Device-independent self-test of true multipartite entanglement

Ramij Rahaman

Department of Mathematics

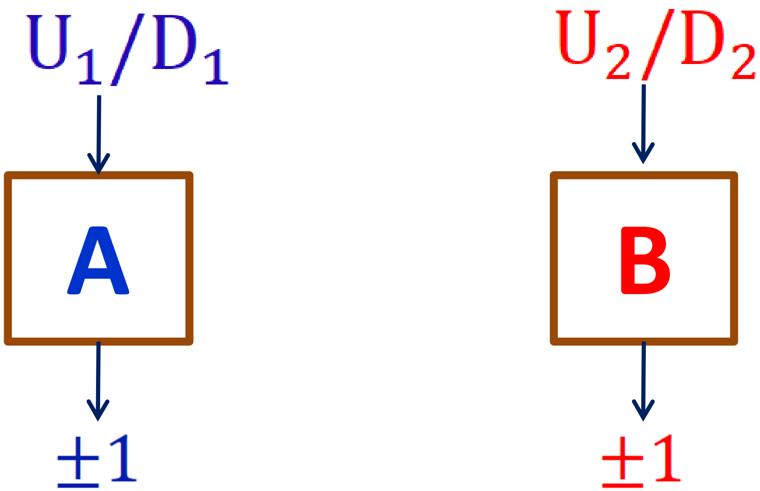
University of Allahabad

Allahabad 211002

Outline

- **Introduction**
  - What is device-independent(DI) self test?
  - Hardy's Paradox (non-locality test like Bell-test).
- **Our works:**
  - Generalized Hardy type test.
  - DI self-test of Hardy correlations.
- **Conclusions**

Hardy's Paradox *[L. Hardy PRL 1992]*



$$P(+,+|U_1,U_2) = q > 0$$
$$P(+,+|U_1,D_2) = 0$$
$$P(+,+|D_1,U_2) = 0$$
$$P(-,-|D_1,D_2) = 0$$

P(a,b|X,Y) is the joint probability of getting the outcome (a,b) for the given input (X,Y).

This set of conditions cannot be satisfied by any Local-Realistic (LR) Theory (Classical Theory).

HARDY'S PARADOX & QM

$P(a, b|X, Y) = |\langle\psi|(|X = a\rangle|Y = b\rangle)|^2$ for the quantum state $|\psi\rangle$.

$|X = a\rangle$ is the eigenstate for the eigenvalue **a**.

$$P(+,+|U_1,U_2) = q > 0 \qquad |\phi_4\rangle = |U_1 = +1\rangle|U_2 = +1\rangle$$
$$P(+,+|U_1,D_2) = 0 \qquad |\phi_3\rangle = |U_1 = +1\rangle|D_2 = +1\rangle$$
$$P(+,+|D_1,U_2) = 0 \qquad |\phi_2\rangle = |D_1 = +1\rangle|U_2 = +1\rangle$$
$$P(-,-|D_1,D_2) = 0 \qquad |\phi_1\rangle = |D_1 = -1\rangle|D_2 = -1\rangle$$

Let $|D_j = +1\rangle = a_j|U_j = +1\rangle + b_j|U_j = -1\rangle, j = A, B;$ with $|a_j|^2 + |b_j|^2 = 1$ & $0 < |a_j| < 1$.

$|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle$ are linearly independent.

If $\mathbf{S} = \{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$, then $\dim(\mathbf{S}) = \mathbf{3}$.

Hardy state $|\Psi\rangle \perp \mathbf{S}$ & $\dim(H_A \otimes H_B) = \mathbf{2} \times \mathbf{2}$.

