

# A Survey of Quantum Property Testing

Ashley Montanaro\*      Ronald de Wolf†

November 13, 2013

## Abstract

The area of property testing tries to design algorithms that can efficiently handle very large amounts of data: given a large object that either has a certain property or is somehow “far” from having that property, a tester should efficiently distinguish between these two cases. In this survey we describe recent results obtained for *quantum* property testing. This area naturally falls into three parts. First, we may consider quantum testers for properties of classical objects. We survey the main examples known where quantum testers can be much (sometimes exponentially) more efficient than classical testers. Second, we may consider classical testers of quantum objects. This is the situation that arises for instance when one is trying to determine if quantum states or operations do what they are supposed to do, based only on classical input-output behavior. Finally, we may also consider quantum testers for properties of quantum objects, such as states or operations. We survey known bounds on testing various natural properties, such as whether two states are equal, whether a state is separable, whether two operations commute, etc. We also highlight connections to other areas of quantum information theory and mention a number of open questions.

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Quantum testing of classical properties . . . . .	4
1.2	Classical testing of quantum properties . . . . .	5
1.3	Quantum testing of quantum properties . . . . .	5
<b>2</b>	<b>Quantum testing of classical properties</b>	<b>6</b>
2.1	Upper bounds . . . . .	7
2.1.1	Using amplitude amplification . . . . .	7
2.1.2	Using the Bernstein-Vazirani algorithm . . . . .	7
2.1.3	Testing juntas . . . . .	8
2.1.4	Using Simon’s algorithm . . . . .	10
2.1.5	Using Shor’s algorithm . . . . .	13

---

\*Department of Computer Science, University of Bristol, UK; [ashley@cs.bris.ac.uk](mailto:ashley@cs.bris.ac.uk).

†CWI and University of Amsterdam, the Netherlands; [rdewolf@cwi.nl](mailto:rdewolf@cwi.nl). Supported by a Vidi grant from the Netherlands Organization for Scientific Research (NWO), and the European Commission IST STREP project Quantum Algorithms (QALGO) 600700.

2.1.6	Using quantum counting . . . . .	14
2.1.7	Using Ambainis’s algorithm . . . . .	16
2.1.8	Quantum speed-ups for testing group-theoretic properties . . . . .	17
2.2	Lower bounds . . . . .	17
2.2.1	The polynomial method . . . . .	17
2.2.2	The adversary method . . . . .	19
2.2.3	A communication complexity method? . . . . .	20
<b>3</b>	<b>Classical testing of quantum properties</b>	<b>21</b>
3.1	Self-testing gates . . . . .	21
3.2	Self-testing protocols . . . . .	24
<b>4</b>	<b>Quantum testing of quantum properties</b>	<b>26</b>
4.1	Pure states . . . . .	26
4.1.1	Equality . . . . .	27
4.1.2	Productness . . . . .	28
4.1.3	Arbitrary finite or infinite sets . . . . .	30
4.1.4	Open questions . . . . .	31
4.2	Mixed states . . . . .	31
4.2.1	Testing equality to a fixed pure state . . . . .	34
4.2.2	Unitarily invariant properties . . . . .	35
<b>5</b>	<b>Testing properties of quantum dynamics</b>	<b>37</b>
5.1	Unitary operators . . . . .	37
5.1.1	Distance measures . . . . .	37
5.1.2	Controlled and inverse unitaries . . . . .	39
5.1.3	From properties of states to properties of unitaries . . . . .	39
5.1.4	Membership of the Pauli and Clifford groups . . . . .	41
5.1.5	Testing commutativity . . . . .	42
5.1.6	Testing quantum juntas . . . . .	42
5.1.7	Other properties of unitary matrices . . . . .	44
5.2	Properties of quantum channels . . . . .	44
5.2.1	Distance measures . . . . .	45
5.2.2	Testing quantum measurements . . . . .	45
5.3	Quantum properties and computational complexity . . . . .	48
5.3.1	Properties of quantum circuits . . . . .	49
<b>6</b>	<b>Conclusion</b>	<b>50</b>

# 1 Introduction

In the last two decades, the amounts of data that need to be handled have exploded: think of the massive amounts of data on the web, or the data warehouses of customer information collected by big companies. In many cases algorithms need to decide whether this data has certain properties or not, without having sufficient time to trawl through all or even most of the data. Somehow we would like to detect the presence or absence of some global property by only making a few “local” checks. The area of *property testing* aims to design algorithms that can efficiently test whether some large object has a certain property, under the assumption that the object either has the property or is somehow “far” from having that property. An assumption like the latter is necessary for efficient property testing: deciding the property for objects that are “just on the boundary” typically requires looking at all or most of the object, which is exactly what we are trying to avoid here. In general, different property testing settings can be captured by the following “meta-definition”:

## Property testing

Let  $\mathcal{X}$  be a set of objects and  $d : \mathcal{X} \times \mathcal{X} \rightarrow [0, 1]$  be a distance measure on  $\mathcal{X}$ . A subset  $\mathcal{P} \subseteq \mathcal{X}$  is called a *property*. An object  $x \in \mathcal{X}$  is  $\epsilon$ -far from  $\mathcal{P}$  if  $d(x, y) \geq \epsilon$  for all  $y \in \mathcal{P}$ ;  $x$  is  $\epsilon$ -close to  $\mathcal{P}$  if there is a  $y \in \mathcal{P}$  such that  $d(x, y) \leq \epsilon$ .

An  $\epsilon$ -property tester for  $\mathcal{P}$  is an algorithm that receives as input either an  $x \in \mathcal{P}$  or an  $x$  that is  $\epsilon$ -far from  $\mathcal{P}$ , and that distinguishes these two cases with success probability at least  $2/3$ .

The value of  $2/3$  for the success probability is arbitrary and can equivalently be replaced with any other constant in  $(1/2, 1)$  since we can efficiently reduce the error probability by repeating the test a few times and taking the majority outcome. We say that the tester has *perfect completeness* if it accepts every state in  $\mathcal{P}$  with certainty. The distance parameter  $\epsilon$  is usually taken to be some positive constant. We will often just speak of a “tester,” leaving the value of  $\epsilon$  implicit.

Clearly, this meta-definition leaves open many choices: what type of objects to consider, what property to test, what distance measure to use, what range of  $\epsilon$  to allow (the larger  $\epsilon$ , the easier it should be to test  $\mathcal{P}$ ), and how to measure the complexity of the testing algorithm. A lot of work has gone into the study of efficient testers for various properties, as well as proofs that certain properties are not efficiently testable, see for instance [33, 71, 62, 134, 70]. Typically,  $\mathcal{X}$  will be the set of all  $N$ -element strings over some finite alphabet, where we think of  $N$  as being very large. The distance will usually be normalized Hamming distance  $d(x, y) = |\{i : x_i \neq y_i\}|/N$ , though also more sophisticated metrics such as “edit distance” have been used. The complexity of the tester is typically measured by the number of *queries* it makes to entries of its input  $x$ , and a tester is deemed efficient if its number of queries is much less than the length of the input  $N$ , say  $\text{polylog}(N)$  or even some constant independent of  $N$ . This captures the goal that a tester is able to efficiently handle huge amounts of data.

In this survey paper we will be concerned with *quantum* property testing. There are several natural ways in which one can generalize property testing to the quantum world:

- Quantum testing of properties of classical objects. In this setting we would like to achieve provable quantum speed-ups over any possible classical algorithm, or to prove limitations on property testers, even if they are allowed to be quantum. By their very nature, efficient quantum query algorithms rely on extracting global information about the input, by querying in superposition; property testing is thus a plausible place to find significant quantum speed-ups.

- Classical testing of properties of quantum objects. Here we imagine we are given a black-box device which is claimed to implement some quantum process, and we would like to test whether it does what is claimed. However, our access to the device is classical: all we can do is feed classical inputs to the device, and receive classical measurement outcomes.
- Quantum testing of properties of quantum objects. In this most general scenario, we are given access to a quantum state or operation as a black box, and apply a quantum procedure to it to determine whether it has some property.

We will discuss each of these settings in turn. We usually concentrate on describing the intuition behind prior work, without giving detailed proofs. Some of the results we present have not appeared in the literature before; these are largely based on combining, generalizing or improving existing works. Various open questions are pointed out throughout the survey.

A vast amount of work in quantum computing can be interpreted through the lens of property testing. Indeed, taken to extremes, any efficient quantum algorithm for a decision problem could be seen as an efficient property tester, and any measurement scheme that tries to learn properties of a quantum state or channel could be seen as a quantum property tester. We therefore concentrate on covering those algorithms which can clearly be understood as distinguishing objects with some property from those “far” from that property, and we make no attempt to be completely comprehensive. Also, our focus is on the computer-science aspects of the field, rather than work which primarily takes a physics perspective, such as the study of interaction-free measurement and the flourishing field of quantum metrology. Finally, we do not attempt to cover the (now very extensive) field of classical testers for classical properties. For much more on these, see the references given earlier.

## 1.1 Quantum testing of classical properties

In the first part of this paper we will consider quantum testing of *classical* properties. Again,  $\mathcal{X}$  will typically be the set of all  $N$ -element strings over some finite alphabet, the distance will be normalized Hamming distance, and the complexity of both quantum and classical property testers will be measured by the number of queries to the input  $x$ .

One of our goals is to survey examples of quantum speed-up, i.e., describe properties where the complexity of quantum testers is substantially less than the complexity of classical testers. Most known quantum speed-ups for testing classical properties were derived from earlier improvements in query complexity: they rely on quantum algorithms such as those of (in chronological order) Bernstein and Vazirani [30], Simon [141], Shor [140], Grover [76], and Ambainis [15]. In Section 2.1 we describe these quantum property testers and the improvements they achieve over classical testers. Some of the properties considered are very natural, and some of the improvements achieved are quite significant.

In Section 2.2 we describe some *lower-bound* methods for quantum property testing, i.e., methods to show query complexity lower bounds for quantum algorithms that want to test specific properties. The main lower bounds in this area have been obtained using the *polynomial* method. We also describe the *adversary* method, which—when applied properly—proves optimal lower bounds. And we ask whether the recent classical property testing lower bounds of Blais et al. [32], based on communication complexity, can be applied to quantum testers as well.

## 1.2 Classical testing of quantum properties

In the second part we will consider *classical* testing of quantum properties. At first sight, this scenario might make no sense—how could a classical algorithm, without the ability to perform any quantum operations, be able to test quantum objects? But suppose someone gives us a quantum state and claims it is an EPR-pair. Or someone builds a quantum device to implement a Hadamard gate, or to measure in a specific basis. How can we test that these quantum objects conform to their specifications? These are questions often faced for instance by experimentalists who try to check that their quantum operations work as intended, or by parties who run quantum cryptographic hardware provided by an untrusted supplier. We do not want to assume here that we already have the ability to implement some other quantum operations reliably, because that would lead to an infinite regress: how did we establish that those other quantum objects are reliable? Accordingly, we somehow would like to test the given quantum object while only trusting our *classical* devices. Of course, in order to test a quantum object there has to be at least *some* interaction with the quantum object-to-be-tested. In the testers we consider, the only quantum involvement is with that object itself in a black-box fashion (whence the name “self-testing”): we can only observe its classical input-output behavior, but not its inner quantum workings.

This notion of quantum self-testing was introduced by Mayers and Yao [114, 115], who described a procedure to test photon sources that are supposed to produce EPR-pairs. Since then quite a lot of work has been done on self-testing. Recently self-testing has found many applications in the area of *device-independent* quantum cryptography, where parties want to run cryptographic protocols for things like key distribution or randomness generation, using quantum states or apparatuses (photon sources, measuring devices, etc.) that they do not fully trust. Self-testing the states or apparatuses makes device-independent cryptography possible in some cases. See, e.g., [23, 56, 9, 145, 146] for references to this fast-growing area.

## 1.3 Quantum testing of quantum properties

In the final part of the paper we will consider cases where  $\mathcal{X}$  is a set of quantum objects and our tester is also quantum, which is a setting of both theoretical and experimental interest.

As experimentalists control ever-larger quantum systems in the lab, the question of how to characterize and certify these systems becomes ever more pressing. Small quantum systems can be characterized via a procedure known as *quantum state tomography* [127, 124]. However, completely determining the state of a system of  $n$  qubits necessarily requires exponentially many measurements in  $n$ . This is already a daunting task for fairly small experiments; for example, Häffner et al. [79] report tomography of a state of 8 ions requiring 656,100 experiments and a total measurement time of 10 hours. One way of reducing this complexity is to start with the assumption that the state is of a certain form (such as a low-rank mixed state [75, 64] or a matrix product state [57]), in which case the number of parameters required to be estimated can be dramatically reduced. The viewpoint of property testing suggests another approach: the direct determination of whether or not something produced in the lab has a particular property of interest, under the assumption that it either has the property or is far away from it.

One can view classical property testing algorithms in two ways: either as testing properties of data (such as graph isomorphism), or properties of functions (such as linearity). If one wishes to generalize property testing to the quantum realm, one is thus naturally led to two different generalizations: testing properties of quantum *states*, and properties of quantum *operations*. One can divide each of these further, according to whether the state is pure or mixed, and whether

the operation is reversible or irreversible; this classification is illustrated in Table 1. We discuss each of these possibilities in Sections 4 and 5. Within some of these categories there are natural generalizations of properties studied classically. For example, testing properties of mixed states is analogous to the classical idea of testing properties of probability distributions. Some quantum properties, however, have no simple classical analog (such as properties relating to entanglement).

	<b>Coherent</b>	<b>Incoherent</b>
<b>Static</b>	Pure state (§4.1)	Mixed state (§4.2)
<b>Dynamic</b>	Unitary operator (§5.1)	Quantum channel (§5.2)

Table 1: The taxonomy of quantum properties

Classically, there are many connections known between property testing and computational complexity. In Section 5.3 we explore the link between quantum property testing and quantum computational complexity, including the use of property testers to prove results in computational complexity, and the use of computational complexity to prove limitations on property testers.

## 2 Quantum testing of classical properties

When considering (quantum or classical) testers for classical objects, those classical objects are usually strings,  $\mathcal{X} = [m]^N$ , and the complexity of testers is measured by the number of *queries* they make to their input  $x$ . Here we briefly define the quantum query model, referring to [45] for more details. We assume some basic familiarity with quantum computing [124].

Informally, a query allows us to “read”  $x_i$  for any  $i$  of our choice. Mathematically, to make this correspond to a quantum operation, it is modeled by the unitary map

$$O_x : |i\rangle|b\rangle \mapsto |i\rangle|b + x_i\rangle.$$

Here the first register has dimension  $N$  and the second has dimension  $m$ . The answer  $x_i$  is added into this second register mod  $m$ . Part of the power of quantum query algorithms comes from their ability to apply a query to a *superposition* of different  $i$ s, thus globally “accessing” the input  $x$  while using only one query.

If  $m = 2$ , then putting the state  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  in the second register has the following effect:

$$O_x : |i\rangle|-\rangle \mapsto |i\rangle \frac{1}{\sqrt{2}}(|0 + x_i\rangle - |1 + x_i\rangle) = (-1)^{x_i} |i\rangle|-\rangle.$$

We will sometimes call this a “phase-query,” because the answer  $x_i$  to the query is inserted in the state as a phase (+1 if  $x_i = 0$ , and  $-1$  if  $x_i = 1$ ).

A  $T$ -query quantum algorithm is described by an initial state, say  $|0^k\rangle$ , and  $T + 1$  fixed  $k$ -qubit unitaries  $U_0, \dots, U_T$ . The final state when the algorithm runs on input  $x$  is obtained by interleaving these unitaries with queries to  $x$  ( $O_x$  may be tensored with the identity operation on the remaining workspace qubits),

$$|\psi_x\rangle = U_T O_x U_{T-1} O_x \cdots O_x U_1 O_x U_0 |0^k\rangle.$$

This final state depends on  $x$  via the  $T$  queries. A measurement of the final state will determine the classical output of the algorithm.

## 2.1 Upper bounds

In this section we will survey the main speed-ups that have been obtained using *quantum* testers for *classical* properties.

### 2.1.1 Using amplitude amplification

A simple but very general way that quantum computers can speed up many classical property testers is via the powerful primitive of *amplitude amplification*, which was introduced by Brassard et al. [36] and can be seen as a generalization of Grover’s quantum search algorithm [76]. We assume we are given access to some function  $f(w)$  (treated as a black box), and have a quantum algorithm which, with probability  $p$ , outputs  $w$  such that  $f(w) = 1$ . Then the result of Brassard et al. is that, for any  $p > 0$ , we can find a  $w$  such that  $f(w) = 1$  with  $O(1/\sqrt{p})$  uses of  $f$ , with success probability at least  $2/3$ .

This algorithm can be immediately applied to speed up classical property testers which have perfect completeness. Here we think of  $w$  as the internal randomness of the algorithm, and  $f(w)$  as the test which is applied to the unknown object, based on the random bits  $w$ . We let  $f(w) = 0$  if the test accepts, and  $f(w) = 1$  if the test rejects. Assuming that the test has perfect completeness, finding  $w$  such that  $f(w) = 1$  is equivalent to determining whether we should reject. Given that the original test used  $q$  queries to find such a  $w$  with probability  $p > 0$ , we therefore obtain a test which uses  $O(q/\sqrt{p})$  queries and rejects with constant probability.

For example, consider the well-studied classical property of **Linearity** [33]. A function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  is said to be linear if  $f(x \oplus y) = f(x) \oplus f(y)$ , where  $\oplus$  is addition modulo 2. (This is equivalent to the condition  $f(x) = \bigoplus_{i \in S} x_i$  for some  $S \subseteq [n]$ .) A simple and natural test for linearity is to pick  $x, y \in \{0, 1\}^n$  uniformly at random and accept if and only if  $f(x) \oplus f(y) = f(x \oplus y)$ . This test uses only 3 queries, has perfect completeness, and can be shown [28] to reject functions  $f$  which are  $\epsilon$ -far from linear with probability at least  $\epsilon$ . Applying amplitude amplification to this tester, we immediately get a quantum tester for **Linearity** which uses  $O(1/\sqrt{\epsilon})$  queries. Another simple example is **Symmetry**, where  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  is said to be symmetric if  $f(x)$  depends only on  $|\{i : x_i = 1\}|$ . A classical tester for this property has been given by Majewski and Pippenger [113]. The tester uses 2 queries, has perfect completeness and rejects functions with are  $\epsilon$ -far from symmetric with probability at least  $\epsilon$ . Therefore, we again obtain a quantum tester which uses  $O(1/\sqrt{\epsilon})$  queries.

Hillery and Andersson [87] gave different quantum testers for these two properties (though also based on amplitude amplification), each of which uses  $O(\epsilon^{-2/3})$  queries, which is worse. Very recently, Chakraborty and Maitra [46] gave an alternative quantum linearity tester which uses  $O(1/\sqrt{\epsilon})$  queries.

### 2.1.2 Using the Bernstein-Vazirani algorithm

One of the first quantum algorithms was the Bernstein-Vazirani algorithm [30]. It efficiently decodes a given *Hadamard codeword*. Let  $N = 2^n$ , and identify  $[N]$  with  $\{0, 1\}^n$  so we can use the  $n$ -bit strings to index the numbers  $1, \dots, N$ . Let  $h : \{0, 1\}^n \rightarrow \{0, 1\}^N$  be the Hadamard encoding, defined by  $h(s)_i = s \cdot i \bmod 2$ ; this is nothing more than identifying  $s$  with the linear function  $h(s)(i) = s \cdot i \bmod 2$  and writing out its truth table. Note that two distinct Hadamard codewords  $h(s)$  and  $h(s')$  are at relative Hamming distance exactly  $1/2$ . Given input  $h(s)$ , the Bernstein-Vazirani algorithm recovers  $s$  with probability 1 using only one quantum query. In contrast, any

classical algorithm needs  $\Omega(\log N)$  queries for this. The quantum algorithm works as follows:

1. Start with  $|0^n\rangle$  and apply Hadamard gates to each qubit to form the uniform superposition  $\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle$
2. Apply a phase-query to obtain  $\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle$
3. Apply Hadamard transforms to each qubit and measure.

If  $x_i = s \cdot i$  for all  $i \in \{0,1\}^n$ , then it is easy to see that the measurement yields  $s$  with probability 1.

Buhrman et al. [43] showed this can be turned into an unbounded quantum speed-up for *testing* most subsets of Hadamard codewords.

**Bernstein-Vazirani property** for  $A \subseteq \{0,1\}^n$ :  
 $\mathcal{P}_{BV}^A = \{x \in \{0,1\}^N : \exists s \in A \text{ such that } x = h(s)\}$

**Theorem 1** (Buhrman et al. [43]). *For every  $A \subseteq \{0,1\}^n$  there is an  $O(1/\sqrt{\epsilon})$ -query quantum  $\epsilon$ -property tester for  $\mathcal{P}_{BV}^A$ , while for most  $A$ , every classical  $1/2$ -property tester for  $\mathcal{P}_{BV}^A$  needs  $\Omega(\log N)$  queries.*

*Proof. Quantum upper bound.* We run the Bernstein-Vazirani algorithm on input  $x$ , which takes one quantum query. The algorithm will output some  $s$ , and if  $x$  equals some  $h(s) \in \mathcal{P}_{BV}^A$  then this will be the corresponding  $s$  with certainty. Hence if  $s \notin A$  we can reject immediately. If  $s \in A$  then choose  $i \in [N]$  at random, query  $x_i$ , and test whether indeed  $x_i = s \cdot i$ . If  $x$  is  $\epsilon$ -far from  $\mathcal{P}_{BV}^A$  then this test will fail with probability  $\epsilon$ . Using amplitude amplification, we can detect any  $x$  that is  $\epsilon$ -far from  $\mathcal{P}_{BV}^A$  with success probability at least  $2/3$  using  $O(1/\sqrt{\epsilon})$  queries.

**Classical lower bound.** Choose the set  $A \subseteq \{0,1\}^n$  uniformly at random. Consider the uniform input distribution over the set  $H$  of all  $N$  Hadamard codewords. Note that the Hadamard codewords that are not in  $\mathcal{P}_{BV}^A$  are  $1/2$ -far from  $\mathcal{P}_{BV}^A$ , because any two distinct Hadamard codewords have relative Hamming distance exactly  $1/2$ . Hence if  $\mathcal{P}_{BV}^A$  can be tested with  $T$  queries, then there exists a deterministic decision tree that is correct on at least  $2/3$  of the  $x \in H$ . Fix a deterministic decision tree  $\mathcal{T}$  of depth  $T$ . For each  $x \in H$ , the probability (over the choice of  $A$ ) that  $x \in \mathcal{P}_{BV}^A$  is  $1/2$ , irrespective of the output that  $\mathcal{T}$  gives on  $x$ , so the probability that  $\mathcal{T}$  correctly decides  $x$  is  $1/2$ . Then the probability that  $\mathcal{T}$  correctly decides at least  $2/3$  of the  $x \in H$  is  $2^{-\Omega(N)}$  by a Chernoff bound. The total number of deterministic decision trees of depth  $T$  is at most  $2^{2^T} N^{2^T-1}$ , because for each of the (at most)  $2^T - 1$  internal nodes we have to choose an index to query, and for each of the (at most)  $2^T$  leaves we have to choose a binary output value. Hence by the union bound, the probability (over the choice of  $A$ ) that there exists a depth- $T$  decision tree that correctly decides at least  $2/3$  of the  $x \in H$  is at most

$$2^{-\Omega(N)} \cdot 2^{2^T} N^{2^T-1}.$$

For  $T = (\log N)/2$  this quantity is negligibly small. This shows that for most choices of  $A$ , there is no classical tester for  $\mathcal{P}_{BV}^A$  with  $(\log N)/2$  queries.  $\square$

### 2.1.3 Testing juntas

Let  $f : \{0,1\}^n \rightarrow \{+1, -1\}$  be a Boolean function (such an  $f$  can also be viewed as a string  $x$  of  $N = 2^n$  bits, with  $x_i = f(i)$ ), and  $J$  be the set of variables on which  $f$  depends. If  $|J| \leq k$  then  $f$  is called a  $k$ -junta.



**$k$ -junta property:**  $\mathcal{P}_{k\text{-junta}} = \{f : \{0, 1\}^n \rightarrow \{+1, -1\} : f \text{ depends on at most } k \text{ variables}\}$

Atıçı and Servedio [17] gave an elegant quantum  $\epsilon$ -property tester for  $\mathcal{P}_{k\text{-junta}}$  using  $O(k/\epsilon)$  quantum queries. This improves upon the best known classical tester, which uses  $O(k \log k + k/\epsilon)$  queries [31].<sup>1</sup>

**Theorem 2** (essentially Atıçı and Servedio [17]). *There is a quantum tester for  $k$ -juntas that uses  $O(k/\sqrt{\epsilon})$  queries.*

“Essentially” in the attribution of the above theorem refers to the fact that [17] prove an  $O(k/\epsilon)$  bound. We observe here that the dependence on  $\epsilon$  can easily be improved by a square root using amplitude amplification.

*Proof.* The basic quantum subroutine is the same as in Section 2.1.2:

1. Start with  $|0^n\rangle$  and apply Hadamard gates to each qubit to form the uniform superposition  $\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle$
2. Apply a phase-query to obtain  $\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} f(i)|i\rangle$
3. Apply Hadamard transforms to each qubit and measure.

Let us analyze this by means of some Fourier analysis on the Boolean cube (see [125, 151] for background). For every  $s \in \{0, 1\}^n$ , let

$$\hat{f}(s) = \frac{1}{2^n} \sum_{i \in \{0,1\}^n} f(i)(-1)^{i \cdot s}$$

be the corresponding Fourier coefficient. Going through the steps of the quantum subroutine, it is easy to see that the final state before the measurement is

$$\sum_{s \in \{0,1\}^n} \hat{f}(s)|s\rangle.$$

Accordingly, the final measurement will sample an  $s \in \{0, 1\}^n$  from the distribution given by the squared Fourier coefficients  $\hat{f}(s)^2$ . This procedure is known as *Fourier Sampling* [30]. It costs one query to  $f$ .

