Quantum discord in quantum computation

Animesh Datta

Department of Physics, University of Oxford

Quantum Coherence and Decoherence, Benasque, 2010

September 9, 2010

Entanglement is an important resource...

- Teleportation and Superdense Coding
- Quantum Algorithms
  - Deutsch-Jozsa, Simon etc
  - Grover
  - Shor
- Quantum Communications and Cryptography
  - Channel Capacity
  - Security
- Quantum Metrology
  - Heisenberg Limit & beyond
- Rich behavior of condensed matter systems

Entanglement is an important resource...

- Teleportation and Superdense Coding
- Quantum Algorithms
  - Deutsch-Jozsa, Simon etc
  - Grover
  - Shor
- Quantum Communications and Cryptography
  - Channel Capacity
  - Security
- Quantum Metrology
  - Heisenberg Limit & beyond
- Rich behavior of condensed matter systems

But actually...

- *For pure state quantum computation ... the presence of multi-partite entanglement, with a number of parties that increases unboundedly with input size, is necessary if the quantum algorithm is to offer an exponential speed-up over classical computation.*

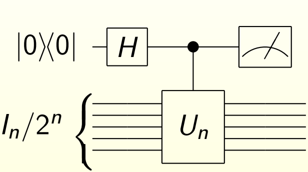
Jozsa & Linden, Proc. R. Soc. Lond. A, **459**, 2011, (2003)

- *An algorithm (quantum system) can be classically efficiently simulated to within a prescribed tolerance η if a suitably small amount of global entanglement (depending on η) is present.*

Vidal, PRL, **91**, 147902, (2003)

Power of one qubit

$$\rho_{n+1} = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & U_n \\ U_n^\dagger & I_n \end{pmatrix}$$



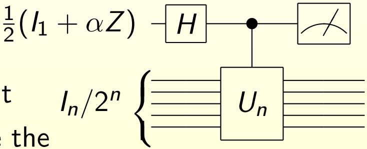
- Measure the top qubit
- $\langle X \rangle = \mathrm{Re}[\mathrm{Tr}(U_n)]/2^n$ and $\langle Y \rangle = \mathrm{Im}[\mathrm{Tr}(U_n)]/2^n$
- Can evaluate $\mathrm{Tr}(U_n)/2^n$ up to a fixed accuracy efficiently
- True only for unitaries that can be represented efficiently by a quantum circuit
- The classical problem is apparently HARD !

Knill & Laflamme, PRL, **81**, 5672, (1998)

sub-unity polarization

If the top qubit is not pure, then

$$\rho_{n+1}(\alpha) = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n \\ \alpha U_n^\dagger & I_n \end{pmatrix}$$

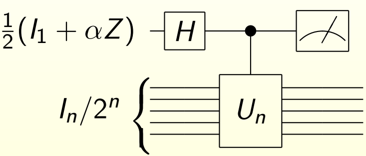


- $\alpha < 1$ makes the evaluation more difficult
- The number of runs required to estimate the normalized trace goes as $L \sim 1/\alpha^2$
- Power of even the tiniest fraction of a qubit
- Tracing out the top qubit leaves the remaining qubits in the completely mixed state

sub-unity polarization

If the top qubit is not pure, then

$$\rho_{n+1}(\alpha) = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n \\ \alpha U_n^\dagger & I_n \end{pmatrix}$$



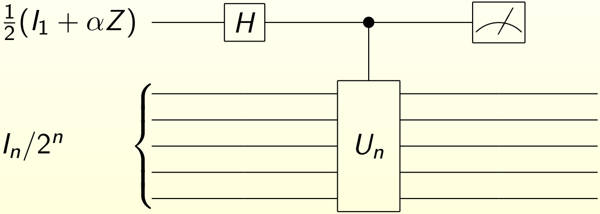
- The top qubit is always separable from the remaining qubits.

$$U_n = \sum_j e^{i\phi_j} |e_j\rangle\langle e_j|$$

$$\rho_{n+1}(\alpha) = \frac{1}{2^{n+1}} \sum_j (|a_j\rangle\langle a_j| + |b_j\rangle\langle b_j|) \otimes |e_j\rangle\langle e_j|$$

- $|a_j\rangle = \cos\theta|0\rangle + e^{i\phi_j}\sin\theta|1\rangle$,
  $|b_j\rangle = \sin\theta|0\rangle + e^{i\phi_j}\cos\theta|1\rangle$, with $\sin 2\theta = \alpha$.

