An efficient test for product states

Aram W. Harrow* and Ashley Montanaro†

January 4, 2010

Abstract

We give a test that can distinguish efficiently between product states of n quantum systems and states which are far from product. If applied to a state $|\psi\rangle$ whose maximum overlap with a product state is $1-\epsilon$, the test passes with probability $1-\Theta(\epsilon)$, regardless of n or the local dimensions of the individual systems. The test uses two copies of $|\psi\rangle$. We prove correctness of this test as a special case of a more general result regarding stability of maximum output purity of the depolarising channel.

One application of the test is to Quantum Merlin-Arthur games, where we show that a witness from two unentangled provers can simulate a witness from arbitrarily many unentangled provers, up to a constant loss of soundness. Our test can also be used to construct an efficient test for determining whether a unitary operator is a tensor product.

1 Introduction

Entanglement of quantum states presents both an opportunity and a difficulty for quantum computing. To describe a pure state of n qudits (d-dimensional quantum systems) requires a comparable number of parameters to a classical probability distribution on d^n items. However, being a pure state means that many tools available to handle probability distributions no longer work. For example, due to interference, the probability of a test passing cannot be simply written as an average over components of the state. Moreover, measuring one part of a state may induce entanglement between other parts of the state that were not previously entangled with each other.

These counter-intuitive properties of entanglement account for many of the main outstanding puzzles in quantum information. In quantum channel coding, the famous additivity violations of [10, 15] reflect how entangled inputs can sometimes have advantages against even uncorrelated noise. For quantum interactive proofs, the primary difficulty is in bounding the ability of provers to cheat using entangled strategies [16]. Even for QMA(k) (the variant of QMA with k unentangled Merlins [18, 2]), most important open questions could be resolved by finding a way to control entanglement within each proof. Here, the recently discovered failure of parallel repetition for entangled provers [17] is a sort of complexity-theoretic analogue of additivity violations.

The situation is different when we consider quantum states that are *product* across the n systems. In this case, while individual systems of course behave quantumly, the lack of correlation between

*Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, UK; a.harrow@bris.ac.uk.

†Department of Computer Science, University of Bristol, Woodland Road, Bristol, BS8 1UB, UK; montanar@cs.bris.ac.uk.

the systems means that classical tools such as Chernoff bounds can be used. For example, in channel coding with product-state inputs, not only does the single-letter Holevo formula give the capacity, so that there is no additivity problem, but so-called strong converse theorems are known proving that attempting to communicate at a rate above the capacity results in an exponentially decreasing probability of successfully transmitting a message [22, 26]. Naturally, many of the difficulties in dealing with entangled proofs and quantum parallel repetition would also go away if quantum states were constrained to be in product form.

In this paper, we present a quantum test to determine whether an n-partite state $|\psi\rangle$ is a product state or far from any product state. We make no assumptions about the local dimensions of $|\psi\rangle$; in fact, the local dimension can even be different for different systems. The test passes with certainty if $|\psi\rangle$ is product, and fails with probability $\Theta(\epsilon)$ if the overlap between $|\psi\rangle$ and the closest product state is $1-\epsilon$. An essential feature of our test (or any possible such test, as we will argue in Section 3.3) is that it requires two copies of $|\psi\rangle$.

The parameters of our test resemble classical *property testing* algorithms [11]. In general, these algorithms make a small number of queries to some object and accept with high probability if the object has some property P (*completeness*), and with low probability if the object is "far" from having property P (*soundness*). Crucially, the number of queries used and the success probability should not depend on the size of the object. The main result of this paper is a test for a property of a quantum state, in contrast to previous work on quantum generalisations of property testing, which has considered quantum algorithms for testing properties of classical (e.g. [9, 4]) and quantum [20] oracles (a.k.a. unitary operators, although see Section 3.2 for an application to this setting). In this sense, our work is closer to a body of research on determining properties of quantum states directly, without performing full tomography (e.g. the "pretty good tomography" of Aaronson [1]). The direct detection of quantities relating to entanglement has received particular attention; see [14] for an extensive review. However, previous work has generally focused on Bell inequalities and entanglement witnesses, which are typically designed to distinguish a *particular* entangled state from any separable state. By contrast, our product test is generic and will detect entanglement in any entangled state $|\psi\rangle$.

The product test is defined in Definition 1 below, and illustrated schematically in Figure 1. It uses as a subroutine the *swap test* for comparing quantum states [8]. This test, which can be implemented efficiently, takes two (possibly mixed) states ρ, σ of equal dimension as input, and returns "same" with probability $\frac{1}{2}+\frac{1}{2}\operatorname{tr}\rho\,\sigma$, otherwise returning "different".

Definition 1 (Product test).

The product test proceeds as follows.

1. *Prepare two copies of* $|\psi\rangle \in \mathbb{C}^{d_1}\otimes\cdots\otimes\mathbb{C}^{d_n}$*; call these* $|\psi_1\rangle$, $|\psi_2\rangle$.
2. *Perform the swap test on each of the* n *pairs of corresponding subsystems of* $|\psi_1\rangle$, $|\psi_2\rangle$.
3. *If all of the tests returned "same", accept. Otherwise, reject.*

In fact, the product test has appeared before in the literature. It was originally introduced in [19] as one of a family of tests for generalisations of the concurrence entanglement measure, and

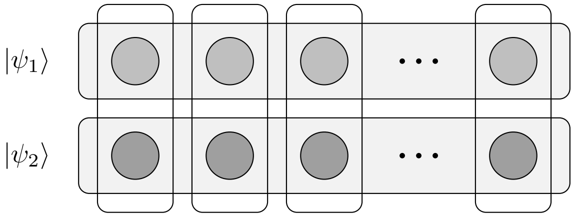

Figure 1: Schematic of the product test applied to an n qudit state $|\psi\rangle$. The swap test (vertical boxes) is applied to the n pairs of corresponding subsystems of two copies of $|\psi\rangle$ (horizontal boxes).

has been implemented experimentally as a means of detecting bipartite entanglement directly [24]. Further, the test was proposed in [20] as a means of determining whether a unitary operator is product. Our contribution here is to prove the correctness of this test for all n. Indeed, we have the following result.

Theorem 1. *Given $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, let*

$$1 - \epsilon = \max\{|\langle\psi|\phi_1, \dots, \phi_n\rangle|^2 : |\phi_i\rangle \in \mathbb{C}^{d_i}, i \leq 1 \leq n\}.$$

Let $P_{test}(|\psi\rangle\langle\psi|)$ be the probability that the product test passes when applied to $|\psi\rangle$. Then

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

Furthermore, if $\epsilon \geq 11/32 > 0.343$, $P_{test}(|\psi\rangle\langle\psi|) \leq 501/512 < 0.979$.

More concisely, $P_{test}(|\psi\rangle\langle\psi|) = 1 - \Theta(\epsilon)$.

The proof is based on relating the probability of the test passing to the action of the qudit depolarising channel. In fact, we prove a considerably more general result regarding this channel. It is known [3] that the maximum output purity of this channel is achieved for product state inputs; our result, informally, says that any state that is "close" to achieving maximum output purity must in fact be "close" to a product state. This is a *stability* result for this channel.

Somewhat more formally, let $\mathcal{D}_\delta$ be the d-dimensional qudit depolarising channel with noise rate $1 - \delta$, i.e.

$$\mathcal{D}_\delta(\rho) = (1 - \delta)(\operatorname{tr}\rho)\frac{I}{d} + \delta\,\rho \tag{1}$$

for ρ a arbitrary mixed state of one d-dimensional system, and define the product state output purity to be

$$P_{prod}(\delta) = \operatorname{tr}(\mathcal{D}_\delta^{\otimes n}\,|\phi\rangle\langle\phi|)^2,$$

where $|\phi\rangle$ is an arbitrary product state. Then our main result, stated formally as Theorem 3 in Section 2 below, is that for constant $0 < \delta < 1$, if

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}\,|\psi\rangle\langle\psi|)^2 \geq (1 - \epsilon)P_{prod}(\delta),$$

then there is a product state $|\phi_1, \dots, \phi_n\rangle$ such that $|\langle\psi|\phi_1, \dots, \phi_n\rangle|^2 \geq 1 - O(\epsilon)$.