Let  $J$  be the set of variables on which the input  $f$  depends. The goal of the tester is to decide whether  $|J| \leq k$  or not. Note that  $\hat{f}(s) \neq 0$  only if the support of  $s$  lies within  $J$ , so each Fourier Sample gives us a subset of  $J$ . The tester will keep track of the union  $W$  of the supports seen so far. We will always have  $W \subseteq J$ , so if  $f$  is a  $k$ -junta then  $W$  will never have more than  $k$  elements. On the other hand, below we show that if  $f$  is  $\epsilon$ -far from any  $k$ -junta, then with high probability after  $O(k/\sqrt{\epsilon})$  queries  $W$  will end up having more than  $k$  elements.

For a subset  $W \subseteq [n]$  of size at most  $k$ , define  $g(i) = \sum_{s \subseteq W} \hat{f}(s)(-1)^{i \cdot s}$ , where we identify sets  $s \subseteq [n]$  with their characteristic vectors  $s \in \{0, 1\}^n$ . This function  $g$  need not be a Boolean

---

<sup>1</sup>In fact, at the time [17] was written the best classical upper bound was  $O((k \log k)^2/\epsilon)$  [63].

function, but we can consider the Boolean function  $h$  that is the sign of  $g$ . This  $h$  only depends on the variables in  $W$ , so it is a  $k$ -junta and hence  $\epsilon$ -far from  $f$ . Now we have

$$\begin{aligned}
\epsilon &\leq \frac{1}{2^n} \sum_{i:f(i)\neq h(i)} 1 \\
&\leq \frac{1}{2^n} \sum_{i:f(i)\neq h(i)} (f(i) - g(i))^2 \\
&\leq \mathbb{E}_{i\in\{0,1\}^n} [(f(i) - g(i))^2] \\
&= \sum_s (\hat{f}(s) - \hat{g}(s))^2 \\
&= \sum_{s\nsubseteq W} \hat{f}(s)^2,
\end{aligned}$$

where the first equality is Parseval's identity. But this means that with probability at least  $\epsilon$ , Fourier Sampling will output an  $s$  that is not fully contained in  $W$ . Now we use amplitude amplification to find such an  $s$ , using an expected number of  $O(1/\sqrt{\epsilon})$  queries. Repeating this at most  $k + 1$  times, after an expected number of  $O(k/\sqrt{\epsilon})$  queries the set  $W$  (which was initially empty) will contain more than  $k$  variables and we can reject the input.  $\square$

However, the best known classical lower bound is only  $\Omega(k)$  [51] (for fixed  $\epsilon$ ), so there might even be a classical tester that is as efficient as the quantum one. It is open whether this quantum tester is optimal. Atıcı and Servedio [17] prove an  $\Omega(\sqrt{k})$  lower bound for testers that use Fourier Sampling as a black box, but no non-trivial general lower bound seems to be known.

**Question 1.** *What is the quantum complexity of testing juntas?*

### 2.1.4 Using Simon's algorithm

The first exponential speed-up for quantum property testing was also obtained by Buhrman et al. [43]. It is inspired by Simon's algorithm [141]. This was the first algorithm to have a provable exponential speed-up over classical algorithms in the black-box model; it also inspired Shor's factoring algorithm [140] which we will see in the next section. Again let  $N = 2^n$  and identify  $[N]$  with  $\{0, 1\}^n$ . Consider an input  $x \in [N]^N$  for which there exists an  $s \in \{0, 1\}^n \setminus \{0^n\}$  such that  $x_i = x_j$  if and only if ( $j = i$  or  $j = i \oplus s$ ). Simon's algorithm finds  $s$  with high probability using  $O(\log N)$  queries. The core of the algorithm is the following quantum subroutine:

1. Start with  $|0^n\rangle|0^n\rangle$  and apply Hadamards to the first  $n$  qubits to form  $\frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle|0^n\rangle$
2. Apply a query to obtain  $\frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle|x_i\rangle$
3. Measure the second register. This yields some  $z = x_i$  and collapses the first register to the two indices with value  $z$ :  $\frac{1}{\sqrt{2}}(|i\rangle + |i \oplus s\rangle)$
4. Apply Hadamards to the first  $n$  qubits and measure the state, obtaining some  $y \in \{0, 1\}^n$ .

It is easy to calculate that the measured state is (up to phases) a uniform superposition over all  $2^{n-1}$  strings  $y \in \{0, 1\}^n$  that satisfy  $s \cdot y = 0 \pmod{2}$ . Each such  $y$  gives us a linear constraint  $(\pmod{2})$  on the bits of  $s$ . Repeating this subroutine  $O(n)$  times gives, with high probability,

$n - 1$  linearly independent  $y^{(1)}, \dots, y^{(n-1)}$  all orthogonal to  $s$ . From these,  $s$  can be calculated classically by Gaussian elimination. Brassard and Høyer [35] subsequently gave an *exact* version of this algorithm, where each new  $y$  is guaranteed to be linearly independent from the previous ones.

Again, this algorithm can be used to obtain a strong quantum speed-up for testing a specific property.

**Simon property:**

$$\mathcal{P}_{Simon} = \{x \in [N]^N : \exists s \in \{0, 1\}^n \setminus \{0^n\} \text{ such that } x_i = x_j \text{ if } j = i \oplus s\}$$

Note that, compared with Simon’s original problem, the ‘if and only if’ has been replaced with an ‘if.’ Hence  $x_i$  and  $x_j$  can be equal even for distinct  $i, j$  for which  $j \neq i \oplus s$ . However, also for such more general inputs, Simon’s quantum subroutine only produces  $y$  such that  $s \cdot y = 0 \pmod{2}$ .

**Theorem 3** (essentially Buhrman et al. [43]). *There is a quantum  $1/4$ -property tester for the Simon property using  $O(\log N)$  queries, while every classical  $1/4$ -property tester needs  $\Omega(\sqrt{N})$  queries.*

“Essentially” in the attribution of the above theorem refers to the fact that Buhrman et al. [43] devised a property of *binary* strings of length  $N$ . In our presentation it will be more convenient to consider a property consisting of strings over alphabet  $[N]$ . As remarked by Aaronson and Ambainis [3], Theorem 3 has an interesting interpretation in terms of when we can hope to achieve exponential quantum speed-ups. In order to obtain a super-polynomial quantum speed-up for computing some function  $f$  in the query complexity model, it is known that there has to be a *promise* on the input, i.e.,  $f$  has to be a partial function [27]. The Simon property indeed involves a promise on the input, namely that it is either in or far from  $\mathcal{P}_{Simon}$ ; however, this promise is in some sense very weak, as the algorithm has to output the right answer on a  $1 - o(1)$  fraction of  $[N]^N$ .

*Proof. Quantum upper bound (sketch).* We run the Brassard-Høyer version of Simon’s subroutine  $n - 1$  times. We then classically compute a non-zero string  $s$  that is orthogonal to all the  $n - 1$  strings  $y$  produced by these runs (there may be several such  $s$ , in which case we just pick any). We then randomly choose  $i \in [N]$ , query  $x_i$  and  $x_{i \oplus s}$ , and check if these two values are equal. If  $x \in \mathcal{P}_{Simon}$  then  $s$  will have the property that  $x_i = x_{i \oplus s}$  for all  $i$ . On the other hand, if  $x$  is  $1/4$ -far from  $\mathcal{P}_{Simon}$ , then there exist at least  $N/4$   $(i, i \oplus s)$ -pairs such that  $x_i \neq x_{i \oplus s}$  (for otherwise we could put  $x$  into  $\mathcal{P}_{Simon}$  by changing one value for each such pair, making fewer than  $N/4$  changes in total). Hence in this case we reject with constant probability. Testing a few different  $(i, i \oplus s)$ -pairs reduces the error probability to below  $1/3$ .

**Classical lower bound.** Consider three distributions:  $\mathcal{D}_1$  is uniform over  $\mathcal{P}_{Simon}$ ,  $\mathcal{D}_0$  is uniform over all  $x \in [N]^N$  that are  $1/4$ -far from  $\mathcal{P}_{Simon}$ , and  $\mathcal{U}$  is uniform over  $[N]^N$ . We first show  $\mathcal{D}_0$  and  $\mathcal{U}$  are very close.

**Claim 4.** The total variation distance between  $\mathcal{D}_0$  and  $\mathcal{U}$  is  $o(1)$ .

*Proof.* Let  $S = \{y : y \text{ is not } 1/4\text{-far from } \mathcal{P}_{Simon}\}$  be the elements that are not in the support of  $\mathcal{D}_0$ . We will upper bound the size of  $S$ . Each element of  $\mathcal{P}_{Simon}$  is specified by giving an  $s \in \{0, 1\}^n \setminus \{0^n\}$  and giving for each of the  $N/2$   $(i, i \oplus s)$ -pairs the value  $x_i = x_{i \oplus s}$ . Hence

$$|\mathcal{P}_{Simon}| \leq (N - 1)N^{N/2}$$

For each  $x$ , the number of  $y$  that are  $1/4$ -close to  $x$  is at most  $\binom{N}{N/4}N^{N/4}$ . Hence the total number of elements  $1/4$ -close to  $\mathcal{P}_{Simon}$  is

$$|S| \leq (N-1)N^{N/2} \binom{N}{N/4} N^{N/4} = o(N^N).$$

Since  $\mathcal{U}$  is uniform over  $[N]^N$  and  $\mathcal{D}_0$  is uniform over  $[N]^N \setminus S$ , the total variation distance between these two distributions is  $O(|S|/N^N) = o(1)$ .  $\square$

To finish the proof, below we slightly adapt the proof in [141] to show that a  $T$ -query classical algorithm distinguishing distributions  $\mathcal{D}_1$  and  $\mathcal{U}$  has advantage  $O(T^2/N)$  over random guessing. Since  $\mathcal{D}_0$  and  $\mathcal{U}$  are  $o(1)$ -close, a  $T$ -query classical algorithm distinguishing distributions  $\mathcal{D}_1$  and  $\mathcal{D}_0$  has advantage  $O(T^2/N) + o(1)$  over random guessing. A classical tester for the Simon property can distinguish  $\mathcal{D}_1$  and  $\mathcal{D}_0$  with success probability at least  $2/3$ , so it needs  $T = \Omega(\sqrt{N})$  queries.

**Claim 5.** A  $T$ -query classical algorithm for distinguishing distributions  $\mathcal{D}_1$  and  $\mathcal{U}$  has advantage  $O(T^2/N)$  over random guessing.

*Proof.* By the Yao principle it suffices to prove this for an arbitrary *deterministic*  $T$ -query algorithm. The proof will show that both under  $\mathcal{D}_1$  and  $\mathcal{U}$  the  $T$  queries are likely to yield a uniformly random sequence of  $T$  distinct values. Suppose the algorithm queries the indices  $i_1, \dots, i_T$  (this sequence depends on  $x$ ) and gets outputs  $x_{i_1}, \dots, x_{i_T}$ . Call a sequence of queries  $i_1, \dots, i_T$  *good* if it shows a collision, i.e.,  $x_{i_k} = x_{i_\ell}$  for some  $k \neq \ell$ . Call the sequence *bad* otherwise. We will now show that the probability of a bad sequence is  $O(T^2/N)$ , both under input distribution  $\mathcal{U}$  and under  $\mathcal{D}_1$ .

First, suppose the input  $x$  is distributed according to  $\mathcal{U}$ . Then each output  $x_{i_k}$  is uniformly distributed over  $[N]$ , independent of the other entries of  $x$ . The probability that  $i_k$  and  $i_\ell$  form a collision is exactly  $1/N$ , so the expected number of collisions among the  $T$  queries is  $\binom{T}{2}/N = O(T^2/N)$ . Hence, by Markov's inequality, the probability that  $i_1, \dots, i_T$  form a good sequence is  $O(T^2/N)$ .

Second, suppose the input  $x$  is distributed according to  $\mathcal{D}_1$ . Then there exists a nonzero  $s \in \{0, 1\}^n$ , unknown to the algorithm, such that  $x_i = x_j$  whenever  $j = i \oplus s$ . Initially, all such  $s$  are equally likely under  $\mathcal{D}_1$  (the probability that there are two distinct such  $s$  for  $x$  is negligibly small, and we will ignore this here). If  $i_1, \dots, i_{k-1}$  is bad, then we have excluded  $\binom{k-1}{2}$  of the  $N-1$  possible values of  $s$ , and all other values of  $s$  are equally likely. Let  $i_k$  be the next query and  $S = \{i_k \oplus i_j : j < k\}$ .  $S$  has only  $k-1$  members, so the probability (under  $\mathcal{D}_1$ ) that  $S$  happens to contain the string  $s$  is  $\frac{k-1}{N-1-\binom{k-1}{2}}$ . If  $S$  does not contain  $s$ , then the only way to make the sequence good is if the uniformly random value  $x_{i_k}$  equals one of the  $k-1$  earlier values, which has probability  $(k-1)/N$ . Hence the probability that the bad sequence  $i_1, \dots, i_{k-1}$  remains bad, after query  $i_k$  is made, is very close to 1. In formulas:

$$\begin{aligned} \Pr[i_1, \dots, i_T \text{ is bad}] &= \prod_{k=2}^T \Pr[i_1, \dots, i_k \text{ is bad} | i_1, \dots, i_{k-1} \text{ is bad}] \\ &\geq \prod_{k=2}^T \left( 1 - \frac{k-1}{N-1-\binom{k-1}{2}} - \frac{k-1}{N} \right) \\ &\geq 1 - \sum_{k=2}^T \left( \frac{k-1}{N-1-\binom{k-1}{2}} + \frac{k-1}{N} \right). \end{aligned}$$

Here we used the fact that  $(1 - a)(1 - b) \geq 1 - (a + b)$  if  $a, b \geq 0$ . The latter sum is  $O(T^2/N)$ , so the probability (under  $\mathcal{D}_1$ ) that  $i_1, \dots, i_T$  form a good sequence is  $O(T^2/N)$ .

In both cases ( $\mathcal{U}$  and  $\mathcal{D}_1$ ), conditioned on seeing a bad sequence, the sequence of outputs is a uniformly random sequence of  $T$  distinct values. Accordingly, the advantage (over random guessing) of the algorithm trying to distinguish these two distributions is upper bounded by the probability of seeing a good sequence, which is  $O(T^2/N)$  in both cases.  $\square$

$\square$

### 2.1.5 Using Shor’s algorithm

Probably the most famous quantum algorithm to date is Shor’s polynomial-time algorithm for factoring integers [140]. Its quantum core is an algorithm that can find the *period* of a periodic sequence. Chakraborty et al. [47] used this to show that *testing* periodicity exhibits a constant-versus-polynomial quantum-classical separation. Note that the Bernstein-Vazirani property (Section 2.1.2) exhibits a constant-versus-logarithmic separation, while the Simon property (Section 2.1.4) exhibits a logarithmic-versus-polynomial separation. Periodicity-testing thus exhibits a separation that is in some ways stronger than either of those.

**Periodicity:**  $x \in [m]^N$  is *1-1-p-periodic* if it satisfies that  $x_i = x_j$  if and only if  $i = j \pmod p$  (equivalently, the elements in the sequence  $x_0, \dots, x_{p-1}$  are all unique, and after that the sequence repeats itself). For integers and  $q \leq p \leq r$  and  $m \geq p$ , such that  $N \geq 2r^2$ , define the property  $\mathcal{P}_{\text{period}}^{q,r} = \{x \in [m]^N : x \text{ is } 1-1-p\text{-periodic for some } p \in \{q, \dots, r\}\}$

Note that *for a given*  $p$  it is easy to test whether  $x$  is  $p$ -periodic or far from it: choose an  $i \in [N]$  uniformly at random, and test whether  $x_i = x_{i+kp}$  for a random positive integer  $k$ . If  $x$  is  $p$ -periodic then these values will be the same, but if  $x$  is far from  $p$ -periodic then we will detect this with good probability. However,  $r - q + 1$  different values of  $p$  are possible in  $\mathcal{P}_{\text{period}}^{q,r}$ , and this makes the property hard to test for classical testers. On the other hand, in the *quantum* case the property can be tested efficiently.

**Theorem 6** (Chakraborty et al. [47]). *For every even integer  $r \in [2, \sqrt{N})$  and constant distance  $\epsilon$ , there is a quantum property tester for  $\mathcal{P}_{\text{period}}^{r/2,r}$  using  $O(1)$  queries, while every classical property tester for  $\mathcal{P}_{\text{period}}^{r/2,r}$  makes  $\Omega(\sqrt{r/\log r \log N})$  queries. In particular, for  $r = \sqrt{N}$  testing can be done with  $O(1)$  quantum queries but requires  $\Omega(N^{1/4}/(\log N)^2)$  classical queries.*

The quantum upper bound is obtained by a small modification of Shor’s algorithm: use Shor to find the period  $p$  of input  $x$  (if there is such a period) and then test this purported period with another  $O(1)$  queries.<sup>2</sup> The classical lower bound is based on modifying proofs from Lachish and Newman [107], who showed classical testing lower bounds for more general (and hence harder) periodicity-testing problems.

In an attempt to construct oracles to separate BQP from the Polynomial Hierarchy, Aaronson [2] analyzed the problem of “Fourier checking”: roughly, the input consists of two  $\ell$ -bit Boolean functions  $f$  and  $g$ , such that  $g$  is either strongly or weakly correlated with the Fourier transform

---

<sup>2</sup>These ingredients are already present in work of Hales and Hallgren [81], and in Hales’s PhD thesis [80]. However, their results are not stated in the context of property testing, and no classical lower bounds are proved there.

of  $f$  (i.e.,  $g(x) = \text{sign}(\hat{f}(x))$ ) either for most  $x$  or for roughly half of the  $x$ ). He proved that quantum algorithms can decide this with  $O(1)$  queries, while classical algorithms need  $\Omega(2^{\ell/4})$  queries. Viewed as a property testing problem on an input of length  $N = 2 \cdot 2^\ell$  bits, this was the first constant-vs-polynomial separation between quantum and classical testers. However, neither his separation nor periodicity-testing fully answers the following question from Buhrman et al. [43].

**Question 2.** *Is there a property of  $N$ -element strings (on a moderately-sized alphabet) that can be tested with  $O(1)$  quantum queries but needs  $\Omega(N)$  classical queries?*

An unpublished result of Aaronson and Ambainis [4] is relevant here: they showed that if a (total or partial) function on  $x \in \{0, 1\}^N$  can be computed with bounded error probability using  $k$  quantum queries, then the same function can be computed by a classical randomized algorithm using  $O(N^{1-1/2k})$  queries. Hence for binary alphabets the answer to the above question is negative: everything that can be tested with  $k = O(1)$  quantum queries can be tested with  $O(N^{1-1/2k}) = o(N)$  classical queries. This can be extended to small alphabets, but the question remains open for instance when the alphabet size is  $N$ .

### 2.1.6 Using quantum counting

Grover’s quantum search algorithm [76] can be used to find the index of a 1-bit in  $x \in \{0, 1\}^N$  with high probability, using  $O(\sqrt{N})$  queries. We will not describe the algorithm here, but just note that it can be generalized to also *estimate*, for given  $S \subseteq [m]$ , the number of occurrences of elements from  $S$  in a string  $x \in [m]^N$ , using a number of queries that is much less than would be needed classically. More precisely, we have the following “quantum approximate counting” lemma, which follows from the work of Brassard et al. [36, Theorem 13]:

**Lemma 7.** *There exists a constant  $C$  such that for every set  $S \subseteq [m]$  and every positive integer  $T$ , there is a quantum algorithm that makes  $T$  queries to input  $x \in [m]^N$  and, with probability at least  $2/3$ , outputs an estimate  $p'$  to  $p = |\{i : x_i \in S\}|/N$  such that  $|p' - p| \leq C(\sqrt{p}/T + 1/T^2)$ .*

We now describe an application of this to property testing, namely to testing whether two probability distributions are equal or  $\epsilon$ -far from each other in total variation distance. Each distribution will be given as an input  $x \in [m]^N$ , which naturally induces a probability distribution  $\mathcal{D}_x$  on  $[m]$  according to the relative frequencies of the different elements:

$$\mathcal{D}_x(j) = \frac{|\{i : x_i = j\}|}{N}.$$

We can obtain a sample according to  $\mathcal{D}_x$  by just querying  $x$  on a uniformly random index  $i$ . Assuming the distribution is given in this way is quite natural in the setting of property testing, where our input is usually a very long string  $x$ , much too long to inspect each of its elements. Note that  $\mathcal{D}_x$  does not change if we permute the elements of  $x$ ; it just depends on the relative frequencies. Also note that Lemma 7 can be used to estimate the probability of  $S \subseteq [m]$  under  $\mathcal{D}_x$ .

Suppose we are given two distributions  $\mathcal{D}_x$  and  $\mathcal{D}_y$  on  $[m]$  (the distributions are given in the form of two inputs  $x, y \in [m]^N$ ), and we want to test whether these two distributions are equal or  $\epsilon$ -far in total variation distance (i.e.,  $\frac{1}{2} \sum_{j \in [m]} |\mathcal{D}_x(j) - \mathcal{D}_y(j)| \geq \epsilon$ ). Batu et al. [25] exhibited classical testers for this using  $O((m/\epsilon)^{2/3} \log m)$  queries<sup>3</sup>, and Valiant [144] proved an almost matching

---

<sup>3</sup>All these classical bounds are stated in terms of number of samples rather than number of queries, but it is not hard to see that these two complexity measures are equivalent here.

lower bound of  $\Omega(m^{2/3})$  for constant  $\epsilon$ . These bounds have both recently been improved by Chan et al. [48] to a tight  $\Theta(m^{2/3}/\epsilon^{4/3})$  (for  $\epsilon = \Omega(m^{-1/4})$ ). Bravyi et al. [38] showed that quantum testers can do better in terms of their dependence on  $m$ :

**Theorem 8** (Bravyi et al. [38]). *There is a quantum tester to test if two given distributions on  $[m]$  are equal or  $\epsilon$ -far using  $O(\sqrt{m}/\epsilon^8)$  queries.*

*Proof. (sketch)* Bravyi et al. [38] actually showed something stronger, namely that the total variation distance between two distributions can be estimated up to small additive error  $\epsilon$  using  $O(\sqrt{m}/\epsilon^8)$  quantum queries; this clearly suffices for testing. We sketch their idea here. Consider the following random process:

$$\begin{array}{l} \text{Sample } j \in [m] \text{ according to } \mathcal{D} = \frac{1}{2}(\mathcal{D}_x + \mathcal{D}_y). \\ \text{Output } \frac{|\mathcal{D}_x(j) - \mathcal{D}_y(j)|}{\mathcal{D}_x(j) + \mathcal{D}_y(j)} \end{array}$$

It is easy to see that the expected value of the output of this process is exactly the total variation distance between  $\mathcal{D}_x$  and  $\mathcal{D}_y$ , so it suffices to approximate that expected value. We sample  $j$  according to  $\mathcal{D}$  (which costs just one query), use the quantum algorithm of Lemma 7 with  $S = \{j\}$  and  $T = O(\sqrt{m}/\epsilon^6)$  queries to approximate both  $\mathcal{D}_x(j)$  and  $\mathcal{D}_y(j)$ , and output the absolute difference between these two approximations divided by their sum. Bravyi et al. [38] show that repeating this  $O(1/\epsilon^2)$  times and taking the average gives, with probability at least  $2/3$ , an  $\epsilon$ -approximation of the expected value of the above random process.  $\square$

A second problem is where we fix one of the two distributions, say to the uniform distribution on  $[m]$  (assume  $m$  divides  $N$  so we can properly “fit” this distribution in  $x \in [m]^N$ ). Goldreich and Ron [72] showed a classical testing lower bound of  $\Omega(\sqrt{m})$  queries for this, and Batu et al. [24] proved a nearly tight upper bound of  $\tilde{O}(\sqrt{m})$  queries. Bravyi et al. [38], and independently also Chakraborty et al. [47], showed that testing can be done more efficiently in the quantum case:

**Theorem 9** (Bravyi et al. [38], Chakraborty et al. [47]). *There is a quantum tester to test if a given distribution on  $[m]$  equals or is  $\epsilon$ -far from the uniform distribution on  $[m]$ , using  $O(m^{1/3}/\epsilon^2)$  quantum queries.*

*Proof. (sketch)* Pick a set  $T \subseteq [N]$  of  $t = m^{1/3}$  indices uniformly at random, and query its elements. If  $\mathcal{D}_x$  is uniform then it is very likely that all values  $\{x_i\}_{i \in T}$  are distinct, so if there is some collision then we can reject immediately. Otherwise, let  $S = \{x_i : i \in T\}$  be the  $t$  distinct results, and define  $p = |\{i : x_i \in S\}|/N$ . If  $\mathcal{D}_x$  is uniform then  $p = t/m$ , but [47, Lemma 13] shows that if  $\mathcal{D}_x$  is  $\epsilon$ -far from uniform then with high probability  $p \geq (1 + c\epsilon^2)t/m$  for some constant  $c > 0$ . Now we use the quantum algorithm of Lemma 7 with  $T = O(m^{1/3}/\epsilon^2)$  queries to obtain an estimate  $p'$  of  $p$  within additive error  $(c\epsilon^2/2)t/m$ . We accept if  $p' \leq (1 + c\epsilon^2/2)t/m$ , and reject otherwise.  $\square$

Both Bravyi et al. [38] and Chakraborty et al. [47] showed that  $\Omega(m^{1/3})$  quantum queries are also necessary, so the above result is essentially tight; the lower bound follows from a reduction from the collision problem [7]. Bravyi et al. [38] also exhibited a quantum tester for whether two distributions are equal or of disjoint support (i.e., orthogonal), using  $O(m^{1/3})$  quantum queries. Chakraborty et al. [47] extended Theorem 9 to testing equality to any fixed distribution, at the expense of a polylog factor in the number of queries. They in turn used this to obtain better quantum testers for graph isomorphism.

### 2.1.7 Using Ambainis’s algorithm

Ambainis’s element distinctness algorithm [15] acts on an input  $x \in [m]^N$ , and finds (with high probability) a pair of distinct indices such that  $x_i = x_j$  if such a pair exist, and reports “no collision” otherwise. It uses  $O(N^{2/3})$  queries, which is optimal [7]. This algorithm spawned a large class of algorithms based on *quantum walks* (see [139] for a survey).

