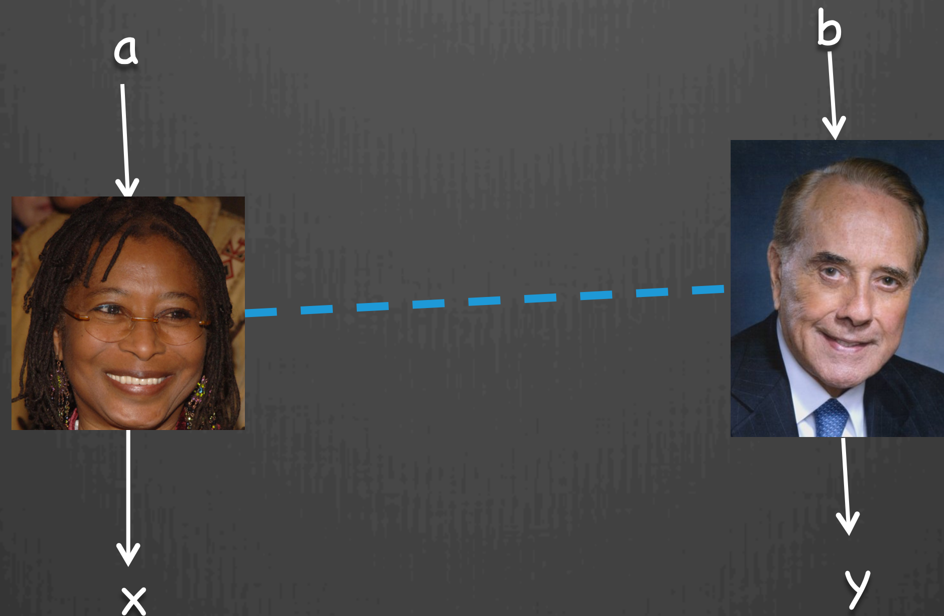
monogamy of non-signalling correlations

Aram Harrow (MIT)
Simons Institute, 27 Feb 2014

based on joint work with
Fernando Brandão (UCL)
arXiv:1210.6367 + ε unpublished

"correlations"

(multipartite conditional probability distributions)



local	$p(x,y\|a,b) = q_A(x\|a)\ q_B(y\|b)$
LHV (local hidden variable)	$p(x,y\|a,b) = \Sigma_r\ \pi(r)\ q_A(x\|a,r)\ q_B(y\|b,r)$
quantum	$p(x,y\|a,b) = \langle\psi\|\ A^a{}_x \otimes B^b{}_y\ \|\psi\rangle$ with $\Sigma_x A^a{}_x = \Sigma_y B^b{}_y = I$
non-signalling	$\Sigma_y\ p(x,y\|a,b) = \Sigma_y\ p(x,y\|a,b')$ $\Sigma_x\ p(x,y\|a,b) = \Sigma_x\ p(x,y\|a',b)$

why study boxes?

Foundational: considering theories more general than quantum mechanics (e.g. Bell's Theorem)

Operational: behavior of quantum states under local measurement (e.g. this work)

Computational: corresponds to constraint-satisfaction problems and multi-prover proof systems.

why non-signalling?

Foundational: minimal assumption for plausible theory

Operational: yields well-defined “partial trace”

$p(x|a) := \Sigma_y\, p(x,y|a,b)$ for any choice of b

Computational: yields efficient linear program

the dual picture: games

<u>Non-local games:</u>
Inputs chosen according to $\mu(a,b)$
Payoff function is $V(x,y|a,b)$
The value of a game using strategy p is
$\Sigma_{x,y,a,b}\, p(x,y|a,b)\ \mu(a,b)\ V(x,y|a,b)$.

<u>Complexity:</u>
classical (local or LHV) value is NP-hard
quantum value has unknown complexity
non-signalling value in P due to linear programming

monogamy

$p(x,y|a,b)$ is k-extendable if there exists a NS box $q(x,y_1,\dots,y_k|a,b_1,\dots,b_k)$ with $q(x,y_i|a,b_i) = p(x,y_i|a,b_i)$ for each i

LHV correlations can be infinitely shared.
This is an alternate definition.

