

# Optimal State Merging Without Decoupling

Joseph M. Renes  and Jean-Christian Boileau 



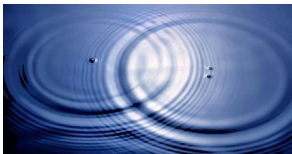
Theoretical Quantum Physics, Institut for Applied Physics  
Technical University of Darmstadt



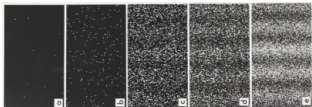
Center for Quantum Information and Quantum Control  
University of Toronto



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

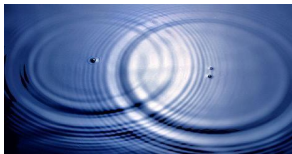


or

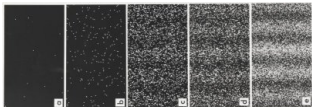


The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

## 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

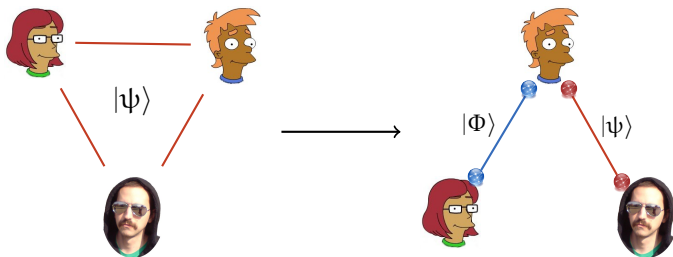
## ...but can we use it in quantum information theory?

YES! We can directly and concretely understand several tasks in QIT in terms of complementarity. In particular, state merging & secret key distillation

## Outline

- 1 Entanglement distillation and state merging via decoupling
- 2 The complementarity approach
  - 👉 It's all about  $X$  and  $Z$
  - 👉 HSW measurement and CSS codes
  - 👉 Copy the  $Z$  information
  - 👉 Compress and use group covariance

# Entanglement Distillation and State Merging



- Initially Alice, Bob, and (St)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 from entanglement distillation via teleportation



Decouple  
Alice & Eve



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

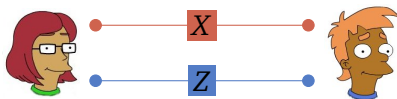
☞ Suppose  $\psi_A \simeq \frac{1}{d_A} \mathbb{1}_A$  and  $\psi_{AE} \simeq \psi_A \otimes \psi_E$

☞ Then  $\exists$  unitary  $U_B$  and partition  $\mathcal{H}_B = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$  such that

1.  $U_B |\psi\rangle_{ABE} \simeq |\Phi\rangle_{AB_1} \otimes |\xi\rangle_{B_2E}$
2.  $|\xi\rangle_{B_2E}$  a purification of  $\psi_E$

## 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.

$$X = \sum_k |k \oplus 1\rangle \langle k|, \quad Z = \sum_k \omega^k |k\rangle \langle k|, \quad \omega = e^{2\pi i/d},$$

- If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .
- Stabilizer-based quantum error correction strategy—protect  $X$  and  $Z$

Claim: If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

**Claim:** If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

☞ Let  $|\tilde{x}\rangle$  be the eigenbasis of  $X$ :  $|\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_z \omega^{xz} |z\rangle$ . Expand  $A$  in  $|z\rangle/|\tilde{x}\rangle$ :

$$|\psi\rangle_{ABE} = \sum_z \sqrt{p_z} |z\rangle_A |\varphi_z\rangle_{BE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle_A |\vartheta_x\rangle_{BE}$$

**Claim:** If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

☞ Let  $|\tilde{x}\rangle$  be the eigenbasis of  $X$ :  $|\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_z \omega^{xz} |z\rangle$ . Expand  $A$  in  $|z\rangle/|\tilde{x}\rangle$ :

$$|\psi\rangle_{ABE} = \sum_z \sqrt{p_z} |z\rangle_A |\varphi_z\rangle_{BE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle_A |\vartheta_x\rangle_{BE}$$

☞  $H(Z_A|B) = H(X_A|B) = 0$  implies both sets  $\{(\varphi_z)_B\}$  and  $\{(\vartheta_x)_B\}$  perfectly distinguishable.

