The Fidelity Alternative and Quantum Measurement Simulation

Patrick Hayden (McGill)
Andreas Winter (Bristol, Singapore)

arXiv: out.soon (2009) ...

Outline

1. What does it mean to transmit a state?

2. Simulation of binary measurements

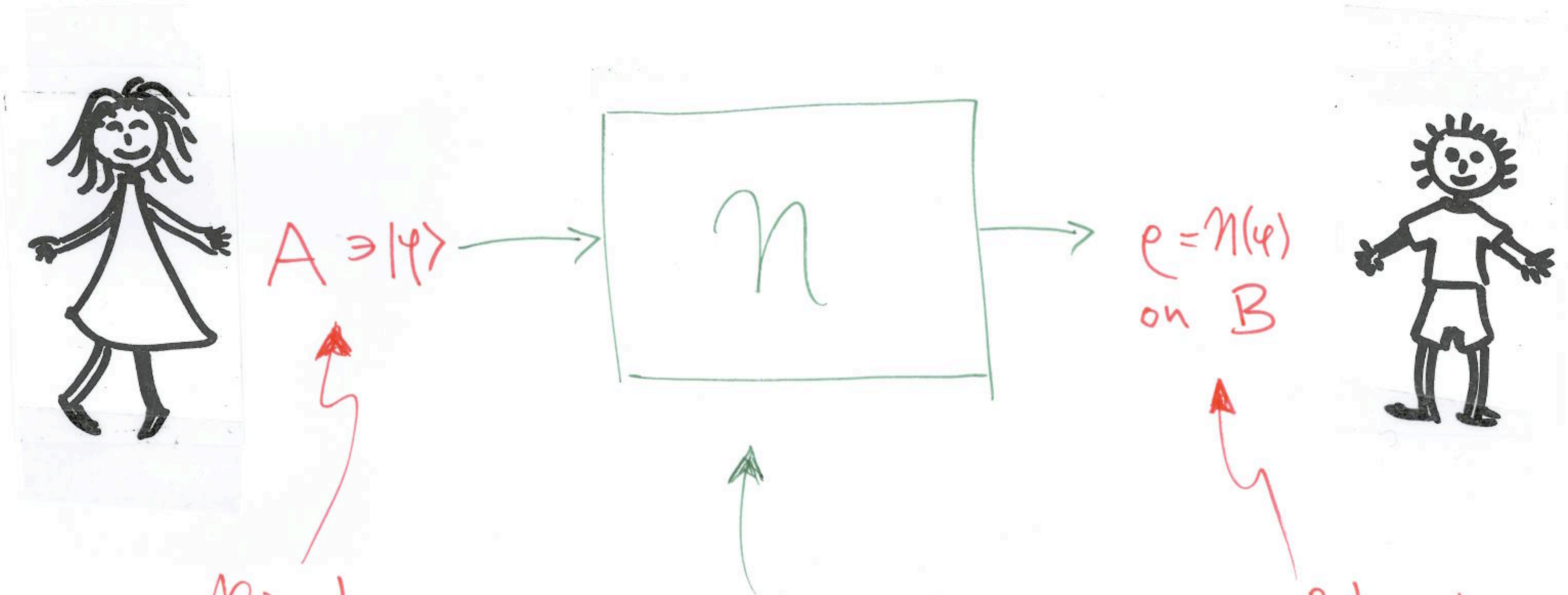
3. Identification (c. + qu.)

4. Quantum-ID ... Fidelity... Forgetfulness

5. Capacity results

6. Outlook

1. What does it mean to transmit a state?



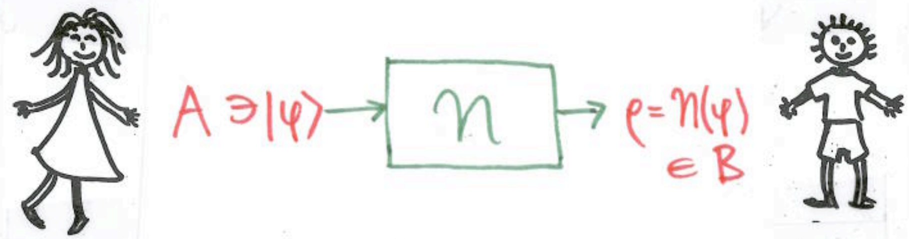
Alice has some quantum state $\varphi = |\varphi\rangle\langle\varphi|$ (only consider pure)

superoperator (completely positive & trace preserving — cptp — map) a.k.a. channel

Bob gets an output state ρ (generally mixed)

*$A, B, \ldots$ have finite dimension $|A|, |B|, \ldots$ throughout

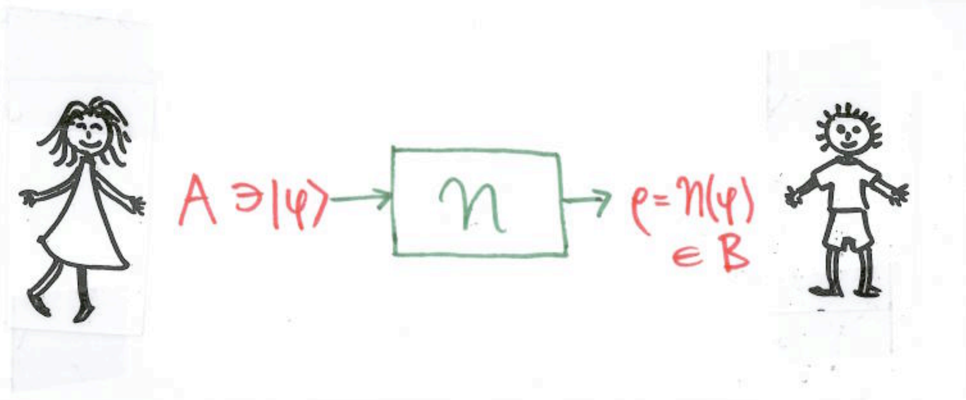
For faithful transmission of Alice's state φ we need:



(1) $B = A$ [to be able to compare ρ to φ]

(2) $\rho = \mathcal{N}(\varphi) = \varphi$ for all $|\varphi\rangle \in A$

For <u>faithful</u> transmission of Alice's state φ we need:

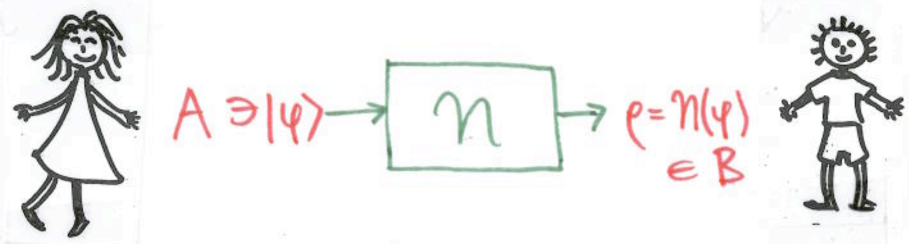


(1) $B = A$ [to be able to compare ρ to φ]

(2) $\rho = \mathcal{N}(\varphi) = \varphi$ for all $|\varphi\rangle \in A$

... but that's perhaps asking too much: only leaves $\mathcal{N} = \mathrm{id}$; and what about small loss of coherence in practice?

For *faithful* transmission of Alice's state φ we need:



(1) $B = A$ [to be able to compare ρ to φ]

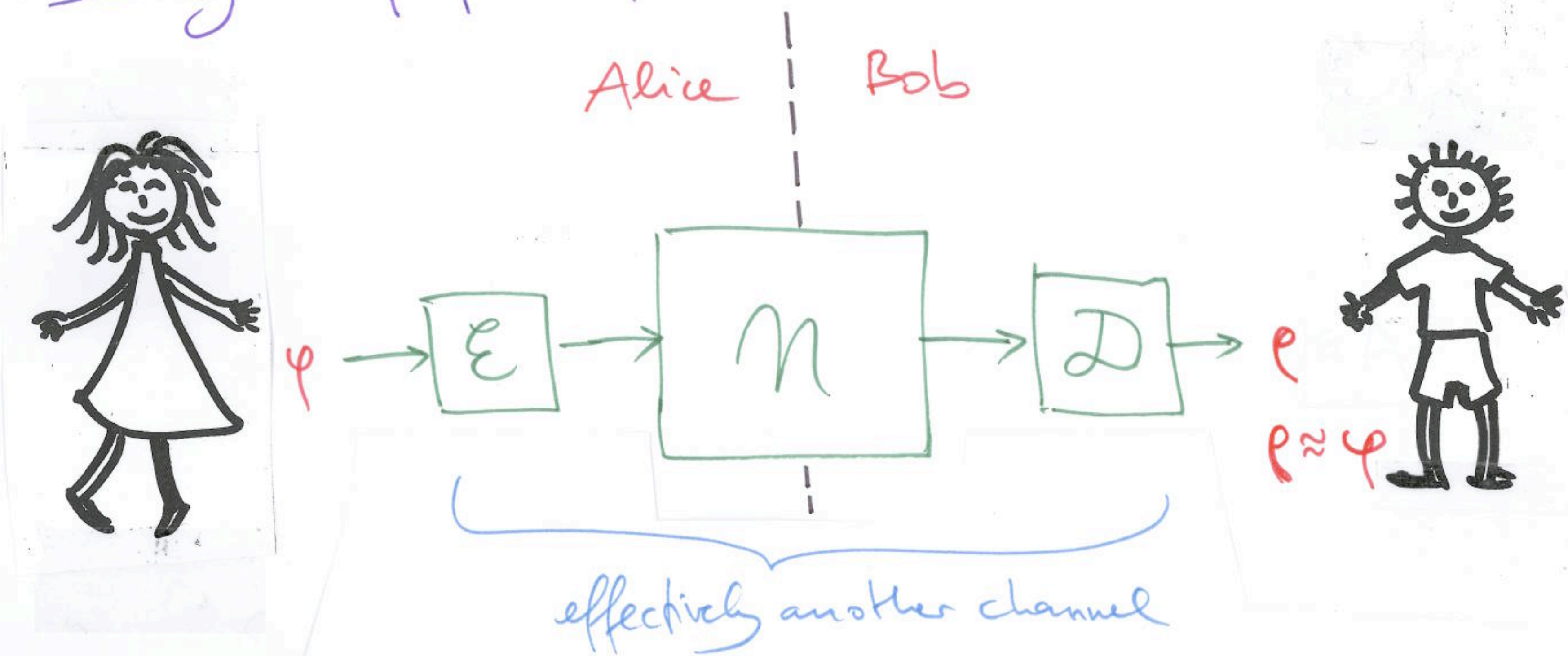
(2) $\rho = \mathcal{N}(\varphi) \approx \varphi$ for all $|\varphi\rangle \in A$

Approximation measured by *fidelity* $F(\varphi, \rho) = \langle\varphi|\rho|\varphi\rangle = \mathrm{Tr}\, \rho\varphi$

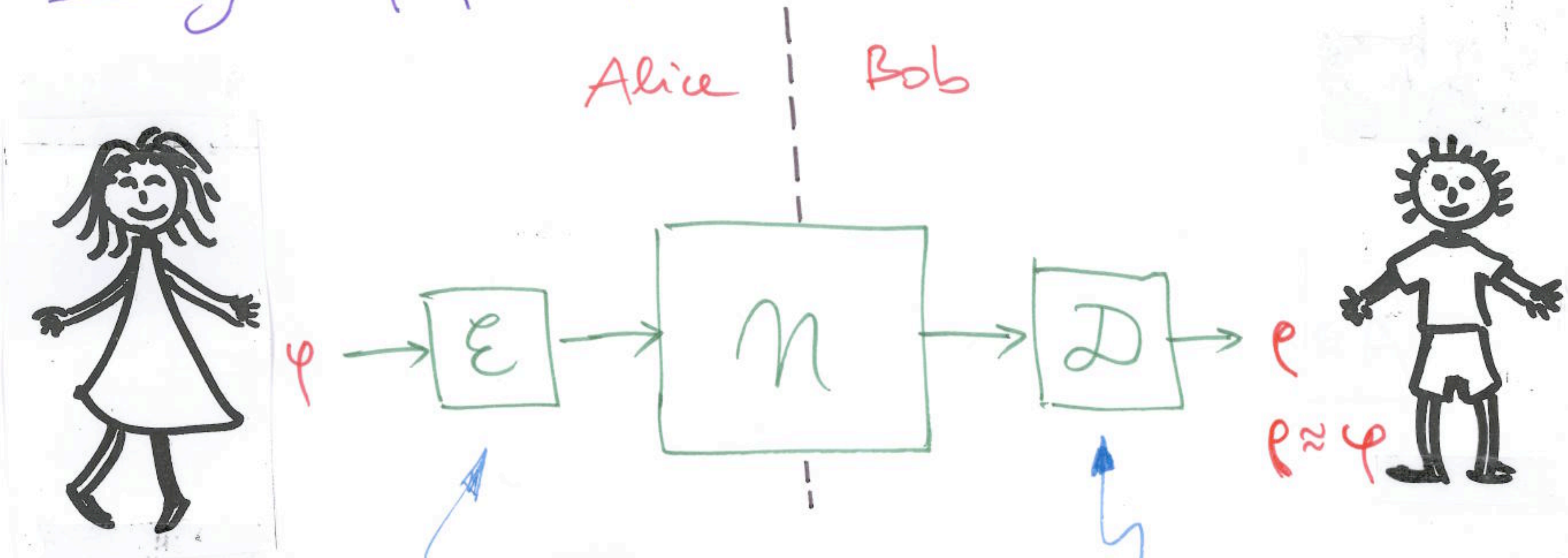
[... extends to *mixed state fidelity*
$F(\rho, \sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)^2 = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$]

Condition: $F(\varphi, \rho) \geq 1 - \epsilon$ for all $|\varphi\rangle \in A$

Relaxed condition: there exist encoding and decoding cptp maps $\mathcal{E}$ and $\mathcal{D}$ s.t.



Relaxed condition: there exist encoding and decoding cptp maps $\mathcal{E}$ and $\mathcal{D}$ s.t.

