Private Information via the Unruh Effect

Prakash Panangaden
McGill University
joint work with
Kamil Bradler and Patrick Hayden

Relativistic Quantum Information Theory

- Does this make sense?
- If we are going to use quantum communication on a large scale, relativistic effects are essential.
- Relativistic effects in classical information theory had already been investigated as early as 1981.

Early Work

- Jarrett and Cover 1981: Relativistic classical information theory.
- Relativistic effects on transmission rates and energy requirements.
- Closely related to time dilation: special relativity.

Our direct inspiration

- Alsing and Milburn 2002 : Entanglement and Lorentz invariance. How does the entanglement of maximally entangled states transform under Lorentz transformation?
- Entanglement fidelity is preserved even though the finite dimensional Lorentz transformations are not unitary.
- Remarks on the effect of Unruh or Hawking radiation.

"It is tantalizing to contemplate whether Unruh and/or Hawking radiation might be derived from an information theoretic point of view."

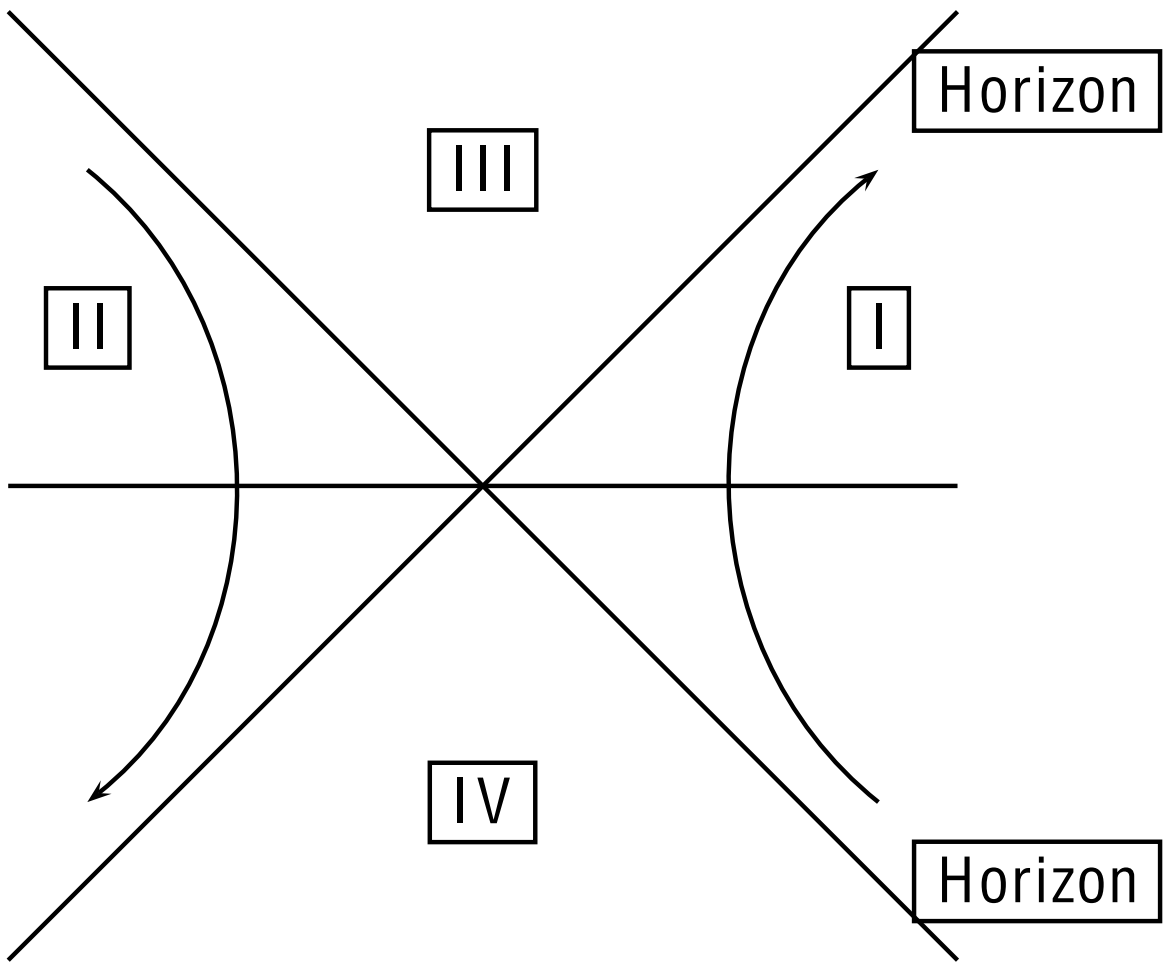
Alsing and Milburn

Teleportation with a uniformly accelerated partner : PRL Alsing and Milburn

We decided to investigate the information-theoretic properties of the Unruh effect.

Outline

- QFT in curved spacetimes: the Unruh effect.
- Private capacity and quantum private capacity.
- Private information via the Unruh effect.



Rindler spacetime.

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

where $\tilde{a}$ is the accelerating observer's annihilation operator.

The change of annihilation and creation operators is called a *Bogolioubov transformation*

There will be modes corresponding to the inaccessible region,

so the accelerating observer's density matrix will involve a partial trace over the modes of the inaccessible region.

Unruh Effect

The inertial observer's vacuum will look like a bath of thermal radiation to the accelerating observer.

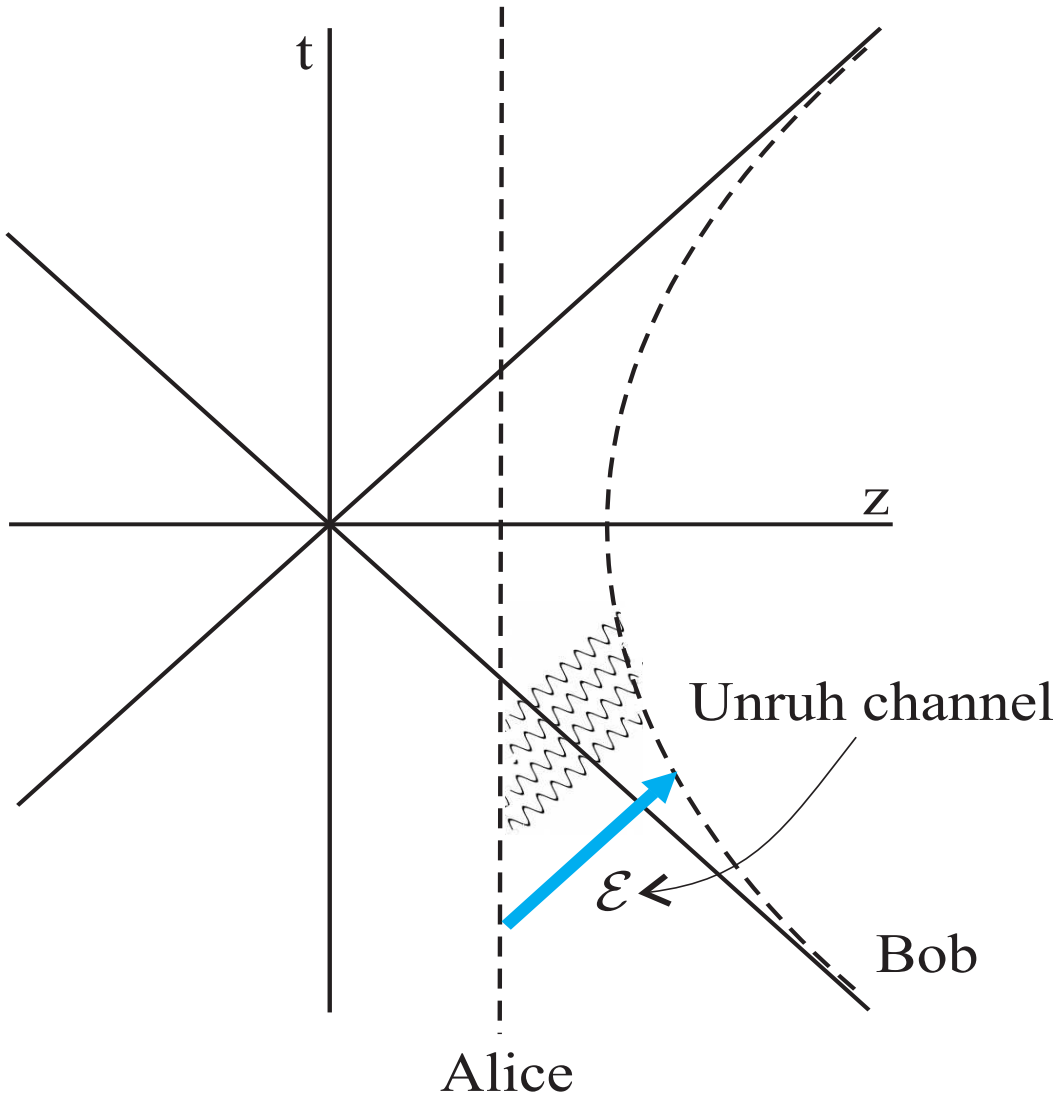
The notion of "particle" is not absoute:

it only refers to the effects of a detector interacting with a field.

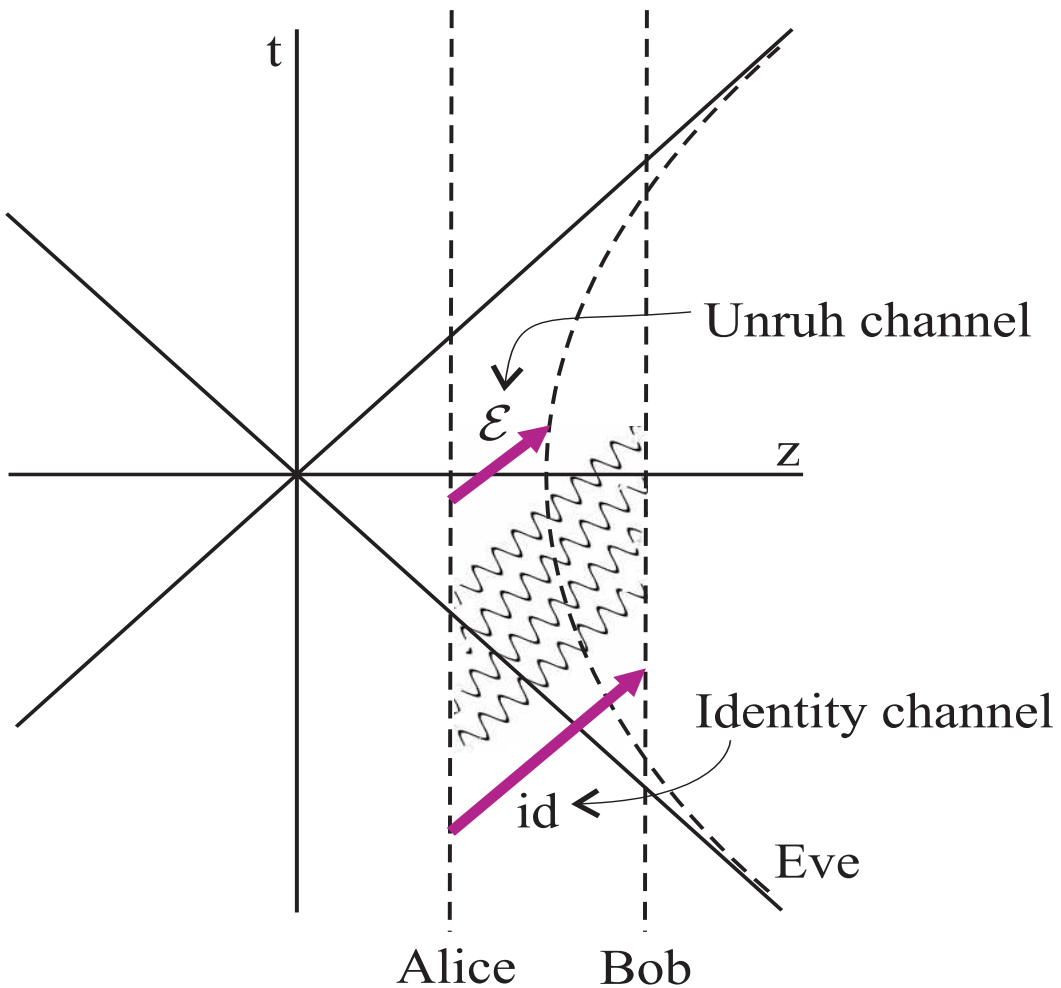
Scenarios for Communication

- We consider the effect of the thermal noise on communication in two scenarios.
- Alice (inertial) sends messages to Bob (accelerating); what is the channel capacity?
- Alice sends messages to Bob (both inertial) but Eve (accelerating) eavesdrops. How well can she wiretap given the noise that she detects?

Scenario 1



Scenario 2


t
z
Unruh channel
$\mathcal{E}$
Identity channel
id
Eve
Alice
Bob

Surprises

1. The quantum capacity, i.e. the optimal rate at which a sender can transmit qubits through a noisy channel usually exhibits a threshold behaviour. Not so with the Unruh channel: the capacity is always positive and is zero only in the limit of infinite acceleration.

Surprises

2. The private quantum capacity also has no threshold behaviour. Furthermore, it has a *single-letter* formula. This formula shows that the private quantum capacity is *exactly* the same as the entanglement-assisted capacity to the eavesdropper's environment, even though there is *no connection* between these two situations!

We have no idea what this means.

Channel Capacity

- The basic measure of information transmission.
- Shannon's coding theorem: All transmission rates below the capacity are achievable with asymptotically zero probability of error.

Quantum Channels 1

- We want to send quantum data from Alice to Bob.
- Sending classical data: choose a basis to represent classical data and encode classical data in a quantum state. Bob has to extract the classical data from the quantum state.
- Sending quantum data: Alice wants to send the whole quantum state.

Quantum Channels 2

- New possibility: If Alice uses multiple copies of the channel she could entangle the quantum states across multiple uses of the channel.
- We do not know how to compute the capacity in this case!

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$$

One for each use of the channel

$C^{(1)}(\mathcal{E})$ the one-shot capacity

In this case we have the Holevo-Schumacher-Westmoreland theorem, which gives us a "formula" for the capacity.

Background on quantum information theory

Quantum channel: completely positive, trace-preserving linear map.

Trace norm: $||X||_1 \stackrel{\text{def}}{=} \text{Tr}\sqrt{X^\dagger X}$.

Trace distance: $\frac{1}{2}||\rho - \rho'||_1$, where ρ, ρ' are density matrices.

