# An efficient test for product states

Aram Harrow and **Ashley Montanaro**

Department of Mathematics and Department of Computer Science,
University of Bristol, UK

arXiv:1001.0017

University of Bristol

EPSRC Engineering and Physical Sciences Research Council

# The basic problem

Given a quantum state, is it entangled?

# The basic problem

Given a quantum state, is it entangled?

Recall:

- A pure $n$-partite state $|\psi\rangle$ is product if it can be written as $|\psi_1\rangle \dots |\psi_n\rangle$, for some states $|\psi_1\rangle, \dots, |\psi_n\rangle$, and is entangled if it is not product.

- A mixed $n$-partite state $\rho$ is separable if it can be written as

$$\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_1^i| \otimes \cdots \otimes |\psi_n^i\rangle\langle\psi_n^i|,$$

  and is entangled if it is not separable.

# Variants

Many different variants of the problem of detecting entanglement:

- How are we given the input state?
- Is it pure or mixed?
- Is the state bipartite or multipartite?
- What level of accuracy do we demand?
- Do we want to detect entanglement in all states, or just some of them?

These different variants have wildly differing complexities...

# Good news and bad news

- Given a bipartite pure state $|\psi\rangle$ as a $d^2$-dimensional vector, whether $|\psi\rangle$ is entangled can be determined efficiently using the Schmidt decomposition.

# Good news and bad news

- Given a bipartite pure state $|\psi\rangle$ as a $d^2$-dimensional vector, whether $|\psi\rangle$ is entangled can be determined efficiently using the Schmidt decomposition.

- Given a bipartite mixed state $\rho$ as a $d^2$-dimensional matrix, it's NP-hard to determine whether $\rho$ is separable (up to accuracy $1/\mathrm{poly}(d)$).

# Good news and bad news

- Given a bipartite pure state $|\psi\rangle$ as a $d^2$-dimensional vector, whether $|\psi\rangle$ is entangled can be determined efficiently using the Schmidt decomposition.

- Given a bipartite mixed state $\rho$ as a $d^2$-dimensional matrix, it's NP-hard to determine whether $\rho$ is separable (up to accuracy $1/\text{poly}(d)$).
  - This was shown by [Gurvits '03] for accuracy $1/\exp(d)$ via a reduction from the NP-hard Clique problem.
  - Later improved to $1/\text{poly}(d)$ by [Gharibian '10] (using techniques of [Liu '07]) and also (implicitly) by [Beigi '08].

- See [Ioannou '07] for an extensive discussion of the state of the art circa 2006.

# Our main result

- Let $|\psi\rangle$ be a pure $n$-partite state with local dimensions $d_1, \ldots, d_n$.
- Let the nearest product state to $|\psi\rangle$ be $|\phi_1\rangle \ldots |\phi_n\rangle$.
- Let $|\langle\psi|\phi_1, \ldots, \phi_n\rangle|^2 = 1 - \epsilon$.

# Our main result

- Let $|\psi\rangle$ be a pure $n$-partite state with local dimensions $d_1, \ldots, d_n$.
- Let the nearest product state to $|\psi\rangle$ be $|\phi_1\rangle \ldots |\phi_n\rangle$.
- Let $|\langle\psi|\phi_1, \ldots, \phi_n\rangle|^2 = 1 - \epsilon$.

**Theorem**

There is an efficient quantum test, called the **product test**, that accepts with probability $1 - \Theta(\epsilon)$, given two copies of $|\psi\rangle$.

# Our main result

- Let $|\psi\rangle$ be a pure $n$-partite state with local dimensions $d_1, \ldots, d_n$.
- Let the nearest product state to $|\psi\rangle$ be $|\phi_1\rangle \ldots |\phi_n\rangle$.
- Let $|\langle\psi|\phi_1, \ldots, \phi_n\rangle|^2 = 1 - \epsilon$.

**Theorem**

There is an efficient quantum test, called the **product test**, that accepts with probability $1 - \Theta(\epsilon)$, given two copies of $|\psi\rangle$.