$\therefore |\Psi\rangle$ is unique. [G Kar PLA 97]

HARDY STATE

$$|\phi_1\rangle = |D_1 = -1\rangle|D_2 = -1\rangle \quad |\phi_3\rangle = |U_1 = +1\rangle|D_2 = +1\rangle$$

$$|\phi_2\rangle = |D_1 = +1\rangle|U_2 = +1\rangle \quad |\phi_4\rangle = |U_1 = +1\rangle|U_2 = +1\rangle$$

By Gram-Schmidt orthogonalization procedure

$$|\phi_1'\rangle = |\phi_1\rangle;$$

$$|\phi_i'\rangle = \frac{|\phi_i\rangle - \sum_{j=1}^{i-1}\langle\phi_j'|\phi_i\rangle|\phi_j'\rangle}{\sqrt{1 - \sum_{j=1}^{i-1}\left|\langle\phi_j'|\phi_i\rangle\right|^2}}; i = 2,3,4$$

$\therefore$ Hardy state $|\Psi\rangle = |\phi_4'\rangle$

PROBABILITY OF SUCCESS

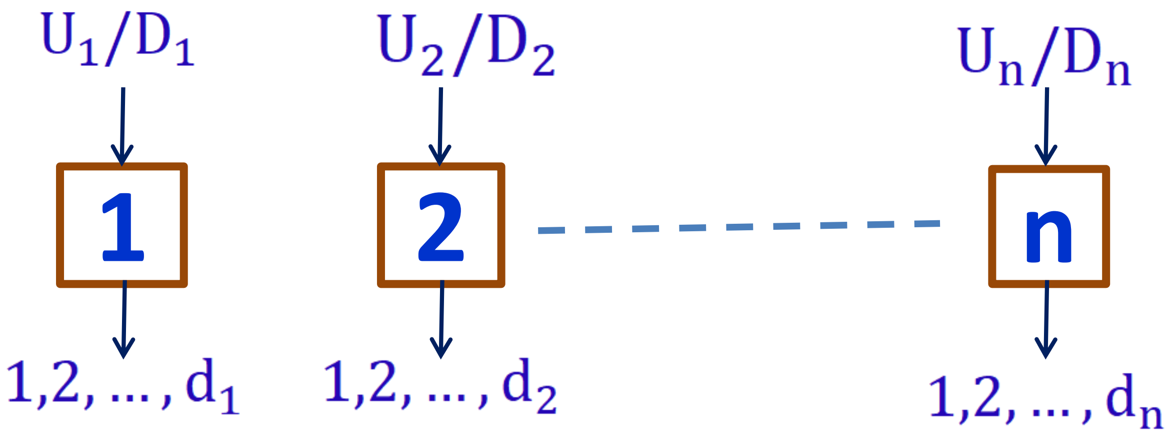
Probability of Success $q = |\langle\Psi|\phi_4\rangle|^2 = \dfrac{|a_1 a_2|^2 |b_1 b_2|^2}{1 - |a_1 a_2|^2}$.

Its maximum is $\dfrac{5\sqrt{5} - 11}{2} = 0.09$, where $|a_1| = |a_2| = \sqrt{\frac{\sqrt{5}-1}{2}}$.

$\therefore U_1 \equiv U_2$ & $D_1 \equiv D_2$.

GENERALIZED HARDY PARADOX

Consider a system $H = H_1 \otimes H_2 \otimes \ldots \otimes H_n$; Dim. $(H) = d_1 . d_2 \ldots d_n$



$$P(11 \ldots 1 | D_1 D_2 \ldots D_n) = 0$$

$$P(a_r 1 | D_r U_{r+1}) = 0 \quad a_r \neq 1$$

$$P(11 \ldots 1 | U_1 U_2 \ldots U_n) = q > 0$$

Again cannot be satisfied by any LR theory

Also, states of the form $|\phi\rangle_K \otimes |\xi\rangle_{\bar{K}}$; $K \subset \{1,2,\ldots,n\}$ cannot.