Fidelity: $F(\rho, \rho') = ||\sqrt{\rho}\sqrt{\rho'}||_1^2$.

von Neumann entropy: $-\mathrm{Tr}\rho\log_2\rho$

If ρ_{AB} is a density matrix defined on $\mathcal{H}_A\otimes\mathcal{H}_B$ we write ρ_A for $\mathrm{Tr}_B\rho_{AB}$ and $H(A)_\rho$ for the vN-entropy of ρ_A.

Mutual information:
$I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho.$

Conditional entropy:
$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho.$

Coherent information:
$I(A\rangle B)_\rho = H(B)_\rho - H(AB)_\rho = -H(A|B)_\rho.$

Quantum capacity

Idea: Want to transmit qubits along a noisy channel reliably (i.e. preserving the state) and preserving *pre-existing entanglement*.

Use error-correcting codes to counteract the noise and send it across the channel where it is decoded.

Define a *rate* in terms of the limit of many uses of the channel and small error.
The capacity is the optimal achievable rate.

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Holevo χ quantity

If $\rho = \sum_i p_i \rho_i$ then define

$$\chi(\rho) = H(\rho) - \sum_i p_i H(\rho_i)$$

Holevo bound: χ is an upper bound on accessible information in ρ.

The Holevo-Schumacher-Westmoreland Theorem

$$C^{(1)}(\mathcal{E}) = \max_{(p_j,\rho_j)} [H(\mathcal{E}(\sum_j p_j \rho_j) - \sum_j p_j H(\mathcal{E}(\rho_j))]$$

ρ_j are the possible input states.

Pure state ensembles suffice.

C

$\left|\Phi_{2^k}\right\rangle = 2^{-k/2} \sum_{j=1}^{2^\kappa} \left|k\right\rangle \left|k\right\rangle$ will denote the maximally entangled state on k

pairs of qubits.

Definition 1. *An* (n, k, δ) entanglement transmission code *from Alice to Bob consists of an encoding channel* $\mathcal{A}$ *taking a* k*-qubit system* R' *into the input of* $\mathcal{N}^{\otimes n}$ *and a decoding channel* $\mathcal{B}$ *taking the output of* $\mathcal{N}^{\otimes n}$ *to a* k*-qubit system* $C \cong R'$ *satisfying*

$$\left\| (\mathrm{id} \otimes \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \Phi_{2^k} \right\|_1 \leq \delta. \tag{2}$$

A rate Q *is an* achievable rate *for entanglement transmission if for all* $\delta > 0$ *and sufficiently large* n *there exist* $(n, \lfloor nQ \rfloor, \delta)$ *entanglement transmission codes. The* quantum capacity $Q(\mathcal{N})$ *is the supremum of all the achievable rates.*

Unknown how to compute a one-shot formula for this.

Regularization

Quantum informatic quantities are usually computed by:

allowing n uses of the channel and computing

$$\lim_{n \to \infty} \frac{1}{n} Q(n)$$

where Q is the quantity of interest.

1. Easier to compute
2. Essentially using the law of large numbers to get better behaviour

Single-letter formulas

In classical information theory Shannon gave a formula for capacity that is calculated by considering only a single use of the channel.

To get a similar formula in quantum information theory is still an open question!

Recently Max Hastings disproved the additivity conjecture which dashed hopes that the existing approaches for finding such a formula would work.

Additivity Conjecture

$$\chi(\Phi^{\otimes n}) = n\,\chi(\Phi)$$

This would clearly make regularization unnecessary.

More generally, $\chi(\Phi \otimes \Omega) = \chi(\Phi) + \chi(\Omega)$

In terms of minimum output entropy:

$$S_{\min}(\Phi) = \inf_{\rho} S(\Phi(\ \ ))$$

or Renyi variant: $S_{p,\min}(\Phi) = \inf_{\rho} \frac{1}{1-p} \log \mathrm{Tr}\,(\Phi(\rho)^p)$

$$S_{p,\min}(\Phi \otimes \Omega) = S_{p,\min}(\Phi) + S_{p,\min}(\Omega)$$

The best general result

Theorem 2 (Lloyd-Shor-Devetak [33, 40, 18]). *Let* $|\psi\rangle_{A'A}$ *be a pure state,* $\mathcal{N}$ *a quantum channel from* A *to* B *and define* $\rho = (\mathrm{id}_{A'} \otimes \mathcal{N})(\psi)$. *The quantum capacity* $Q(\mathcal{N})$ *of* $\mathcal{N}$ *is at least* $I(A'\rangle B)$.

We can give an explicit single-letter formula for the quantum capacity of the Unruh channel.

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

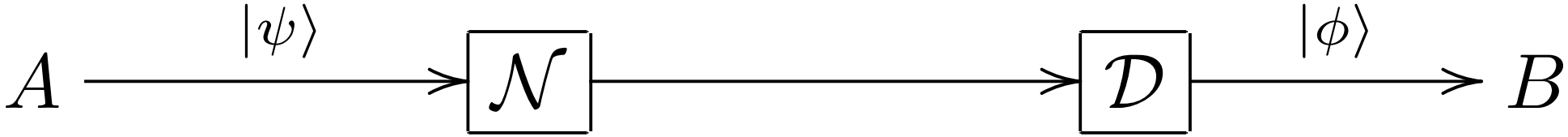
What is the capacity for sending *private* data?

Purely classical: Maurer (1994) and Ahlswede & Csiszar (1993)

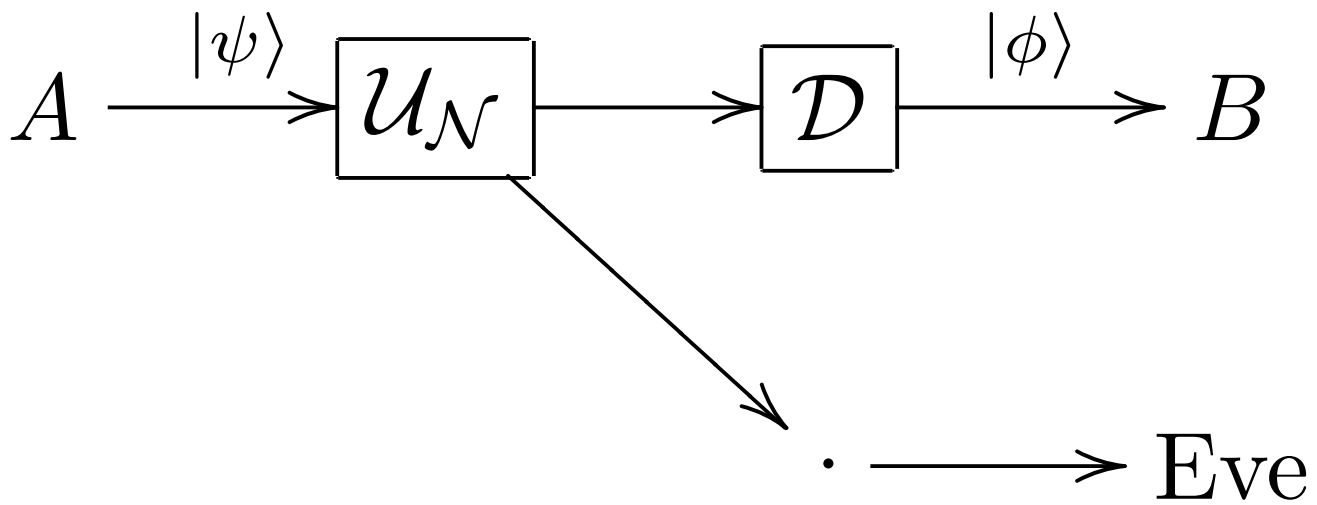
What is the private capacity of a quantum channel for communicating classical data? [Devetak 2005]