Applications

1. Non-shareability ≅ secrecy
   can be certified by Bell tests

2. Gives a hierarchy of approximations for LHV correlations running in time $\mathrm{poly}(|X|\ |Y|^k\ |A|\ |B|^k)$

3. de Finetti theorems (i.e. k-extendable states ≈ separable)

results

Theorem 1: If p is k-extendable and μ is a distribution on A, then there exists q∈LHV such that

$$\max_b \mathop{\mathbb{E}}_{a\sim\mu} \|p(X,Y|a,b) - q(X,Y|a,b)\|_1 \leq \sqrt{\frac{2\ln|X|}{k}}$$

cf. Terhal-Doherty-Schwab quant-ph/0210053

If $k \geq |B|$ then p∈LHV.

Theorem 2: If $p(x_1,\ldots,x_k|a_1,\ldots,a_k)$ is symmetric, $0<n<k$, and $\mu = \mu_1 \otimes \ldots \otimes \mu_k$ then $\exists\ \nu$ such that

$$\mathop{\mathbb{E}}_{a_1,\ldots,a_n\sim\mu} \|p(X_1,\ldots,X_n|a_1,\ldots,a_n) - \mathop{\mathbb{E}}_{q\sim\nu} q(X_1|a_1)\cdots q(X_n|a_n)\|_1 \leq \sqrt{\frac{2n^2\ln|X|}{k-n}}$$

cf. Christandl-Toner 0712.0916 $\quad \cdots \leq \dfrac{n^2|A|}{k}$

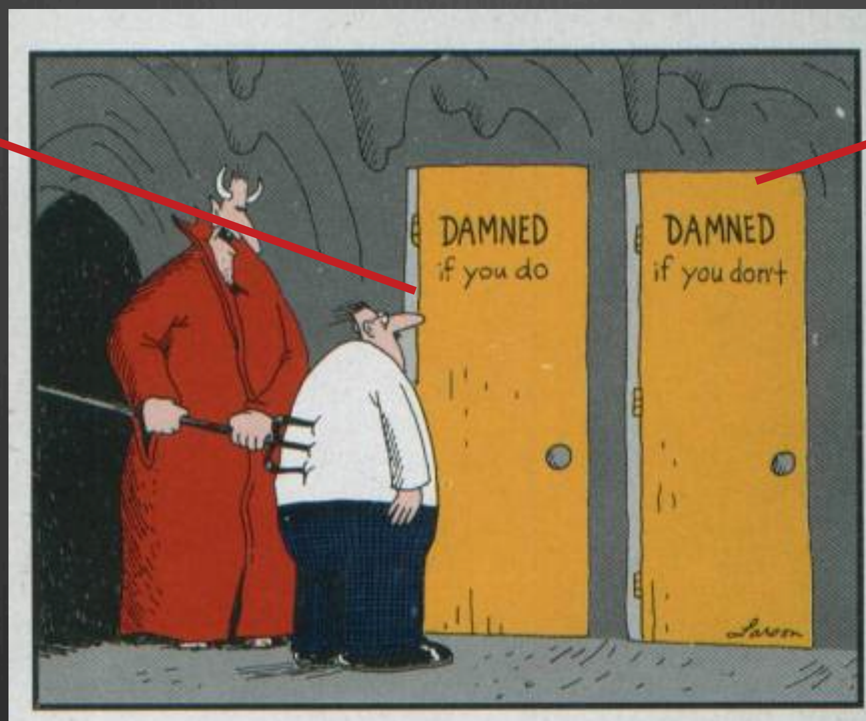
with q independent of μ

proof idea of thm 1

consider extension $p(x,y_1,\dots,y_k|a,b_1,\dots,b_k)$

<u>case 1</u>

$p(x,y_1|a,b_1) \approx$
$p(x|a) \cdot p(y_1|b_1)$



"C'mon, c'mon — it's either one or the other."

