The classical analogue of quantum mechanics

Māris Ozols

Based on joint work with
Graeme Smith and
John Smolin from IBM

January 16, 2014

Outline

The classical analogue of

1. Mixed states
2. Quantum entropy
3. Multipartite states
4. Bound entanglement and superactivation

The right attitude…

I think I can safely say that nobody understands quantum mechanics. So do not take the lecture too seriously, feeling that you really have to understand in terms of some model what I am going to describe, but just relax and enjoy it. I am going to tell you what nature behaves like. If you will simply admit that maybe she does behave like this, you will find her a delightful, entrancing thing. Do not keep saying to yourself, if you can possibly avoid it, 'But how can it be like that?' because you will get 'down the drain', into a blind alley from which nobody has yet escaped. Nobody knows how it can be like that.

Richard P. Feynman, The Messenger Lectures, 1964, Cornell

The right attitude…

I think I can safely say that nobody understands quantum mechanics. So do not take the lecture too seriously, ~~feeling that you really have to understand in terms of some model what I am going to describe~~, but just relax and enjoy it. I am going to tell you what nature behaves like. If you will simply admit that maybe she does behave like this, you will find her a delightful, entrancing thing. Do not keep saying to yourself, if you can possibly avoid it, 'But how can it be like that?' because you will get 'down the drain', into a blind alley from which nobody has yet escaped. Nobody knows how it can be like that.

Richard P. Feynman, The Messenger Lectures, 1964, Cornell

Classical-quantum interplay

Examples

- Classical / quantum walks [Sze04]
- Classical / quantum error correcting codes
- Classical / quantum rejection sampling [ORR13]
- Conditional distributions / superoperators [Lei06, LS11]
- …

Classical-quantum interplay

Examples

- Classical / quantum walks [Sze04]
- Classical / quantum error correcting codes
- Classical / quantum rejection sampling [ORR13]
- Conditional distributions / superoperators [Lei06, LS11]
- ...

New insights

- New bound entangled states with private key
- Implications for classical key distillation protocols

Motivation

The Horodecki *Magnum Opus* [HHHH09]

The classical key agreement scenario is an elder sibling of an entanglement-distillation-like scenario. [...] The analogy has been recently explored and proved to be fruitful for establishing new phenomena in classical cryptography, and new links between privacy and entanglement theory. The connections are quite beautiful, however, they still remain not fully understood.

Previous work

Classical information theory

Secret key from common randomness by public discussion [Mau93, AC93]

Entanglement and distillation

- Classical analog of entanglement [CP02]

Quantum	Classical
$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$p_{00} = p_{11} = \frac{1}{2}$
Quantum bits	Secret classical bits
Classical bits	Public classical bits

- Classical vs. quantum key distillation [CEH$^+$07]

Negative information

- Conditional quantum entropy can be negative [HOW05]
- This has a classical analogue [OSW05]

Distributions vs. quantum states

State space

Classical	Quantum
$P_A \in \mathbb{R}^n_+$	$\|\psi\rangle_A \in \mathbb{C}^n$
$\sum_a p(a) = 1$	$\sum_a \|\psi(a)\|^2 = 1$

Correspondence

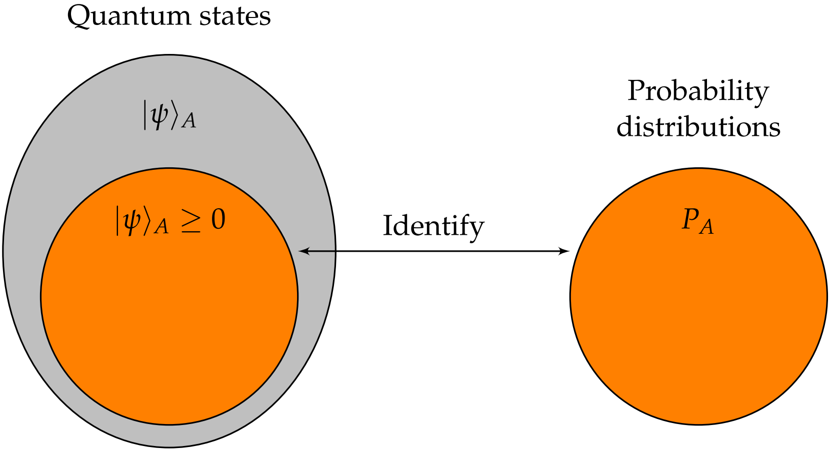
$$p(a) = |\psi(a)|^2 \qquad \left(P_A = |\psi\rangle_A^2\right)$$

$$|\psi\rangle_A = \sum_a \sqrt{p(a)}|a\rangle_A \qquad \left(|\psi\rangle_A = \sqrt{P_A}\right)$$

"Classical" quantum states

If $|\psi\rangle_A \geq 0$ we can identify $|\psi\rangle_A$ and P_A
(they are different descriptions of the same object)

The basic quantum-classical correspondence



Manifesto

1. In quantum mechanics, we never talk or think of a pure or mixed state on a given quantum system. Instead, we only use the notion of a pure state on the given system *and* a purifying system (often referred to as environment or eavesdropper). This is w.l.o.g. and is commonly referred to as the "Church of the Larger Hilbert Space".