Taking stock...



We have exponential speedup without any entanglement across the most relevant split

AD, Flammia, Caves, PRA, **72**, 042316, (2005)

Let's step back and recall...

- Measure of Ignorance: $H(A)$
- Measure of Correlations : $J(A:B) = H(A) - H(A|B)$.

$$p_a = \sum_b p_{a,b} \qquad p_b = \sum_a p_{a,b}$$

$$p_{a|b=B} = \frac{p_{a,b=B}}{p_{b=B}}$$

Since $H(A|B) = H(A,B) - H(A)$,

$$I(A:B) = H(A) + H(B) - H(A,B)$$

- $I(A:B) = J(A:B)$ for a classical distribution

H is the Shannon entropy

For quantum systems

- With a joint density matrix, ρ_{AB}

$$\mathcal{I}(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

- To get the conditional entropy
  Make projective measurements on a subsystem $\{\Pi_j^B\}$. Then,

$$\rho_{A|\Pi_j^B} = \Pi_j^B \rho_{AB} \Pi_j^B / p_j, \quad p_j = \mathrm{Tr}(\Pi_j^B \rho_{AB} \Pi_j^B)$$

- $J(A:B) = S(\rho_A) - \sum_j p_j S(\rho_{A|\Pi_j^B})$. Then,

$$\begin{aligned} D &= \mathcal{I}(A:B) - J(A:B) \\ &= S(\rho_A) - S(\rho_{AB}) + \sum_j p_j S(\rho_{A|\Pi_j^B}) \end{aligned}$$

For quantum systems

- With a joint density matrix, ρ_{AB}

$$\mathcal{I}(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

- To get the conditional entropy
  Make projective measurements on a subsystem $\{\Pi_j^B\}$. Then,

$$\rho_{A|\Pi_j^B} = \Pi_j^B \rho_{AB} \Pi_j^B / p_j, \quad p_j = \mathrm{Tr}(\Pi_j^B \rho_{AB} \Pi_j^B)$$

- $J(A:B) = S(\rho_A) - \sum_j p_j S(\rho_{A|\Pi_j^B})$. Then,

$$\begin{aligned} D &= \mathcal{I}(A:B) - J(A:B) \\ &= S(\rho_A) - S(\rho_{AB}) + \sum_j p_j S(\rho_{A|\Pi_j^B}) \end{aligned}$$

Dependance on measurements

- Maximum extractable classical information: $\mathcal{J}(A:B) = \max_{\{\Pi_j^B\}} J(A:B)$
- Purely quantum correlations:

$$\begin{aligned} \mathcal{D} &= \mathcal{I}(A:B) - \mathcal{J}(A:B) \\ &= S(\rho_B) - S(\rho_{AB}) + \min_{\{\Pi_j^B\}} \sum_j p_j S(\rho_{A|\Pi_j^B}) \end{aligned}$$

$\mathcal{D}$ is a measure of ‘purely quantum’ correlations

Zurek, Ann. der Physik (Leipzig), **9**, 855 (2000), Ollivier & Zurek, PRL, **88**, 017901, (2002)

Another way of looking at it

A measure for classical correlations $\mathcal{C}$ should be such that

- $\mathcal{C}(\rho) = 0$ if and only if $\rho = \rho_A \otimes \rho_B$
- $\mathcal{C}$ is invariant under local unitary operations
- $\mathcal{C}$ is non-increasing under local operations

Another way of looking at it

A measure for classical correlations $\mathcal{C}$ should be such that

- $\mathcal{C}(\rho) = 0$ if and only if $\rho = \rho_A \otimes \rho_B$
- $\mathcal{C}$ is invariant under local unitary operations
- $\mathcal{C}$ is non-increasing under local operations

$$\mathcal{C}_B(\rho_{AB}) = \max_{\{\mathfrak{P}_i\}} \left\{ S(\rho_A) - \sum_i p_i S(\rho_{A|i}) \right\},$$

$$\rho_{A|i} = \mathrm{Tr}_B(\rho_{AB}\mathfrak{P}_i)/p_i, \quad p_i = \mathrm{Tr}_{AB}(\rho_{AB}\mathfrak{P}_i)$$

