2-Message QIPs + the Quantum Separability Problem

1211.6120

1

Main Question

Given a description of a circuit to generate a state ρ_{AB}, is the state separable or entangled? (call this QSEP-CIRCUIT)

Relevance

Might want to know the answer after running some quantum computation.

Main Results

QSEP-CIRCUIT $\in$ QIP(2)

QSEP-CIRCUIT is hard for QSZK + NP

History

Much prior work has focused on the matrix version of the separability problem, formulated as a promise problem:

SEP: Given a matrix description of ρ_{AB}, decide whether

YES: $\rho_{AB} \in S$

NO: $\min_{\sigma_{AB} \in S} \| \rho_{AB} - \sigma_{AB} \|_2 \geq \varepsilon$

where $\sigma_{AB} \in S$ if σ_{AB} can be written as

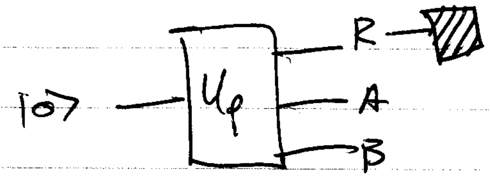
$$\sigma_{AB} = \sum_x p(x) \, |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_B$$

Gurvits: SEP is NP-hard if $\varepsilon \geq \frac{1}{\exp(d)}$
2003

Ghariban: " " " if $\varepsilon \geq \frac{1}{\mathrm{poly}(d)}$
2010

BCY2011: if ε is constant, then $\exists$ a quasi-polynomial time algorithm to decide

QSEP-CIRCUIT: Given a description of a circuit to generate ρ_{AB}



decide

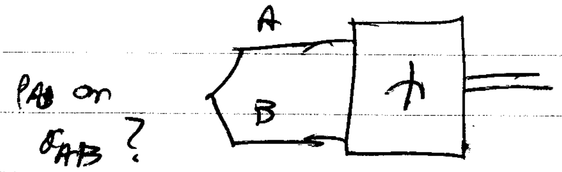
YES: $\min_{\sigma_{AB} \in S} \| \rho_{AB} - \sigma_{AB} \|_1 \leq \delta_c$

NO: $\min_{\sigma_{AB} \in S} \| \rho_{AB} - \sigma_{AB} \|_{1\text{-LOCC}} \geq \delta_s$

Background

Trace norm $\|A\|_1 = \mathrm{Tr}\{\sqrt{A^\dagger A}\}$

related to error prob. when distinguishing ρ_{AB} from σ_{AB} when using arbitrary measurement

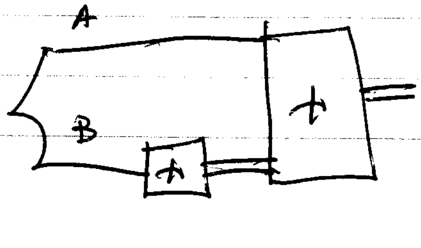


$p_e = \frac{1}{2}\left(1 - \frac{1}{2}\|\rho - \sigma\|_1\right)$

1-LOCC norm:

$$\| \rho_{AB} - \sigma_{AB} \|_{1\text{-LOCC}} = \max_{\Lambda_{B\to X}} \| (\mathrm{id}_A \otimes \Lambda_{B\to X})(\rho_{AB} - \sigma_{AB}) \|$$

$$\Lambda_{B\to X}(\omega) = \sum_x \mathrm{Tr}\{\omega \Lambda_x\} |x\rangle\langle x|$$



Matthews et al, '09 ~~$\|\rho-\sigma\|_{1\text{-}LOCC} \gtrsim \frac{1}{\sqrt{153}}\|\rho-\sigma\|_2$~~

$$\|\rho-\sigma\|_{1\text{-}LOCC} \gtrsim \frac{1}{\sqrt{153}}\|\rho-\sigma\|_2$$

Fidelity $\quad F(\rho,\sigma) \equiv \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$

