Perfect Embezzlement

Vern Paulsen
Institute for Quantum Computing
Department of Pure Mathematics
University of Waterloo

QMath13

October 10, 2016

Based on:
Perfect Embezzlement of Entanglement(R. Cleve, L. Liu, V. Paulsen)
A non-commutative unitary analogue of Kirchberg's conjecture(S. Harris)

Outline

- Van Dam and Hayden Approximate Embezzlement
- Impossibility of Perfect Embezzlement in Tensor Framework
- Commuting Framework
- The C*-algebra of Non-commuting Unitaries
- Perfect Embezzlement
- New Versions of Tsirelson, Connes, and Kirchberg
- The Coherent Embezzlement Game

Approximate Embezzlement of A Bell State

It is well-known that entangled states cannot be produced from unentangled states by local operations. But Van Dam and Hayden showed a method that, in a certain sense, *appears* to produce entanglement by local methods. Hence, their term *embezzlement*. They showed that by sharing an entangled *catalyst* vector ψ in a bipartite resource space $\mathcal{R} = \mathcal{R}_A \otimes \mathcal{R}_B$ one could use local unitary operations to transform

$$|0\rangle_A |0\rangle_B \otimes \psi \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \otimes \psi_\epsilon$$

where $\|\psi - \psi_\epsilon\| < \epsilon$ for any $\epsilon > 0$.

More precisely, given $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$, there are finite dimensional spaces $\mathcal{R}_A, \mathcal{R}_B$ and unitaries, U_A on $\mathcal{H}_A \otimes \mathcal{R}_A$, U_B on $\mathcal{R}_B \otimes \mathcal{H}_B$ such that on $(\mathcal{H}_A \otimes \mathcal{R}_A) \otimes (\mathcal{R}_B \otimes \mathcal{H}_B)$,

$$(U_A \otimes id_B)(id_A \otimes U_B)(|0\rangle \otimes \psi \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes \psi_\epsilon \otimes |0\rangle + |1\rangle \otimes \psi_\epsilon \otimes |1\rangle).$$

Van Dam and Hayden even proved that as $\epsilon \to 0$ necessarily $dim(\mathcal{R}_A), dim(\mathcal{R}_B) \to +\infty$ with particular bounds.
This leaves open the possibility that by taking $dim(\mathcal{R}_A) = dim(\mathcal{R}_B) = +\infty$ one could achieve *perfect embezzlement*, by which we mean, have $\psi = \psi_\epsilon$.
We now show why perfect embezzlement is impossible, in this tensor product framework.

Proposition (CLP)

Perfect embezzlement is impossible in the above tensor product framework.

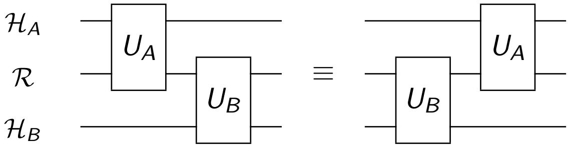
Proof: Write a Schmidt decomposition

$$|0\rangle \otimes \psi \otimes |0\rangle = \sum_j t_j(|0\rangle \otimes u_j) \otimes (v_j \otimes |0\rangle),$$

with $u_j \in \mathcal{R}_A$ orthonormal and $v_j \in \mathcal{R}_B$ orthonormal.
The operators $U_A \otimes id_B$ and $id_A \otimes U_B$ act locally and so preserve Schmidt coefficients.
But the Schmidt coefficients of $\frac{1}{\sqrt{2}}(|0\rangle \otimes \psi \otimes |0\rangle + |1\rangle \otimes \psi \otimes |1\rangle)$ are $\frac{t_1}{\sqrt{2}}, \frac{t_1}{\sqrt{2}}, \frac{t_2}{\sqrt{2}}, \frac{t_2}{\sqrt{2}}, \ldots$.

The Commuting Operator Framework

We no longer require that the resource space have a bipartite structure.
Instead, we only ask for a resource space $\mathcal{R}$, and unitaries, U_A on $\mathcal{H}_A \otimes \mathcal{R}$ and U_B on $\mathcal{R} \otimes \mathcal{H}_B$ such that $(U_A \otimes id_B)$ commutes with $(id_A \otimes U_B)$.



