A quantum e-meter

Detecting pure entanglement is easy, so detecting mixed entanglement is hard

Aram Harrow (University of Washington)
and
Ashley Montanaro (University of Cambridge)

arXiv:1001.0017

Waterloo IQC
9 Apr, 2012

Outline

1. Testing pure state entanglement is easy

2. Testing mixed-state entanglement is hard

The basic problem

Given a quantum state, is it entangled?

The basic problem

Given a quantum state, is it entangled?

This can mean two different things:

- Pure product states are of the form

$$|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes \cdots |\psi_k\rangle\langle\psi_k|.$$

  For pure states, entangled = not product.

- Sep= {Separable states} = convex hull of product states. For mixed states, entangled = not separable.

Variants

- Pure- or mixed-state entanglement?
- Are we given 1 copy, k copies, or an explicit description?
- Bipartite or multipartite?
- How much accuracy is necessary?
- Are we detecting entanglement in general or verifying a specific state?

Variants

- Pure- or mixed-state entanglement?
- Are we given 1 copy, k copies, or an explicit description?
- Bipartite or multipartite?
- How much accuracy is necessary?
- Are we detecting entanglement in general or verifying a specific state?

This talk

1. Pure state, two copies, constant accuracy
2. Mixed state, explicit description, constant accuracy

Our main result

Let $|\psi\rangle \in \mathbb{C}^{d^k}$ be a pure state on k d-dimensional systems and

$$1 - \epsilon = \max \left\{ |\langle\psi|\phi\rangle|^2 : |\phi\rangle \text{ is a product state} \right\}.$$

Theorem

There exists a product test which, given $|\psi\rangle \otimes |\psi\rangle$, accepts with probability $1 - \Theta(\epsilon)$.

Our main result

Let $|\psi\rangle \in \mathbb{C}^{d^k}$ be a pure state on k d-dimensional systems and

$$1 - \epsilon = \max\left\{ |\langle\psi|\phi\rangle|^2 : |\phi\rangle \text{ is a product state} \right\}.$$

Theorem

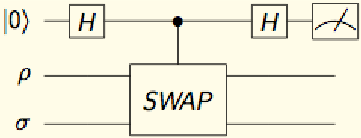
There exists a product test which, given $|\psi\rangle \otimes |\psi\rangle$, accepts with probability $1 - \Theta(\epsilon)$.

- Note: no dependence on k or d.
- The test takes time $O(k \log d)$.
- One copy of $|\psi\rangle$ contains no information about ϵ.
- Our test is optimal among all tests that always accept product states.
- It was previously proposed by [Mintert-Kuś-Buchleitner '05] and implemented experimentally by [Walborn *et al* '06]. Our theorem was conjectured by [Montanaro-Osborne '09].

Key primitive

[Buhrman-Cleve-Watrous-de Wolf, Phys. Rev. Lett. '01]

SWAP test



Accept if the outcome of the measurement is "0", reject if not.

The probability of accepting is $\frac{1+\text{tr}\,\rho\sigma}{2}$.

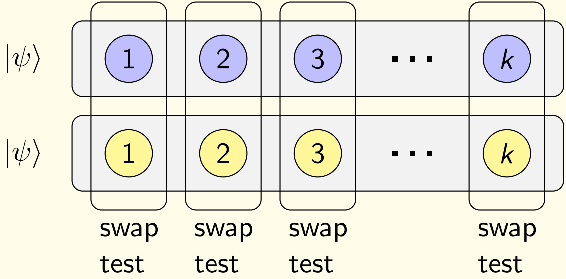
If $\rho = \sigma$, then this is related to $\text{tr}\,\rho^2$, which is the purity of ρ.

John Travolta - Actor, OT III, currently on his False Purpose Rundown counselling.

As demonstrated by John Travolta.

Testing productness

Product test algorithm



Accept iff all n swap tests pass.

Why it works: If $|\psi\rangle$ is entangled, some of its subsystems must be mixed and so some swap tests are likely to fail.

Maximum vs. average entanglement

Lemma

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

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

Maximum vs. average entanglement

Lemma

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

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

- Measures average purity of the input $|\psi\rangle$ across bipartitions.
- $P_{\text{test}}(\rho) = 1$ if and only if ρ is a pure product state.
- Main result rephrased: "If the average entanglement across bipartitions of $|\psi\rangle$ is low, $|\psi\rangle$ must be close to a product state."
- Similarly $P_{\text{test}}(\rho)$ is related to
  - The average overlap of ρ with a random product state.
  - The purity of $D_{1/\sqrt{d+1}}^{\otimes k}(\rho)$.