What is the private capacity of a quantum channel for communicating quantum data? [Hayden et al. in progress]

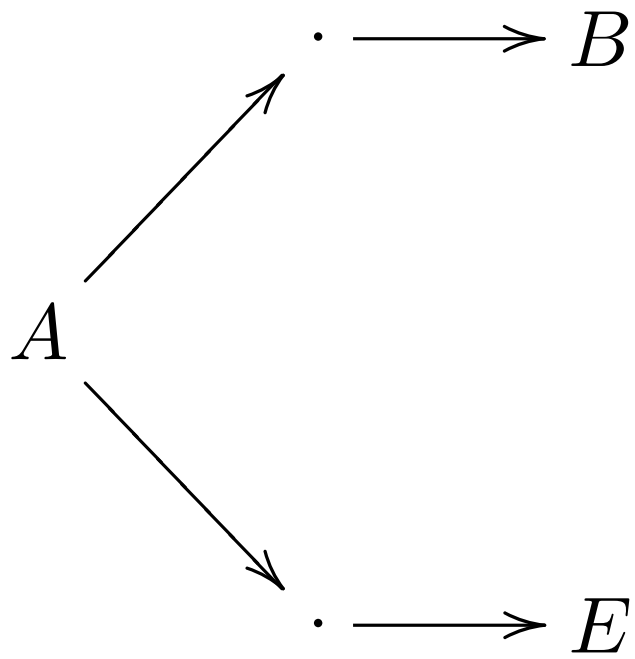
Private Quantum Communication



Noisy channel Decoder



Eve cannot get a copy of ϕ: automatic privacy.

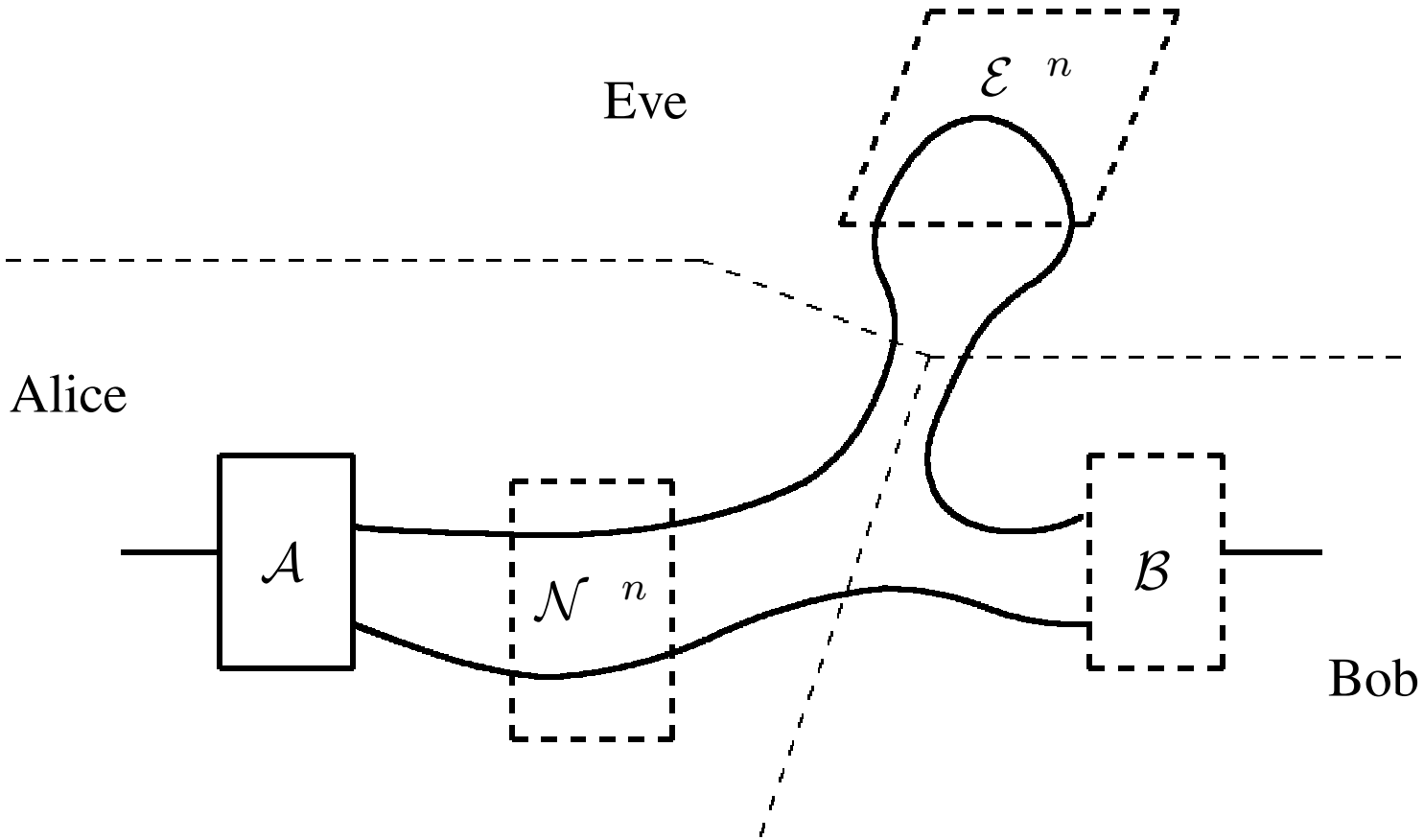


Quantum state is a density matrix on $B \otimes E$
Alice wants to send a message to Bob
so that with high probability Bob can decode it
and Eve is very unlikely to be able to decode it.

An (n, ϵ) private channel code
of rate R allows Alice to send one of 2^{nR}
messages,Bob can decode with error less than ϵ
and Eve cannot find out more than ϵ bits.