Ambainis et al. [16] use the element distinctness algorithm to give better quantum testers for certain *graph properties*. Graph properties have some amount of symmetry: they are invariant under relabelling of vertices. Problems with “too much” symmetry are known not to admit exponential quantum speed-up in the query complexity model [3], and the symmetry inherent to graph properties makes them an interesting test case for the question of how symmetric the problems can be for which we do obtain a significant quantum advantage. Ambainis et al. [16] use the element distinctness algorithm to give  $O(N^{1/3})$ -query quantum testers for the properties of bipartiteness and being an expander in bounded-degree graphs. It is known that for classical testers,  $\tilde{\Theta}(\sqrt{N})$  queries are necessary and sufficient to test these properties. Together with the graph isomorphism tester mentioned briefly at the end of Section 2.1.6, these are the only quantum results we are aware of for testing graph properties. In contrast, graph properties have been one of the main focuses in classical property testing.

Let us describe the results of [16] a bit more precisely. The object to be tested is an  $N$ -vertex graph  $G$  of degree  $d$ , so each vertex has at most  $d$  neighbors. We think of  $d$  as a constant. The input is given as an *adjacency list*. Formally, it corresponds to an  $x \in ([N] \cup \{*\})^{N \times d}$ . The entries of  $x$  are indexed by a pair of a vertex  $v \in [N]$  and a number  $i \in [d]$ , and  $x_{v,i}$  is the  $i$ th neighbor of vertex  $v$ ;  $x_{v,i} = *$  in case  $v$  has fewer than  $i$  neighbors. A graph is **Bipartite** if its set of vertices can be partitioned into two disconnected sets, and is an **Expander** if there is a constant  $c > 0$  such that every set  $S \subseteq [N]$  of at most  $N/2$  vertices has at least  $c|S|$  neighbors outside of  $S$ .<sup>4</sup>

**Theorem 10** (Ambainis et al. [16]). *There exist quantum testers for **Bipartite** and **Expander** using  $\tilde{O}(N^{1/3})$  queries.*

*Proof. (sketch)* At a high level, the optimal *classical* testers for both properties look for collisions in a set of roughly  $\sqrt{N}$  elements. Using Ambainis’s algorithm, this can be done in roughly  $N^{1/3}$  queries.

A bipartite graph has no odd cycles. In contrast, for a graph that is far from bipartite one can show that among  $\sqrt{N}$  short ( $O(\log N)$ -step) random walks, there is likely to be a pair forming an odd cycle. Hence, fixing the randomness of the classical tester, it suffices to detect collisions in a string  $x \in [m]^{c\sqrt{N}}$ , for some constant  $c > 0$ , where the alphabet  $[m]$  corresponds to short walks in the graph. A variant of Ambainis’s algorithm can do this in  $O((c\sqrt{N})^{2/3}) = O(N^{1/3})$  queries to  $x$ . Each query to  $x$  corresponds to an  $O(\log N)$ -walk through the graph, so we use  $O(N^{1/3} \log N)$  queries to the input graph in total.

In the case of expanders, a short random walk will quickly converge to the uniform distribution. In contrast, for a graph that is far from any expander, such a walk will typically not be very close to uniform. If we sample  $k$  times from the uniform distribution over some  $s$ -element set, the expected number of collisions is  $\binom{k}{2}/s$ . In particular, for  $k \approx \sqrt{2s}$  we expect to see one collision. In contrast,  $k$  samples from a non-uniform distribution give a higher expected number of collisions. Hence if we

---

<sup>4</sup>Equivalently, if there is a constant gap between the first and second eigenvalue of  $G$ ’s normalized adjacency matrix. A crucial property of an expander is that the endpoint of a short ( $O(\log N)$ -step) random walk starting from any vertex is close to uniformly distributed over  $[N]$ . We refer to [89] for much more background on expander graphs and their many applications.



do  $c\sqrt{N}$  short random walks, for some constant  $c$ , then the expected number of collisions among the  $c\sqrt{N}$  endpoints is likely to be significantly smaller in the case of an expander than in the case of a graph that is far from every expander. Again we use a variation of Ambainis’s algorithm, this time to approximately *count* the number of collisions in an input  $x \in [m]^{c\sqrt{N}}$ , consisting of the endpoints of the  $c\sqrt{N}$  random walks. If this number is too high, we reject. This uses  $\tilde{O}(N^{1/3})$  queries to the graph. The technical details are non-trivial, but we will skip them here.  $\square$

Ambainis et al. also proved an  $\tilde{\Omega}(N^{1/4})$  quantum lower bound for testing expanders, using the polynomial lower bound method (see Section 2.2.1). They were not able to show  $N^{\Omega(1)}$  lower bounds for testing bipartiteness. This all leaves the following very interesting question open:

**Question 3.** *Is there any graph property which admits an exponential quantum speed-up?*

### 2.1.8 Quantum speed-ups for testing group-theoretic properties

Finally, a number of authors have considered quantum testers for properties of groups; we list these here without explaining them in detail.

- Friedl et al. [67] give efficient quantum testers for the property of periodic functions on groups (the testers are even *time-efficient* for Abelian groups), as well as a few other group-theoretic properties. The testers are based on the use of the (Abelian and non-Abelian) quantum Fourier transform.
- Friedl et al. [66] exhibit an efficient (poly(log  $N$ ,  $1/\epsilon$ )-query) *classical* tester for the property of  $N \times N$  multiplication tables corresponding to  $N$ -element Abelian groups, which is based on “dequantizing” a quantum tester. The distance used is the so-called “edit distance.”
- Inui and Le Gall [92], extending [66], exhibit an efficient (poly(log  $N$ ,  $1/\epsilon$ )-query) quantum tester for the property of  $N \times N$  multiplication tables corresponding to  $N$ -element *solvable* groups. In this case, no efficient classical tester is known.
- Le Gall and Yoshida [108] give classical lower bounds on various group testing problems, which in particular demonstrate an exponential separation between the classical and quantum complexities of testing whether the input is an Abelian group generated by  $k$  elements (where  $k$  is fixed).

## 2.2 Lower bounds

### 2.2.1 The polynomial method

The first *lower bounds* for quantum property testing were proven by Buhrman et al. [43]. They were based on the polynomial method [27], which we now briefly explain. The key property is:

The acceptance probability of a  $T$ -query quantum algorithm on input  $x \in \{0, 1\}^N$  can be written as an  $N$ -variate multilinear polynomial  $p(x)$  of degree  $\leq 2T$ .

Note that if we have a  $T$ -query quantum tester for some property  $\mathcal{P} \subseteq \{0, 1\}^N$ , then its acceptance probability  $p$  is a degree- $2T$  polynomial  $p$  such that  $p(x) \in [2/3, 1]$  if  $x \in \mathcal{P}$ ,  $p(x) \in [0, 1/3]$  if  $x$  is far from  $\mathcal{P}$ , and  $p(x) \in [0, 1]$  for all other  $x$ . The polynomial method derives lower bounds on the query complexity  $T$  from lower bounds on the minimal degree of such polynomials.

Our first application of this method is a result which is essentially from [43]. It says the following: if we have a property  $\mathcal{P}$  such that a (not necessarily uniform) random  $x \in \mathcal{P}$  is indistinguishable from a random  $N$ -bit string if we only look at up to  $k$  bits, then the quantum query complexity of testing  $\mathcal{P}$  is  $\Omega(k)$ .

**Theorem 11** (Buhrman et al. [43]). *Let  $\mathcal{P} \subseteq \{0, 1\}^N$  be a property such that the number of elements  $\epsilon$ -close to  $\mathcal{P}$  is  $< 2^{N-1}$ . Let  $\mathcal{D} = (p_z)$  be a distribution on  $\{0, 1\}^N$  such that  $p_z = 0$  for  $z \notin \mathcal{P}$ , and  $\mathbb{E}_{\mathcal{D}}[z_{i_1} \dots z_{i_k}] = 2^{-k}$  for all choices of  $k$  distinct indices  $i_1, \dots, i_k \in [N]$ . Then every quantum  $\epsilon$ -property tester for  $\mathcal{P}$  must make at least  $(k + 1)/2$  queries.*

*Proof.* Suppose there is a quantum algorithm which tests  $\mathcal{P}$  using  $T$  queries, where  $T < (k + 1)/2$ . Then by the polynomial method, its acceptance probability is given by a polynomial  $p(z)$  of degree at most  $2T \leq k$ . Assume towards a contradiction that the algorithm has success probability at least  $2/3$  on every input  $z$  that is in or  $\epsilon$ -far from  $\mathcal{P}$ . Then

$$\mathbb{E}_{z \sim \mathcal{D}}[p(z)] \geq \frac{2}{3}$$

and, letting  $\mathcal{P}_{close}$  be the set of  $z$  that are  $\epsilon$ -close to  $\mathcal{P}$ ,

$$\mathbb{E}_{z \sim \mathcal{U}}[p(z)] \leq \frac{|\mathcal{P}_{close}|}{2^N} + \frac{1}{3} \left( 1 - \frac{|\mathcal{P}_{close}|}{2^N} \right) < \frac{2}{3},$$

where  $\mathcal{U}$  is the uniform distribution. Write  $p(z) = \sum_{S \subseteq [N]} \alpha_S m_S(z)$ , where  $m_S$  is the monomial  $\prod_{i \in S} z_i$ . We have

$$\mathbb{E}_{z \sim \mathcal{D}}[p(z)] = \sum_{S \subseteq [N]} \alpha_S \mathbb{E}_{z \sim \mathcal{D}}[m_S(z)] = \sum_{S \subseteq [N]} \alpha_S 2^{-|S|} = \sum_{S \subseteq [N]} \alpha_S \mathbb{E}_{z \sim \mathcal{U}}[m_S(z)] = \mathbb{E}_{z \sim \mathcal{U}}[p(z)].$$

We have obtained a contradiction, which completes the proof.  $\square$

A variant of Theorem 11, which generalizes the claim to an underlying set  $[m]^N$  ( $m > 2$ ) but does not consider the property testing promise, was independently shown by Kane and Kutin [98]. It is apparently quite hard to satisfy the uniformity constraint of Theorem 11; however, it can sometimes be achieved. For example, consider any property which can be expressed as membership of a linear code  $\mathcal{C} \subseteq \{0, 1\}^N$ . A linear code is described as the set  $\{Mz : z \in \{0, 1\}^\ell\}$  for some  $N \times \ell$  matrix  $M$ . A code has *dual distance*  $d$  if every codeword  $c'$  in the dual code  $\mathcal{C}^\perp := \{z : z \cdot c = 0, \forall c \in \mathcal{C}\}$  satisfies  $|c'| \geq d$ . As Alon et al. [13] observe, it is well-known in coding theory that if  $\mathcal{C}$  has dual distance  $d$ , then any subset of at most  $d - 1$  of the bits of  $\mathcal{C}$  are uniformly distributed. For completeness, we include a proof.

**Theorem 12.** [111, Chapter 1, Theorem 10] *Let  $\mathcal{C} \subseteq \{0, 1\}^N$  be a code with dual distance  $d$ . Then every  $k < d$  bits of codewords in  $\mathcal{C}$  are uniformly distributed.*

*Proof.* Dual distance  $d$  implies that every set of  $k \leq d - 1$  rows in the matrix  $M$  are linearly independent (otherwise such a linear combination would imply the existence of a Hamming weight  $k < d$  vector  $z$  such that  $Mz = 0^N$ ). So for each submatrix  $M'$  formed by choosing  $k$  rows from  $M$ , all the rows of  $M'$  are linearly independent, hence the output  $M'z$  is uniformly distributed over  $\{0, 1\}^k$ .  $\square$

Thus, if  $\mathcal{C}$  has dual distance  $d$ , taking  $\mathcal{D}$  to be uniform over  $\mathcal{C}$  in Theorem 11 gives an  $\Omega(d)$  lower bound on the quantum query complexity of testing membership in  $\mathcal{C}$ . A natural example for which this result gives a tight lower bound is the Reed-Muller code  $R(d, \ell)$ . Each codeword of this code is a binary string of length  $N = 2^\ell$  obtained by evaluating a function  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$ , which can be written as a degree- $d$  polynomial in  $\ell$  variables over  $\mathbb{F}_2$ , at every element  $z \in \{0, 1\}^\ell$ .  $R(d, \ell)$  is known to have dual distance  $2^{d+1}$  [111, Chapter 13], so Theorem 11 implies that any quantum algorithm testing the set of degree- $d$  polynomials in  $\ell$  variables over  $\mathbb{F}_2$  must make  $\Omega(2^d)$  queries. In particular, this means that quantum algorithms obtain no asymptotic speed-up, in terms of their dependence on  $d$ , over the best classical algorithm for testing this property [13]. One can generalize this whole argument to derive quantum lower bounds for testing membership of various interesting properties corresponding to codes over  $\mathbb{F}_q$ , for  $q > 2$ ; we omit the details.

Buhrman et al. also applied the polynomial method to show, by a counting argument, that *most* properties do not have an efficient property tester. Informally speaking, there are too many properties, and too few low-degree polynomials.

**Theorem 13** (Buhrman et al. [43]). *Let  $\mathcal{P} \subset \{0, 1\}^N$  be chosen at random subject to  $|\mathcal{P}| = 2^{N/20}$ , and fix  $\epsilon$  to be a small constant. Then, except with probability exponentially small in  $N$ , any quantum  $\epsilon$ -property tester for  $\mathcal{P}$  must make  $\Omega(N)$  queries.*

A more involved application of the polynomial method is the tight  $\Omega(\log N)$  lower bound that Koiran et al. [104] proved for the quantum query complexity of Simon’s problem. With a bit of work, their proof also works to show that the property tester presented in Section 2.1.4 is essentially optimal.

Another highly non-trivial application of the polynomial method is the  $\tilde{\Omega}(N^{1/4})$  lower bound of Ambainis et al. [16] for testing the property of a bounded-degree graph being an **Expander** (see Section 2.1.7). Their lower bound is inspired by the one for the collision problem [7], and at a high level works as follows. They give an input distribution  $\mathcal{D}_\ell$  over  $N$ -vertex  $d$ -regular graphs with  $\ell$  components, and show that the acceptance probability of a  $T$ -query quantum tester can be written as an  $O(T \log T)$ -degree bivariate polynomial  $p(\ell, M)$  in  $\ell$  and another parameter  $M \approx N$ . A random graph of  $\ell = 1$  components is very likely to be an expander, so  $p(1, M) \approx 1$ ; on the other hand, every graph with  $\ell > 1$  components will be far from an expander, so  $p(\ell, M) \approx 0$  for integers  $\ell > 1$ . They then use results about polynomial approximation to show that such polynomials need degree  $\Omega(N^{1/4})$ .

## 2.2.2 The adversary method

The two main lower bound methods that we know for quantum query complexity are the above polynomial method, and the so-called *adversary method*, introduced by Ambainis [14]. For a long time this adversary method faced the so-called “property testing barrier” [91]: for every  $N$ -bit partial Boolean function where 0-inputs and 1-inputs have Hamming distance  $\Omega(N)$ , the method can prove only a *constant* lower bound on the query complexity. Note that all testing problems for classical properties fall in this regime, since the 0-inputs are required to be far from all 1-inputs (i.e., elements of the property).

However, Høyer et al. [91] generalized Ambainis’s method to something substantially stronger, which can prove optimal bounds for quantum property testing. We now describe their “negative weights” adversary bound. Let  $F : D \rightarrow \{0, 1\}$ , with  $D \subseteq [m]^N$ , be a Boolean function. An *adversary matrix*  $\Gamma$  for  $F$  is a real-valued matrix whose rows and columns are indexed by all  $x \in D$ , satisfying that  $\Gamma_{xy} = 0$  whenever  $f(x) = f(y)$ . Let  $\Delta_j$  be the Boolean matrix whose

rows and columns are indexed by all  $x \in D$ , such that  $\Delta_j[x, y] = 1$  if and only if  $x_j \neq y_j$ . The (negative-weights) adversary bound for  $F$  is given by the following expression:

$$\text{ADV}^\pm(F) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{j \in [N]} \|\Gamma \circ \Delta_j\|},$$

where  $\Gamma$  ranges over all adversary matrices for  $F$ , ‘ $\circ$ ’ denotes entry-wise product of two matrices, and ‘ $\|\cdot\|$ ’ denotes operator norm (largest singular value) of the matrix.

Høyer et al. [91] showed that this quantity is a valid lower bound: every quantum algorithm that computes  $F$  with error probability  $\leq \epsilon$  needs to make at least  $\frac{1}{2}(1 - \sqrt{\epsilon(1 - \epsilon)})\text{ADV}^\pm(F)$  queries. Subsequently, Reichardt et al. [132, 109] showed this lower bound is actually essentially tight: for every Boolean function  $F$  there is a quantum algorithm computing it with error  $\leq 1/3$  using  $O(\text{ADV}^\pm(F))$  queries. Since property testing is just a special of this (the 1-inputs of  $F$  are all  $x \in \mathcal{P}$ , and the 0-inputs are all  $x$  that are far from  $\mathcal{P}$ ), in principle the adversary bound characterizes the quantum complexity of testing classical properties. However, in practice it is often hard to actually calculate the value of  $\text{ADV}^\pm(F)$ , and we are not aware of good quantum property testing lower bounds that have been obtained using this method.

### 2.2.3 A communication complexity method?

Recently, a very elegant lower bound method for classical property testing was developed by Blais et al. [32], based on *communication complexity*. In the basic setting of communication complexity [154, 106], two parties (Alice with input  $x$  and Bob with input  $y$ ) try to compute a function  $F(x, y)$  that depends on both of their inputs, using as little communication as possible. This is a very well-studied model with many applications, particularly to lower bounds. Blais et al. [32] showed for the first time how to get property testing lower bounds from communication complexity. Their idea is to convert a  $T$ -query property tester for some property  $\mathcal{P}$  into a protocol for some related communication problem  $F$ , by showing that 1-inputs  $(x, y)$  for  $F$  somehow correspond to elements of  $\mathcal{P}$ , while 0-inputs  $(x, y)$  for  $F$  correspond to elements that are far from  $\mathcal{P}$ . The more efficient the tester, the less communication the protocol needs. Communication complexity lower bounds for  $F$  then imply lower bounds on the complexity  $T$  of the tester.

This is best explained by means of an example. A  $k$ -linear function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  is a linear function that depends on exactly  $k$  of its input bits: there exists a weight- $k$   $x \in \{0, 1\}^n$  such that  $f(i) = i \cdot x \bmod 2$  for all  $i \in \{0, 1\}^n$ . Let  $\mathcal{P}$  be the set of  $k$ -linear functions, and assume  $k$  is even. Suppose we have a randomized  $T$ -query tester  $\mathcal{T}$  for  $\mathcal{P}$ . We will show how such a tester induces an efficient communication protocol for the communication complexity problem of deciding whether weight- $k/2$  strings  $x$  and  $y$  are *disjoint* or not (i.e., whether  $x \wedge y = 0^n$ ). Alice, who received input  $x$ , forms the function  $f(i) = i \cdot x$  and Bob forms the function  $g(i) = i \cdot y$ . Consider the function  $h(i) = i \cdot (x \oplus y)$ . Since  $|x \oplus y| = |x| + |y| - 2|x \wedge y|$  and  $|x| + |y| = k$ , the function  $h$  is a  $(k - 2|x \wedge y|)$ -linear function. In particular,  $h$  is a  $k$ -linear function if  $x$  and  $y$  are disjoint, and  $1/2$ -far from any  $k$ -linear function if  $x$  and  $y$  intersect. Now Alice and Bob use a shared random coin to jointly sample one of the deterministic testers that make up the property tester  $\mathcal{T}$ . Note that they can simulate a query  $i$  to  $h$  by 2 bits of communication: Alice sends  $i \cdot x$  to Bob and Bob sends  $i \cdot y$  to Alice. Hence a  $T$ -query tester for  $\mathcal{P}$  implies a  $2T$ -bit communication protocol for disjointness on  $k$ -bit inputs  $x$  and  $y$ . Plugging in the known communication lower bound of  $\Omega(k)$  bits for multi-round disjointness on weight- $k/2$  inputs implies that every classical tester for  $k$ -linear functions needs  $\Omega(k)$  queries, which is nearly tight [31]. And plugging in a better  $\Omega(k \log k)$  lower bound for *one-way* communication complexity gives  $T = \Omega(k \log k)$  for *non-adaptive* classical

testers (i.e., testers where the next index to query is independent of the outcomes of the earlier queries), which is tight [60, 44].

Can we use the same idea to prove lower bounds on *quantum* testers? In principle we can, but notice that the overhead when converting a *quantum* tester into a communication protocol is much worse than in the classical case. In the classical case, thanks to the fact that Alice and Bob can use shared randomness to fix a deterministic tester, they both know at each point in the protocol which query  $i$  will be made next. Hence they only need to communicate the constant number of bits corresponding to the answer to that query, so the overall communication is  $O(T)$ . In the quantum case, the queries can be made in superposition, so the conversion will have an overhead of  $O(n)$  qubits of communication: each query will be “simulated” by an  $n$ -qubit message (superposition over  $is$ ) from Alice to Bob, and another such message from Bob to Alice. Now a  $T$ -query quantum tester induces an  $O(Tn)$ -qubit quantum protocol for disjointness. But the best lower bound one can hope for on communication complexity problems with  $n$ -bit inputs is  $\Omega(n)$ , which gives only a trivial  $T = \Omega(1)$  lower bound! This, however, is not because we did the reduction in a suboptimal way: for example, testing  $k$ -linear functions can be done with  $O(1)$  quantum queries, similarly to Section 2.1.2.

**Question 4.** *Can some modification of the ideas of Blais et al. [32] be used for non-trivial lower bounds on quantum testers?*

### 3 Classical testing of quantum properties

In this section we will survey what is known about classical testing of two kinds of quantum objects: implementations of basic unitary operations, and implementations of quantum protocols for certain games.

Before we go there, let us mention that there is another way in which one can consider classical testing of quantum properties: by imagining that we are given classical access to a quantum object which is too large for an efficient classical description. For example, we might be given access to an unknown pure state  $|\psi\rangle$  of  $n$  qubits by being allowed to query arbitrary amplitudes in the computational basis at unit cost. This then becomes an entirely classical property testing problem. Some natural properties of quantum states in this context have indeed been studied classically; one example is the *Schmidt rank*. A bipartite state  $|\psi\rangle$  on systems  $AB$  is said to have Schmidt rank  $r$  if it can be written as  $|\psi\rangle = \sum_{i=1}^r \sqrt{\lambda_i} |v_i\rangle |w_i\rangle$  for pairwise orthonormal sets of states  $\{|v_i\rangle\}$ ,  $\{|w_i\rangle\}$  and non-negative  $\lambda_i$ ; this is known as the Schmidt decomposition of  $|\psi\rangle$ . A tester for this property follows from work of Krauthgamer and Sasson [105], who have given an efficient tester for low-rank matrices. Their algorithm distinguishes between the cases that a  $d \times d$  matrix  $M$  is rank at most  $r$ , or at least an  $\epsilon$ -fraction of the entries in  $M$  must be changed to make  $M$  rank at most  $r$ , and queries only  $O((r/\epsilon)^2)$  elements of the matrix. If we think of  $M$  as the amplitudes of a bipartite pure quantum state  $|\psi\rangle \in (\mathbb{C}^d)^{\otimes 2}$  (i.e.,  $M_{ij} = \langle i | \langle j | \psi \rangle$ ), this is equivalent to a tester for the property of  $|\psi\rangle$  having Schmidt rank at most  $r$ .

#### 3.1 Self-testing gates

When experimentalists try to implement a quantum computer in the usual circuit model, they will have to faithfully implement a number of basic quantum operations, called elementary *gates*. Suppose we can implement some superoperator<sup>5</sup>  $\mathbf{G}$ . How can we test whether it indeed implements

<sup>5</sup>Completely positive trace-preserving linear map, a.k.a. “quantum channel.”

the gate it is supposed to implement? We can prepare a computational basis state, apply  $\mathbf{G}$  to it a number of times, and measure the resulting state in the computational basis. Say  $\mathbf{G}$  is supposed to implement the Hadamard gate. If we prepare  $|0\rangle$ , apply  $\mathbf{G}$  once and measure in the computational basis, the probability to see a 0 should be  $1/2$ . Similarly, if we prepare  $|0\rangle$ , apply  $\mathbf{G}$  *twice* and measure, the probability to see 0 should be 1. These are so-called *experimental equations* that a self-tester can test by repeatedly performing the corresponding experiments. It should be noted that such equations cannot fully determine a gate. For example, if  $\mathbf{G}$  is the Hadamard gate in a basis where  $|1\rangle$  is replaced with  $e^{i\phi}|1\rangle$ , then no experiment as described above can detect this:  $H$  and its cousin satisfy exactly the same experimental equations. Still, van Dam et al. [59] showed that such experimental equations are surprisingly powerful and can essentially characterize many gate sets, including some universal sets.<sup>6</sup> For concreteness we will focus below on a specific universal set, namely the one consisting of the Hadamard gate  $H$ , the  $\pi/4$ -phase gate  $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ , and the controlled-NOT operation. This set has the added benefit that it supports fault-tolerant quantum computing: implementing these gates up to small error suffices for universal quantum computing.

Let us first define experimental equations a bit more precisely. Following van Dam et al. [59], we use  $\Pr^c[\rho]$  to denote the probability that measuring the (pure or mixed) state  $\rho$  in the computational basis gives outcome  $c$ . Then an experimental equation in one superoperator variable  $\mathbf{G}$  is of the form

$$\Pr^c[\mathbf{G}^k(|b\rangle\langle b|)] = r,$$

for  $b, c \in \{0, 1\}$ , positive integer  $k$ , and  $r \in [0, 1]$ . Note that we assume here that we can apply exactly the same superoperator  $\mathbf{G}$  more than once. An experimental equation in two variables  $\mathbf{F}$  and  $\mathbf{G}$  is of the form

$$\Pr^0[\mathbf{F}^{k_1}\mathbf{G}^{\ell_1} \dots \mathbf{F}^{k_t}\mathbf{G}^{\ell_t}(|b\rangle\langle b|)] = r,$$

for  $b \in \{0, 1\}$ , integers  $k_1, \dots, k_t, \ell_1, \dots, \ell_t$ , and  $r \in [0, 1]$  (concatenation of superoperators here denotes composition). We can similarly write experimental equations in more than two operators, and on systems of more than one qubit. Such experimental equations are all the things a self-tester can test.