Generalization: stability of the depolarizing channel

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

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

Generalization: stability of the depolarizing channel

Consider the qudit depolarizing 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

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

for some constant γ depending on δ and d.

Generalization: stability of the depolarizing channel

Consider the qudit depolarizing 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

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

for some constant γ depending on δ and d.
A generalized version of our main result is that:

- For small enough δ...

Generalization: stability of the depolarizing channel

Consider the qudit depolarizing 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

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

for some constant γ depending on δ and d.
A generalized version of our main result is that:

- For small enough δ...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes k}\,|\psi\rangle\langle\psi|)^2 \geq (1-\epsilon)\operatorname{tr}((\mathcal{D}_\delta(|0\rangle\langle 0|)^{\otimes k})^2$...

Generalization: stability of the depolarizing channel

Consider the qudit depolarizing 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

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

for some constant γ depending on δ and d.
A generalized version of our main result is that:

- For small enough δ...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes k} |\psi\rangle\langle\psi|)^2 \geq (1-\epsilon)\operatorname{tr}((\mathcal{D}_\delta(|0\rangle\langle 0|)^{\otimes k})^2$...
- ...there is a product state $|\phi_1, \dots, \phi_k\rangle$ such that $|\langle\psi|\phi_1, \dots, \phi_k\rangle|^2 \geq 1 - O(\epsilon)$.

Generalization: stability of the depolarizing channel

Consider the qudit depolarizing 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

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

for some constant γ depending on δ and d.
A generalized version of our main result is that:

- For small enough δ...
- ...if $\operatorname{tr}(\mathcal{D}_\delta^{\otimes k}\,|\psi\rangle\langle\psi|)^2 \geq (1-\epsilon)\operatorname{tr}((\mathcal{D}_\delta(|0\rangle\langle 0|)^{\otimes k})^2$...
- ...there is a product state $|\phi_1,\dots,\phi_k\rangle$ such that $|\langle\psi|\phi_1,\dots,\phi_k\rangle|^2 \geq 1-O(\epsilon)$.

This is a stability result for this channel.

Outline

1. Testing pure state entanglement is easy

2. Testing mixed-state entanglement is hard

Separable states

Definition

$\text{Sep}^k(d) := \text{conv}\{\psi_1 \otimes \cdots \otimes \psi_k : |\psi_1\rangle, \ldots, |\psi_k\rangle \in S(\mathbb{C}^d)\}$
$\psi := |\psi\rangle\langle\psi|$ *and* $S(\mathbb{C}^d) :=$ *unit vectors.*

Separable states

Definition

$\text{Sep}^k(d) := \text{conv}\{\psi_1 \otimes \cdots \otimes \psi_k : |\psi_1\rangle, \ldots, |\psi_k\rangle \in S(\mathbb{C}^d)\}$
$\psi := |\psi\rangle\langle\psi|$ *and* $S(\mathbb{C}^d)$:= *unit vectors.*

Two related tasks

1. Weak membership: Given ρ and the promise that either $\rho \in \text{Sep}^k(d)$ or ρ is ϵ-far from $\text{Sep}^k(d)$, determine which is the case.
2. Weak optimization: Given $0 \leq M \leq I$, approximately compute

$$h_{\text{Sep}^k(d)}(M) := \max_{\rho \in \text{Sep}^k(d)} \text{tr}\, M\rho.$$

Approximate equivalence proved by [Grötschel-Lovász-Schrijver], [Liu: 0712.3041] and [Gharibian: 0810.4507].

TFA≈E

- Estimating $h_{\mathrm{Sep}^2(d)}(\cdot)$.
- Weak membership for $h_{\mathrm{Sep}^2(d)}$.
- $\mathrm{QMA}_{\log}(2)_{1-\epsilon,1}$
- Computing $\max \sum_{i,j,k} A_{ijk} x_i y_j z_k$ over unit vectors $\vec{x}, \vec{y}, \vec{z}$.
- Estimating the minimum entanglement of any state in a subspace of a bipartite space.
- Estimating the capacity or minimum output entropy of a noisy quantum channel.
- Estimating superoperator norms.
- Estimating the ground-state energy of a mean-field Hamiltonian.