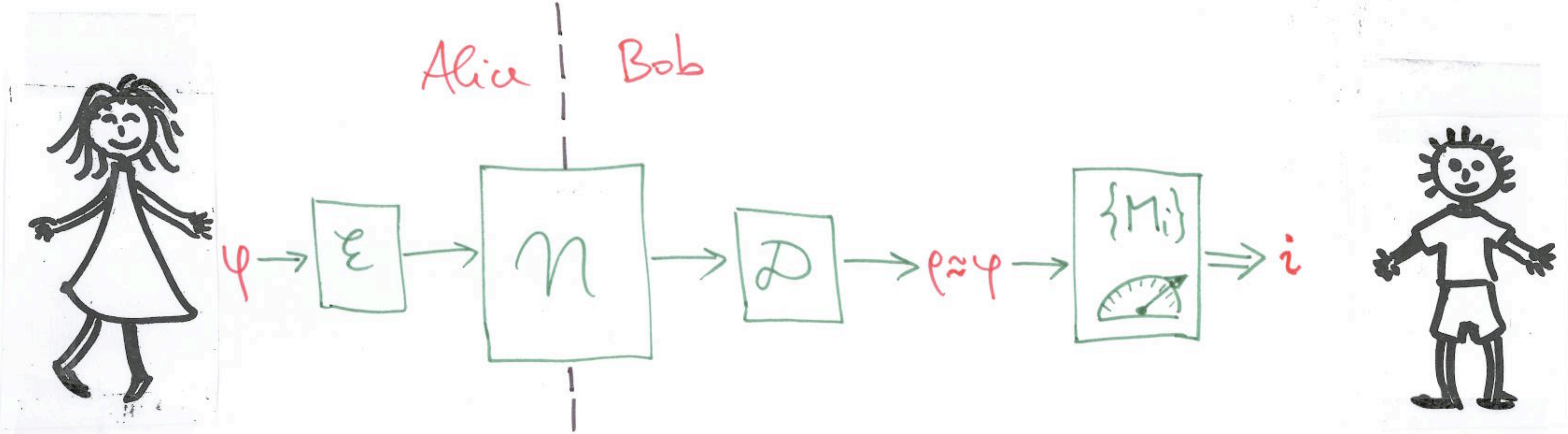


Purpose: to prepare the state for $\mathcal{N}$

This is basically an error correction step.

Also: Allows $B \neq A$

...if this is the case, Bob can perform any measurement (POVM) $\{M_i\}$ [i.e. $M_i \geq 0$, $\sum_i M_i = \mathbb{1}$] on φ:

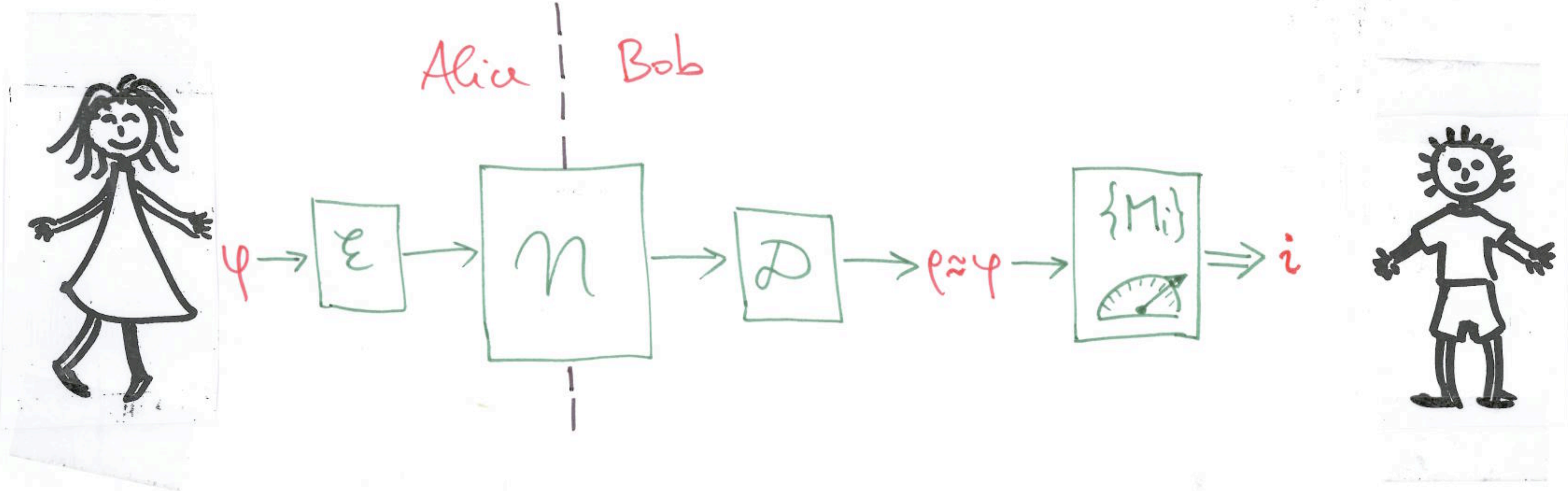


I.e.,

$$\Pr\{M_i|\varphi\} = \mathrm{Tr}\,\varphi M_i \approx \mathrm{Tr}\,\rho M_i$$

ℓ^1-distance $\leq \delta = 2\sqrt{\epsilon}$

... if this is the case, Bob can perform any measurement (POVM) $\{M_i\}$ [i.e. $M_i \geq 0$, $\sum_i M_i = \mathbb{1}$] on φ:



I.e.,

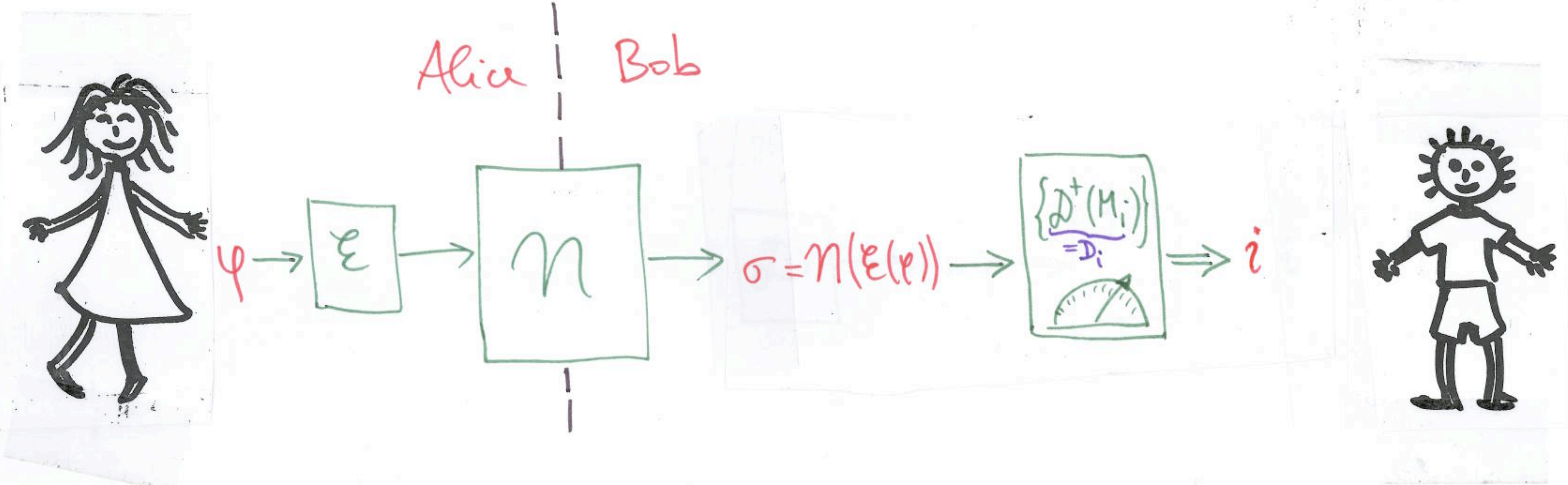
$$\Pr\{M_i|\varphi\} = \mathrm{Tr}\,\varphi M_i \approx \mathrm{Tr}\,\rho M_i = \mathrm{Tr}\left[\mathcal{D}(\mathcal{N}(\mathcal{E}(\varphi)))\cdot M_i\right]$$

ℓ^1-distance $\leq \delta = 2\sqrt{\epsilon}$

(Heisenberg picture: action on observables)

$$= \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi))\cdot \mathcal{D}^{\dagger}(M_i)\right] = \Pr\{D_i|\sigma\}$$

... if this is the case, Bob can perform any measurement (POVM) $\{M_i\}$ [i.e. $M_i \geq 0$, $\sum_i M_i = \mathbb{1}$] on φ:



I.e.,

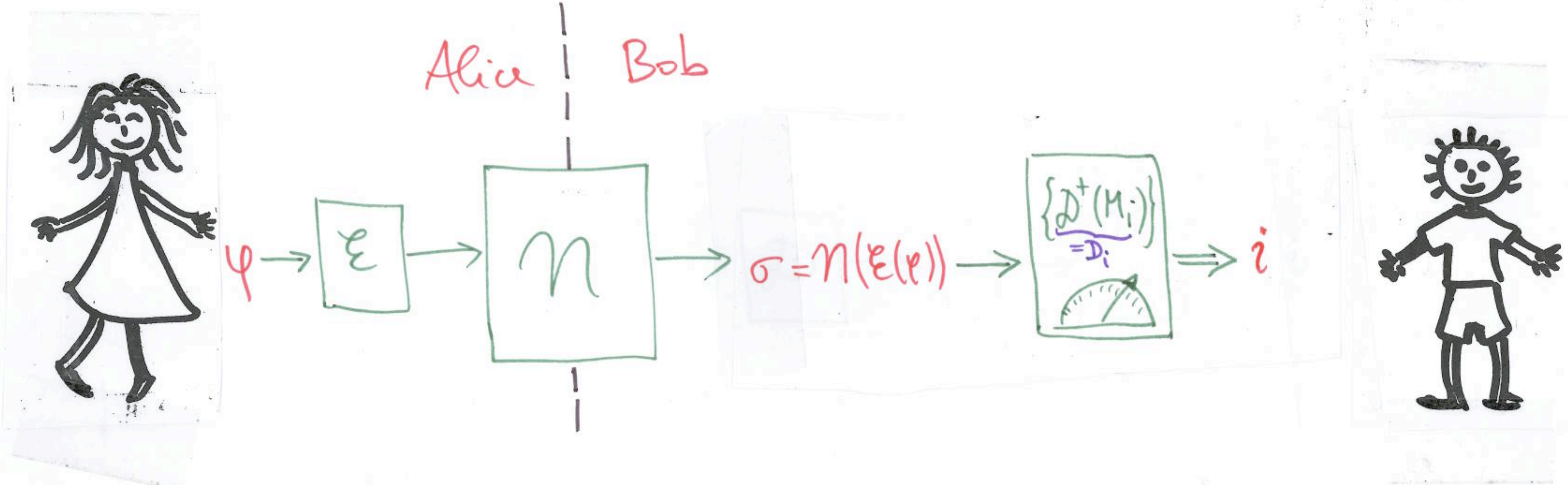
$$\Pr\{M_i|\varphi\} = \mathrm{Tr}\,\varphi M_i \approx \mathrm{Tr}\,\rho M_i = \mathrm{Tr}\left[\mathcal{D}(\mathcal{N}(\mathcal{E}(\varphi)))\cdot M_i\right]$$

ℓ^1-distance $\leq \delta = 2\sqrt{\epsilon}$

(Heisenberg picture: action on observables)

$$= \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi))\cdot \mathcal{D}^\dagger(M_i)\right] = \Pr\{D_i|\sigma\}$$

... if this is the case, Bob can perform any measurement (POVM) $\{M_i\}$ [i.e. $M_i \geq 0$, $\sum_i M_i = \mathbb{1}$] on φ:



I.e.,

$$\Pr\{M_i|\varphi\} = \mathrm{Tr}\,\varphi M_i \approx \mathrm{Tr}\,\rho M_i = \mathrm{Tr}\left[\mathcal{D}(\mathcal{N}(\mathcal{E}(\varphi)))\cdot M_i\right]$$

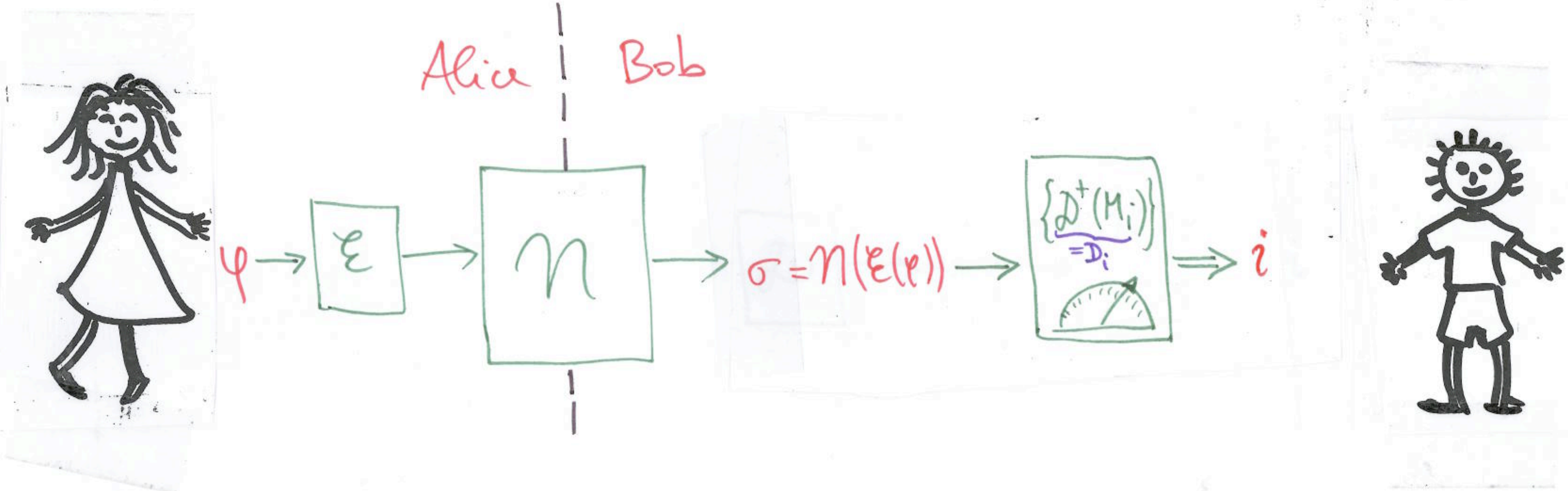
ℓ^1- distance $\leq \delta = 2\sqrt{\varepsilon}$

(Heisenberg picture: action on observables)

$$= \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi))\cdot \mathcal{D}^\dagger(M_i)\right] = \Pr\{D_i|\sigma\}$$

In other words: By measuring $\{D_i\}$ on σ, Bob can <u>simulate</u> the measurement of $\{M_i\}$ on φ.