- $\{\mathfrak{P}_i\}$ are POVMs, *i.e.*, $\sum_i \mathfrak{P}_i = \mathbb{I}, \mathfrak{P}_i \geq 0$

Henderson & Vedral, J. Phys. A, **34**, 6899, (2001)

Properties of Discord

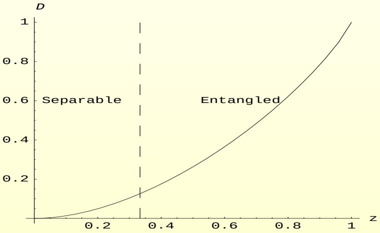
- $0 \leq \mathcal{D} \leq S(\rho_B)$
- $\mathcal{D} = 0 \Leftrightarrow \rho_{AB} = \sum_j \Pi_j^B \rho_{AB} \Pi_j^B$
- For pure states

$$\begin{aligned} \mathcal{D} &= S(\rho_B) - \cancelto{0}{S(\rho_{AB})} + \min_{\{\Pi_j^B\}} \sum_j p_j \cancelto{0}{S(\rho_{A|\Pi_j^B})} \\ &= S(\rho_B) \end{aligned}$$

- $\mathcal{D}$ is an entanglement monotone on pure states

Discord *vs* Entanglement

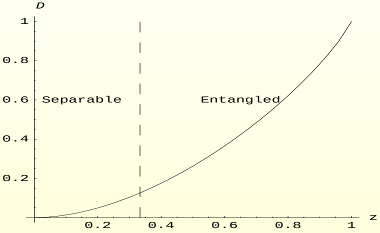
- Fundamentally different from Werner's notion of classicality



$$\rho_W = \frac{1-z}{4}\mathbb{I} + z|\Phi^+\rangle\langle\Phi^+|$$

Discord *vs* Entanglement

- Fundamentally different from Werner's notion of classicality

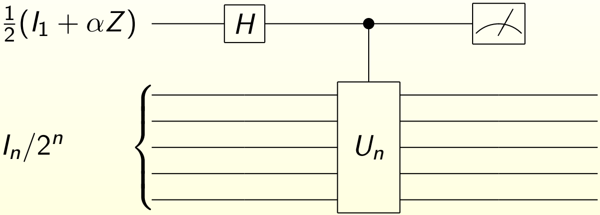


$$\rho_W = \frac{1-z}{4}\mathbb{I} + z|\Phi^+\rangle\langle\Phi^+|$$

- As another example

$$\rho = \frac{1}{4}\Big(|+\rangle\langle+|\otimes|0\rangle\langle 0| + |-\rangle\langle-|\otimes|1\rangle\langle 1| + |0\rangle\langle 0|\otimes|-\rangle\langle-| + |1\rangle\langle 1|\otimes|+\rangle\langle+|\Big)$$

$\mathcal{D}(\rho) = \frac{3}{4}\log_2\frac{4}{3} = 0.311$

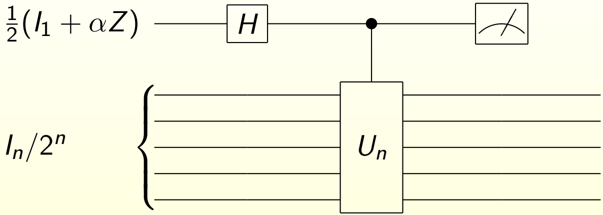


Density matrix just prior to the measurement is

$$\rho_{n+1}(\alpha) = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n \\ \alpha U_n^\dagger & I_n \end{pmatrix}$$

AD, Shaji, Caves, PRL, **100**, 050502, (2008)

DQC1



Density matrix just prior to the measurement is

$$\rho_{n+1}(\alpha) = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n \\ \alpha U_n^\dagger & I_n \end{pmatrix}$$

- $S(\rho_{n+1}) = n + 1 - \frac{1}{2}[(1+\alpha)\log(1+\alpha) + (1-\alpha)\log(1-\alpha)]$
- $\rho_X = \frac{1}{2}\begin{pmatrix} 1 & \alpha\tau \\ \alpha\tau^* & 1 \end{pmatrix}, \qquad \tau = \mathrm{Tr}[U]/2^n$

Discord in DQC1

Measurements:

