Dissecting Quantum Information

Classical conditions for quantum error-correction

TECHNISCHE UNIVERSITÄT DARMSTADT

Joseph M. Renes

Dissecting Quantum Information

Classical conditions for quantum error-correction

TECHNISCHE UNIVERSITÄT DARMSTADT

Joseph M. Renes

Prolog:

How do we design quantum information processing protocols?

TECHNISCHE UNIVERSITÄT DARMSTADT

Answer: Begin with the end in mind (i.e. work backwards)

Prolog:

How do we design quantum information processing protocols?

TECHNISCHE UNIVERSITÄT DARMSTADT

Answer: Begin with the end in mind (i.e. work backwards)

Ok, what are we interested in making/doing?

quantum communication / entanglement or key distillation / state merging / etc.

use these to build other protocols

Prolog:

How do we design quantum information processing protocols?

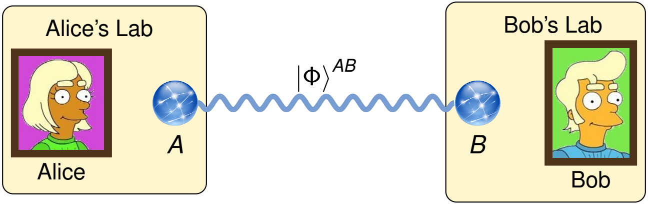
TECHNISCHE UNIVERSITÄT DARMSTADT

Answer: Begin with the end in mind (i.e. work backwards)

Ok, what are we interested in making/doing?

quantum communication / entanglement or key distillation / state merging / etc.

use these to build other protocols



Take entanglement distillation. When can Bob recover entanglement from B?

two criteria: decoupling & crypto-based

Prolog:

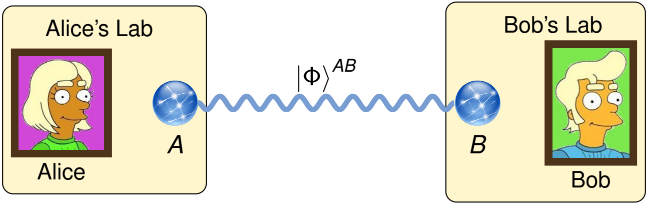
How do we design quantum information processing protocols?

Answer: Begin with the end in mind (i.e. work backwards)

Ok, what are we interested in making/doing?

quantum communication / entanglement or key distillation / state merging / etc.

use these to build other protocols



Take entanglement distillation. When can Bob recover entanglement from B?

two criteria: decoupling & crypto-based

Here I add **2 new approximate quantum error correction conditions** to this list

Outline

1. Existing approaches
2. Introduce new approaches
3. Some Details...
4. Applications & Open Questions

Part I

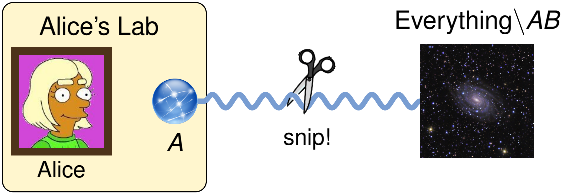
TECHNISCHE UNIVERSITÄT DARMSTADT

Existing Approaches

Current Approaches:

1. Decoupling

2. Crypto-based



Single quantum assumption: Bob can locally recover entanglement when A is mixed & decoupled from E. More technically:

if $\psi^{AE} \approx \tau^{A} \otimes \psi^{E}$ for $\tau^{A} = \mathbb{1}^{A}/\dim(A)$,

then there exists a $U^{B\to BCD}$ such that $U^{B\to BCD}\,|\psi\rangle^{ABE} \approx |\Phi\rangle^{AD}\,|\psi\rangle^{CBE}$

Great! Now we can start to design a protocol.

For any input state we just need to find a subspace of A which is decoupled and mixed.

