

# Quantum Info as Complementary Classical Info: Secret Key and Entanglement Distillation via Processing Complementary Information

Joseph M. Renes  and Jean-Christian Boileau 

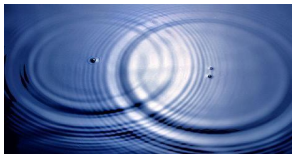


Theoretical Quantum Physics, Institut für Angewandte Physik  
Technische Universität Darmstadt

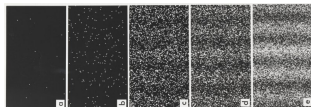


Center for Quantum Information and Quantum Control  
University of Toronto

## Complementarity is the essence of quantum mechanics...

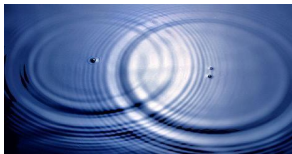


or

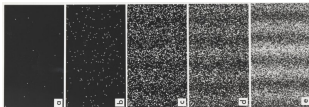


The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

## Complementarity is the essence of quantum mechanics...



or



The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

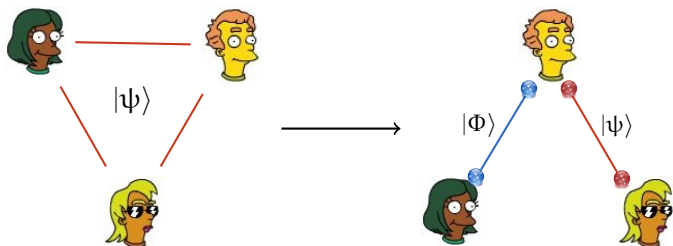
## ...but does it really *explain* anything?

YES! We can directly and concretely understand several tasks in quantum information theory in terms of complementarity.

## Outline

- 1 Entanglement distillation and state merging via decoupling
- 2 The complementarity approach
- 3 Key distillation, channel superactivation & quantum data hiding

# Entanglement Distillation and State Merging



- ☞ Initially Alice, Bob, and Eve share (many copies of) a pure state  $|\psi\rangle$ .
- ☞ In *entanglement distillation* Alice and Bob create entangled states  $|\Phi\rangle$  using only one-way classical communication.
- ☞ In the *state merging* protocol Alice transfers her part of the purification of Eve's system to Bob.
- ➡ Both can be performed simultaneously.

☞ Entanglement distillation rate

$$E_{\rightarrow}(\psi) \geq H(B) - H(AB) = -H(A|B).$$

☞ Communication cost

$$C_{\rightarrow}(\psi) \geq H(A) + H(E) - H(AE) = I(A : E)$$

☞ State merging at the same rates/costs Horodecki, Oppenheim, Winter  
Nature **436** 7051 (2005)

☞ Channel coding theorem from entanglement distillation via teleportation



Decouple  
Alice & Eve



☞ Uhlmann's theorem for entanglement distillation: Schumacher & Westmoreland QIP 1 5 (2002).

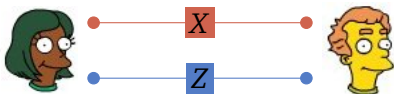
$$\begin{aligned} \psi^A &\simeq \mathbb{1}^A/d^A \quad \text{and} \quad \psi^{AE} \simeq \psi^A \otimes \psi^E \\ &\Downarrow \quad \exists U^B \quad \text{s.t.} \\ U^B |\psi\rangle^{ABE} &\simeq \sum_{jk} \sqrt{q_k/d^A} |j\rangle^A |j, k\rangle^B |k\rangle^E \end{aligned}$$

- $d^A$  is the dimension of  $A$
- eigenvalues/vectors of  $\psi^A$  ( $\psi^E$ ) are  $1/d^A$ ,  $|j\rangle^A$  ( $q_k, |k\rangle^E$ ),
- $|j, k\rangle^B$  are orthonormal.