- $\Pi_\pm = \frac{1}{2}(I_1 + \mathbf{a}.\boldsymbol{\sigma})$
- Then, for a random U,

$$\sum_j p_j S(\rho_{Y|\Pi_j^X}) = \frac{1}{2}[H(\mathbf{q}_+) + H(\mathbf{q}_-)] + \frac{\alpha}{2}(\tau_R \cos\phi + \tau_I \sin\phi)[H(\mathbf{q}_+) - H(\mathbf{q}_-)]$$

where

$$q_{k\pm} = \frac{1}{2^n} \frac{1 \pm \alpha \cos(\theta_k - \phi)}{1 \pm \alpha(\tau_R \cos\phi + \tau_I \sin\phi)}$$

Discord in DQC1

Measurements:

- $\Pi_\pm = \frac{1}{2}(I_1 + \mathbf{a}.\boldsymbol{\sigma})$
- Then, for a random U,

$$\sum_j p_j S(\rho_{Y|\Pi_j^X}) = \frac{1}{2}[H(\mathbf{q}_+) + H(\mathbf{q}_-)] + \frac{\alpha}{2}(\tau_R \cos\phi + \tau_I \sin\phi)[H(\mathbf{q}_+) - H(\mathbf{q}_-)]$$

where

$$q_{k\pm} = \frac{1}{2^n}\frac{1 \pm \alpha\cos(\theta_k - \phi)}{1 \pm \alpha(\tau_R\cos\phi + \tau_I\sin\phi)}$$

Finally...

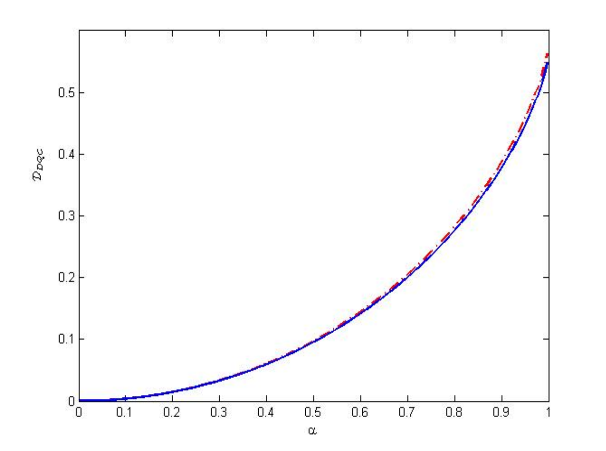
$$\sum_j p_j S(\rho_{Y|\Pi_j^X}) = n + 1 - \log\left(1 + \sqrt{1-\alpha^2}\right) - \left(1 - \sqrt{1-\alpha^2}\right)\log e$$

Putting the pieces together...

- $S(\rho_{X,Y}) = n + 1 - \frac{1}{2}[(1+\alpha)\log(1+\alpha) + (1-\alpha)\log(1-\alpha)]$
- $\rho_X = \frac{1}{2}\begin{pmatrix} 1 & \alpha\tau \\ \alpha\tau^* & 1 \end{pmatrix}, \qquad \tau = \mathrm{Tr}[U]/2^n$
- $S(\rho_X) \simeq 1$ and
- $\mathcal{D} = S(\rho_X) - S(\rho_{X,Y}) + \min_{\{\Pi_j^X\}} \sum_j p_j S(\rho_{Y|\Pi_j^X})$

we have...

$$\begin{aligned} \mathcal{D}_{DQC} &= 1 + \frac{1}{2}[(1+\alpha)\log(1+\alpha) + (1-\alpha)\log(1-\alpha)] \\ &- \log(1+\sqrt{1-\alpha^2}) - (1-\sqrt{1-\alpha^2})\log e. \end{aligned}$$



$$\begin{aligned}\mathcal{D}_{DQC} &= 1+\frac{1}{2}[(1+\alpha)\log(1+\alpha)+(1-\alpha)\log(1-\alpha)] \\ &- \log(1+\sqrt{1-\alpha^2})-(1-\sqrt{1-\alpha^2})\log e.\end{aligned}$$

Recent results

Simulating concordant computations, Eastin, arxiv:1006.4402

This shows that ... a quantum computation must generate quantum discord if it is to efficiently solve a problem that requires super-polynomial time classically.

Entanglement, quantum discord, and the power of the quantum computer, Fanchini *et. al.*, arxiv:1006.2460

The power of the quantum computer can be thus attributed to both, entanglement and quantum discord, which are always present and distributed following a monogamic relation