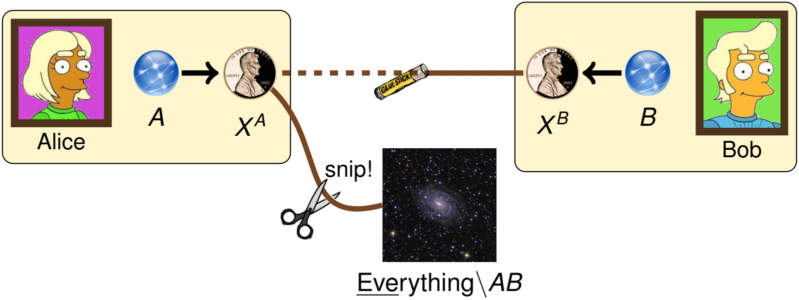
Just pick a (sufficiently small) random subspace, it'll work with high probability...

Current Approaches:

1. Decoupling

2. Crypto-based

TECHNISCHE UNIVERSITÄT DARMSTADT



Two c-q assumptions: $U^{B \to BCD}$ exists when Bob knows X^A and Eve does not.

$$p_{\text{guess}}(X^A|B) \approx 1 \text{ and } p_{\text{guess}}(X^A|E) \approx 0 \text{ implies } U^{B\to BCD} |\psi\rangle^{ABE} \approx |\Phi\rangle^{AD} |\psi\rangle^{CBD}$$

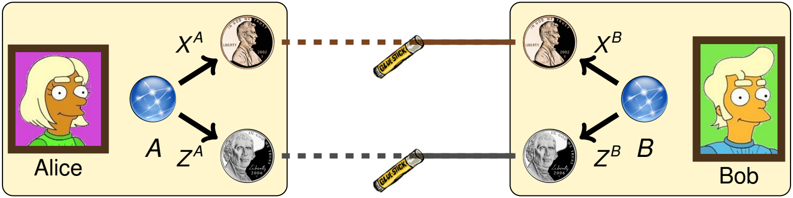
Part II

New Approaches

Two New Approaches

1. Complementary Classical Correlations for Bob

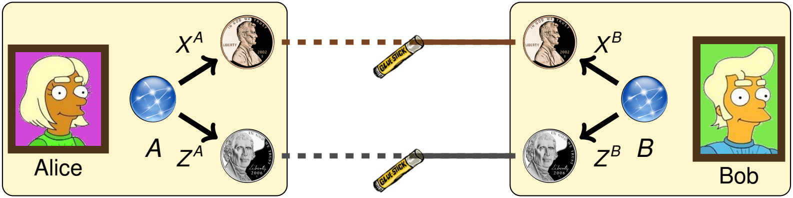
2. Complementary Classical Uncorrelations for Eve



Two New Approaches

1. Complementary Classical Correlations for Bob

2. Complementary Classical Uncorrelations for Eve



For an arbitrary ψ^{AB}, if

1. $p_{\text{guess}}(Z^A|B) \approx 1$ and
2. $p_{\text{guess}}(X^A|BC) \approx 1$,

then there exists a $U^{B\to BCD}$ with

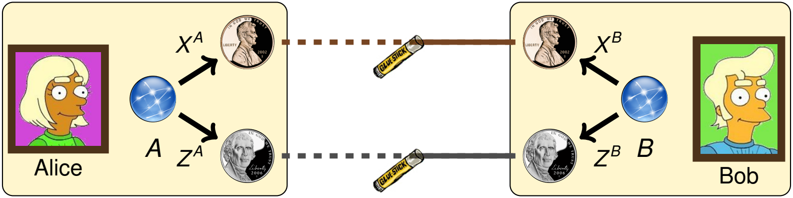
$$U^{B\to BCD}\,|\psi\rangle^{ABE} \approx |\Phi\rangle^{AD}\,|\psi\rangle^{CBE}$$

(C: copy of Z^A // X, Z: Weyl-Heisenberg ops)

Two New Approaches

1. Complementary Classical Correlations for Bob

2. Complementary Classical Uncorrelations for Eve

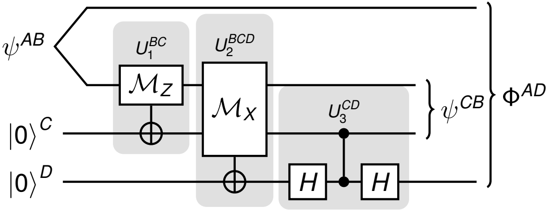


For an arbitrary ψ^{AB}, if

1. $p_{\text{guess}}(Z^A|B) \approx 1$ and
2. $p_{\text{guess}}(X^A|BC) \approx 1$,

then there exists a $U^{B\rightarrow BCD}$ with

$$U^{B\rightarrow BCD}\,|\psi\rangle^{ABE} \approx |\Phi\rangle^{AD}\,|\psi\rangle^{CBE}$$