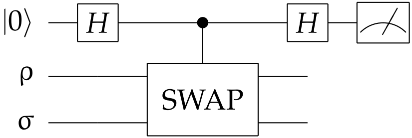
- Note that the parameters of the test don't depend on the local dimension $d$ or the number of subsystems $n$.
- This is similar to classical property testing algorithms.

# The rest of this talk

- Introduction to the product test
- Correctness of the product test
- Quantum Merlin-Arthur games
- Computational hardness of quantum information theory tasks:
  - Computing minimum output entropy
  - Separability testing

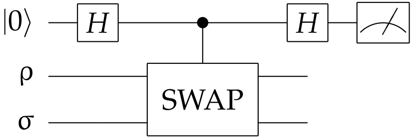
# The swap test

The product test uses as a subroutine the swap test.



# The swap test

The product test uses as a subroutine the swap test.




This test takes two (possibly mixed) states ρ, σ as input, returning "same" with probability

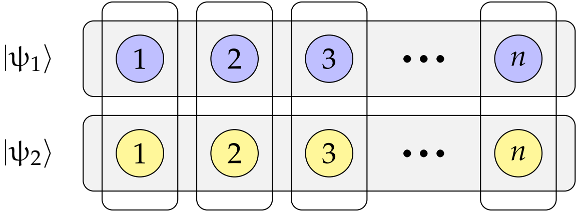
$$\frac{1}{2} + \frac{1}{2}\,\mathrm{tr}(\rho\,\sigma),$$

otherwise returning "different".

# The product test

## Product test

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.



# Previous use of the product test

The product test has appeared before in the literature.

- Originally introduced by [Mintert, Kuś, Buchleitner '05] as one of a family of tests for generalisations of the concurrence entanglement measure.

# Previous use of the product test

The product test has appeared before in the literature.

- Originally introduced by [Mintert, Kuś, Buchleitner '05] as one of a family of tests for generalisations of the concurrence entanglement measure.
- Implemented experimentally for bipartite states by [Walborn et al '06].

# Previous use of the product test

The product test has appeared before in the literature.

- Originally introduced by [Mintert, Kuś, Buchleitner '05] as one of a family of tests for generalisations of the concurrence entanglement measure.
- Implemented experimentally for bipartite states by [Walborn et al '06].
- Proposed by [AM, Osborne '08] as a means of determining whether a unitary operator is product.

# Previous use of the product test

The product test has appeared before in the literature.

- Originally introduced by [Mintert, Kuś, Buchleitner '05] as one of a family of tests for generalisations of the concurrence entanglement measure.
- Implemented experimentally for bipartite states by [Walborn et al '06].
- Proposed by [AM, Osborne '08] as a means of determining whether a unitary operator is product.

Our contribution: to prove correctness of the test for all $n$.

# Analysing the product test

**Lemma**

Let $P_{\text{test}}(\rho)$ be the probability that the product test passes on input $\rho$. Then

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

# Analysing the product test

**Lemma**

Let $P_{\text{test}}(\rho)$ be the probability that the product test passes on input $\rho$. Then

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

- Thus the product test measures the average purity of the input $|\psi\rangle$ across bipartitions.
- Note that it's immediate that $P_{\text{test}}(\rho) = 1$ if and only if $\rho$ is a pure product state.
- So our main result says: if the average entanglement across bipartitions of $|\psi\rangle$ is low, $|\psi\rangle$ must be close to a product state.

# Our main result

**Theorem**

Let the nearest product state to $|\psi\rangle$ be $|\phi_1\rangle \dots |\phi_n\rangle$, and set $|\langle\psi|\phi_1, \dots, \phi_n\rangle|^2 = 1 - \epsilon$. Then

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

Furthermore, if $\epsilon \geqslant 11/32$, $P_{\text{test}}(|\psi\rangle\langle\psi|) \leqslant 501/512$.