Manifesto

1. In quantum mechanics, we never talk or think of a pure or mixed state on a given quantum system. Instead, we only use the notion of a pure state on the given system *and* a purifying system (often referred to as environment or eavesdropper). This is w.l.o.g. and is commonly referred to as the "Church of the Larger Hilbert Space".

2. Similarly, in classical theory, we never talk or think of a probability distribution on a given state space. Instead, we always explicitly include an extra eavesdropper system and describe the joint distribution on both systems.

   Talking of probability distributions without referring to the extra eavesdropper system makes no sense!

States on a single system

$$\cancel{|\psi\rangle_A}$$

States on a single system
(and environment!)

$$|\psi\rangle_A \mapsto |\psi\rangle_A |0\rangle_E$$

Classical Schmidt decomposition

- Schmidt decomposition:

$$|\psi\rangle_{AE} = \sum_i \sqrt{\lambda_i}|\alpha_i\rangle_A|\varepsilon_i\rangle_E$$

$$\langle\alpha_i|\alpha_j\rangle = \delta_{ij} \qquad \langle\varepsilon_i|\varepsilon_j\rangle = \delta_{ij}$$

Classical Schmidt decomposition

- Schmidt decomposition:

$$|\psi\rangle_{AE} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$\langle \alpha_i | \alpha_j \rangle = \delta_{ij} \qquad \langle \varepsilon_i | \varepsilon_j \rangle = \delta_{ij}$$

- P_{AE} has a *classical Schmidt decomposition* if

$$|\psi\rangle_{AE} = \sqrt{P_{AE}} \quad \text{has} \quad |\alpha_i\rangle \geq 0 \quad \text{and} \quad |\varepsilon_i\rangle \geq 0$$

$$\begin{tikzcd}
P_{AE} \arrow[r, "\sqrt{\cdot}"] \arrow[d, rightsquigarrow, "\text{classical Schmidt decomposition}"'] & |\psi\rangle_{AE} \arrow[d, "\text{Schmidt decomposition}"] \\
??? & |\alpha_i\rangle_A, |\varepsilon_i\rangle_E \arrow[l, "(\,\cdot\,)^2"']
\end{tikzcd}$$

Mixed distributions

Definition

P_{AE} has a *classical Schmidt decomposition* (CSD) if

$$\sqrt{P_{AE}} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$|\alpha_i\rangle \geq 0 \text{ have disjoint supports}$$

$$|\varepsilon_i\rangle \geq 0 \text{ have disjoint supports}$$

Mixed distributions

Definition

P_{AE} has a *classical Schmidt decomposition* (CSD) if

$$\sqrt{P_{AE}} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$|\alpha_i\rangle \geq 0 \text{ have disjoint supports}$$

$$|\varepsilon_i\rangle \geq 0 \text{ have disjoint supports}$$

Postulate

If P_{AE} has no CSD, it is not a “valid” distribution!

Mixed distributions

Definition

P_{AE} has a *classical Schmidt decomposition* (CSD) if

$$\sqrt{P_{AE}} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$|\alpha_i\rangle \geq 0 \text{ have disjoint supports}$$

$$|\varepsilon_i\rangle \geq 0 \text{ have disjoint supports}$$

Postulate

If P_{AE} has no CSD, it is not a "valid" distribution!

Observations

- Just as we identify $|\psi\rangle_{AE}$ and ρ_A, we also identify "valid" P_{AE} with *mixed distributions* on A

Mixed distributions

Definition

P_{AE} has a *classical Schmidt decomposition* (CSD) if

$$\sqrt{P_{AE}} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$|\alpha_i\rangle \geq 0 \text{ have disjoint supports}$$

$$|\varepsilon_i\rangle \geq 0 \text{ have disjoint supports}$$

Postulate

If P_{AE} has no CSD, it is not a “valid” distribution!

Observations

- Just as we identify $|\psi\rangle_{AE}$ and ρ_A, we also identify “valid” P_{AE} with *mixed distributions* on A
- P_{AE} is *pure* iff the sum contains one term

Mixed distributions

Definition

P_{AE} has a *classical Schmidt decomposition* (CSD) if

$$\sqrt{P_{AE}} = \sum_i \sqrt{\lambda_i} |\alpha_i\rangle_A |\varepsilon_i\rangle_E$$

$$|\alpha_i\rangle \geq 0 \text{ have disjoint supports}$$

$$|\varepsilon_i\rangle \geq 0 \text{ have disjoint supports}$$

Postulate

If P_{AE} has no CSD, it is not a "valid" distribution!

