properties, and it seems important to explore quantum datasets in the context of other testing problems. As highlighted in Table 1, quantum low-degree testing of Boolean functions is a natural next challenge, with the more general class of locally characterized affine-invariant properties [20] as a longer-term goal.

One may aim to tighten our bounds to precisely pin down the power of quantum data for these testing tasks. Here, having established that the constructions from classical passive monotonicity testing lower bounds are inadequate for the quantum case, we consider it especially interesting to obtain a n-dependent lower bound for passive quantum monotonicity testing in the constant ε regime. Settling the n-dependence of the quantum sample complexity for passive quantum monotonicity testing is a tantalizing question for future work.

Characterizing properties with constant-complexity passive quantum testers. In the classical case, [27] gave a complete characterization of those properties that can be tested with a constant number of samples. Achieving an analogous characterization for properties that can be tested from constantly-many function state copies would help demarcate the boundary of quantum advantage for this model.

The quantum case raises a further question about the constant complexity regime: For properties that admit a constant-copy passive quantum testers, can this always be achieved by algorithms that do not use entangled multi-copy measurements? The role of single- versus multi-copy quantum processing has recently been explored in the literature on learning and testing for quantum objects (see, e.g., [42, 68, 36, 67]) and in quantum computational learning theory [10], but the picture is far from clear for properties of function states (and of pure states more generally). Concretely, while our testers for monotonicity and symmetry are single-copy algorithms, our triangle-freeness tester uses two-copy SWAP tests and there does not seem to be an immediate way of replacing this by single-copy quantum processing.

One may also ask about the necessity of auxiliary systems in quantum sample-based testers with constant sample complexity; for example, our symmetry tester relied on auxiliary systems to implement the symmetric subspace projector. The number of available auxiliary systems is already known to play an important role in, for instance, Pauli channel learning [41, 40, 43], and exploring its relevance for constant-complexity passive quantum testing may shed new light on how these quantum testers achieve their better-than-classical performance.

Other quantum datasets for classical properties. We have considered only one kind of quantum representation of classical functions: coherent superpositions of evaluations of f (as function states). Already these are enough to gain major advantages over testing from classical data, but one could ask for more. Are there other, better quantum datasets that lead to even faster testers or extend quantum advantage to more properties? To keep this question interesting, one would require that the dataset be not too tailored to any property.

In fact, this question may be best phrased as a sort of "compression game": we are first given a very long list of questions that we might be asked regarding some black-box function f. We then have $T(n)$ time to interact with an oracle for f, during which period we generate whatever data we would like. What is the best quantum dataset to generate, so that we are best prepared to answer a random (or perhaps worst-case) question from the list?

Passive quantum testing for quantum properties. Recently there is a growing interest in property testing for quantum objects, such as states [64, 83, 63, 35, 15, 62, 92, 42, 61, 11, 45, 9, 16], unitaries [49, 46, 90], channels [42, 3, 17], and Hamiltonians [76, 28, 12]. It is an interesting challenge to design datasets to enable passive versions of these tasks. Just as above, we would want quantum datasets that are agnostic to the property to be tested.

Some existing work can be viewed as advocating for quantum datasets. When restricting ourselves to collecting classical data, classical shadows [70, 69] serve as a useful representation, but place restrictions on the properties that can be tested after-the-fact. Shadow tomography procedures [1, 14, 36] can remove such restrictions but use multi-copy measurements that depend on the properties of interest, and thus in general seem to require quantum data storage to enable passivity.[5] The relevance of data storage in a quantum memory for certain quantum process learning tasks has also been explored in [22, 23, 89, 78, 77]. In this context, our work can be viewed as investigating the power of quantum data, stored in quantum

[5] (Non-adaptive) Pauli shadow tomography [71, 36, 75, 44] in some sense interpolates between the (dis-)advantages of classical shadows and shadow tomography for the current discussion: When promised in advance that the properties in question are characterized by expectation values of arbitrary Pauli observables, some of the relevant data can be collected and stored classically in advance, without knowing which specific Pauli observables matter. However, part of the quantum processing still requires knowing the specific Paulis of interest, so to achieve passivity, it seems that some data still has to be stored quantumly.

memory, for testing properties of diagonal unitary processes arising from classical Boolean functions. We hope that this will inspire future attempts at using quantum data as a resource for passively quantumly testing properties of more general quantum processes.

2 Passive quantum testing upper bounds

2.1 Defining passive quantum property testing

As outlined in Section 1, passive property testing considers testing from (non-adaptively chosen) data that does not depend on the property to be tested. We propose a quantum version of this model by considering quantum testing algorithms that have access to copies of a quantum data state. Here, we consider the following form of quantum data encoding for a Boolean function $f : \{0,1\}^n \to \{0,1\}$: We work with *function states*

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

We now formally define the notion of passive quantum property testing for Boolean functions.

▶ **Definition 6** (Passive quantum property testing). *Let $\mathcal{P}_n \subseteq \{0,1\}^{\{0,1\}^n}$ be some property of Boolean functions on n bits, let $\delta, \varepsilon \in (0,1)$. A quantum algorithm is a* passive quantum tester *with accuracy/distance parameter ε and confidence parameter δ for $\mathcal{P}_n$ from $m = m(\varepsilon,\delta)$ function state copies if the following holds: When given m copies of $|\Psi_f\rangle$, the quantum algorithm correctly decides, with success probability $\geq 1-\delta$, whether*

(i) *$f \in \mathcal{P}_n$, or*
(ii) *$\Pr_{x\sim\{0,1\}^n}[f(x) \neq g(x)] \geq \varepsilon$ holds for all $g \in \mathcal{P}_n$,*

promised that f satisfies either (i) or (ii).

This work explores Definition 6 in the context of several properties. We develop testers for monotonicity, symmetry, and triangle-freeness. The main ideas underlying our algorithms are introduced in Section 2.2. The next section presents the passive quantum monotonicity tester in detail, while the symmetry and triangle-freeness testers are deferred to [37, Appendix A.2].

2.2 Passive quantum monotonicity testing

We define the natural partial order $\preceq$ on the Boolean hypercube $\{0,1\}^n$ via $x \preceq y :\Leftrightarrow (x_i \leq y_i$ holds for all $1 \leq i \leq n)$. A function $f : \{0,1\}^n \to \{0,1\}$ is called monotone if $f(x) \leq f(y)$ holds for all $x, y \in \{0,1\}^n$ with $x \preceq y$. The associated classical testing problem can be formulated as follows:

▶ **Problem 7** (Classical monotonicity testing). *Given query access to an unknown function $f : \{0,1\}^n \to \{0,1\}$ and an accuracy parameter $\varepsilon \in (0,1)$, decide with success probability $\geq 2/3$ whether*

(i) *f is monotone, or*
(ii) *f is ε-far from all monotone functions, that is, we have $\Pr_{x\sim\{0,1\}^n}[f(x) \neq g(x)] \geq \varepsilon$ for all monotone functions $g : \{0,1\}^n \to \{0,1\}$,*

promised that f satisfies either (i) or (ii).

Here, as well as in our other property testing tasks below, will think of (i) as the accept case and of (ii) as the reject case. This then allows us to speak of completeness (for getting case (i) right) and soundness (for getting case (ii) right). Here, the chosen success probability of $2/3$ is an arbitrary constant $> 1/2$, it can be boosted arbitrarily close to 1 through repetition and majority voting.

Functions far from the set of all monotone functions necessarily violate monotonicity on a non-negligible fraction of all possible x and i. This makes it possible to test for monotonicity by checking for violations on a small number of randomly chosen x and i.

▶ **Theorem 8** (Soundness of monotonicity testing (compare [58])). *If $f : \{0,1\}^n \to \{0,1\}$ is exactly ε-far from all monotone functions, then*

$$\frac{\varepsilon}{n} \leq \Pr_{x\sim\{0,1\}^n, i\sim[n]}\left[(x_i = 0 \wedge f(x) = 1 \wedge f(x+e_i) = 0) \vee (x_i = 1 \wedge f(x) = 0 \wedge f(x+e_i) = 1)\right] \leq 2\varepsilon\,. \tag{2}$$

Therefore, we can solve Problem 7 from only $\mathcal{O}(n/\varepsilon)$ many queries to the unknown function, which was exactly the celebrated conclusion of [58]. While this query complexity does depend on n, the dependence is only logarithmic in the size of the function domain, and it in particular is exponentially better than the n-dependence in the query complexity of learning monotone functions [29].

Our passive quantum monotonicity tester also crucially relies on Theorem 8. Here, we first reinterpret the probability appearing in Equation (2) in terms of Fourier-analytic quantities, which we then estimate based on quantum Fourier sampling. Our procedure is summarized in Algorithm 1, and our next theorem establishes that it is both complete and sound.