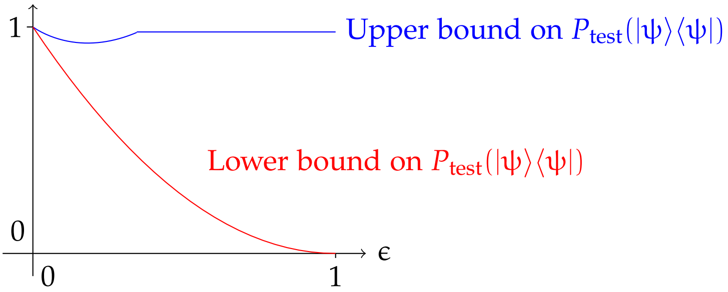
# Our main result

**Theorem**

Let the nearest product state to $|\psi\rangle$ be $|\phi_1\rangle \dots |\phi_n\rangle$, and set $|\langle\psi|\phi_1,\dots,\phi_n\rangle|^2 = 1-\epsilon$. Then

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

Furthermore, if $\epsilon \geqslant 11/32$, $P_{\text{test}}(|\psi\rangle\langle\psi|) \leqslant 501/512$.



# Proof of correctness: plan of attack

- The lower bound is easy: any test using two copies and accepting all product states with certainty must accept $|\psi\rangle$ with probability at least $(1-\epsilon)^2$.

# Proof of correctness: plan of attack

- The lower bound is easy: any test using two copies and accepting all product states with certainty must accept $|\psi\rangle$ with probability at least $(1-\epsilon)^2$.

- The upper bound for states close to product is based on writing $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$, allowing us to calculate $\sum_S \operatorname{tr} \psi_S^2$ explicitly in terms of $\epsilon$, $|\phi\rangle$.

# Proof of correctness: plan of attack

- The lower bound is easy: any test using two copies and accepting all product states with certainty must accept $|\psi\rangle$ with probability at least $(1-\epsilon)^2$.

- The upper bound for states close to product is based on writing $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$, allowing us to calculate $\sum_S \operatorname{tr} \psi_S^2$ explicitly in terms of $\epsilon$, $|\phi\rangle$.

- The upper bound for states far from product is based on showing that one can find a $k$-partition such that the distance from the closest product state (wrt this partition) falls into the regime where the first upper bound works.

# Optimality of the product test

Can we do better than the product test?

# Optimality of the product test

Can we do better than the product test?

**Theorem**

- No non-trivial test can use only one copy of $|\psi\rangle$.
- The product test is optimal among all tests that use two copies of $|\psi\rangle$ and accept product states with certainty.

# Optimality of the product test

Can we do better than the product test?

**Theorem**

- No non-trivial test can use only one copy of $|\psi\rangle$.
- The product test is optimal among all tests that use two copies of $|\psi\rangle$ and accept product states with certainty.

How bad is our analysis of the product test?

# Optimality of the product test

Can we do better than the product test?

**Theorem**

- No non-trivial test can use only one copy of $|\psi\rangle$.
- The product test is optimal among all tests that use two copies of $|\psi\rangle$ and accept product states with certainty.

How bad is our analysis of the product test?

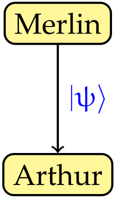
**Theorem**

- The leading order constants cannot be improved.
- There is a state $|\psi\rangle$ which is arbitrarily far from product and has $P_{\text{test}}(|\psi\rangle\langle\psi|) \approx 1/2$.

So (informally) these results can't be improved much without adding dependence on $n$ or $d$.

# Quantum Merlin-Arthur games

The complexity class QMA is the quantum analogue of NP.




- Arthur has some decision problem of size $n$ to solve, and Merlin wants to convince him that the answer is "yes".
- Merlin sends him a quantum state $|\psi\rangle$ of $\text{poly}(n)$ qubits. Arthur runs some polynomial-time quantum algorithm $\mathcal{A}$ on $|\psi\rangle$ and his input and outputs "yes" if the algorithm says "accept".