That is, **only genuine entangled states** can satisfy

[Rahaman et al., Phys. Rev. A 2014]

For qubits system: $\text{Dim.}(H) = 2 \times 2 \times \ldots \times 2$

$$P(11\ldots1|D_1D_2\ldots D_n) = 0;\ |\phi_-\rangle = |D_1 = 1\rangle|D_2 = 2\rangle \ldots |D_n = 1\rangle$$

$$P(a_r1|D_rU_{r+1}) = 0\ ;\ \ |\phi_{k_r}\rangle = |..\rangle \ldots |D_r = 2\rangle|U_{r+1} = 1\rangle \ldots |..\rangle$$

$$P(11\ldots1|U_1U_2\ldots U_n) = q;\ |\phi_+\rangle = |U_1 = 1\rangle|U_2 = 1\rangle \ldots |U_n = 1\rangle$$

Define a new basis: $|00\ldots0\ldots0\rangle = |\phi_+\rangle,$

$$|00\ldots01_l0\ldots0\rangle = \frac{1}{\beta_l}\left[|\phi_k(0,\ldots,0,+_l,0,\ldots,0)\rangle - \alpha_l|\phi_+\rangle\right], \forall\ l,$$

$$\begin{aligned}|0\ldots01_l0\ldots01_m0\ldots0\rangle = {} & \frac{1}{\beta_l\beta_m}[|\phi_k(0,\ldots,0,+_l,0,\ldots,0,+_m,0,\ldots,0)\rangle - \alpha_l\alpha_m|\phi_+\rangle \\ & - \beta_l\alpha_m|00\ldots01_l0\ldots0\rangle - \alpha_l\beta_m|00\ldots01_m0\ldots0\rangle], \forall\ l \neq m,\end{aligned}$$

$$\begin{aligned}|0\ldots01_l0\ldots01_m0\ldots01_k0\ldots0\rangle = {} & \frac{1}{\beta_l\beta_m\beta_k}[|\phi_k(0,\ldots,0,+_l,0,\ldots,0,+_m,0,\ldots,0,+_k,0,\ldots,0)\rangle \\ & - \alpha_l\alpha_m\alpha_k|\phi_+\rangle - \alpha_l\alpha_m\beta_k|00\ldots01_k0\ldots0\rangle \\ & - \alpha_l\beta_m\alpha_k|00\ldots01_m0\ldots0\rangle - \beta_l\alpha_m\alpha_k|00\ldots01_l0\ldots0\rangle \\ & - \alpha_l\beta_m\beta_k|00\ldots01_m0\ldots01_k0\ldots0\rangle \\ & - \beta_l\alpha_m\beta_k|00\ldots01_l0\ldots01_k0\ldots0\rangle - \beta_l\beta_m\alpha_k|00\ldots01_l0\ldots01_m0\ldots0\rangle],\end{aligned}$$

$$\forall\ l \neq m \neq k \neq l, \ldots$$

$$\begin{aligned}|11\ldots1\ldots1\rangle = {} & \frac{(-1)^N}{\prod_{i=1}^N \alpha_i^*}\Bigg[|\phi_0\rangle - \Bigg\{\left(\prod_{j=1}^N \beta_j^*\right)|\phi_+\rangle + (-1)^1\sum_{i=1}^N \alpha_i^*\left(\prod_{j=1,j\neq i}^N \beta_j^*\right)|00\ldots01_i0\ldots0\rangle \\ & + (-1)^2\sum_{i,l=1,i\neq l}^N \alpha_i^*\alpha_l^*\left(\prod_{j=1,j\neq i,l}^N \beta_j^*\right)|00\ldots01_i0\ldots01_l0\ldots0\rangle \\ & + \cdots + (-1)^{N-1}\sum_{j=1}^N \beta_j^*\left(\prod_{i=1,i\neq j}^N \alpha_i^*\right)|11\ldots10_j1\ldots1\rangle\Bigg\}\Bigg],\end{aligned}$$