Measure  $B$  with  $P_z$  and  $\tilde{P}_x$  (project onto disjoint supports). First  $P_z: |\psi\rangle_{ABE} \rightarrow |\psi'\rangle_{ACBE}$ ,

**Claim:** If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

☞ Let  $|\tilde{x}\rangle$  be the eigenbasis of  $X$ :  $|\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_z \omega^{xz} |z\rangle$ . Expand  $A$  in  $|z\rangle/|\tilde{x}\rangle$ :

$$|\psi\rangle_{ABE} = \sum_z \sqrt{p_z} |z\rangle_A |\varphi_z\rangle_{BE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle_A |\vartheta_x\rangle_{BE}$$

☞  $H(Z_A|B) = H(X_A|B) = 0$  implies both sets  $\{(\varphi_z)_B\}$  and  $\{(\vartheta_x)_B\}$  perfectly distinguishable.

Measure  $B$  with  $P_z$  and  $\tilde{P}_x$  (project onto disjoint supports). First  $P_z$ :  $|\psi\rangle_{ABE} \rightarrow |\psi'\rangle_{ACBE}$ ,

$$|\psi'\rangle_{ACBE} = \sum_{z,z'} \sqrt{p_z} |z,z'\rangle_{AC} (P_{z'})_B |\varphi_z\rangle_{BE} = \sum_z \sqrt{p_z} |z,z\rangle_{AC} |\varphi_z\rangle_{BE}$$

**Claim:** If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

☞ Let  $|\tilde{x}\rangle$  be the eigenbasis of  $X$ :  $|\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_z \omega^{xz} |z\rangle$ . Expand  $A$  in  $|z\rangle/|\tilde{x}\rangle$ :

$$|\psi\rangle_{ABE} = \sum_z \sqrt{p_z} |z\rangle_A |\varphi_z\rangle_{BE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle_A |\vartheta_x\rangle_{BE}$$

☞  $H(Z_A|B) = H(X_A|B) = 0$  implies both sets  $\{(\varphi_z)_B\}$  and  $\{(\vartheta_x)_B\}$  perfectly distinguishable.

Measure  $B$  with  $P_z$  and  $\tilde{P}_x$  (project onto disjoint supports). First  $P_z$ :  $|\psi\rangle_{ABE} \rightarrow |\psi'\rangle_{ACBE}$ ,

$$\begin{aligned} |\psi'\rangle_{ACBE} &= \sum_{z,z'} \sqrt{p_z} |z,z'\rangle_{AC} (P_{z'})_B |\varphi_z\rangle_{BE} = \sum_z \sqrt{p_z} |z,z\rangle_{AC} |\varphi_z\rangle_{BE} \\ &= \frac{1}{\sqrt{d}} \sum_{xz} \sqrt{q_x} \omega^{xz} |z,z\rangle_{AC} |\vartheta_x\rangle_{BE} = \sum_x \sqrt{q_x} Z_C^x |\Phi\rangle_{AC} |\vartheta_x\rangle_{BE}, \end{aligned}$$

since  $\sqrt{p_z} |\varphi_z\rangle_{BE} = \frac{1}{\sqrt{d}} \sum_x \sqrt{q_x} \omega^{xz} |\vartheta_x\rangle_{BE}$ .

Claim: If  $H(Z_A|B) = H(X_A|B) = 0$ , then by local operations  $\psi_{AB} \rightarrow \Phi_{AB}$ .

Let  $|\tilde{x}\rangle$  be the eigenbasis of  $X$ :  $|\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_z \omega^{xz} |z\rangle$ . Expand  $A$  in  $|z\rangle/|\tilde{x}\rangle$ :

$$|\psi\rangle_{ABE} = \sum_z \sqrt{p_z} |z\rangle_A |\varphi_z\rangle_{BE} = \sum_x \sqrt{q_x} |\tilde{x}\rangle_A |\vartheta_x\rangle_{BE}$$

$H(Z_A|B) = H(X_A|B) = 0$  implies both sets  $\{|\varphi_z\rangle_B\}$  and  $\{|\vartheta_x\rangle_B\}$  perfectly distinguishable.