# Quantum Merlin-Arthur games

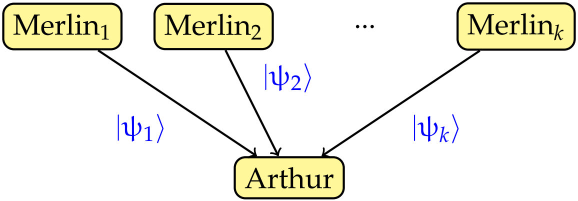
We say that the language $L$ (where $L$ is the set of bit strings we want to accept) is in QMA if there is an $\mathcal{A}$ such that, for all $x$:

- **Completeness:** If $x \in L$, there exists a witness $|\psi\rangle$, a state of poly$(n)$ qubits, such that $\mathcal{A}$ outputs "accept" with probability at least $2/3$ on input $|x\rangle|\psi\rangle$.
- **Soundness:** If $x \notin L$, then $\mathcal{A}$ outputs "accept" with probability at most $1/3$ on input $|x\rangle|\psi\rangle$, for all states $|\psi\rangle$.

The constants $1/3$ and $2/3$ can be amplified to be exponentially close to 0 and 1, respectively.

# Quantum Merlin-Arthur games

QMA($k$) is a variant where Arthur has access to $k$ unentangled Merlins.




This might be more powerful than QMA because the lack of entanglement helps Arthur tell when the Merlins are cheating.

# Quantum Merlin-Arthur games

A language $L$ is in $\mathrm{QMA}(k)_{s,c}$ if there is an $\mathcal{A}$ such that, for all $x$:

- **Completeness:** If $x \in L$, there exist $k$ witnesses $|\psi_1\rangle, \ldots, |\psi_k\rangle$, each a state of $\mathrm{poly}(n)$ qubits, such that $\mathcal{A}$ outputs "accept" with probability at least $c$ on input $|x\rangle|\psi_1\rangle \ldots |\psi_k\rangle$.

- **Soundness:** If $x \notin L$, then $\mathcal{A}$ outputs "accept" with probability at most $s$ on input $|x\rangle|\psi_1\rangle \ldots |\psi_k\rangle$, for all states $|\psi_1\rangle, \ldots, |\psi_k\rangle$.

Also define $\mathrm{QMA}_m(k)_{s,c}$ to indicate that $|\psi_1\rangle, \ldots, |\psi_k\rangle$ each involve $m$ qubits, where $m$ may be a function of $n$ other than $\mathrm{poly}(n)$.

# What can we do with $k$ Merlins?

**Theorem [Aaronson et al '08]**

Given a boolean CNF formula with $n$ clauses, Arthur can decide in poly$(n)$ time whether it's satisfiable, given $O(\sqrt{n}\,\mathrm{polylog}(n))$ unentangled quantum proofs of $O(\log n)$ qubits each.

# What can we do with $k$ Merlins?

**Theorem [Aaronson et al '08]**

Given a boolean CNF formula with $n$ clauses, Arthur can decide in poly$(n)$ time whether it's satisfiable, given $O(\sqrt{n}\,\mathrm{polylog}(n))$ unentangled quantum proofs of $O(\log n)$ qubits each.

Arthur's algorithm always accepts satisfiable formulae (perfect completeness) and rejects unsatisfiable formulae with constant probability (constant soundness).

In complexity-theoretic language:

$$SAT \subseteq \mathrm{QMA}_{\log}(\sqrt{n}\,\mathrm{polylog}(n))_{\Omega(1),1}$$

# Replacing $k$ Merlins with 2 Merlins

- Our results imply that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ (that is, $k$ Merlins can be replaced with 2 Merlins), up to a constant loss of soundness.

# Replacing $k$ Merlins with 2 Merlins

- Our results imply that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ (that is, $k$ Merlins can be replaced with 2 Merlins), up to a constant loss of soundness.

- The idea: given two (unentangled) copies of the $k$ proofs, Arthur can use the product test to certify that the proofs are actually unentangled.