<u>case 2</u>

$p(x,y_2|y_1,a,b_1,b_2)$
has less mutual
information

proof sketch of thm 1

$$\begin{aligned}\log|X| &\geq I(X:Y_1,\ldots,Y_k)\\ &= I(X:Y_1)+I(X:Y_2|Y_1)+\ldots+I(X:Y_k|Y_1,\ldots,Y_{k-1})\end{aligned}$$

$\therefore$ for some j we have $I(X:Y_j|Y_1,\ldots,Y_{j-1}) \leq \dfrac{\log|X|}{k}$

$Y_1, \ldots, Y_{j-1}$ constitute a "hidden variable" which we can condition on to leave X, Y_j nearly decoupled.

Trace norm bound follows from Pinsker's inequality.

what about the inputs?

$$\log|X| \geq \max_{b_1,\ldots,b_k} I(X:Y_1,\ldots,Y_k|A,b_1,\ldots,b_k)$$

$$= \max_{b_1,\ldots,b_{k-1}} \Big(I(X:Y_1|A,b_1) + I(X:Y_2|A,b_1,b_2,Y_1) + \ldots +$$

$$I(X:Y_{k-1}|A,b_1,\ldots,b_{k-1},Y_1,\ldots,Y_{k-2}) +$$

$$\boxed{\max_{b_k} I(X:Y_k|A,b_1,\ldots,b_k,Y_1,\ldots,Y_{k-1})}\Big)$$

Apply Pinsker here to show that this is
$\gtrsim \|\, p(X,Y_k \mid A,b_k) - \text{LHV} \,\|_1^2$

then repeat for $Y_{k-1}, \ldots, Y_1$

interlude: Nash equilibria

Non-cooperative games:
Players choose strategies $p^A \in \Delta_m$, $p^B \in \Delta_n$.
Receive values $\langle V_A, p^A \otimes p^B \rangle$ and $\langle V_B, p^A \otimes p^B \rangle$.

Nash equilibrium: neither player can improve own value
ε-approximate Nash: cannot improve value by $> \varepsilon$

Correlated equilibria:
Players follow joint strategy $p^{AB} \in \Delta_{mn}$.
Receive values $\langle V_A, p^{AB} \rangle$ and $\langle V_B, p^{AB} \rangle$.
Cannot improve value by unilateral change.

- Can find in poly(m,n) time with linear programming (LP).
- Nash equilibrium = correlated equilibrum with $p = p^A \otimes p^B$

finding (approximate) Nash eq

Known complexity:
Finding exact Nash eq. is PPAD complete.
Optimizing over exact Nash eq is NP-complete.

Algorithm for ε-approx Nash in time $\exp(\log(m)\log(n)/\varepsilon^2)$
based on enumerating over nets for Δ_m, Δ_n.
Planted clique reduces to optimizing over ε-approx Nash.

New result: Another algorithm for finding
ε-approximate Nash with the same run-time.

(uses k-extendable distributions)

algorithm for approx Nash

Search over $p^{AB_1\ldots B_k} \in \Delta_{mn^k}$
such that the $A{:}B_i$ marginal is a correlated equilibrium conditioned on any values for $B_1, \ldots, B_{i-1}$.

LP, so runs in time poly(mn^k)

<u>Claim</u>: Most conditional distributions are ≈ product.

<u>Proof</u>: $\mathbb{E}_i\ I(A{:}B_i|B_{<i}) \leq \log(m)/k$.
$\therefore$ $k = \log(m)/\varepsilon^2$ suffices.

application: free games

free games: $\mu = \mu_A \otimes \mu_B$

Corollary:
The classical value of a free game can be approximated by optimizing over k-extendable non-signaling strategies.

run-time is polynomial in $|X||A| \exp\left(\frac{\log(|X|)\log(|B||Y|)}{\epsilon^2}\right)$

(independently proved by Aaronson, Impagliazzo, Moshkovitz)

Corollary:
From known hardness results for free games, implies that estimating the value of entangled games with $\sqrt{n}$ players and answer alphabets of size $\exp(\sqrt{n})$ is at least as hard as 3-SAT instances of length n.