Suppose one-qubit operators  $\mathbf{H}$  and  $\mathbf{T}$  are intended to be the Hadamard gate  $H$  and the  $\pi/4$ -phase gate  $T$ , respectively, and two-qubit operator  $\mathbf{C}$  is supposed to be CNOT (with slight abuse of notation we identify unitary gates with the corresponding superoperators here). Let us see to what extent we can test this. To start, the following experimental equations are clearly necessary for  $\mathbf{H}$ :

$$\Pr^0[\mathbf{H}(|0\rangle\langle 0|)] = 1/2$$

$$\Pr^0[\mathbf{H}^2(|0\rangle\langle 0|)] = 1$$

$$\Pr^1[\mathbf{H}^2(|1\rangle\langle 1|)] = 1$$

Van Dam et al. [59, Theorem 4.2] showed that these equations *characterize* the Hadamard gate up to the one remaining degree of freedom that we already mentioned, in the following sense:  $\mathbf{H}$  satisfies the above three equations if and only if there exists  $\phi \in [0, 2\pi)$  such that  $\mathbf{H}$  equals (the

---

<sup>6</sup>A finite set of gates is *universal* if every  $n$ -qubit unitary can be approximated arbitrarily well (in the operator norm) by means of a circuit consisting of these gates. We cannot hope to represent all unitaries *exactly*, because the set of circuits over a finite (or even countable) set of elementary gates is only countable, hence much smaller than the uncountable set of all unitaries.

superoperator corresponding to)  $H_\phi$ , which is the Hadamard gate where  $|1\rangle$  is replaced with  $e^{i\phi}|1\rangle$ . The unknown phase  $\phi$  cannot be ignored, because it might interact with the effects of other gates.

The following two experimental equations are clearly necessary for  $\mathbf{T}$ :

$$\begin{aligned}\Pr^0[\mathbf{T}(|0\rangle\langle 0|)] &= 1 \\ \Pr^1[\mathbf{T}(|1\rangle\langle 1|)] &= 1\end{aligned}$$

These two equations are far from sufficient for characterizing the  $T$  gate; for example, every diagonal unitary will satisfy these two equations, as would the superoperator that fully decoheres a qubit in the computational basis. However, by introducing some additional equations involving both  $\mathbf{H}$  and  $\mathbf{T}$  we can do better:

$$\begin{aligned}\Pr^0[\mathbf{HT}^8\mathbf{H}(|0\rangle\langle 0|)] &= 1 \\ \Pr^0[\mathbf{HTH}(|0\rangle\langle 0|)] &= \frac{1}{2}(1 + \cos(\pi/4))\end{aligned}$$

Note that if  $\mathbf{H} = H$ , then both  $\mathbf{T} = T$  and its inverse  $\mathbf{T} = T^{-1}$  would satisfy the above equations. Van Dam et al. [59, Theorem 4.4] showed that a pair of superoperators  $\mathbf{H}$  and  $\mathbf{T}$  satisfy the above set of 7 equations if and only if there exists  $\phi \in [0, 2\pi)$  such that  $\mathbf{H} = H_\phi$ , and  $\mathbf{T}$  corresponds to either  $T$  or  $T^{-1}$ .

To complete our self-test, consider the superoperator  $\mathbf{C}$ . The following experimental equations are clearly necessary for  $\mathbf{C}$  to equal CNOT:

$$\begin{aligned}\Pr^{00}[\mathbf{C}(|00\rangle\langle 00|)] &= 1 \\ \Pr^{01}[\mathbf{C}(|01\rangle\langle 01|)] &= 1 \\ \Pr^{11}[\mathbf{C}(|10\rangle\langle 10|)] &= 1 \\ \Pr^{10}[\mathbf{C}(|11\rangle\langle 11|)] &= 1\end{aligned}$$

These equations ensure that  $\mathbf{C}$  implements the same permutation of basis states as the CNOT gate. This is still far from sufficient. We add the following experimental equations, which describe the desired interaction between CNOT and  $H$ :

$$\begin{aligned}\Pr^{00}[(\mathbf{I} \otimes \mathbf{H})\mathbf{C}(\mathbf{I} \otimes \mathbf{H})(|00\rangle\langle 00|)] &= 1 \\ \Pr^{10}[(\mathbf{I} \otimes \mathbf{H})\mathbf{C}(\mathbf{I} \otimes \mathbf{H})(|10\rangle\langle 10|)] &= 1 \\ \Pr^{00}[(\mathbf{H} \otimes \mathbf{I})\mathbf{C}^2(\mathbf{H} \otimes \mathbf{I})(|00\rangle\langle 00|)] &= 1 \\ \Pr^{01}[(\mathbf{H} \otimes \mathbf{I})\mathbf{C}^2(\mathbf{H} \otimes \mathbf{I})(|01\rangle\langle 01|)] &= 1 \\ \Pr^{00}[(\mathbf{H} \otimes \mathbf{H})\mathbf{C}(\mathbf{H} \otimes \mathbf{H})(|00\rangle\langle 00|)] &= 1\end{aligned}$$

Van Dam et al. [59, Theorem 4.5] showed that if superoperators  $\mathbf{H}$ ,  $\mathbf{T}$ ,  $\mathbf{C}$  satisfy the above 16 experimental equations, then there exists  $\phi \in [0, 2\pi)$  such that:

$$\mathbf{H} = H_\phi; \mathbf{T} = T \text{ or } \mathbf{T} = T^{-1}; \mathbf{C} = C_\phi,$$

where  $C_\phi$  denotes (the superoperator corresponding to the) controlled-NOT gate with  $|1\rangle$  replaced with  $e^{i\phi}|1\rangle$ .

Because our apparatuses are never perfect, we cannot hope to implement the elementary gates exactly. Fortunately, thanks to quantum fault-tolerant computing it suffices if we can implement

them up to small error (in fact different applications of the same superoperator can have different errors and need not all be identical). Hence we also cannot expect the gates that we are testing to *exactly* satisfy all of the above experimental equations. Furthermore, even if they did satisfy these equations exactly, we would never be able to perfectly test this with a finite number of experiments. Accordingly, we would like the test consisting of these experimental equations to be *robust*, in the sense that if  $\mathbf{H}$ ,  $\mathbf{T}$ , and  $\mathbf{C}$  *approximately* satisfy these equations, then they will be *close* to the gates they purport to be. We say that superoperators  $\epsilon$ -satisfy a set of experimental equations if for each of the equations, the left- and right-hand sides differ by at most  $\epsilon$ . Closeness between superoperators is measured in the superoperator norm induced by the trace norm:  $\|G\|_\infty = \sup\{\|G(V)\|_1 : \|V\|_1 = 1\}$ . Van Dam et al. [59, Theorem 6.5, last item] indeed showed that the above equations constitute a robust self-test:

**Theorem 14** (van Dam et al. [59]). *There exists a constant  $c$  such that for all  $\epsilon > 0$  the following holds. If superoperators  $\mathbf{H}$ ,  $\mathbf{T}$ ,  $\mathbf{C}$   $\epsilon$ -satisfy the above 16 experimental equations, then there exists  $\phi \in [0, 2\pi)$  such that:*

$$\|\mathbf{H} - H_\phi\|_\infty \leq c\sqrt{\epsilon}; \|\mathbf{T} - T\|_\infty \leq c\sqrt{\epsilon} \text{ or } \|\mathbf{T} - T^{-1}\|_\infty \leq c\sqrt{\epsilon}; \|\mathbf{C} - C_\phi\|_\infty \leq c\sqrt{\epsilon}.$$

Each triplet  $\mathbf{H}$ ,  $\mathbf{T}$ ,  $\mathbf{C}$  that passes the above test is a universal (and fault-tolerant) set of elementary gates, so can in principle be used to realize any quantum circuit. The fact that we do not know  $\phi$  is not important when implementing a circuit using this triplet of gates: since  $\phi$  cannot be detected by any experimental equations, it cannot affect the classical input-output behavior of a quantum circuit built from these superoperators. We also do not know whether  $\mathbf{T}$  approximately equals  $T$  or its inverse  $T^{-1}$ . Using Hadamard and CNOTs cannot help distinguish these two cases, because they only differ in a minus sign for the imaginary unit (something gates with real entries cannot pick up). However, precisely because such a change is undetectable experimentally, we can just build our circuit assuming  $\mathbf{T}$  is close to  $T$ ; if it is close to  $T^{-1}$  instead, that will incur no observable differences in the input-output behavior of our circuit.

In addition to the above result, van Dam et al. [59] also showed a number of other families of gates to be robustly self-testable, and proved more general robustness results. In follow-up work, Magniez et al. [112] study self-testing of quantum circuits together with measurement apparatuses and sources of EPR-pairs, introducing notions of simulation and equivalence.

## 3.2 Self-testing protocols

In addition to quantum gates and circuits, a large area of application of quantum self-testing is in multi-party quantum *protocols*. Here typically two or more parties share an entangled state (in the two-party case these are often EPR-pairs) on which they operate locally. Experimentalists often need to test that their apparatuses produce the required entangled state, or at least something close to it, and that the local operations and measurements act as required. Unless we somehow already have some other trusted quantum objects available, we are in the self-testing regime: we would like to test a quantum object by classically interacting with it, without making assumptions about the measurement apparatuses, the states used, or even the dimension of the Hilbert spaces that are involved.

Again, for concreteness we will focus on testing protocols for one specific example in the two-party setting<sup>7</sup>, namely the famous CHSH game [55]. This is defined as follows.

---

<sup>7</sup>In the three-party setting, the most famous game is the GHZ game [74]. Colbeck [56] seems to have been the first to give a self-testing result for this.



Alice and Bob receive uniformly distributed inputs  $x, y \in \{0, 1\}$ , respectively. They output  $a, b \in \{0, 1\}$ , respectively. They *win* the game if the XOR of the outputs equals the AND of the inputs:  $a \oplus b = xy$ .

Alice and Bob want to maximize their probability of winning this game, without communication between them. It is known that classical protocols can win with probability 0.75, but not more, even when they use shared randomness. In contrast, there exists a quantum protocol that wins the game with probability  $\cos(\pi/8)^2 \approx 0.854$ , which is optimal even if the players are allowed to share much larger entangled states [54]. This “Bell inequality violation” has been confirmed by many experiments, albeit with a few remaining experimental “loopholes,” suggesting that Nature does not behave according to classical physics (see the recent survey by Brunner et al. [40] for much more on such nonlocality).

The specific quantum protocol  $P^*$  that achieves the optimal winning probability  $\cos(\pi/8)^2$  uses one EPR-pair as starting state. Depending on their respective inputs  $x$  and  $y$ , Alice and Bob do the following specific projective measurements (defined in terms of the Pauli matrices, see Eq. (3) below): Alice measures the observable  $\frac{1}{\sqrt{2}}(Z + (-1)^x X)$ , and Bob measures the observable  $Z$  if  $y = 0$  and  $X$  if  $y = 1$ . How much freedom do we have in such “good” quantum protocols for the CHSH game? Popescu and Rohrlich [130] and Braunstein et al. [37] independently showed that any protocol that wins CHSH with maximal probability needs to start with an EPR-pair<sup>8</sup>, or something that can be turned into an EPR-pair (possibly in tensor product with another state shared between Alice and Bob) using local unitary operations. The correct attribution of this result is not completely clear, see also the work of Summers and Werner [142] and Tsirelson [143, p. 11].

However, as in the previous section, *robustness* is important: we expect that if a protocol wins the CHSH game with *close-to-maximal* probability, then its entangled state must be *close* to an EPR-pair.<sup>9</sup> Such a robust result was proved independently in [117, 118]:

**Theorem 15** ([117, 118]). *If a protocol wins CHSH with probability at least  $\cos(\pi/8)^2 - \epsilon$ , then (up to local operations on Alice and Bob’s side) its starting state must be  $O(\sqrt{\epsilon})$ -close to an EPR-pair, and its measurements must be  $O(\sqrt{\epsilon})$ -close to the measurements of protocol  $P^*$ .*

Accordingly, we can use this to test whether given states are close to EPR-pairs: run the CHSH protocol on them and see if the winning probability is close to the optimal value  $\cos(\pi/8)^2$ . McKague et al. [117] give a more general framework for bipartite robust self-testing that subsumes the CHSH inequality, the Mayers-Yao self-test (simplifying [112]), as well as others. Yang and Navascués [152] give robust self-tests for any entangled two-qubit states, not just maximally entangled ones; the noise-resistance was further improved in [153]. McKague [116] and Miller and Shi [118] give results about self-testing of states shared by more than two parties.

Recently, Reichardt et al. [133] proved a robustness result for playing *many instances* of CHSH: every quantum protocol that wins roughly 85% of a sequence of  $k$  given instances of the CHSH game, must have a block of  $m = k^{\Omega(1)}$  instances where it starts essentially (up to local operations and small differences) from  $m$  EPR-pairs and runs  $m$  instances of protocol  $P^*$ . This is an important step towards the goal of having a classical system “command” an untrusted quantum system, in the sense of forcing that system to either use the states and operations that you want it to use, or be detected if it deviates too much from those states and operations. Such control enables

<sup>8</sup>Or a direct sum of EPR-pairs in case of higher-dimensional spaces.

<sup>9</sup>The earlier work of Mayers and Yao [114, 115] that started the area of self-testing of quantum states also had a protocol for self-testing EPR-pairs, albeit based on more than the CHSH game.

various kinds of device-independent quantum cryptography, as well as the ability to offload general quantum computation to untrusted devices.

## 4 Quantum testing of quantum properties

In the third part of this survey we discuss quantum testers for quantum properties. The first decision we have to take in this setting is how the quantum object which we wish to test is presented to us. The two options are a quantum presentation (i.e., we are given access to the object as a black box, which can be used in a quantum algorithm), or a classical presentation (i.e., we are given an efficient classical description of the object, such as a quantum circuit). We concentrate on the former option (Sections 4.1–5.2), as this seems to be the most natural generalization of ideas from classical property testing. However, in Section 5.3 we also discuss the latter option, which turns out to be important in quantum computational complexity.

Our focus in this survey is on quantum tests for quantum properties which generalize the idea of classical property testing. That is, tests which are designed to distinguish quantum states (or operations) with some property from those far from having that property, given access to the state (or operation) as a black box. We also mention here two related and well-studied areas elsewhere in quantum information theory. The first is quantum state discrimination, which can be seen as a quantum generalization of classical hypothesis testing. The archetypal problem in this setting is as follows: given the ability to create copies of an unknown quantum state  $\rho$  picked from a known set  $S$  of quantum states, identify  $\rho$ . See the surveys [22, 49] for detailed reviews of this area. The second is the question of directly estimating some quantity of interest about a completely unknown quantum state  $\rho$ , given access to multiple copies of the state, without performing full tomography. Results of this form include direct estimation of the spectrum of  $\rho$  [100], estimation of polynomials in the entries of  $\rho$  [39], and estimation of quantities related to entanglement (e.g., [77]).

We begin our discussion of quantum properties by considering properties of quantum states.

### 4.1 Pure states

A pure state  $|\psi\rangle$  of a  $d$ -dimensional quantum system is described by a  $d$ -dimensional complex unit vector (technically, a ray; that is,  $e^{i\theta}|\psi\rangle$  is equivalent to  $|\psi\rangle$  for all real  $\theta$ ). A property of  $d$ -dimensional, pure quantum states is therefore a set  $\mathcal{P} \subseteq \mathbb{C}^d$ . One can naturally generalize this to properties of pairs of quantum states, where  $\mathcal{P} \subseteq \mathbb{C}^d \times \mathbb{C}^d$ , etc.

There is a natural measure of distance between quantum states  $|\psi\rangle$  and  $|\phi\rangle$ : the trace distance

$$D(|\psi\rangle, |\phi\rangle) := \frac{1}{2} \|\ |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1 = \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \quad (1)$$

Here  $\|\cdot\|_1$  is the trace norm (Schatten 1-norm)  $\|M\|_1 := \text{tr}|M|$ . If two states have trace distance  $\epsilon$ , the optimal worst-case success probability of distinguishing them via a measurement is exactly  $(1 + \epsilon)/2$  [86, 124]. We therefore say that  $|\psi\rangle$  is  $\epsilon$ -close to having property  $\mathcal{P}$  if

$$D(|\psi\rangle, \mathcal{P}) := \inf_{|\phi\rangle \in \mathcal{P}} D(|\psi\rangle, |\phi\rangle) \leq \epsilon,$$

and similarly that  $|\psi\rangle$  is  $\epsilon$ -far from having property  $\mathcal{P}$  if  $D(|\psi\rangle, \mathcal{P}) \geq \epsilon$ . If  $|\psi\rangle$  is  $\epsilon$ -close to having property  $\mathcal{P}$ , there is no hope of certifying that  $|\psi\rangle \notin \mathcal{P}$  with worst-case bias larger than  $\epsilon$ .

The complexity of algorithms for testing pure quantum states is measured by the number of copies of the test state  $|\psi\rangle$  required to distinguish between the two cases that a)  $|\psi\rangle \in \mathcal{P}$ , or b)

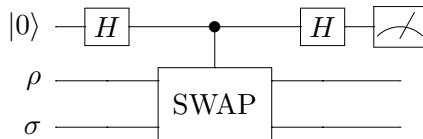
$|\psi\rangle$  is  $\epsilon$ -far away from having property  $\mathcal{P}$ . We therefore say that  $\mathcal{P}$  can be  $\epsilon$ -tested with  $q$  copies if there exists a quantum algorithm which uses  $q$  copies of the input state to distinguish between these two cases, and fails with probability at most  $1/3$  on any input. As with classical property testers, we say that a tester has *perfect completeness* if it accepts every state in  $\mathcal{P}$  with certainty. Crucially, we look for algorithms where the number of copies used scales only in terms of  $\epsilon$ , and there is no dependence on the dimension  $d$ , making this a fair analog of the classical concept. If we cannot find such an algorithm, we attempt to minimize the dependence on  $d$ .

#### 4.1.1 Equality

The first property we consider is extremely basic, but a useful building block for more complicated protocols: whether the input state is equal to some fixed state. We say that a state  $|\psi\rangle$  satisfies the **Equality to  $|\phi\rangle$**  property if  $|\psi\rangle = e^{i\theta}|\phi\rangle$  for some real  $\theta$ ; it is necessary to allow an arbitrary phase  $\theta$  in the definition of this property, as  $|\psi\rangle$  cannot be distinguished from  $e^{i\theta}|\psi\rangle$  by any measurement. A natural test for **Equality to  $|\phi\rangle$**  is simply to perform the measurement  $\{|\phi\rangle\langle\phi|, I - |\phi\rangle\langle\phi|\}$  on  $|\psi\rangle$ , and accept if and only if the first outcome is obtained. The probability of acceptance is precisely  $|\langle\psi|\phi\rangle|^2$ , so if  $|\psi\rangle$  satisfies the property, the test accepts with certainty. On the other hand, if  $D(|\psi\rangle, |\phi\rangle) = \epsilon$ , the test rejects with probability  $\epsilon^2$ . Via repetition, we find that for any  $|\phi\rangle$ , **Equality to  $|\phi\rangle$**  can be tested with  $O(1/\epsilon^2)$  copies.

We remark that this immediately generalizes to the problem of testing whether  $|\psi\rangle \in \mathbb{C}^d$  is contained in a known subspace  $S \subseteq \mathbb{C}^d$ . Here the prescription is to perform the measurement  $\{\Pi_S, I - \Pi_S\}$   $O(1/\epsilon^2)$  times, where  $\Pi_S$  is the projector onto  $S$ , and accept if and only if the first outcome is obtained every time. For example, this allows the property **Permutation Invariance** to be tested efficiently, where  $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$  satisfies the property if it is invariant under any permutation of the  $n$  subsystems. As  $|\psi\rangle$  is permutation-invariant if and only if it is contained in the symmetric subspace of  $(\mathbb{C}^d)^{\otimes n}$ , projecting onto this subspace gives an efficient test for this property. This procedure, which is known as *symmetrization*, has been studied in the context of quantum fault-tolerance and can be performed efficiently [21]; see Section 4.2.2 below for a description of how this can be achieved via the powerful primitive of generalized phase estimation.

Another immediate generalization of **Equality to  $|\phi\rangle$**  is the question of testing whether two *unknown* states are the same. We say that two states  $|\psi\rangle, |\phi\rangle$  satisfy the **Equality** property if  $|\psi\rangle = e^{i\theta}|\phi\rangle$  for some real  $\theta$ . In order to test this property, we will use a simple but important procedure known as the *swap test*. This was used by Buhrman et al. [42] to demonstrate an exponential separation between the quantum and classical models of simultaneous message passing (SMP) communication complexity, and has since become a standard tool in quantum algorithm design. In the test, we take two (possibly mixed) states  $\rho, \sigma$  as input and attach an ancilla qubit in state  $|0\rangle$ . We then apply a Hadamard gate to the ancilla, followed by a controlled-SWAP gate (controlled on the ancilla), and another Hadamard gate. We then measure the ancilla qubit and accept if the answer is 0. This is illustrated by the following circuit.



One can show [42, 103] that the swap test accepts with probability

$$\frac{1}{2} + \frac{1}{2} \text{tr}(\rho\sigma),$$

which for pure states  $|\psi\rangle, |\phi\rangle$  is equal to  $(1 + |\langle\psi|\phi\rangle|^2)/2 = 1 - D(|\psi\rangle, |\phi\rangle)^2/2$ . In particular, if this test is applied to two pure states which satisfy the **Equality** property then the test accepts with certainty. On the other hand, if the states are  $\epsilon$ -far away from equal, then by definition

$$\inf_{|\xi\rangle} D(|\psi\rangle|\phi\rangle, |\xi\rangle^{\otimes 2}) \geq \epsilon.$$

But

$$\inf_{|\xi\rangle} D(|\psi\rangle|\phi\rangle, |\xi\rangle^{\otimes 2}) = \sqrt{1 - \sup_{|\xi\rangle} |\langle\psi|\xi\rangle\langle\phi|\xi\rangle|^2} \leq \sqrt{1 - |\langle\psi|\phi\rangle|^2} = D(|\psi\rangle, |\phi\rangle),$$

where the inequality follows by taking  $|\xi\rangle = |\phi\rangle$ . Thus the test rejects with probability at least  $\epsilon^2/2$ , so  $O(1/\epsilon^2)$  repetitions suffice to detect states  $\epsilon$ -far away from equal with constant probability; in other words, **Equality** can be tested with  $O(1/\epsilon^2)$  copies. The swap test is in fact optimal among all testers for this property which have perfect completeness and use one copy of each of the input states. To see this, observe that the swap test is precisely the operation of projecting onto the symmetric subspace of  $(\mathbb{C}^d)^{\otimes 2}$ . Any tester which accepts every pair of equal states  $|\psi\rangle^{\otimes 2}$  must accept every state in this subspace, so the swap test is the most refined test of this type. One can generalize this to prove that the swap test is also optimal (in some sense) among tests which are allowed two-sided error [97].

The property of **Equality** can be generalized further, to the question of testing whether  $n$  pure states  $|\psi_1\rangle, \dots, |\psi_n\rangle$  are equal. The natural tester for this property, generalizing the swap test, is to project onto the symmetric subspace of  $(\mathbb{C}^d)^{\otimes n}$ , i.e., to perform symmetrization [21]. Kada et al. [97] have studied this procedure under the name of the *permutation test*, and show that the test accepts  $n$ -tuples where at least one pair of states is orthogonal with probability at most  $1/n$ , and that this is optimal among tests with perfect completeness. They also study a related tester, called the *circle test*, and prove that this test is also optimal for prime  $n$ .

#### 4.1.2 Productness

A pure state  $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$  of  $n$   $d$ -dimensional subsystems is said to be *product* (i.e., satisfy the **Product** property) if it can be written as  $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle$  for some local states  $|\psi_1\rangle, \dots, |\psi_n\rangle \in \mathbb{C}^d$ . A state which is not product is called *entangled*. Entanglement is a ubiquitous phenomenon in quantum information theory (see for example [90] for an extensive review), so the property of being a product state is an obvious target to test.

Given just one copy of  $|\psi\rangle$ , our ability to test whether it is product is very limited. Indeed, as every quantum state can be written as a linear combination of product states, any tester which accepts all product states with certainty must accept all states with certainty. However, if we are given two copies of  $|\psi\rangle$ , there are non-trivial tests we can perform. In particular, consider the following procedure, which was first discussed by Mintert et al. [120] and is called the *product test* [83]: apply the swap test across each corresponding pair of subsystems of  $|\psi\rangle^{\otimes 2}$ , and accept if and only if all of the tests accept. The overall procedure is illustrated in Figure 1.

If  $|\psi\rangle$  is indeed product, then all of the swap tests will accept. On the other hand, if  $|\psi\rangle$  is far from product, the intuition is that the entanglement in  $|\psi\rangle$  will cause at least some of the tests to reject with fairly high probability. This intuition can be formalized to give the following result.

**Theorem 16** (Harrow and Montanaro [83]). *If  $|\psi\rangle$  is  $\epsilon$ -far from product, the product test rejects with probability  $\Omega(\epsilon^2)$ .*

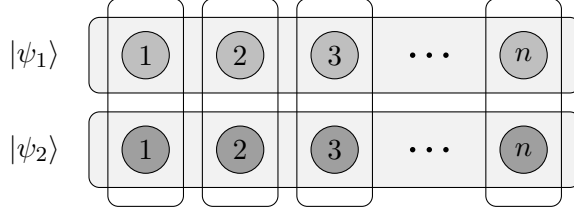


Figure 1: Schematic of the product test applied to an  $n$ -partite state  $|\psi\rangle$ . The swap test (vertical boxes) is applied to the  $n$  pairs of corresponding subsystems of two copies of  $|\psi\rangle$  (horizontal boxes).

Thus the property of productness can be tested with  $O(1/\epsilon^2)$  copies. We will not give the full, and somewhat technical, proof of Theorem 16 here, but merely sketch the proof technique; see [83] for details.