We give two applications of the product test. First, the test can be used to determine whether a unitary operator is a tensor product. This can be seen [20] as one possible generalisation of the well-studied problem of testing whether a boolean function $\{0,1\}^n \rightarrow \{0,1\}$ is linear [7]. This application is described in Section 3.2.

Second, the product test can be used to relate QMA(k) to QMA(2), as we will discuss in Section 4. The complexity class QMA(k) is defined to be the class of languages that can be decided with bounded error by a poly-time quantum verifier that receives poly-size witnesses from k unentangled provers [18, 2]. To put QMA(k) inside QMA(2) with constant loss of soundness, we can have two provers simulate k provers by each submitting k unentangled proofs, whose lack of entanglement can be verified with our product test. Indeed, this gives an alternate way to understand our test as a way of using bipartite separability to certify k-partite separability. As a result, we can improve upon the results of [1, 6] to obtain a protocol in QMA(2) that verifies 3-SAT with constant soundness gap and $O(\sqrt{n}\operatorname{poly}\log(n))$ qubits (where n is the number of clauses).

These different applications of the product test reflect the many different interpretations of $P_{test}(|\psi\rangle\langle\psi|)$. It is related to

- The purity of $|\psi\rangle$ after it is subjected to independent depolarising noise (in Section 2).
- The maximum overlap of $|\psi\rangle$ with any product state (proved in Section 3). The logarithm of this maximum overlap is known as the geometric measure of entanglement (see [25] and references therein).
- The overlap of $|\psi\rangle^{\otimes 2}$ with the tensor product of the symmetric subspaces of $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1} \dots \mathbb{C}^{d_n} \otimes \mathbb{C}^{d_n}$ (discussed in Section 3.3).
- The average overlap of $|\psi\rangle$ with a *random* product state (discussed in Section 5).
- The average purity of $|\psi\rangle$ across a random partition of $[n]$ into two subsets (also discussed in Section 5).

In the remainder of the paper, we deal with proving all these results, starting with the connection to the depolarising channel.

2 The depolarising channel

Let $\mathcal{D}_\delta$ be the qudit depolarising channel as defined in (1). We will be interested in applying the n-fold product $\mathcal{D}_\delta^{\otimes n}$ to states of n qudits, and in particular in the purity of the resulting states. This has the following characterisation.

Lemma 2. *We have*

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}\,\rho)^2 = \left(\frac{1-\delta^2}{d}\right)^n \sum_{S\subseteq[n]} \left(\frac{d\delta^2}{1-\delta^2}\right)^{|S|} \operatorname{tr}(\rho_S^2),$$

and in particular

$$\operatorname{tr}(\mathcal{D}_{1/\sqrt{d+1}}^{\otimes n}\,\rho)^2 = \frac{1}{(d+1)^n} \sum_{S\subseteq[n]} \operatorname{tr}(\rho_S^2),$$

and for pure product states,

$$P_{prod}(\delta) := \operatorname{tr}(\mathcal{D}_\delta^{\otimes n}\,(|\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_n\rangle\langle\psi_n|))^2 = \left(\frac{d-1}{d}\delta^2 + \frac{1}{d}\right)^n.$$

Proof. Consider some Hermitian operator basis for $\mathcal{B}(\mathbb{C}^d)$ which contains the identity and is orthonormal with respect to the normalised Hilbert-Schmidt inner product $\langle A, B\rangle = \frac{1}{d}\operatorname{tr} A^\dagger B$, and extend this basis to $\mathcal{B}((\mathbb{C}^d)^{\otimes n})$ by tensoring. Expand ρ in terms of the resulting basis as

$$\rho = \sum_{\mathbf{t}\in\{0,\dots,d^2-1\}^n} \hat{\rho}_{\mathbf{t}} \chi_{\mathbf{t}}.$$

where $\hat{\rho}_{\mathbf{t}} \in \mathbb{R}$, $\chi_{\mathbf{t}}$ represents an element of the tensor product basis corresponding to the string $\mathbf{t} \in \{0,\dots,d^2-1\}^n$, and the identity is indexed by 0 at each position. Then we have

$$\operatorname{tr}(\rho_S^2) = d^{2n-|S|}\left(\sum_{\mathbf{t},\,\mathbf{t}_i=0,\,\forall i\in\bar{S}} \hat{\rho}_{\mathbf{t}}^2\right),$$

and hence, for any δ,

$$\begin{aligned}
\sum_{S\subseteq[n]} \delta^{|S|}\operatorname{tr}(\rho_S^2) &= d^{2n}\sum_{S\subseteq[n]}(\delta/d)^{|S|}\left(\sum_{\mathbf{t},\,\mathbf{t}_i=0,\,\forall i\in\bar{S}}\hat{\rho}_{\mathbf{t}}^2\right) = d^{2n}\sum_{\mathbf{t}}\hat{\rho}_{\mathbf{t}}^2\left(\sum_{\substack{S\subseteq[n],\\ \mathbf{t}_i=0,\,\forall i\in\bar{S}}}(\delta/d)^{|S|}\right)\\
&= d^{2n}\sum_{\mathbf{t}}\hat{\rho}_{\mathbf{t}}^2\left(\sum_{x=0}^{n-|\mathbf{t}|}\binom{n-|\mathbf{t}|}{x}(\delta/d)^{x+|\mathbf{t}|}\right)\\
&= d^{2n}\sum_{\mathbf{t}}\hat{\rho}_{\mathbf{t}}^2\,(\delta/d)^{|\mathbf{t}|}(1+\delta/d)^{n-|\mathbf{t}|}\\
&= (d(d+\delta))^n\sum_{\mathbf{t}}\hat{\rho}_{\mathbf{t}}^2\,(\delta/(\delta+d))^{|\mathbf{t}|}\\
&= (d+\delta)^n\operatorname{tr}(\mathcal{D}^{\otimes n}_{\sqrt{\delta/(\delta+d)}}\rho)^2.
\end{aligned}$$

Rearranging completes the proof; the two special cases in the statement of the lemma can be verified directly. □

Using the above lemma, it is easy to see that maximal output purity is obtained only for product states. We will now prove our main result, which is a "stability" theorem for the depolarising channel: if a state achieves close to maximal output purity, it must be close to a product state.

Theorem 3. *Given $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$, let*

$$1-\epsilon = \max\{|\langle\psi|\phi_1,\dots,\phi_n\rangle|^2 : |\phi_1\rangle,\dots,|\phi_n\rangle \in \mathbb{C}^d\}. \tag{2}$$

Then

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}|\psi\rangle\langle\psi|)^2 \le P_{prod}(\delta)\left(1-4\epsilon(1-\epsilon)\frac{d\delta^2(1-\delta^2)}{(1+(d-1)\delta^2)^2} + 4\epsilon^{3/2}\left(\frac{(1-\delta^2)^2+d^2\delta^4}{(1+(d-1)\delta^2)^2}\right)^2\right).$$

In particular,

$$\operatorname{tr}(\mathcal{D}^{\otimes n}_{1/\sqrt{d+1}}|\psi\rangle\langle\psi|)^2 \le P_{prod}(1/\sqrt{d+1})\left(1-\epsilon+\epsilon^2+\epsilon^{3/2}\right).$$

Proof. Without loss of generality assume that one of the states achieving the maximum in Eq. (2) is $|0\rangle^{\otimes n}$, which we will abbreviate simply as $|0^n\rangle$, or $|0\rangle$ when there is no ambiguity. We thus have

$$|\psi\rangle = \sqrt{1-\epsilon}|0\rangle + \sqrt{\epsilon}|\phi\rangle$$

for some state $|\phi\rangle$ such that $\langle 0|\phi\rangle = 0$, and $|\phi\rangle = \sum_{x \neq 0} \alpha_x |x\rangle$ for some $\{\alpha_x\}$. We write down explicitly

$$\psi := |\psi\rangle\langle\psi| = (1-\epsilon)|0\rangle\langle 0| + \sqrt{\epsilon(1-\epsilon)}(|0\rangle\langle\phi| + |\phi\rangle\langle 0|) + \epsilon|\phi\rangle\langle\phi|.$$