Measure  $B$  with  $P_z$  and  $\tilde{P}_x$  (project onto disjoint supports). First  $P_z$ :  $|\psi\rangle_{ABE} \rightarrow |\psi'\rangle_{ACBE}$ ,

$$\begin{aligned} |\psi'\rangle_{ACBE} &= \sum_{z,z'} \sqrt{p_z} |z,z'\rangle_{AC} (P_{z'})_B |\varphi_z\rangle_{BE} = \sum_z \sqrt{p_z} |z,z\rangle_{AC} |\varphi_z\rangle_{BE} \\ &= \frac{1}{\sqrt{d}} \sum_{xz} \sqrt{q_x} \omega^{xz} |z,z\rangle_{AC} |\vartheta_x\rangle_{BE} = \sum_x \sqrt{q_x} Z_C^x |\Phi\rangle_{AC} |\vartheta_x\rangle_{BE}, \end{aligned}$$

since  $\sqrt{p_z} |\varphi_z\rangle_{BE} = \frac{1}{\sqrt{d}} \sum_x \sqrt{q_x} \omega^{xz} |\vartheta_x\rangle_{BE}$ .

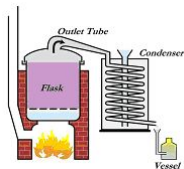
Measuring  $(\tilde{P}_x)_B$  and applying  $Z_C^x$  gives  $|\psi''\rangle_{ACBE} = |\Phi\rangle_{AC} \otimes \sum_x \sqrt{q_x} |\vartheta_x\rangle_{BE}$

Full  $X$  and  $Z$  information enough to create entanglement (not too surprising)

- also performed state merging! Bob has purification of  $E$ :  $\sum_x \sqrt{q_x} |\vartheta_x\rangle_{BE}$ .
- and it works approximately:

If  $\Lambda_z$  and  $\tilde{\Lambda}_x$  are measurements such that the discrimination error probability is low, then the output is nearly  $|\Phi\rangle_{AC}$ .

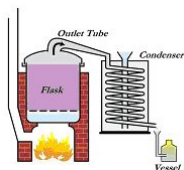
## Entanglement Distillation. . .



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. . .



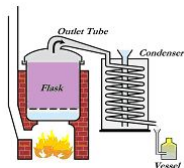
Given many copies of an arbitrary resource state,  $\Psi_{AB} = \psi_{AB}^{\otimes n}$ , convert into an (approximate) maximally entangled state using local operations and (one-way) classical communication (with high probability).

. . . by transmitting “missing” information

$X$	$I(X_A : B)$	$H(X_A B)$
-----	--------------	------------

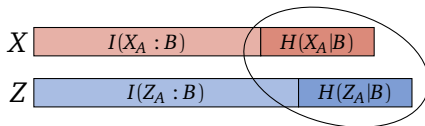
$Z$	$I(Z_A : B)$	$H(Z_A B)$
-----	--------------	------------

## 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).

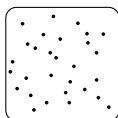
. . . by transmitting “missing” information



send this info to Bob.

## Appeal to the Holevo-Schumacher-Westmoreland theorem

- ☞ For  $X_A$  and  $Z_A$  individually, apply the “static” HSW theorem.  
(static = Alice chooses the code after the fact)
  - ☞ Take  $Z_A$ . Alice measures  $|z\rangle_A$ , sends Bob random (2-universal) hash of  $\mathbf{z}$ .
  - ☞ Bob uses PrettyGoodMmt to distinguish between remaining possible  $(\varphi_{\mathbf{z}})_B$ .
  - ⇒ Size of hash  $\approx nH(Z_A|B)$ .