application: de Finetti theorems for local measurements

Theorem 1′: If ρ^{AB} is k-extendable and μ is a distribution over quantum operations mapping A to A′, then there exists a separable state σ such that

$$\max_{M_B} \mathop{\mathbb{E}}_{M_A \sim \mu} \|(M_A \otimes M_B)(\rho - \sigma)\|_1 \leq \sqrt{\frac{2 \ln |A'|}{k}}$$

Theorem 2′: If ρ is a symmetric state on $A_1 \ldots A_k$ then there exists a measure ν on single-particle states such that

$$\max_{M_2,\ldots,M_n} \left\| (\mathrm{id} \otimes M_2 \otimes \ldots \otimes M_n)(\rho^{A_1 \ldots A_n} - \mathop{\mathbb{E}}_{\sigma \sim \nu} \sigma^{\otimes n} \right\|_1 \leq \sqrt{\frac{2n^2 \ln |A|}{k-n}}$$

improvements on Brandão-Christandl-Yard 1010.1750
1) A′ dependence. 2) multipartite. 3) explicit. 4) simpler proof

ε-nets vs. info theory

Problem	ε-nets	info theory
approx Nash $\max_{p\in\Delta} p^T A p$	LMM '03	H. '14
free games	AIM '14	Brandão-H '13
$\max_{\rho\in Sep} tr[M\rho]$ QMA(2)	Shi-Wu '11 Brandão '14	BCY '10 Brandão-H '12 BKS '13

general games?

Theorem 1: If p is k-extendable and μ is a distribution on A, then there exists q∈LHV such that

$$\max_b \mathop{\mathbb{E}}_{a\sim\mu} \|p(X,Y|a,b) - q(X,Y|a,b)\|_1 \leq \sqrt{\frac{2\ln|X|}{k}}$$

Can we remove the dependence of q on μ?

Conjecture?: p∈k-ext → ∃q∈LHV such that

$$\max_{a,b} \|p(X,Y|a,b) - q(X,Y|a,b)\|_1 \leq \sqrt{\frac{2\ln|X|}{k}}$$

would imply that non-signalling games (in P) can be used to approximate the classical value of games (NP-hard)

→ (probably) FALSE

general quantum games

Conjecture: If ρ^{AB} is k-extendable, then there exists a separable state σ such that

$$\max_{M_A:A\to X}\ \max_{M_B:B\to Y} \|(M_A \otimes M_B)(\rho - \sigma)\|_1 \leq \sqrt{\frac{2\ln|X|}{k}}$$

Would yield alternate proofs of recent results of Vidick:

- NP-hardness of entangled quantum games with 4 players
- $\mathrm{NEXP} \subseteq \mathrm{MIP}^*$

Proof would require strategies that work for quantum states but not general non-signalling distributions.

application: BellQMA(m)

3-SAT on n variables is believed to require a proof of size $\Omega(n)$ bits or qubits according to the ETH (Exp. Time Hypothesis)

Chen-Drucker 1011.0716 (building on Aaronson et al 0804.0802) gave a 3-SAT proof using $m = n^{1/2}\text{polylog}(n)$ states each with $O(\log(n))$ qubits (promised to be not entangled with each other).

Verifier uses local measurements and classical post-processing.

Our Theorem 2' can simulate this with a $m^2 \log(n)$-qubit proof. Implies $m \geq (n/\log(n))^{1/2}$ or else ETH is false.

other applications

- tomography
  Can do "pretty good tomography" on symmetric states instead of on product states.

- polynomial optimization using SDP hierarchies
  Can optimize certain polynomials over n-dim hypersphere using O(log n) rounds.
  Suggests route to algorithms for unique games and small-set expansion.

- multi-partite separability testing
  can efficiently estimate 1-LOCC distance to Sep

open questions

1. Switch quantifiers and find a separable approximation
   (a) independent of the distribution on measurements
   (b) with error depending on the size of the output.

2. We know the non-signalling version of this is false. Can we find a simple counter-example?

3. Can one proof of size $O(m^2)$ simulate two proofs of size m? i.e. is QMA = QMA(2)?

4. Better de Finetti theorems, perhaps combining with the exponential de Finetti theorems or the post-selection principle.

5. Unify ε-nets and information theory approaches.