Observations

- Just as we identify $|\psi\rangle_{AE}$ and ρ_A, we also identify "valid" P_{AE} with *mixed distributions* on A
- P_{AE} is *pure* iff the sum contains one term
- "Valid" P_{AE}, $|\psi\rangle_{AE}$, and ρ_A describe the same object. It needs a new name…

quant[um]

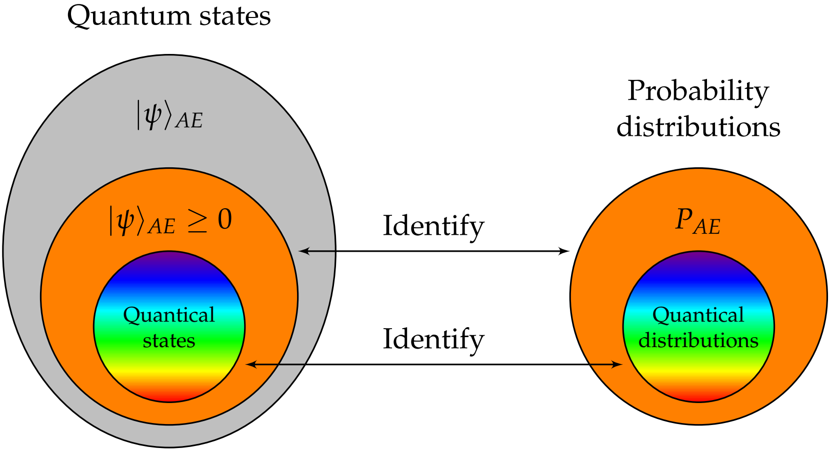
+

[class]*ical*

=

quantical

Correspondences



Examples

		E	
		0	1
A	0	$\frac{1}{2}$	
	1	$\frac{1}{2}$	

Examples

		E	
		0	1
A	0	$\frac{1}{2}$	
	1	$\frac{1}{2}$	

$$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$$

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_E + \frac{1}{\sqrt{2}} |1\rangle_A |1\rangle_E$$

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_E + \frac{1}{\sqrt{2}} |1\rangle_A |1\rangle_E$$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_E + \frac{1}{\sqrt{2}} |1\rangle_A |1\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Not quantical!

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_E + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Not quantical!

- Reduced distributions P_A are the *same* in all three cases

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_E + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_E$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Not quantical!

- Reduced distributions P_A are the *same* in all three cases
- E's knowledge about A *differs* in all three cases

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$

$\rho_A = |+\rangle\langle+|$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_E + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_E$

$\rho_A = I/2$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Not quantical!

- Reduced distributions P_A are the *same* in all three cases
- E's knowledge about A *differs* in all three cases

Examples

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{2}$	

$|\psi\rangle_{AE} = |+\rangle_A |0\rangle_E$

$\rho_A = |+\rangle\langle+|$

A \ E	0	1
0	$\frac{1}{2}$	
1		$\frac{1}{2}$

$|\psi\rangle_{AE} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_E + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_E$

$\rho_A = I/2$

A \ E	0	1
0	$\frac{1}{2}$	
1	$\frac{1}{4}$	$\frac{1}{4}$

Not quantical!

- Reduced distributions P_A are the *same* in all three cases
- E's knowledge about A *differs* in all three cases
- The quantical state space is *not* convex:

$$\frac{1}{2}\begin{bmatrix} 1 & \\ & \end{bmatrix} + \frac{1}{4}\begin{bmatrix} & \\ 1 & \end{bmatrix} + \frac{1}{4}\begin{bmatrix} & \\ & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \\ \frac{1}{4} & \frac{1}{4} \end{bmatrix}$$

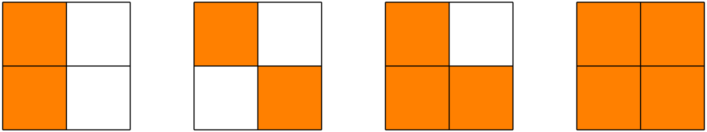
When is P_{AE} quantical?

(i) $\sqrt{P_{AE}}$ has a classical Schmidt decomposition

(ii) P_{AE} is block-diagonal:

$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

where $\Lambda_i = u_i \cdot v_i^{\mathsf{T}}$ for some column vectors $u_i, v_i > 0$



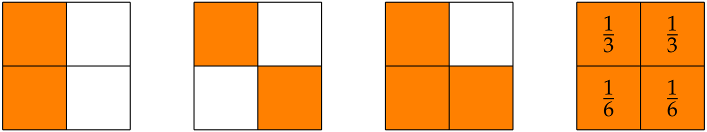
When is P_{AE} quantical?

(i) $\sqrt{P_{AE}}$ has a classical Schmidt decomposition

(ii) P_{AE} is block-diagonal:

$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

where $\Lambda_i = u_i \cdot v_i^\mathsf{T}$ for some column vectors $u_i, v_i > 0$



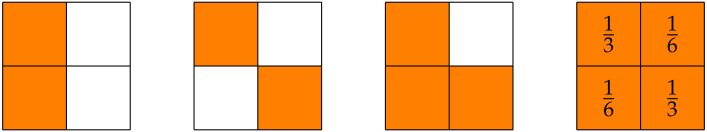
When is P_{AE} quantical?