☞ By coherently measuring  $B$ ,  $\psi^{AB}$  can be (nearly) transformed into  $\Phi^{AB}$ .

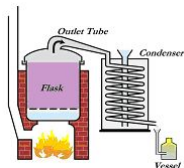
## Complementarity-based Approach

Couple Alice and Bob classically, twice.



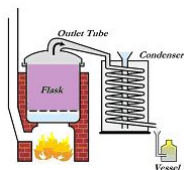
- ☞ Quantum correlations between Alice and Bob are equivalent to two complementary classical correlations, say  $X$  and  $Z$  correlations.
- ☞ If  $H(Z^A|B) = H(X^A|B) = 0$ , then by local operations  $\psi^{AB} \rightarrow \Phi^{AB}$ .
- ☞ Quantum error correction strategy. But can we achieve the known rates? YES!
- ☞ Gives an explicit construction of the decoder

## Entanglement Distillation. . .



Given many copies of an arbitrary resource state,  $\Psi^{AB} = (\psi^{AB})^{\otimes n}$ , convert into an (approximate) maximally entangled state using local operations and (one-way) classical communication (with high probability).

## Entanglement Distillation. . .



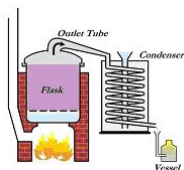
Given many copies of an arbitrary resource state,  $\Psi^{AB} = (\psi^{AB})^{\otimes n}$ , convert into an (approximate) maximally entangled state using local operations and (one-way) classical communication (with high probability).

... by transmitting “missing” information

X H(X<sup>A</sup>)

Z H(Z<sup>A</sup>)

## Entanglement Distillation. . .



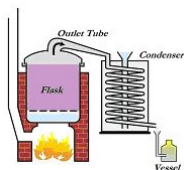
Given many copies of an arbitrary resource state,  $\Psi^{AB} = (\psi^{AB})^{\otimes n}$ , convert into an (approximate) maximally entangled state using local operations and (one-way) classical communication (with high probability).

... by transmitting “missing” information

$$X \quad \begin{array}{|c|c|} \hline I(X^A : B) & H(X^A|B) \\ \hline \end{array}$$

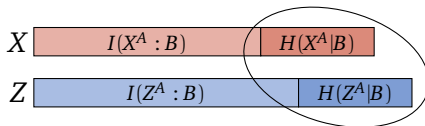
$$Z \quad \begin{array}{|c|c|} \hline I(Z^A : B) & H(Z^A|B) \\ \hline \end{array}$$

## Entanglement Distillation. . .



Given many copies of an arbitrary resource state,  $\Psi^{AB} = (\psi^{AB})^{\otimes n}$ , convert into an (approximate) maximally entangled state using local operations and (one-way) classical communication (with high probability).

. . . by transmitting “missing” information



send this info to Bob.

Here's how:

Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

👉 Task is to extract  $z$  from  $\varphi_k^B$  and  $x$  from  $\vartheta_x^{BS}$ .



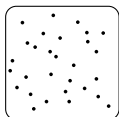
Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

☞ Task is to extract  $z$  from  $\varphi_k^B$  and  $x$  from  $\vartheta_x^{BS}$ .



☞ Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.



Possible  $z$ s



Support of  $\varphi_z^B$

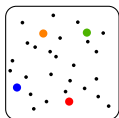
Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

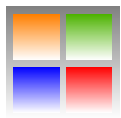
☞ Task is to extract  $z$  from  $\varphi_k^B$  and  $x$  from  $\vartheta_x^{BS}$ .



☞ Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.



Possible  $z$ s



Support of  $\varphi_z^B$

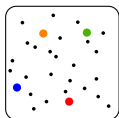
Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

Task is to extract  $z$  from  $\varphi_k^B$  and  $x$  from  $\vartheta_x^{BS}$ .



Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.