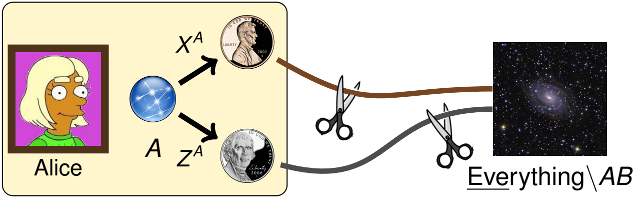


(C: copy of Z^A // X, Z: Weyl-Heisenberg ops)

Two New Approaches

1. Complementary Classical Correlations for Bob

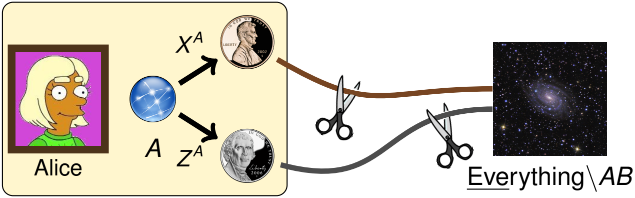
2. Complementary Classical Uncorrelations for Eve



Two New Approaches

1. Complementary Classical Correlations for Bob

2. Complementary Classical Uncorrelations for Eve



For an arbitrary ψ^{AB}, if

1. $p_{\text{guess}}(X^A|CE) \approx 0$ and
2. $p_{\text{guess}}(Z^A|E) \approx 0$,

then there exists a $U^{B\to BCD}$ with

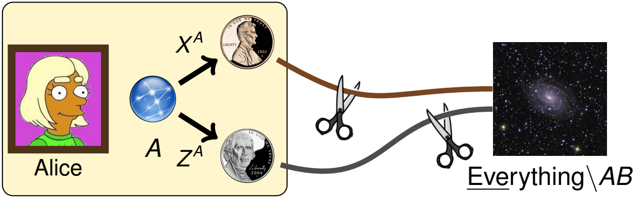
$$U^{B\to BCD}\,|\psi\rangle^{ABE} \approx |\Phi\rangle^{AD}\,|\psi\rangle^{CBE}$$

(C is a copy of Z^A)

Two New Approaches

1. Complementary Classical Correlations for Bob

2. Complementary Classical Uncorrelations for Eve



For an arbitrary ψ^{AB}, if

1. $p_{\text{guess}}(X^A|CE) \approx 0$ and
2. $p_{\text{guess}}(Z^A|E) \approx 0$,

then there exists a $U^{B\to BCD}$ with

$$U^{B\to BCD}\,|\psi\rangle^{ABE} \approx |\Phi\rangle^{AD}\,|\psi\rangle^{CBE}$$

(C is a copy of Z^A)

Duality: $p_{\text{guess}}(Z^A|B) \approx 1 \Leftrightarrow p_{\text{guess}}(X^A|CE) \approx 0$

Part III

Details: Bob's Decoder & Eve's Duality

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

♠ implies there exists a $U_1^{B\to BC}$ taking $|\psi\rangle^{ABE}$ to $|\psi_Z\rangle^{ABCE}$

Why? Because Bob can measure B coherently to recover z, storing the result in C.

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

♠ implies there exists a $U_1^{B\to BC}$ taking $|\psi\rangle^{ABE}$ to $|\psi_Z\rangle^{ABCE}$

Why? Because Bob can measure B coherently to recover z, storing the result in C.

♢ We can write $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Insert $|z\rangle = \frac{1}{\sqrt{d}} \sum_x \omega^{-xz}\,|\widetilde{x}\rangle$ in $|\psi_Z\rangle$ and use $\omega^{-xz}\,|z\rangle = Z^{-x}\,|z\rangle$

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

♠ implies there exists a $U_1^{B\to BC}$ taking $|\psi\rangle^{ABE}$ to $|\psi_Z\rangle^{ABCE}$

Why? Because Bob can measure B coherently to recover z, storing the result in C.