(i) $\sqrt{P_{AE}}$ has a classical Schmidt decomposition

(ii) P_{AE} is block-diagonal:

$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

where $\Lambda_i = u_i \cdot v_i^{\mathsf{T}}$ for some column vectors $u_i, v_i > 0$



Entropy

Quantical entropy

Computing entropy from purification

- Let $\lambda_i :=$ the sum of entries of Λ_i

$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

Quantical entropy

Computing entropy from purification

- Let $\lambda_i :=$ the sum of entries of Λ_i

$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

- The *quantical entropy* of P_{AE} is

$$H(P_{AE}) := H(\lambda_1, \ldots, \lambda_m)$$

Quantical entropy

Computing entropy from purification

- Let $\lambda_i :=$ the sum of entries of Λ_i

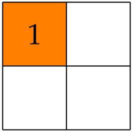
$$P_{AE} = \begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda_m \end{pmatrix}$$

- The *quantical entropy* of P_{AE} is

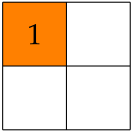
$$H(P_{AE}) := H(\lambda_1, \ldots, \lambda_m)$$

- Claim: $H(P_{AE}) = S(\rho_A)$

Quiz!

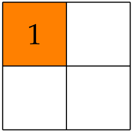


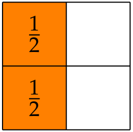
Quiz!



$$H(1) = 0$$

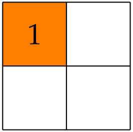
Quiz!



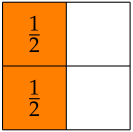


$$H(1) = 0$$

Quiz!

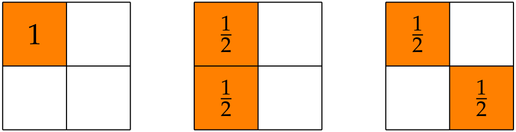


$$H(1) = 0$$



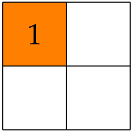
$$H(1) = 0$$

Quiz!

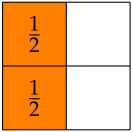


$H(1) = 0$ $\quad$ $H(1) = 0$

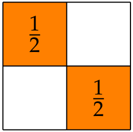
Quiz!



$H(1) = 0$

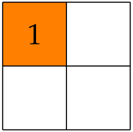


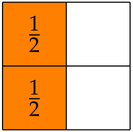
$H(1) = 0$

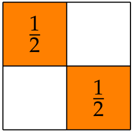


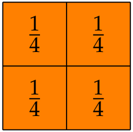
$H\left(\frac{1}{2}, \frac{1}{2}\right) = 1$

Quiz!



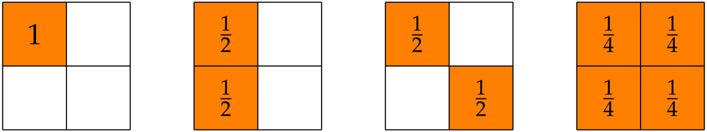






$H(1) = 0$ $\quad$ $H(1) = 0$ $\quad$ $H\left(\frac{1}{2}, \frac{1}{2}\right) = 1$

Quiz!



$H(1) = 0$ $\quad$ $H(1) = 0$ $\quad$ $H\left(\frac{1}{2}, \frac{1}{2}\right) = 1$ $\quad$ $H(1) = 0$

Quiz!

1	

$H(1) = 0$

$\frac{1}{2}$	
$\frac{1}{2}$	

$H(1) = 0$

$\frac{1}{2}$	
	$\frac{1}{2}$

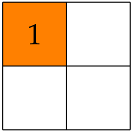
$H\left(\frac{1}{2}, \frac{1}{2}\right) = 1$

$\frac{1}{4}$	$\frac{1}{4}$
$\frac{1}{4}$	$\frac{1}{4}$

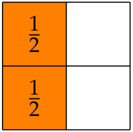
$H(1) = 0$

$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$
$\frac{1}{8}$	0	$\frac{1}{8}$
$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$

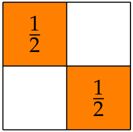
Quiz!



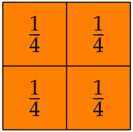
$H(1) = 0$



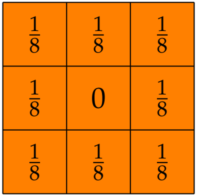
$H(1) = 0$



$H\left(\frac{1}{2}, \frac{1}{2}\right) = 1$



$H(1) = 0$

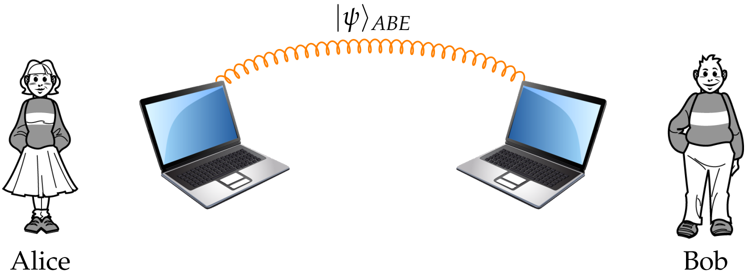


Gotcha!