By Lemma 2,

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}\,\psi)^2 = \left(\frac{1-\delta^2}{d}\right)^n \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr} \psi_S^2,$$

where we set $\gamma = d\delta^2/(1-\delta^2)$ for brevity. Now

$$\sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr} \psi_S^2 = \sum_{S \subseteq [n]} \gamma^{|S|} \left(\operatorname{tr}((1-\epsilon)|0\rangle\langle 0|_S + \sqrt{\epsilon(1-\epsilon)}(|0\rangle\langle\phi|_S + |\phi\rangle\langle 0|_S) + \epsilon|\phi\rangle\langle\phi|_S)^2 \right),$$

and for any subset S,

$$\begin{aligned} \operatorname{tr} \psi_S^2 &= (1-\epsilon)^2 \operatorname{tr} |0\rangle\langle 0|_S^2 + \epsilon(1-\epsilon) \operatorname{tr}(|0\rangle\langle\phi| + |\phi\rangle\langle 0|)_S^2 + \epsilon^2 \operatorname{tr} |\phi\rangle\langle\phi|_S^2 \\ &+ 2\sqrt{\epsilon}(1-\epsilon)^{3/2} \operatorname{tr} |0\rangle\langle 0|_S (|0\rangle\langle\phi| + |\phi\rangle\langle 0|)_S + 2\epsilon(1-\epsilon) \operatorname{tr} |0\rangle\langle 0|_S |\phi\rangle\langle\phi|_S \\ &+ 2\epsilon^{3/2}\sqrt{1-\epsilon} \operatorname{tr} |\phi\rangle\langle\phi|_S (|0\rangle\langle\phi| + |\phi\rangle\langle 0|)_S. \end{aligned}$$

We now bound the sum over S (weighted by $\gamma^{|S|}$) of each of these terms, in order. Note that we repeatedly use the notation $[E]$ for a term which evaluates to 1 if the expression E is true, and 0 if E is false.

1. As $|0\rangle$ is product, clearly

$$\sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr} |0\rangle\langle 0|_S^2 = \sum_{S \subseteq [n]} \gamma^{|S|} = (1+\gamma)^n.$$

2. We have

$$\operatorname{tr}(|0\rangle\langle\phi| + |\phi\rangle\langle 0|)_S^2 = \operatorname{tr} |0\rangle\langle\phi|_S^2 + \operatorname{tr} |\phi\rangle\langle 0|_S^2 + 2 \operatorname{tr} |0\rangle\langle\phi|_S |\phi\rangle\langle 0|_S.$$

   It is easy to see that the first two terms must be 0 for all S (as only the off-diagonal entries of the first row of the matrix $|0\rangle\langle\phi|$ can be non-zero). For the third, we explicitly calculate

$$|0\rangle\langle\phi|_S |\phi\rangle\langle 0|_S = \sum_{x \neq 0} |\alpha_x|^2 [x_i = 0, \forall i \in \bar{S}] |0\rangle\langle 0|^{\otimes k},$$

   and hence

$$\begin{aligned} \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr} |0\rangle\langle\phi|_S |\phi\rangle\langle 0|_S &= \sum_{x \neq 0} |\alpha_x|^2 \sum_{S \subseteq [n]} \gamma^{|S|} [x_i = 0, \forall i \in \bar{S}] \\ &= \sum_{x \neq 0} |\alpha_x|^2 \sum_{k=|x|}^{n} \gamma^k \binom{n-|x|}{n-k} \\ &= (1+\gamma)^n \sum_{x \neq 0} |\alpha_x|^2 \left(\frac{\gamma}{1+\gamma}\right)^{|x|}. \end{aligned}$$

3. It clearly holds that $\operatorname{tr}|\phi\rangle\langle\phi|_S^2 \le 1$, so as in part (1),

$$\sum_{S\subseteq[n]} \gamma^{|S|} \operatorname{tr}|\phi\rangle\langle\phi|_S^2 \le (1+\gamma)^n,$$

and this will be tight if and only if $|\phi\rangle$ is product itself.

4. Using the same argument as in part (2), $\operatorname{tr}|0\rangle\langle 0|_S|0\rangle\langle\phi|_S = \operatorname{tr}|0\rangle\langle 0|_S|\phi\rangle\langle 0|_S = 0$.

5. Write the state $\phi = |\phi\rangle\langle\phi|$ as

$$\phi = \sum_{x,y} \phi_{x_1,\dots,y_n}|x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|.$$

Then, for any $S = \{i_1,\dots,i_k\}$,

$$\phi_S = \sum_{x,y}[x_i = y_i, \forall i \in \bar{S}]\phi_{x_1,\dots,y_n}|x_{i_1}\rangle\langle y_{i_1}| \otimes \cdots \otimes |x_{i_k}\rangle\langle y_{i_k}|,$$

which implies

$$\operatorname{tr}|0\rangle\langle 0|_S|\phi\rangle\langle\phi|_S = \sum_x [x_i = 0, \forall i \in S]|\alpha_x|^2,$$

and hence, similarly to part (2),

$$\sum_{S\subseteq[n]} \gamma^{|S|} \operatorname{tr}|0\rangle\langle 0|_S|\phi\rangle\langle\phi|_S = \sum_{k=0}^{n-|x|} \gamma^k \binom{n-|x|}{k} = (1+\gamma)^n \sum_{x\neq 0} |\alpha_x|^2 \left(\frac{1}{1+\gamma}\right)^{|x|}.$$

6. The last term can be trivially bounded using

$$|\operatorname{tr}|\phi\rangle\langle\phi|_S(|0\rangle\langle\phi| + |\phi\rangle\langle 0|)_S| \le 2.$$

However, it is possible to get a better bound with a bit more work. We expand

$$\begin{aligned}
&\sum_{S\subseteq[n]} \gamma^{|S|} \operatorname{tr}|\phi\rangle\langle\phi|_S|0\rangle\langle\phi|_S = \\
&\sum_{S\subseteq[n]} \gamma^{|S|} \sum_{x,y,z} \alpha_x\alpha_y^*\alpha_z^*[z_i = 0, i \in \bar{S}][x_i = y_i, i \in \bar{S}] \operatorname{tr}|x_1\rangle\langle y_1|0\rangle\langle z_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|0\rangle\langle z_n| \\
&\qquad = \sum_{S\subseteq[n]} \gamma^{|S|} \sum_{x,y,z} \alpha_x\alpha_y^*\alpha_z^*[z_i = 0, i \in \bar{S}][x_i = y_i, i \in \bar{S}][y_i = 0, i \in S][x_i = z_i, i \in S] \\
&\qquad = \sum_{|y\wedge z|=0} \alpha_{y\vee z}\alpha_y^*\alpha_z^* \sum_{S\subseteq[n]} \gamma^{|S|}[y_i = 0, i \in S][z_i = 0, i \in \bar{S}] \\
&\qquad = \sum_{|y\wedge z|=0} \alpha_{y\vee z}\alpha_y^*\alpha_z^* \gamma^{|z|}(1+\gamma)^{n-|y|-|z|}.
\end{aligned}$$

This expression can be upper bounded as follows:

$$\begin{aligned}
\sum_{|y\wedge z|=0} \alpha_{y\vee z}\alpha_y^*\alpha_z^*\gamma^{|z|}(1+\gamma)^{-(|y|+|z|)} &\le \sqrt{\sum_{|y\wedge z|=0}|\alpha_y|^2|\alpha_z|^2}\sqrt{\sum_{|y\wedge z|=0}\frac{\gamma^{2|z|}}{(1+\gamma)^{2|y\vee z|}}|\alpha_{y\vee z}|^2}\\
&\le \left(\sum_x (1+\gamma)^{-2|x|}|\alpha_x|^2\left(\sum_{|y\wedge z|=0}\gamma^{2|z|}[y\vee z=x]\right)\right)^{1/2}\\
&= \left(\sum_x\left(\frac{1+\gamma^2}{(1+\gamma)^2}\right)^{|x|}|\alpha_x|^2\right)^{1/2}.
\end{aligned}$$