♢ We can write $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Insert $|z\rangle = \frac{1}{\sqrt{d}} \sum_x \omega^{-xz}\,|\widetilde{x}\rangle$ in $|\psi_Z\rangle$ and use $\omega^{-xz}\,|z\rangle = Z^{-x}\,|z\rangle$

♣ implies $\exists\ U_2^{BC\to BCD}$ taking $|\psi_Z\rangle^{ABCE}$ to $|\psi_{ZX}\rangle = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A\,|-\widetilde{x}\rangle^D \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Coherent mmt, same as before.

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A |\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A |z\rangle^C |\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

♠ implies there exists a $U_1^{B\to BC}$ taking $|\psi\rangle^{ABE}$ to $|\psi_Z\rangle^{ABCE}$

Why? Because Bob can measure B coherently to recover z, storing the result in C.

♢ We can write $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Insert $|z\rangle = \frac{1}{\sqrt{d}} \sum_x \omega^{-xz} |\widetilde{x}\rangle$ in $|\psi_Z\rangle$ and use $\omega^{-xz}|z\rangle = Z^{-x}|z\rangle$

♣ implies $\exists\ U_2^{BC\to BCD}$ taking $|\psi_Z\rangle^{ABCE}$ to $|\psi_{ZX}\rangle = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A |-\widetilde{x}\rangle^D \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Coherent mmt, same as before.

♡ using a control phase from D to C (U_3^{CD}), we get $|\Phi\rangle^{AD} |\psi\rangle^{CBE}$

It just so happens that $|\Phi\rangle^{AD} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A |-\widetilde{x}\rangle^D$.

A look at the details (Bob)

Building a decoder from Bob's measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A |\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A |z\rangle^C |\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|B) = 1$ and ♣ $p_{\text{guess}}(X^A|BC) = 1$

♠ implies there exists a $U_1^{B\to BC}$ taking $|\psi\rangle^{ABE}$ to $|\psi_Z\rangle^{ABCE}$

Why? Because Bob can measure B coherently to recover z, storing the result in C.

♢ We can write $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Insert $|z\rangle = \frac{1}{\sqrt{d}} \sum_x \omega^{-xz} |\widetilde{x}\rangle$ in $|\psi_Z\rangle$ and use $\omega^{-xz}|z\rangle = Z^{-x}|z\rangle$

♣ implies $\exists\ U_2^{BC\to BCD}$ taking $|\psi_Z\rangle^{ABCE}$ to $|\psi_{ZX}\rangle = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A |-\widetilde{x}\rangle^D \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

Coherent mmt, same as before.

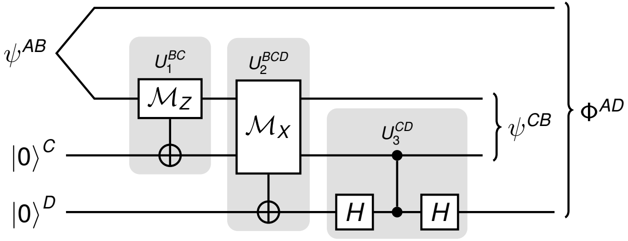
♡ using a control phase from D to C (U_3^{CD}), we get $|\Phi\rangle^{AD} |\psi\rangle^{CBE}$

It just so happens that $|\Phi\rangle^{AD} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A |-\widetilde{x}\rangle^D$.

Bob's decoder is $U^{B\to BCD} = U_3^{CD} U_2^{BC\to BCD} U_1^{B\to BC}$. Also works approximately!!!!