Possible  $z$ s



Support of  $\varphi_z^B$

The hints are generated by measuring stabilizers of a (suitably-chosen) CSS code; this ensures hint information exists simultaneously

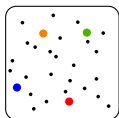
Here's how:

We start with  $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z} |z\rangle^A |\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle^A |\vartheta_x\rangle^{BSE}$

- Task is to extract  $z$  from  $\varphi_k^B$  and  $x$  from  $\vartheta_x^{BS}$ .



- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.



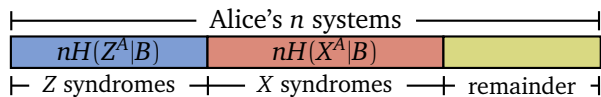
Possible  $z$ s



Support of  $\varphi_z^B$

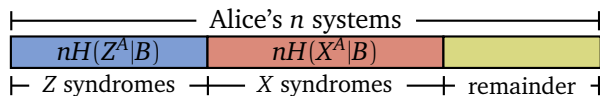
- The hints are generated by measuring stabilizers of a (suitably-chosen) CSS code; this ensures hint information exists simultaneously
- Finally, the (static) HSW theorem sets the size of the hints  $\Rightarrow H(Z^A|B)$ .

At what rates?



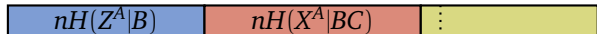
Naïve rate  
 $\Rightarrow 1 - H(Z^A|B) - H(X^A|B)$

## At what rates?



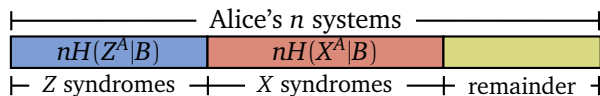
Naïve rate  
 $1 - H(Z^A|B) - H(X^A|B)$

- But it's a two-step process! After step one Bob has a  $Z^A$  basis copy of Alice's system in  $C$ .



Refined rate  
 $1 - H(Z^A|B) - H(X^A|BC)$

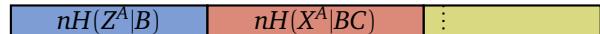
## At what rates?



Naïve rate

$$1 - H(Z^A|B) - H(X^A|B)$$

- But it's a two-step process! After step one Bob has a  $Z^A$  basis copy of Alice's system in  $C$ .



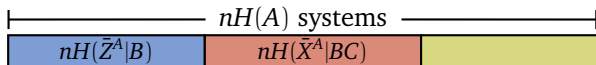
Refined rate

$$1 - H(Z^A|B) - H(X^A|BC)$$

- Voilà! Can show refined rate equals  $-H(A|B)$ .
- However, too much communication is used in the process:  
 $1 + H(E) - H(AE) > I(A : E)$ .

## State merging?

- ☞ The purification of Eve's state is merged in the protocol  
Since Alice and Bob end up with  $|\Phi\rangle$ , the purification has nowhere else to go
- ☞ To fix the communication rate, first compress Alice's state and then run the protocol:  $\psi^A$  eigenbasis defines  $Z^A, Z^A \rightarrow \bar{Z}^A, X^A \rightarrow \bar{X}^A$



- ➡ This would give optimal rates. Can we construct the necessary mmts?
- ☞ Bob can reuse  $Z^A$  mmt for  $\bar{Z}^A$ : compression just throws out nontypical  $Z$ .
- ☞ But what about the  $\bar{X}^A$  measurement?  $\bar{X}^A$  and  $X^A$  have no such relation.
- ➡ Fortunately, the states  $\vartheta_x^{BC}$  are group covariant, which implies that the original HSW mmt can be suitably modified for the compressed state.

## Fundamental results of quantum information theory rest on the phenomenon of complementarity

- ☞ Details: PRA **78**, 032335 (2008); arXiv:0803.3096v2 & upcoming TQC meeting
- ☞ Also useful for key distillation
- ➡ Gives a new take on channel superactivation (send shield over erasure channel)
- ➡ Also highlights link between superactivation and quantum data hiding