Algorithm 1 Monotonicity testing from quantum examples.

Input: accuracy parameter $\varepsilon \in (0,1)$; confidence parameter $\delta \in (0,1)$; $\tilde{\mathcal{O}}\left(\frac{n^2\log(1/\delta)}{\varepsilon^2}\right)$ many copies of a function state $|f\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x, f(x)\rangle$.
Output: "accept" or "reject".
Initialization: $\varepsilon_2 = \frac{\varepsilon}{3}$, $\varepsilon_5 = \frac{\varepsilon}{3n}$, $\delta_1 = \delta_2 = \frac{\delta}{3}$, $\delta_5 = \frac{\delta}{3n}$, $m_1 = \max\{3m_2, \lceil 18\ln(2/\delta_1)\rceil\}$, $m_2 = \left\lceil \frac{n^2\ln(2/\delta_2)}{2\varepsilon_2^2}\right\rceil$, $m_4 = m_5 = \left\lceil\frac{4\ln(2/\delta_5)}{\varepsilon_5^2}\right\rceil$

1: Use m_1 many copies of $|f\rangle$ to produce m_2 many Fourier samples $S_1, \ldots, S_{m_2} \subseteq [n]$ from $g = (-1)^f$.
2: Take $\hat{\mathbf{I}} = \frac{1}{m_2}\sum_{\ell=1}^{m_2}|S_\ell|$.
3: Use m_4 many copies of $|f\rangle$ to generate m_5 many classical samples $(x_1, f(x_1)), \ldots, (x_{m_5}, f(x_{m_5})$ from f.
4: **for** $1 \leq i \leq n$ **do**
5: Take $\tilde{g}_i = \frac{1}{m_5}\sum_{k=1}^{m_5}(-1)^{x_k\cdot e_i + f(x_k)}$.
6: **end for**
7: Set $\hat{p} = \frac{1}{2n}\hat{\mathbf{I}} - \frac{1}{2n}\sum_{i=1}^n \tilde{g}_i$.
8: If $\hat{p} \leq \varepsilon/3n$, conclude that f is monotone and accept. If $\hat{p} \geq 2\varepsilon/3n$, conclude that f is ε-far from all monotone functions and reject.

▶ **Theorem 9** (Passive quantum monotonicity testing). *Algorithm 1 is an efficient quantum algorithm that uses $\tilde{\mathcal{O}}\left(\frac{n^2\log(1/\delta)}{\varepsilon^2}\right)$ copies of $|f\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x, f(x)\rangle$ to decide, with success probability $\geq 1-\delta$, whether f is monotone or ε-far from monotone.*

In particular, Theorem 9 shows that passive quantum testers can exponentially outperform the classical passive monotonicity testing lower bound of $\exp\left(\Omega\left(\min\{\sqrt{n}/\varepsilon, n\}\right)\right)$ [58, 24].

Proof. We begin with a useful rewriting of the probability from Equation (2). To this end, as is commonly done in the analysis of Boolean functions, consider the induced function $g : \{-1,1\}^n \to \{-1,1\}$ obtained from f via the relabeling $0 \leftrightarrow 1$ and $1 \leftrightarrow -1$. Next, we recall the definition of the ith derivative in Boolean analysis (compare, *e.g.*, [82, Definition 2.16]): For $i \in [n]$,

$$D_i g(x) \coloneqq \frac{g(x^{(i\mapsto 1)}) - g(x^{(i\mapsto -1)})}{2},$$

where we used the notation $x^{(i\mapsto b)}$ to denote the n-bit string obtained from x by replacing the ith bit with b. Consequently, we can compute

$$\begin{aligned}\frac{(D_i g(x))^2 - D_i g(x)}{2} &= \begin{cases} 1 & \text{if } g(x^{(i\mapsto 1)}) = -1 \wedge g(x^{(i\mapsto -1)}) = 1 \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & \text{if } f(x^{(i\mapsto 0)}) = 1 \wedge f(x^{(i\mapsto 1)}) = 0 \\ 0 & \text{otherwise} \end{cases}.\end{aligned}$$

Therefore, we can now rewrite our probability of interest as

$$\begin{aligned}&\Pr_{x\sim\{0,1\}^n, i\sim[n]}\left[(x_i = 0 \wedge f(x) = 1 \wedge f(x+e_i) = 0) \vee (x_i = 1 \wedge f(x) = 0 \wedge f(x+e_i) = 1)\right] \\ &= \mathbb{E}_{x\sim\{0,1\}^n, i\sim[n]}\left[\frac{(D_i g(x))^2 - D_i g(x)}{2}\right] \\ &= \frac{1}{2}\mathbb{E}_{i\sim[n]}\mathbb{E}_{x\sim\{0,1\}^n}\left[(D_i g(x))^2\right] - \frac{1}{2}\mathbb{E}_{i\sim[n]}\mathbb{E}_{x\sim\{0,1\}^n}\left[D_i g(x)\right] \\ &= \frac{1}{2}\mathbb{E}_{i\sim[n]}\left[\mathbf{Inf}_i[g]\right] - \frac{1}{2n}\sum_{i=1}^{n}\widehat{g}(\{i\}) \\ &= \frac{1}{2n}\mathbf{I}[g] - \frac{1}{2n}\sum_{i=1}^{n}\widehat{g}(\{i\}),\end{aligned}$$

where the second-to-last step used the definition of the ith influence (compare [82, Definition 2.17]) as well as [82, Proposition 2.19], and where the last step used the definition of the total influence (compare [82, Definition 2.27]).

With this rewriting established, let us first analyze the probabilities that the different steps of Algorithm 1 succeed and discuss what this implies for the estimator $\hat{p}$. Then, we will see how this gives rise to completeness and soundness. We have the following:

- Using the procedure of [19], one copy of $|f\rangle$ suffices to produce one Fourier sample from $g = (-1)^f$ – an n-bit string sampled from the probability distribution $\{|\hat{g}(S)|^2\}_{S\subseteq[n]}$ – with success probability $1/2$. Additionally, one knows whether the sampling attempt was successful.[6] So, by simply repeating the above m_1 many times, we see that Step 1 succeeds in producing m_2 Fourier samples with success probability $\geq 1 - \delta_1$.
- By a Chernoff-Hoeffding bound, we have $|\hat{\mathbf{I}} - \mathbb{E}_{S\sim\mathcal{S}_g}[|S|]| \leq \varepsilon_2$ with success probability $\geq 1 - \delta_2$. Here, $\mathcal{S}_g$ denotes the Fourier distribution of g, defined via $\mathcal{S}_g(S) = |\widehat{g}(S)|^2$.
- For any $1 \leq i \leq n$, by a standard Chernoff-Hoeffding bound, Step 5 produces a ε_5-accurate estimate $\tilde{g}_i$ of $\widehat{g}(\{i\})$ with probability $\geq 1 - \delta_5$.

[6] To see this, note that the procedure works as follows: Apply $H^{\otimes(n+1)}$; measure the last qubit; abort if that produces a 0, continue if produces a 1; measure the first n qubits to produce an n-bit string.

Therefore, by a union bound, we have that, with overall success probability $\geq 1-(\delta_1+\delta_2+n\delta_5)=1-\delta$, the estimates $\hat{\mathbf{I}}$ and $\tilde{g}_i$ simultaneously satisfy $|\hat{\mathbf{I}}-\mathbb{E}_{S\sim\mathcal{S}_g}[|S|]|\leq\varepsilon_2$ and $|\tilde{g}_i-\widehat{g}(\{i\})|\leq\varepsilon_5$ for all $1\leq i\leq n$. We condition on this high probability success event for the rest of the proof. In this event, our rewriting of the probability of interest from the beginning of the proof implies:

$$\begin{aligned}
&\left|\Pr_{x\sim\{0,1\}^n,i\sim[n]}[(x_i=0\wedge f(x)=1\wedge f(x+e_i)=0)\vee(x_i=1\wedge f(x)=0\wedge f(x+e_i)=1)]-\hat{p}\right|\\
&\leq\frac{1}{2n}\left|\mathbf{I}[g]-\hat{\mathbf{I}}\right|+\frac{1}{2n}\sum_{i=1}^{n}|\widehat{g}(\{i\})-\tilde{g}_i|\\
&=\frac{1}{2n}\left|\mathbb{E}_{S\sim\mathcal{S}_g}[|S|]-\hat{\mathbf{I}}\right|+\frac{1}{2n}\sum_{i=1}^{n}|\widehat{g}(\{i\})-\tilde{g}_i|\\
&\leq\frac{\varepsilon_2}{2n}+\frac{\varepsilon_5}{2}\leq\frac{\varepsilon}{3n}\,,
\end{aligned}$$

where we used the identity $\mathbf{I}[g]=\mathbb{E}_{S\sim\mathcal{S}_g}[|S|]$ (compare [82, Theorem 2.38]). So, we see that $\hat{p}$ is a $(\varepsilon/3n)$-accurate estimate for our probability of interest.