... if this is the case, Bob can perform any measurement (POVM) $\{M_i\}$ [i.e. $M_i \geq 0$, $\sum_i M_i = \mathbb{1}$] on φ:

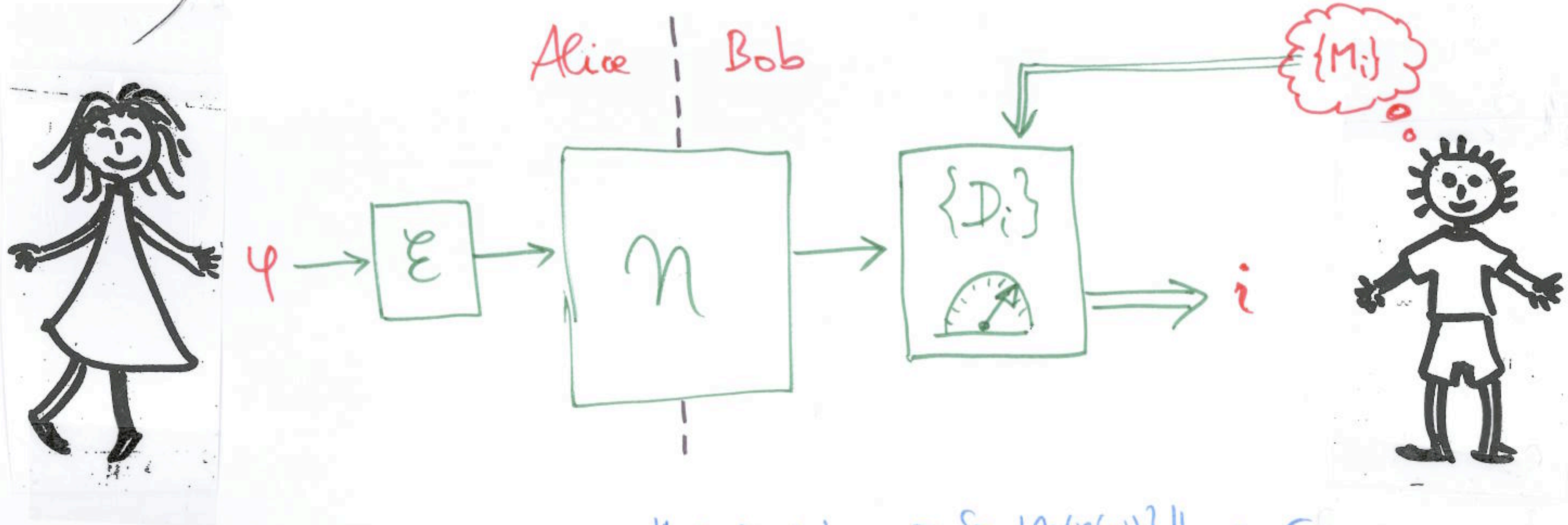


Conversely: If $|\varphi\rangle \in$ d-dim. system, and Bob can accurately simulate the discrete Weyl operators X_d & Z_d, then he can also build a decoder $\mathcal{D}$ s.t.

$\varphi \approx \mathcal{D}(\mathcal{N}(\mathcal{E}(\varphi)))$ [see Hayden/Shor/W., OSID 15(1), 2008
building on Christandl/W., IEEE-IT 51(9), 2005]

2. Simulation of (binary) measurements

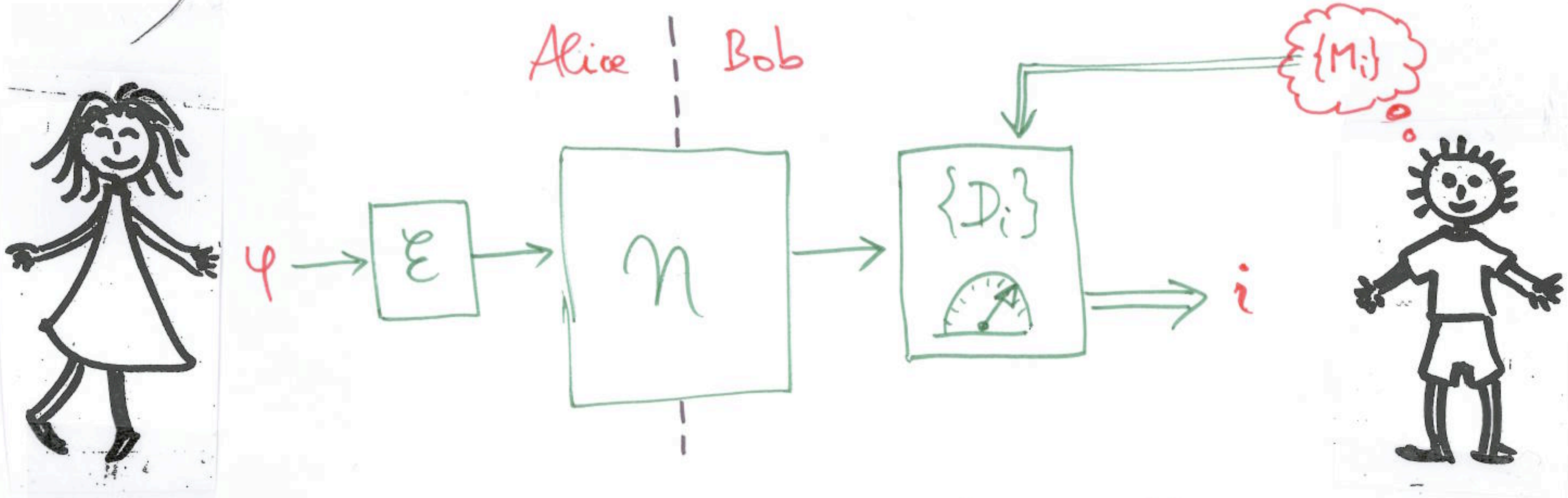
Since we can characterize transmission of φ by Bob's ability to simulate measurements on it:



s.t. for all $|\varphi\rangle$, $\quad \| \Pr\{M_i|\varphi\} - \Pr\{D_i|\mathcal{N}(\mathcal{E}(\varphi))\}\|_1 \leq \epsilon, \ldots$

2. Simulation of (binary) measurements

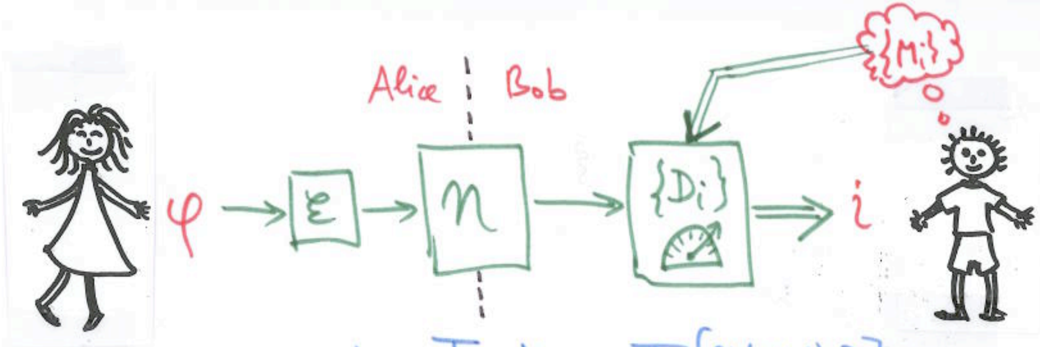
Since we can characterize transmission of φ by Bob's ability to simulate measurements on it:



s.t. for all $|\varphi\rangle$, $\quad \left\| \Pr\{M_i | \varphi\} - \Pr\{D_i | \mathcal{N}(\mathcal{E}(\varphi))\} \right\|_1 \leq \epsilon, \ldots$

... we are motivated to modify the game via restrictions on the POVMs we wish to be able to simulate.

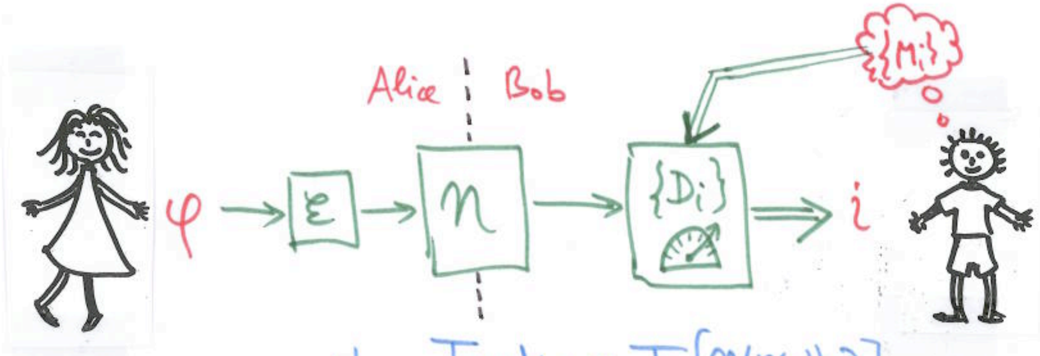
Here is what we get for various classes of POVMs $\{M_i\}$:



s.t. $\operatorname{Tr} \varphi M_i \approx \operatorname{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi)) \cdot D_i\right]$

$\{M_i\}$	Information task
single von Neumann measurement, say Z	classical communication (eigenbasis of Z)

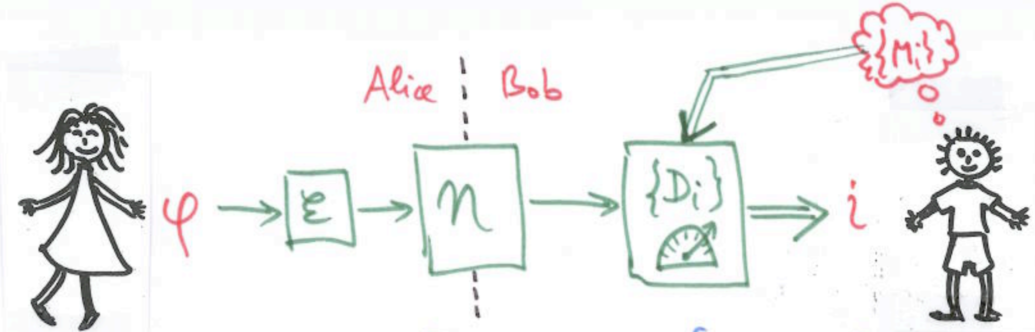
Here is what we get for various classes of POVMs $\{M_i\}$:



s.t. $\mathrm{Tr}\, \varphi M_i \approx \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi)) \cdot D_i\right]$

$\{M_i\}$	Information task
single von Neumann measurement, say Z	classical communication (eigenbasis of Z)
all POVMs	quantum communication (since we can build a decoder $\mathcal{D}$ for the state φ)
Z and X	—— " ——
all binary coarse-grainings of Z and X	—— " ——

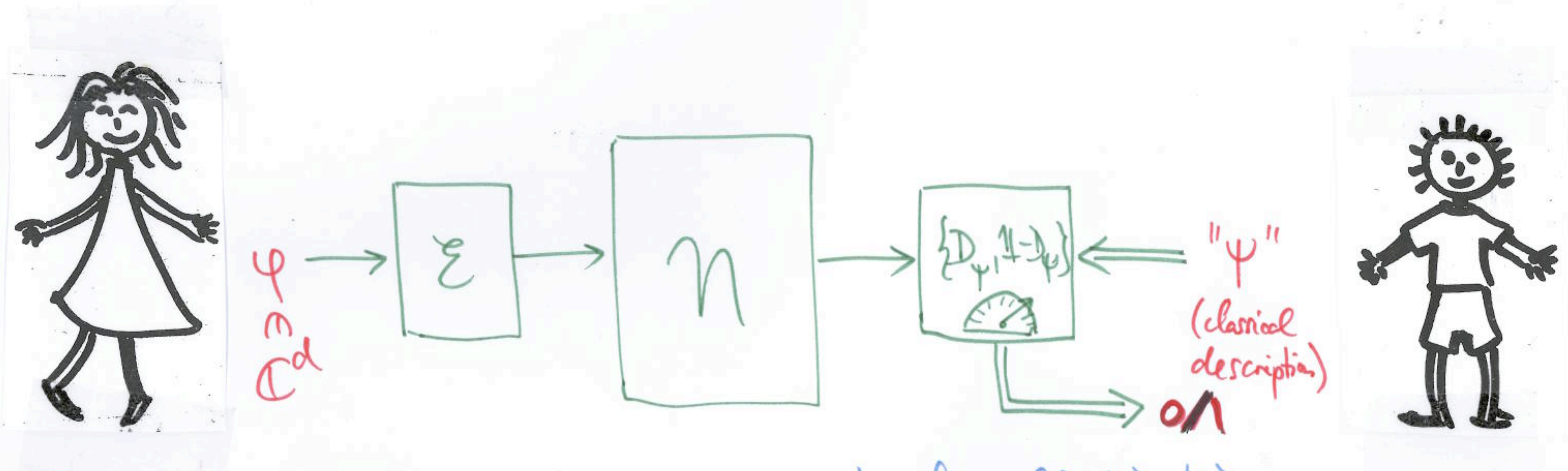
Here is what we get for various classes of POVMs $\{M_i\}$:



s.t. $\mathrm{Tr}\,\varphi M_i \approx \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi)) \cdot D_i\right]$

$\{M_i\}$	Information task
single von Neumann measurement, say Z	classical communication (eigenbasis of Z)
all POVMs	quantum communication (since we can build a decoder $\mathcal{D}$ for the state φ)
Z and X	—— " ——
all binary coarse-grainings of Z and X	—— " ——
all POVMs of the form $(\lvert\psi\rangle\langle\psi\rvert, \mathbb{1} - \lvert\psi\rangle\langle\psi\rvert)$, $\lvert\psi\rangle$ pure state	quantum identification

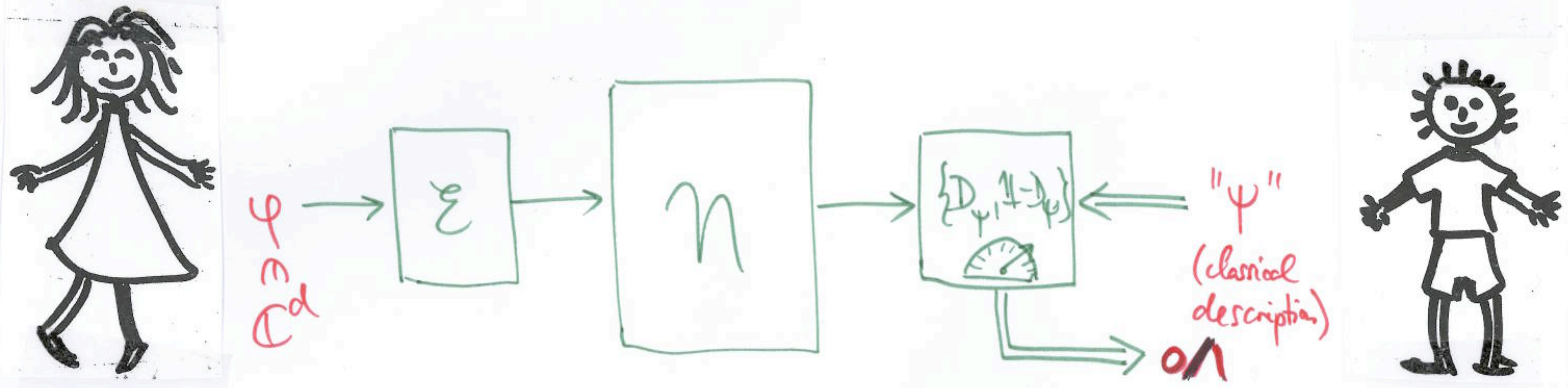
3. Identification



s.t. for all $|\varphi\rangle, |\psi\rangle$

$$\left| \mathrm{Tr}\, \varphi\psi - \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi)) D_\psi\right] \right| \leq \epsilon$$