Uhlmann $\quad F(\rho,\sigma) = \max |\langle\phi_\rho|\phi_\sigma\rangle|^2$

where $\quad \rho = \mathrm{Tr}_R\{|\phi_\rho\rangle\langle\phi_\rho|_{RA}\}$

$\quad \sigma = \mathrm{Tr}_R\{|\phi_\sigma\rangle\langle\phi_\sigma|_{RA}\}$

Also $\quad F(\rho,\sigma) \equiv \max_U |\langle\phi_\rho|(U\otimes I)|\phi_\sigma\rangle|^2$

Fuchs-van-de-Graaf:

$$\|\rho-\sigma\|_1 \approx 1 - F(\rho,\sigma)$$

at extremes

k-extendibility DPS 2004

ρ_{AB} is k-ext. if $\exists\ \omega_{AB_1\cdots B_k}$ such that

1) $\omega_{AB_1\cdots B_k} = \left(I \otimes W^{\pi}_{B_1\cdots B_k}\right) \omega_{AB_1\cdots B_k} \left(I_A \otimes W^{\pi}\right)^{\dagger}$

2) $\mathrm{Tr}_{B_2\cdots B_k}\left\{\omega_{AB_1\cdots B_k}\right\} = \rho_{AB}$

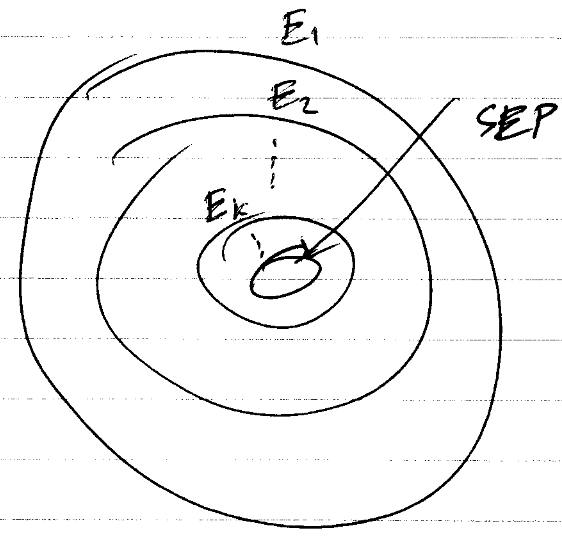
Let $\mathcal{E}_k$ denote the set of k-extendible states

Every separable state is ~~k~~-extendible $\forall k$

choice of extension is just

$\sum_x p(x)\ |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_{B_1} \otimes \cdots \otimes |\phi_x\rangle\langle\phi_x|_{B_k}$

If state ρ_{AB} is not separable, then $\exists\ l$ such that $\rho_{AB} \notin \mathcal{E}_{l'}$ $\forall\ l' \geq l$



$\lim_{k\to\infty} \mathcal{E}_k = S$

maximum k-extendible fidelity

$\max_{\sigma_{AB}\in\mathcal{E}_k} F(\rho_{AB}, \sigma_{AB})$

$\max_{\sigma_{AB}\in S} F(\rho_{AB}, \sigma_{AB}) = \lim_{k\to\infty}$ max k fid

Lemma for Approx. k-ext. fidelity [extension of BCY11]

If $\min_{\sigma_{AB} \in S} \| \rho_{AB} - \sigma_{AB} \|_{1\text{-LOCC}} \geq \varepsilon > 0$

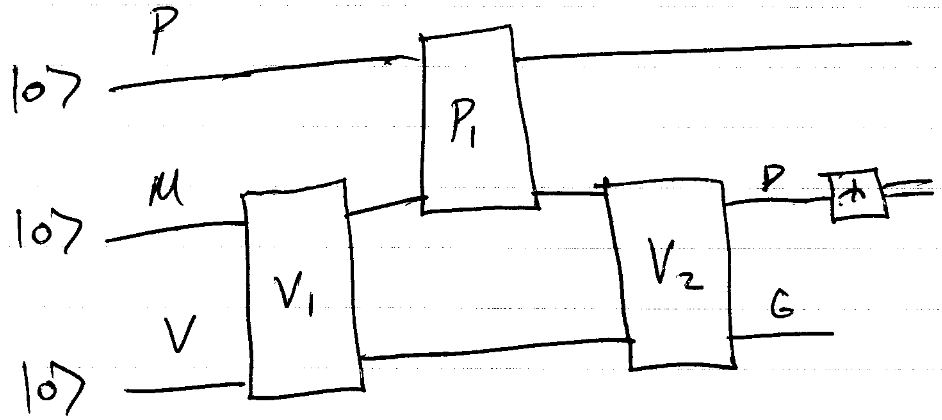
then $\min_{\sigma_{AB} \in \mathcal{E}_k} \| \rho_{AB} - \sigma_{AB} \|_1 \geq \delta$