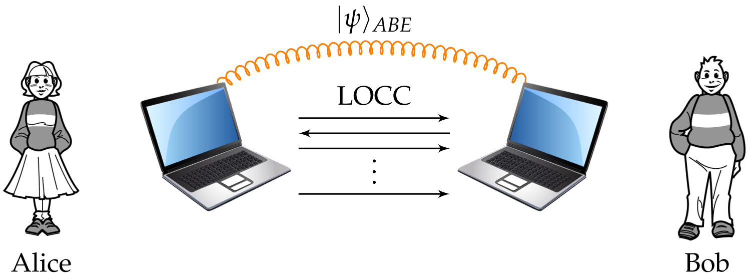
Multipartite states

$\left(|\psi\rangle_{ABE} \text{ and } P_{ABE}\right)$

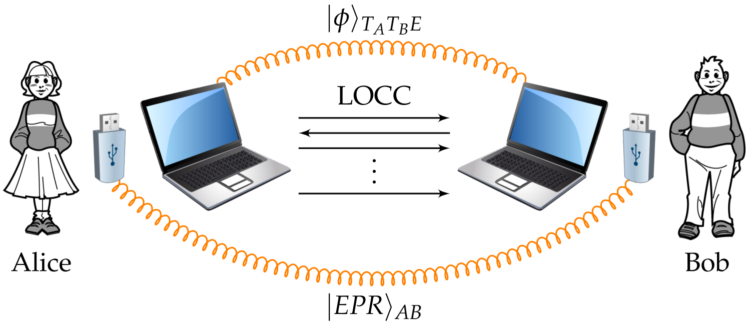
Distillation with remanent devices



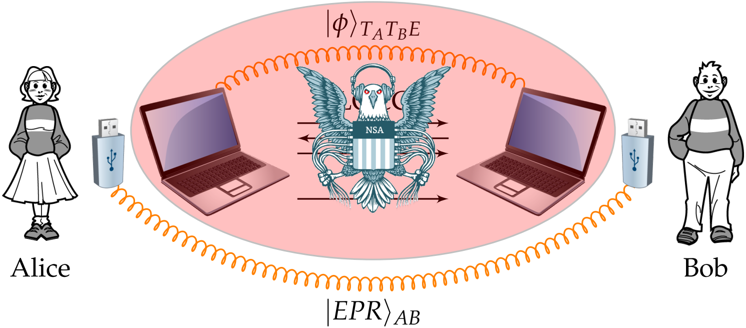
Distillation with remanent devices



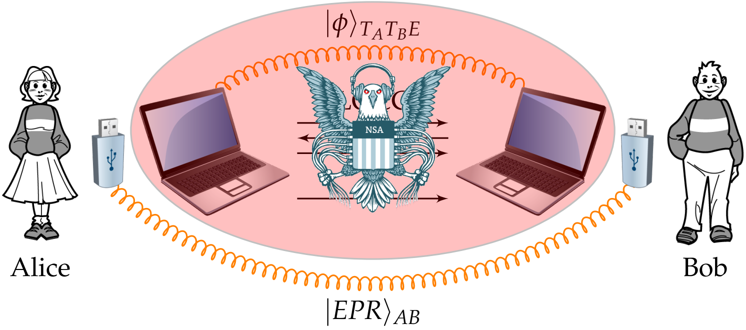
Distillation with remanent devices

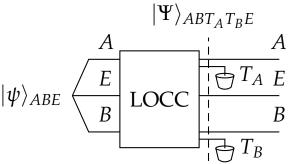


Distillation with remanent devices



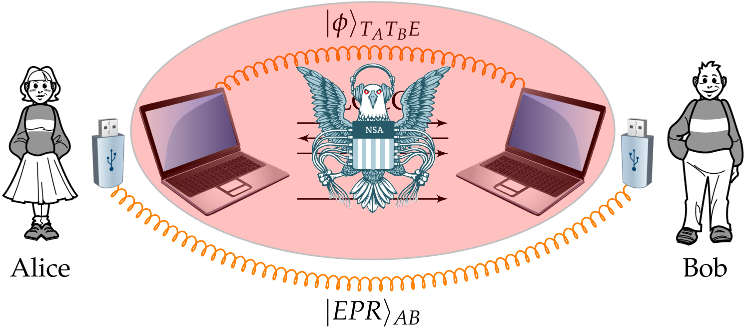
Distillation with remanent devices

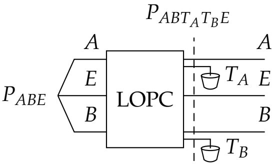




If A and B can distill an EPR pair, their key is safe even if E can also access the trash systems T_A and T_B