Wiretap Channels

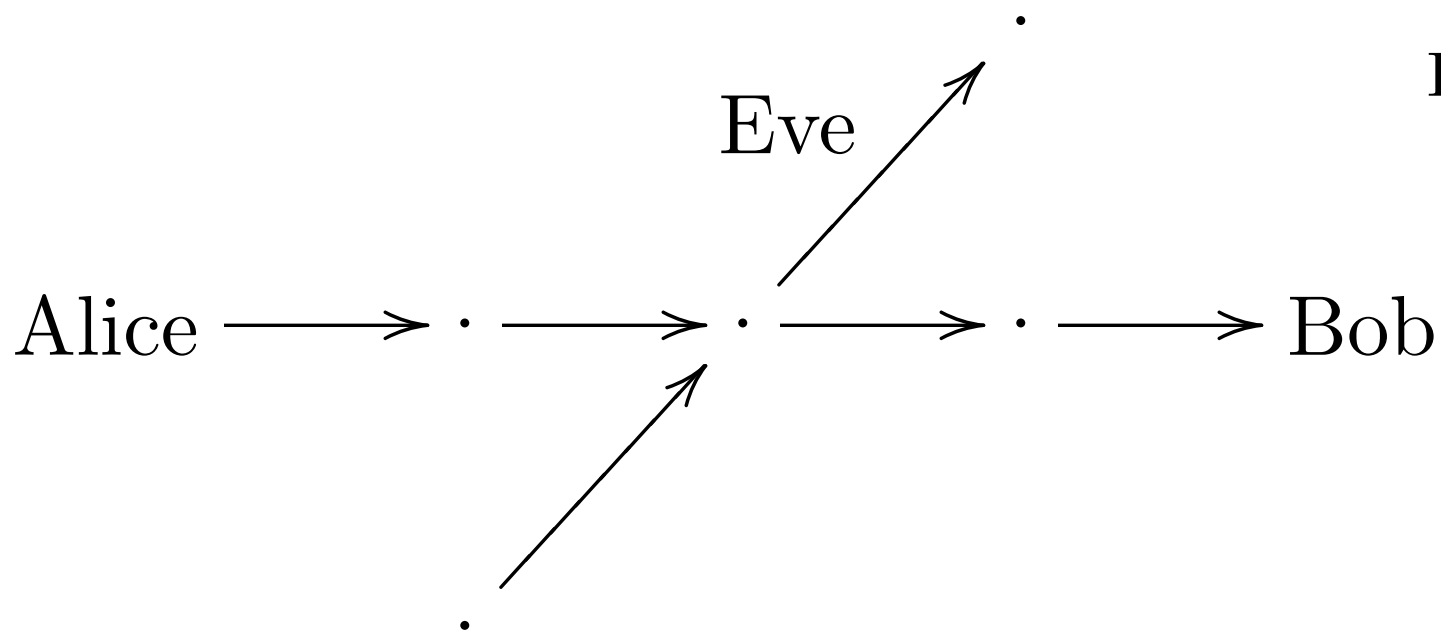
Definition 3. *A* quantum wiretap channel *consists of a pair of quantum channels* $(\mathcal{N}_{A\to B}, \mathcal{E}_{A\to E})$ *taking the density operators on* A *to those on* B *and* E*, respectively.*



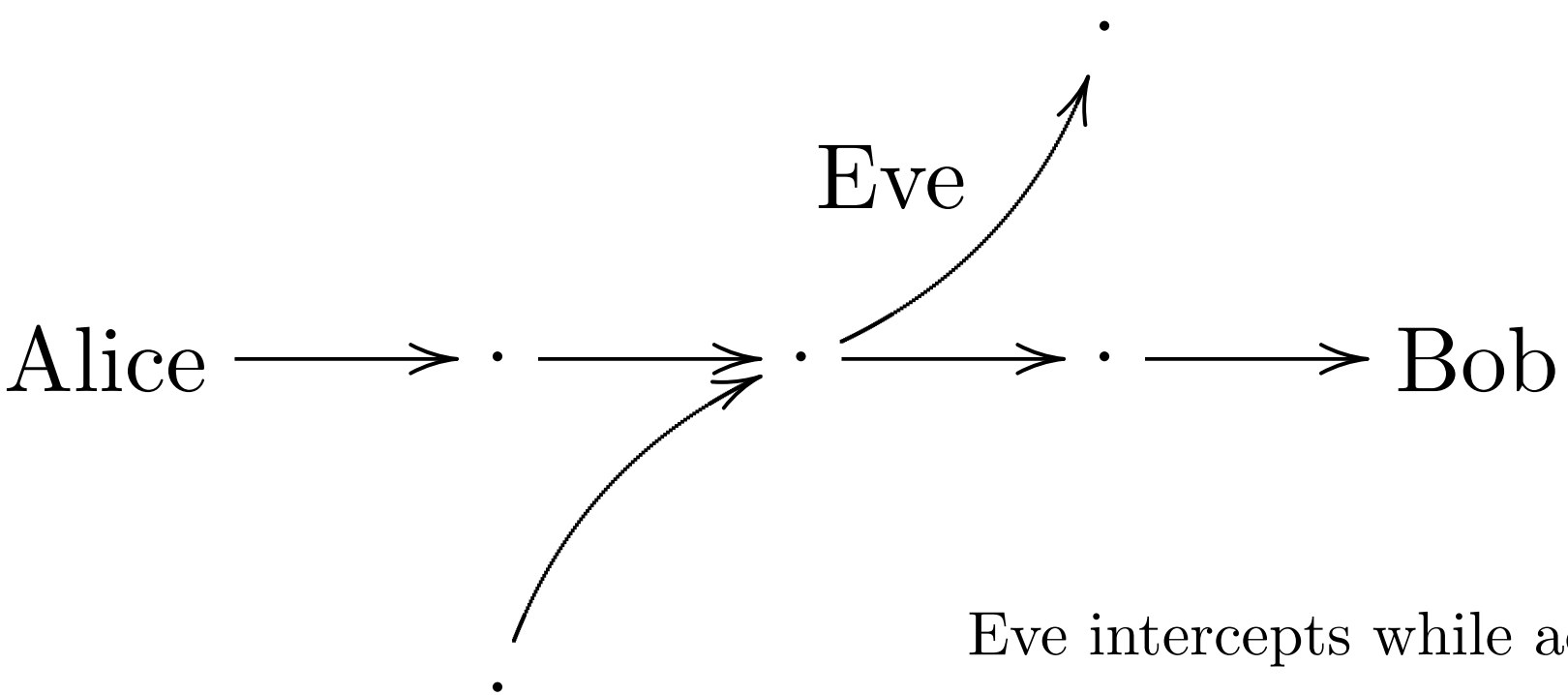
Wiretap channels apply to the Unruh scenario but also to many other situations.

Our Setting Today

- Quantum communication: Alice sending quantum data to Bob, and Eve intercepts.
- However, Eve is accelerating so gets Unruh noise.
- What is the private capacity for Alice to Bob? Can we use the Unruh noise?



Eve intercepts.



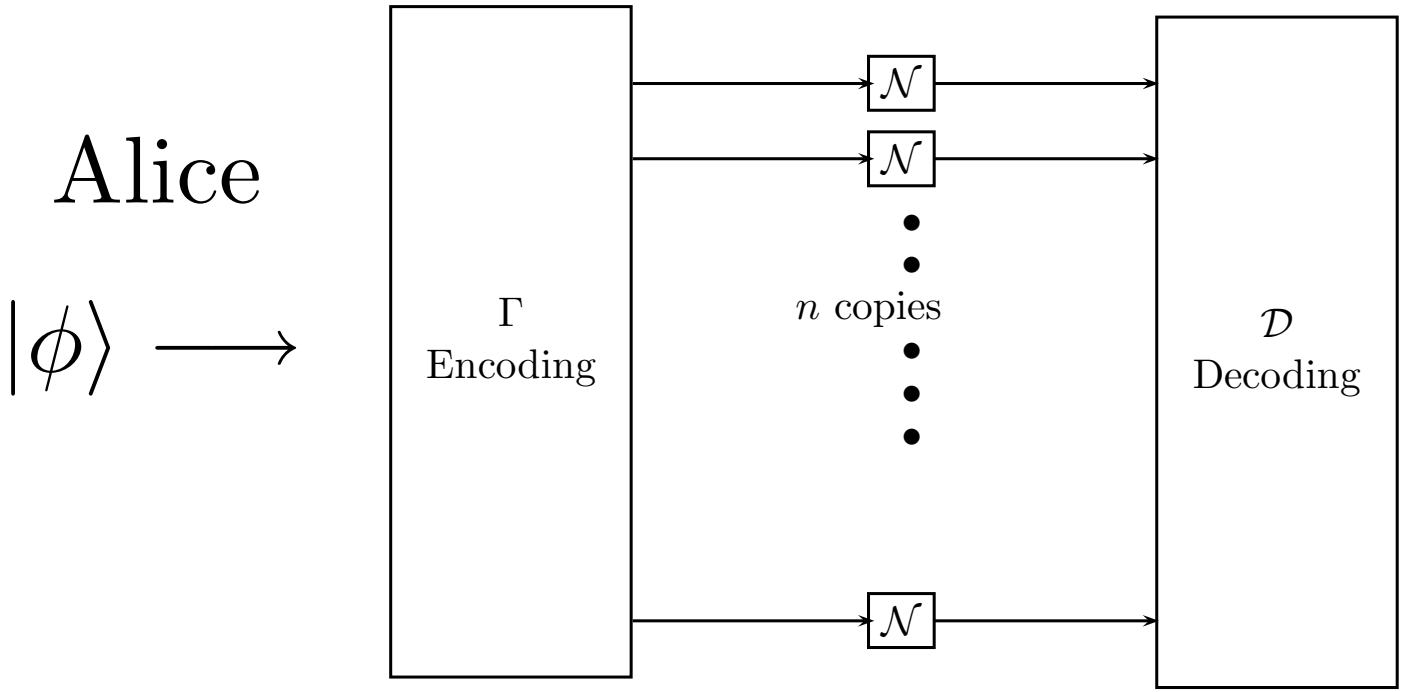
Eve intercepts while accelerating.