Combining these terms, we have

$$\sum_{S\subseteq[n]}\gamma^{|S|}\operatorname{tr}\psi_S^2 \le (1+\gamma)^n((1-\epsilon)^2+2\epsilon(1-\epsilon)\sum_{x\neq 0}|\alpha_x|^2(1+\gamma)^{-|x|}(\gamma^{|x|}+1)+\epsilon^2+$$
$$4\epsilon^{3/2}\sqrt{1-\epsilon}\left(\sum_x\left(\frac{1+\gamma^2}{(1+\gamma)^2}\right)^{|x|}|\alpha_x|^2\right)^{1/2}).$$

Note that $(1+\gamma)^{-|x|}(\gamma^{|x|}+1)$ decreases with $|x|$ for all $\gamma>0$, as does $(1+\gamma^2)^{|x|}(1+\gamma)^{-2|x|}$. To complete the proof, we will show that $|\phi\rangle$ has no weight 1 components (i.e. $\alpha_x=0$ for $|x|<2$). In the contribution from Eq. (3), this implies that only the $|x|\ge 4$ terms contribute (since $x=y\vee z$ and $y\wedge z=\emptyset$). Therefore, $|\phi\rangle$ having no weight 1 components would imply that

$$\sum_{S\subseteq[n]}\gamma^{|S|}\operatorname{tr}\psi_S^2 \le (1+\gamma)^n\left(1-\frac{4\epsilon}{(1+\gamma)^2}\left(\gamma(1-\epsilon)-\left(\frac{(1+\gamma^2)^2}{(1+\gamma)^2}\right)\epsilon^{1/2}\right)\right),$$

which would imply the theorem. Now, for any θ, φ, we have $1-\epsilon\ge|(\cos\theta\langle 0|+e^{i\varphi}\sin\theta\langle 1|)\otimes\langle 0|^{\otimes n-1}|\psi\rangle|^2$. Picking θ such that

$$\cos\theta=\frac{|\langle 0|\psi\rangle|}{\sqrt{|\langle 0|\psi\rangle|^2+|\langle 10^{n-1}|\psi\rangle|^2}},$$

and φ such that $e^{i\varphi}\langle 10^{n-1}|\psi\rangle>0$, it is easy to see that

$$1-\epsilon\ge|\cos\theta\langle 0|\psi\rangle+e^{i\varphi}\sin\theta\langle 10^{n-1}|\psi\rangle|^2=|\langle 0|\psi\rangle|^2+|\langle 10^{n-1}|\psi\rangle|^2.$$

However, we have assumed that $1-\epsilon=|\langle 0|\psi\rangle|^2$, so this implies that $\langle 10^{n-1}|\psi\rangle=0$. Repeating the argument for the other $n-1$ subsystems shows that $|\psi\rangle$ is indeed orthogonal to every state with Hamming weight at most 1, so $|\phi\rangle$ has no weight 1 components. □

3 Correctness and applications of the product test

3.1 Proof of Theorem 1

In this section, we prove correctness of the product test (Theorem 1). Let the test be defined as in Definition 1. The following lemma from [20] allows the probability of passing to be understood; we include a proof for completeness.

Lemma 4. *Let $P_{test}(\rho, \sigma)$ denote the probability that the product test passes when applied to two mixed states $\rho, \sigma \in \mathcal{B}(\mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n})$. Define $P_{test}(\rho) := P_{test}(\rho, \rho)$. Then*

$$P_{test}(\rho, \sigma) = \frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr} \rho_S \sigma_S,$$

and in particular

$$P_{test}(\rho) = \frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr} \rho_S^2.$$

If $d_1 = d_2 = \cdots = d_n = d$, for some d, then

$$P_{test}(\rho) = \left(\frac{d+1}{2}\right)^n \operatorname{tr}(\mathcal{D}_{1/\sqrt{d+1}}^{\otimes n} \rho)^2.$$

Note that we can in fact assume that $d_1 = d_2 = \cdots = d_n = d$ without loss of generality by setting $d = \max(d_1, \dots, d_n)$, and embedding each of $\mathbb{C}^{d_1}, \dots, \mathbb{C}^{d_n}$ into $\mathbb{C}^d$ in the natural way. This padding operation neither affects the probability of the swap tests passing nor changes the distance to the closest product state.

Proof. Let $\mathcal{F}$ denote the swap (or flip) operator that exchanges two quantum systems of equal but arbitrary dimension, with $\mathcal{F}_S$ denoting the operator that exchanges only the qudits in the set S. Then we have

$$P_{test}(\rho) = \operatorname{tr}(\rho \otimes \sigma) \left(\frac{I + \mathcal{F}}{2}\right)^{\otimes n} = \frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr}(\rho \otimes \sigma)\, \mathcal{F}_S = \frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr} \rho_S \sigma_S.$$

The second part then follows from Lemma 2. □

We now analyse the probability of the product test passing for general n. We first note that, in the special case where $n = 2$, it is possible to analyse the probability of passing quite tightly. The proof of the following result, which is implicit in previous work of Wei and Goldbart [25], is essentially immediate from Lemma 4.

Lemma 5. *Let $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, where $d_1 \le d_2$, be a bipartite pure state with Schmidt coefficients $\sqrt{\lambda_1} \ge \sqrt{\lambda_2} \ge \cdots \ge \sqrt{\lambda_{d_1}}$. Then*

$$P_{test}(|\psi\rangle\langle\psi|) = \frac{1}{2}\left(1 + \sum_i \lambda_i^2\right),$$

while

$$1 - \epsilon := \max_{|\phi_1\rangle, |\phi_2\rangle} |\langle\psi|\phi_1\rangle|\phi_2\rangle|^2 = \lambda_1.$$

In particular,

$$1 - \epsilon + \frac{d_1}{2(d_1 - 1)}\epsilon^2 \le P_{test}(|\psi\rangle\langle\psi|) \le 1 - \epsilon + \epsilon^2.$$

We are finally ready to prove Theorem 1. The proof is split into two parts, which we formalise as separate theorems. The first part holds when ϵ is small, and depends on the results of Section 2. The second part holds when ϵ is large, and is proved using the first part.

Theorem 6. *Given* $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$*, let*

$$1-\epsilon = \max\{|\langle\psi|\phi_1,\dots,\phi_n\rangle|^2 : |\phi_i\rangle \in \mathbb{C}^{d_i}, i \leq 1 \leq n\}.$$

Then

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

Proof. The lower bound holds by general arguments. It is immediate that, if applied to $|\phi_1,\dots,\phi_n\rangle$, the product test succeeds with probability 1. As the test acts on two copies of $|\psi\rangle$, which has overlap $1-\epsilon$ with $|\phi_1,\dots,\phi_n\rangle$, it must succeed when applied to $|\psi\rangle$ with probability at least $(1-\epsilon)^2$. The upper bound follows from Lemma 4 and Theorem 3. The statement of Theorem 3 only explicitly covers the case where the dimensions of all the subsystems are the same; however, as noted above, we can assume this without loss of generality. □

This result is close to optimal. At the low end, the state $|\psi\rangle = \sqrt{1-\epsilon}|0^n\rangle + \sqrt{\epsilon}|1^n\rangle$ has $P_{test}(|\psi\rangle\langle\psi|) = 1-2\epsilon+2\epsilon^2+o(1)$. At the high end, for $|\psi\rangle = \sqrt{1-\epsilon}|00\rangle + \sqrt{\epsilon}|11\rangle$, $P_{test}(|\psi\rangle\langle\psi|) = 1-\epsilon+\epsilon^2$. We also note that this result does not extend to a test for separability of mixed states; the maximally mixed state on n qudits is separable but it is easy to verify that $P_{test}(I/d^n) = ((d+1)/2d)^n$, which approaches zero for large n.

Theorem 6 only gives a non-trivial upper bound on the probability of passing when ϵ is small (up to $\epsilon = \frac{1}{2}(3-\sqrt{5}) \approx 0.38$). We now show that the product test also works in the case where the state under consideration is far from any product state. We will need two lemmas.