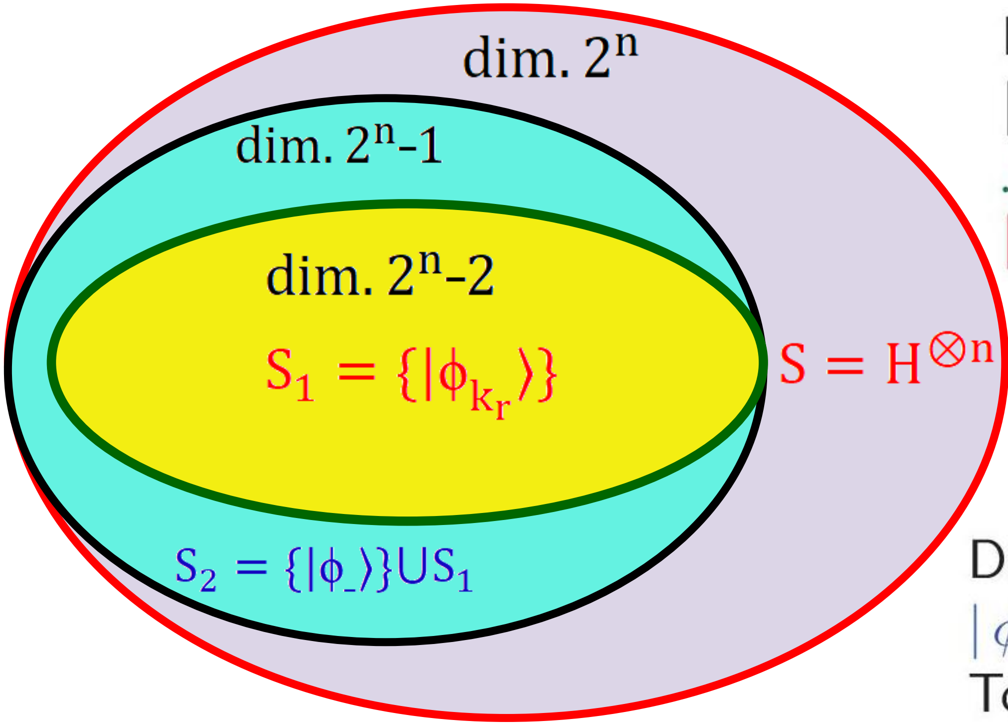
where $|+\rangle_j = \alpha_j|0\rangle_j + \beta_j|1\rangle_j$, and $|-\rangle_j = \beta_j^*|0\rangle_j - \alpha_j^*|1\rangle_j$

For qubits system: Dim. (H) = 2 × 2 × … × 2

$$P(11\dots1|D_1D_2\dots D_n) = 0;\ |\phi_-\rangle = |D_1 = 1\rangle|D_2 = 2\rangle\dots|D_n = 1\rangle$$

$$P(a_r1|D_rU_{r+1}) = 0\ ;\ |\phi_{k_r}\rangle = |..\rangle\dots|D_r = 2\rangle|U_{r+1} = 1\rangle\dots|..\rangle$$

$$P(11\dots1|U_1U_2\dots U_n) = q;\ |\phi_+\rangle = |U_1 = 1\rangle|U_2 = 1\rangle\dots|U_n = 1\rangle$$



Let $\mathcal{S}_1 = \{|\phi_{k_r}\rangle\}$

$|\phi_-\rangle \perp \{\mathcal{S}_1\}$ and $|\phi_-\rangle \not\perp |\phi_+\rangle$.

$\therefore\ |\phi_+\rangle \notin \{\mathcal{S}_1\}$

$|\phi_+\rangle \neq |\phi_-\rangle$, $\therefore$ dim.$(\mathcal{S}_1) = 2^n - 2$

Define: $\mathcal{S}_2 = \{|\phi_-\rangle\} \cup \mathcal{S}_1$.

$|\phi_+\rangle \notin \mathcal{S}_2$, $\therefore$ dim.$(\mathcal{S}_2) = 2^n - 1$.

To satisfy Hardy conditions: $|\psi\rangle \perp \mathcal{S}_2$.