Possible  $\mathbf{z}$ s

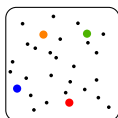


Support of  $(\varphi_{\mathbf{z}})_B$

- ☞ Same would work for  $X_A$ , with hash size  $\approx nH(X_A|B)$ .
- ⇒ Put them together in a CSS code!  
Linear hash value is the result of measuring an associated stabilizer operator.  
Can choose stabilizers to commute.

## Appeal to the Holevo-Schumacher-Westmoreland theorem

- ☞ For  $X_A$  and  $Z_A$  individually, apply the “static” HSW theorem.  
(static = Alice chooses the code after the fact)
  - ☞ Take  $Z_A$ . Alice measures  $|z\rangle_A$ , sends Bob random (2-universal) hash of  $\mathbf{z}$ .
  - ☞ Bob uses PrettyGoodMmt to distinguish between remaining possible  $(\varphi_{\mathbf{z}})_B$ .
  - ☞ Size of hash  $\approx nH(Z_A|B)$ .



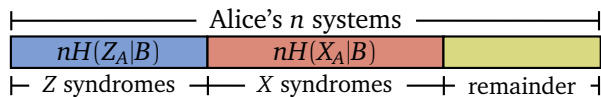
Possible  $\mathbf{z}$ s



Support of  $(\varphi_{\mathbf{z}})_B$

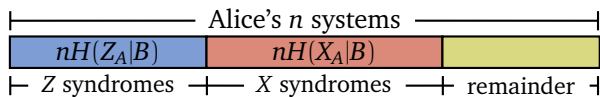
- ☞ Same would work for  $X_A$ , with hash size  $\approx nH(X_A|B)$ .
- ☞ Put them together in a CSS code!  
Linear hash value is the result of measuring an associated stabilizer operator.  
Can choose stabilizers to commute.

At what rates?



$$\Rightarrow \text{Naïve rate } E_n(\psi) = 1 - H(Z_A|B) - H(X_A|B)$$

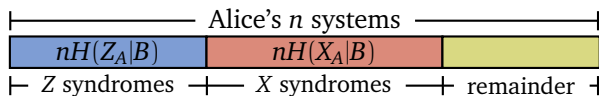
## At what rates?



$$\Rightarrow \text{Naïve rate } E_n(\psi) = 1 - H(Z_A|B) - H(X_A|B)$$

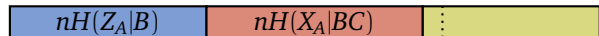
☞ Doesn't work.  $E_n(\psi)$  is too small.

## At what rates?



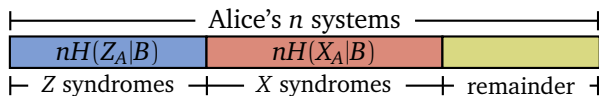
$$\Rightarrow \text{Naïve rate } E_n(\psi) = 1 - H(Z_A|B) - H(X_A|B)$$

- Doesn't work.  $E_n(\psi)$  is too small.
- But it's a two-step process. After step one Bob has a  $Z_A$  basis copy of Alice's system in some register  $C$ .  $|\Psi_c\rangle_{ABCE} = \sum_{\mathbf{z}} \sqrt{p_{\mathbf{z}}} |\mathbf{z}, \mathbf{z}\rangle_{AC} |\varphi_{\mathbf{z}}\rangle_{BE}$



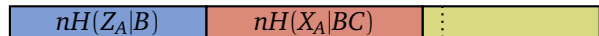
$$\Rightarrow \text{Refined rate } E_r(\psi) = 1 - H(Z_A|B) - H(X_A|BC)$$

## At what rates?



$$\Rightarrow \text{Naïve rate } E_n(\psi) = 1 - H(Z_A|B) - H(X_A|B)$$

- Doesn't work.  $E_n(\psi)$  is too small.
- But it's a two-step process. After step one Bob has a  $Z_A$  basis copy of Alice's system in some register  $C$ .  $|\Psi_c\rangle_{ABCE} = \sum_{\mathbf{z}} \sqrt{p_{\mathbf{z}}} |\mathbf{z}, \mathbf{z}\rangle_{AC} |\varphi_{\mathbf{z}}\rangle_{BE}$

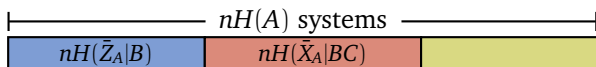


$$\Rightarrow \text{Refined rate } E_r(\psi) = 1 - H(Z_A|B) - H(X_A|BC)$$

- $\Rightarrow$  Voilà! Can show  $E_r(\psi) = -H(A|B)$ .