Distillation with remanent devices





If A and B can distill an EPR pair, their key is safe even if E can also access the trash systems T_A and T_B

cl[assical] *en*[t]*anglement*

=

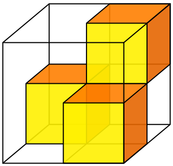
enclanglement

Unambiguous tripartite distributions

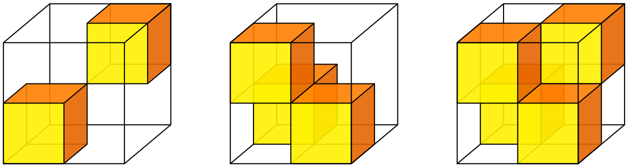
Olive property

P_{ABE} is *unambiguous* if any single party's state can be unambiguously determined by the rest of the parties

$$\forall b,e : |\{a : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a,b : |\{e : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a,e : |\{b : p(a,b,e) \neq 0\}| \leq 1$$



Genuine tripartite enclanglement



GHZ	W	Odd
000	100	100
111	010	010
	001	001
		111

Three qubits can be entangled only in two ways [DVC00] because $|GHZ\rangle$ and $|Odd\rangle$ are equivalent via $H^{\otimes 3}$

Private bound entanglement and superactivation

Bound entanglement with private key

Bound entanglement

- **Task:** Distill EPR pairs from a mixed state by LOCC
- *Bound entangled states* require entanglement to make, but no EPR pairs can be distilled from them by LOCC
- Example: PPT states

Bound entanglement with private key

Bound entanglement

- **Task:** Distill EPR pairs from a mixed state by LOCC
- *Bound entangled states* require entanglement to make, but no EPR pairs can be distilled from them by LOCC
- Example: PPT states

Private key

- **Task:** Distill private random bits by LOCC
- Possible strategy: distill EPR pairs and measure them
- Sometimes key can be extracted even when no EPR pairs can be distilled [HHHO05, HPHH08]
- We call this phenomenon *private bound entanglement*

Classical analogue

Bound enclanglement

- **Task:** Distill private key by two-way *public discussion* from a quantical distribution (this includes error correction and privacy amplification)
- Public discussion preserves quanticality
- Key cannot be distilled from a quantical PPT distribution (otherwise EPR pairs could be distilled by LOCC)

Classical analogue

Bound enclanglement

- **Task:** Distill private key by two-way *public discussion* from a quantical distribution (this includes error correction and privacy amplification)
- Public discussion preserves quanticality
- Key cannot be distilled from a quantical PPT distribution (otherwise EPR pairs could be distilled by LOCC)

Private key

- **Task:** Distill private key by public discussion followed by *local noisy processing* (i.e., erasing trash registers)
- **Rate:** $$K(P_{ABE}) = \max_{A\to X\to M} \left[I(X;B|M) - I(X;E|M) \right]$$ $$\geq \max_{A\to X} \left[I(X;B) - I(X;E) \right]$$

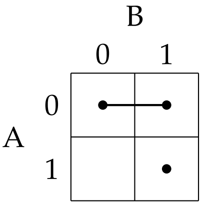
Correspondence

	Quantum	*Classical*
Unambiguous states	$\|\psi\rangle_{ABE}$	P_{ABE}
Entanglement distillation (public trash)	$D(\psi_{ABE})$	$K_{\mathrm{PD}}(P_{ABE})$
Private key distillation (private trash)	$K(\psi_{ABE})$	$K(P_{ABE})$

Theorem

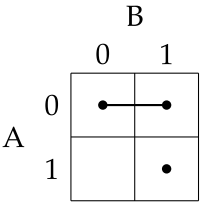
1. If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is unambiguous then $D(\psi_{ABE}) \geq K_{\mathrm{PD}}(P_{ABE})$ and $K(\psi_{ABE}) \geq K(P_{ABE})$
2. There exist unambiguous distributions P_{ABE} with $K_{\mathrm{PD}}(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Recipe



$$\big(a|00\rangle_{AB} + b|01\rangle_{AB}\big)\,|x\rangle_E$$
$$+\, c|11\rangle_{AB}|y\rangle_E$$

Recipe



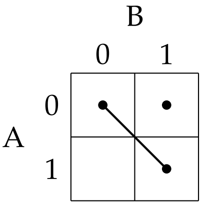
$$\big(a|00\rangle_{AB} + b|01\rangle_{AB}\big)\,|x\rangle_E$$

$$+\,c|11\rangle_{AB}|y\rangle_E$$

Unambiguous

- Union of disjoint cliques
- No repeated rows or columns within a clique

Recipe

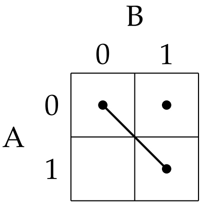


$$\left(a|00\rangle_{AB} + b|11\rangle_{AB}\right)|x\rangle_E$$
$$+\, c|01\rangle_{AB}|y\rangle_E$$

Unambiguous

- Union of disjoint cliques
- No repeated rows or columns within a clique

Recipe



$$\big(a|00\rangle_{AB} + b|11\rangle_{AB}\big)|x\rangle_E$$
$$+ c|01\rangle_{AB}|y\rangle_E$$