for $\delta < \varepsilon$ +

$$k = \left\lceil \frac{c \log |A|}{(\varepsilon - \delta)^2} \right\rceil$$

Quantum Interactive Proof Systems

QIP(2) – all promise problems that can be decided by a QIP system w/ 2 messages



$\mathrm{QIP}(2) \subseteq \mathrm{PSPACE}$

Given a problem instance, verifier has unitaries V_1 + V_2 corresponding to it, + prover chooses P_1 to maximize the chances that verifier accepts.

if problem is a YES instance ~~,~~,
there should exist a QIP(2) that convinces verifier to accept w/ prob. $\geq 1-\varepsilon$

if problem is ~~an~~ NO instance,
max. prob w/ which verifier accepts should be $\leq \varepsilon$

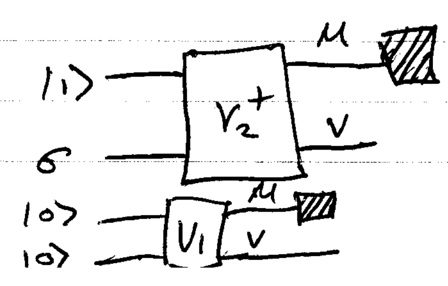
most important parameter:
<u>max. acceptance probability</u>

$$\max_{P_1} \left\| \langle 1|_D (V_2)_{MV \to DG} (P_1)_{PM} |0\rangle_P |\phi\rangle_{MV} \right\|_2^2$$

$$= \max_{P_1, |\psi\rangle_{PG}} \left| \langle 1|_D \langle \psi|_{PG} (V_2)_{MV \to DG} (P_1)_{PM} |0\rangle_P |\phi\rangle_{MV} \right|^2 = \max_{\sigma} F(\omega, \mathcal{N}(\sigma))$$

channel $\mathcal{N}$

state ω



If we are to put QSEP-CIRCUIT into QIP(2)

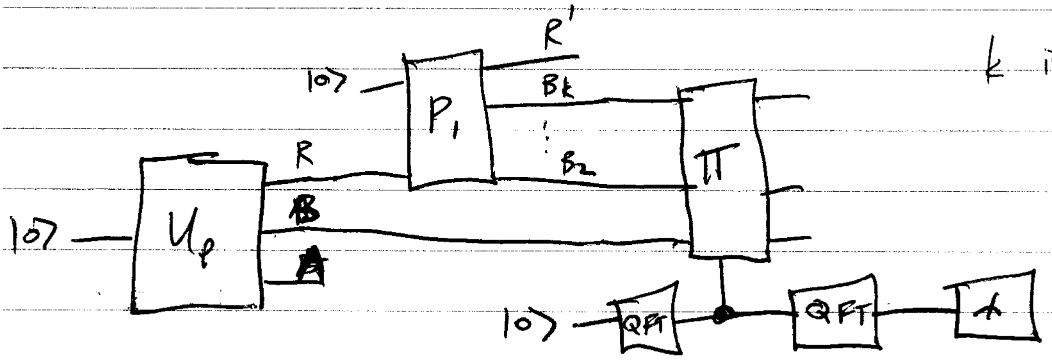
which state, which channel?

state ρ_{AB} — channel should test for k-extendibility (random permutation followed by tracing out)