## 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
- ☞ However, protocol uses too much communication:  
 $C_r(\psi) = H(Z_A|B) + H(X_A|BC) = 1 + H(A|B) = 1 + H(E) - H(AE) > I(A : E)$ .
- ☞ The fix: first compress Alice's state and then run the protocol  
 $\psi_A$  eigenbasis defines  $Z_A, X_A \rightarrow \bar{Z}_A, \bar{X}_A \equiv F_A \bar{Z}_A F_A^\dagger$



- ☞ This would give known rates:

$$E_c(\psi) = H(A) - H(\bar{Z}_A|B) - H(\bar{X}_A|BC) = -H(A|B)$$

$$C_c(\psi) = H(\bar{Z}_A|B) - H(\bar{X}_A|BC) = H(A) + H(A|B) = I(A:E)$$

- ☞ But can we construct the necessary measurements?

- ☞ Bob can reuse HSW  $Z_A$  measurement for  $\bar{Z}_A$ :  
compression throws out nontypical  $\mathbf{z}$  and lowers the error probability.
- ☞ But what about the  $\bar{X}_A$  mmt?  $\bar{X}_A$  and  $X_A$  have no simple relation.
- ☞ System  $C$  comes to the rescue again. Examine  $|\Psi_c\rangle$ :

$$\begin{aligned} |\Psi_c\rangle_{ABCE} &= \sum_{\mathbf{z}} \sqrt{p_{\mathbf{z}}} |\mathbf{z}, \mathbf{z}\rangle_{AC} |\varphi_{\mathbf{z}}\rangle_{BE} = \frac{1}{\sqrt{d}} \sum_{\mathbf{x}, \mathbf{z}} \sqrt{p_{\mathbf{z}}} |\tilde{\mathbf{x}}\rangle_A \omega^{-\mathbf{x} \cdot \mathbf{z}} |\mathbf{z}\rangle_C |\varphi_{\mathbf{z}}\rangle_{BE} \\ &= \frac{1}{\sqrt{d}} \sum_{\mathbf{x}} |\tilde{\mathbf{x}}\rangle_A Z_C^{-\mathbf{x}} \left( \sum_{\mathbf{z}} \sqrt{p_{\mathbf{z}}} |\mathbf{z}\rangle_C |\varphi_{\mathbf{z}}\rangle_{BE} \right) = \frac{1}{\sqrt{d}} \sum_{\mathbf{x}} |\tilde{\mathbf{x}}\rangle_A Z_C^{-\mathbf{x}} |\vartheta\rangle_{CBE} \end{aligned}$$

- ☞  $|\vartheta_{\mathbf{x}}\rangle_{BCE} = Z_C^{-\mathbf{x}} |\vartheta\rangle_{CBE}$  group covariant, as are their compressed cousins.

Thus the HSW measurement is also group covariant, and can be easily adapted for the compressed case.

Can perform optimal state merging without decoupling,  
based entirely on complementarity.

- ☞ Also useful for secret key distillation
- ☞ Details: [PRA 78, 032335 \(2008\)](#) & [arXiv:0905.1324 \[quant-ph\]](#)
- ➡ How far does the complementarity approach take us? In particular, can we formulate one-shot versions of the asymptotic iid results we now have?
- ➡ Can we learn anything about channel superactivation from this approach? For instance, in the Smith/Yard example (entanglement-binding channel with private capacity + erasure channel) there's an interesting connection to data hiding. Is it just a curiosity or is there something more fundamental at work?