Mean-field Hamiltonians

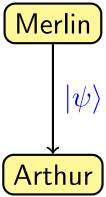
For $M \in \mathcal{L}(\mathbb{C}^d \otimes \mathbb{C}^d)$, define $H \in \mathcal{L}((\mathbb{C}^d)^{\otimes n})$ by

$$H = \frac{-1}{n(n-1)} \sum_{1 \leq i \neq j \leq n} M^{(i,j)}.$$

[Fannes-Vanderplas; quant-ph/0605216] showed that the ground state energy is $\approx - \max_{\rho \in \mathrm{Sep}} \operatorname{tr} M\rho = -h_{\mathrm{Sep}^2(d)}(M)$.

Quantum Merlin-Arthur games

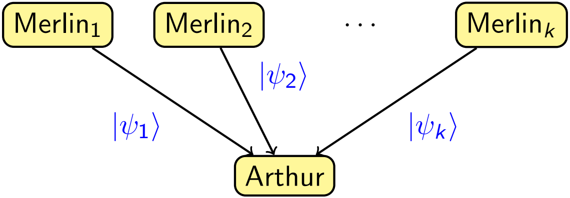
The complexity class QMA is like NP but with a quantum proof and a quantum poly-time verifier, and with some probability of error allowed.



- Completeness: For YES instances, there exists a witness $|\psi\rangle$ that Arthur accepts with probability $\geq c$.
- Soundness: For NO instances, there is no witness $|\psi\rangle$ that Arthur accepts with probability $\geq s$.
- What this means: Arthur's measurement is parametrized by the input, and Merlin is trying to convince Arthur to accept.

Quantum Merlin-Arthur games

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



More generally, $\text{QMA}_m(k)_{s,c}$ means that there are k messages, each with m qubits (i.e. dimension 2^m).

$\mathsf{QMA}_m(k)$ as an optimization problem

Arthur's measurement is a 2^{km}-dimensional matrix M with $0 \leq M \leq I$.

$\mathsf{QMA}_m(k)_{s,c}$ = determine whether

$$\max_{|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle} \langle\psi|M|\psi\rangle$$

is $\geq c$ or $\leq s$.

When $k = 1$, this is an eigenvalue problem with a $\exp(m)$-time algorithm.

For $k > 1$, this problem is to estimate

$$h_{\mathrm{Sep}^k(2^m)}(M)$$

When $k = 2$, no $\exp(m)$ time algorithm is known, so even $\mathsf{QMA}_{\log}(2)$ is not likely to be in BQP.

Hardness? Algorithms?

Input: $0 \leq M \leq I$.

1. NP-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 1/n^{1.01}$.
   [Gurvits, Blier-Tapp, Gharibian, Hillar-Lim, Le Gall-Nakagawa-Nishimura]

Hardness? Algorithms?

Input: $0 \leq M \leq I$.

1. NP-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 1/n^{1.01}$.
   [Gurvits, Blier-Tapp, Gharibian, Hillar-Lim, Le Gall-Nakagawa-Nishimura]
2. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon \operatorname{tr} M$.
   - Runs in time $n^{\mathrm{poly}(1/\epsilon)}$.
   - [de la Vega *et al.*](see also [Shi-Wu; 1112.0808])

Hardness? Algorithms?

Input: $0 \leq M \leq I$.

1. NP-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 1/n^{1.01}$.
   [Gurvits, Blier-Tapp, Gharibian, Hillar-Lim, Le Gall-Nakagawa-Nishimura]
2. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon \operatorname{tr} M$.
   - Runs in time $n^{\mathrm{poly}(1/\epsilon)}$.
   - [de la Vega *et al.*](see also [Shi-Wu; 1112.0808])
3. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon$
   - Runs in time $n^{O(\log n)/\epsilon^2}$
   - Requires that M is 1-LOCC: i.e. $M = \sum_i A_i \otimes B_i$ with $A_i, B_i \geq 0$, $\sum_i A_i \leq I$, $B_i \leq I$.
   - [Brandão-Christandl-Yard:1010.1750]

Hardness? Algorithms?

Input: $0 \leq M \leq I$.