To prove completeness of Algorithm 1, assume f to be monotone. Then, Theorem 8 together with the above inequality imply that $\hat{p}\leq\varepsilon/3n\leq\varepsilon/2n$, and thus the final step in Algorithm 1 correctly concludes that f is monotone and accepts.

To prove soundness, assume f to be ε-far from monotone. Then, the lower bound in Theorem 8 together with the above inequality implies that $\hat{p}\geq 2\varepsilon/3n$, and thus the final step in Algorithm 1 correctly concludes that f is ε-far from monotone and rejects.

The overall number of copies of $|f\rangle$ used by the algorithm is m_1+m_4. Plugging in the choices of the different m_i, we see that

$$\begin{aligned}
m_1+m_4&\leq\max\{3m_2,\lceil 18\ln(2/\delta_1)\rceil\}+\left\lceil\frac{4\ln(2/\delta_5)}{\varepsilon_5^2}\right\rceil\\
&\leq\max\left\{3\left\lceil\frac{n^2\ln(2/\delta_2)}{2\varepsilon_2^2}\right\rceil,\lceil 18\ln(2/\delta_1)\rceil\right\}+\left\lceil\frac{36n^2\ln(6n/\delta)}{\varepsilon^2}\right\rceil\\
&\leq\max\left\{3\left\lceil\frac{9n^2\ln(6/\delta)}{2\varepsilon^2}\right\rceil,\lceil 18\ln(6/\delta)\rceil\right\}+\left\lceil\frac{36n^2\ln(6n/\delta)}{\varepsilon^2}\right\rceil\\
&\leq\tilde{\mathcal{O}}\left(\frac{n^2\log(1/\delta)}{\varepsilon^2}\right),
\end{aligned}$$

where the $\tilde{\mathcal{O}}$ hides a logarithmic dependence on n.

The quantum computational efficiency of Algorithm 1 follows immediately from the efficiency of quantum Fourier sampling. The classical computational efficiency is immediately apparent from our sample complexity bounds and the fact that the classical computation is dominated by the complexity of computing the empirical averages in Steps 2 and 4. ◀

We note that because of the second inequality in Theorem 8, the above procedure and proofs can be modified to quantumly efficiently solve the *tolerant* version (as defined in [84]) of the monotonicity testing problem – *i.e.*, distinguishing between f being ε_1-close or ε_2-far from monotone – using $\tilde{\mathcal{O}}\left(\frac{n^2\log(1/\delta)}{(\varepsilon_2-\varepsilon_1)^2}\right)$ copies of a quantum function state, assuming that $\varepsilon_2>Cn\varepsilon_1$ holds with $C>1$ some constant.[7] Because of this assumption on how ε_1 and ε_2 relate, this still falls short of a general tolerant passive quantum monotonicity tester.

[7] In more generality, one can see: If an inequality like Equation (2) holds with lower bound $\ell_n(\varepsilon)$ and upper bound $u_n(\varepsilon)$, satisfying $\ell_n(0)=0=u_n(0)$, then estimating the relevant probability to accuracy $\sim\ell_n(\varepsilon_2-\varepsilon_1)$ suffices for tolerant property testing in the parameter range where there is a constant $c\in(0,1/2)$ such that $\ell_n(\varepsilon_2)-c\cdot\ell_n(\varepsilon_2-\varepsilon_1)>u_n(\varepsilon_1)+c\cdot\ell_n(\varepsilon_2-\varepsilon_1)$.

Let us also note room for a qualitative improvement in our passive quantum monotonicity tester. Classical query-based testers typically enjoy perfect completeness, *i.e.*, accept monotone functions with unit probability. In contrast, our tester can be made to accept monotone functions with probability arbitrarily close but not equal to 1. We leave open whether our passive quantum monotonicity tester can be modified to achieve perfect completeness, while enjoying similar guarantees on the quantum sample and time complexity of the procedure.

3 Fourier sampling does not suffice

The passive quantum testers for symmetry and triangle-freeness in [37, Appendix A] do not use quantum Fourier sampling. One might ask if this is necessary, given that Fourier sampling (augmented by classical samples) suffices for so many other learning and testing tasks. This section presents a class of functions, Maiorana–McFarland bent functions, which can be tested with $\mathcal{O}(1)$ function state copies, but any algorithm relying solely on Fourier samples and classical samples requires exponentially many classical samples to succeed.

The *Maiorana–McFarland (MM)* functions [34, Section 6.1] on $2n$ bits, denoted MM_n, are given by ${}_h : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, $(x, y) \mapsto \langle x, y\rangle + h(x)$, where h ranges over all functions $\mathbb{F}_2^n \to \mathbb{F}_2$. MM functions are a subset of the class of *bent* Boolean functions $g : \{0,1\}^m \to \{0,1\}$, those with $\widehat{g}(S)^2 = 1/2^m$ for all $S \subset [m]$ (so they are maximally-far from any $\mathbb{F}_2^n$-linear function). MM functions were also recently used to prove an exponential separation between classical query complexity and a single quantum query in zero-error quantum computation [55].

We begin by proving hardness of testing MM_n using only classical samples $\big(x, f(x)\big)$ and Fourier samples.

▶ **Theorem 10.** *Suppose a tester for* MM_n *using exclusively classical samples and Fourier samples succeeds with probability more than* $1/2 + 2^{-0.7n}$ *for the accuracy parameter* $\varepsilon = 1/2 - 2^{-0.3n}$*. Then the tester uses at least* $2^{0.1n}$ *classical samples.*

Proof. Define $\mathcal{H}$ be the set of Boolean functions on n bits with bias at most $2^{-n/3}$. From Chernoff we have that for uniformly random $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the bias almost always satisfies this bound:

$$\Pr_f \left[\left| \mathop{\mathbb{E}}_x \left[(-1)^{f(x)} \right] \right| \geq 2^{-n/3} \right] \leq \exp(-\mathsf{const} \cdot 2^{n/3}) \,. \tag{3}$$

Now consider the two ensembles of Boolean functions $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$

$$\mathcal{F}_1 = \big\{(x,y) \mapsto \langle x, y\rangle + h(x)\big\}_{h\sim\mathcal{H}} \qquad \text{and} \qquad \mathcal{F}_2 = \big\{(x,y) \mapsto \langle x, y\rangle + h(y)\big\}_{h\sim\mathcal{H}} \,,$$

Note that for any $f = \langle x, y\rangle + h(x) \in \mathrm{MM}_n$ and any $g = \langle x, y\rangle + m(y) \in \operatorname{supp} \mathcal{F}_2$,

$$\left| \mathop{\mathbb{E}}_{x,y} (-1)^{f(x,y)} (-1)^{g(x,y)} \right| = \left| \mathop{\mathbb{E}}_{x,y} (-1)^{h(x)} (-1)^{m(y)} \right| = |\mathrm{bias}(h)\mathrm{bias}(m)| \leq 2^{-n/3} \,.$$

Thus all $g \in \operatorname{supp} \mathcal{F}_2$ are at least $(1/2 - 2^{-n/3})$-far from $\mathrm{MM}_n \supseteq \operatorname{supp} \mathcal{F}_1$.

Suppose a testing algorithm A using $R \leq 2^{0.1n}$ classical samples succeeds with probability δ. This means that, given access to a function drawn uniformly at random from $\mathcal{F}_1$ or from $\mathcal{F}_2$ with equal probability, the algorithm A can guess which of the two ensembles the function was drawn from with success probability at least δ.

Define $\widetilde{\mathcal{F}}_1$ (resp. $\widetilde{\mathcal{F}}_2$) to be $\mathcal{F}_1$ (resp. $\mathcal{F}_2$) but where h is drawn uniformly at random from all Boolean functions. Because of the bound (3), we know

$$\left| \Pr_{f\sim\widetilde{\mathcal{F}}_1} [A \text{ accepts } f] - \Pr_{f\sim\mathcal{F}_1} [A \text{ accepts } f] \right| \leq \exp(-\mathsf{const} \cdot 2^{-n/3}),$$

and similarly for $\mathcal{F}_2, \widetilde{\mathcal{F}}_2$. This means that in the $\widetilde{\mathcal{F}}$ version of the distinguishing game, A succeeds with probability at least $\delta - \exp(-\mathsf{const} \cdot 2^{-n/3})$.