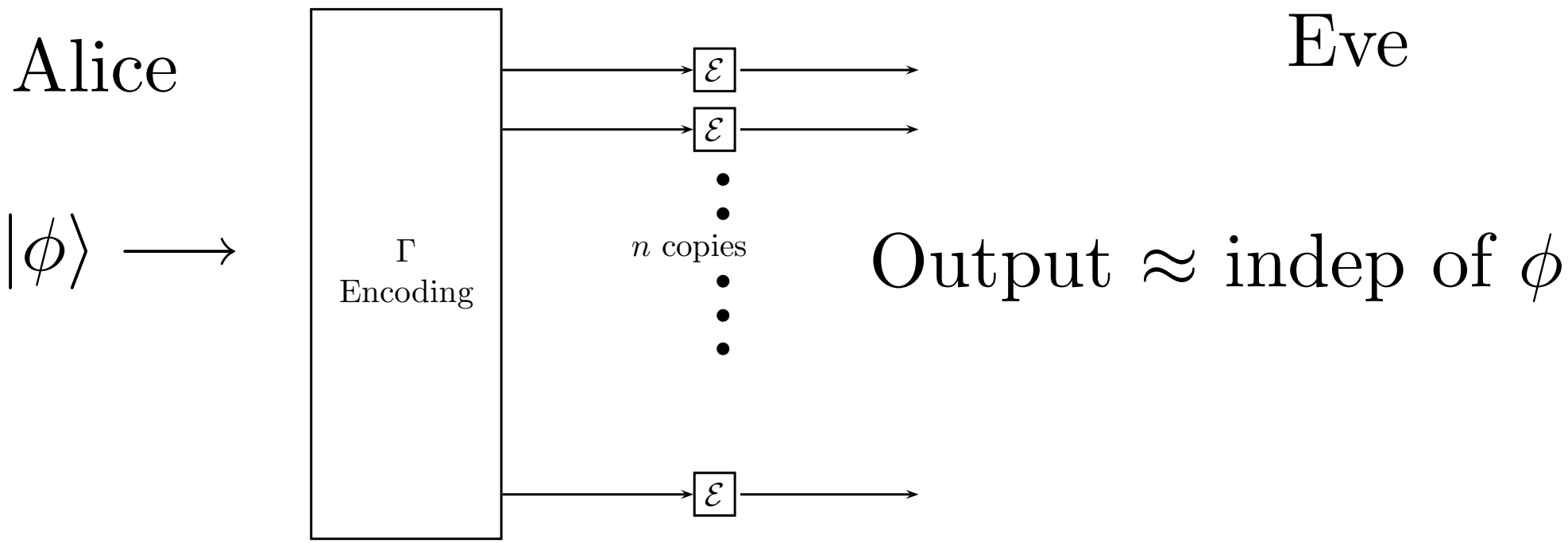
$$\text{Alice} \longrightarrow \mathcal{N} \longrightarrow \text{Bob}$$

$$\text{Alice} \longrightarrow \mathcal{E} \longrightarrow \text{Eve}$$

Eve is not a "part" of the environment $[Eve \not\subseteq Env]$

Does the Unruh effect give a channel from Alice to Bob with nonzero quantum and classical private capacity?


Alice
$|\phi\rangle$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding
Bob
$|\tilde{\phi}\rangle$
$|\phi\rangle \approx |\tilde{\phi}\rangle$


Alice
$|\phi\rangle$
Γ
Encoding
$\mathcal{E}$
$\mathcal{E}$
n copies
$\mathcal{E}$
Eve
Output ≈ indep of ϕ

Definition 4. *An* (n, k, δ, ϵ) private entanglement transmission code *from Alice to Bob consists of an encoding channel* $\mathcal{A}$ *taking a* k*-qubit system* R' *into the input of* $\mathcal{N}^{\otimes n}$ *and a decoding channel* $\mathcal{B}$ *taking the output of* $\mathcal{N}^{\otimes n}$ *to a* k*-qubit system* $C \cong R'$ *satisfying*

1. *Transmission:* $\|(\mathrm{id} \otimes \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \Phi_{2^k}\|_1 \leq \delta$.
2. *Privacy:* $\|(\mathrm{id} \otimes \mathcal{E}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \pi_{2^k} \otimes (\mathcal{E}^{\otimes n} \circ \mathcal{A})(\pi_{2^k})\|_1 \leq \epsilon$.

$\pi_{2^k} = \mathbb{I}/2^k$ the maximally mixed state on k qubits.

A rate Q *is an* achievable rate *for private entanglement transmission if for all* $\delta, \epsilon > 0$ *and sufficiently large* n *there exist* $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ *private entanglement transmission codes. The* private quantum capacity $Q_p(\mathsf{N}, \mathsf{E})$ *is the supremum of all the achievable rates.*

The main result

Theorem 5 (Private quantum capacity)**.** *The private quantum capacity* $Q_p(\mathrm{id}, \mathsf{E})$ *when the channel from Alice to Bob is noiseless is given by the formula* $\max \frac{1}{2} I(A\,;E_c)_\rho$*, where the maximization is over all pure states* $\left|\psi\right\rangle_{A'A}$ *and* $\rho = (\mathrm{id} \otimes \mathsf{E}_c)(\psi)$.

If we can get the output in a simple enough form we can hope to get a single-letter formula for the private capacity.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

A Bogolioubov transformation will change the modes to Eve's Fock space.

$$U_{abcd}(r) = U_{ac}(r) \otimes U_{bd}(r) = e^{r(a^\dagger c^\dagger + b^\dagger d^\dagger) - r(ac+bd)}$$
$$= \frac{1}{\cosh^2 r} e^{\tanh r(a^\dagger c^\dagger + b^\dagger d^\dagger)}$$
$$\times e^{-\ln\cosh r(a^\dagger a + b^\dagger b + c^\dagger c + d^\dagger d)} e^{-\tanh r(ac+bd)}.$$

The output density matrix is infinite dimensional and block diagonal.

The only hope: deal with it block by block.