- So we go from having $k$ proofs of $m$ qubits each to having 2 proofs of $km$ qubits each.

# Replacing $k$ Merlins with 2 Merlins

- Our results imply that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ (that is, $k$ Merlins can be replaced with 2 Merlins), up to a constant loss of soundness.

- The idea: given two (unentangled) copies of the $k$ proofs, Arthur can use the product test to certify that the proofs are actually unentangled.

- So we go from having $k$ proofs of $m$ qubits each to having 2 proofs of $km$ qubits each.

- Use of the product test seems to limit us to constant soundness (as even highly entangled states can be accepted with constant probability).

# Replacing $k$ Merlins with 2 Merlins

Imagine Arthur's QMA($k$) verification algorithm is $\mathcal{A}$, and the original proofs are $|\psi_1\rangle, \dots, |\psi_k\rangle$. Then the QMA(2) protocol is:

1. Each of the two Merlins sends $|\psi_1\rangle \otimes \dots \otimes |\psi_k\rangle$ 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.

# Replacing $k$ Merlins with 2 Merlins

Imagine Arthur's QMA($k$) verification algorithm is $\mathcal{A}$, and the original proofs are $|\psi_1\rangle, \ldots, |\psi_k\rangle$. Then the QMA(2) protocol is:

1. Each of the two Merlins sends $|\psi_1\rangle \otimes \ldots \otimes |\psi_k\rangle$ 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.

Intuitively: if the product test passes with high probability, the states were close to product, so the QMA($k$) algorithm works.

# From QMA(2) to hardness results

- Our results show that satisfiability of CNF formulae can be verified by a quantum algorithm with constant probability, given two unentangled proofs of length $O(\sqrt{n}\,\mathrm{polylog}(n))$ qubits each.

# From QMA(2) to hardness results

- Our results show that satisfiability of CNF formulae can be verified by a quantum algorithm with constant probability, given two unentangled proofs of length $O(\sqrt{n}\,\mathrm{polylog}(n))$ qubits each.
- We can turn this round and obtain hardness results for problems relating to QMA(2).

# From $\mathrm{QMA}(2)$ to hardness results

- Our results show that satisfiability of CNF formulae can be verified by a quantum algorithm with constant probability, given two unentangled proofs of length $O(\sqrt{n}\,\mathrm{polylog}(n))$ qubits each.
- We can turn this round and obtain hardness results for problems relating to $\mathrm{QMA}(2)$.
- Imagine we could (classically) estimate the success probability of a $\mathrm{QMA}(2)$ protocol that uses witnesses of dimension $d$, up to a constant, in time $\mathrm{poly}(d)$.
- Then this would give a subexponential-time ($2^{O(\sqrt{n}\,\mathrm{polylog}(n))}$) algorithm for SAT!

We show hardness results, based on the assumption that this isn't possible (the Exponential Time Hypothesis **(ETH)**).

# Hardness of estimating minimum output entropy

Let $\mathcal{N}$ be a quantum channel (CPTP map). Then the maximum output $p$-norm of $\mathcal{N}$ is

$$\|\mathcal{N}\|_p = \max_{\rho} \|\mathcal{N}(\rho)\|_p,$$

where

$$\|\rho\|_p = (\operatorname{tr} \rho^p)^{1/p}.$$

The minimum output Rényi $\alpha$-entropy is

$$S_\alpha(\mathcal{N}) = \frac{\alpha}{1-\alpha} \log \|\mathcal{N}\|_\alpha.$$

As $\alpha \to 1$, we obtain the minimum output von Neumann entropy, which is closely related to channel capacity.

# Hardness of estimating minimum output entropy

- The maximum acceptance probability of a QMA(2) protocol is precisely $\|\mathcal{N}\|_\infty$ for some quantum channel $\mathcal{N}$!