Let $b \sim \{1,2\}$ and $f \sim \mathcal{F}_b$. With probability at least $1 - R^2/2^n$, all $x^{(r)}$'s and all $y^{(r)}$'s in the R-many samples are distinct (collision bound and union bound). Call this event D. Conditioned on D, the distribution of observed values $\left(f(x^{(1)}, y^{(1)}), \ldots, f(x^{(R)}, y^{(R)})\right)$ is uniformly random because in $\widetilde{\mathcal{F}}_b$, h is a uniformly random Boolean function. Thus conditioned on D, the data observed is independent of b. Moreover, all functions under consideration are bent, so Fourier sampling provides no information whatsoever. The distinguishing probability is thus bounded by:

$$\delta \leq \Pr[D] \cdot \frac{1}{2} + \Pr[D^c] \cdot 1 + e^{-\mathsf{const} \cdot 2^{-n/3}} \leq \frac{1}{2} + \frac{R^2}{2^n} + e^{-\mathsf{const} \cdot 2^{-n/3}} \leq \frac{1}{2} + 2^{-0.7n}$$

for n large enough. ◀

Having established that the MM class is hard to test from classical samples and Fourier samples alone, we now give a very efficient passive quantum tester for MM_n. While this tester still uses quantum Fourier sampling at the end of the algorithm, it crucially preprocesses the function state in superposition before applying performing Fourier sampling.

▶ **Theorem 11.** *There is an efficient quantum algorithm that uses $\mathcal{O}(1)$ copies of the function state $|f\rangle = \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} |x, y, f(x,y)\rangle$ to decide, with success probability $\geq 2/3$, whether f is in MM_n or $(1/3)$-far from MM_n.*

Proof. Let U denote the $(2n+1)$-qubit unitary acting as $|x, y, b\rangle \mapsto |x, y, b \oplus \langle x, y\rangle\rangle$. Note that U can be implemented by a quantum circuit with $\mathcal{O}(n)$ many 2-qubit gates and depth $\mathcal{O}(\log n)$. Moreover, notice that $U|f\rangle = |\tilde{f}\rangle$ for $\tilde{f}(x,y) := f(x,y) \oplus \langle x, y\rangle$.

The quantum algorithm works as follows. Recall that one function state copy suffices to obtain one Fourier sample with success probability $1/2$, using only $2n$ many single-qubit gates. Applying this subroutine to $\mathcal{O}(1)$ copies of $U|f\rangle$ thus suffices to obtain, with success probability $\geq 5/6$, $m \geq C$ many Fourier samples $S_1, \ldots, S_m \subseteq [2n]$ of the function $\tilde{f}$, where $C > 0$ is a universal constant to be chosen later. Let $J = \{n+1, n+2, \ldots, n\}$ and compute

$$\hat{p} = \frac{1}{m} \left| \left\{ 1 \leq k \leq m : J \cap S_k \neq \emptyset \right\} \right| .$$

If $\hat{p} \leq 1/9$, output "$f \in \mathrm{MM}_n$". Otherwise, output "f is $(1/3)$-far from MM_n."

First, let us show completeness of the protocol. So, suppose $f \in \mathrm{MM}_n$. Then there is a function $h : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$U|f\rangle = \frac{1}{2^n} \sum_{x,y} |x, y, h(x)\rangle = |h\rangle ,$$

where we abused notation by using h to denote the function $h : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ defined as $h(x,y) = h(x)$. As $h(x,y)$ depends only on the first n variables, we have

$$p := \sum_{S \subseteq [2n],\, J \cap S \neq \emptyset} |\hat{h}(S)|^2 = 0 .$$

The constant C can be chosen such that, conditioned on the high probability event that we obtained at least C many Fourier samples, we have $|p - \hat{p}| \leq 1/9$ with probability $\geq 5/6$ (by Chernoff-Hoeffding). So $\hat{p} \leq 1/9$, and our tester correctly outputs "$f \in \mathrm{MM}_n$" with probability $\geq 2/3$.

Next, we analyze soundness. Suppose f is (1/3)-far from MM_n. Equivalently, $\tilde{f}(x,y) = f(x,y) \oplus \langle x,y \rangle$ is (1/3)-far from any Boolean h that depends only on the first n variables, $h(x,y) = h(x)$, where we again abused notation. Consider the function g defined as

$$g(x,y) = \sum_{S \subseteq [2n] : J \cap S = \emptyset} \hat{\tilde{f}}(S) \chi_S(x,y)\,.$$

Notice that $g(x,y)$ depends only on x, but g is in general not Boolean. Define $\tilde{g}(x,y) = \mathbf{1}_{g(x,y) \geq 1/2}$. Notice that $\tilde{g}$ is a Boolean function and that $\tilde{g}(x,y)$ depends only on x. Then (compare [13, Fact II.2]) we have

$$\frac{1}{3} \leq \mathbb{P}_{x_1,x_2}[\tilde{f}(x_1,x_2) \neq \tilde{g}_2(x_2)] \leq \mathbb{E}_{x_1,x_2}[(\tilde{f}(x_1,x_2) - g(x_1,x_2))^2] = \sum_{\substack{S \subset [2n]: \\ J \cap S \neq \emptyset}} \left|\hat{\tilde{f}}(S)\right|^2 = p\,.$$

Again, conditioned on having produced at least C many Fourier samples, with probability $\geq 5/6$, we have $|p - \hat{p}| \leq 1/9$ and thus $\hat{p} \geq 2/9$. So, our tester correctly outputs "f is (1/3)-far from MM_n" with probability $\geq 2/3$. ◀

4 Separating passive quantum from query-based classical property testing

In this section we give a property for which classical queries have exponential advantage over quantum testing from function states. This property is closely related to the inability of quantum computers to measure the intersection of three subset states, where for a subset $S \subseteq \mathbb{F}_2^n$, the corresponding subset state is defined as $|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle$. We explain this connection at the end of the section.

The main result of this section is the following theorem.

▶ **Theorem 12.** *There exist two sets of Boolean functions F_0, F_1 such that*

$$\min_{f_0 \in F_0, f_1 \in F_1} \|f_0 - f_1\|_1 \geq \frac{1}{64}$$

and such that:

- *Any passive quantum tester requires $\Omega(2^{n/2})$ copies of a function state to distinguish F_0 and F_1 with constant probability 2/3.*
- *F_0 and F_1 may be distinguished with probability 2/3 from $\mathcal{O}(1)$ classical queries.*

The families F_0 and F_1 arise from certain encodings of triples of subsets $A, B, C \subseteq \{0,1\}^n$. Consider the class of Boolean functions $f_{(A,B,C)} : \{0,1\}^{n+2} \to \{0,1\}$ on $n+2$ bits parameterized by subsets $A, B, C \subseteq \{0,1\}^n$ and defined as follows:

$$f_{(A,B,C)}(x,a) = \begin{cases} \mathbf{1}_{x \in A} & a = 00 \\ \mathbf{1}_{x \in B} & a = 01 \\ \mathbf{1}_{x \in C} & a = 10 \\ 0 & a = 11 \end{cases}.$$

With A, B, C drawn uniformly from subsets of $\{0,1\}^n$, we define two function state ensembles $\{|f_{(A,B,C)}\rangle\}_{A,B,C}$ and $\{|f_{(A,B,A\Delta B)}\rangle\}_{A,B}$, with their mixed state average over t-copy states given by

$$\mathcal{E}_0 = \mathop{\mathbb{E}}_{A,B,C} \left[\left|f_{(A,B,C)}\right\rangle \left\langle f_{(A,B,C)}\right|^{\otimes t} \right], \qquad \mathcal{E}_1 = \mathop{\mathbb{E}}_{A,B} \left[\left|f_{(A,B,A\Delta B)}\right\rangle \left\langle f_{(A,B,A\Delta B)}\right|^{\otimes t} \right].$$

We now show that these two mixed state averages over t-copy states are close in trace distance unless t scales exponentially in n. This means that exponentially-in-n many copies are needed to distinguish between the two function state ensembles.

▶ **Theorem 13.** $\|\mathcal{E}_0 - \mathcal{E}_1\|_1 \leq \mathcal{O}(t/2^{n/2})$.

Proof. It will help to reinterpret $\left|f_{(A,B,C)}\right\rangle$ as a subset state via the rewriting

$$|x,a\rangle\left|f_{(A,B,C)}(x,a)\right\rangle = \sum_{b\in\{0,1\}} \mathbf{1}_{x\in S_{a,b}} |x,(a,b)\rangle\,, \tag{4}$$

where $S_{a,b}$ denotes A, B, C, or $\emptyset$ according to a when $b = 1$, or the respective complements if $b = 0$. Using r to represent the concatenation of a and b we may then write

$$\left|f_{(A,B,C)}\right\rangle = \frac{1}{\sqrt{4N}} \sum_{r\in\{0,1\}^3} \sum_{x\in\{0,1\}^n} \mathbf{1}_{x\in S_r} |x,r\rangle\,,$$

where $N := 2^n$ and, like before, S_r denotes one of A, B, C, or $\emptyset$ or the complements thereof.