Given a commuting operator framework, we say that $\psi \in \mathcal{R}$ *is a catalyst vector for perfect embezzlement of a Bell state* provided that

$$(U_A \otimes id_B)(id_A \otimes U_B)(|0\rangle \otimes \psi \otimes |0\rangle) = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes \psi \otimes |0\rangle + |1\rangle \otimes \psi \otimes |1\rangle\big).$$

Theorem (CLP)

Perfect embezzlement of a Bell state is possible in a commuting operator framework.

An application.

The Coherent Embezzlement Game

This game was introduced by Regev and Vidick, also known as the T_2 game.
Alice and Bob both receive one of two states, ϕ_0, ϕ_1 where

$$\phi_c = \frac{1}{\sqrt{2}}|00\rangle \otimes |00\rangle + \frac{1}{\sqrt{2}}(-1)^c\big(\frac{1}{\sqrt{2}}|10\rangle \otimes |01\rangle + \frac{1}{\sqrt{2}}|11\rangle \otimes |11\rangle\big),$$

$c \in \{0, 1\}$.
Alice receives the first qubits which is $\mathcal{H}_A$ and Bob receives the second qubits, $\mathcal{H}_B$. They each output a classical bit a, b.
They win if input $\phi_0 \implies a + b = 0$, and input $\phi_1 \implies a + b = 1$.

Assume that they are allowed to share a state $\psi \in \mathcal{R}$ and act with unitaries on $\mathcal{H}_A \otimes \mathcal{R}$ and $\mathcal{R} \otimes \mathcal{H}_B$, respectively, where necessarily these unitaries commute.

Theorem (CLP)

There is a perfect strategy for the coherent embezzlement game in the commuting framework. But there is no perfect strategy if we require that $\mathcal{R} = \mathcal{R}_A \otimes \mathcal{R}_B$ and that their unitaries act locally, even when we allow $\mathcal{R}_A$ and $\mathcal{R}_B$ to be infinite dimensional.

Idea of proof: 1)This game is embezzlement in reverse!
2) Unitaries are reversible, i.e., invertible.

In the rest of this talk, I want to outline the proof and show why the fact that perfect embezzlement is possible in this commuting framework but not possible in a tensor product framework is closely related to the Tsirelson conjectures and to Connes' embedding conjecture.

Suppose that $\mathcal{H}_A = \mathbb{C}^n$ and identify $\mathbb{C}^n \otimes \mathcal{R} = \mathcal{R} \oplus \cdots \oplus \mathcal{R}$(n times). Using this identification, we write $U_A = (U_{i,j})$ where $U_{i,j} \in B(\mathcal{R})$, $0 \le i, j \le n-1$. Similarly, if $\mathcal{H}_B = \mathbb{C}^m$, then we may identify $U_B = (V_{k,l})$ where $V_{k,l} \in B(\mathcal{R})$, $0 \le k, l \le m-1$.

Lemma

$(U_A \otimes id_B)$ commutes with $(id_A \otimes U_B)$ if and only if $U_{i,j}V_{k,l} = V_{k,l}U_{i,j}$ and $U_{i,j}^*V_{k,l} = V_{k,l}U_{i,j}^*$ for all i, j, k, l.

This last condition is called **-commuting*.

Thus, we see that having commuting operator frameworks as above is exactly the same as having operator matrices $U_A = (U_{i,j})$ and $U_B = (V_{k,l})$ that yield unitaries and whose entries pairwise *-commute.

Theorem (CLP)

Perfect embezzlement of a Bell state is possible in a commuting operator framework if and only if there are 2×2 *unitary operators* $U_A = (U_{i,j})$ *and* $U_B = (V_{k,l})$ *whose entries *-commute and a unit vector* $|\psi\rangle$ *satisfying* $\langle\psi|U_{00}V_{00}|\psi\rangle = \langle\psi|U_{10}V_{10}|\psi\rangle = 1/\sqrt{2}$ *and* $\langle\psi|U_{00}V_{10}|\psi\rangle = \langle\psi|U_{10}V_{00}|\psi\rangle = 0$*.*

The van Dam–Hayden approximate embezzlement results, together with some functional analysis imply that such unitaries exist. We now want to draw an analogy with quantum correlation matrices.