Lemma 7. *Given* $|\psi\rangle \in \mathbb{C}^{d_1}\otimes\cdots\otimes\mathbb{C}^{d_n}$*, let* $P^P_{test}(|\psi\rangle\langle\psi|)$ *be the probability that the* P*-product test – the test for being product across partition* P *– passes. Then, for all* P*,* $P^P_{test}(|\psi\rangle\langle\psi|) \leq P_{test}(|\psi\rangle\langle\psi|)$*.*

Proof. The subspace corresponding to the usual product test passing is contained within the subspace corresponding to the P-product test passing. □

Lemma 8. *Let* $|\psi\rangle$*,* $|\phi\rangle$ *be pure states such that* $|\langle\psi|\phi\rangle|^2 = 1-\epsilon$*, and let* P *be a projector. Then* $|\langle\psi|P|\psi\rangle - \langle\phi|P|\phi\rangle| \leq \sqrt{\epsilon}$*.*

Proof. We can directly calculate $\frac{1}{2}\|\, |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\,\|_1 = \sqrt{\epsilon}$. This then gives the claimed upper bound on $|\operatorname{tr} P(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|)|$ (see [21, Chapter 9]). □

Theorem 9. *Given* $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$*, let*

$$1-\epsilon = \max\{|\langle\psi|\phi_1,\dots,\phi_n\rangle|^2 : |\phi_i\rangle \in \mathbb{C}^{d_i}, 1 \leq i \leq n\}.$$

Then, if $\epsilon \geq 11/32 > 0.343$*,* $P_{test}(|\psi\rangle\langle\psi|) \leq 501/512 < 0.979$*.*

Proof. For simplicity, in the proof we will use a quadratic upper bound on $P_{test}(|\psi\rangle\langle\psi|)$ that follows by elementary methods from Theorem 1: $P_{test}(|\psi\rangle\langle\psi|) \leq 1-\frac{3}{4}\epsilon+2\epsilon^2$. For a contradiction, assume that $P_{test}(|\psi\rangle\langle\psi|) > p := 501/512$, while $\epsilon \geq 11/32$.

For any partition P of $[n]$ into $1 \leq k \leq n$ parts, let $|\phi_P\rangle$ be the product state (with respect to P) that maximises $|\langle\psi|\phi\rangle|^2$ over all product states $|\phi\rangle$ (with respect to P). If

$$1 - h \leq |\langle\psi|\phi_P\rangle|^2 \leq 1 - \ell,$$

where for readability we define $\ell := 1/32$ and $h := 11/32$, then by the quadratic bound given above the P-product test passes with probability $P_{test}^P(|\psi\rangle\langle\psi|) \leq p$, implying by Lemma 7 that $P_{test}(|\psi\rangle\langle\psi|) \leq p$. Therefore, as we are assuming that $|\psi\rangle$ is a counterexample to the present theorem, there exists a k such that $|\langle\psi|\phi\rangle|^2 > 1 - \ell$ for some $|\phi\rangle$ that is product across k parties, and yet $|\langle\psi|\phi\rangle|^2 < 1 - h$ for all $|\phi\rangle$ that are product across $k + 1$ parties.

So, for this k, let $|\phi_1\rangle \cdots |\phi_k\rangle$ be the state that maximises $|\langle\psi|\phi_1, \dots, \phi_k\rangle|^2$. Thus there is some $\epsilon' < \ell$ such that we can write $|\psi\rangle$ as

$$|\psi\rangle = \sqrt{1 - \epsilon'}|\phi_1\rangle \cdots |\phi_k\rangle + \sqrt{\epsilon'}|\xi\rangle,$$

and by the arguments at the end of Theorem 3, the i^{th} marginal of $|\xi\rangle$ has support orthogonal to $|\phi_i\rangle$. Assume without loss of generality that $|\phi_1\rangle$ is a state of two or more qudits. Now we know that

$$\max_{|\phi'_{1,1}\rangle, |\phi'_{1,2}\rangle} |\langle\phi_1|\phi'_{1,1}\rangle|\phi'_{1,2}\rangle|^2(1 - \epsilon') < 1 - h, \tag{3}$$

or $|\phi'_{1,1}\rangle|\phi'_{1,2}\rangle|\phi_2\rangle \cdots |\phi_k\rangle$ would be a $(k + 1)$-partite state with overlap at least $1 - h$ with $|\psi\rangle$. (Here we have used the fact that $|\xi\rangle$ is orthogonal to $|\phi'_{1,1}\rangle|\phi'_{1,2}\rangle|\phi_2\rangle \cdots |\phi_k\rangle$ for any choice of $|\phi'_{1,1}\rangle$, $|\phi'_{1,2}\rangle$.) Let $1 - \delta = \max_{|\phi'_{1,1}\rangle, |\phi'_{1,2}\rangle} |\langle\phi_1|\phi'_{1,1}\rangle|\phi'_{1,2}\rangle|^2$. Then Eq. (3) implies that

$$1 - \delta < \frac{1 - h}{1 - \epsilon'} < \frac{1 - h}{1 - \ell} = \frac{21}{31}.$$

Using Lemma 5, we find that $P_{test}(|\psi_1\rangle\langle\psi_1|) \leq 1 - \delta + \delta^2 < 751/961$. Next we use Lemma 8 to obtain

$$\begin{aligned} P_{test}(|\psi\rangle\langle\psi|) &\leq P_{test}(|\phi_1\rangle\langle\phi_1| \otimes \cdots \otimes |\phi_k\rangle\langle\phi_k|) + \sqrt{\epsilon'} \\ &< P_{test}(|\phi_1\rangle\langle\phi_1|) + \sqrt{\ell} \\ &< \frac{751}{961} + \sqrt{\frac{1}{32}} < 0.96. \end{aligned}$$

But we previously assumed that $P_{test}(|\psi\rangle\langle\psi|) > p > 0.978$. We have reached a contradiction, so the proof is complete. □

Combining Theorems 6 and 9, we obtain Theorem 1 and thus have proven correctness of the product test. The constants in Theorem 9 have not been optimised as far as possible and could probably be significantly improved.

3.2 Testing for product unitaries

As well as being useful for testing quantum states, the product test has applications to testing properties of unitary operators. The results we obtain will be in terms of the normalised Hilbert-Schmidt inner product, which is defined as

$$\langle M, N\rangle := \frac{1}{d} \operatorname{tr} M^\dagger N$$

for $M, N \in M(d)$, where $M(d)$ denotes the set of $d \times d$ matrices. Note that, with this normalisation, $|\langle U, V\rangle| \leq 1$ for unitary operators U, V. The following correspondence, which we formalise as a lemma, underlies our ability to apply the product test to unitaries.

Lemma 10. *Let $|\Phi\rangle$ be a maximally entangled state of two d-dimensional qudits, written as $\frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i, i\rangle$ in terms of some basis $\mathcal{B} = (|1\rangle, \dots, |d\rangle)$. For any matrix $M \in M(d^n)$, define $|v(M)\rangle := (M \otimes I)|\Phi\rangle^{\otimes n}$. Then $\langle j|\langle k|v(M)\rangle = \frac{\langle j|M|k\rangle}{\sqrt{d^n}}$. In particular, for any matrices $M, N \in M(d^n)$, $\langle M, N\rangle = \langle v(M)|v(N)\rangle = \operatorname{tr} M^\dagger N/d^n$.*

Proof. This is just the well-known Choi-Jamiołkowski isomorphism. Written out explicitly, we have

$$\begin{aligned} \langle j|\langle k|(M \otimes I)|\Phi\rangle^{\otimes n} &= \langle j|\langle k|(M \otimes I) \left(\frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i, i\rangle_{AB} \right)^{\otimes n} \\ &= \frac{1}{\sqrt{d^n}} \sum_{i_1, \dots, i_n = 1}^{d} \langle j|M|i_1, \dots, i_n\rangle \langle k|i_1, \dots, i_n\rangle = \frac{\langle j|M|k\rangle}{\sqrt{d^n}}. \end{aligned}$$

The second claim in the lemma follows immediately from the first. □

We consider the problem of testing whether a unitary operator is a tensor product. That is, we are given access to a unitary U on the space of n qudits (for simplicity, restricting to the case where each of the qudits has the same dimension d), and we would like to decide whether $U = U_1 \otimes \cdots \otimes U_n$. This is one possible generalisation of the classical problem of testing linearity of functions $f : \{0,1\}^n \to \{0,1\}$ [7]; the classical special case is obtained by restricting U to be diagonal in the computational basis and to have diagonal entries all equal to ±1.