3. Identification



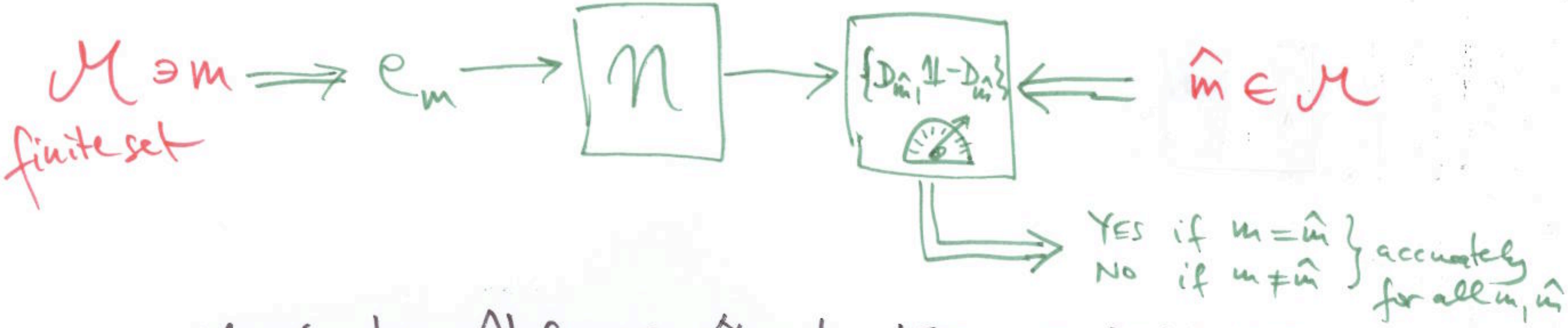
s.t. for all $|\varphi\rangle, |\psi\rangle$

$$\left| \mathrm{Tr}\, \varphi\psi - \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi)) D_\psi\right] \right| \leq \epsilon$$

<u>Quantum-ID code</u>: $\mathcal{E}$ and the collection of $0 \leq D_\psi \leq \mathbb{1}$ ($|\psi\rangle \in \mathbb{C}^d$).

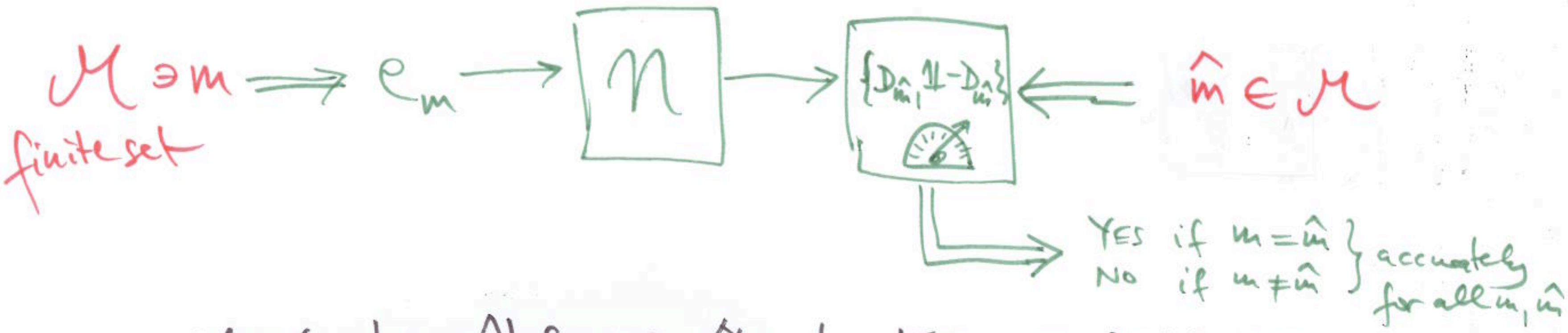
<u>Parameters</u>: Error $\underline{\epsilon}$ and encoded dimension $\underline{d}$.

Classical version :



was considered by Ahlswede/Dueck, IEEE-IT $\underline{35}$(1), 1989
for classical channel $\mathcal{N}$

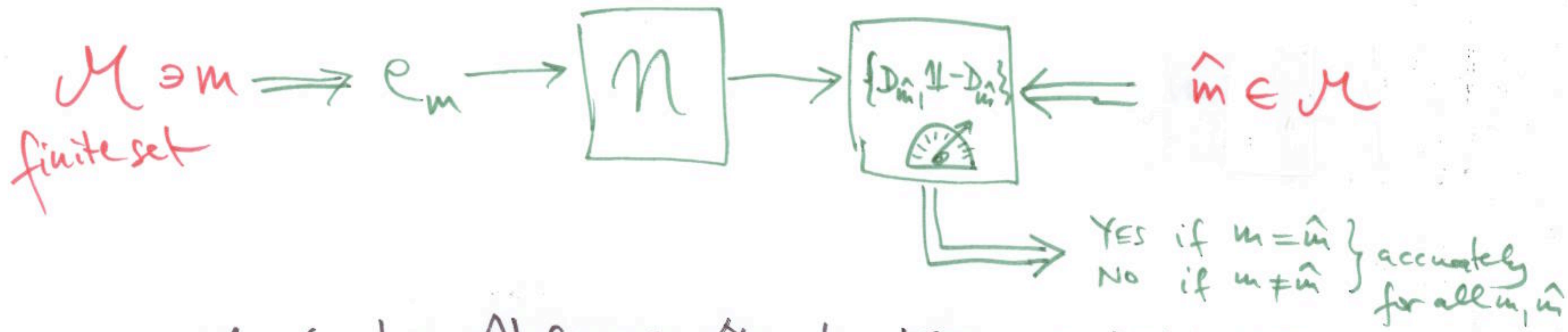
Classical version:



was considered by Ahlswede/Dueck, IEEE-IT $\underline{35}$(1), 1989 for classical channel $\mathcal{N}$

$\rightsquigarrow$ For n channel uses $\mathcal{N}^{\otimes n}$, $\max|\mathcal{M}| = 2^{2^{C(\mathcal{N})n+o(n)}}$, where $C(\mathcal{N})$ is the Shannon capacity of $\mathcal{N}$.

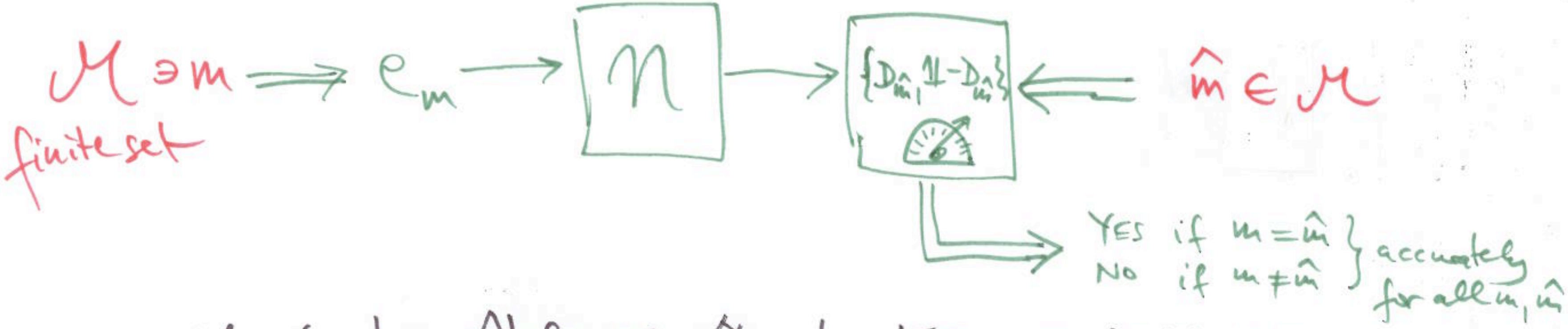
Classical version:



was considered by Ahlswede/Dueck, IEEE-IT $\underline{35}$(1), 1989
for classical channel $\mathcal{N}$
⇝ For n channel uses $\mathcal{N}^{\otimes n}$, $\max|\mathcal{M}| = 2^{2^{C(\mathcal{N})n+o(n)}}$,
where $C(\mathcal{N})$ is the Shannon capacity of $\mathcal{N}$.

Löber looked at general quantum channels (PhD thesis, Bielefeld 1999),
but with restrictions on en-/decoding.
Ahlswede/W., IEEE-IT $\underline{48}$(3), 2002 show for cq-channel $\mathcal{N}$, that
$\max|\mathcal{M}| = 2^{2^{C(\mathcal{N})n+o(n)}}$, where $C(\mathcal{N})$ = classical capacity of $\mathcal{N}$.

Classical version:



was considered by Ahlswede/Dueck, IEEE-IT $\underline{35}$(1), 1989 for classical channel $\mathcal{N}$

⤳ For n channel uses $\mathcal{N}^{\otimes n}$, $\max|\mathcal{M}| = 2^{2^{C(\mathcal{N})n+o(n)}}$, where $C(\mathcal{N})$ is the Shannon capacity of $\mathcal{N}$.

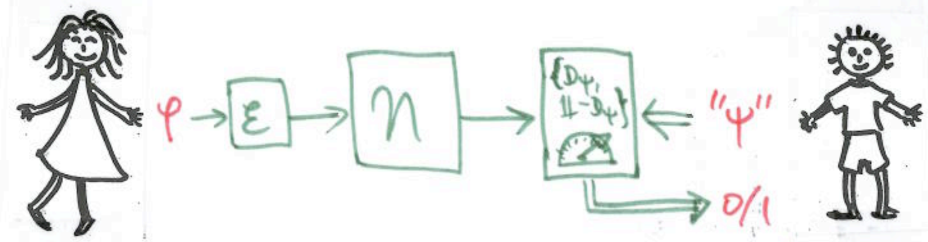
Löber looked at general quantum channels (PhD thesis, Bielefeld 1999), but with restrictions on en-/decoding.

Ahlswede/W., IEEE-IT $\underline{48}$(3), 2002 show for cq-channel $\mathcal{N}$, that $\max|\mathcal{M}| = 2^{2^{C(\mathcal{N})n+o(n)}}$, where $C(\mathcal{N})$ = classical capacity of $\mathcal{N}$.

W. ("Holevo 60" festschrift, Rinton 2004) shows: for $\mathcal{N} = id_2$ (noiseless qubit), $\max|\mathcal{M}| = 2^{2^{2n+o(n)}}$

{with pure ρ_m get only $2^{2^{n+o(n)}}$ by "fingerprint" states of Buhrman et al., PRL 2001}

4. Quantum-ID, Fidelity and Forgetfulness

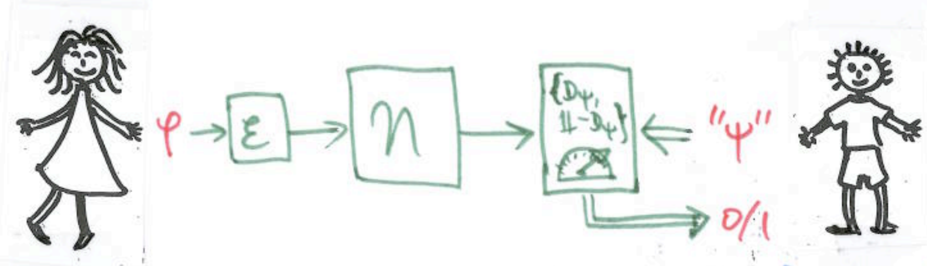


s.t. $\operatorname{Tr} \varphi\psi \approx \operatorname{Tr}[\mathcal{N}(\mathcal{E}(\varphi)) D_\psi]$

1st observation: $\mathcal{N} \circ \mathcal{E}$ is δ-geometry preserving $[\delta = \delta(\epsilon)]$ for pretty much any distance measure of states that is monotonic under cptp maps; incl. fidelity $F(\rho,\sigma)$ and trace distance $\|\rho-\sigma\|_1$.

E.g. $\left| F(\varphi,\psi) - F(\mathcal{N}(\mathcal{E}(\varphi)), \mathcal{N}(\mathcal{E}(\psi))) \right| \leq \delta$

4. Quantum-ID, Fidelity and Forgetfulness



s.t. $\mathrm{Tr}\,\varphi\psi \approx \mathrm{Tr}\left[\mathcal{N}(\mathcal{E}(\varphi))\,D_\psi\right]$

1st observation: $\mathcal{N}\circ\mathcal{E}$ is δ-geometry preserving [$\delta = \delta(\epsilon)$]

for pretty much any distance measure of states that is monotonic under cptp maps; incl. fidelity $F(\rho,\sigma)$ and trace distance $\|\rho-\sigma\|_1$.