Circuit for Bob's Decoder

TECHNISCHE
UNIVERSITÄT
DARMSTADT



- Easy to prove that decoder also exists when $p_{\text{guess}}(X|B) \approx 1$.
- C takes care of correlations between X and Z; removes need to digitize errors
- C is also important for constructing optimal secret key & entanglement distillation protocols.
- Decoder of resulting protocol explicitly constructed

Details of Decoupling Eve

Duality of $p_{\text{guess}}(X^A|EC) \approx 0$ and $p_{\text{guess}}(Z^A|B) \approx 1$

TECHNISCHE UNIVERSITÄT DARMSTADT

Fairly easy to see that $p_{\text{guess}}(Z^A|B) \approx 1 \Rightarrow p_{\text{guess}}(X^A|E) \approx 0$.

Bob's copy of Z^A dephases A in the Z basis; X^A is then random.

Converse is not true; consider state $|\psi\rangle^{ABE} = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}\,|1\rangle\right)^A |\varphi\rangle^{BE}$.

Both Bob and Eve ignorant: $p_{\text{guess}}(Z^A|B) = p_{\text{guess}}(X^A|E) = 0$.

Details of Decoupling Eve

Duality of $p_{\text{guess}}(X^A|EC) \approx 0$ and $p_{\text{guess}}(Z^A|B) \approx 1$

TECHNISCHE UNIVERSITÄT DARMSTADT

Fairly easy to see that $p_{\text{guess}}(Z^A|B) \approx 1 \Rightarrow p_{\text{guess}}(X^A|E) \approx 0$.

Bob's copy of Z^A dephases A in the Z basis; X^A is then random.

Converse is not true; consider state $|\psi\rangle^{ABE} = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}\,|1\rangle\right)^A |\varphi\rangle^{BE}$.

Both Bob and Eve ignorant: $p_{\text{guess}}(Z^A|B) = p_{\text{guess}}(X^A|E) = 0$.

Two ways out: $p_{\text{guess}}(X^A|E) \approx 0 \Rightarrow p_{\text{guess}}(Z^A|B) \approx 1$ if either

1. Bob has a copy of X^A or
2. Eve has a copy of Z^A.

Case 1 leads back to the crypto scenario of entanglement distillation:
it says that Bob can recover entanglement when $p_{\text{guess}}(X^A|B) \approx 1$ and $p_{\text{guess}}(X^A|E) \approx 0$.

Case 2 corresponds to the case of a cq state for Alice and Bob:
Alice holds the classical variable Z^A due to dephasing from Eve.

More Duality (Eve)

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|E) = 1$ and ♣ $p_{\text{guess}}(X^A|E) = 0$

More Duality (Eve)

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\, |z\rangle^A\, |\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\, |z\rangle^A\, |z\rangle^C\, |\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|E) = 1$ and ♣ $p_{\text{guess}}(X^A|E) = 0$

♠ means we might as well start with $|\psi_Z\rangle^{ABCE}$, where Eve holds CE.

remember that $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A\, |\vartheta_x\rangle^{BCE}$

More Duality (Eve)

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\, |z\rangle^A |\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\, |z\rangle^A |z\rangle^C |\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|E) = 1$ and ♣ $p_{\text{guess}}(X^A|E) = 0$

♠ means we might as well start with $|\psi_Z\rangle^{ABCE}$, where Eve holds CE.
remember that $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A |\vartheta_x\rangle^{BCE}$

♣ means Eve's conditional marginals ϑ_x^{CE} are identical.
$\vartheta_x^{CE} = \vartheta_{x'}^{CE} \Rightarrow \vartheta_x^{CE} = \psi_Z^{CE}$ (just add the ϑ_x^{CE} together). In particular, $\vartheta_0^{CE} = \psi_Z^{CE}$, or $\psi^{CE} = \psi_Z^{CE}$

More Duality (Eve)

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\, |z\rangle^A\, |\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\, |z\rangle^A\, |z\rangle^C\, |\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|E) = 1$ and ♣ $p_{\text{guess}}(X^A|E) = 0$

♠ means we might as well start with $|\psi_Z\rangle^{ABCE}$, where Eve holds CE.

remember that $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE} = \frac{1}{\sqrt{d}} \sum_x |\widetilde{x}\rangle^A\, |\vartheta_x\rangle^{BCE}$

♣ means Eve's conditional marginals ϑ_x^{CE} are identical.