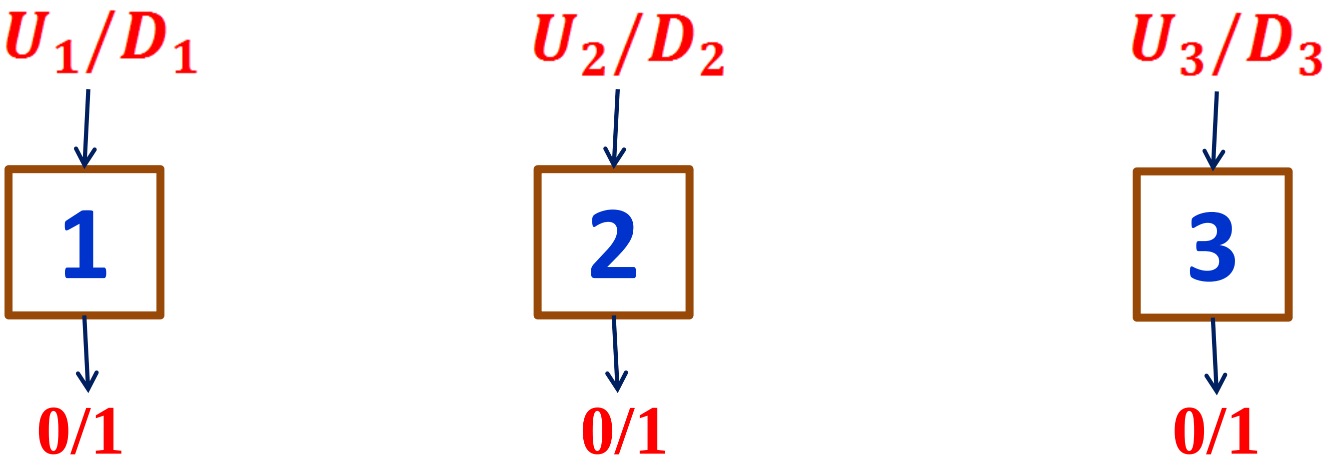
Hardy state $|\psi\rangle$ **is** <u>unique & genuinely entangled</u>

[Rahaman et al., Phys. Rev. A 2014]

<u>THREE QUBITS HARDY PARADOX</u>

Consider a system $H=H_1 \otimes H_2 \otimes H_3$

Dim.(H)=$2X2X2=8$



$$P(000|U_1U_2U_3) = q > 0$$

$$P(00|U_iD_j) = 0 \quad i \neq j$$

$$P(111|D_1D_2D_3) = 0$$

Again cannot be satisfied by any LR theory

For 3-qubits system: Dim.(H)=2X2X2

Let us assign:

$$P(000|U_1U_2U_3) = q \quad |\phi_+\rangle = |0\rangle|0\rangle|0\rangle$$

$$P\left(00\middle|U_iD_j\right) = 0 \quad \left|\phi_{k_r}\right\rangle = |..\rangle|0_i\rangle|0'_j\rangle$$

$$P(111|D_1D_2D_3) = 0 \quad |\phi_-\rangle = |1'\rangle|1'\rangle|1'\rangle$$

$$\text{Let } S_1 = \{\backslash\phi_{k_r}\} \cup \{|\phi_-\}.$$

$$\text{Then } dim.(S_1) = 2^3 - 1$$

Hardy state $|\Psi\rangle \perp S_1$

Hardy state |□□ **is** unique & genuinely entangled.