E.g. $\left| F(\varphi,\psi) - F\big(\mathcal{N}(\mathcal{E}(\varphi)), \mathcal{N}(\mathcal{E}(\psi))\big)\right| \leq \delta$

Intuitive reason: on $\mathrm{span}\{|\varphi\rangle, |\psi\rangle\} =: Q < A$ we can simulate any measurement $\Longrightarrow$ hence it is an error correcting code and we can construct a decoding $\mathcal{D}$:

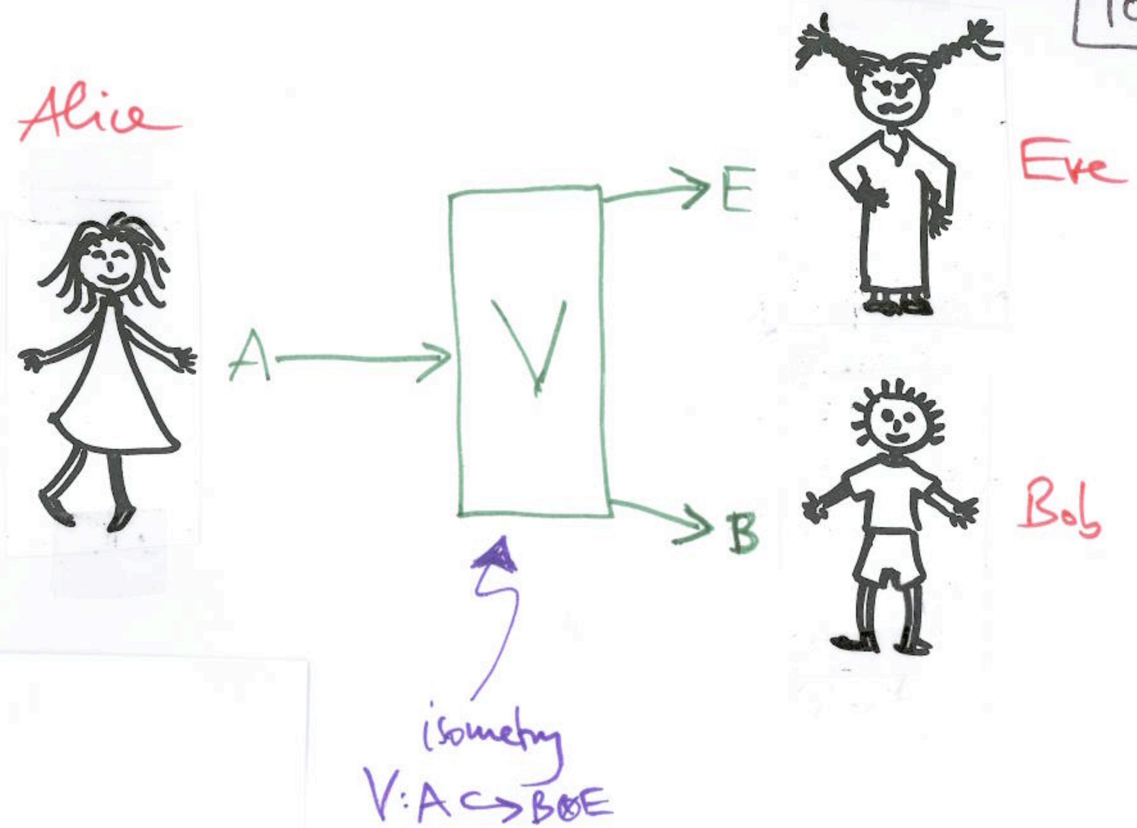
$$\varphi \longmapsto \mathcal{N}(\mathcal{E}(\varphi)) \longmapsto \approx \varphi$$
$$\psi \longmapsto \mathcal{N}(\mathcal{E}(\psi)) \longmapsto \approx \psi$$

... now monotonicity ...

For the next steps contract $\mathcal{N} \circ \mathcal{E}$ to one channel — still called $\mathcal{N}$.

We derive further insights from the Stinespring dilation of it:

$$\mathcal{N}(\varrho) = \mathrm{Tr}_E V \varrho V^\dagger$$

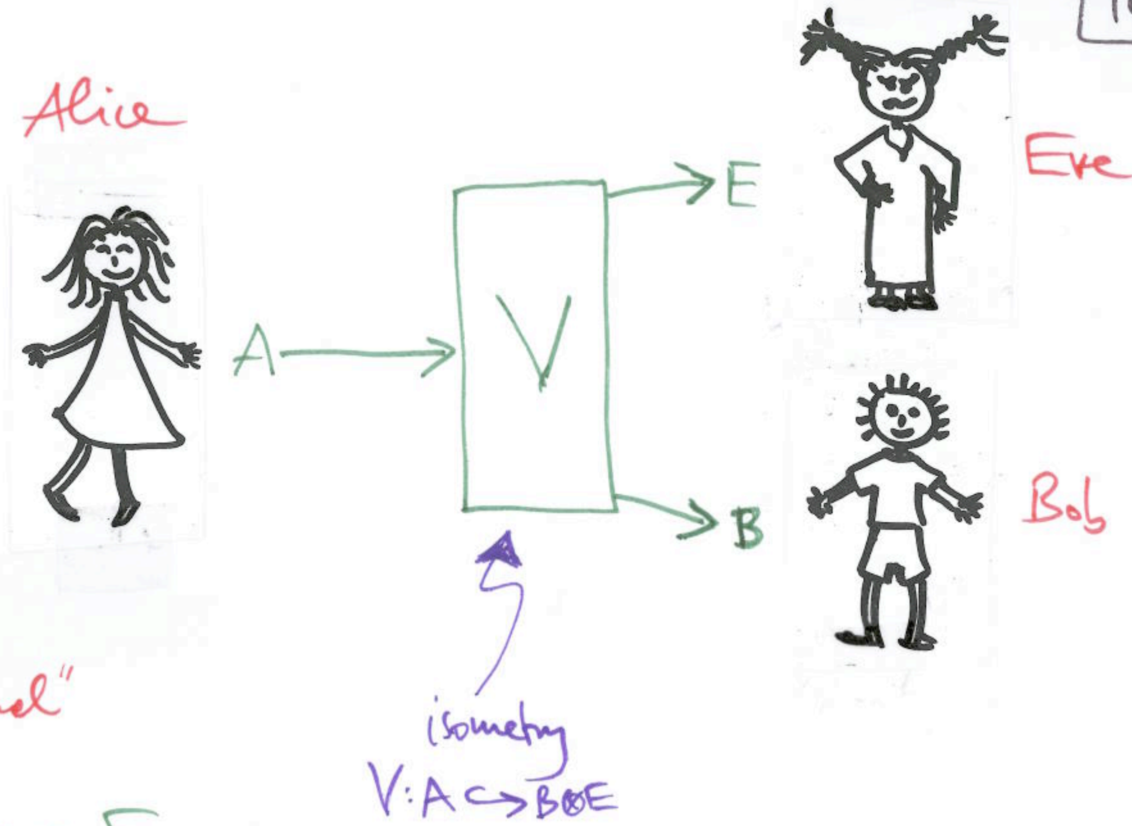


For the next steps contract $\mathcal{N}\circ\mathcal{E}$ to one channel — still called $\mathcal{N}$.

We derive further insights from the Stinespring dilation of it:

$$\mathcal{N}(\rho) = \mathrm{Tr}_E\, V\rho V^\dagger$$

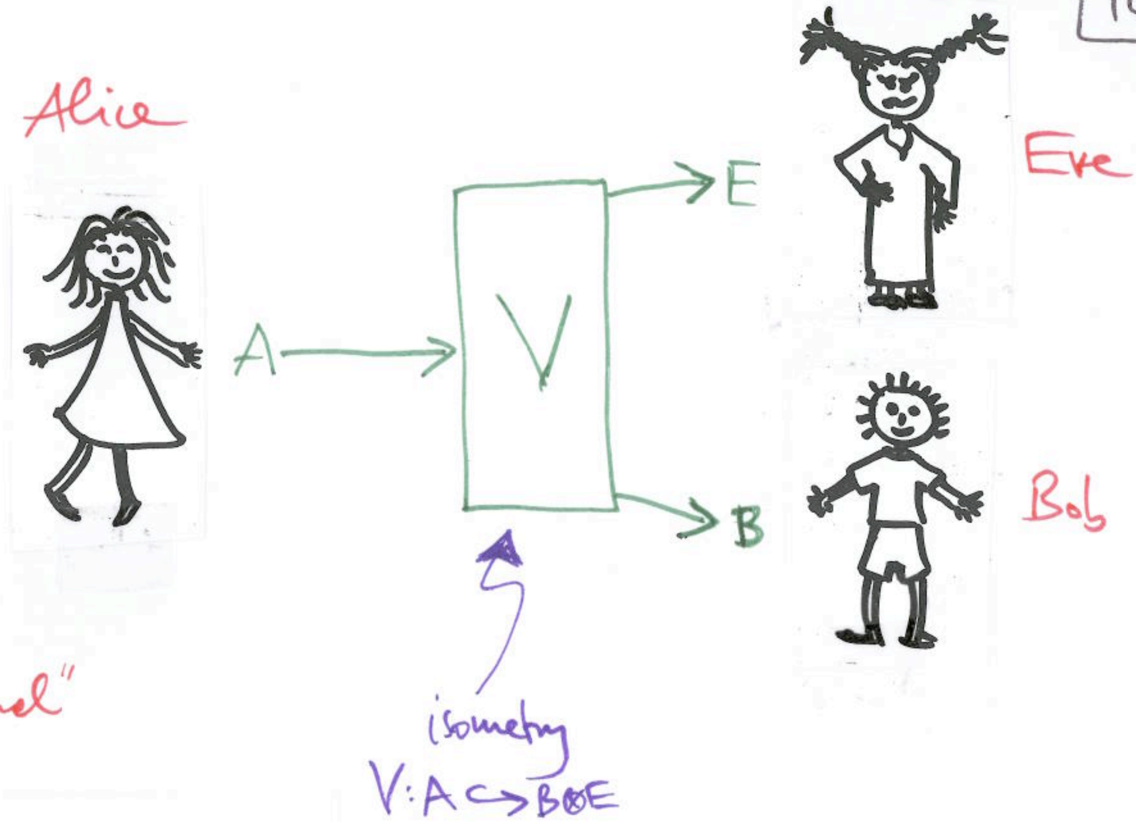
$$\mathcal{N}^c(\rho) = \mathrm{Tr}_B\, V\rho V^\dagger \quad \text{"complementary channel"}$$



- $\mathcal{N}^c$ essentially unique up to unitaries on E
- V allows us to identify the channel $\mathcal{N}$ with a subspace $S := VA \subset B\otimes E$ of the combined Bob+Eve system

For the next steps contract $\mathcal{N}\circ\mathcal{E}$ to one channel — still called $\mathcal{N}$.

We derive further insights from the Stinespring dilation of it:



$$\mathcal{N}(\rho) = \mathrm{Tr}_E\, V\rho V^\dagger$$

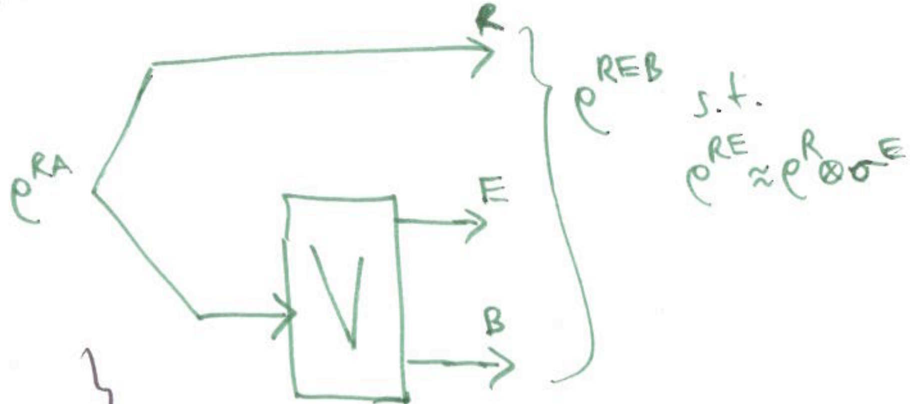
$$\mathcal{N}^c(\rho) = \mathrm{Tr}_B\, V\rho V^\dagger$$ "complementary channel"

Recall the important decoupling principle:

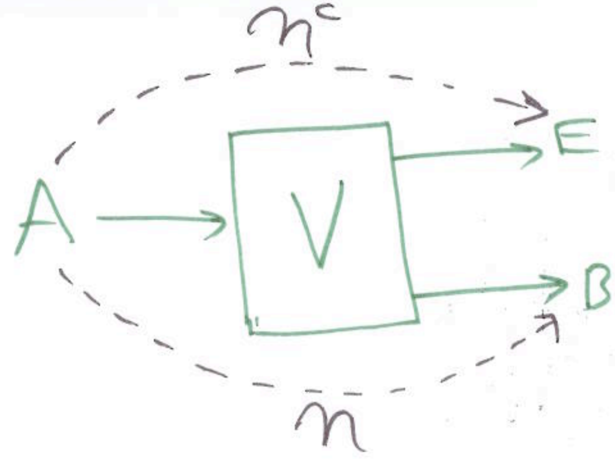
$\mathcal{N}$ is (approx.) correctable [i.e. $\exists\, \mathcal{D}$ cptp s.t. $\mathcal{D}\circ\mathcal{N} \approx \mathrm{id}_A$]

$\Updownarrow$

$\mathcal{N}^c$ is completely forgetful [i.e. $\forall \rho^{RA}$ $(\mathrm{id}\otimes\mathcal{N}^c)\rho^{RA} \approx \rho^R \otimes \sigma^E$]



{Schumacher/Westmoreland, QIP 1(1+2), 2002.
Kretschmann/Schlingemann/Werner, IEEE-IT 54(4), 2008.}



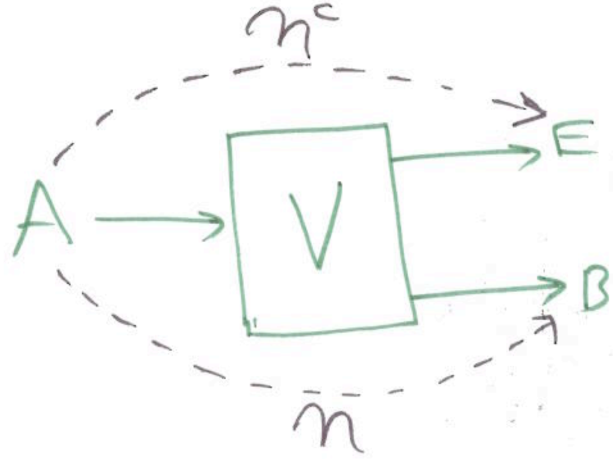
2nd (Fidelity-Alternative): $\mathcal{N}$ is ϵ-fidelity preserving iff $\mathcal{N}^c$ is δ-forgetful [i.e. for all ρ^A on A, $F(\mathcal{N}^c(\rho^A), \sigma^E) \geq 1-\delta$]

2nd (Fidelity-Alternative): $\mathcal{N}$ is

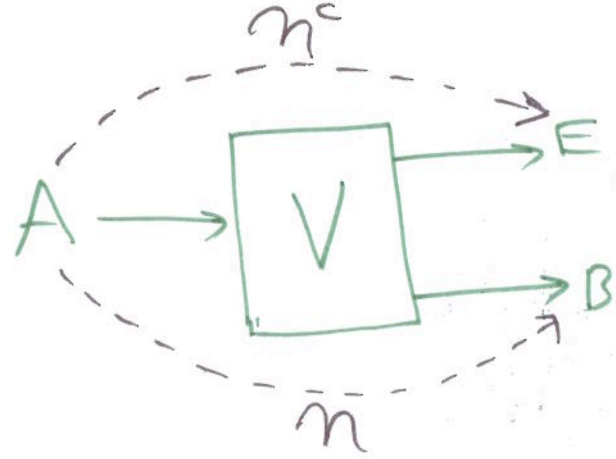
ϵ-fidelity preserving iff $\mathcal{N}^c$ is

δ-forgetful [i.e. for all ρ^A on A,

$$F(\mathcal{N}^c(\rho^A), \sigma^E) \geq 1-\delta]$$



{Intuitively: clear by applying decoupling principle to the 2-dim. subspaces spanned by $|\varphi\rangle, |\psi\rangle$... }



2nd (Fidelity-Alternative): $\mathcal{N}$ is ϵ-fidelity preserving iff $\mathcal{N}^c$ is δ-forgetful [i.e. for all ρ^A on A,

$$F(\mathcal{N}^c(\rho^A), \sigma^E) \geq 1-\delta \,]$$

{Intuitively: clear by applying decoupling principle to the 2-dim. subspaces spanned by $|\varphi\rangle, |\psi\rangle$...}

3rd: If $\mathcal{N}$ is ϵ-fidelity preserving and all states $\mathcal{N}(\varphi)$ [for pure $\varphi = |\varphi\rangle\langle\varphi|$] have sufficiently "flat" spectrum [non-zero eigenvalue range from μ to λ], then one can complete the channel to a q-ID code with error $\eta \leq O\left(\frac{\lambda}{\mu}\right) \epsilon^{O(1)}$ [by constructing suitable operators $0 \leq D_\psi \leq \mathbb{1}$ for $|\psi\rangle \in A$].