The output of the Unruh channel
for an input qudit is:

$$|\sigma\rangle_{AC} = \frac{1}{\cosh^{d+1} r} \sum_{k=1}^{\infty} \tanh^{k-1} r \sum_{I} \left[\sum_{i=1}^{d} \beta_i \sqrt{l_{I,i} + 1}\, |I^{(i)}\rangle_A |I\rangle_C \right]$$

Note: ∞ dimensional and block diagonal.

Group theory to the rescue:
the blocks of the output density matrix
live in completely symmetric subspaces
because we are creating bosons.

In fact the Unruh channel "behaves well"
with respect to the Lie algebra $\mathsf{sl}(d, \mathbb{C})$,
the Lie algebra of $SU(d)$.

Physicists' approach:
guess the answer, then check!

Theorem 12. *Let the first block of σ_A in Eq. (51) be written as*

$$\sigma_A^{(1)} = \mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(1)}, \tag{53}$$

where $\lambda_\alpha^{(1)}$ are generators of the fundamental representation of the $\mathsf{sl}(d,\mathbb{C})$ algebra, $L = \frac{3d}{2}(d-1)$ and n_α are functions of $\beta_i\bar{\beta}_j$. Then the remaining blocks in Eq. (51) can be expanded with the same coefficients n_α

$$\sigma_A^{(k)} = \mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(k)}, \tag{54}$$

where $\lambda_\alpha^{(k)}$ are generators of the k^{th} completely symmetric representation of the $\mathsf{sl}(d,\mathbb{C})$ algebra. The blocks $\sigma_A^{(k)}$ are in general not normalized.

What "well behaved" means.

Definition 16. *Let* G *be a group,* $\mathcal{H}_{in}, \mathcal{H}_{out}$ *be Hilbert spaces and let* $\mathsf{r}_1 : \mathsf{G} \to \mathsf{GL}(\mathcal{H}_{in}), \mathsf{r}_2 : \mathsf{G} \to \mathsf{GL}(\mathcal{H}_{out})$ *be unitary representations of the group. Let* $\mathcal{K} : \mathcal{DM}(\mathcal{H}_{in}) \to \mathcal{DM}(\mathcal{H}_{out})$ *be a channel. We say that* $\mathcal{K}$ *is* ***covariant with respect to*** G*, if*

$$\mathcal{K}\left(\mathsf{r}_1(\mathsf{g})\rho\mathsf{r}_1(\mathsf{g})^\dagger\right) = \mathsf{r}_2(\mathsf{g})\mathcal{K}(\rho)\mathsf{r}_2(\mathsf{g})^\dagger \tag{66}$$

holds for all $\mathsf{g} \in \mathsf{G}, \rho \in \mathcal{DM}(\mathcal{H}_{in})$.

Covariance signifies that certain equations that hold in a representation, hold for "Lie algebraic reasons" and not because of some special property of the representation. Thus we can diagonalize *all the blocks* at the same time.

Theorem 12 implies that:

The qudit Unruh channel is $SU(d)$-covariant.

In addition, the Unruh channel has a property called *conjugate degradability*

If a channel is covariant and conjugate degradable then the maximization in the formula for the channel capacity is achieved for a maximally mixed input state.

We can explicitly calculate this and obtain an explicit expression for the channel capacity and for the private quantum capacity.

Stinespring dilation:
Every cptp map
$\mathcal{N} : DM(A) \to DM(B)$
can be written as

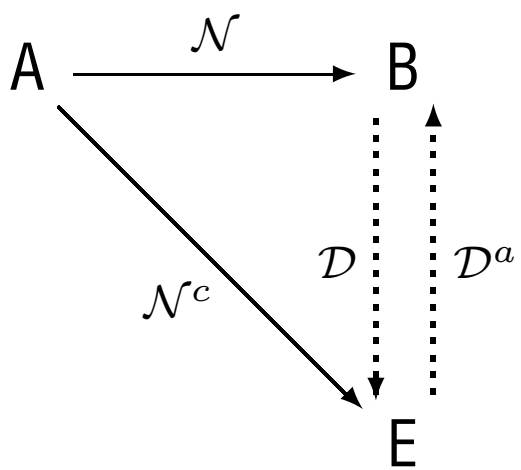
$\mathcal{N}(\varrho) = \mathrm{Tr}_E(U \varrho U^\dagger)$ where

$U : A \to B \otimes E$ is unitary.

We call E the environment.

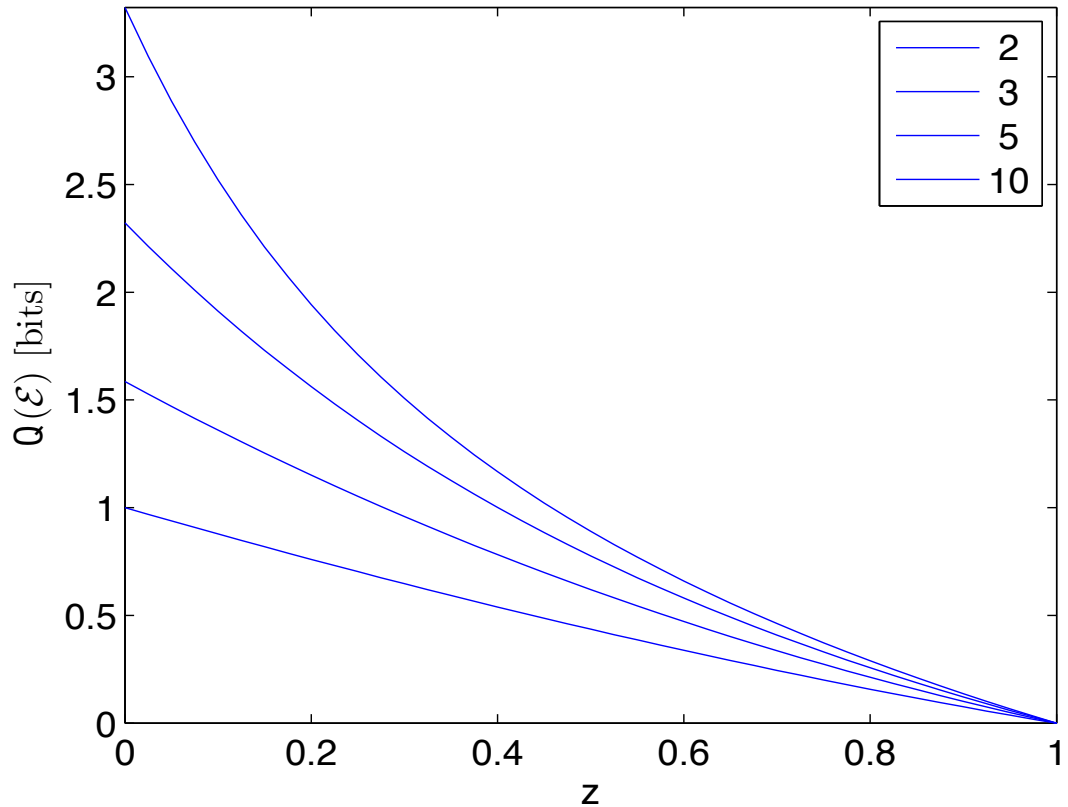
$\mathcal{N}^c$ is the *complementary* channel.