In Definition 2 we give a test that solves this problem using the product test. The test always accepts product unitaries, and rejects unitaries that are far from product, as measured by the normalised Hilbert-Schmidt inner product.

Definition 2 (Product unitary test).

The product unitary test proceeds as follows.

1. *Prepare two copies of the state $|\Phi\rangle^{\otimes n}$, then in both cases apply U to the n first halves of each pair of qudits to create two copies of the state $|v(U)\rangle \in (\mathbb{C}^{d^2})^{\otimes n}$.*
2. *Return the result of applying the product test to the two copies of $|v(U)\rangle$, with respect to the partition into n d^2-dimensional subsystems.*

In order to analyse this test, we will need the following lemma.

Lemma 11. *Given $U \in U(d^n)$, let*

$$1 - \epsilon = \max\{|\langle U, A_1 \otimes \cdots \otimes A_n\rangle|^2 : A_i \in M(d), \langle A_i, A_i\rangle = 1, 1 \leq i \leq n\}.$$

Then, if $\epsilon \leq 1/2$, there exist $V_1, \dots, V_n \in U(d)$ such that $|\langle U, V_1 \otimes \cdots \otimes V_n\rangle|^2 \geq (1 - 2\epsilon)^2$.

Proof. For all $1 \leq i \leq n$, let the polar decomposition of A_i be $|A_i|C_i$, where $|A_i| = \sqrt{A_i A_i^\dagger}$ and $C_i \in U(d)$. Set $A = \bigotimes_{i=1}^n A_i$, $C = \bigotimes_{i=1}^n C_i$. Then

$$\langle C, A\rangle = \frac{1}{d^n}\prod_{i=1}^n \operatorname{tr} C_i^\dagger |A_i| C_i = \frac{1}{d^n}\prod_{i=1}^n \operatorname{tr}|A_i| = \frac{1}{d^n}\max_{V\in U(d^n)} |\operatorname{tr} VA| \geq \sqrt{1-\epsilon}.$$

This implies that we can expand

$$U = \sqrt{1-\epsilon}\, A + D, \quad C = \sqrt{1-\epsilon'}\, A + E$$

for some $\epsilon' \leq \epsilon$ and matrices D, E such that $\langle D, D\rangle = \epsilon$, $\langle E, E\rangle = \epsilon'$, $\langle A, D\rangle = 0$, $\langle A, E\rangle = 0$. So

$$|\langle U, C\rangle| = |\sqrt{1-\epsilon}\sqrt{1-\epsilon'} + \langle D, E\rangle| \geq |\sqrt{1-\epsilon}\sqrt{1-\epsilon'} - \sqrt{\epsilon}\sqrt{\epsilon'}| \geq 1 - 2\epsilon,$$

for $\epsilon \leq 1/2$. This implies the lemma. □

We are now ready to prove correctness of the product unitary test. Let the probability that this test passes when applied to some unitary U be $P_{test}(U)$. Then we have the following theorem, which proves a conjecture from [20].

Theorem 12. *Given $U \in U(d^n)$, let*

$$1 - \epsilon = \max\{|\langle U, V_1 \otimes \cdots \otimes V_n\rangle|^2 : V_1, \ldots, V_n \in U(d)\}.$$

Then, if $\epsilon = 0$, $P_{test}(U) = 1$. If $\epsilon \lesssim 0.106$, then $P_{test}(U) \leq 1 - \frac{1}{4}\epsilon + \frac{1}{16}\epsilon^2 + \frac{1}{8}\epsilon^{3/2}$. If $0.106 \lesssim \epsilon \leq 1$, $P_{test}(U) \leq 501/512$.

Proof. By Lemma 10, there is a direct correspondence between operators $M \in M(d)$ with $|\langle M, M\rangle| = 1$ and quantum states $|v(M)\rangle$. If we define

$$1 - \epsilon' := \max\{|\langle U, A_1 \otimes \cdots \otimes A_n\rangle|^2 : A_i \in M(d), \langle A_i, A_i\rangle = 1, 1 \leq i \leq n\},$$

then by Theorem 1, if $\epsilon' \lesssim 0.0265$, $P_{test}(U) \leq 1 - \epsilon' + \epsilon'^2 + \epsilon'^{3/2}$, and if $\epsilon' \gtrsim 0.0265$, $P_{test}(U) \leq 501/512$. If $\epsilon' \geq 1/2$, then the result follows immediately. On the other hand, by Lemma 11, if $\epsilon' \leq 1/2$, there exist $V_1, \ldots, V_n \in U(d)$ such that $|\langle U, V_1 \otimes \cdots \otimes V_n\rangle|^2 \geq (1-2\epsilon')^2 \geq 1 - 4\epsilon'$. Thus we have $\frac{1}{4}\epsilon \leq \epsilon' \leq \epsilon$. The theorem follows by combining the bound on ϵ and the bound on $P_{test}(U)$. □

Our test is sensitive to the Hilbert-Schmidt distance of a unitary from the set of product unitaries. One might hope to design a similar test that instead uses a notion of distance based on the operator norm. However, this is not possible. For example, if we could detect a constant difference in the operator norm between an arbitrary unitary U and the set of product unitaries then we could find a single marked item in a set of size d^n. By the optimality of Grover's algorithm, this requires $\Omega(d^{n/2})$ queries to U. More generally, any test that uses a constant number of queries to U can only detect an $\Omega(1)$ difference in an $\Omega(1)$ fraction of the d^n dimensions that U acts upon.

3.3 Optimality of the product test

Our test has perfect completeness in the sense that if $|\psi\rangle$ is exactly a product state then it will always pass the product test. It is hard to precisely define soundness, since no state is orthogonal to all product states: however, we can say that our test has constant soundness in that if $|\psi\rangle$ has overlap at most $1-\epsilon$ with any product state then it will pass the product test with probability at most $1-\Theta(\epsilon)$.

In fact, if we consider only product-state tests with perfect completeness, then we can show that our test has optimal soundness: that is, it rejects as often as possible given the constraint of always accepting product states. More generally, suppose that a product-state test T is given $|\psi\rangle^{\otimes k}$ as input. Since the outcome of the test is binary, we can say that T is an operator on the nk-qudit Hilbert space with $0 \leq T \leq I$ and that the test accepts with probability $\operatorname{tr} T\psi^{\otimes k}$.

Let S be the set of product states in $\mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, and define S^k to be the span of $\{|\phi\rangle^{\otimes k} : |\phi\rangle \in S\}$. For a single system $\mathbb{C}^d$, the span of $\{|\phi\rangle^{\otimes k} : |\phi\rangle \in \mathbb{C}^d\}$ is denoted $\operatorname{Sym}^k \mathbb{C}^d$. This is the symmetric subspace of $(\mathbb{C}^d)^{\otimes k}$, meaning that it can be equivalently defined to be the set of vectors in $(\mathbb{C}^d)^{\otimes k}$ that is invariant under permutation by the symmetric group S_k. This fact allows the projector onto $\operatorname{Sym}^k \mathbb{C}^d$, which we denote $\Pi^{\mathrm{sym}}_{d,k}$, to be implemented efficiently [5]. Also, it implies that $S^k = \operatorname{Sym}^k \mathbb{C}^{d_1} \otimes \cdots \otimes \operatorname{Sym}^k \mathbb{C}^{d_n}$ and the projector onto S^k, denoted Π_{S^k}, is $\Pi^{\mathrm{sym}}_{d_1,k} \otimes \cdots \otimes \Pi^{\mathrm{sym}}_{d_n,k}$.

Now we return to our discussion of product-state tests. If $\operatorname{tr} T\phi^{\otimes k} = 1$ for all $\phi \in S$, then $T \geq \Pi_{S^k}$. Thus, T will always accept at least as often as Π_{S^k} will on any input, or equivalently, taking $T = \Pi_{S^k}$ yields the test which rejects as often as possible given the constraint of accepting every state in S^k.