In summary:

Quantum-ID code for channel $\mathcal{N}$ $\xLeftrightarrow[\text{(more or less)}]{}$ $\mathcal{N}$ (approx.) geometry preserving $\Longleftrightarrow$ $\mathcal{N}^c$ (approx.) forgetful

In summary:

Quantum-ID code for channel $\mathcal{N}$ $\Longleftrightarrow$ (more or less) $\mathcal{N}$ (approx.) geometry preserving $\Longleftrightarrow$ $\mathcal{N}^c$ (approx.) forgetful

[Compare to the decoupling principle:

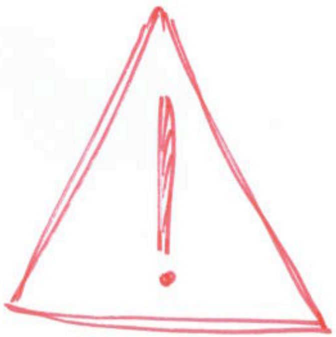
Quantum info decoder for channel $\mathcal{N}$ $\Longleftrightarrow$ $\mathcal{N}^c$ (approximately) completely forgetful]

In summary:

Quantum-ID code for channel $\mathcal{N}$ $\Longleftrightarrow$ (more or less) $\mathcal{N}$ (approx.) geometry preserving $\Longleftrightarrow$ $\mathcal{N}^c$ (approx.) forgetful

[Compare to the decoupling principle:

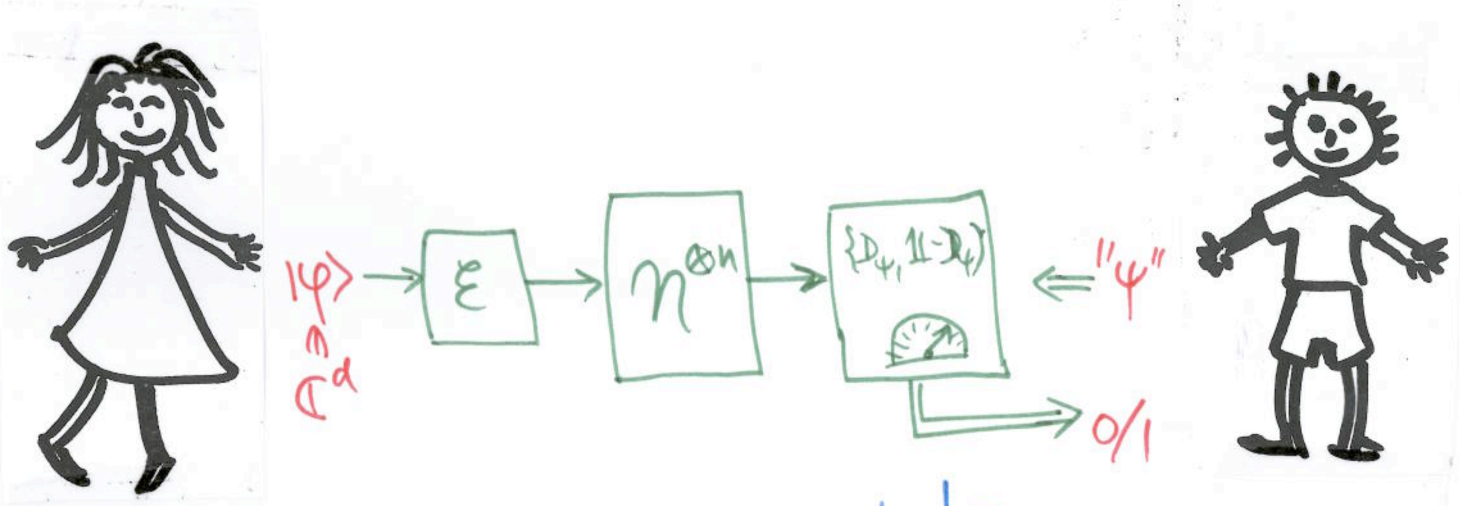
Quantum info decoder for channel $\mathcal{N}$ $\Longleftrightarrow$ $\mathcal{N}^c$ (approximately) completely forgetful]



Big difference between forgetfulness and complete forgetfulness (cf. difference between naive norm & diamond norm on superoperators): e.g. consider the $d \to d$ channel $\rho \longmapsto \frac{d\mathbb{1} - \rho^T}{d^2-1}$ or examples in Bennett et al., IEEE-IT 51(1), 2005.

5. Quantum-ID capacity

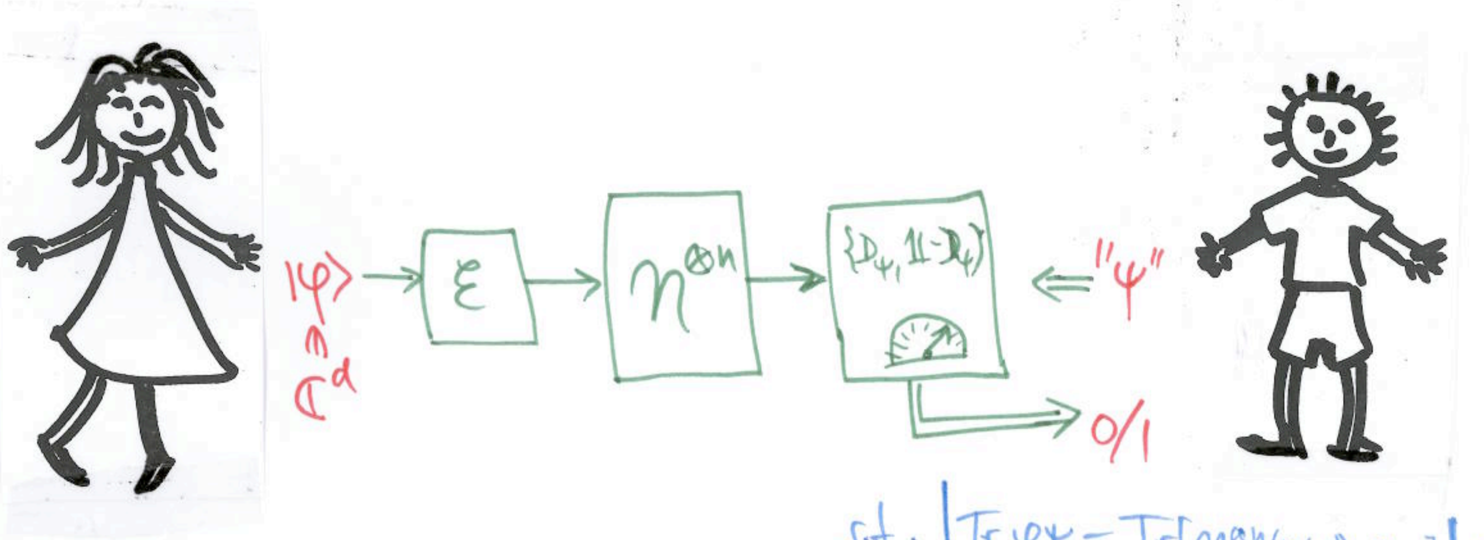
Now consider using the same channel n times, as $\epsilon \to 0$ and with maximum dimension d:



s.t. $\left| \mathrm{Tr}\, \varphi\psi - \mathrm{Tr}\left[\eta^{\otimes n}(\mathcal{E}(\varphi)) \cdot D_\psi\right] \right| \leq \epsilon$

5. Quantum-ID capacity

Now consider using the same channel n times, as $\epsilon \to 0$ and with maximum dimension d:

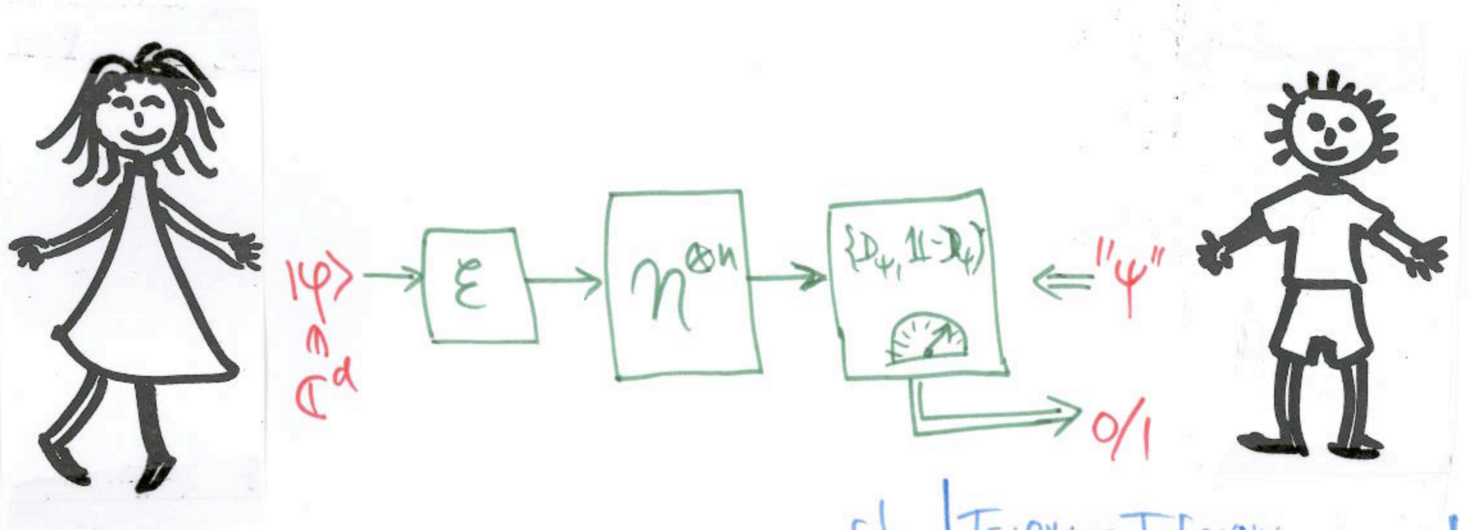


s.t. $\left| \operatorname{Tr} \varphi\psi - \operatorname{Tr}\left[\mathcal{N}^{\otimes n}(\mathcal{E}(\varphi)) \cdot D_\psi\right] \right| \leq \epsilon$

Observe: d can be at most exponential in n [because we can use $2^{\Theta(d)}$ fingerprinting states (Buhrman et al., PRL 2001) to get classical ID code ... which is at most $2^{2^{O(n)}}$ large]

5. Quantum-ID capacity

Now consider using the same channel n times, as $\epsilon \to 0$ and with maximum dimension d:



s.t. $\left| \operatorname{Tr} \varphi\psi - \operatorname{Tr}\left[\eta^{\otimes n}(\mathcal{E}(\varphi)) \cdot D_\psi\right] \right| \leq \epsilon$

<u>Observe</u>: d can be at most exponential in n [because we can use $2^{\Theta(d)}$ fingerprinting states (Buhrman et al., PRL 2001) to get classical ID code ... which is at most $2^{2^{O(n)}}$ large]

Hence the <u>definition</u>: the rate of the above code is $\frac{1}{n}\log d =: R$. The maximum achievable rate R s.t. $\epsilon \to 0$ as $n \to \infty$ is the <u>quantum-ID capacity $Q_{ID}(\eta)$</u>.

What do we know about $Q_{ID}(\mathcal{N})$?

(i) From the Fidelity Alternative: $Q_{ID}(\mathcal{N})>0 \Rightarrow Q(\mathcal{N})>0$

I.e., only channels with positive quantum capacity can have quantum-ID capacity.

[In particular: quantum-ID is not cloneable!]

What do we know about $Q_{ID}(\mathcal{N})$?

(i) From the Fidelity Alternative: $Q_{ID}(\mathcal{N})>0 \Rightarrow Q(\mathcal{N})>0$

I.e., only channels with positive quantum capacity can have quantum-ID capacity.

[In particular: quantum-ID is not cloneable!]

(ii) W., "Holevo 60" festschrift, Rinton 2004, proves that $Q_{ID}(\mathrm{id}_2)=2$, while of course $Q(\mathrm{id}_2)=1$.

[Encoding by appending $O(\log n)$ ancilla qubits in a pure state to the $2n$ data qubits, applying a random unitary, and tracing out the last n qubits ....]

What do we know about $Q_{ID}(\mathcal{N})$?

(i) From the Fidelity Alternative: $Q_{ID}(\mathcal{N})>0 \Rightarrow Q(\mathcal{N})>0$

I.e., only channels with positive quantum capacity can have quantum-ID capacity.

[In particular: quantum-ID is not clonable!]

(ii) W., "Holevo 60" festschrift, Rinton 2004, proves that $Q_{ID}(id_2) = 2$, while of course $Q(id_2) = 1$.

[Encoding by appending $O(\log n)$ ancilla qubits in a pure state to the $2n$ data qubits, applying a random unitary, and tracing out the last n qubits ....]

(iii) NEW results — using the Fidelity Alternative we can prove capacity results by forcing forgetfulness for Eve....

Theorem A: The quantum-ID capacity of $\mathcal{N}$ is the regularization of $Q^{(1)}_{ID}(\mathcal{N}) = \sup\left\{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\sigma^{AA'} \text{ and } I(A\rangle B) = S(B) - S(AB) > 0 \right\}$

I.e., $Q_{ID}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}_{ID}(\mathcal{N}^{\otimes n})$.

Theorem B:

Theorem A: The quantum-ID capacity of $\mathcal{N}$ is the regularization of $Q^{(1)}_{ID}(\mathcal{N}) = \sup \{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\sigma^{AA'}$ and $I(A\rangle B) = S(B) - S(AB) > 0 \}$

I.e., $$Q_{ID}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}_{ID}(\mathcal{N}^{\otimes n}).$$

Motivated by the ugliness of this formula, and by $Q_{ID}(id_2) = 2$, we allow use of noiseless qubit channels — at a cost of 2 per qubit.