# Hardness of estimating minimum output entropy

- The maximum acceptance probability of a QMA(2) protocol is precisely $\|\mathcal{N}\|_\infty$ for some quantum channel $\mathcal{N}$!
- This implies that there is some constant $c$ such that, given a channel $\mathcal{N}$, there is no polynomial-time algorithm to distinguish between $S_\alpha(\mathcal{N}) = 0$ and $S_\alpha(\mathcal{N}) \geqslant c$, assuming **(ETH)**.

# Hardness of estimating minimum output entropy

- The maximum acceptance probability of a $\mathrm{QMA}(2)$ protocol is precisely $\|\mathcal{N}\|_\infty$ for some quantum channel $\mathcal{N}$!
- This implies that there is some constant $c$ such that, given a channel $\mathcal{N}$, there is no polynomial-time algorithm to distinguish between $S_\alpha(\mathcal{N}) = 0$ and $S_\alpha(\mathcal{N}) \geqslant c$, assuming **(ETH)**.
- This improves a result by [Beigi, Shor '07], who proved this for accuracy $1/\operatorname{poly}(d)$ (but with weaker complexity assumptions).

# Hardness of estimating minimum output entropy

- The maximum acceptance probability of a QMA(2) protocol is precisely $\|\mathcal{N}\|_\infty$ for some quantum channel $\mathcal{N}$!

- This implies that there is some constant $c$ such that, given a channel $\mathcal{N}$, there is no polynomial-time algorithm to distinguish between $S_\alpha(\mathcal{N}) = 0$ and $S_\alpha(\mathcal{N}) \geqslant c$, assuming **(ETH)**.

- This improves a result by [Beigi, Shor '07], who proved this for accuracy $1/\operatorname{poly}(d)$ (but with weaker complexity assumptions).

- This also implies that certain approaches for proving "weak" additivity theorems won't work...

# Hardness of separability testing

- Recall that it's NP-hard to distinguish between bipartite $d \times d$ mixed states that are separable, and those that are $1/\operatorname{poly}(d)$ far from separable.

# Hardness of separability testing

- Recall that it's NP-hard to distinguish between bipartite $d \times d$ mixed states that are separable, and those that are $1/\text{poly}(d)$ far from separable.

- Our results imply that it's hard to estimate the set SEP of separable $d \times d$ states by a convex set within constant trace distance of SEP, assuming **(ETH)**.

# Hardness of separability testing

- Recall that it's NP-hard to distinguish between bipartite $d \times d$ mixed states that are separable, and those that are $1/\text{poly}(d)$ far from separable.

- Our results imply that it's hard to estimate the set SEP of separable $d \times d$ states by a convex set within constant trace distance of SEP, assuming **(ETH)**.

- Why? Because (roughly) if we can detect membership in this set, we can optimise over it, so we can approximate the success probability of a $\text{QMA}(2)$ protocol.

# Hardness of separability testing

- Recall that it's NP-hard to distinguish between bipartite $d \times d$ mixed states that are separable, and those that are $1/\mathrm{poly}(d)$ far from separable.

- Our results imply that it's hard to estimate the set SEP of separable $d \times d$ states by a convex set within constant trace distance of SEP, assuming **(ETH)**.

- Why? Because (roughly) if we can detect membership in this set, we can optimise over it, so we can approximate the success probability of a $\mathrm{QMA}(2)$ protocol.

- So easy detection of pure state entanglement implies hardness of detecting mixed state entanglement!

# Conclusions

- The product test is an efficient test for pure product states of $n$ quantum systems.

- The product test ties together many concepts in quantum information theory and proves computational hardness of several information-theoretic tasks.

- Quantum information theory and quantum computation are intimately linked.

# Open questions

- Can QMA(2) protocols be amplified to exponentially small error?

- Can stability of other output entropies be proven for the depolarising channel – or for all channels where additivity holds?

- Can the constants in our proof be improved? (Yes.)

# Open questions

- Can QMA(2) protocols be amplified to exponentially small error?
- Can stability of other output entropies be proven for the depolarising channel – or for all channels where additivity holds?
- Can the constants in our proof be improved? (Yes.)