$\mathcal{N}$ is *degradable* if there exists a cptp map $\mathcal{D}$ such that:

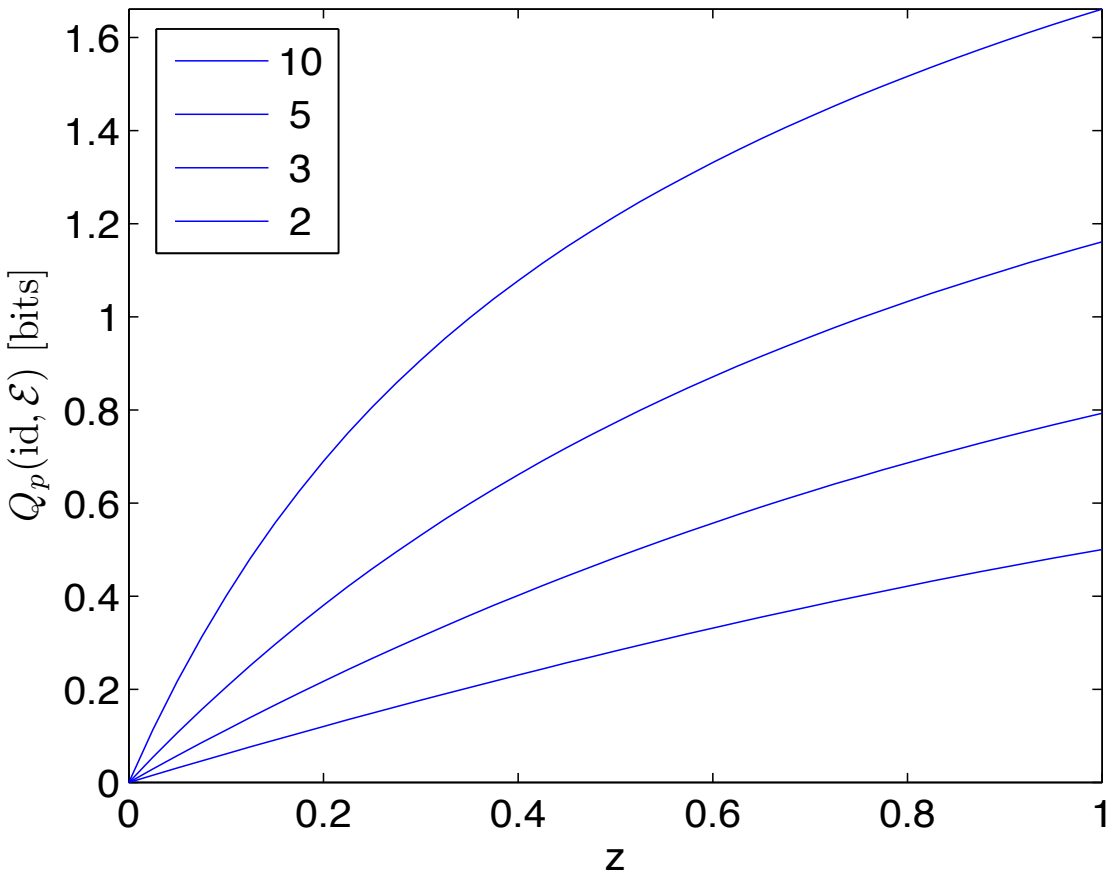


Conjugate degradable means that we get to throw in a complex conjugation map $\mathcal{C}$

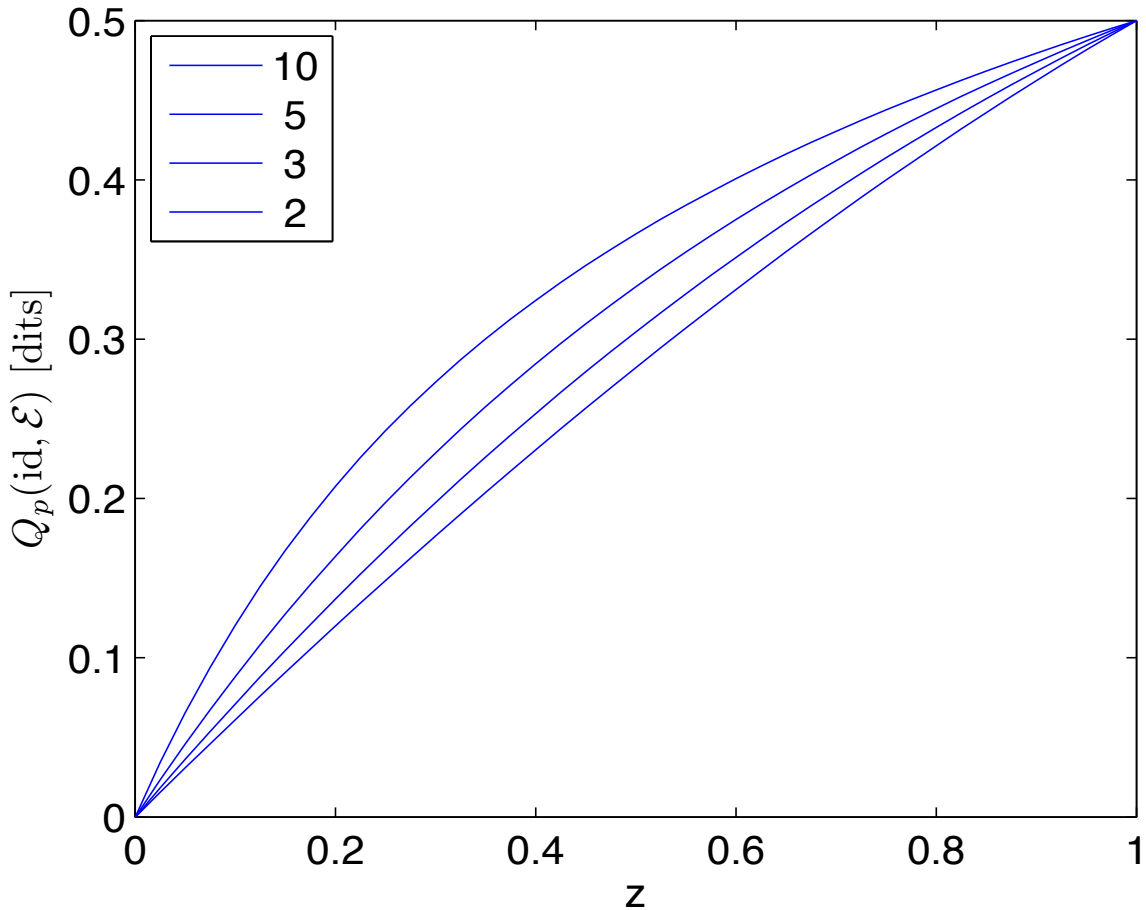
$$\mathcal{D} \circ \mathcal{N} = \mathcal{C} \circ \mathcal{N}^c.$$



Capacity for various values of d (the dimensionality of the encoding space - qudits). The $d = 2$ case corresponds to the lowest curve. The x axis gives the acceleration.



The private quantum capacity for various values of d.
The $d = 2$ case corresponds to the lowest curve.
The x axis gives the acceleration.



The private quantum capacity for various values of d. Here we are showing the results in dits.

Conclusions

Surprises: absence of threshold behaviour and strange coincidence between the explicit formu for the private quantum capacity and the entanglement-assisted capacity.

How are these modified if we consider acceleration for a finite time only?

What next?

Can an accelerating observer prepare a pure state? How will she cancel out Unruh noise?

Communication capacity in curved spacetime? Information as a probe of geometry??

Black holes seem to be optimal cloners! Why??