Amortised rate of a code on $\mathcal{N}^{\otimes n}$, using rn qubits extra: $\frac{1}{n}\log d - r =: \tilde{R}$;

$\tilde{Q}_{ID}(\mathcal{N}) :=$ maximum achievable amortised rate.

Theorem B:

Theorem A: The quantum-ID capacity of $\mathcal{N}$ is the regularization of $Q^{(1)}_{ID}(\mathcal{N}) = \sup \{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\sigma^{AA'}$ and $I(A\rangle B) = S(B) - S(AB) > 0 \}$

I.e., $Q_{ID}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}_{ID}(\mathcal{N}^{\otimes n})$.

Motivated by the ugliness of this formula, and by $Q_{ID}(id_2) = 2$, we allow use of noiseless qubit channels — at a cost of 2 per qubit.

Amortised rate of a code on $\mathcal{N}^{\otimes n}$, using rn qubits extra: $\frac{1}{n}\log d - r =: \tilde{R}$;

$\tilde{Q}_{ID}(\mathcal{N}) :=$ maximum achievable amortised rate.

Theorem B: $\tilde{Q}_{ID}(\mathcal{N}) = \sup_{k \geq 0} \{ Q_{ID}(\mathcal{N} \otimes id_2^{\otimes k}) - 2k \}$

$= \sup \{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\phi^{AA'} \}$

Theorem A: The quantum-ID capacity of $\mathcal{N}$ is the regularization of $Q^{(1)}_{ID}(\mathcal{N}) = \sup \{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\sigma^{AA'}$ and $I(A\rangle B) = S(B) - S(AB) > 0 \}$

I.e., $Q_{ID}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}_{ID}(\mathcal{N}^{\otimes n})$.

Motivated by the ugliness of this formula, and by $Q_{ID}(id_2) = 2$, we allow use of noiseless qubit channels — at a cost of 2 per qubit.

Amortised rate of a code on $\mathcal{N}^{\otimes n}$, using rn qubits extra: $\frac{1}{n}\log d - r =: \tilde{R}$;

$\tilde{Q}_{ID}(\mathcal{N}) :=$ maximum achievable amortised rate.

Theorem B: $\tilde{Q}_{ID}(\mathcal{N}) = \sup_{k\geq 0} \{ Q_{ID}(\mathcal{N} \otimes id_2^{\otimes k}) - 2k \}$

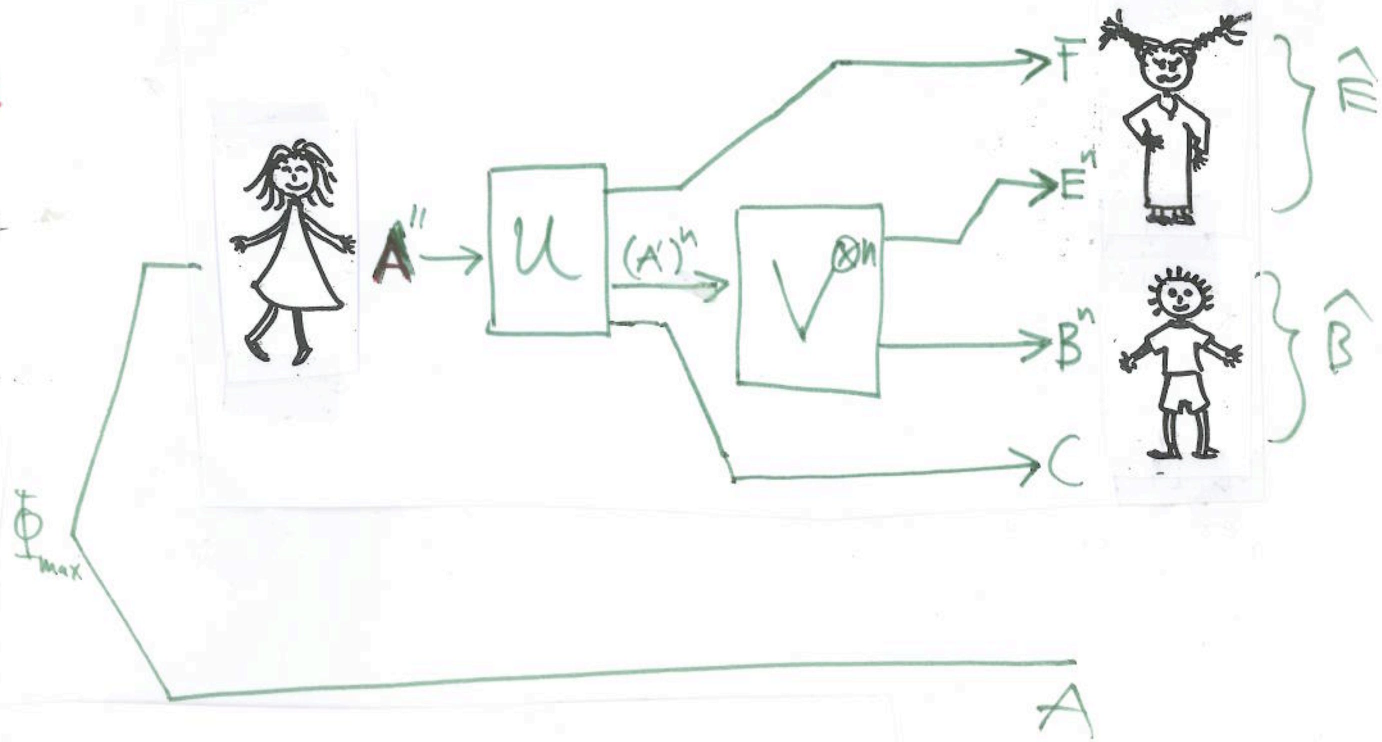
$$= \sup \{ I(A:B) \mid \rho^{AB} = (id \otimes \mathcal{N})\phi^{AA'} \}$$

⚠ equals the entanglement-assisted classical capacity of $\mathcal{N}$! [Bennett et al., IEEE-IT 48(10), 2002]

Ideas for the proof — both Thm. A & B:

Converse (upper bound):

The typical q-ID code on the right maps the encoded space A to a subspace $S \subset \hat{B} \otimes \hat{E}$.

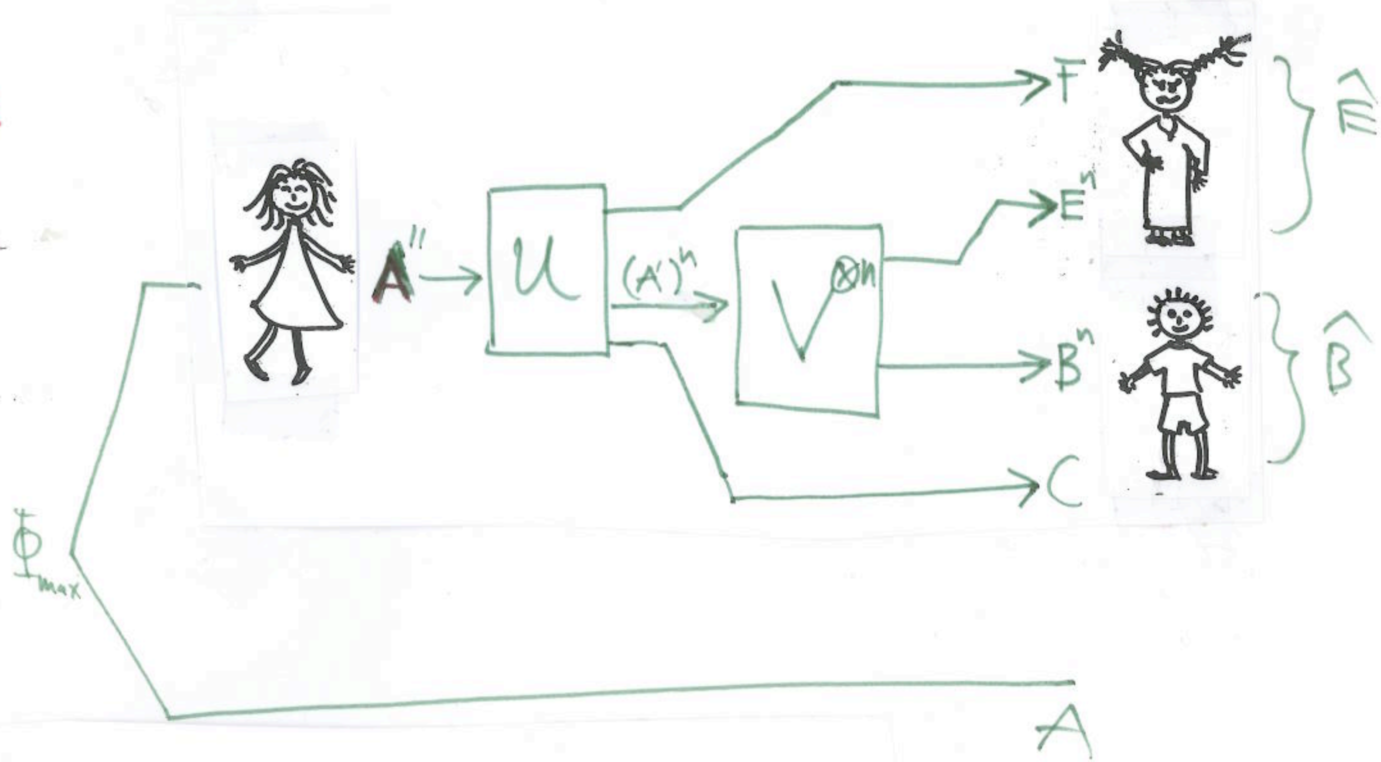


Ideas for the proof — both Thm. A & B:

Converse (upper bound):

The typical q-ID code on the right maps the encoded space A to a subspace $S \subset \hat{B} \otimes \hat{E}$.

An observation: Let $\sum_x p_x \phi_x = \frac{1\!\!1}{|S|}$,
then (by fidelity alt.)
$S(\hat{B}) > S(\hat{B}|X) = S(\hat{E}|X) \approx S(\hat{E})$.

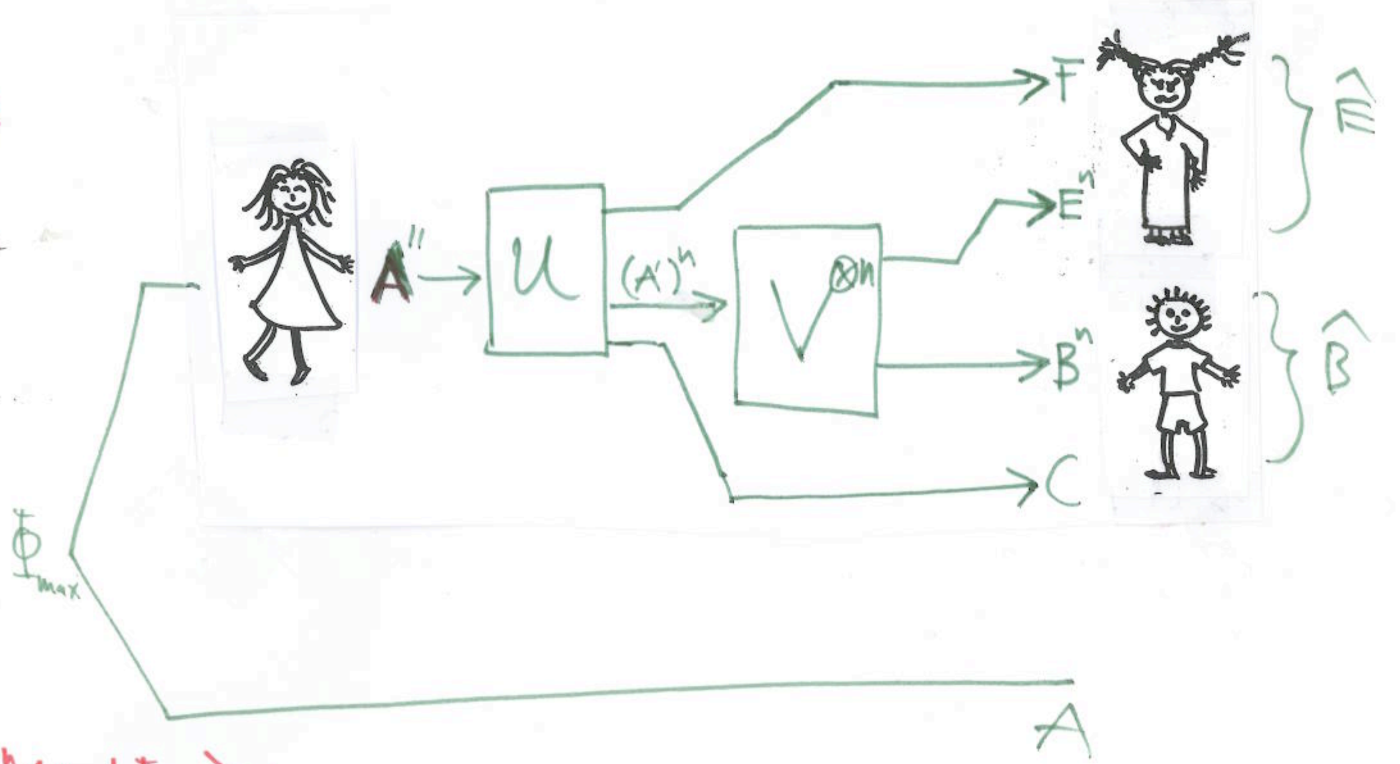


Ideas for the proof — both Thm. A & B:

Converse (upper bound):

The typical q-ID code on the right maps the encoded space A to a subspace $S \subset \hat{B} \otimes \hat{E}$.

An observation: Let $\sum_x p_x \phi_x = \frac{\mathbb{1}}{|S|}$, then (by fidelity alt.) $S(\hat{B}) \geq S(\hat{B}|X) = S(\hat{E}|X) \approx S(\hat{E})$.