With this notation let us consider the basis for the space of t copies of function states given by

$$\left\{ |x_1,r_1,\ldots,x_t,r_t\rangle : x_j \in \{0,1\}^n, r_j \in \{0,1\}^3, j = 1,\ldots,t \right\}.$$

Let Π denote the projector onto the subspace spanned by those $|x_1,r_1,\ldots,x_t,r_t\rangle$ for which all x_j are distinct.

First, we claim

$$\|\mathcal{E}_0 - \Pi\mathcal{E}_0\Pi\|_1,\ \|\mathcal{E}_1 - \Pi\mathcal{E}_1\Pi\|_1 \ \leq\ \mathcal{O}\left(\frac{t}{\sqrt{N}}\right). \tag{5}$$

These bounds follow from applying the triangle inequality to the following estimate: for any fixed A, B, C, we have

$$\left\| \left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t} - \Pi \left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t} \Pi \right\|_1 = \sqrt{\left(1 + 3\frac{4^t N^{\underline{t}}}{(4N)^t}\right)\left(1 - \frac{4^t N^{\underline{t}}}{(4N)^t}\right)} \tag{6}$$

$$\leq \frac{2t}{\sqrt{N}}\,, \tag{7}$$

where $(x)^{\underline{t}} = x(x-1)\ldots(x-t+1)$ denotes falling factorial, and where in the second step we applied the bound

$$\frac{4^t N^{\underline{t}}}{(4N)^t} \geq \left(1 - \frac{t}{N}\right)^t \geq 1 - \frac{t^2}{N}.$$

To see Equation (6), note that

$$M := \left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t} - \Pi \left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t} \Pi$$

has the following block form after reordering columns:

$$M = \frac{1}{(4N)^t} \underbrace{\left(\begin{array}{c|c|c} 0 & 1 & 0 \\ \hline 1 & 1 & 0 \\ \hline 0 & 0 & 0 \end{array}\right)}_{\substack{4^t N^{\underline{t}} \quad 4^t(N^t - N^{\underline{t}}) \quad (8N)^t - (4N)^t}} \begin{array}{l} \} 4^t N^{\underline{t}} \\ \} 4^t(N^t - N^{\underline{t}}) \\ \} (8N)^t - (4N)^t \end{array}.$$

This is because $\left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t}$ is an all-zeros matrix except for the principal submatrix associated to indices $\big((x_1,r_1),\dots,(x_t,r_t)\big)$ where $x_j \in S_{r_j}$ for all j, and here it is equal to $(4N)^{-t}$. There are $(4N)^t$ such entries. Moreover, $\Pi\left|f_{(A,B,C)}\right\rangle\left\langle f_{(A,B,C)}\right|^{\otimes t}\Pi$ is an all-zeros matrix except for the principal submatrix associated to indices $\big((x_1,r_1),\dots,(x_t,r_t)\big)$ where $x_j \in S_{r_j}$ for all j and $x_j \neq x_k$ for $j \neq k$ and here it is also equal to $(4N)^{-t}$ – and there are $4^t N^{\underline{t}}$ of these entries. M thus has rank 2 and its spectrum is easily determined, leading to the estimate in Equation (6).

Now we claim that in fact

$$\Pi\mathcal{E}_0\Pi = \Pi\mathcal{E}_1\Pi\,. \tag{8}$$

Let us consider a specific entry in $\Pi\mathcal{E}_0\Pi$ with row and column indices

$$\mathbf{r} = (\dots,(x_j,r_j),\dots), \qquad \mathbf{s} = (\dots,(y_j,s_j),\dots)\,.$$

It will be useful to write $\mathcal{S}_z = \mathcal{S}_z(\mathbf{r},\mathbf{s})$ for the set types that appear with a particular string $z \in \{0,1\}$ in $\mathbf{r}$ and $\mathbf{s}$. That is, for any $z \in \{0,1\}^n$ define

$$\mathcal{S}_z = \mathcal{S}_z(\mathbf{r},\mathbf{s}) = \big\{q \in \{0,1\}^3 : (z,q) \in \mathbf{r} \text{ or } (z,q) \in \mathbf{s}\big\}.$$

Then

$$\begin{aligned}\langle\mathbf{r}|\,\Pi\mathcal{E}_0\Pi\,|\mathbf{s}\rangle &= (4N)^{-t}\mathop{\mathbb{E}}_{A,B,C}\Big(\textstyle\prod_j \mathbf{1}_{x_j\in S_{r_j}}\Big)\Big(\prod_j \mathbf{1}_{y_j\in S_{s_j}}\Big)\\ &= (4N)^{-t}\prod_{z\in\{x_j\}_j\cup\{y_j\}_j}\mathop{\mathbb{E}}_{A,B,C}\textstyle\prod_{q\in\mathcal{S}_z}\mathbf{1}_{z\in S_q}\,.\end{aligned}$$

It follows from the definition of Π that $|\mathcal{S}_z| \le 2$ for any $z \in \{x_j\}_j \cup \{y_j\}_j$: there is at most one contribution to $\mathcal{S}_z$ from each of $\mathbf{r}$ and $\mathbf{s}$. As a result we have for any z that

$$\mathop{\mathbb{E}}_{A,B,C\overset{\text{iid}}{\sim}\mathcal{P}\{0,1\}^n}\textstyle\prod_{q\in\mathcal{S}_z}\mathbf{1}_{z\in S_q} = \mathop{\mathbb{E}}_{\substack{A,B\overset{\text{iid}}{\sim}\mathcal{P}\{0,1\}^n\\ C=A\Delta B}}\textstyle\prod_{q\in\mathcal{S}_z}\mathbf{1}_{z\in S_q}.$$

This follows from mild case analysis, the most important part of which is to note that for any $S \neq T \in \{A,B,C,A\Delta B\}$,

$$(\mathbf{1}_{x\in S},\mathbf{1}_{x\in T}) \sim (b_1,b_2),$$

where b_1 and b_2 are i.i.d. Bernoulli $1/2$ random variables. So we see $\langle\mathbf{r}|\,\Pi\mathcal{E}_0\Pi\,|\mathbf{s}\rangle = \langle\mathbf{r}|\,\Pi\mathcal{E}_1\Pi\,|\mathbf{s}\rangle$ and Equation (8) is satisfied.

Combining the triangle inequality with Equation (5) and Equation (8) gives the result. ◀

Proof of Theorem 12. Consider

$$F_0 = \big\{f_{(A,B,C)} : A,B,C \subseteq \{0,1\}^n, 2^{-n}|A\cap B\cap C| \ge 1/16\big\}$$

and $\quad F_1 = \big\{f_{(A,B,A\Delta B)} : A,B \subseteq \{0,1\}^n\big\},$

First we prove the minimum distance between F_0 and F_1. For any $f_0 \in F_0$, there are $2^n/16$ strings $x \in \{0,1\}^n$ such that $f_0(x00) = f_0(x01) = f_0(x10) = 1$. On the other hand, for all $f_1 \in F_1$, by definition there are no strings x with this property. Thus the minimum L^1 distance between F_0 and F_1 is at least

$$\frac{2^n/16}{4\cdot 2^n} = \frac{1}{64}\,.$$

Now define the state ensembles

$$\mathcal{E}_0' = \mathop{\mathbb{E}}_{f\sim F_0} |f\rangle\langle f|^{\otimes t} \quad \text{and} \quad \mathcal{E}_1 = \mathop{\mathbb{E}}_{f\sim F_1} |f\rangle\langle f|^{\otimes t}\,.$$

$\mathcal{E}_1$ here is exactly $\mathcal{E}_1$ from Theorem 13. To compare $\mathcal{E}_0'$ and $\mathcal{E}_0$ from Theorem 13, note that for $A, B, C \overset{\text{iid}}{\sim} \mathcal{P}\{0,1\}^n$, any string x is in $A \cap B \cap C$ with probability $1/8$ and so from Chernoff we have

$$\Pr\left[|A\cap B\cap C| < \frac{1}{2}\cdot\frac{2^n}{8}\right] \leq \exp\left(-\frac{2^n}{64}\right).$$

This dramatic concentration, together with Theorem 13 implies

$$\|\mathcal{E}_0' - \mathcal{E}_1\|_1 \leq \|\mathcal{E}_0' - \mathcal{E}_0\|_1 + \|\mathcal{E}_1 - \mathcal{E}_0\|_1 \leq \mathcal{O}(t/2^{n/2})\,.$$

To test this property with classical queries, given an unknown $f = f_{(A,B,C)}$ one may simply choose a random $x \in \{0,1\}^n$ and check if $f(x00) = f(x01) = f(x10) = 1$. This test accepts with probability $1/8$ when $f \in F_0$ and accepts with probability 0 when $f \in F_1$. ◀

k-fold intersection is "unfeelable" for $k \geq 3$

In this subsection, we reinterpret Theorem 12 in the context of subset states. Given access to copies of k different subset states $|S_1\rangle, \ldots, |S_k\rangle$, it is natural to ask how many copies of each are required to estimate the fractional size of the mutual intersection,

$$\frac{|S_1 \cap \cdots \cap S_k|}{2^n}.$$

When $k = 2$, this can be readily accomplished using ideas similar to our algorithms presented above. In the case of intersection estimation with $k = 2$, we have the identity

$$\frac{|S_1 \cap S_2|}{2^n} = \langle S_{\text{all}}|S_1\rangle\langle S_1|S_2\rangle\langle S_2|S_{\text{all}}\rangle\,,$$

where $S_{\text{all}} := \{0,1\}^n$ denotes the full hypercube. The quantities on the right-hand side are easily estimated via swap tests, so it takes $\mathcal{O}(1)$ copies of $|S_1\rangle, |S_2\rangle$ to estimate the quantity of interest to any constant additive error.