$\vartheta_x^{CE} = \vartheta_{x'}^{CE} \Rightarrow \vartheta_x^{CE} = \psi_Z^{CE}$ (just add the ϑ_x^{CE} together). In particular, $\vartheta_0^{CE} = \psi_Z^{CE}$, or $\psi^{CE} = \psi_Z^{CE}$

♢ Uhlmann's theorem: $\exists\ U^{B\to MB}$ such that $U^{B\to MB}\, |\psi\rangle^{CBE} = |\psi_Z\rangle^{MBCE}$

MB belong to Bob, *CE* to Eve.

More Duality (Eve)

TECHNISCHE UNIVERSITÄT DARMSTADT

Start with $|\psi\rangle^{ABE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}$ and $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE}$

Assumptions: ♠ $p_{\text{guess}}(Z^A|E) = 1$ and ♣ $p_{\text{guess}}(X^A|E) = 0$

♠ means we might as well start with $|\psi_Z\rangle^{ABCE}$, where Eve holds CE.
remember that $|\psi_Z\rangle^{ABCE} = \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE} = \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BCE}$

♣ means Eve's conditional marginals ϑ_x^{CE} are identical.
$\vartheta_x^{CE} = \vartheta_{x'}^{CE} \Rightarrow \vartheta_x^{CE} = \psi_Z^{CE}$ (just add the ϑ_x^{CE} together). In particular, $\vartheta_0^{CE} = \psi_Z^{CE}$, or $\psi^{CE} = \psi_Z^{CE}$

♢ Uhlmann's theorem: $\exists\ U^{B\to MB}$ such that $U^{B\to MB}\,|\psi\rangle^{CBE} = |\psi_Z\rangle^{MBCE}$
MB belong to Bob, CE to Eve.

♡ Now apply $U^{B\to MB}$ to $|\psi_Z\rangle^{ABCE}$ and see what we get

Duality Cont'd

reminder: $|\psi_Z\rangle^{ABCE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^C\,|\varphi_z\rangle^{BE} = \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi\rangle^{CBE}$

TECHNISCHE UNIVERSITÄT DARMSTADT

$$
\begin{aligned}
U^{B\to MB}\,|\psi\rangle^{ABE} &= U^{B\to MB}\,|\psi_Z\rangle^{ABCE} \quad (\spadesuit) && (1)\\
&= \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C U^{B\to MB}\,|\psi\rangle^{BCE} && (2)\\
&= \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C |\psi_Z\rangle^{MBCE} \quad (\clubsuit) && (3)\\
&= \frac{1}{\sqrt{d}}\sum_x |\widetilde{x}\rangle^A \left(Z^{-x}\right)^C \sum_z \sqrt{p_z}\,|z\rangle^M\,|z\rangle^C\,|\varphi_z\rangle^{BE} && (4)\\
&= \frac{1}{\sqrt{d}}\sum_{x,z} \sqrt{p_z}\,\omega^{-xz}\,|\widetilde{x}\rangle^A\,|z\rangle^M\,|z\rangle^C\,|\varphi_z\rangle^{BE} && (5)\\
&= \sum_z \sqrt{p_z}\,|z\rangle^A\,|z\rangle^M\,|z\rangle^C\,|\varphi_z\rangle^{BE} && (6)
\end{aligned}
$$

Thus, Bob can apply $U^{B\to MB}$ and then measure M to recover Z^A. Works approximately!!!!

Applications & Open Questions

TECHNISCHE UNIVERSITÄT DARMSTADT

- Intuitive way to think about quantum information (processing)
  results in arXiv:1003.0703 & arXiv:1003.1150
- Construct optimal protocols with new approximate error-correction conditions.
  Secret-key / Entanglement distillation in PRA 78, 032335 (2008), *state merging* in LNCS 5906, 76 (2009), *mother of all protocols* coming soon.
- Proof of the quantum noisy channel coding theorem (with classical assistance).
- Quantum decoder explicitly constructed from classical decoders. Helpful in finding new quantum codes?
- Simple proof of HSW theorem (sending classical info over quantum channels), if we can convert these static results to the dynamic setting.
- Universal communication schemes? Quantum from 2x classical?
- One-shot versions?
- Weak string erasure... (quantum capacity !?!)