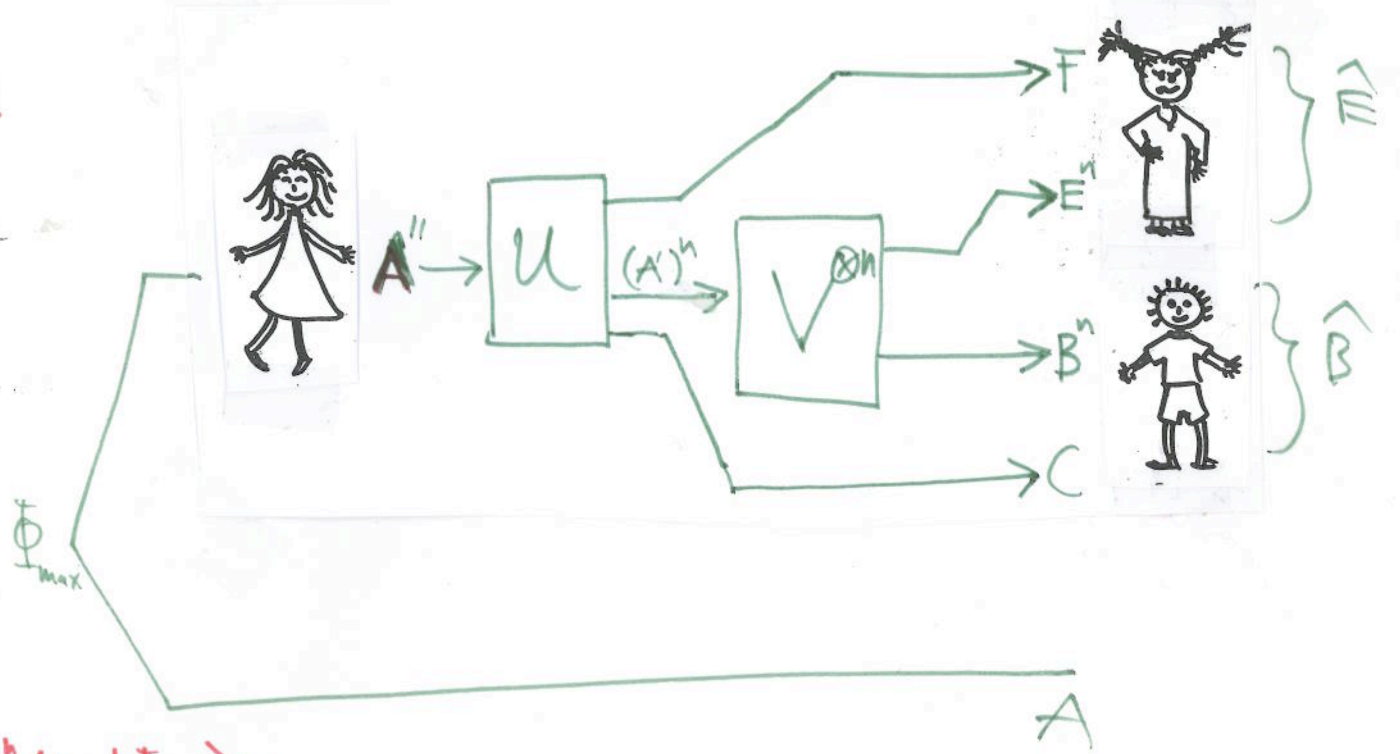
Now, w.r.t. the state $|\psi\rangle = V^{\otimes n}\,\mathcal{U}\,|\Phi_{max}\rangle$:

$$\begin{aligned}
\log|A| = S(A) &\leq S(A) + S(\hat{B}) - S(\hat{E}) + o(n) && \text{[above observation]}\\
&= I(A:\hat{B}) + o(n) && \text{[def]}\\
&= I(A:B^n) + I(A:C|B^n) + o(n) && \text{[chain rule]}\\
&\leq I(A:B^n) + 2\log|C| + o(n)
\end{aligned}$$

Ideas for the proof — both Thm. A & B:

Converse (upper bound):

The typical q-ID code on the right maps the encoded space A to a subspace $S \subset \hat{B} \otimes \hat{E}$.



An observation: Let $\sum_x p_x \phi_x = \frac{1\!\!1}{S}$, then (by fidelity alt.)

$S(\hat{B}) \geq S(\hat{B}|X) = S(\hat{E}|X) \approx S(\hat{E})$.

Now, w.r.t. the state $|\psi\rangle = V^{\otimes n}\mathcal{U}|\Phi_{max}\rangle$:

$$
\begin{aligned}
\log|A| = S(A) &\leq S(A) + S(\hat{B}) - S(\hat{E}) + o(n) && \text{[above observation]}\\
&= I(A:\hat{B}) + o(n) && \text{[def]}\\
&= I(A:B^n) + I(A:C|B^n) + o(n) && \text{[chain rule]}\\
&\leq I(A:B^n) + 2\log|C| + o(n)
\end{aligned}
$$

At the same time, for $|C| = 1$:

$I(A\rangle B^n) = I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) \geq 0.$ ▨

Direct part (lower bound):

[Can again do both Thms. A & B together]

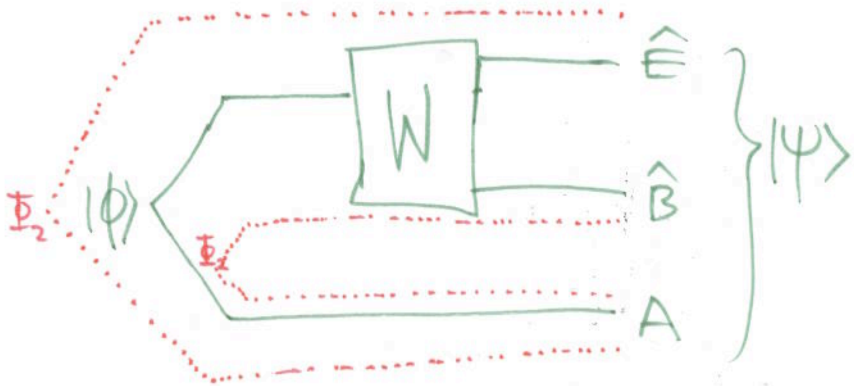
Direct part (lower bound):

[Can again do both Thms. A&B together]

- In the situation on the right, it is enough to show achievability of $S(A)$, assuming $I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) > 0$

Direct part (lower bound):

[Can again do both Thms. A&B together]



- In the situation on the right, it is enough to show achievability of $S(A)$, assuming $I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) > 0$

[Sending a qubit from Alice to Bob shares an ebit Φ_2, increasing $I(A:\hat{B})$ by 2, exactly the amortised amount; sending a qubit from Alice to Eve, sharing an ebit, doesn't change $I(A:\hat{B})$ but reduces $S(\hat{B}) - S(\hat{E}) = I(A\rangle\hat{B})$ by 1, so can get $S(\hat{B}) - S(\hat{E}) \gtrsim 0$]

Direct part (lower bound):

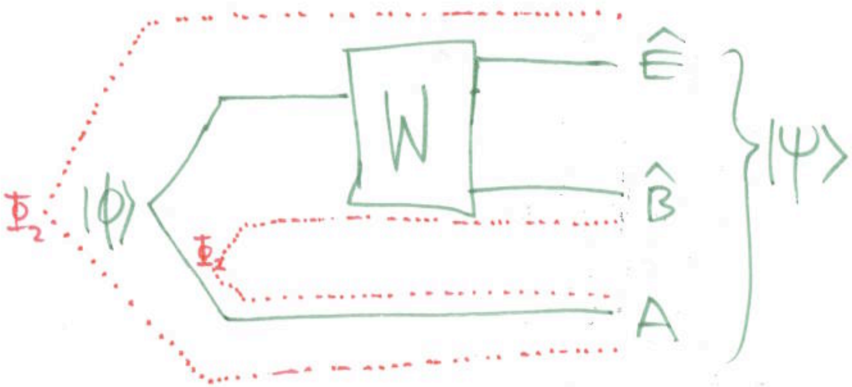
[Can again do both Thms. A & B together]

- In the situation on the right, it is enough to show achievability of $S(A)$, assuming $I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) > 0$

  [Sending a qubit from Alice to Bob shares an ebit Φ_2, increasing $I(A:\hat{B})$ by 2, exactly the amortised amount; sending a qubit from Alice to Eve, sharing an ebit, doesn't change $I(A:\hat{B})$ but reduces $S(\hat{B})-S(\hat{E})=I(A\rangle\hat{B})$ by 1, so can get $S(\hat{B})-S(\hat{E}) \gtrsim 0$]

- Consider $|\phi\rangle^{\otimes n}$ $(|\psi\rangle^{\otimes n})$ and pick S as a random subspace of the typical subspace of $(\psi^A)^{\otimes n}$; $|S| = 2^{n(S(A)-\epsilon)}$. By Popescu/Short/W., Nat. Phys. $\underline{2}$(11), 2006, the channel $\mathrm{Tr}_{\hat{B}}: S \longrightarrow \hat{E}^n$ is approximately forgetful*, hence — by fidelity alt. — the complementary $\mathrm{Tr}_{\hat{E}}: S \longrightarrow \hat{B}^n$ is fidelity-preserving*.

Direct part (lower bound):



[Can again do both Thms. A & B together]

- In the situation on the right, it is enough to show achievability of $S(A)$, assuming $I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) > 0$

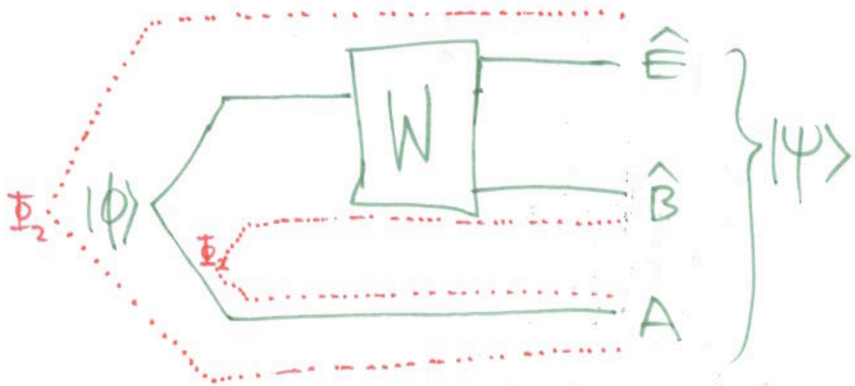
[Sending a qubit from Alice to Bob shares an ebit Φ_2, increasing $I(A:\hat{B})$ by 2, exactly the amortised amount; sending a qubit from Alice to Eve, sharing an ebit, doesn't change $I(A:\hat{B})$ but reduces $S(\hat{B}) - S(\hat{E}) = I(A\rangle\hat{B})$ by 1, so can get $S(\hat{B}) - S(\hat{E}) \gtrsim 0$]

- Consider $|\phi\rangle^{\otimes n}$ $\left(|\psi\rangle^{\otimes n}\right)$ and pick S as a random subspace of the typical subspace of $(\psi^A)^{\otimes n}$; $|S| = 2^{n(S(A)-\epsilon)}$. By Popescu/Short/W., Nat. Phys $\underline{2}$(11), 2006, the channel $\mathrm{Tr}_{\hat{B}}: S \to \hat{E}^n$ is approximately forgetful*, hence — by fidelity alt. — the complementary $\mathrm{Tr}_{\hat{E}}: S \to \hat{B}^n$ is fidelity-preserving*.

* with error $e^{-\Theta(\epsilon)n}$!

Direct part (lower bound):

[Can again do both Thms. A & B together]



- In the situation on the right, it is enough to show achievability of $S(A)$, assuming $I(A\rangle\hat{B}) = S(\hat{B}) - S(\hat{E}) > 0$

  [Sending a qubit from Alice to Bob shares an ebit Φ_2, increasing $I(A:\hat{B})$ by 2, exactly the amortised amount; sending a qubit from Alice to Eve, sharing an ebit, doesn't change $I(A:\hat{B})$ but reduces $S(\hat{B}) - S(\hat{E}) = I(A\rangle\hat{B})$ by 1, so can get $S(\hat{B}) - S(\hat{E}) \gtrsim 0$]

- Consider $|\phi\rangle^{\otimes n}$ ($|\psi\rangle^{\otimes n}$) and pick S as a random subspace of the typical subspace of $(\psi^A)^{\otimes n}$; $|S| = 2^{n(S(A)-\epsilon)}$. By Popescu/Short/W., Nat. Phys $\underline{2}$(11), 2006, the channel $\mathrm{Tr}_{\hat{B}} : S \rightarrow \hat{E}^n$ is approximately forgetful*, hence — by fidelity alt. — the complementary $\mathrm{Tr}_{\hat{E}} : S \rightarrow \hat{B}^n$ is fidelity-preserving*. By typicality, can even apply the strong form of the duality, as $\frac{\lambda}{\mu} = 2^{o(n)} \Longrightarrow$ get an ID code. $\boxed{\;}$

* with error $e^{-\Theta(\epsilon)n}$!

6. Outlook

* Theory of quantum identification in complete analogy to that of qubit transmission: both have
  - characterization in terms of simulation of measurements
  - char. via a degree of forgetfulness from the environment's point of view

6. Outlook

* Theory of quantum identification in complete analogy to that of qubit transmission: both have
  - characterization in terms of simulation of measurements
  - char. via a degree of forgetfulness from the environment's point of view

* (Under consideration) Other classes of POVMs? (E.g. bounded rank projectors)

  Visibly given input state $|\varphi\rangle$? (I.e. Alice knows the state)

  Restrictions on the allowed $|\varphi\rangle$?

* Closed form expression for $Q_{ID}(\mathcal{N})$?
(single-letter)

How much amortised rate r is necessary for a given channel $\mathcal{N}$ to achieve $\tilde{Q}_{ID}(\mathcal{N})$? E.g. $r \searrow 0$ for cq-channels!

* Closed form expression for $Q_{ID}(\mathcal{N})$?
(single-letter)

How much amortized rate r is necessary for a given channel $\mathcal{N}$ to achieve $\tilde{Q}_{ID}(\mathcal{N})$? } E.g. $r \searrow 0$ for cq-channels!

* Corollaries: all sorts of lower bounds on plain & amortized classical ID capacities of $\mathcal{N}$... } But C_{ID} and $\tilde{C}_{ID}$ still open!

* Closed form expression for $Q_{ID}(\mathcal{N})$?
(single-letter)

How much amortized rate r is necessary for a given channel $\mathcal{N}$ to achieve $\widetilde{Q}_{ID}(\mathcal{N})$?

E.g. $r \searrow 0$ for cq-channels!

* Corollaries: all sorts of lower bounds on plain & amortized <u>classical</u> ID capacities of $\mathcal{N}$ ...

But C_{ID} and $\widetilde{C}_{ID}$ still open!

* There ought to be a deep reason why $\widetilde{Q}_{ID} = C_E$!?

* Closed form expression for $Q_{ID}(\mathcal{N})$?
(single-letter)

How much amortized rate r is necessary for a given channel $\mathcal{N}$ to achieve $\widetilde{Q}_{ID}(\mathcal{N})$? } E.g. $r \searrow 0$ for cq-channels!

* Corollaries: all sorts of lower bounds on plain & amortized classical ID capacities of $\mathcal{N}$... } But C_{ID} and $\widetilde{C}_{ID}$ still open!

* There ought to be a deep reason why $\widetilde{Q}_{ID} = C_E$!?