Max (q)= 0.*0181938*

[Rahaman et al., Phys. Rev. A 2014]

Relaxed Hardy type test for genuine multiparty entangled states

$$P(11\ldots1|D_1D_2\ldots D_n) = 0$$

$$P(1\ldots\neg1\ldots1|U_1\ldots D_r\ldots U_n) = 0$$

$$P\left(1..1\ldots1\ldots1\middle|U_1\ldots D_i\ldots D_j\ldots U_n\right) = q$$

Only **genuine** multiparty entangled states can satisfy

[S. S. Bhattacharya, A. Roy, A. Mukherjee & R. Rahaman, Phys. Rev. A, 92, 012111 (2015)]

DI-Self test

Lemma: For any two Hermitian operators X_0 & X_1 with eigenvalues □**1** acting on a Hilbert space **H** there is a decomposition of H as a direct sum of subspaces H^i of dimension **d□ 2** each, such that both X_0 & X_1 act within each H^i

$$X_0 = \otimes_i X_0^i \ \& \ X_1 = \otimes_i X_1^i \text{ and each act on } H^i.$$

Ref.: L. Masanes PRL 06 & Rabelo et.al. PRL 12.

DI-Self test

$\mathbf{X_0} = \otimes_i \mathbf{X_0^i}$ & $\mathbf{X_1} = \otimes_i \mathbf{X_1^i}$ and each act on $\mathbf{H^i}$.

Let $X_0 = \Pi_{+|X_0} - \Pi_{-|X_0}$ & $X_1 = \Pi_{+|X_1} - \Pi_{-|X_1}$

where $\Pi_{a|x} = \otimes_i \Pi^i_{a|x}$ & $\Pi^i_{a|x}$ acts on $\mathbf{H^i}$.

$$\mathbf{P}(a, \dots, b|x, \dots, y)$$
$$= \sum_{i,\dots,j} q_{i\dots j} \mathrm{Tr}\left[\rho_{i\dots j} \Pi^i_{a|x} \otimes \dots \Pi^j_{b|y}\right],$$
$$= \sum_{i,\dots,j} q_{i\dots j}\, p_{i\dots j}(a, \dots, b|x, \dots y),$$

where $q_{i\dots j} = \mathrm{Tr}\left(\rho \Pi^i \otimes \Pi^j\right)$ & $\rho_i \dots j = \left[\Pi^i \otimes \dots \Pi^j \rho \Pi^i \otimes \dots \Pi^j\right]/q_{i\dots j}$.

Thus the concern Hardy probability is given by

$$\mathbf{P}(+, \dots, +|U_1, \dots, U_n) = \sum_{i,\dots,j} q_{i\dots j}\, p_{i\dots j}(+, \dots, +|U_1, \dots U_n).$$

DI-Self test

Thus the concern Hardy probability is given by

$$\mathbf{q} = \mathbf{P}(+,\dots,+|\mathbf{U_1},\dots,\mathbf{U_n}) = \sum_{\mathbf{i},\dots,\mathbf{j}} \mathbf{q_{i\dots j}}\, \mathbf{p_{i\dots j}}(+,\dots,+|\mathbf{U_1},\dots\mathbf{U_n}).$$

Theorem: If max. q is observed in an ideal Hardy's test, then the state of the system is equivalent up to local isometries to $|\sigma\rangle \times |\Psi\rangle$ *where* $|\sigma\rangle$ *and* $|\Psi\rangle$ are arbitrary n-partite state and concerne Hardy states corresponding to maximum probability of success in n-qubit system respectively.

A state can lead to a maximal value of q if, and only if, the sate is of the form

$$|\psi\rangle = \oplus_{i\dots j}\sqrt{q_{i\dots j}}\,|\Psi\rangle_{i\dots j};\ |\Psi\rangle_{i\dots j} \equiv |\Psi\rangle_{k\dots m}$$

CONCLUSIONS

- Proposed generalized Hardy type test for detection of genuine multiparty entanglement.
- For n-qubits- the Hardy correlation is unique for a given set of local observables pairs.
  - For maximum success probability the test is a DI self test.

- Possible applications: Provides secure quantum protocols for various cryptographic & communication tasks. E.g.,
  - Key distribution
  - Digital signatures
  - Secret sharing
  - Byzantine agreement
  - Random number generator
  - Oblivious transfer
  - Dining cryptographers
  - Anonymous veto etc.

Thank You