In the case of a YES instance of QSEP-CIRCUIT, (ρ_{AB} is separable), we know that

$$\sum_x \sqrt{p(x)}\,|x\rangle_{R'}\,|\psi_x\rangle_A\,|\phi_x\rangle_{B_1}\cdots|\phi_x\rangle_{B_k}$$

is a purification of ρ_{AB}, so make prover generate this purification



k is only polynomial in circuit size due to Lemma

if all zeros, accept

if state is separable, test passes w/probability 1,

If close $\overset{\delta_c}{\approx}$, then " " $\geq 1-\delta_c$

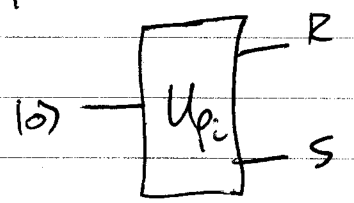
upper bound on acc. prob. is

$$\max_{\sigma_{AB}\in\mathcal{E}_k} F(\rho_{AB},\sigma_{AB}) \approx 1-\min_{\sigma_{AB}\in\mathcal{E}_k}\|\rho_{AB}-\sigma_{AB}\|_1 \approx 1-\delta_s$$

QSZK - restricted version of QIP(2) where in case of YES instance, verifier could have generated state himself (Watrous)

complete problem for QSZK

QSD : Given U_{ρ_0} + U_{ρ_1}

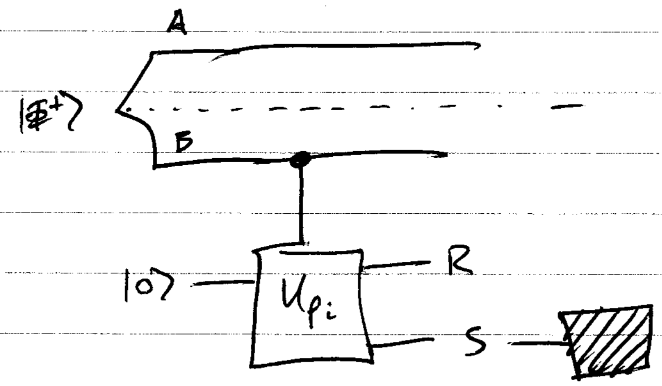


YES: $\|\rho_0 - \rho_1\|_1 \geq 2 - \varepsilon$

No: $\|\rho_0 - \rho_1\|_1 \leq \varepsilon$

want to show that we can use QSEP-CIRCUIT to solve QSD (for reduction, should map YES instances to YES instances + No " " No ")

Idea



state is

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B|\psi_{\rho_0}\rangle_{RS} + |1\rangle_A|1\rangle_B|\psi_{\rho_1}\rangle_{RS}\right)$$

In case of YES instance

$\|\rho_0 - \rho_1\|_1 \geq 2 - \varepsilon$, this implies states are approximately orthogonal on S system, so that tracing it out decoheres the superposition to

$$\overset{\varepsilon}{\approx} \frac{1}{2}\Big(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B \otimes (\psi_{\rho_0})_R + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \otimes (\psi_{\rho_1})_R \Big)$$

state on $A|BR$ is then close to separable

In case of NO instance, we have

$\|\rho_0 - \rho_1\|_1 \leq \varepsilon$ would like to distill a Bell state

$F(\rho_0, \rho_1) \geq 1 - \varepsilon$ &

$$\sqrt{F(\rho_0, \rho_1)} = \langle \psi_{\rho_0}|_{RS} (U_R \otimes I_S) |\psi_{\rho_1}\rangle_{RS} \geq \sqrt{1-\varepsilon}$$

can perform local operation on BR

$$|0\rangle\langle 0|_B \otimes I_R + |1\rangle\langle 1|_B \otimes U_R$$

& gives

$$|\varphi'\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle_A |0\rangle_B |\psi_{\rho_0}\rangle_{RS} + |1\rangle_A |1\rangle_B (U_R \otimes I_S) |\psi_{\rho_1}\rangle_{RS} \Big)$$

$$\left(\langle \Phi^+|_{AB} \otimes \langle \psi_{po}|_{RS} \right) |\psi'\rangle$$

$$\geq \sqrt{1-\varepsilon}$$

can distill a Bell state.

For a Bell state, we can play CHSH game to show a separation between it & a separable state in 1-LOCC distance.

play CHSH game, if win say Bell state
... " lose " separable state

$$\| (.85, .15) - (.75, .25) \|_1 \geq 0.2$$

$$\Rightarrow \| \omega_{A:BR} - \sigma_{A:BR} \|_{1\text{-LOCC}} \geq 0.2 - 2\sqrt{\varepsilon}$$

done.

Open problem: characterize complement of QSEP-CIRCUIT (we know it is QSZK-hard)