Suppose that Alice and Bob each have n quantum experiments and each experiment has m outcomes.
We let $p(a, b|x, y)$ denote the conditional probability that Alice gets outcome a and Bob gets outcome b given that they perform experiments x and y respectively. Tsirelson realized that there are several possible mathematical models for describing the set of all such tuples.
For each experiment a, Alice has projections $\{E_{x,a}, 1 \le a \le m\}$ such that $\sum_a E_{x,a} = I_A$. Similarly, for each b, Bob has projections $\{F_{y,b} : 1 \le b \le m\}$ such that $\sum_b F_{y,b} = I_B$.
If they share an entangled state $\psi \in \mathcal{H}_A \otimes \mathcal{H}_B$ then

$$p(a, b|x, y) = \langle \psi | E_{x,a} \otimes F_{b,y} | \psi \rangle.$$

We let $C_q(n,m) = \{p(a,b|x,y) : \text{ obtained as above } \} \subseteq \mathbb{R}^{n^2m^2}$.
We let $C_{qs}(n,m)$ denote the possibly larger set that we could obtain if we allowed the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ to also be infinite dimensional.
We let $C_{qc}(n,m)$ denote the possibly larger set that we could obtain if instead of requiring the common state space to be a tensor product, we just required one common state space, and demanded that $E_{x,a}F_{y,b} = F_{y,b}E_{x,a}$ for all a,b,x,y, i.e., a commuting model.
Tsirelson was the first to examine these sets and study the relations between them. In fact, he wondered if they could all be equal.
Here are some of the things that we know/don't know about these sets.

- $C_q(n,m) \subseteq C_{qs}(n,m) \subset C_{qc}(n,m)$.
- We don't know if the sets $C_q(n,m)$ and $C_{qs}(n,m)$ are closed.
- $C_q(n,m)^- = C_{qs}(n,m)^-$ and this can be identified with the states on a minimal tensor product.
- Werner-Scholz speculated that $C_{qs}(n,m) = C_q(n,m)^-$.
- (JNPPSW + Ozawa)$C_q(n,m)^- = C_{qc}(n,m)$, $\forall n,m$ iff Connes' Embedding conjecture has an affirmative answer.
- (Slofstra, April 2016) there exists an n,m(very large) such that $C_{qs}(n,m) \neq C_{qc}(n,m)$.
  So either Werner-Scholz is false or Connes is false.

Unitary Correlation Sets

We set

$$UC_q(n,m) = \{\langle\psi|X \otimes Y|\psi\rangle : (U_{i,j}), (V_{k,l}) \text{ are unitary,}$$
$$U_{i,j} \in M_p, V_{k,l} \in M_q, \exists p, q, ||\psi|| = 1$$
$$X \in \{I, U_{i,j}, U^*_{i,j}\}, Y \in \{I, V_{k,l}, V^*_{k,l}\}\}$$

so these are $(2n^2+1)(2m^2+1)$-tuples.
For the set $UC_{qs}(n,m)$ we drop the requirement that each $U_{i,j}$ and $V_{k,l}$ act on finite dimensional spaces.
For the set $UC_{qc}(n,m)$ we replace the tensor product of two spaces by a single space and instead demand that the $U_{i,j}$'s *-commute with the $V_{k,l}$'s.
Here are some of the things that we know/don't know about these sets.

- $UC_q(n,m) \subseteq UC_{qs}(n,m) \subseteq UC_{qc}(n,m)$.
- For each n,m, $UC_q(n,m)$ and $UC_{qs}(n,m)$ are not closed.
- $UC_{qc}(n,m)$ is closed.
- $UC_q(n,m)^- = UC_{qs}(n,m)^- = \{\big(s(x \otimes y)\big) :$
  $s : U_{nc}(n) \otimes_{min} U_{nc}(m) \to \mathbb{C}$ is a state, x, y as above $\}$.
- $UC_{qs}(2,2) \neq UC_{qc}(2,2)$.
- (Harris) $UC_q(n,m)^- = UC_{qc}(n,m), \forall n,m \iff$ Connes Embedding is true.

Summary: Problems of Connes and Tsirelson are closely tied to embezzlement and to coherent embezzlement games.
Maybe embezzlement will give us a way to swindle a solution to these problems!

Thanks!