*Proof. (sketch)* Let  $P_{\text{test}}(|\psi\rangle)$  denote the probability of the product test accepting when applied to two copies of  $|\psi\rangle$ , and let the distance of  $|\psi\rangle$  from the nearest product state be  $\epsilon$ . The proof is split into two parts, depending on whether  $\epsilon$  is low or high. For  $S \subseteq [n]$ , let  $\psi_S$  be the mixed state obtained by tracing out (discarding) the qubits not in  $S$ . Then the starting point is the observation that

$$P_{\text{test}}(|\psi\rangle) = \frac{1}{2^n} \sum_{S \subseteq [n]} \text{tr}(\psi_S)^2, \quad (2)$$

i.e., that the probability that the test passes is equal to the average purity of the reduced state obtained by a random bipartition of the  $n$  systems. Writing  $|\psi\rangle = \sqrt{1 - \epsilon^2}|0^n\rangle + \epsilon|\phi\rangle$  (without loss of generality), for some product state  $|0^n\rangle$  and arbitrary orthogonal state  $|\phi\rangle$ , Eq. (2) allows an explicit expression for  $\text{tr} \psi_S^2$  in terms of  $\epsilon$  and  $|\phi\rangle$  to be obtained. Expanding  $|\phi\rangle = \sum_{x \in \{0, \dots, d-1\}^n} \alpha_x |x\rangle$  and summing over  $S$ , we get an expression containing terms of the form  $\sum_{x \in \{0, \dots, d-1\}^n} |\alpha_x|^2 c^{|x|}$  for some  $c < 1$ , where  $|x| := |\{i : x_i \neq 0\}|$ . In order to obtain a non-trivial bound from this, the final step of the first part of the proof is to use the fact that  $|0^n\rangle$  is the closest product state to  $|\psi\rangle$  to argue that  $|\phi\rangle$  cannot have any amplitude on basis states  $|x\rangle$  such that  $|x| \leq 1$ . A bound is eventually obtained that is applicable when  $\epsilon$  is small, namely that

$$P_{\text{test}}(|\psi\rangle) \leq 1 - \epsilon^2 + \epsilon^3 + \epsilon^4.$$

In the case where  $\epsilon$  is large, this does not yet give a useful upper bound, so the second part of the proof finds a constant upper bound on  $P_{\text{test}}(|\psi\rangle)$ . This quantity can be shown to be upper bounded by the probability that a relaxed test, for being product across any partition of the  $n$  subsystems into  $k \leq n$  parties, passes. If  $|\psi\rangle$  is far from product across the  $n$  subsystems, the proof shows that one can find a partition into  $k$  parties such that the distance from the closest product state (with respect to this partition) falls into the regime where the first part of the proof works. The eventual result is that if  $\epsilon^2 \geq 11/32 > 0.343$ , then  $P_{\text{test}}(|\psi\rangle) \leq 501/512 < 0.979$ ; combining these two bounds completes the proof.  $\square$

We mention two implications of Theorem 16. First, by the characterization (2), the content of Theorem 16 can be understood as: if a pure state of  $n$  systems is still fairly pure on average after discarding a random subset of the systems, it must in fact have been close to a product state in the first place. In the classical property testing literature, one of the motivations for analysing tests for

combinatorial properties is to obtain some insight into the structure of the property being tested; Theorem 16 can be seen as achieving something similar in a quantum setting.

Second, by allowing one to efficiently certify productness given two copies of  $|\psi\rangle$ , this test can be used to show that quantum Merlin-Arthur proof systems with multiple provers can be simulated efficiently by two provers, or in complexity-theoretic terminology that  $\text{QMA}(k) = \text{QMA}(2)$  [83]. Via a previous result of Aaronson et al. [5] giving a multiple-prover quantum proof system for 3-SAT, this in turn allows one to prove hardness of various tasks in quantum information theory, conditioned on the hardness of 3-SAT [83]. This is again analogous to the classical literature, where efficient property testers are used as components in hardness-of-approximation results.

Although the product test itself is natural, the detailed proof of Theorem 16 given in [83] is a lengthy case analysis which does not provide much intuition and gives suboptimal constants. For example, the lower bound obtained on the probability of the product test rejecting does not increase monotonically with  $\epsilon$ , which presumably should be the case for an optimal bound. We therefore highlight the following open question.

**Question 5.** *Can the analysis of the product test be improved?*

### 4.1.3 Arbitrary finite or infinite sets

The following algorithm of Wang [147] gives a tester for *any* finite property  $\mathcal{P} \subset \mathbb{C}^d$ . However, the tester cannot necessarily be implemented efficiently in general. Given access to copies of an input state  $|\psi\rangle$ , the tester proceeds as follows:

1. Create the state  $|\psi\rangle^{\otimes T}$ , for some  $T$  to be determined.
2. Let  $S = \text{span}\{|\phi\rangle^{\otimes T} : |\phi\rangle \in \mathcal{P}\}$ . Perform the measurement  $\{\Pi_S, I - \Pi_S\}$ , where  $\Pi_S$  is the projector onto  $S$ , and accept if the first outcome is obtained. Otherwise, reject.

**Theorem 17** (Wang [147]). *Let  $\mathcal{P} \subset \mathbb{C}^d$  be such that  $\min_{|\phi\rangle \neq |\phi'\rangle \in \mathcal{P}} D(|\phi\rangle, |\phi'\rangle) = \delta$ . Then it suffices to take  $T = O(\log |\mathcal{P}| \max\{\epsilon^{-2}, \delta^{-2}\})$  to obtain a tester which accepts every state in  $\mathcal{P}$  with certainty, and rejects every state  $|\psi\rangle$  such that  $D(|\psi\rangle, \mathcal{P}) \geq \epsilon$  with probability at least  $2/3$ .*

The intuition behind Theorem 17 is that, if all the states in  $\mathcal{P}$  have large pairwise distances,  $\{|\phi\rangle^{\otimes T}\}$  is an approximately orthonormal basis for  $S$ , so if  $|\psi\rangle$  is  $\epsilon$ -far from  $\mathcal{P}$ , the probability of incorrectly accepting is

$$\langle \psi |^{\otimes T} \Pi_S | \psi \rangle^{\otimes T} \approx \sum_{|\phi\rangle \in \mathcal{P}} |\langle \psi | \phi \rangle|^{2T} \leq |\mathcal{P}| (1 - \epsilon^2)^T,$$

which is sufficiently small when  $T = O((\log |\mathcal{P}|)/\epsilon^2)$ . It is an interesting question whether the dependence on  $\delta$  can be improved or removed, either by better analysis of the above test or by designing a new tester.

**Question 6.** *Does there exist a tester for arbitrary finite properties  $\mathcal{P} \subset \mathbb{C}^d$  whose parameters have no dependence on  $\min_{|\phi\rangle \neq |\phi'\rangle \in \mathcal{P}} D(|\phi\rangle, |\phi'\rangle)$ ?*

The above tester is a general algorithm for testing any property  $\mathcal{P}$ , and for some properties  $\mathcal{P}$  it is possible to prove better bounds than Theorem 17. For example, the product test is a particular case of this algorithm (with  $T = 2$ ), and Theorem 16 gives non-trivial bounds on its performance, even though it is applied to the infinite set of product states. We also remark that an alternative

algorithm to the above tester would be to produce  $|\psi\rangle^{\otimes T}$ , and for each  $|\phi\rangle \in \mathcal{P}$  in turn, perform the measurement  $\{|\phi\rangle\langle\phi|^{\otimes T}, I - |\phi\rangle\langle\phi|^{\otimes T}\}$ , and accept if and only if the first outcome is obtained from any measurement. This algorithm would achieve similar scaling in terms of  $\epsilon$  and  $\delta$  (as can be shown using the “quantum union bound” of Aaronson [1], or the “gentle measurement lemma” of Winter [150] and Ogawa and Nagaoka [126]) but would not have perfect completeness.

We finally observe that *any* (even infinite) property  $\mathcal{P} \subseteq \mathbb{C}^d$  can be tested using  $O(d/\epsilon^2)$  copies of the input state  $|\psi\rangle$ ; it suffices to obtain an estimate  $|\psi'\rangle$  such that  $D(|\psi'\rangle, |\psi\rangle) < \epsilon/2$ , and accept if and only if  $D(|\psi'\rangle, \mathcal{P}) \leq \epsilon/2$ . In order to produce such an estimate one can use a procedure known as *quantum state estimation*, which needs  $O(d/\epsilon^2)$  copies of  $|\psi\rangle$  to achieve the required accuracy with success probability at least  $2/3$  [41].

#### 4.1.4 Open questions

There are a number of interesting sets of pure states for which an efficient tester is not known. One such set is the *stabilizer states*. The Pauli matrices on one qubit are defined to be the set

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (3)$$

They form a basis for the space of single-qubit linear operators, and by tensoring form a basis for the space of linear operators on  $n$  qubits; for  $s \in \{I, X, Y, Z\}^n$ , we write  $\sigma_s$  for the corresponding operator on  $n$  qubits. We call each such tensor product operator a ( $n$ -qubit) Pauli matrix, and use  $\mathcal{P}_n$  to denote the set of all  $n$ -qubit Pauli matrices, together with phases  $\pm 1, \pm i$ , which forms a group under multiplication.

A state  $|\psi\rangle$  of  $n$  qubits is said to be a stabilizer state if there exists a maximal Abelian subgroup  $G$  of  $\mathcal{P}_n$  such that  $U|\psi\rangle = |\psi\rangle$  for all  $U \in G$ . Stabilizer states are important in the study of quantum error-correction [73] and measurement-based quantum computation [131], as well as many other areas of quantum information. It is known that, given access to copies of an unknown stabilizer state  $|\psi\rangle$  of  $n$  qubits,  $|\psi\rangle$  can be learned with  $O(n)$  copies [6]; there is a matching  $\Omega(n)$  lower bound following from an information-theoretic argument [88]. However, it might be possible to *test* whether  $|\psi\rangle$  is a stabilizer state using far fewer copies.

**Question 7.** *Is there a tester for the property of being a stabilizer state whose parameters do not depend on the number of qubits  $n$ ?*

Other sets of pure states for which it would be interesting to have an efficient tester are matrix product states (see, e.g., [128]) and states of low Schmidt rank. See Section 4.2 below for evidence for a lower bound on the complexity of testing the latter property.

## 4.2 Mixed states

A mixed state  $\rho$  is a convex combination of pure states. Mixed states are described by density matrices, which are positive semidefinite matrices with unit trace; we let  $\mathcal{B}(\mathbb{C}^d)$  denote the set of  $d$ -dimensional density matrices. The concept of property testing can easily be generalized from pure states to mixed states. We retain the same, natural distance measure

$$D(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1,$$

which is called the trace distance between  $\rho$  and  $\sigma$ . As before, say that  $\rho$  is  $\epsilon$ -far from having property  $\mathcal{P} \subseteq \mathcal{B}(\mathbb{C}^d)$  if

$$D(\rho, \mathcal{P}) := \inf_{\sigma \in \mathcal{P}} D(\rho, \sigma) \geq \epsilon,$$

and  $\epsilon$ -close to having property  $\mathcal{P}$  if  $D(\rho, \mathcal{P}) \leq \epsilon$ . Another important distance measure for mixed states is the *fidelity*, which is defined as  $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$ . The fidelity and trace distance satisfy the inequalities [124, Eq. 9.110]

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}. \quad (4)$$

In a mixed-state property testing scenario, we are given  $k$  copies of  $\rho$ , for some unknown  $\rho$ , and asked to perform a measurement on  $\rho$  to determine whether  $\rho \in \mathcal{P}$ , or  $\rho$  is  $\epsilon$ -far away from  $\mathcal{P}$ . Some properties of mixed states can indeed be tested efficiently. A simple example is the property **Purity**, where  $\rho$  satisfies the property if and only if it is a pure state. A natural way to test purity is to apply the swap test to two copies of  $\rho$ . This accepts with probability  $(1 + \text{tr } \rho^2)/2$ , which is equal to 1 if and only if  $\rho$  is pure. On the other hand, if we let  $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$  be the eigendecomposition of  $\rho$ , where eigenvalues are listed in non-increasing order, a closest pure state to  $\rho$  is  $|\psi_1\rangle$ . If  $\rho$  is  $\epsilon$ -far away from pure, then  $\lambda_1 = 1 - \epsilon$ . Note that

$$\text{tr } \rho^2 = \sum_i \lambda_i^2 \leq \lambda_1^2 + \left( \sum_{i>1} \lambda_i \right)^2 = \lambda_1^2 + (1 - \lambda_1)^2.$$

For  $\epsilon \leq 1/2$ ,  $\text{tr } \rho^2 \leq (1 - \epsilon)^2 + \epsilon^2$  and hence the test accepts with probability at most  $1 - \epsilon + \epsilon^2 = 1 - \Theta(\epsilon)$ ; for  $\epsilon \geq 1/2$ ,  $\text{tr } \rho^2 \leq 1/2$ . Thus **Purity** can be tested with  $O(1/\epsilon)$  copies of  $\rho$ .

On the other hand, consider the “dual” property of **Mixedness**, where  $\rho \in \mathcal{B}(\mathbb{C}^d)$  satisfies the property if and only if it is the maximally mixed state  $I/d$ . A strong lower bound has been shown by Childs et al. [50] on the number of copies required to test this property.

**Theorem 18** (Childs et al. [50]). *Let  $d$  and  $r$  be integers such that  $r$  divides  $d$ . Any algorithm which distinguishes, with probability of success at least  $2/3$ , between the two cases that  $\rho = I/d$  or  $\rho$  is maximally mixed on a uniformly random subspace of dimension  $r$  must use  $\Omega(r)$  copies of  $\rho$ . Further, there exists an algorithm which solves this problem using  $O(r)$  copies.*

Childs et al. call the problem which they consider the *quantum collision problem*. To see how their result can be applied to **Mixedness**, consider the space of  $n$  qubits, whose dimension is  $d = 2^n$ . As a state  $\rho$  which is maximally mixed on a dimension- $r$  subspace of  $\mathbb{C}^{2^n}$  satisfies  $D(\rho, I/2^n) = 1 - r/2^n$ , taking  $r = 2^{n-1}$  implies that any algorithm distinguishing between the cases that  $\rho = I/2^n$  and  $\rho$  is  $1/2$ -far from  $I/2^n$  must use  $\Omega(2^n)$  copies of  $\rho$ . This result also puts strong lower bounds on a number of other property testing problems which one might wish to solve. For example, consider the following three properties:

- **Equality** of pairs of mixed states, where the pair  $(\rho, \sigma)$  satisfies the property if  $\rho = \sigma$ . This can be seen as the quantum generalization of the classical question of testing whether two probability distributions on  $d$  elements are equal or  $\epsilon$ -far from equal (with respect to the total variation distance), given access to samples from the distributions. A sublinear tester for the classical problem has been given by Batu et al. [25], and recently improved by Chan et al. [48]; for constant  $\epsilon$  the tester uses  $O(d^{2/3})$  samples. By fixing  $\sigma = I/d$ , the result of [50] implies that the quantum generalization of this problem is more difficult.



- Whether a mixed state  $\rho$  has **rank at most**  $r$ . Theorem 18 immediately implies that this requires  $\Omega(r)$  copies of  $\rho$ , which has an interesting implication for testing pure states. Recall that a bipartite state  $|\psi\rangle$  on systems  $AB$  is said to have Schmidt rank  $r$  if it can be written as  $|\psi\rangle = \sum_{i=1}^r \sqrt{\lambda_i} |v_i\rangle |w_i\rangle$  for pairwise orthonormal sets of states  $\{|v_i\rangle\}$ ,  $\{|w_i\rangle\}$  and non-negative  $\lambda_i$ . If one looks only at the  $A$  subsystem, the rank of the reduced state is precisely the Schmidt rank of  $|\psi\rangle$ . Therefore, Theorem 18 implies that any algorithm which tests whether a pure state  $|\psi\rangle$  has Schmidt rank  $r$  by producing  $k$  copies of  $|\psi\rangle$  and acting only on the first subsystems  $A_1, \dots, A_k$  of  $|\psi\rangle^{\otimes k}$  must satisfy  $k = \Omega(r)$ .
- **Separability** of mixed states. A bipartite quantum state  $\rho \in \mathcal{B}((\mathbb{C}^d)^{\otimes 2})$  is said to be *separable* if it can be written as a convex combination of product states, and is said to be *entangled* otherwise. Determining separability up to accuracy which is inversely polynomial in the dimension  $d$  is known to be NP-hard [78, 68], and there is some evidence for intractability of the problem even up to constant accuracy [83]. This does not preclude the existence of a tester for separability which is efficient in terms of the number of copies of  $\rho$  used; however, Theorem 18 can be used to show that such a tester cannot exist.

The idea is to show that the maximally mixed state on a random subspace of dimension  $r$  is far from separable, if  $r$  is picked suitably. This can be achieved by combining some previously known results. The *entanglement of formation* of a bipartite state  $\rho$ , is defined by

$$E_F(\rho) = \min_{\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho} \sum_i p_i S(\text{tr}_B |\psi_i\rangle\langle\psi_i|),$$

where  $S(\rho) = -\text{tr} \rho \log_2 \rho$  is the von Neumann entropy. Of course, if  $\rho$  is separable,  $E_F(\rho) = 0$ . Let  $\rho$  be the maximally mixed state on a random subspace of  $\mathbb{C}^d \otimes \mathbb{C}^d$  of dimension  $r = \lfloor Bd^2 \rfloor$ , for some fixed  $0 < B < 1$ . Hayden et al. [84] have shown that there exists a universal constant  $A > 0$  such that, for any choice of  $B$  with  $0 < B \leq A$ , there exists  $C > 0$  such that  $E_F(\rho) \geq C \log_2 d$ , except with probability exponentially small in  $d$ . Also, Nielsen [123] has shown a continuity property for the entanglement of formation:

$$E_F(\rho) - E_F(\sigma) \leq 18(\log_2 d) \sqrt{1 - F(\rho, \sigma)} + 2(\log_2 e)/e.$$

Combining these two properties, and relating the fidelity to the trace distance using (4), we have that  $\rho$  is distance  $\Omega(1)$  from the set of separable states with high probability. On the other hand, the maximally mixed state  $I/d^2$  is clearly separable. Therefore, any tester which distinguishes separable states from states a constant distance from any separable state can be used to distinguish the maximally mixed state from a random dimension- $r$  subspace; by Theorem 18, this task requires  $\Omega(d^2)$  copies of the input state.

We remark that the theory of *entanglement witnesses* takes an alternative approach to the direct detection of entanglement (see for example [77, 90] for extensive reviews). An entanglement witness for a state  $\rho$  is an observable corresponding to a hyperplane separating  $\rho$  from the convex set of separable states; measuring the observable allows one to certify that  $\rho$  is entangled. Each such witness will only be useful for certain entangled states, however, so this approach does not provide a means of certifying entanglement of a completely unknown state  $\rho$ .

Conversely to the above lower bounds, and similarly to the case of pure states, *any* property  $\mathcal{P} \subseteq \mathcal{B}(\mathbb{C}^d)$  can be tested with  $O(d^4/\epsilon^2)$  copies. To distinguish between the two cases that  $\rho \in \mathcal{P}$  or  $\rho$  is  $\epsilon$ -far from  $\mathcal{P}$ , it suffices to use an estimate  $\tilde{\rho}$  such that  $D(\tilde{\rho}, \rho) < \epsilon/2$ , and accept if and only if  $D(\tilde{\rho}, \mathcal{P}) \leq \epsilon/2$ . Producing such an estimate can be achieved using quantum state

tomography [127, 124]; in order to achieve the required accuracy with success probability  $2/3$ ,  $O(d^4/\epsilon^2)$  copies suffice [64]. If one knows in advance that  $\rho$  is rank  $r$ , compressed sensing techniques allow this bound to be improved to  $O((rd/\epsilon)^2 \log d)$  [64].

There is still a gap between the best known lower and upper bounds for testing **Equality** and **Separability**. We therefore highlight the following open question:

**Question 8.** *What is the complexity of testing **Equality** and **Separability**?*

#### 4.2.1 Testing equality to a fixed pure state

We have seen that testing whether  $\rho \in \mathcal{B}(\mathbb{C}^d)$  is the maximally mixed state  $I/d$  can require  $\Omega(d)$  copies of  $\rho$ . By contrast, testing whether  $\rho$  is a fixed *pure* state  $|\psi\rangle\langle\psi|$  is easy: the obvious test is to perform the measurement  $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$ , and to accept if the first outcome is returned. The probability of acceptance is  $\langle\psi|\rho|\psi\rangle$ , which is upper bounded by  $1 - D(\rho, |\psi\rangle\langle\psi|)^2$  [124], so this property can be tested with  $O(1/\epsilon^2)$  copies of  $\rho$ .

However, there is a more interesting related question of relevance to experimentalists. Imagine we have some experimental apparatus which is claimed to produce a state  $|\phi\rangle$  of  $n$  qubits, and we would like to certify this fact. In this setting, the above test does not seem to make sense; being able to measure  $|\phi\rangle$  is essentially precisely what we wish to certify! We further imagine that  $n$  is too large for full state tomography to be efficient. In order to solve this self-certification problem, we would therefore like a procedure which makes a small number of measurements, can easily be implemented experimentally, and certifies that the state produced is approximately equal to  $|\phi\rangle$ . This question has been considered by da Silva et al. [58], and independently Flammia and Liu [65], who show that certain states  $|\phi\rangle$  can be certified using significantly fewer copies of  $|\phi\rangle$  than would be required for full tomography, and indeed that any state  $|\phi\rangle$  can be certified using quadratically fewer copies ( $O(2^n)$  rather than  $O(2^{2n})$ ). The measurements used are also simple: Pauli measurements.

The Pauli matrices  $\{\sigma_s\}$  on  $n$  qubits form a basis for the space of  $n$ -qubit linear operators and satisfy  $\text{tr } \sigma_s \sigma_t = 2^n \delta_{st}$ . So any state  $\rho \in \mathcal{B}(\mathbb{C}^{2^n})$  can be expanded as

$$\rho = \sum_{s \in \{I, X, Y, Z\}^n} \hat{\rho}_s \sigma_s$$

for some real coefficients  $\hat{\rho}_s = (\text{tr } \rho \sigma_s) / 2^n$ . Writing  $\phi := |\phi\rangle\langle\phi|$  for conciseness, the squared fidelity between  $|\phi\rangle$  and  $\rho$  is

$$\langle\phi|\rho|\phi\rangle = \text{tr } \rho \phi = 2^n \sum_{s \in \{I, X, Y, Z\}^n} \hat{\rho}_s \hat{\phi}_s.$$

The works [58, 65] propose the following scheme. First, pick  $s \in \{I, X, Y, Z\}^n$  with probability  $2^n \hat{\phi}_s^2$ ; orthonormality of the Pauli matrices implies that this is indeed a valid probability distribution. Then repeatedly measure copies of  $\rho$  in the eigenbasis of  $\sigma_s$ , and take the average of the eigenvalues corresponding to the measurement results to produce an estimate  $\tilde{\rho}_s$  of  $2^n \hat{\rho}_s = \text{tr } \rho \sigma_s$ . Finally, output  $\tilde{\rho}_s / \hat{\phi}_s$  as our guess for the squared fidelity. The expectation of  $\tilde{\rho}_s$  is precisely  $\text{tr } \rho \sigma_s$ , and if we assume that this estimate is exact (i.e.,  $\tilde{\rho}_s = \text{tr } \rho \sigma_s$ ), the expected value of the output is

$$\sum_{s \in \{I, X, Y, Z\}^n} (2^n \hat{\phi}_s^2) \frac{\hat{\rho}_s}{\hat{\phi}_s} = \text{tr } \rho \phi.$$

Of course, in general we cannot produce an exact estimate without using an infinite number of copies of  $\rho$ . However, to estimate the fidelity up to constant additive error with constant success

probability, it suffices to use a finite number of copies. The number of copies required turns out to depend on the quantity  $\min_{s, \hat{\phi}_s \neq 0} |\hat{\phi}_s|$ ; for certain classes of states  $|\phi\rangle$  (such as stabilizer states), the number of copies used does not depend on  $n$ .

### 4.2.2 Unitarily invariant properties

Generalizing the properties **Purity** and **Mixedness**, one can consider properties  $\mathcal{P}$  of mixed quantum states which are unitarily invariant, in the following sense: If  $\rho \in \mathcal{P}$ , then  $(U\rho U^\dagger) \in \mathcal{P}$  for all  $U \in U(d)$ , where  $U(d)$  denotes the unitary group in  $d$  dimensions. Observe that this implies that, if  $\rho$  is  $\epsilon$ -far from  $\mathcal{P}$ , then so is  $U\rho U^\dagger$ , for all  $\epsilon$  and all  $U \in U(d)$ . For any  $\rho$ ,  $D(\rho, \mathcal{P})$  must necessarily be a symmetric function of the spectrum of  $\rho$ . We can see unitarily invariant properties as quantum analogs of symmetric properties of classical probability distributions [144].

In order to take advantage of the unitary symmetry, one can use a concept known as *Schur-Weyl duality*. We will only briefly summarize this beautiful theory here, and sketch the consequences for property testing; for much more detailed introductions, see the theses [53, 82]. Schur-Weyl duality implies that any linear operator  $M$  on  $(\mathbb{C}^d)^{\otimes k}$  which commutes with permutations of the  $k$  subsystems, and also with local unitaries on each subsystem (i.e.,  $U^{\otimes k} M (U^{-1})^{\otimes k} = M$  for all  $U \in U(d)$ ) can be written as  $M = \sum_{\lambda \vdash k} \alpha_\lambda P_\lambda$  for some coefficients  $\alpha_\lambda$  and projectors  $P_\lambda$ , where the sum is over partitions  $\lambda$  of  $k$  (e.g., the partitions of 4 are  $(4)$ ,  $(3, 1)$ ,  $(2, 2)$ ,  $(2, 1, 1)$ ,  $(1, 1, 1, 1)$ ). Each partition  $\lambda$  corresponds to an irreducible representation (irrep) of  $S_k$ , the symmetric group on  $k$  elements; one important irrep is the trivial irrep  $(k)$  which maps  $\pi \mapsto 1$  for all  $\pi \in S_k$ . The operators  $P_\lambda$  are defined by

$$P_\lambda := \frac{d_\lambda}{k!} \sum_{\pi \in S_k} \chi_\lambda(\pi) U_\pi.$$

In the above expression,  $d_\lambda$  is the dimension of the corresponding irrep  $V_\lambda$  of  $S_k$ , which associates a  $d_\lambda$ -dimensional square matrix with each permutation  $\pi \in S_k$ . Then  $\chi_\lambda$  is the corresponding character  $\text{tr } V_\lambda$  and  $U_\pi$  is the operator which acts by permuting  $k$   $d$ -dimensional systems according to  $\pi$ :

$$U_\pi |i_1\rangle \dots |i_k\rangle = |i_{\pi^{-1}(1)}\rangle \dots |i_{\pi^{-1}(k)}\rangle.$$

One can show that each operator  $P_\lambda$  is indeed a projector, that  $P_\lambda P_\mu = \delta_{\lambda\mu} P_\lambda$ , and that  $\sum_{\lambda \vdash k} P_\lambda = I$ . These operators therefore define a measurement (POVM), and performing this measurement is known as weak Schur sampling [50]. This can be implemented efficiently via a procedure which is known as generalized phase estimation [82, 50] and generalizes the swap test [42] (cf. Section 4.1.1) and symmetrization [21]. Generalized phase estimation is based on the quantum Fourier transform (QFT) over  $S_k$  [26], which is a unitary operation that performs a change of basis from  $\{|\pi\rangle : \pi \in S_k\}$  to  $\{|\lambda, i, j\rangle : \lambda \vdash k, 1 \leq i, j \leq d_\lambda\}$ . It follows from basic representation theory that this makes sense, i.e., that  $\sum_{\lambda \vdash k} d_\lambda^2 = k!$ .