Further reading: **arXiv:1001.0017**

# Open questions

- Can QMA(2) protocols be amplified to exponentially small error?

- Can stability of other output entropies be proven for the depolarising channel – or for all channels where additivity holds?

- Can the constants in our proof be improved? (Yes.)

Further reading: **arXiv:1001.0017**

Thanks for your time!

# The upper bound

The map of the first part of the proof:

- Let $|0^n\rangle$ be the closest product state to $|\psi\rangle$.
- Write $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$.

# The upper bound

The map of the first part of the proof:

- Let $|0^n\rangle$ be the closest product state to $|\psi\rangle$.
- Write $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$.
- This allows us to calculate $\sum_S \operatorname{tr}\psi_S^2$ explicitly in terms of $\epsilon$, $|\phi\rangle$.

# The upper bound

The map of the first part of the proof:

- Let $|0^n\rangle$ be the closest product state to $|\psi\rangle$.
- Write $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$.
- This allows us to calculate $\sum_S \operatorname{tr}\psi_S^2$ explicitly in terms of $\epsilon$, $|\phi\rangle$.
- Writing $|\phi\rangle = \sum_x \alpha_x |x\rangle$, can upper bound $\sum_S \operatorname{tr}\psi_S^2$ in terms of how much weight $|\phi\rangle$ has on low Hamming weight basis states.

# The upper bound

The map of the first part of the proof:

- Let $|0^n\rangle$ be the closest product state to $|\psi\rangle$.
- Write $|\psi\rangle = \sqrt{1-\epsilon}\,|0^n\rangle + \sqrt{\epsilon}\,|\phi\rangle$ for some $|\phi\rangle$.
- This allows us to calculate $\sum_S \operatorname{tr} \psi_S^2$ explicitly in terms of $\epsilon$, $|\phi\rangle$.
- Writing $|\phi\rangle = \sum_x \alpha_x |x\rangle$, can upper bound $\sum_S \operatorname{tr} \psi_S^2$ in terms of how much weight $|\phi\rangle$ has on low Hamming weight basis states.
- Showing that there can be no weight on states of Hamming weight 1 completes the proof.

# The second part of the proof

The first part of the proof ends up showing

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

This bound is greater than 1 for large $\epsilon$!

# The second part of the proof

The first part of the proof ends up showing

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

This bound is greater than 1 for large $\epsilon$!

We fix up the proof by showing (roughly):

- $P_{\text{test}}(|\psi\rangle\langle\psi|)$ is upper bounded by the probability that the product test across any partition into $k$ parties passes.

# The second part of the proof

The first part of the proof ends up showing

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

This bound is greater than 1 for large $\epsilon$!

We fix up the proof by showing (roughly):

- $P_{\text{test}}(|\psi\rangle\langle\psi|)$ is upper bounded by the probability that the product test across any partition into $k$ parties passes.
- If $|\psi\rangle$ is far from product across the $n$ subsystems, one can find a $k$-partition such that the distance from the closest product state (wrt this partition) falls into the regime where the first part of the proof works.

# The second part of the proof

The first part of the proof ends up showing

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

This bound is greater than 1 for large $\epsilon$!

We fix up the proof by showing (roughly):

- $P_{\text{test}}(|\psi\rangle\langle\psi|)$ is upper bounded by the probability that the product test across any partition into $k$ parties passes.
- If $|\psi\rangle$ is far from product across the $n$ subsystems, one can find a $k$-partition such that the distance from the closest product state (wrt this partition) falls into the regime where the first part of the proof works.
- This leads to the result that, if $\epsilon \geqslant 11/32$, $P_{\text{test}}(|\psi\rangle\langle\psi|) \leqslant 501/512$.

These constants can clearly be improved somewhat...

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1-\delta$, i.e.

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

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1 - \delta$, i.e.

