An efficient test for product states, with applications to quantum Merlin-Arthur games

Ashley Montanaro[*]

December 2, 2010

Abstract

In this talk, I will discuss a test that can distinguish efficiently between pure product states of n quantum systems and states which are far from product. A key application of the test is to quantum Merlin-Arthur games with multiple Merlins, where it allows us to prove several structural results that had been previously conjectured, including the fact that soundness amplification is possible and that two Merlins can simulate many Merlins: $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ for $k \geq 2$. These results imply that 3-SAT can be solved efficiently given two short unentangled quantum proofs, which in turn implies complexity-theoretic obstructions to the existence of fast algorithms for a variety of tasks in quantum information theory and elsewhere.

1 Testing product states

The main result I will discuss in this talk is a quantum test to determine whether an n-partite state $|\psi\rangle$ is a product state or far from any product state, and the applications of this test. 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 this test (indeed, as we show, any possible such test) is that it requires two copies of $|\psi\rangle$.

The product test is defined in Protocol 1 below. It uses as a subroutine the *swap test* for comparing quantum states [4]. 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". The product test was originally introduced in [7] as one of a family of tests for generalisations of the concurrence entanglement measure, and has been implemented experimentally as a means of detecting bipartite entanglement directly [9]. Further, the test was proposed in [8] as a means of determining whether a unitary operator is product. Our contribution here is to prove the correctness of the product test for all n, as formalised in the following theorem.

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

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

Let $P_{test}(|\psi\rangle\langle\psi|)$ be the probability that the product test passes when applied to $|\psi\rangle$.
Then $P_{test}(|\psi\rangle\langle\psi|) = 1 - \Theta(\epsilon)$.

Crucially, the parameters of the test do not depend on n or the local dimensions of $|\psi\rangle$.

[*] Department of Applied Mathematics and Theoretical Physics, University of Cambridge; `am994@cam.ac.uk`. Talk based on joint work [5] with Aram Harrow at the University of Bristol.

Protocol 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.

The proof of Theorem 1 is based on relating the probability of the product test passing to the action of the qudit depolarising channel. It is known that the maximum output purity of this channel is achieved for product state inputs [2]; our result, informally, says that any state that is "close" to achieving maximum output purity must in fact be "close" to a product state.

2 Applications of the product test

I will describe several applications of the product test. The most important of these is that this test can be used to relate $\mathsf{QMA}(k)$ to $\mathsf{QMA}(2)$. The complexity class $\mathsf{QMA}(k)$ 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 [6, 1]. To put $\mathsf{QMA}(k)$ inside $\mathsf{QMA}(2)$, we can have two provers simulate k provers by each submitting k unentangled proofs, whose lack of entanglement can be verified with the product test. A byproduct of this simulation allows us to prove amplification of $\mathsf{QMA}(2)$ protocols to exponentially small probability of error, and even to show that, in $\mathsf{QMA}(2)$ protocols, the verifier's measurement operator corresponding to an "accept" outcome can be taken to be separable.

As a consequence of these results, we can improve upon the results of [1, 3] to obtain a protocol in $\mathsf{QMA}(2)$ that verifies 3-SAT with constant soundness gap and $O(\sqrt{n}\,\mathrm{poly}\log(n))$ qubits (where n is the number of clauses). This allows us to prove hardness results for various $\mathsf{QMA}(2)$-complete problems (i.e. problems which are equivalent to optimising a linear functional over the set of separable states), under restrictive assumptions on the hardness of 3-SAT; stronger assumptions naturally lead to stronger hardness results.

An example of such a hardness result is the following statement about the difficulty of approximating $\mathrm{SEP}(d,d)$, the set of separable quantum states on $d \times d$ dimensions. We show that, if K_d is a convex set that approximates $\mathrm{SEP}(d,d)$ to within constant trace distance, then membership in K_d cannot be decided in polynomial time unless 3-SAT $\in \mathsf{DTIME}(\exp(\sqrt{n}\log^{O(1)}(n)))$. Another example is that the minimum output entropy of a quantum channel cannot be estimated up to a constant in polynomial time, under the same assumption on the complexity of 3-SAT. Making the stronger assumption that there are no subexponential-time algorithms for 3-SAT even allows us to rule out algorithms for these problems running in time $d^{O(\log^{1-\epsilon} d)}$, for any $\epsilon > 0$.

References

[1] 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`.

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

[3] 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. arXiv:0709.0738.

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

[5] A. Harrow and A. Montanaro. An efficient test for product states, with applications to quantum Merlin-Arthur games. In *Proc. 51st Annual Symp. Foundations of Computer Science*, 2010. `arXiv:1001.0017`.

[6] 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`.

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

[8] A. Montanaro and T. Osborne. Quantum boolean functions. *Chicago Journal of Theoretical Computer Science*, 2010. `arXiv:0810.2435`.

[9] 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.