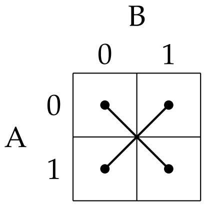
Unambiguous

- Union of disjoint cliques
- No repeated rows or columns within a clique

PT-invariant

- Union of crosses
- Each cross has zero determinant

Recipe



$$\left(a|00\rangle_{AB} + b|11\rangle_{AB}\right)|x\rangle_E$$
$$+\left(c|01\rangle_{AB} + d|10\rangle_{AB}\right)|y\rangle_E$$

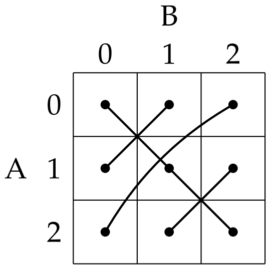
Unambiguous

- Union of disjoint cliques
- No repeated rows or columns within a clique

PT-invariant

- Union of crosses
- Each cross has zero determinant

Example in 3×3

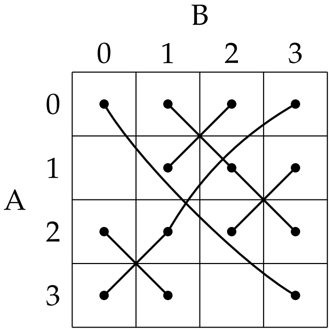


$$K(P_{ABE}) \geq 0.0057852$$

$$P_{AB} = \begin{pmatrix} 0.167184 & 0.171529 & 0.001243 \\ 0.089041 & 0.091355 & 0.017492 \\ 0.441714 & 0.017157 & 0.003285 \end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix} 1 & 0 & 0.670965 \\ 0 & 1 & 0.329035 \end{pmatrix}$$

Example in 4 × 4

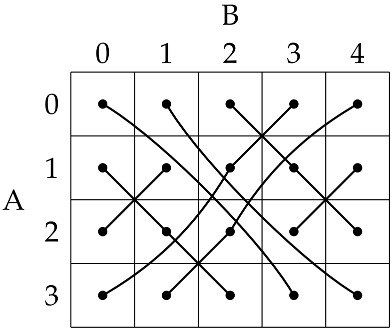


$$K(P_{ABE}) \geq 0.0293914$$

$$K(P_{ABE}) \geq 0.0213399$$

in [HPHH08]

Example in 4×5



$$K(P_{ABE}) \geq 0.0480494$$

Superactivation

Superactivation [SY08]

- Let $\mathcal{N}$ have bound entangled Choi matrix with private key
- Let $\mathcal{E}$ be the 50% erasure channel
- $Q(\mathcal{N}) = Q(\mathcal{E}) = 0$
- $Q(\mathcal{N} \otimes \mathcal{E}) \geq \frac{1}{2}P(\mathcal{N})$
- This holds also for the quantical capacities!

Summary

1. Classical analogue of quantum mechanics

Summary

1. Classical analogue of quantum mechanics
2. It is essential to always include environment

Summary

1. Classical analogue of quantum mechanics
2. It is essential to always include environment
3. Classical analogue of bound entanglement

Summary

1. Classical analogue of quantum mechanics
2. It is essential to always include environment
3. Classical analogue of bound entanglement
4. Better examples of bound entanglement with key

Summary

1. Classical analogue of quantum mechanics
2. It is essential to always include environment
3. Classical analogue of bound entanglement
4. Better examples of bound entanglement with key
5. Noisy processing is essential for classical key agreement

Summary

1. Classical analogue of quantum mechanics
2. It is essential to always include environment
3. Classical analogue of bound entanglement
4. Better examples of bound entanglement with key
5. Noisy processing is essential for classical key agreement

Richard Feynman: *I think I can safely say that nobody understands quantum mechanics*

This work: *To fully understand something quantum, one has to at least understand its quantical equivalent*

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart
2. How does quantical mechanics fit into existing axiomatizations of quantum theory?

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart
2. How does quantical mechanics fit into existing axiomatizations of quantum theory?
3. Can Bell inequalities be violated in quantical theory? (Probably not.)

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart
2. How does quantical mechanics fit into existing axiomatizations of quantum theory?
3. Can Bell inequalities be violated in quantical theory? (Probably not.)
4. Is there *quantical* NPT bound enclanglement?

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart
2. How does quantical mechanics fit into existing axiomatizations of quantum theory?
3. Can Bell inequalities be violated in quantical theory? (Probably not.)
4. Is there *quantical* NPT bound enclanglement?
5. Is the optimal protocol for distilling entanglement or key from a quantical state also quantical?

Open questions

1. Other ways of bringing quantum and classical worlds closer together or further apart
2. How does quantical mechanics fit into existing axiomatizations of quantum theory?
3. Can Bell inequalities be violated in quantical theory? (Probably not.)
4. Is there *quantical* NPT bound enclanglement?
5. Is the optimal protocol for distilling entanglement or key from a quantical state also quantical?
6. Does quantical theory add anything to the ontic [PBR12] vs. epistemic [Spe07] debate?