The generalized phase estimation procedure proceeds as follows:

1. Start with a quantum state  $\sigma \in \mathcal{B}((\mathbb{C}^d)^{\otimes k})$ .
2. Prepend a  $k!$ -dimensional ancilla register whose basis states correspond to triples  $|\lambda, i, j\rangle$ , initialized in the state  $|(k), 1, 1\rangle$  corresponding to the trivial irrep.
3. Apply the inverse quantum Fourier transform over  $S_k$  to the ancilla to produce the state  $\frac{1}{\sqrt{k!}} \sum_{\pi \in S_k} |\pi\rangle$ .
4. Apply the controlled permutation operation  $\sum_{\pi \in S_k} |\pi\rangle\langle\pi| \otimes U_\pi$ , controlled on the ancilla.

5. Apply the quantum Fourier transform over  $S_k$  to the ancilla and measure it, receiving outcome  $(\lambda, i, j)$ .
6. Output  $\lambda$ .

One can show [20, 82] that, on input  $\sigma$ , generalized phase estimation does indeed output  $\lambda$  with probability  $\text{tr } P_\lambda \sigma$ .<sup>10</sup>

It turns out that any test for a unitarily invariant property can, essentially, be taken to consist of performing weak Schur sampling and classically post-processing the results. This provides a kind of quantum analog of the classical notion of a canonical tester for properties of probability distributions [144].

**Lemma 19.** *Let  $\mathcal{P} \subseteq \mathcal{B}(\mathbb{C}^d)$  be a unitarily invariant property. Assume there exists a tester which uses  $k$  copies of the input state  $\rho$ , and accepts all states  $\rho \in \mathcal{P}$  with probability at least  $1 - \delta$ , but accepts all states which are  $\epsilon$ -far from  $\mathcal{P}$  with probability at most  $1 - f(\epsilon)$  for  $\epsilon > 0$ . Then there exists a tester with the same parameters which consists of performing weak Schur sampling on  $\rho^{\otimes k}$  and classically postprocessing the results.*

*Proof.* Let  $M$  be the measurement operator corresponding to the tester accepting, and for each  $\epsilon$ , let  $\rho_\epsilon$  be the state which is distance  $\epsilon$  from  $\mathcal{P}$  and achieves the worst-case probability of acceptance (so  $\rho_0$  is the state in  $\mathcal{P}$  with the lowest probability of acceptance, and for  $\epsilon > 0$ ,  $\rho_\epsilon$  is the state with the highest probability of acceptance such that  $D(\rho_\epsilon, \mathcal{P}) = \epsilon$ ). Then, by the permutation invariance of  $\rho_\epsilon^{\otimes k}$ , we have

$$\text{tr } M \rho_\epsilon^{\otimes k} = \frac{1}{k!} \sum_{\pi \in S_k} \text{tr } M U_\pi \rho_\epsilon^{\otimes k} U_\pi^{-1} =: \text{tr } \overline{M} \rho_\epsilon^{\otimes k},$$

where we define  $\overline{M} = \frac{1}{k!} \sum_{\pi \in S_k} U_\pi M U_\pi^{-1}$ , and by the unitary invariance of  $\mathcal{P}$ ,

$$\text{tr } \overline{M} \rho_0^{\otimes k} \leq \int \text{tr } \overline{M} (U \rho_0 U^{-1})^{\otimes k} dU = \text{tr} \left( \int U^{\otimes k} \overline{M} (U^{-1})^{\otimes k} dU \right) \rho_0 =: \text{tr } \overline{\overline{M}} \rho_0,$$

where the integral is taken according to Haar measure on  $U(d)$ , and similarly  $\text{tr } \overline{M} \rho_\epsilon^{\otimes k} \geq \text{tr } \overline{\overline{M}} \rho_\epsilon^{\otimes k}$  for  $\epsilon > 0$ . Therefore, it suffices to implement  $\overline{\overline{M}}$  to achieve the same parameters as  $M$ . But  $\overline{\overline{M}}$  commutes with local unitaries and permutations of the  $k$  systems, so by Schur-Weyl duality we can write  $\overline{\overline{M}} = \sum_\lambda \alpha_\lambda P_\lambda$  for some coefficients  $\alpha_\lambda$ ; as  $\overline{\overline{M}}$  is a measurement operator, for each  $\lambda$  it holds that  $0 \leq \alpha_\lambda \leq 1$ . So we can implement  $\overline{\overline{M}}$  by performing weak Schur sampling, obtaining outcome  $\lambda$ , then accepting with probability  $\alpha_\lambda$ .  $\square$

Further, one can write down the probability of obtaining each outcome  $\lambda$  as follows: if the input state  $\rho$  has eigenvalues  $(x_1, \dots, x_d)$ , then

$$\text{tr } P_\lambda \rho^{\otimes k} = d_\lambda s_\lambda(x_1, \dots, x_d),$$

where  $s_\lambda$  is a Schur polynomial (see, e.g., [18] for a discussion). In principle, this allows one to calculate the parameters of the optimal test for any unitarily invariant property; in practice, the calculations required are somewhat daunting. Nevertheless, a careful analysis of the output distributions resulting from weak Schur sampling was the approach taken by Childs et al. [50] to

<sup>10</sup>Some works describe the procedure as instead starting with a QFT and finishing with an inverse QFT [50, 121], but this does not appear correct as the QFT should map from the group algebra of  $S_k$  to the space of irreps of  $S_k$  [26].

prove their bounds on the quantum collision problem. Indeed, their approach is an example of how one can prove lower bounds on quantum property testers more generally: first use symmetry arguments to prove that the optimal test must be of a certain form, then analyse the optimal test directly.

## 5 Testing properties of quantum dynamics

### 5.1 Unitary operators

We continue to let  $U(d)$  denote the unitary group in  $d$  dimensions, and let  $M(d)$  denote the set of  $d \times d$  matrices. A property of unitary operators is simply a (discrete or continuous) subset  $\mathcal{P} \subseteq U(d)$ . Properties of unitary operators display some interesting similarities to and differences from properties of states.

#### 5.1.1 Distance measures

As compared with the case of pure states, it is less obvious which distance measure between unitary operators is the right one to choose to obtain interesting property testing results. For quantum states, the distinguishability of any two states is controlled by their trace distance. A natural way to generalize this to unitary operations would be to maximize the distinguishability of the output states over all input states<sup>11</sup>, to produce

$$D^{\max}(U, V) := \max_{|\psi\rangle} D(U|\psi\rangle, V|\psi\rangle) = \max_{|\psi\rangle} \sqrt{1 - |\langle\psi|U^\dagger V|\psi\rangle|^2}.$$

Unfortunately, there are extremely simple properties which are hard to test with respect to this distance measure. One such example is the **Identity** property: does an input unitary  $U$  satisfy  $U = e^{i\theta}I$ ? (Note that, as with the case of pure state properties, we allow an arbitrary phase  $\theta$  in the definition, as  $U$  cannot be distinguished from  $e^{i\theta}U$ .) Consider the family of  $n$ -dimensional unitary operators  $U_i$ ,  $i \in [n]$ , where  $U_i|j\rangle = (-1)^{\delta_{ij}}|j\rangle$ . Each of these has maximal distance from  $I$ , according to the distance measure  $D^{\max}$ . However, a quantum algorithm which uses the input operator  $U$   $k$  times and distinguishes between the case where  $U$  is equal to the identity, and the case where  $U = U_i$  for some  $i$ , would imply a quantum algorithm which computes the OR function of  $n$  input bits, promised to have Hamming weight at most 1, using  $O(k)$  queries. As this problem is known to require  $\Omega(\sqrt{n})$  quantum queries [29], it follows that  $k = \Omega(\sqrt{n})$ . This is a lower bound on the complexity of identity-testing in an oracular setting; we discuss a lower bound based on computational complexity arguments in Section 5.3.

It is perhaps not surprising that  $D^{\max}$  is not the right measure of distance to choose for property testing problems, as it is a “best-case” rather than “average-case” measure. A suitable such alternative measure can be defined as follows. For any  $d$ -dimensional operators  $A, B \in M(d)$ , let  $\langle A, B \rangle$  denote the *normalized Hilbert-Schmidt* inner product

$$\langle A, B \rangle := \frac{1}{d} \operatorname{tr} A^\dagger B.$$

---

<sup>11</sup>One might wonder whether distinguishability could be improved further by allowing the unknown unitary operator to act on part of an entangled state; it turns out that this is not the case [149].

Assume that  $\langle A, A \rangle = \langle B, B \rangle = 1$  (a property satisfied, for example, if  $A$  and  $B$  are unitary). Then the distance between  $A$  and  $B$  is given by

$$D(A, B) := \sqrt{1 - |\langle A, B \rangle|^2}.$$

For  $\mathcal{P} \subseteq U(d)$ , we analogously define

$$D(U, \mathcal{P}) := \inf_{V \in \mathcal{P}} D(U, V).$$

Note the close analogy to the distance between pure states (1). The distance measure  $D(A, B)$  seems to have been first explicitly introduced by Low [110]; Wang [147] has defined a closely related alternative measure as  $D'(A, B) := \sqrt{1 - |\langle A, B \rangle|}$ . As  $D(A, B)/\sqrt{2} \leq D'(A, B) \leq D(A, B)$ , the two measures are essentially interchangeable. For any operators  $A$  and  $B$  such that  $\langle A, A \rangle = \langle B, B \rangle = 1$ ,  $D(A, B)$  has the following properties.

- $0 \leq D(A, B) \leq 1$ , with  $D(A, B) = 0$  if and only if  $A = e^{i\phi} B$  for some overall phase  $\phi$ . As there exist  $A \neq B$  with  $D(A, B) = 0$ , this implies that  $D(\cdot, \cdot)$  is not a metric, but only a “pseudometric.” Further,  $D(A, B) = D(WA, WB) = D(AW, BW)$  for any unitary  $W$ .
- $D(A, B)$  can alternatively be defined as

$$D(A, B) = \frac{1}{\sqrt{2}} \|A \otimes A^\dagger - B \otimes B^\dagger\|_2,$$

where  $\|\cdot\|_2$  is the normalized matrix 2-norm  $\|M\|_2 = \sqrt{\frac{1}{d} \sum_{i,j=1}^d |M_{ij}|^2}$  [110]. Observe that this representation shows that  $D(\cdot, \cdot)$  satisfies the triangle inequality.

- We have  $\|M\|_2^2 = \langle M, M \rangle$ . Therefore,  $\|A - B\|_2^2 = \langle A - B, A - B \rangle = 2 - 2\text{Re}\langle A, B \rangle$ . This implies that  $D(A, B) \leq \|A - B\|_2$ .

The following justifies the claim that  $D(\cdot, \cdot)$  is indeed an “average-case” measure of distance.

**Proposition 20.** *Fix  $d$ -dimensional unitary operators  $U$  and  $V$ . Then*

$$\int d\psi D(U|\psi\rangle, V|\psi\rangle)^2 = \frac{d}{d+1} D(U, V)^2,$$

where the integral is taken according to Haar measure on  $U(d)$ .

*Proof.* We have

$$\begin{aligned} \int d\psi D(U|\psi\rangle, V|\psi\rangle)^2 &= 1 - \int d\psi |\langle \psi | U^\dagger V | \psi \rangle|^2 \\ &= 1 - \int d\psi \text{tr}[(U^\dagger V \otimes V^\dagger U) |\psi\rangle\langle \psi|^{\otimes 2}] \\ &= 1 - \text{tr}(U^\dagger V \otimes V^\dagger U) \left( \frac{I + F}{d(d+1)} \right) \\ &= \frac{d}{d+1} \left( 1 - \left| \frac{\text{tr} U^\dagger V}{d} \right|^2 \right) \\ &= \frac{d}{d+1} D(U, V)^2. \end{aligned}$$

In the third equality we use the fact that  $\int |\psi\rangle\langle\psi|^{\otimes 2} d\psi = (I + F)/(d(d+1))$ , where  $F$  is the flip (or swap) operator which interchanges two  $d$ -dimensional systems. The fourth equality follows from the facts that, for any  $d$ -dimensional operators  $A, B$ ,  $\text{tr}(A \otimes B) = (\text{tr } A)(\text{tr } B)$  and  $\text{tr}((A \otimes B)F) = \text{tr}(AB)$ .  $\square$

The quantity  $\int d\psi |\langle\psi|U^\dagger V|\psi\rangle|^2$  appearing in the proof was previously introduced by Acín [8] as an average-case variant of the fidelity.

### 5.1.2 Controlled and inverse unitaries

As well as being given access to a unitary operator  $U$ , we may be given access to the inverse  $U^{-1}$  and/or the controlled unitary  $c-U$ , or in other words the operator  $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ . This may be a reasonable assumption if we would like to apply our property testing algorithm to a unitary operator given in the form of a quantum circuit; on the other hand, it may not be reasonable in an adversarial scenario where we only assume access to  $U$  as a black box.

For any  $U, V$  we have  $\langle c-U, c-V \rangle = (1 + \langle U, V \rangle)/2$ , implying

$$\begin{aligned} D(c-U, c-V) &= \sqrt{1 - \left| \frac{1 + \langle U, V \rangle}{2} \right|^2} \\ &= \frac{1}{2} \sqrt{3 - 2\text{Re}\langle U, V \rangle - |\langle U, V \rangle|^2} \\ &= \frac{1}{2} \sqrt{\|U - V\|_2^2 + D(U, V)^2}. \end{aligned}$$

Recalling that  $D(U, V) \leq \|U - V\|_2$ , we therefore have the inequalities

$$\|U - V\|_2/2 \leq D(c-U, c-V) \leq \|U - V\|_2/\sqrt{2}. \quad (5)$$

Thus, given access to controlled unitaries, one can hope to design tests which are sensitive to the 2-norm distance  $\|U - V\|_2$ . For example, if we are allowed access to controlled unitaries we can distinguish  $U$  from  $-U$ , whereas this is impossible given access to  $U$  alone.

Being given access to  $U^{-1}$  can also be powerful. In particular, it allows us to apply the important primitive of amplitude amplification [36] to property testing algorithms. Imagine we have a test for a property  $\mathcal{P} \subseteq U(d)$  which uses  $q$  copies of the input unitary  $U$ , and such that for  $U \in \mathcal{P}$  the test always accepts (it has perfect completeness), and for  $U$   $\epsilon$ -far from  $\mathcal{P}$ , the test accepts with probability at most  $f(\epsilon)$ . Then amplitude amplification allows us to test  $\mathcal{P}$  with  $O(q/\sqrt{f(\epsilon)})$  copies of  $U$ , rather than the  $O(q/f(\epsilon))$  copies that would be required by simple repetition. For example, we will see below that this gives a square-root speed-up for testing equality of unitary operators. In the complexities we quote below, we assume that amplitude amplification has not been applied.

### 5.1.3 From properties of states to properties of unitaries

There is a correspondence between pure quantum states and unitary operators, which is known as (a special case of) the Choi-Jamiołkowski isomorphism [52, 95] and will sometimes allow us to translate tests for properties of states to tests for analogous properties of unitaries. Given access to  $U \in U(d)$ , we first prepare the maximally entangled state of two  $d$ -dimensional systems

$$|\Phi\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle|i\rangle$$

and then apply  $U$  to the first system. We obtain the state

$$|U\rangle = \frac{1}{\sqrt{d}} \sum_{i,j=1}^d U_{ji}|j\rangle|i\rangle.$$

The state  $|U\rangle$  faithfully represents the original operator  $U$ ; in particular, it is easy to see that  $\langle U|V\rangle = \langle U, V\rangle$  and hence  $D(U, V) = D(|U\rangle, |V\rangle)$ . So, if we have a tester for some property  $\mathcal{P}$  of  $d^2$ -dimensional quantum states, by applying the test to  $|U\rangle$  we obtain a tester with the same parameters for an analogous property  $\mathcal{P}'$  of  $d$ -dimensional unitary operators.

On the other hand, one sometimes has to be careful. Imagine we have a tester which accepts states with property  $\mathcal{P}$  with certainty, and accepts states which are  $\epsilon$ -far away from having property  $\mathcal{P}$  with probability at most  $\delta$ . Then, via the Choi-Jamiołkowski isomorphism, this translates into a tester which accepts unitary matrices with property  $\mathcal{P}'$  with certainty, and accepts, with probability at most  $\delta$ , unitaries which are  $\epsilon$ -far away from any *matrix*  $M$  with  $\langle M, M\rangle = 1$  such that  $M$  has property  $\mathcal{P}'$ . Therefore, in principle it could be the case that  $U$  is far from any unitary matrix with property  $\mathcal{P}'$ , but is close to some non-unitary matrix  $M$  which has property  $\mathcal{P}'$ . In this situation the tester might incorrectly accept. Nevertheless, in various cases of interest one can show that this situation does not arise. In particular, we have the following lemma (which generalizes similar claims in [83, 147]).

**Lemma 21.** *Let  $\mathcal{P} \subseteq M(d)$ , and  $U \in U(d)$ . For  $M \in \mathcal{P}$  such that  $\langle M, M\rangle = 1$ , let  $M = AV$  be a polar decomposition of  $M$ , with  $A = \sqrt{MM^\dagger}$  and  $V$  unitary. Then, if  $V \in \mathcal{P}$  and  $D(U, M) = \epsilon$ ,  $D(U, \mathcal{P} \cap U(d)) \leq 2\epsilon$ .*

*Proof.* We have

$$\langle M, V\rangle = \frac{1}{d} \operatorname{tr} \sqrt{MM^\dagger} = \frac{1}{d} \|M\|_1 = \frac{1}{d} \max_{W \in U(d)} |\operatorname{tr} WM| \geq \sqrt{1 - \epsilon^2},$$

using the definition of the trace norm and that  $D(U, M) = \epsilon$ . Thus

$$D(U, V) \leq D(U, M) + D(M, V) \leq 2\epsilon.$$

□

The following are some examples where one can use this isomorphism to test properties of unitary operators:

- The **Equality to  $V$**  property, where  $U$  satisfies the property if  $U = e^{i\theta}V$ , for some  $\theta$ . The test creates the state  $|U\rangle$  and measures in the basis  $\{|V\rangle\langle V|, I - |V\rangle\langle V|\}$ . Using the analysis of the corresponding property for pure states, this property is testable with  $O(1/\epsilon^2)$  uses of  $U$ . A simple special case of this is the previously discussed **Identity** property.
- The **Equality** property for unitary operators, where  $U$  and  $V$  satisfy the property if  $U = e^{i\theta}V$ , for some  $\theta$ . This can be tested by applying the swap test to  $|U\rangle$  and  $|V\rangle$ ; again, the analysis of the **Equality** property for states goes through unchanged, implying that this property is testable with  $O(1/\epsilon^2)$  uses of  $U$  and  $V$ .
- The **Inverses** property, where  $U, V \in U(d)$  satisfy the property if  $U = e^{i\theta}V^{-1}$ , for some  $\theta$ . The test is to create the state  $|UV\rangle$  with one use of each of  $U$  and  $V$ , then to test for equality to  $|\Phi\rangle$ . The probability of rejection is  $D(UV, I)^2 = D(U, V^{-1})^2$ , so if  $D(U, V^{-1}) = \epsilon$ , the test rejects with probability  $\epsilon^2$ . Note that there is no need to have access to  $U^{-1}$  or  $V^{-1}$ .



- The **Product** property for unitary operators, where an operator  $U \in U(d^n)$  satisfies the property if  $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$  for some  $U_1, \dots, U_n \in U(d)$ . This can be tested by applying the product test described in Section 4.1.2 to  $|U\rangle$  [83]. One also needs to show that, if  $U$  is close to an operator  $A \in M(d^n)$  such that  $A = A_1 \otimes \cdots \otimes A_n$ ,  $U$  is in fact close to a *unitary* operator of this form; this claim follows from Lemma 21. The eventual result is that if  $U$  is product the test accepts with certainty, whereas if  $U$  is  $\epsilon$ -far from product, the test rejects with probability  $\Theta(\epsilon^2)$ .

#### 5.1.4 Membership of the Pauli and Clifford groups

Let  $B = \{B_1, \dots, B_{d^2}\}$  be a unitary operator basis for the set of  $d$ -dimensional square matrices which is orthonormal with respect to the Hilbert-Schmidt inner product, i.e.,  $\langle B_i, B_j \rangle = \delta_{ij}$ . Then the set  $|B_i\rangle$  forms an orthonormal basis for  $\mathbb{C}^{d^2}$  with respect to the standard inner product, implying that one can test membership of a unitary operator  $U$  in  $B$  with the following procedure, which we call the *operator basis test*.

1. Create two copies of  $|U\rangle$ .
2. Measure each copy in the basis  $\{|B_1\rangle, \dots, |B_{d^2}\rangle\}$ .
3. Accept if both measurements give the same result.

The probability of getting outcome  $i$  from each measurement is independent and equal to  $|\langle U, B_i \rangle|^2$ . Thus, if  $U = e^{i\theta} B_i$  for some  $i$ , then the test will accept with certainty. On the other hand, if  $\min_{V \in B} D(U, V) = \epsilon$ , the probability of getting the same measurement outcome twice is

$$\sum_{i=1}^{d^2} |\langle U, B_i \rangle|^4 \leq \max_i |\langle U, B_i \rangle|^2 \sum_{i=1}^{d^2} |\langle U, B_i \rangle|^2 = 1 - \epsilon^2.$$

Therefore, by repeating the operator basis test and rejecting if any of the individual tests reject, the property of **Membership in  $B$**  can be tested with  $O(1/\epsilon^2)$  uses of  $U$ .

A natural operator basis to which this test can be applied is the set of Pauli matrices on  $n$  qubits [122, 147], which form a basis for the space of linear operators on  $n$  qubits. This basis is orthonormal with respect to the Hilbert-Schmidt inner product. We call the corresponding basis for  $\mathbb{C}^{2^{2n}}$  obtained via the Choi-Jamiołkowski isomorphism the *Pauli basis*. The operator basis test can be immediately applied to test whether an  $n$ -qubit operator is proportional to an  $n$ -qubit Pauli matrix, or is far from any such matrix; we call this special case the *Pauli test*. As pointed out in [122], this is a natural quantum generalization of the important classical property of linearity of Boolean functions [33] discussed in Section 2.1. Given access to an oracle for  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , one can readily construct the diagonal unitary operator  $U_f$  where  $U_f|z\rangle = (-1)^{f(z)}|z\rangle$ , and also the controlled unitary operator  $c-U_f$ ; it is easy to see that  $f$  is linear if and only if  $U_f$  is a tensor product of identity and  $Z$  operators. Further, if  $\ell : \{0, 1\}^n \rightarrow \{0, 1\}$  is a linear Boolean function, the distance between  $c-U_f$  and  $c-U_\ell$  is

$$\begin{aligned} D(c-U_f, c-U_\ell) &= \sqrt{1 - \left( \frac{1}{2} + \frac{1}{2^{n+1}} \sum_{z \in \{0,1\}^n} (-1)^{f(z)+\ell(z)} \right)^2} \\ &= \sqrt{1 - (1 - |\{z : f(z) \neq \ell(z)\}|/2^n)^2} \\ &= \sqrt{2d(f, \ell) - d(f, \ell)^2}. \end{aligned}$$

This implies that the Pauli test can be used to test linearity of Boolean functions, recovering the  $O(1)$  complexity of Section 2.1.1.

The Pauli test can also be used as a subroutine in an algorithm for testing membership in the *Clifford group*. The Clifford group  $\mathcal{C}_n$  on  $n$  qubits is the normalizer of the Pauli group  $\mathcal{P}_n$ , or in other words the set  $\{C \in U(2^n) : \forall P \in \mathcal{P}_n, CPC^{-1} \in \mathcal{P}_n\}$ . The Clifford group plays an important role in many areas of quantum information theory, including quantum error-correction and simulation of quantum circuits [73, 124]. Wang [147] has shown that, given access to a unitary  $U$  and its inverse  $U^{-1}$ , whether  $U$  is a member of the Clifford group can be tested with  $O(1/\epsilon^2)$  uses of  $U$  and  $U^{-1}$ ; this result improves a previous test of Low [110] by removing any dependence on  $n$ , and can in turn be improved to  $O(1/\epsilon)$  using amplitude amplification [36].

Wang’s test is very natural: pick a Pauli matrix  $P \in \mathcal{P}_n$  uniformly at random, and apply the Pauli test to the operator  $UPU^{-1}$ . If  $U \in \mathcal{C}_n$ , this test will always accept. Intuitively, if  $U$  is far from any Clifford operator, then we expect that for most Pauli operators  $P$ ,  $UPU^{-1}$  will be far from being a Pauli operator, so repeating this test a constant number of times would suffice to detect this. Making this intuition precise requires some work; see [147] for the details.

**Question 9.** *Is there an efficient test for the property of membership in the Clifford group which does not require access to  $U^{-1}$ ?*

### 5.1.5 Testing commutativity

Say that  $U, V \in U(d)$  satisfy the **Commuting** property if  $UV = VU$ . Assuming that we are given access to the controlled operators  $c-U$  and  $c-V$ , consider the following tester for this property:

1. Create the states  $|c-Uc-V\rangle, |c-Vc-U\rangle$  by applying controlled- $U$  and controlled- $V$  operations to the first half of each of two maximally entangled states.
2. Apply the swap test to these states and accept if the test accepts.

If  $U$  and  $V$  commute, then  $c-U$  and  $c-V$  also commute, so  $|c-Uc-V\rangle = |c-Vc-U\rangle$  and hence the swap test accepts with certainty. On the other hand, if  $\|UV - VU\|_2 = \epsilon$ , then by (5) the test rejects with probability at least  $\epsilon^2/8$ . In order for this to be a good test for commutativity, we therefore need to show that, if  $\|UV - VU\|_2 = \epsilon$ ,  $U$  and  $V$  are close to a pair of unitary operators  $\tilde{U}, \tilde{V}$  such that  $\tilde{U}$  and  $\tilde{V}$  commute. Precisely this result has recently been shown by Glebsky [69] in the form of the following theorem, whose proof we omit.