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

It turns out that

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}(\rho))^2 \propto \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr}\rho_S^2,$$

for some constant $\gamma$ depending on $\delta$ and $d$.

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1 - \delta$, i.e.

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

It turns out that

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}(\rho))^2 \propto \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr} \rho_S^2,$$

for some constant $\gamma$ depending on $\delta$ and $d$.

An interpretation of (a generalisation of) our main result is:

- For small enough $\delta$...

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1 - \delta$, i.e.

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

It turns out that

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}(\rho))^2 \propto \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr}\rho_S^2,$$

for some constant $\gamma$ depending on $\delta$ and $d$.

An interpretation of (a generalisation of) our main result is:

- For small enough $\delta$...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes n} |\psi\rangle\langle\psi|)^2 \geqslant (1-\epsilon)P_{\text{prod}}(\delta)$...

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1-\delta$, i.e.

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

It turns out that

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}(\rho))^2 \propto \sum_{S\subseteq[n]} \gamma^{|S|} \operatorname{tr}\rho_S^2,$$

for some constant $\gamma$ depending on $\delta$ and $d$.

An interpretation of (a generalisation of) our main result is:

- For small enough $\delta$...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}|\psi\rangle\langle\psi|)^2 \geqslant (1-\epsilon)P_{\text{prod}}(\delta)$...
- ...there is a product state $|\phi_1,\dots,\phi_n\rangle$ such that $|\langle\psi|\phi_1,\dots,\phi_n\rangle|^2 \geqslant 1-O(\epsilon)$.

# The depolarising channel

Consider the qudit depolarising channel with noise rate $1 - \delta$, i.e.

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

It turns out that

$$\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}(\rho))^2 \propto \sum_{S \subseteq [n]} \gamma^{|S|} \operatorname{tr}\rho_S^2,$$

for some constant $\gamma$ depending on $\delta$ and $d$.

An interpretation of (a generalisation of) our main result is:

- For small enough $\delta$...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes n}|\psi\rangle\langle\psi|)^2 \geqslant (1-\epsilon)P_{\text{prod}}(\delta)$...
- ...there is a product state $|\phi_1, \dots, \phi_n\rangle$ such that $|\langle\psi|\phi_1, \dots, \phi_n\rangle|^2 \geqslant 1 - O(\epsilon)$.

This is a stability result for this channel.

# Correctness and amplification

- It's immediate that, if the Merlins don't cheat, Arthur will accept with the same probability as the $\mathrm{QMA}(k)$ protocol does.

# Correctness and amplification

- It's immediate that, if the Merlins don't cheat, Arthur will accept with the same probability as the $\mathrm{QMA}(k)$ protocol does.
- One can show that the Merlins can't increase their success probability by sending different states.

# Correctness and amplification

- It's immediate that, if the Merlins don't cheat, Arthur will accept with the same probability as the QMA($k$) protocol does.
- One can show that the Merlins can't increase their success probability by sending different states.
- If the product test accepts, the state must be close to product, so correctness of the QMA($k$) protocol implies correctness of the QMA(2) protocol.

# Correctness and amplification

- It's immediate that, if the Merlins don't cheat, Arthur will accept with the same probability as the QMA($k$) protocol does.
- One can show that the Merlins can't increase their success probability by sending different states.
- If the product test accepts, the state must be close to product, so correctness of the QMA($k$) protocol implies correctness of the QMA(2) protocol.
- This also implies that QMA(2) protocols can be amplified up to constant soundness by taking $k$ unentangled copies of the proofs.

# Correctness and amplification

- It's immediate that, if the Merlins don't cheat, Arthur will accept with the same probability as the QMA($k$) protocol does.
- One can show that the Merlins can't increase their success probability by sending different states.
- If the product test accepts, the state must be close to product, so correctness of the QMA($k$) protocol implies correctness of the QMA(2) protocol.
- This also implies that QMA(2) protocols can be amplified up to constant soundness by taking $k$ unentangled copies of the proofs.
- Whether they can be amplified to exponentially small soundness remains an open question...