To understand Π_{S^k}, note that the projector onto $\operatorname{Sym}^k \mathbb{C}^d$ is given by $\frac{1}{k!}\sum_{\pi \in \mathcal{S}_k} P(\pi)$, where

$$P(\pi) = \sum_{i_1,\ldots,i_k \in [d]} |i_1, \ldots, i_k\rangle\langle i_{\pi(1)}, \ldots, i_{\pi(k)}|.$$

For $k = 1$, $\operatorname{Sym}^1 \mathbb{C}^d$ simply equals $\mathbb{C}^d$, and Π_{S^1} is the identity operator on $(\mathbb{C}^d)^{\otimes n}$. Thus, no non-trivial product-state test is possible when given one copy of $|\psi\rangle$.

When $k = 2$, $\operatorname{Sym}^2 \mathbb{C}^d$ is the $+1$ eigenspace of $(I + \mathcal{F})/2$, which is the space that passes the swap test. Thus, the product test (in Definition 1) performs the projection onto S^2 and therefore rejects non-product states as often as possible for a test on $|\psi\rangle^{\otimes 2}$ that always accepts when $|\psi\rangle$ is a product state. These arguments also imply that given $|\psi\rangle^{\otimes k}$, projecting onto S^k yields an optimal k-copy product-state test of $|\psi\rangle$. The strength of these tests is strictly increasing with k, but we leave the problem of analysing them carefully to future work.

Finally, this interpretation of the product test allows us to consider generalisations to testing membership in other sets S. However, we will not explore these possibilities further in this paper.

4 QMA(2) vs. QMA(k)

In this section, we apply the product test to a problem in quantum complexity theory: whether k unentangled provers are better than 2 unentangled provers. This question can be formalised as whether the complexity classes QMA(k) and QMA(2) are equal [18, 2]. These classes are defined as follows.

Definition 3. *A language L is in QMA(k)$_{s,c}$ if there exists a polynomial-time quantum algorithm $\mathcal{A}$ such that, for all inputs $x \in \{0,1\}^n$:*

1. **Completeness:** *If $x \in L$, there exist k witnesses $|\psi_1\rangle, \dots, |\psi_k\rangle$, each a state of $\mathrm{poly}(n)$ qubits, such that $\mathcal{A}$ outputs "accept" with probability at least c on input $|x\rangle|\psi_1\rangle \dots |\psi_k\rangle$.*
2. **Soundness:** *If $x \notin L$, then $\mathcal{A}$ outputs "accept" with probability at most s on input $|x\rangle|\psi_1\rangle \dots |\psi_k\rangle$, for all states $|\psi_1\rangle, \dots, |\psi_k\rangle$.*

We use QMA(k) as shorthand for QMA(k)$_{1/3,2/3}$, and QMA as shorthand for QMA(1). We always assume $1 \leq k \leq \mathrm{poly}(n)$.

It has been conjectured [18, 2] that in fact QMA(k)=QMA(2). We do not quite succeed in proving this conjecture, but we do show that, using the product test, any QMA(k) protocol can be simulated by a QMA(2) protocol, as long as one is willing to accept some loss of soundness.

Theorem 13. *For any $0 < s < 1$, there exists an $s' < 1$ such that $QMA(k)_{s,c} \subseteq QMA(2)_{s',c}$. When $s < \frac{1}{2}(3-\sqrt{5}) \approx 0.382$, s' can be taken to be $s + \sqrt{(3-\sqrt{5})/2} \approx s + 0.618$.*

To prove this theorem, we need to simulate a QMA(k) protocol achieving soundness s and completeness c using two unentangled proofs. Suppose the proofs in the original protocol are $|\psi_1\rangle, \dots, |\psi_k\rangle$, each of which has dimension d, and Arthur's original verification algorithm is $\mathcal{A}$. Then the QMA(2) protocol acts as specified in Definition 4.

Definition 4 (**QMA(k) to QMA(2)**).

The QMA(2) protocol proceeds as follows.

1. *Each of the two Merlins sends $|\psi\rangle := |\psi_1\rangle \otimes \ldots \otimes |\psi_k\rangle$ to Arthur.*
2. *Arthur runs the product test with the two states as input.*
3. *If the test fails, Arthur rejects. Otherwise, Arthur runs the algorithm $\mathcal{A}$ on one of the two states, picked uniformly at random, and outputs the result.*

It is obvious that this protocol achieves completeness c: if the Merlins follow the protocol, the product test passes with certainty, and hence Arthur accepts with the same probability that $\mathcal{A}$ accepts, which is at least c. Showing soundness is somewhat more complicated.

We first show that we can assume that the two states Arthur receives are identical. Imagine that this does not hold, and Arthur receives different states $|\phi\rangle, |\varphi\rangle$. Then the probability that the product test accepts is

$$\begin{aligned}
\frac{1}{d^n} \sum_{S \subseteq [n]} \operatorname{tr} \phi_S \varphi_S &\leq \frac{1}{d^n} \sum_{S \subseteq [n]} \sqrt{\operatorname{tr} \phi_S^2} \sqrt{\operatorname{tr} \varphi_S^2} \\
&\leq \frac{1}{2\,d^n} \sum_{S \subseteq [n]} \operatorname{tr} \phi_S^2 + \operatorname{tr} \varphi_S^2 \\
&= \frac{1}{2} \left(P_{test}(\phi) + P_{test}(\varphi) \right),
\end{aligned}$$

where the first inequality is Cauchy-Schwarz and the second is the AM-GM inequality. As we run $\mathcal{A}$ on a random choice of the two states in the second stage, the probability that the whole algorithm accepts is also upper bounded by the average probability of it accepting when run on $|\phi\rangle$ and $|\varphi\rangle$. So, to achieve maximal probability of accepting, the two states might as well be identical.

To prove the remainder of the theorem, we will need the following "gentle measurement" lemma.

Lemma 14 (Gentle measurement lemma [26, 23])**.** *Let ρ be a density operator, and let $0 \leq X \leq I$ be a projector such that $\operatorname{tr} \rho X \geq 1 - \delta$. Then $\|\rho - X\rho X\|_1 \leq 2\sqrt{\delta}$.*

Assume the product test accepts with probability $1 - \delta$. By Lemma 14, the probability that $\mathcal{A}$, and hence Arthur, accepts is at most $s + \sqrt{\delta}$. Further assume that the maximal overlap of $|\psi\rangle$ with a product state is $1 - \epsilon$. Then, by Lemma 8, the probability that $\mathcal{A}$ accepts is also upper bounded by $s + \sqrt{\epsilon}$. For any choice of $0 \leq \epsilon \leq 1$, the overall soundness is therefore upper bounded by

$$\begin{aligned} s'(\epsilon) &:= \min\{s + \sqrt{\delta}, s + \sqrt{\epsilon}, 1 - \delta\} \\ &\leq \begin{cases} \min\{s + 1 - \epsilon, s + \sqrt{\epsilon}, 1 - \epsilon + \epsilon^2 + \epsilon^{3/2}\} & \text{if } \epsilon \leq 11/32 \\ \min\{s + 1 - \epsilon, s + \sqrt{\epsilon}, 501/512\} & \text{if } \epsilon > 11/32, \end{cases} \end{aligned}$$

where the inequality follows from Theorem 1. We now want to maximise this expression over ϵ. First note that, whatever the value of ϵ, we have the upper bound $s'(\epsilon) \leq \min\{s + 1 - \epsilon, s + \sqrt{\epsilon}\}$, which is easily seen to be at most $s + \sqrt{(3 - \sqrt{5})/2}$ for all $0 \leq \epsilon \leq 1$. Second, note that for any $0 \leq \epsilon \leq 1$, and any $s < 1$, the upper bound on $s'(\epsilon)$ is always a constant strictly less than 1. This completes the proof.

As a corollary, the $k = O(\sqrt{n} \operatorname{poly} \log(n))$ protocol for 3-SAT (where n is the number of clauses) from Ref. [1] can be simulated by two provers. The result is a QMA(2) protocol for 3-SAT with perfect completeness and constant soundness that uses $O(\sqrt{n} \operatorname{poly} \log(n))$ qubits.

5 Interpretation as an average over product states

We have seen (via Lemma 4) that the probability of the product test passing when applied to some state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ is equal to the average purity, across all choices of subsystem $S \subseteq [n]$, of $\operatorname{tr} |\psi\rangle\langle\psi|_S$. One interpretation of the proof of correctness of the product test is therefore that, if the average entanglement of $|\psi\rangle$ across all bipartite partitions of $[n]$ is low, as measured by the purity, then $|\psi\rangle$ must in fact be close to a product state across all subsystems.