**Theorem 22** (Glebsky [69]). *Let  $U, V \in U(d)$  satisfy  $\|UV - VU\|_2 = \epsilon$ . Then there exist  $\tilde{U}, \tilde{V} \in U(d)$  such that  $\tilde{U}$  and  $\tilde{V}$  commute and  $\|U - \tilde{U}\|_2 \leq 30\epsilon^{1/9}, \|V - \tilde{V}\|_2 \leq 30\epsilon^{1/9}$ .*

The consequence is that the above tester rejects pairs  $(U, V)$  such that  $U$  and  $V$  are  $\epsilon$ -far from a pair of commuting matrices with probability  $\Omega(\epsilon^{18})$ . By repeating the test  $\text{poly}(1/\epsilon)$  times, we obtain a tester which rejects such pairs with constant probability.

**Question 10.** *Is there an efficient test for commutativity which does not require access to the controlled unitaries  $c-U, c-V$ , but just uses  $U$  and  $V$ ?*

### 5.1.6 Testing quantum juntas

Analogously to the classical case of Boolean functions  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , a unitary operation on  $n$  qubits is said to be a *k-junta* if it acts non-trivially on at most  $k$  of the qubits, or in other

words is of the form  $U_S \otimes I_{S^c}$ , where  $U \in U(2^k)$  and  $S$  is a  $k$ -subset of  $[n]$ . Wang [147] has given a tester for whether a unitary operator  $U$  is a  $k$ -junta, which turns out to be a direct generalization of the tester of Atııcı and Servedio [17] for the classical property of a Boolean function being a  $k$ -junta (Section 2.1.3). The work [122] had previously studied a different tester for being a 1-junta (“dictator”), but did not prove correctness. Wang’s tester proceeds as follows:

1. Set  $W = \emptyset$ .
2. Repeat the following procedure  $T$  times, for some  $T$  to be determined:
  - (a) Create the state  $|U\rangle$  and measure in the Pauli basis, obtaining outcome  $s \in \{I, X, Y, Z\}^n$ .
  - (b) Update  $W \leftarrow W \cup \{i : s_i \neq I\}$ .
  - (c) If  $|W| > k$ , reject.
3. Accept.

To show correctness of this test, it suffices to prove the following claim:

**Theorem 23** (Wang [147]). *If  $U$  is  $\epsilon$ -far from any  $k$ -junta, and  $T = \Theta(k/\epsilon^2)$ , the above procedure accepts with probability at most  $1/3$ .*

The result originally shown by Wang [147] was a somewhat worse bound of  $T = \Theta(k \log(k/\epsilon)/\epsilon^2)$ , but the bound can be improved to  $\Theta(k/\epsilon^2)$  via a straightforward generalization of the analysis of Atııcı and Servedio [17], as we now show (cf. Section 2.1.3). If we are given access to  $U^{-1}$  as well, the bound can be improved further to  $T = \Theta(k/\epsilon)$  via amplitude amplification.

*Proof.* As the Pauli matrices form a basis for the space of  $n$ -qubit operators, we can expand

$$U = \sum_{s \in \{I, X, Y, Z\}^n} \widehat{U}_s \sigma_s,$$

where  $\sigma_s$  is the  $n$ -qubit Pauli operator corresponding to the string  $s$ , and  $\widehat{U}_s \in \mathbb{C}$ . Pauli matrices are orthonormal with respect to the Hilbert-Schmidt inner product, hence  $\sum_{s \in \{I, X, Y, Z\}^n} |\widehat{U}_s|^2 = 1$ . Assume that  $U$  is  $\epsilon$ -far from any unitary operator  $V$  that is a  $k$ -junta, and for  $s \in \{I, X, Y, Z\}^n$ , let  $\text{supp } s = \{i : s_i \neq I\}$ . Then, for any subset  $W \subseteq [n]$  of size at most  $k$ ,

$$w_W := \sum_{s, \text{supp } s \subseteq W} |\widehat{U}_s|^2 \leq \sqrt{1 - \epsilon^2/4} \leq 1 - \epsilon^2/8. \quad (6)$$

To see this, assume the opposite and consider the operator  $M_W = \sum_{s, \text{supp } s \subseteq W} \widehat{U}_s \sigma_s$ . Then  $D(U, M_W) = (1 - w_W^2)^{1/2} < \epsilon/2$ .  $M_W$  is clearly a  $k$ -junta, but is not necessarily unitary; however, by Lemma 21, there must exist some unitary operator  $V$  such that  $V$  is a  $k$ -junta and  $D(U, V) \leq \epsilon$ , contradicting that  $U$  is  $\epsilon$ -far from any unitary  $k$ -junta.

For each measurement, the probability that a string  $s$  is returned such that  $\text{supp } s \not\subseteq W$  is therefore at least  $\epsilon^2/8$ . Thus the expected number of new indices learned on which  $U$  acts non-trivially is at least  $\epsilon^2/8$ , so the expected number of measurements required to find  $k+1$  such indices is at most  $8(k+1)/\epsilon^2$ . The theorem then follows from Markov’s inequality.  $\square$

### 5.1.7 Other properties of unitary matrices

We finish this section by mentioning a few other properties of unitary matrices which have fairly straightforward testers. Say that a unitary matrix  $U$  satisfies the **Diagonality** property if  $U_{ij} = 0$  for  $i \neq j$ . Consider the following easy tester for this property: Apply  $U$  to a uniformly random computational basis state  $|i\rangle$ , measure in the computational basis, and accept if and only if the outcome is  $i$ . Writing  $U_{kk} = r_k e^{i\gamma_k}$  for  $r_k \geq 0$  and  $0 \leq \theta_k < 2\pi$ , we have

$$\max_{D \text{ diagonal}} |\langle U, D \rangle| = \frac{1}{d} \max_{D \text{ diagonal}} \left| \sum_{k=1}^d U_{kk}^* D_{kk} \right| = \frac{1}{d} \max_{\theta_k} \left| \sum_{k=1}^d r_k e^{i(\theta_k - \gamma_k)} \right| = \frac{1}{d} \left| \sum_{k=1}^d r_k \right| = \frac{1}{d} \sum_{k=1}^d |U_{kk}|.$$

On the other hand, the probability of accepting is precisely

$$\frac{1}{d} \sum_{k=1}^d |U_{kk}|^2 \leq \frac{1}{d} \max_k |U_{kk}| \sum_{k=1}^d |U_{kk}| \leq \frac{1}{d} \sum_{k=1}^d |U_{kk}|.$$

Thus, if the test accepts with probability  $1 - \epsilon$ ,  $U$  is distance at most  $\sqrt{2\epsilon}$  from a diagonal unitary matrix  $D$ , implying that **Diagonality** can be tested with  $O(1/\epsilon^2)$  uses of  $U$ .

This tester is simple, but can be applied to the following more general problem: Given a basis  $B$  for  $\mathbb{C}^d$ , is every vector in  $B$  an eigenvector of  $U$ ? This is equivalent to asking whether  $VUV^{-1}$  is diagonal, where  $V$  is the change of basis matrix for  $B$ . This problem can be solved by applying the test for diagonality to  $VUV^{-1}$ , noting that the distance of  $VUV^{-1}$  from the nearest diagonal matrix is the same as the distance of  $U$  from the nearest matrix  $\tilde{U}$  such that every vector in  $B$  is an eigenvector of  $\tilde{U}$ . For example, this allows us to test  $U$  for being a **Circulant** matrix (i.e., a matrix of the form  $U_{xy} = f(x - y)$  for some  $f : \{0, \dots, d - 1\} \rightarrow \mathbb{C}$ , where subtraction is understood modulo  $d$ ) as such matrices are characterized by being diagonalized by the quantum Fourier transform over  $\mathbb{Z}_d$ .

Finally, Wang [147] has proven that membership of a unitary operator  $U \in U(d)$  in the orthogonal group  $O(d) := \{M \in M(d) : MM^T = I\}$  can be tested with  $O(1/\epsilon^2)$  uses of  $U$ . The tester is based on applying  $U \otimes U$  to  $|\Phi\rangle$ , which produces the state  $|UU^T\rangle$ , then performing the measurement  $\{|\Phi\rangle\langle\Phi|, I - |\Phi\rangle\langle\Phi|\}$ . If  $U \in O(d)$ , the test always accepts; Wang shows that if the test accepts with high probability, then  $U$  is close to an orthogonal matrix.

## 5.2 Properties of quantum channels

Not all physical processes which occur in quantum mechanics are reversible. The mathematical framework in which the most general physically realizable operations are studied is the formalism of *quantum channels*. A quantum channel (or “superoperator”) is a completely positive, trace-preserving linear map  $\mathcal{E} : \mathcal{B}(\mathbb{C}^{d_{\text{in}}}) \rightarrow \mathcal{B}(\mathbb{C}^{d_{\text{out}}})$ . Here “completely positive” means that the operator  $\mathcal{E} \otimes \text{id}$  preserves positivity, where  $\text{id}$  is the identity map on some ancilla system of arbitrary dimension. A comprehensive introduction to the world of quantum channels is provided by lecture notes of Watrous [149].

There has been less work on testing properties of quantum channels than the other categories of property considered above, although the problem of discriminating between quantum channels has been considered by a number of authors (e.g. [138, 61, 129]).

### 5.2.1 Distance measures

In the context of property testing, the first task when considering quantum channels is to define a suitable measure of distance. One approach is to use the same idea as for unitary operators, and take the distance induced by the Choi-Jamiołkowski isomorphism [52, 95]. In the case of channels, this isomorphism states that there is a bijection between the set of quantum channels  $\mathcal{E} : \mathcal{B}(\mathbb{C}^{d_{\text{in}}}) \rightarrow \mathcal{B}(\mathbb{C}^{d_{\text{out}}})$  and the set of bipartite density matrices  $\rho$  on a  $(d_{\text{out}} \times d_{\text{in}})$ -dimensional system such that applying the partial trace to the first subsystem of  $\rho$  leaves the maximally mixed state  $I/d_{\text{in}}$ . The bijection can be explicitly given as

$$\mathcal{E} \leftrightarrow \frac{1}{d_{\text{in}}} \sum_{i,j=1}^{d_{\text{in}}} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j| =: \chi_{\mathcal{E}}.$$

Then one distance measure that can be put on quantum channels  $\mathcal{E}, \mathcal{F}$  is

$$D(\mathcal{E}, \mathcal{F}) := D(\chi_{\mathcal{E}}, \chi_{\mathcal{F}}).$$

As with the correspondence between unitary operators and pure states, this distance measure allows one to translate tests for properties of mixed states to properties of channels. For example, consider the property **Unitarity**, where  $\mathcal{E} : \mathcal{B}(\mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{C}^d)$  satisfies the property if and only if it is a unitary operator.  $\mathcal{E}$  is unitary if and only if  $\chi_{\mathcal{E}}$  is a pure state (and hence maximally entangled). In order to test this property, we can apply the test for **Purity** of mixed states to  $\chi_{\mathcal{E}}$ . From the analysis of Section 4.2, we see that if the test accepts with probability  $1 - \delta$ , there exists a pure state  $|\psi\rangle$  such that  $D(\chi_{\mathcal{E}}, |\psi\rangle\langle\psi|) = O(\delta)$ . We still need to show that  $\chi_{\mathcal{E}}$  is in fact close to a pure state which is maximally entangled. To do so, first write  $|\psi\rangle = \sum_{i=1}^d \sqrt{\lambda_i} |v_i\rangle |w_i\rangle$  for the Schmidt decomposition of  $|\psi\rangle$ , and define the maximally entangled state  $|\eta\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |v_i\rangle |w_i\rangle$ .

Then we have the sequence of inequalities and equalities

$$\begin{aligned} D(\chi_{\mathcal{E}}, |\psi\rangle\langle\psi|) &\geq D(I/d, \text{tr}_B |\psi\rangle\langle\psi|) \geq 1 - F(I/d, \text{tr}_B |\psi\rangle\langle\psi|) = 1 - \frac{1}{\sqrt{d}} \sum_{i=1}^d \sqrt{\lambda_i} \\ &= 1 - |\langle\psi|\eta\rangle| \geq D(|\psi\rangle\langle\psi|, |\eta\rangle\langle\eta|)^2/2. \end{aligned}$$

The first inequality holds because the trace norm does not increase under partial trace [124, Theorem 9.2], and the second is (4). Therefore, if the test accepts with probability  $1 - \delta$ ,

$$D(\chi_{\mathcal{E}}, |\eta\rangle\langle\eta|) \leq D(\chi_{\mathcal{E}}, |\psi\rangle\langle\psi|) + D(|\psi\rangle\langle\psi|, |\eta\rangle\langle\eta|) = O(\delta + \sqrt{2\delta}) = O(\sqrt{\delta}),$$

implying that **Unitarity** of a quantum channel can be tested with  $O(1/\epsilon^2)$  uses of the channel.

### 5.2.2 Testing quantum measurements

An important special case of quantum channels is the case of *quantum measurements*. In full generality, a measurement on a  $d$ -dimensional quantum mechanical system is defined by a sequence of linear operators  $M = (M_1, \dots, M_k)$  such that  $\sum_{i=1}^k M_i^\dagger M_i = I$ . If  $M$  is performed on the state  $\rho$ , the probability of receiving outcome  $i$  is  $\text{tr} M_i \rho M_i^\dagger$ , and the resulting state of the system, given that outcome  $i$  occurred, is

$$\rho_i = \frac{M_i \rho M_i^\dagger}{\text{tr} M_i \rho M_i^\dagger}.$$

The quantum channel corresponding to performing the measurement  $M$  and storing the outcome in a new register is the map  $\mathcal{M}$  where

$$\mathcal{M}(\rho) = \sum_{i=1}^k M_i \rho M_i^\dagger \otimes |i\rangle\langle i|,$$

so the Choi-Jamiołkowski state is

$$\chi_{\mathcal{M}} = \frac{1}{d} \sum_{i,j=1}^d \left( \sum_{\ell=1}^k M_\ell |i\rangle\langle j| M_\ell^\dagger \otimes |\ell\rangle\langle \ell| \right) \otimes |i\rangle\langle j|$$

which, by reordering subsystems, is equivalent to

$$\sum_{\ell=1}^k \left( \frac{1}{\sqrt{d}} \sum_{i=1}^d M_\ell |i\rangle\langle i| \right) \left( \frac{1}{\sqrt{d}} \sum_{j=1}^d M_\ell^\dagger |j\rangle\langle j| \right) \otimes |\ell\rangle\langle \ell| =: \sum_{\ell=1}^k |\psi_M^{(\ell)}\rangle\langle \psi_M^{(\ell)}| \otimes |\ell\rangle\langle \ell|.$$

For any two measurements  $M$  and  $N$  with at most  $k$  outcomes, we can therefore compute the distance between the corresponding channels as

$$D(\mathcal{M}, \mathcal{N}) = \sum_{\ell=1}^k D \left( |\psi_M^{(\ell)}\rangle, |\psi_N^{(\ell)}\rangle \right),$$

where if  $M$  (resp.  $N$ ) has  $\ell < k$  outcomes, we set  $M_i = 0$  (resp.  $N_i = 0$ ) for  $\ell < i \leq k$ . Observe that, using this measure of distance, we take into account the distance of the post-measurement states as well as the distance between the probability distributions corresponding to the measurement outcomes. One can explicitly calculate that, for any (potentially unnormalized) vectors  $|\psi\rangle, |\phi\rangle$ ,

$$D(|\psi\rangle, |\phi\rangle) = \sqrt{\frac{1}{4} (\langle \psi | \psi \rangle + \langle \phi | \phi \rangle)^2 - |\langle \psi | \phi \rangle|^2},$$

which implies that

$$D(\mathcal{M}, \mathcal{N}) = \frac{1}{2} \sum_{i=1}^k \sqrt{(\langle M_i, M_i \rangle + \langle N_i, N_i \rangle)^2 - 4|\langle M_i, N_i \rangle|^2}.$$

Recent work by Wang [148] has given efficient tests for a number of properties of quantum measurements, but with respect to a measure of distance which appears somewhat different to the measure  $D(\cdot, \cdot)$ . Given two measurements  $M$  and  $N$  with at most  $k$  outcomes, Wang's distance measure is

$$\Delta(M, N) := \sqrt{\frac{1}{2} \sum_{i=1}^k \langle M_i, M_i \rangle + \langle N_i, N_i \rangle - 2|\langle M_i, N_i \rangle|}.$$

Wang demonstrates that  $\Delta(\cdot, \cdot)$  has a number of desirable properties, including satisfying the triangle inequality and being an ‘‘average-case’’ measure of distance [148]. It turns out that  $\Delta(\cdot, \cdot)$  is in fact closely related to  $D(\cdot, \cdot)$ , which we encapsulate as the following lemma.

**Lemma 24.** *Given two measurements  $M$  and  $N$ , let  $\mathcal{M}$  and  $\mathcal{N}$  be the corresponding channels. Then*

$$D(\mathcal{M}, \mathcal{N})/\sqrt{2} \leq \Delta(M, N) \leq D(\mathcal{M}, \mathcal{N})^{1/2}.$$

*Proof.* To prove the upper bound part of the lemma, it suffices to show that, for each  $i$ ,

$$(\langle M_i, M_i \rangle + \langle N_i, N_i \rangle - 2|\langle M_i, N_i \rangle|)^2 \stackrel{?}{\leq} (\langle M_i, M_i \rangle + \langle N_i, N_i \rangle)^2 - 4|\langle M_i, N_i \rangle|^2.$$

Setting  $x_i = \langle M_i, M_i \rangle + \langle N_i, N_i \rangle$ ,  $y_i = 2|\langle M_i, N_i \rangle|$  and rearranging terms, we get the claimed inequality

$$(x_i - y_i)^2 \stackrel{?}{\leq} (x_i - y_i)(x_i + y_i),$$

which holds because  $y_i \leq x_i$  by Cauchy-Schwarz. For the lower bound, we need to show

$$\frac{1}{2\sqrt{2}} \sum_{i=1}^k (x_i - y_i)^{1/2} (x_i + y_i)^{1/2} \stackrel{?}{\leq} \sqrt{\frac{1}{2} \sum_{i=1}^k (x_i - y_i)}.$$

By Cauchy-Schwarz,

$$\begin{aligned} \frac{1}{2\sqrt{2}} \sum_{i=1}^k (x_i - y_i)^{1/2} (x_i + y_i)^{1/2} &\leq \frac{1}{2\sqrt{2}} \sqrt{\sum_{i=1}^k (x_i - y_i)} \sqrt{\sum_{i=1}^k (x_i + y_i)} \\ &\leq \frac{1}{\sqrt{2}} \sqrt{\frac{1}{2} \sum_{i=1}^k (x_i - y_i)} \sqrt{2 \sum_{i=1}^k x_i} \\ &= \sqrt{\frac{1}{2} \sum_{i=1}^k (x_i - y_i)} \end{aligned}$$

as required, using  $\sum_{i=1}^k \langle M_i, M_i \rangle = \sum_{i=1}^k \langle N_i, N_i \rangle = 1$ .  $\square$

Lemma 24 implies that Wang's results with respect to the distance measure  $\Delta(\cdot, \cdot)$  can be translated into results with respect to  $D(\cdot, \cdot)$ . In particular, Wang [148] gives efficient testers for the following properties of quantum measurements:

- The property of being a **Pauli** measurement (called “stabilizer measurement” in [148]):  $M$  is a Pauli measurement if it is a two-outcome projective measurement onto the  $\pm 1$  eigenspaces of an  $n$ -qubit Pauli operator  $\sigma_s$ , for some  $s \in \{I, X, Y, Z\}^n$ . Wang shows that this property can be tested with  $O(1/\epsilon^4)$  measurements.
- The property of being a  **$k$ -local** measurement of  $n$  qubits, i.e., acting non-trivially on at most  $k$  qubits. Wang gives a tester for this property which uses  $O(k \log(k/\epsilon)/\epsilon^2)$  measurements.
- The property of being a **Permutation invariant** measurement of  $n$   $d$ -dimensional systems, i.e., a measurement which is unchanged when the  $n$  systems are permuted arbitrarily. This property can be tested with  $O(1/\epsilon^2)$  measurements.
- Being contained within any finite set of measurements  $\mathcal{S} = \{M_i\}$  with  $k$  outcomes on a  $d$ -dimensional system. If  $\Delta(M_i, M_j) \geq \gamma$  for all  $i \neq j$ , and we set  $\delta = \min\{\gamma, \epsilon\}$ , membership in  $\mathcal{S}$  can be tested with  $O(k^2(\log k)/\delta^8 + (\log |\mathcal{S}|)/\delta^2)$  measurements.
- **Equality** of measurements, which can be tested with  $O(k^5(\log k)/\epsilon^{12})$  measurements. This is based on a more general algorithm for estimating the distance between measurements.

All of the above testers are based on constructing multiple copies of the Choi-Jamiołkowski state corresponding to the measurement to be tested, and performing some measurements on the states. As remarked in [148], it is an interesting question whether efficient testers can be designed in a setting where one is not allowed access to entanglement.

**Question 11.** *Can testers for the properties of unitary operators and quantum channels discussed above be designed which do not require entanglement with an ancilla system?*

### 5.3 Quantum properties and computational complexity

A different perspective from which to study the question of testing properties of quantum systems is to consider problems where, instead of being given access to a quantum object, we are given a concise classical description of that object (for example, a quantum circuit on  $n$  qubits with  $\text{poly}(n)$  gates), and aim to determine whether the corresponding quantum object has some property, or is far from having that property. Here we generally assume we have full knowledge of this description, and aim to test the corresponding object for having some property in time polynomial in the size of the description. This type of problem turns out to be naturally addressed via the framework of computational complexity.

A classic and important example is the *local Hamiltonian problem*. Here we are given as input a Hamiltonian  $H$  on  $n$  qubits, described by a set of Hermitian operators  $H_i$  such that  $H = \sum_{i=1}^m H_i$ , with each operator  $H_i$  acting non-trivially on at most  $k = O(1)$  qubits and satisfying  $\|H_i\| = O(1)$ . We are also given two real numbers  $a$  and  $b$  such that  $b - a \geq 1/\text{poly}(n)$ . We are promised that the lowest eigenvalue of  $H$  is either smaller than  $a$ , or larger than  $b$ ; our task is to determine which of these is the case.

This problem was proven QMA-complete<sup>12</sup> for  $k = 5$  by Kitaev [101], which was later improved to  $k = 2$  by Kempe et al. [99] (the case where  $k = 1$  is easily seen to be in P). One way in which this hardness result could potentially be improved is in the scaling of the gap between  $b$  and  $a$ . Indeed, it could be the case that the local Hamiltonian problem remains QMA-hard if we have the promise  $b - a \geq cm$  for some constant  $0 < c < 1$ . This is (one formulation of) the quantum PCP conjecture; see a recent survey of Aharonov et al. [10] for much more on this conjecture and its implications. Classically, one version of the famous PCP Theorem states that there exist constraint satisfaction problems for which it is hard to distinguish between there existing an assignment to the variables that satisfies all of the constraints, and there being no assignment that satisfies more than a constant fraction of them; the quantum PCP conjecture would be a direct quantization of this result. One way of looking at this is as the conjecture that the local Hamiltonian problem remains hard in a “property-testing-type” scenario where there is a large gap between “yes” and “no” instances.

**Question 12.** *Is there a quantum PCP theorem?*

Classically, the proof of the PCP Theorem relied on efficient property testers, so it seems plausible that property testing could be useful in proving a quantum generalization. Indeed, the analysis of a *classical* property tester in a quantum setting has recently been central to establishing a quantum complexity-theoretic result. MIP is the class of languages decided by multiple-prover interactive proof systems, which was shown to be equal to NEXP by Babai et al. [19]. Recently Ito and Vidick [93] have shown that the quantum generalization MIP\*, where the provers are allowed to share entanglement, is at least as powerful:  $\text{MIP} \subseteq \text{MIP}^*$ . Their proof is based on proving soundness

---

<sup>12</sup>QMA is the quantum analog of NP [101].



of the classical multilinearity test of Babai et al. [19] in the presence of entanglement. Another application of quantum property testing to quantum complexity is the use of the analysis of an efficient quantum property tester to prove the complexity class equality  $\text{QMA}(k) = \text{QMA}(2)$  [83], as discussed in Section 4.1.2.

Yet another connection is explored in very recent work of Aharonov and Eldar [11] on a quantum generalization of *locally testable codes* (LTCs). Classically, LTCs are codes for which the property of being a codeword can be tested efficiently by means of a few local checks; such codes played a crucial role in the proof of the PCP Theorem. The “qLTCs” studied in [11] are zero eigenspaces of  $k$ -local Hamiltonians  $H = \sum_i H_i$ , such that containment of a state in the eigenspace can be tested with good accuracy by performing measurements corresponding to only a few of the individual  $k$ -local terms  $H_i$ . Aharonov and Eldar [11] prove some surprising upper bounds on the soundness for qLTCs that are *stabilizer* codes, showing that in some regimes these behave quite differently from classical LTCs.

### 5.3.1 Properties of quantum circuits

When studied through the prism of computational complexity, many problems related to testing quantum circuits turn out to be QMA-complete (see [34] for a recent survey). These hardness results provide an interesting counterpoint to the largely positive results obtained in the “average-case” scenarios considered by property testing. A prototypical example of this phenomenon is “non-identity-check,” which was proven to be QMA-complete by Janzing et al. [96]. Here the input is a quantum circuit implementing a unitary  $U$ , and two numbers  $a, b$  such that  $b - a \geq 1/\text{poly}(n)$ , and the problem is to distinguish between the two cases that  $\min_{\theta \in \mathbb{R}} \|U - e^{i\theta} I\| \leq a$  and  $\min_{\theta \in \mathbb{R}} \|U - e^{i\theta} I\| \geq b$ . Observe that, if we replace the operator norm with the normalized 2-norm in this definition, this problem is in BQP by the efficient tester for the **Equality to  $V$**  property discussed in Section 5.1.3.