In contrast, as a consequence of Theorem 12, the same question for $k = 3$ has a very different answer: it requires $\Omega(2^{n/2})$ copies to achieve constant additive error. To see this, note that from any $|f_{(A,B,C)}\rangle$ one may obtain each of $|A\rangle$, $|B\rangle$, $|C\rangle$ with constant probability by measuring the a and $f(x,a)$ registers, provided that the minimum among $|A|$, $|B|$, and $|C|$ is at least a constant fraction of 2^n – and this condition is satisfied by the overwhelming majority of functions in the families F_0 and F_1 of Theorem 12. From F_0 and F_1 we obtain:

▶ **Corollary 14.** *There are two families $\mathcal{S}_0$ and $\mathcal{S}_1$ of triples of subsets of $\{0,1\}^n$ such that*

$$\forall (A_0,B_0,C_0) \in \mathcal{S}_0, \quad |A_0\cap B_0\cap C_0|/2^n \geq 1/16$$

and $$\forall (A_1,B_1,C_1) \in \mathcal{S}_1, \quad |A_1\cap B_1\cap C_1|/2^n = 0\,,$$

and yet any quantum algorithm distinguishing the two families via their subset states requires $\Omega(2^{n/2})$ copies of $|A\rangle, |B\rangle,$ or $|C\rangle$.

▶ Remark 15. In contrast to 3-fold intersection detection, 2-fold intersection detection is quantumly easy. 2-fold intersection detection from function states can be achieved with quantum Fourier sampling and exactly estimating the intersection $|A\cap B|/2^n$.

5 A challenge: lower bounds for monotonicity testing

We show that the ensembles used in [58] to establish lower bounds on monotonicity testing from samples do not improve upon the basic $\Omega(1/\varepsilon)$ quantum sample complexity lower bound. To prove this, we consider the pair of distributions over functions from [58], constructed such that one is supported entirely on monotone functions, and the other with high probability on functions that are ε-far from monotone. We show that the associated t-copy quantum function state ensembles become distinguishable with constant success probability as soon as $t = \Omega(1/\varepsilon)$. We sketch the ensembles used as well as the argument to bound the trace distance between the t-copy ensembles. We defer to full version [37] for the detailed argument.

We recall the *twin ensembles* from [58].

▶ **Definition 16** (Twin ensembles). *Let $M = \{(u_i, v_i)\}_{i=1}^m$ be a set of pairs of elements in $\{0,1\}^n$ s.t. all $u_1, v_1, \ldots, u_m, v_m$ are distinct. Let $\cup M := \cup_{(u,v)\in M}\{u, v\}$ be the complete set of elements in the matching. Fix a function $g : \{0,1\}^n \backslash (\cup M) \to \{0,1\}$. We now define the* twin ensembles *associated to M and g, which are two sets F_0, F_1 of functions on $\{0,1\}^n$.*

For any bipartition of M, $M = A \sqcup B$, define the following two functions.

1. *$f^{(0)}_{A,B}$ is defined as follows:*
   - *For $(u, v) \in A$, we set $f^{(0)}_{A,B}(u) = f^{(0)}_{A,B}(v) = 1$.*
   - *For $(u, v) \in B$, we set $f^{(0)}_{A,B}(u) = f^{(0)}_{A,B}(v) = 0$.*
   - *If $x \notin \cup M$, then define $f^{(0)}_{A,B}(x) = g(x)$.*
2. *$f^{(1)}_{A,B}$ is defined as follows:*
   - *For $(u, v) \in A$, we set $f^{(1)}_{A,B}(u) = 1$ and $f^{(1)}_{A,B}(v) = 0$.*
   - *For $(u, v) \in B$, we set $f^{(1)}_{A,B}(u) = 0$ and $f^{(1)}_{A,B}(v) = 1$.*
   - *If $x \notin \cup M$, then define $f^{(1)}_{A,B}(x) = g(x)$.*

The twin ensembles associated to M and g are $F_0 = \{f^{(0)}_{A,B}\}_{A\sqcup B=M}$ and $F_1 = \{f^{(1)}_{A,B}\}_{A\sqcup B=M}$.

All functions in F_0 are monotone, while with high probability, a uniformly random function from F_1 is $\Omega(\varepsilon)$-far from monotone [58].

For the quantum analysis it is convenient to work with *phase states*

$$|\Psi^{\mathrm{ph}}_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \ ,$$

which are unitarily equivalent to the usual function states, $|\Psi^{\mathrm{ph}}_f\rangle = (I^{\otimes n} \otimes H)\,|f\rangle$. A lower bound on the distinguishability of the phase state ensembles associated with F_0 and F_1 thus lifts to the distinguishability of the function states.

We show that, in contrast to the classical case analyzed in [58], the twin ensembles actually become quantumly distinguishable already for $t \sim 1/\varepsilon$. Namely, we prove:

▶ **Theorem 17.** *Define $\varepsilon > 0$ so that $\varepsilon 2^n = m = |M|$. Then*

$$\left\| \mathbb{E}_B \left[\left(|\Psi^{\mathrm{ph}}_{f^{(0)}_{A,B}}\rangle\langle\Psi^{\mathrm{ph}}_{f^{(0)}_{A,B}}| \right)^{\otimes t} \right] - \mathbb{E}_B \left[\left(|\Psi^{\mathrm{ph}}_{f^{(1)}_{A,B}}\rangle\langle\Psi^{\mathrm{ph}}_{f^{(1)}_{A,B}}| \right)^{\otimes t} \right] \right\|_1 \geq \Omega(1) \tag{9}$$

for $t = \Omega(1/\varepsilon)$.

We now sketch the argument and defer to [37] for the full proof. The difference matrix A between the t-copy averages of the phase state ensembles of F_0 and F_1 turns out to have a remarkable combinatorial structure. Each index $\mathbf{x}$ (which can be thought of as a t-tuple of integers) belongs to a well-defined equivalence class or "type" determined solely by the underlying matching $M = A \sqcup B$. Furthermore, every matrix entry $A_{(\mathbf{x},\mathbf{y})}$ depends only on a relationship between the types of $\mathbf{x}$ and $\mathbf{y}$. This then induces a block decomposition of A, indexed by the possible types. Within each block, the structure simplifies further – in particular, with each type, the block is the adjacency matrix of a complete bipartite graph. We can then exactly characterize the 1-norm of the matrix A by summing over the singular values of each of the blocks. We obtain the following expression for the trace norm:

$$\|A\|_1 = \Theta\big(1 - (1-2\varepsilon)^t\big) \pm o(1)\,.$$

When $t = \Omega(1/\varepsilon)$, we have $1 - (1-2\varepsilon)^t \geq \Omega(1)$. Hence, this construction cannot improve upon the trivial lower bound of $\Omega(1/\varepsilon)$ on the number of quantum copies required.

We can also extend the above analysis to the ensembles from [24]. The construction in [24], based on *Talagrand's random DNFs* [94], establishes a lower bound of $\exp(\Omega(\sqrt{n}/\varepsilon))$ for passive classical monotonicity testing via a birthday paradox argument. The construction randomly selects DNF terms of fixed width to define a partial partition of the Boolean cube into disjoint sets U_j such that any two points in different U_j are incomparable. The difference between the monotone D_{yes} and non-monotone D_{no} case lies in the function value assignments: in D_{yes}, values within each disjoint set U_j are structured monotonically while in D_{no}, values with each U_j are randomly assigned. Classically, distinguishing these distributions requires $\exp(\Omega(\sqrt{2^n}/\varepsilon))$ samples, as a tester must sample at least two points from the same U_j to gain information. This leads to an exponential lower bound when parameters are chosen appropriately.