In this section, we discuss a similar interpretation of our results in terms of an average over product states, via the following proposition.

Proposition 15. *Given $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$,*

$$P_{test}(|\psi\rangle\langle\psi|) = \left(\frac{d(d+1)}{2}\right)^n \mathbb{E}_{|\phi_1\rangle,\dots,|\phi_n\rangle} \left[|\langle\psi|\phi_1 \dots \phi_n\rangle|^4\right].$$

Proof. Similarly to before, let the input to the product state be two copies ψ_A, ψ_B of a state

$\psi := |\psi\rangle\langle\psi|$, and let $\mathcal{F}$ denote the swap operator that exchanges systems A and B. Then

$$\begin{aligned}\mathbb{E}_{|\phi_1\rangle,\dots,|\phi_n\rangle}\left[|\langle\psi|\phi_1,\dots,\phi_n\rangle|^4\right] &= \mathbb{E}_{|\phi_1\rangle,\dots,|\phi_n\rangle}\left[\operatorname{tr}(\psi_A\otimes\psi_B)((\phi_1\otimes\cdots\otimes\phi_n)_A\otimes(\phi_1\otimes\cdots\otimes\phi_n)_B)\right]\\ &= \operatorname{tr}(\psi_A\otimes\psi_B)\left(\mathbb{E}_{|\phi\rangle}\left[\phi_A\otimes\phi_B\right]\right)^{\otimes n}\\ &= \operatorname{tr}(\psi_A\otimes\psi_B)\left(\frac{I+\mathcal{F}}{d(d+1)}\right)^{\otimes n} = \left(\frac{2}{d(d+1)}\right)^n P_{test}(|\psi\rangle\langle\psi|).\end{aligned}$$

□

We note that, in this interpretation, our main result is reminiscent of the so-called inverse theorem for the second Gowers uniformity norm [12, 13], which we briefly outline. Let $f : \{0,1\}^n \to \mathbb{R}$ be some function such that $\frac{1}{2^n}\sum_x f(x)^2 = 1$, and let the p-norms of f on the Fourier side be defined as

$$\|\hat{f}\|_p = \left(\sum_{x\in\{0,1\}^n}\left|\frac{1}{2^n}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}f(y)\right|^p\right)^{1/p}.$$

Then it is straightforward to show that

$$\|\hat{f}\|_\infty^4 \le \|\hat{f}\|_4^4 \le \|\hat{f}\|_\infty^2,$$

where the quantity in the middle is known as the (fourth power of) the second Gowers uniformity norm of f. That is, $\|\hat{f}\|_\infty^2$ (representing the largest overlap of f with a parity function) is well approximated by $\|\hat{f}\|_4^4$ (the *average* of the squared overlaps with parity functions). This simple approximation has proven useful in arithmetic combinatorics [12].

Via the correspondence of Proposition 15, Theorem 1 shows that a similar result holds if we replace the cube $\{0,1\}^n$ with the space $(\mathbb{C}^d)^{\otimes n}$: the largest overlap with a product state can be well approximated by the average squared overlap with product states. Note that if one attempts to use the classical proof technique for the Gowers uniformity norm to prove this result, one does not obtain Theorem 1, but a considerably weaker result containing a term exponentially large in n. Intuitively, this is because the set of overlaps with parity functions for some function $f : \{0,1\}^n \to \mathbb{R}$ is essentially arbitrary, whereas the set of overlaps of some state $|\psi\rangle$ with product states is highly constrained.

6 Conclusion

Our main result can be seen as a "stability" theorem for the output purity of the depolarising channel. It is an interesting problem to determine whether a similar result holds for all output Rényi entropies for the depolarising channel, or even for all channels where additivity holds. As a more modest open question, can Theorem 3 be tightened further, perhaps by improving the constant in the $\epsilon^{3/2}$ term? It would also be interesting to improve the constants in Theorem 1 in the regime of large ϵ, as at present they are extremely pessimistic. The regime of large ϵ is generally somewhat mysterious: for example, we do not know the minimum value of P_{test}, or the largest distance from any product state that can be achieved by a state of n qudits. Finally, we hope that a suitably strengthened version of our result can be used to prove the amplification conjecture for QMA(2), which states that QMA(2) protocols can be amplified to have exponentially small error probability. This would require a tight analysis of the case when ϵ is very close to 1.

Acknowledgements

AM was supported by the EC-FP6-STREP network QICS and an EPSRC Postdoctoral Research Fellowship. AWH was supported by the EPSRC grant "QIP-IRC". We would like to thank Andreas Winter and Toby Cubitt for inspiring discussions.

References

[1] S. Aaronson. The learnability of quantum states. *Proceedings of the Royal Society A*, 463:2088, 2007. `quant-ph/0608142`.

[2] 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`.

[3] G. Amosov, A. Holevo, and R. Werner. On some additivity problems in quantum information theory, 2000. `math-ph/0003002`.

[4] A. Atici and R. A. Servedio. Quantum algorithms for learning and testing juntas. *Quantum Information Processing*, 6:323–348, 2007. `arXiv:0707.3479`.

[5] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello. Stabilisation of quantum computations by symmetrisation. *SIAM J. Comput.*, 26(5):1541–1557, 1997. `quant-ph/9604028`.

[6] H. Blier and A. Tapp. All languages in NP have very short quantum proofs. In *First International Conference on Quantum, Nano, and Micro Technologies*, pages 34–37, Los Alamitos, CA, USA, 2009. IEEE Computer Society.

[7] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3):549–595, 1993.

[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, 2001. `quant-ph/0102001`.

[9] H. Buhrman, L. Fortnow, I. Newman, and H. Röhrig. Quantum property testing. *SIAM J. Comput.*, 37(5):1387–1400, 2008. `quant-ph/0201117`.

[10] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin. Quantum channel capacity of very noisy channels. *Phys. Rev. A.*, 57:830, 1998. `quant-ph/9706061`.

[11] E. Fischer. The art of uninformed decisions: A primer to property testing. *Bulletin of the European Association for Theoretical Computer Science*, 75:97–126, 2001.

[12] W. T. Gowers. A new proof of Szeméredi's theorem for progressions of length four. *Geometric and Functional Analysis*, 8(3):529–551, 1998.

[13] W. T. Gowers. A new proof of Szeméredi's theorem. *Geometric and Functional Analysis*, 11(3):465–588, 2001.

[14] O. Gühne and G. Toth. Entanglement detection. *Physics Reports*, 471(1), 2009. `arXiv:0811.2803`.

[15] M. B. Hastings. A counterexample to additivity of minimum output entropy. *Nature Physics*, 5, 2009. `arXiv:0809.3972`.

[16] T. Ito, H. Kobayashi, and K. Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies, 2008. `arXiv:0810.0693`.

[17] J. Kempe and O. Regev. No strong parallel repetition with entangled and non-signaling provers, 2009. `arXiv:0911.0201`.

[18] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: are multiple Merlins more helpful to Arthur? In *Proc. ISAAC '03*, pages 189–198, 2003. `quant-ph/0306051`.

[19] F. Mintert, M. Kuś, and A. Buchleitner. Concurrence of mixed multipartite quantum states. *Phys. Rev. Lett.*, 95(26):260502, 2005. `quant-ph/0411127`.

[20] A. Montanaro and T. Osborne. Quantum boolean functions, 2008. `arXiv:0810.2435`.

[21] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2000.

[22] T. Ogawa and H. Nagaoka. Strong converse to the quantum channel coding theorem. *ieeeit*, 45(7):2486–2489, 1999. `quant-ph/9808063`.

[23] T. Ogawa and H. Nagaoka. A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In *Proc. 2002 IEEE International Symposium on Information Theory*, page 73, 2002. `quant-ph/0208139`.

[24] S. Walborn, P. Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner. Experimental determination of entanglement with a single measurement. *Nature*, 440(7087):1022–1024, 2006.

[25] T. Wei and P. Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Phys. Rev. A.*, 68(4):42307, 2003. `quant-ph/0307219`.

[26] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inform. Theory*, 45(7):2481–2485, 1999.