If one generalizes to quantum circuits acting on mixed states, where each elementary gate is a quantum channel, some natural problems even become PSPACE-complete. In particular, Rosgen and Watrous [137] showed that this holds for the problem of testing whether two mixed-state quantum circuits are distinguishable, which remains hard when the quantum circuits are restricted to be logarithmic depth [135], degradable or anti-degradable [136]. In this case, distinguishability is measured in the so-called diamond norm for quantum channels [101]; the diamond norm of a linear operator  $\Phi : \mathcal{B}(\mathbb{C}^{d_{\text{in}}}) \rightarrow \mathcal{B}(\mathbb{C}^{d_{\text{out}}})$  is defined to be

$$\|\Phi\|_{\diamond} := \max_{X, \|X\|_1=1} \|(\Phi \otimes \text{id})(X)\|_1,$$

where  $\text{id}$  is the identity map acting on an ancilla system, which may be taken to be of dimension at most  $d_{\text{in}}$ . Then the Quantum Circuit Distinguishability problem is to determine, given two mixed-state quantum circuits  $Q_0, Q_1$  and constants  $a < b$ , whether  $\|Q_0 - Q_1\|_{\diamond} \leq a$  or  $\|Q_0 - Q_1\|_{\diamond} \geq b$ .

These distinguishability problems were originally shown to be hard for the complexity class QIP of languages decided by quantum interactive proof systems, but this class was later proven to equal PSPACE [94]. The proof technique of [137] starts by using a result of Kitaev and Watrous [102], which states that all quantum interactive proofs can be parallelized to three rounds. A mathematical reformulation of this result is that the Close Images problem is QIP-hard. This problem is defined as follows: given two quantum circuits  $Q_0, Q_1$  and constants  $a < b$ , distinguish between the cases that there is an input  $\rho$  such that  $F(Q_0(\rho), Q_1(\rho)) \geq b$ , or that for all inputs  $\rho$ ,  $F(Q_0(\rho), Q_1(\rho)) \leq a$ . Hardness of Quantum Circuit Distinguishability is then shown by a reduction from Close Images [137].

On the other hand, recent work by Hayden et al. [85] demonstrates that quantum property testers can be used to prove positive results regarding the complexity of testing properties of quantum circuits. The problem considered by these authors is a variant of the separability-testing problem (cf. Sections 4.1.2 and 4.2). In this variant the input is the description of a mixed-state quantum circuit  $Q$  on  $n$  qubits, and one considers the output of the circuit as a bipartite state by dividing these qubits into two disjoint sets. The problem is to distinguish between the two cases that: a) the output of  $Q$ , when applied to the input  $|0^n\rangle$ , is close to separable; b) the output is far from separable. Hayden et al. [85] show that this problem can be solved by a quantum interactive proof system with two messages (i.e., a message from verifier to prover, followed by a reply from prover to verifier), and hence sits in the complexity class QIP(2). The protocol is based on the verifier applying the permutation test discussed in Section 4.1.1. In this result “close” and “far” are defined asymmetrically (the former in terms of the trace distance, the latter in terms of the so-called “1-way LOCC” distance); see [85] for details.

Very recently, Milner et al. [119] have generalised this work to give entanglement detection problems which are complete for a variety of quantum complexity classes. Some of these results are based on property testers too; for example, they use the product test of [83] (see Section 4.1.2) to show that testing whether the output of a pure-state quantum circuit is a product state is in BQP.

## 6 Conclusion

The goal of property testing is to design efficient algorithms (“testers”) to decide whether a given object has a property or is somehow “far” from that property. When the objects that need to be tested are very large, exact algorithms that are also required to work for objects that “almost” have the property become infeasible, and property testing is often the best we can hope for. Classical property testing is by now a very well-developed area, but *quantum* property testing is just starting out. In this paper we surveyed what is known about this:

1. Quantum testers for classical properties (Section 2).
2. Classical testers for quantum properties (Section 3).
3. Quantum testers for quantum properties (Sections 4 and 5).

We hope the overview given here, as well as the open questions mentioned along the way, will give rise to much more research in this area. As well as the properties mentioned previously, there are many other properties which have been of great interest in the classical property testing literature, and whose quantum complexity is unknown. Examples include monotonicity of Boolean functions, membership of error-correcting codes, and almost all properties of graphs. In the case of quantum properties, natural targets include testing whether a unitary operator is implemented by a small circuit, and whether a Hamiltonian is  $k$ -local (which would be yet another variant of junta testing).

Another very broad open question not discussed previously is to what extent one could characterize the properties (classical or quantum) that have efficient quantum testers. This may seem a hopelessly ambitious goal; nevertheless, in the case of classical algorithms it has already been achieved in some important cases, such as graph properties [12] and symmetric properties of probability distributions [144]. Such a characterization could have importance far beyond property testing, by shedding light on the structure of problems that have efficient quantum algorithms.

## Acknowledgements

We thank Scott Aaronson, Robin Blume-Kohout, Sourav Chakraborty, Wim van Dam, Aram Harrow, Frédéric Magniez, Marcelo Marchioli, Miguel Navascués, Falk Unger, Lev Vaidman, Andreas Winter and Tzyh Haur Yang for helpful comments, answers to questions and pointers to literature.

## References

- [1] S. Aaronson. QMA/qpoly  $\subseteq$  PSPACE/poly: De-Merlinizing quantum protocols. In *Proceedings of 21st Annual IEEE Conference on Computational Complexity (CCC)*, pages 261–273, 2006. [quant-ph/0510230](#).
- [2] S. Aaronson. BQP and the Polynomial Hierarchy. In *Proceedings of 42nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 141–150, 2010. [arXiv:0910.4698](#).
- [3] S. Aaronson and A. Ambainis. The need for structure in quantum speedups. In *Proceedings of Innovations in Computer Science (ICS)*, pages 338–352, 2011. [arXiv:0911.0996](#).
- [4] S. Aaronson and A. Ambainis. Forrelation: A problem capturing the power of quantum algorithms, October 2011. Unpublished manuscript.
- [5] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009. [arXiv:0804.0802](#).
- [6] S. Aaronson and D. Gottesman. Identifying stabilizer states, 2008. <http://pirsa.org/08080052/>.
- [7] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004. Earlier versions in STOC’02 and FOCS’02.
- [8] A. Acín. Statistical distinguishability between unitary operations. *Physical Review Letters*, 87(17):177901, 2001. [quant-ph/0102064](#).
- [9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2008.
- [10] D. Aharonov, I. Arad, and T. Vidick. The quantum PCP conjecture. *ACM SIGACT News*, 44(2):47–79, 2013. Enhanced version at [arXiv:1309.7495](#).
- [11] D. Aharonov and L. Eldar. Quantum locally testable codes, Oct 21 2013. [arXiv:1310.5664](#).
- [12] N. Alon, E. Fischer, I. Newman, and A. Shapira. A combinatorial characterization of the testable graph properties: it’s all about regularity. *SIAM Journal on Computing*, 39(1):143–167, 2009.
- [13] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron. Testing Reed-Muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4038, 2005.
- [14] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. Earlier version in STOC’00. [quant-ph/0002066](#).
- [15] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007. Earlier version in FOCS’04. [quant-ph/0311001](#).
- [16] A. Ambainis, A. Childs, and Y-K. Liu. Quantum property testing for bounded-degree graphs. In *Proceedings of 15th RANDOM*, volume 6845 of *Lecture Notes in Computer Science*, pages 365–376, 2011. [arXiv:1012.3174](#).
- [17] A. Atıcı and R. Servedio. Quantum algorithms for learning and testing juntas. *Quantum Information Processing*, 6(5):323–348, 2009. [arXiv:0707.3479](#).
- [18] K. Audenaert. A digest on representation theory of the symmetric group, 2006. Available at [http://personal.rhul.ac.uk/usah/080/QITNotes\\_files/I](http://personal.rhul.ac.uk/usah/080/QITNotes_files/I)
- [19] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991. Earlier version in FOCS’90.
- [20] D. Bacon, I. Chuang, and A. Harrow. Efficient quantum circuits for Schur and Clebsch-Gordan transforms. *Physical Review Letters*, 97(17):170502, 2006. [quant-ph/0407082](#).
- [21] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello. Stabilisation of quantum computations by symmetrisation. *SIAM Journal on Computing*, 26(5):1541–1557, 1997. [quant-ph/9604028](#).

- [22] S. Barnett and S. Croke. Quantum state discrimination. *Advances in Optics and Photonics*, 1(2):238–278, 2009. [arXiv:0810.1970](#).
- [23] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, June 2005.
- [24] T. Batu, L. Fortnow, E. Fischer, R. Kumar, R. Rubinfeld, and P. White. Testing random variables for independence and identity. In *Proceedings of 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 442–451, 2001.
- [25] T. Batu, L. Fortnow, R. Rubinfeld, W. Smith, and P. White. Testing closeness of discrete distributions. *Journal of the ACM*, 60(1), 2013. Previous version in FOCS’00. [arXiv:1009.5397](#).
- [26] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proceedings of 29th Annual ACM Symposium on Theory of Computing (STOC)*, pages 48–53, 1997.
- [27] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. Earlier version in FOCS’98. [quant-ph/9802049](#).
- [28] M. Bellare, D. Coppersmith, J. Høastad, M. Kiwi, and M. Sudan. Linearity testing in characteristic two. *IEEE Transactions on Information Theory*, 42(6), 1996.
- [29] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. [quant-ph/9701001](#).
- [30] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Earlier version in STOC’93.
- [31] E. Blais. Testing juntas nearly optimally. In *Proceedings of 41st Annual ACM Symposium on Theory of Computing (STOC)*, pages 151–158, 2009.
- [32] E. Blais, J. Brody, and K. Matulef. Property testing lower bounds via communication complexity. *Computational Complexity*, 21(2):311–358, 2012. Earlier version in Complexity’11.
- [33] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993. Earlier version in STOC’90.
- [34] A. Bookatz. QMA-complete problems, 2012. [arXiv:1212.6312](#).
- [35] G. Brassard and P. Høyer. An exact quantum polynomial-time algorithm for Simon’s problem. In *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems (ISTCS’97)*, pages 12–23, 1997. [quant-ph/9704027](#).
- [36] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*, pages 53–74. 2002. [quant-ph/0005055](#).
- [37] S. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Physical Review Letters*, 68(22):3259–3261, 1992.
- [38] S. Bravyi, A. Hassidim, and A. Harrow. Quantum algorithms for testing properties of distributions. *IEEE Transactions on Information Theory*, 57(6):3971–3981, 2011. Earlier version in STACS’10. [arXiv:0907.3920](#).
- [39] T. Brun. Measuring polynomial functions of states. *Quantum Information and Computation*, 4:401, 2004. [quant-ph/0401067](#).
- [40] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 2013. To appear. Preprint at [arXiv:1303.2849](#).
- [41] D. Bruß and C. Macchiavello. Optimal state estimation for  $d$ -dimensional quantum systems. *Physical Review A*, 253(5–6):249–251, 1999. [quant-ph/9812016](#).
- [42] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. [quant-ph/0102001](#).
- [43] H. Buhrman, L. Fortnow, I. Newman, and H. Röhrig. Quantum property testing. *SIAM Journal on Computing*, 37(5):1387–1400, 2008. Earlier version in SODA’03. [quant-ph/0201117](#).
- [44] H. Buhrman, D. García-Soriano, A. Matsliah, and R. de Wolf. The non-adaptive query complexity of testing  $k$ -parities. *Chicago Journal of Theoretical Computer Science*, 6, 2013. [arXiv:1209.3849](#).

- [45] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288(1):21–43, 2002.
- [46] K. Chakraborty and S. Maitra. Improved quantum test for linearity of a Boolean function, 2013. [arXiv:1306.6195](#).
- [47] S. Chakraborty, E. Fischer, A. Matsliah, and R. de Wolf. New results on quantum property testing. In *Proceedings of FSTTCS*, pages 145–156, 2010. [arXiv:1005.0523](#).
- [48] S.-O. Chan, I. Diakonikolas, G. Valiant, and P. Valiant. Optimal algorithms for testing closeness of discrete distributions, 2013. [arXiv:1308.3946](#).
- [49] A. Chefles. Quantum state discrimination. *Contemporary Physics*, 41(6):401–424, 2001. [quant-ph/0010114](#).
- [50] A. Childs, A. Harrow, and P. Wocjan. Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem. In *Proceedings of 24th Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 598–609, 2007. [quant-ph/0609110](#).
- [51] H. Chockler and D. Gutfreund. A lower bound for testing juntas. *Information Processing Letters*, 90(6):301–305, 2004.
- [52] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975.
- [53] M. Christandl. *The Structure of Bipartite Quantum States – Insights from Group Theory and Cryptography*. PhD thesis, University of Cambridge, 2006. [quant-ph/0604183](#).
- [54] B. S. Cirel’son. Quantum generalizations of Bell’s inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.
- [55] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.
- [56] R. Colbeck. *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge, 2006. [arXiv:0911.3814](#).
- [57] M. Cramer, M. Plenio, S. Flammia, R. Somma, D. Gross, S. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu. Efficient quantum state tomography. *Nature Communications*, 1(9):49, 2010. [arXiv:1101.4366](#).
- [58] M. da Silva, O. Landon-Cardinal, and D. Poulin. Practical characterization of quantum devices without tomography. *Physical Review Letters*, 107:210404, 2011. [arXiv:1104.3835](#).
- [59] W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM Journal on Computing*, 37(2):611–629, 2007. Earlier version in STOC’00. [quant-ph/9904108](#).
- [60] A. Dasgupta, R. Kumar, and D. Sivakumar. Sparse and lopsided set disjointness via information theory. In *Proceedings of 16th RAN-DOM*, pages 517–528, 2012.
- [61] R. Duan, Y. Feng, and M. Ying. Perfect distinguishability of quantum operations. *Physical Review Letters*, 103:210501, 2009. [arXiv:0908.0119](#).
- [62] E. Fischer. The art of uninformed decisions. *Bulletin of the EATCS*, 75:97, 2001.
- [63] E. Fischer, G. Kindler, D. Ron, S. Safra, and A. Samorodnitsky. Testing juntas. *Journal of Computer and System Sciences*, 68(4):753–787, 2004. Earlier version in FOCS’02.
- [64] S. Flammia, D. Gross, Y.-K. Liu, and J. Eisert. Quantum tomography via compressed sensing: Error bounds, sample complexity, and efficient estimators. *New Journal of Physics*, 14:095022, 2012. [arXiv:1205.2300](#).
- [65] S. Flammia and Y.-K. Liu. Direct fidelity estimation from few Pauli measurements. *Physical Review Letters*, 106:230501, 2011. [arXiv:1104.4695](#).
- [66] K. Friedl, G. Ivanyos, and M. Santha. Efficient testing of groups. In *Proceedings of 37th Annual ACM Symposium on Theory of Computing (STOC)*, pages 157–166, 2005.
- [67] K. Friedl, F. Magniez, M. Santha, and P. Sen. Quantum testers for hidden group properties. *Fundamenta Informaticae*, 91(2):325–340, 2009. Earlier version in MFCS’03.
- [68] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information and Computation*, 10(3&4):343–360, 2010. [arXiv:0810.4507](#).
- [69] L. Glebsky. Almost commuting matrices with respect to normalized Hilbert-Schmidt norm, 2010. [arXiv:1002.3082](#).

- [70] O. Goldreich, editor. *Property Testing: Current Research and Surveys*, volume 6390 of *Lecture Notes in Computer Science*. Springer, 2010.
- [71] O. Goldreich, S. Goldwasser, and D. Ron. Property testing and its connection to learning and approximation. *Journal of the ACM*, 45(4):653–750, 1998.
- [72] O. Goldreich and D. Ron. On testing expansion in bounded-degree graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 7(20), 2000.
- [73] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, Caltech, 1999. [quant-ph/9705052](#).
- [74] D. Greenberger, M. Horne, and A. Zeilinger. Going beyond Bell’s theorem. In M. Kafatos, editor, *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, pages 69–72. Kluwer, 1989. [arXiv:0712.0921](#).
- [75] D. Gross, Y.-K. Liu, S. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Physical Review Letters*, 105:150401, 2010. [arXiv:0909.3304](#).
- [76] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219, 1996. [quant-ph/9605043](#).
- [77] O. Gühne and G. Toth. Entanglement detection. *Physics Reports*, 471(1), 2009.
- [78] L. Gurvits. Classical deterministic complexity of Edmonds’ problem and quantum entanglement. In *Proceedings of 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 10–19, 2003. [quant-ph/0303055](#).
- [79] H. Häffner, W. Hänsel, C. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. Rapol, M. Riebe, P. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt. Scalable multiparticle entanglement of trapped ions. *Nature*, 438:643–646, 2005. [quant-ph/0603217](#).
- [80] L. Hales. *The Quantum Fourier Transform and Extensions of the Abelian Hidden Subgroup Problem*. PhD thesis, University of California, Berkeley, 2002. [quant-ph/0212002](#).
- [81] L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applications. In *Proceedings of 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 515–525, 2000.
- [82] A. Harrow. *Applications of coherent classical communication and the Schur transform to quantum information theory*. PhD thesis, Massachusetts Institute of Technology, 2005. [quant-ph/0512255](#).
- [83] A. Harrow and A. Montanaro. Testing product states, quantum Merlin-Arthur games and tensor optimization. *Journal of the ACM*, 60(1), 2013. Earlier version in FOCS’10. [arXiv:1001.0017](#).
- [84] P. Hayden, D. Leung, and A. Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265(1):95–117, 2006. [quant-ph/0407049](#).
- [85] P. Hayden, K. Milner, and M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. In *Proceedings of 28th Annual IEEE Conference on Computational Complexity (CCC)*, pages 156–167, 2012. [arXiv:1211.6120](#).
- [86] C. W. Helstrom. *Quantum detection and estimation theory*. Academic Press, New York, 1976.
- [87] M. Hillery and E. Andersson. Quantum tests for the linearity and permutation invariance of Boolean functions. *Physical Review A*, 84:062329, 2011. [arXiv:1106.4831](#).
- [88] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation *Problems of Information Transmission*, vol. 9, pp. 177–183, 1973.
- [89] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulletin of the AMS*, 43:439–561, 2006.
- [90] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, 2009. [quant-ph/0702225](#).
- [91] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proceedings of 39th Annual ACM Symposium on Theory of Computing (STOC)*, pages 526–535, 2007. [quant-ph/0611054](#).
- [92] Y. Inui and F. Le Gall. Quantum property testing of group solvability. In *Proceedings of 8th Latin American Theoretical Informatics conference (LATIN)*, pages 772–783, 2008.

- [93] T. Ito and T. Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. In *Proceedings of 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 243–252, 2012. [arXiv:1207.0550](#).
- [94] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP=PSPACE. *Journal of the ACM*, 58(6):30, 2011. Earlier version in STOC’10. [arXiv:0907.4737](#).
- [95] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.
- [96] D. Janzing, P. Wocjan, and T. Beth. Non-identity check is QMA-complete. *International Journal of Quantum Information*, 3:463, 2005. [quant-ph/0305050](#).
- [97] M. Kada, H. Nishimura, and T. Yamakami. The efficiency of quantum identity testing of multiple states. *Journal of Physics A: Mathematical and Theoretical*, 41:395309, 2008. [arXiv:0809.2037](#).
- [98] D. Kane and S. Kutin. Quantum interpolation of polynomials, 2009. [arXiv:0909.5683](#).
- [99] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006. [quant-ph/0406180](#).
- [100] M. Keyl and R. Werner. Estimating the spectrum of a density operator. *Physical Review A*, 64(5):052311, 2001. [quant-ph/0102027](#).
- [101] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. AMS, 2002.
- [102] A. Yu Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 608–617, 2000.
- [103] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009. Earlier version in ISAAC’03. [quant-ph/0306051](#).
- [104] P. Koiran, V. Nesme, and N. Portier. A quantum lower bound for the query complexity of Simon’s problem. In *Proceedings of 32nd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 1287–1298, 2005. [quant-ph/0501060](#).
- [105] R. Krauthgamer and O. Sasson. Property testing of data dimensionality. In *Proceedings of 14th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 18–27, 2003.
- [106] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.
- [107] O. Lachish and I. Newman. Testing periodicity. *Algorithmica*, 60(2):401–420, 2011. Earlier version in RANDOM’05.
- [108] F. Le Gall and Y. Yoshida. Property testing for cyclic groups and beyond. In *Proceedings of 17th Computing and Combinatorics conference (COCOON)*, pages 432–443, 2011. [arXiv:1105.1842](#).
- [109] T. Lee, R. Mittal, B. Reichardt, R. Špalek, and M. Szegedy. Quantum query complexity of state conversion. In *Proceedings of 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 344–353, 2011. [arXiv:1011.3020](#).
- [110] R. Low. Learning and testing algorithms for the Clifford group. *Physical Review A*, 80:052314, 2009. [arXiv:0907.2833](#).
- [111] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1983.
- [112] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In *Proceedings of 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 4051 of *Lecture Notes in Computer Science*, pages 72–83, 2006. [quant-ph/0512111](#).
- [113] K. Majewski and N. Pippenger. Attribute estimation and testing quasi-symmetry. *Information Processing Letters*, 109(4):233–237, 2007. [arXiv:0708.2105](#).
- [114] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 503–509, 1998. [quant-ph/9809039](#).

- [115] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Information and Computation*, 4(4):273–286, 2004. [quant-ph/0307205](#).
- [116] M. McKague. Self-testing graph states. In *Proceedings of 6th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC)*, 2011. [arXiv:1010.1989](#).
- [117] M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(455304), 2012. [arXiv:1203.2976](#).
- [118] C. Miller and Y. Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. [arXiv:1207.1819](#), 2012.
- [119] K. Milner, G. Gutoski, P. Hayden, and M. Wilde. Quantum interactive proofs and the complexity of entanglement detection, 2013. [arXiv:1308.5788](#).
- [120] F. Mintert, M. Kuś, and A. Buchleitner. Concurrence of mixed multipartite quantum states. *Physical Review Letters*, 95(26):260502, 2005. [quant-ph/0411127](#).
- [121] A. Montanaro. Symmetric functions of qubits in an unknown basis. *Physical Review A*, 79(6):062316, 2009. [arXiv:0903.5466](#).
- [122] A. Montanaro and T. Osborne. Quantum boolean functions. *Chicago Journal of Theoretical Computer Science*, 1, 2010. [arXiv:0810.2435](#).
- [123] M. Nielsen. Continuity bounds for entanglement. *Physical Review A*, 61(6):064301, 2000. [quant-ph/9908086](#).
- [124] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [125] R. O’Donnell. Some topics in analysis of boolean functions. Technical report, ECCC Report TR08–055, 2008. Paper for an invited talk at STOC’08.
- [126] T. Ogawa and H. Nagaoka. A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In *Proceedings of 2002 IEEE International Symposium on Information Theory*, page 73, 2002. [quant-ph/0208139](#).
- [127] M. Paris and J. Řeháček (eds.). *Quantum State Estimation*, volume 649 of *Lecture Notes in Physics*. Springer-Verlag, 2004.
- [128] D. Pérez-García, F. Verstraete, M. Wolf, and J. Cirac. Matrix product state representations. *Quantum Information and Computation*, 7:401, 2007. [quant-ph/0608197](#).
- [129] M. Piani and J. Watrous. All entangled states are useful for channel discrimination. *Physical Review Letters*, 102:250501, 2009. [arXiv:0901.2118](#).
- [130] S. Popescu and D. Rohrlich. Which states violate Bell’s inequality maximally? *Physics Letters A*, 166:411–414, 1992.
- [131] R. Raussendorf, D. Browne, and H. Briegel. Measurement-based quantum computation with cluster states. *Physical Review A*, 68:022312, 2003. [quant-ph/0301052](#).
- [132] B. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proceedings of 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 544–551, 2009.
- [133] B. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, 2013. [arXiv:1209.0448](#) and [arXiv:1209.0449](#).
- [134] D. Ron. Property testing: A learning theory perspective. *Foundations and Trends in Machine Learning*, 1(3):307–402, 2008.
- [135] W. Rosgen. Distinguishing short quantum computations. In *Proceedings of 25th Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 597–608, 2008. [arXiv:0712.2595](#).
- [136] W. Rosgen. Computational distinguishability of degradable and antidegradable channels. *Quantum Information and Computation*, 10:735–746, 2010. [arXiv:0911.2109](#).
- [137] W. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of 20th Annual IEEE Conference on Computational Complexity (CCC)*, pages 344–354, 2005. [cs/0407056](#).
- [138] M. Sacchi. Optimal discrimination of quantum operations. *Physical Review A*, 71:062340, 2005. [quant-ph/0505183](#).
- [139] M. Santha. Quantum walk based search algorithms. In *Proceedings of 5th conference on Theory and Applications of Models of Computation (TAMC)*, pages 31–46, 2008. [arXiv:0808.0059](#).



- [140] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. Earlier version in FOCS’94. [quant-ph/9508027](#).
- [141] D. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. Earlier version in FOCS’94.
- [142] S. Summers and R. Werner. Maximal violation of Bell’s inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987.
- [143] B. S. Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993. Available at <http://www.tau.ac.il/~tsirel/download/hadron.pdf>.
- [144] P. Valiant. Testing symmetric properties of distributions. *SIAM Journal on Computing*, 40(6):1927–1968, 2011.
- [145] U. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of 44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 61–76, 2012. [arXiv:1111.6054](#).
- [146] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. [arXiv:1210.1810](#), 2012.
- [147] G. Wang. Property testing of unitary operators. *Physical Review A*, 84:052328, 2011. [arXiv:1110.1133](#).
- [148] G. Wang. Property testing of quantum measurements, 2012. [arXiv:1205.0828](#).
- [149] J. Watrous. *Theory of Quantum Information* lecture notes, 2008. <http://www.cs.uwaterloo.ca/~watrous/quant-info/>.
- [150] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999.
- [151] R. de Wolf. A brief introduction to Fourier analysis on the Boolean cube. *Theory of Computing*, 2008. ToC Library, Graduate Surveys 1.
- [152] T. H. Yang and M. Navascués. Robust self testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87(5):050102(R), 2013. [arXiv:1210.4409](#).
- [153] T. H. Yang, T. Vértesi, J-D. Bancal, V. Scarani, and M. Navascués. Opening the black box: how to estimate physical properties from non-local correlations, 26 Jul 2013. [arXiv:1307.7053](#).
- [154] A. C-C. Yao. Some complexity questions related to distributive computing. In *Proceedings of 11th Annual ACM Symposium on Theory of Computing (STOC)*, pages 209–213, 1979.