1. NP-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 1/n^{1.01}$.
   [Gurvits, Blier-Tapp, Gharibian, Hillar-Lim, Le Gall-Nakagawa-Nishimura]
2. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon \, \mathrm{tr}\, M$.
   - Runs in time $n^{\mathrm{poly}(1/\epsilon)}$.
   - [de la Vega *et al.*](see also [Shi-Wu; 1112.0808])
3. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon$
   - Runs in time $n^{O(\log n)/\epsilon^2}$
   - Requires that M is 1-LOCC: i.e. $M = \sum_i A_i \otimes B_i$ with $A_i, B_i \geq 0$, $\sum_i A_i \leq I$, $B_i \leq I$.
   - [Brandão-Christandl-Yard:1010.1750]
4. NP-hard to estimate $h_{\mathrm{Sep}^{\sqrt{n}\,\mathrm{poly}\log n}(n)}(M) \pm 0.99$. [0804.0802]

Hardness? Algorithms?

Input: $0 \leq M \leq I$.

1. NP-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 1/n^{1.01}$.
   [Gurvits, Blier-Tapp, Gharibian, Hillar-Lim, Le Gall-Nakagawa-Nishimura]
2. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon \operatorname{tr} M$.
   - Runs in time $n^{\mathrm{poly}(1/\epsilon)}$.
   - [de la Vega *et al.*](see also [Shi-Wu; 1112.0808])
3. Algorithm to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon$
   - Runs in time $n^{O(\log n)/\epsilon^2}$
   - Requires that M is 1-LOCC: i.e. $M = \sum_i A_i \otimes B_i$ with $A_i, B_i \geq 0$, $\sum_i A_i \leq I$, $B_i \leq I$.
   - [Brandão-Christandl-Yard:1010.1750]
4. NP-hard to estimate $h_{\mathrm{Sep}^{\sqrt{n}\,\mathrm{poly}\log n}(n)}(M) \pm 0.99$. [0804.0802]
5. This work: $\mathrm{NP}_{\log^2}$-hard to estimate $h_{\mathrm{Sep}^2(n)}(M) \pm 0.99$.

Assuming the Exponential Time Hypothesis, this implies an $n^{\tilde{\Omega}(\log(n))}$ lower bound on constant-error approximations to $h_{\mathrm{Sep}^2(n)}(\cdot)$.

What our product test implies about QMA(k)

Theorem (2 provers can simulate k provers)

$\mathrm{QMA}_m(k)_{s=1-\epsilon,c} \subseteq \mathrm{QMA}_{mk}(2)_{1-\frac{\epsilon}{50},c}$

Proof.

- If the QMA(k) protocol had proofs $|\psi_1\rangle, \ldots, |\psi_k\rangle$ then simulate in QMA(2) by asking each prover to submit $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$.
- Then use the product test to verify that they indeed submit product states.

□

What our product test implies about $\mathrm{QMA}(k)$

Theorem (2 provers can simulate k provers)

$\mathrm{QMA}_m(k)_{s=1-\epsilon,c} \subseteq \mathrm{QMA}_{mk}(2)_{1-\frac{\epsilon}{50},c}$

Proof.

- If the $\mathrm{QMA}(k)$ protocol had proofs $|\psi_1\rangle, \ldots, |\psi_k\rangle$ then simulate in $\mathrm{QMA}(2)$ by asking each prover to submit $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$.
- Then use the product test to verify that they indeed submit product states.

□

Corollary: 3-SAT $\in \mathrm{QMA}_{\sqrt{n}\,\mathrm{poly}\log(n)}(2)_{0.99,1}$.

Corollary: Estimating $h_{\mathrm{Sep}^k(d)}(\cdot)$ reduces to estimating $h_{\mathrm{Sep}^2(d^k)}(\cdot)$.

Hardness of separability testing

Let K be a set that approximates $\mathrm{Sep}^2(d)$.

Things we want

1. K is convex.
2. Hausdorff distance from K to $\mathrm{Sep}^2(d)$ is ≤ 0.99.
3. Weak membership for K (with error ϵ) can be performed in time $\mathrm{poly}(d, 1/\epsilon)$.

Corollary

Not all of the above are possible if the Exponential Time Hypothesis holds.

Hardness of separability testing

Let K be a set that approximates $\mathrm{Sep}^2(d)$.

Things we want

1. K is convex.
2. Hausdorff distance from K to $\mathrm{Sep}^2(d)$ is ≤ 0.99.
3. Weak membership for K (with error ϵ) can be performed in time $\mathrm{poly}(d, 1/\epsilon)$.

Corollary

Not all of the above are possible if the Exponential Time Hypothesis holds.

We suspect that the convexity requirement isn't necessary, but don't know how to prove this.