Thank you!

Bibliography I

[AC93] Rudolph F. Ahlswede and Imre Csiszár.
Common randomness in information theory and cryptography. I. Secret sharing.
Information Theory, IEEE Transactions on, 39(4):1121–1132, 1993.
doi:10.1109/18.243431.

[CEH+07] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner.
Unifying classical and quantum key distillation.
In Salil P. Vadhan, editor, *Theory of Cryptography*, volume 4392 of *Lecture Notes in Computer Science*, pages 456–478. Springer, 2007.
arXiv:quant-ph/0608199,
doi:10.1007/978-3-540-70936-7_25.

[CP02] Daniel Collins and Sandu Popescu.
Classical analog of entanglement.
Phys. Rev. A, 65(3):032321, Feb 2002.
arXiv:quant-ph/0107082,doi:10.1103/PhysRevA.65.032321.

[DVC00] Wolfgang Dür, Guifre Vidal, and J. Ignacio Cirac.
Three qubits can be entangled in two inequivalent ways.
Phys. Rev. A, 62(6):062314, Nov 2000.
arXiv:quant-ph/0005115,doi:10.1103/PhysRevA.62.062314.

Bibliography II

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki.
Quantum entanglement.
Rev. Mod. Phys., 81(2):865–942, Jun 2009.
`arXiv:arXiv:quant-ph/0702225`,
`doi:10.1103/RevModPhys.81.865`.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim.
Secure key from bound entanglement.
Phys. Rev. Lett., 94(16):160502, Apr 2005.
`arXiv:quant-ph/0309110`,
`doi:10.1103/PhysRevLett.94.160502`.

[HOW05] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter.
Partial quantum information.
Nature, 436:673–676, 2005.
`arXiv:quant-ph/0505062`,`doi:10.1038/nature03909`.

[HPHH08] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki.
Low-dimensional bound entanglement with one-way distillable cryptographic key.
Information Theory, IEEE Transactions on, 54(6):2621–2625, 2008.
`arXiv:quant-ph/0506203`,`doi:10.1109/TIT.2008.921709`.

Bibliography III

[Lei06] Matthew S. Leifer.
Quantum dynamics as an analog of conditional probability.
Phys. Rev. A, 74(4):042310, Oct 2006.
arXiv:quant-ph/0606022, doi:10.1103/PhysRevA.74.042310.

[LS11] Matthew S. Leifer and Robert W. Spekkens.
Formulating quantum theory as a causally neutral theory of Bayesian inference.
2011.
arXiv:1107.5849.

[Mau93] Ueli M. Maurer.
Secret key agreement by public discussion from common information.
Information Theory, IEEE Transactions on, 39(3):733–742, 1993.
doi:10.1109/18.256484.

[ORR13] Maris Ozols, Martin Roetteler, and Jérémie Roland.
Quantum rejection sampling.
ACM Trans. Comput. Theory, 5(3):11:1–11:33, August 2013.
arXiv:1103.2774, doi:10.1145/2493252.2493256.

[OSW05] Jonathan Oppenheim, Robert W. Spekkens, and Andreas Winter.
A classical analogue of negative information.
2005.
arXiv:quant-ph/0511247.

Bibliography IV

[PBR12] Matthew F. Pusey, Jonathan Barrett, and Terry Rudolph.
On the reality of the quantum state.
Nature Physics, 8(6):475–478, 2012.
arXiv:1111.3328, doi:10.1038/nphys2309.

[Spe07] Robert W. Spekkens.
Evidence for the epistemic view of quantum staappendices oftes: A toy theory.
Phys. Rev. A, 75(3):032110, Mar 2007.
arXiv:quant-ph/0401052, doi:10.1103/PhysRevA.75.032110.

[SY08] Graeme Smith and Jon Yard.
Quantum communication with zero-capacity channels.
Science, 321(5897):1812–1815, 2008.
arXiv:0807.4935, doi:10.1126/science.1162242.

[Sze04] Mario Szegedy.
Quantum speed-up of Markov chain based algorithms.
In *Proceedings of the 45th IEEE Symposium on Foundations of Computer Science (FOCS'04)*, pages 32–41. IEEE Computer Society Press, 2004.
doi:10.1109/FOCS.2004.53.

Capacities

Quantum capacity

$$Q(\mathcal{N}) \geq \max_{|\psi\rangle_{AA'}} \frac{1}{2} \left[I(A;B) - I(A;E) \right]_{|\phi\rangle_{ABE}}$$

where $\mathcal{N}^{A' \to BE}$ and $|\phi\rangle_{ABE} = U_{\mathcal{N}} |\psi\rangle_{AA'}$

Private capacity

$$P(\mathcal{N}) \geq \max_{\rho_{XA'}} \left[I(X;B) - I(X;E) \right]_{\sigma_{XBE}}$$

where $\rho_{XA'} = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_x^{A'}$ and $\sigma_{XBE} = U_{\mathcal{N}} \rho_{XA'} U_{\mathcal{N}}^\dagger$