Following an argument structured similarly to the one above, one can see that the difference matrix between the induced function state ensembles in the quantum setting decomposes into blocks corresponding to complete multipartite graphs. Also in analogy to our analysis of the [58] construction, the construction from [24] results in a graph such that some of the contributions from the block components yield distinguishability in the quantum case. The ensembles remain distinguishable when $t = \Omega(1/\varepsilon)$, and thus they achieve no improvement over the generic lower bound.

References

1 Scott Aaronson. Shadow tomography of quantum states. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, pages 325–338, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3188745.3188802.

2 Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 307–316, New York, NY, USA, 2015. Association for Computing Machinery. doi:10.1145/2746539.2746547.

3 Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. Quantum algorithmic measurement. *Nature Communications*, 13(1):1–9, 2022. doi:10.1038/s41467-021-27922-0.

4 Noga Alon, Rani Hod, and Amit Weinstein. On active and passive testing. *Comb. Probab. Comput.*, 25(1):1–20, 2016. doi:10.1017/S0963548315000292.

5 Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing low-degree polynomials over gf (2). In *International Workshop on Randomization and Approximation Techniques in Computer Science*, pages 188–199. Springer, 2003. doi:10.1007/978-3-540-45198-3_17.

6 Andris Ambainis, Aleksandrs Belovs, Oded Regev, and Ronald de Wolf. Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing. In *Proceedings of the 2016 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Proceedings, pages 903–922. Society for Industrial and Applied Mathematics, December 2015. doi:10.1137/1.9781611974331.ch65.

7 Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998. doi:10.1145/278298.278306.

8 Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of np. *Journal of the ACM (JACM)*, 45(1):70–122, 1998. doi:10.1145/273865.273901.

9 Srinivasan Arunachalam, Sergey Bravyi, and Arkopal Dutt. A note on polynomial-time tolerant testing stabilizer states, 2024. doi:10.48550/arXiv.2410.22220.

10 Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal Algorithms for Learning Quantum Phase States. In Omar Fawzi and Michael Walter, editors, *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, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.TQC.2023.3.

11 Srinivasan Arunachalam and Arkopal Dutt. Towards tolerant testing stabilizer states, 2024. arXiv:2408.06289.

12 Srinivasan Arunachalam, Arkopal Dutt, and Francisco Escudero Gutiérrez. Testing and learning structured quantum hamiltonians. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 1263–1270, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718289.

13 Alp Atıcı and Rocco A Servedio. Quantum algorithms for learning and testing juntas. *Quantum Information Processing*, 6(5):323–348, 2007. doi:10.1007/s11128-007-0061-6.

14 Costin Bădescu and Ryan O'Donnell. Improved quantum data analysis. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1398–1411, 2021. doi:10.1145/3406325.3451109.

15 Costin Bădescu and Ryan O'Donnell. Lower bounds for testing complete positivity and quantum separability. In *Latin American Symposium on Theoretical Informatics*, pages 375–386. Springer, 2020. doi:10.1007/978-3-030-61792-9_30.

16 Zongbo Bao, Philippe van Dordrecht, and Jonas Helsen. Tolerant testing of stabilizer states with a polynomial gap via a generalized uncertainty relation. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 1254–1262, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718201.

17 Zongbo Bao and Penghui Yao. On testing and learning quantum junta channels. In Gergely Neu and Lorenzo Rosasco, editors, *Proceedings of Thirty Sixth Conference on Learning Theory*, Proceedings of Machine Learning Research, pages 1064–1094. PMLR, July 2023. URL: https://proceedings.mlr.press/v195/bao23b.html.

18 Aleksandrs Belovs and Eric Blais. Quantum algorithm for monotonicity testing on the hypercube. *Theory of Computing*, 11(1):403–412, 2015. doi:10.4086/toc.2015.v011a016.

19 Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997. doi:10.1137/S0097539796300921.

20 Arnab Bhattacharyya, Eldar Fischer, Hamed Hatami, Pooya Hatami, and Shachar Lovett. Every locally characterized affine-invariant property is testable. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 429–436, 2013. doi:10.1145/2488608.2488662.

21 Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of reed-muller codes. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 488–497. IEEE, 2010. doi:10.1109/FOCS.2010.54.

22 Alessandro Bisio, Giulio Chiribella, Giacomo Mauro D'Ariano, Stefano Facchini, and Paolo Perinotti. Optimal quantum learning of a unitary transformation. *Physical Review A—Atomic, Molecular, and Optical Physics*, 81(3):032324, 2010. doi:10.1103/PhysRevA.81.032324.

23 Alessandro Bisio, Giacomo Mauro D'Ariano, Paolo Perinotti, and Michal Sedlák. Quantum learning algorithms for quantum measurements. *Physics Letters A*, 375(39):3425–3434, 2011. doi:10.1016/j.physleta.2011.08.002.

24 Hadley Black. Nearly Optimal Bounds for Sample-Based Testing and Learning of k-Monotone Functions. In Amit Kumar and Noga Ron-Zewi, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2024)*, volume 317 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 37:1–37:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.APPROX/RANDOM.2024.37.

25 Eric Blais. Testing juntas nearly optimally. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, STOC '09, pages 151–158, New York, NY, USA, May 2009. Association for Computing Machinery. doi:10.1145/1536414.1536437.

26 Eric Blais, Amit Weinstein, and Yuichi Yoshida. Partially symmetric functions are efficiently isomorphism testable. *SIAM Journal on Computing*, 44(2):411–432, 2015. doi:10.1137/140971877.

27 Eric Blais and Yuichi Yoshida. A characterization of constant-sample testable properties. *Random Struct. Algorithms*, 55(1):73–88, 2019. doi:10.1002/RSA.20807.

28 Andreas Bluhm, Matthias C. Caro, and Aadil Oufkir. Hamiltonian property testing, 2024. doi:10.48550/arXiv.2403.02968.

29 Avrim Blum, Carl Burch, and John Langford. On learning monotone boolean functions. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, pages 408–415. IEEE Computer Society, 1998. doi:10.1109/SFCS.1998.743491.

30 Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 73–83, 1990. doi:10.1145/100216.100225.

31 Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019. doi:10.1007/978-3-030-36030-6_10.

32 Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical review letters*, 87(16):167902, 2001. doi:10.1103/PhysRevLett.87.167902.

33 Harry Buhrman, Lance Fortnow, Ilan Newman, and Hein Röhrig. Quantum property testing. *SIAM Journal on Computing*, 37(5):1387–1400, 2008. doi:10.1137/S0097539704442416.

34 Claude Carlet and Sihem Mesnager. Four decades of research on bent functions. *Designs, codes and cryptography*, 78(1):5–50, 2016. doi:10.1007/s10623-015-0145-8.

35 Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Probing quantum state space: does one have to learn everything to learn something? *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 473(2201):20160866, 2017. doi:10.1098/rspa.2016.0866.

36 Matthias C. Caro. Learning quantum processes and Hamiltonians via the Pauli transfer matrix. *ACM Transactions on Quantum Computing*, 5(2), June 2024. doi:10.1145/3670418.

37 Matthias C. Caro, Preksha Naik, and Joseph Slote. Testing classical properties from quantum data, 2025. doi:10.48550/arXiv.2411.12730.

38 Sourav Chakraborty, Eldar Fischer, Arie Matsliah, and Ronald de Wolf. New Results on Quantum Property Testing. In Kamal Lodaya and Meena Mahajan, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 145–156, Dagstuhl, Germany, 2010. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.FSTTCS.2010.145.

39 Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, Fernando G.S.L. Brandão, and Patrick Hayden. Efficient unitary designs from random sums and permutations. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 476–484, 2024. doi:10.1109/FOCS61266.2024.00037.

40 Senrui Chen, Changhun Oh, Sisi Zhou, Hsin-Yuan Huang, and Liang Jiang. Tight bounds on pauli channel learning without entanglement. *Physical Review Letters*, 132(18):180805, 2024. doi:10.1103/PhysRevLett.132.180805.

41 Senrui Chen, Sisi Zhou, Alireza Seif, and Liang Jiang. Quantum advantages for pauli channel estimation. *Physical Review A*, 105(3):032435, 2022. doi:10.1103/PhysRevA.105.032435.

42 Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. Exponential separations between learning with and without quantum memory. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 574–585. IEEE, 2022. doi:10.1109/FOCS52979.2021.00063.

43 Sitan Chen and Weiyuan Gong. Efficient pauli channel estimation with logarithmic quantum memory. *PRX Quantum*, 6(2):020323, 2025. doi:10.1103/PRXQuantum.6.020323.

44 Sitan Chen, Weiyuan Gong, and Qi Ye. Optimal tradeoffs for estimating pauli observables. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1086–1105, 2024. doi:10.1109/FOCS61266.2024.00072.