Coming attraction: application to unique games

[Barak, Brandão, H, Kelner, Steurer, Zhou; to appear, STOC 2012]

Small-Set Expansion (SSE) Conjecture

It is NP-hard to distinguish, given an n-vertex graph, whether

1. Some small (size ϵn) set doesn't expand very much.
2. All small sets expand a lot.

Coming attraction: application to unique games

[Barak, Brandão, H, Kelner, Steurer, Zhou; to appear, STOC 2012]

Small-Set Expansion (SSE) Conjecture

It is NP-hard to distinguish, given an n-vertex graph, whether

1. Some small (size ϵn) set doesn't expand very much.
2. All small sets expand a lot.

- The SSE conjecture is roughly equivalent to the Unique Games Conjecture.
- The SSE of a graph can be approximated by the $2 \to 4$ norm of a matrix (defined as $\|A\|_{2\to 4} := \max_x \|Ax\|_4 / \|x\|_2$.)
- Estimating $\|A\|_{2\to 4}$ is equivalent in difficulty to estimating $h_{\mathrm{Sep}^2(n)}(\cdot)$.

Summary

Justifying the title:

Detecting pure-state entanglement is easy.
Therefore detecting mixed-state entanglement is hard.

Summary

Justifying the title:

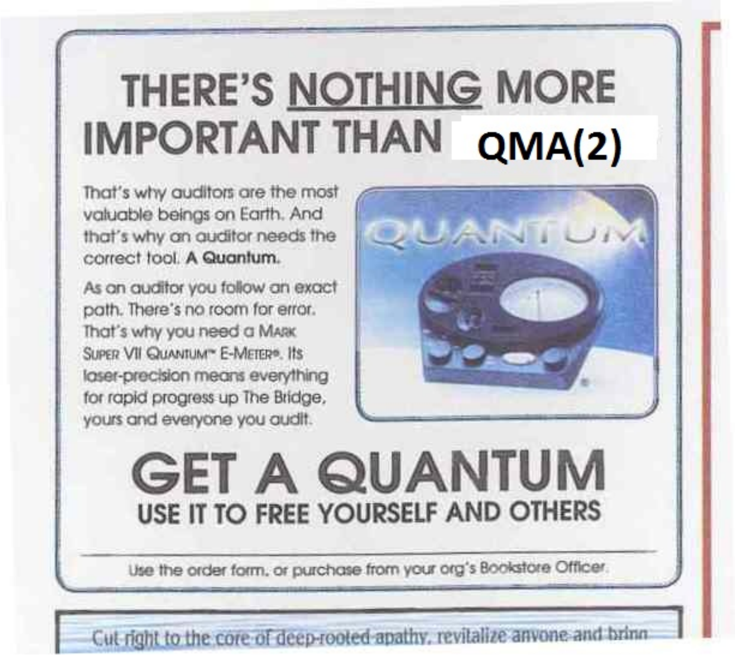
Detecting pure-state entanglement is easy. Therefore detecting mixed-state entanglement is hard.

There are lots of great open questions:

- More progress on small-set expansion/unique games!
- We know $\mathsf{NP}_{\log^2} \subseteq \mathsf{QMA}_{\log}(2)_{1/2,1} \subseteq \mathsf{NP}^{\mathsf{BQP}}$. Which one is tight?
- Similarly the $\mathsf{QMA}_{\mathsf{poly}}(2) \subseteq \mathsf{NEXP}$ bound seems pretty loose.
- Improve our hardness results for weak membership in Sep.
- Estimate $h_{\mathrm{Sep}^2(n)}(M) \pm \epsilon$ in time $n^{O(\log n)/\epsilon^2}$?
- Improve the product test, e.g. in special cases.
- Relate stability to additivity and strong converses.

arXiv:1001.0017

Closing message



THERE'S NOTHING MORE IMPORTANT THAN QMA(2)

That's why auditors are the most valuable beings on Earth. And that's why an auditor needs the correct tool. **A Quantum.**

As an auditor you follow an exact path. There's no room for error. That's why you need a MARK SUPER VII QUANTUM™ E-METER®. Its laser-precision means everything for rapid progress up The Bridge, yours and everyone you audit.

GET A QUANTUM

USE IT TO FREE YOURSELF AND OTHERS

Use the order form, or purchase from your org's Bookstore Officer.

Cut right to the core of deep-rooted apathy, revitalize anyone and brinn