45 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, pages 429–438, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718191.

46 Thomas Chen, Shivam Nadimpalli, and Henry Yuen. Testing and learning quantum juntas nearly optimally. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1163–1185. SIAM, 2023. doi:10.1137/1.9781611977554.ch43.

47 Hana Chockler and Dan Gutfreund. A lower bound for testing juntas. *Information Processing Letters*, 90(6):301–305, June 2004. doi:10.1016/j.ipl.2004.01.023.

48 Marcel Dall'Agnol, Tom Gur, and Oded Lachish. A structural theorem for local algorithms with applications to coding, testing, and verification. *SIAM J. Comput.*, 52(6):1413–1463, 2023. doi:10.1137/21M1422781.

49 Marcel Dall'Agnol, Tom Gur, Subhayan Roy Moulik, and Justin Thaler. Quantum Proofs of Proximity. *Quantum*, 6:834, October 2022. doi:10.22331/q-2022-10-13-834.

50 Irit Dinur. The pcp theorem by gap amplification. *J. ACM*, 54(3):12–es, 2007. doi:10.1145/1236457.1236459.

51 Eldar Fischer. The art of uninformed decisions: A primer to property testing. In *Current Trends in Theoretical Computer Science: The Challenge of the New Century Vol 1: Algorithms and Complexity Vol 2: Formal Models and Semantics*, pages 229–263. World Scientific, 2004. doi:10.1142/9789812562494_0014.

52 Eldar Fischer. A basic lower bound for property testing, 2024. doi:10.48550/arXiv.2403.04999.

53 Eldar Fischer, Oded Lachish, and Yadu Vasudev. Trading query complexity for sample-based testing and multi-testing scalability. In Venkatesan Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 1163–1182. IEEE Computer Society, 2015. doi:10.1109/FOCS.2015.75.

54 Jacob Fox. A new proof of the graph removal lemma. *Annals of Mathematics*, pages 561–579, 2011. doi:10.4007/annals.2011.174.1.17.

55 Uma Girish and Rocco A. Servedio. Forrelation is extremally hard, 2025. arXiv:2508.02514.

56 Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states, 2023. doi:10.48550/arXiv.2312.09206.

57 Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, 2017. doi:10.1017/9781108135252.

58 Oded Goldreich, Shafi Goldwasser, Eric Lehman, Dana Ron, and Alex Samorodnitsky. Testing monotonicity. *Combinatorica*, pages 301–337, March 2000. doi:10.1007/s004930070011.

59 Oded Goldreich, Shafi Goldwasser, and Dana Ron. Property testing and its connection to learning and approximation. *Journal of the ACM (JACM)*, 45(4):653–750, 1998. doi:10.1145/285055.285060.

60 Oded Goldreich and Dana Ron. On Sample-Based Testers. *ACM Transactions on Computation Theory*, 8(2):7:1–7:54, April 2016. doi:10.1145/2898355.

61 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, pages 1352–1363, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3618260.3649738.

62 David Gross, Sepehr Nezami, and Michael Walter. Schur-Weyl duality for the Clifford group with applications: property testing, a robust Hudson theorem, and de Finetti representations. *Comm. Math. Phys.*, 385(3):1325–1393, 2021. doi:10.1007/s00220-021-04118-7.

63 Aram W. Harrow, Cedric Yen-Yu Lin, and Ashley Montanaro. Sequential measurements, disturbance and property testing. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1598–1611. SIAM, 2017. doi:10.1137/1.9781611974782.105.

64 Aram W Harrow and Ashley Montanaro. Testing product states, quantum merlin-arthur games and tensor optimization. *Journal of the ACM (JACM)*, 60(1):1–43, 2013. doi:10.1145/2432622.2432625.

65 Hamed Hatami, Pooya Hatami, Shachar Lovett, et al. Higher-order fourier analysis and applications. *Foundations and Trends® in Theoretical Computer Science*, 13(4):247–448, 2019. doi:10.1561/0400000064.

66 Pooya Hatami, Sushant Sachdeva, and Madhur Tulsiani. An arithmetic analogue of Fox's triangle removal argument, 2016. arXiv:1304.4921.

67 Marcel Hinsche and Jonas Helsen. Single-copy stabilizer testing. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 439–450, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718169.

68 Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, and Jarrod R. McClean. Quantum advantage in learning from experiments. *Science*, 376(6598):1182–1186, 2022. doi:10.1126/science.abn7293.

69 Hsin-Yuan Huang, Sitan Chen, and John Preskill. Learning to predict arbitrary quantum processes. *PRX Quantum*, 4(4):040337, 2023. doi:10.1103/PRXQuantum.4.040337.

70 Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16:1050–1057, 2020. doi:10.1038/s41567-020-0932-7.

71 Hsin-Yuan Huang, Richard Kueng, and John Preskill. Information-theoretic bounds on quantum advantage in machine learning. *Physical Review Letters*, 126(19):190505, 2021. doi:10.1103/PhysRevLett.126.190505.

72 Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Pseudorandom and pseudoentangled states from subset states, 2024. arXiv:2312.15285.

73 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018. doi:10.1007/978-3-319-96878-0_5.

74 Subhash Khot, Dor Minzer, and Muli Safra. On monotonicity testing and boolean isoperimetric-type theorems. *SIAM J. Comput.*, 47(6):2238–2276, 2018. doi:10.1137/16M1065872.

75 Robbie King, David Gosset, Robin Kothari, and Ryan Babbush. Triply efficient shadow tomography. *PRX Quantum*, 6(1):010336, 2025. doi:10.1103/PRXQuantum.6.010336.

76 Margarite L. LaBorde and Mark M. Wilde. Quantum algorithms for testing hamiltonian symmetry. *Physical Review Letters*, 129(16):160503, 2022. doi:10.1103/PhysRevLett.129.160503.

77 Paulina Lewandowska and Ryszard Kukulski. Storage and retrieval of von neumann measurements via indefinite causal order structures. *Physical Review A*, 110(4):042422, 2024. doi:10.1103/PhysRevA.110.042422.

78 Paulina Lewandowska, Ryszard Kukulski, Łukasz Pawela, and Zbigniew Puchała. Storage and retrieval of von neumann measurements. *Physical Review A*, 106(5):052423, 2022. doi:10.1103/PhysRevA.106.052423.

79 Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 806–809, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718254.

80 Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple Constructions of Linear-Depth t-Designs and Pseudorandom Unitaries . In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 485–492, Los Alamitos, CA, USA, October 2024. IEEE Computer Society. doi:10.1109/FOCS61266.2024.00038.

81 Ashley Montanaro and Ronald de Wolf. *A Survey of Quantum Property Testing*. Number 7 in Graduate Surveys. Theory of Computing Library, 2016. doi:10.4086/toc.gs.2016.007.

82 Ryan O'Donnell. Analysis of boolean functions, 2021. arXiv:2105.10386.

83 Ryan O'Donnell and John Wright. Quantum spectrum testing. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 529–538, 2015. doi:10.1145/2746539.2746582.

84 Michal Parnas, Dana Ron, and Ronitt Rubinfeld. Tolerant property testing and distance approximation. *Journal of Computer and System Sciences*, 72(6):1012–1042, 2006. doi:10.1016/j.jcss.2006.03.002.

85 Dana Ron. Algorithmic and analysis techniques in property testing. *Found. Trends Theor. Comput. Sci.*, 5(2):73–205, 2009. doi:10.1561/0400000029.

86 Ronitt Rubinfeld. *Sublinear time algorithms*, pages 1095–1110. EMS Press, May 2007. doi:10.4171/022-3/53.

87 Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, 1996. doi:10.1137/S0097539793255151.

88 Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *Science*, 389(6755):92–96, 2025. doi:10.1126/science.adv8590.

89 Michal Sedlák, Alessandro Bisio, and Mário Ziman. Optimal probabilistic storage and retrieval of unitary channels. *Physical review letters*, 122(17):170502, 2019. doi:10.1103/PhysRevLett.122.170502.

90 Adrian She and Henry Yuen. Unitary Property Testing Lower Bounds by Polynomials. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 96:1–96:17, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2023.96.

91 Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997. doi:10.1137/S0097539796298637.

92 Mehdi Soleimanifar and John Wright. Testing matrix product states. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1679–1701. SIAM, 2022. doi:10.1137/1.9781611977073.68.

93 Madhu Sudan. Invariance in property testing. In Oded Goldreich, editor, *Property Testing - Current Research and Surveys*, volume 6390 of *Lecture Notes in Computer Science*, pages 211–227. Springer, 2010. doi:10.1007/978-3-642-16367-8_12.

94 Michel Talagrand. How much are increasing sets positively correlated? *Combinatorica*, 16(2):243–258, 1996. doi:10.1007/BF01844850.