Title: Entanglement Transmission over Arbitrarily Varying Quantum Channels

Date: Oct 03, 2011 04:00 PM

URL: http://pirsa.org/11100073

Abstract: The model of an arbitrarily varying quantum channel will be introduced in strict analogy to the classical definition by Blackwell, Breiman and Thomasian. We will then consider the task of entanglement transmission over such a channel and take a look at the methods, both from classical and quantum information theory, that enter the direct part of our proof of a quantum version of Ahlswede's dichotomy for the capacity of classical arbitrarily varying channels. Differences to the classical setting will be pointed out.

Entanglement Transmission over Arbitrarily Varying Quantum Channels

R. Ahlswede[1], I. Bjelaković[2], H. Boche[2], J. Nötzel[2]

[1]Universität Bielefeld,
Arbeitsgruppe Information und Komplexität

[2]Technische Universität München,
Lehrstuhl für Theoretische Informationstechnik

Perimeter Institute
for Theoretical Physics
October 3, 2011

Entanglement Fidelity

- Sender $\mathcal{S}$ has a pure entangled state $|\psi\rangle\langle\psi| \in \mathcal{S}(\mathcal{F} \otimes \mathcal{F})$.
- He wishes to transmit one half of it to receiver $\mathcal{R}$ by use of the channel $\mathcal{N} \in CPTPM(\mathcal{H}, \mathcal{K})$.
- $\mathcal{S}$ uses the encoding map $\mathcal{P} \in CPTPM(\mathcal{F}, \mathcal{H})$
- and $\mathcal{R}$ the recovery map $\mathcal{R} \in CPTPM(\mathcal{K}, \mathcal{F})$.
- Measure of success:

$$\langle\psi, Id \otimes \mathcal{R} \circ \mathcal{N} \circ \mathcal{P}(|\psi\rangle\langle\psi|)\psi\rangle =: F_e(\rho, \mathcal{R} \circ \mathcal{N} \circ \mathcal{P}) \in [0,1],$$

where $\rho := Id_{\mathcal{F}} \otimes \mathrm{tr}_{\mathcal{F}}(|\psi\rangle\langle\psi|)$ (the marginal state).

Maximally Mixed / Maximally Entangled

- We are interested in the transmission of maximally entangled states $|\psi_+\rangle\langle\psi_+| \in \mathcal{S}(\mathcal{F} \otimes \mathcal{F})$,
- where (w.l.o.g.) for some o.n.b. $\{e_i\}_{i=1}^{\dim(\mathcal{F})}$ of $\mathcal{F}$,

$$\psi_+ = \frac{1}{\sqrt{\dim(\mathcal{F})}} \sum_{i=1}^{\dim(\mathcal{F})} e_i \otimes e_i .$$

- These states correspond to maximally mixed states

$$\pi_{\mathcal{F}} := \frac{1}{dim\mathcal{F}} \mathbf{1}_{\mathcal{F}} = \mathrm{tr}_{\mathcal{F}}\{|\psi_+\rangle\langle\psi_+|\} \in \mathcal{S}(\mathcal{F}).$$

Motivation

We are given a (finite) set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ of CPTP maps with input Hilbert space $\mathcal{H}$ and output Hilbert space $\mathcal{K}$. For all $m \in \mathbb{N}$,

- the sender controls the input Hilbert spaces $\mathcal{H}^{\otimes m}$,
- the receiver has access to the output Hilbert spaces $\mathcal{K}^{\otimes m}$,
- the adversary is free to choose a sequence $s^m = (s_1, \ldots, s_m) \in \mathbf{S}^m$ and provides the channel

  $$\mathcal{N}_{s^m} := \mathcal{N}_{s_1} \otimes \ldots \otimes \mathcal{N}_{s_m}$$

  for the transmission of entanglement.
- Neither sender nor receiver know the sequence $s^m \in \mathbf{S}^m$.

Goal: Find encoding/decoding schemes that are reliable for the whole family of non-stationary, memoryless quantum channels

$$\{\mathcal{N}_{s^m}\}_{s^m\in\mathbf{S}^m, m\in\mathbb{N}},$$

which we call arbitrarily varying quantum channel (AVQC).

$|\psi\rangle$
$\in \mathcal{H}^{\otimes 4} \otimes \mathcal{H}^{\otimes 4}$
AVQC $\mathfrak{J} = \{\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3\}$

$$\mathcal{N}_1 \otimes \mathcal{N}_3 \otimes \mathcal{N}_1 \otimes \mathcal{N}_3$$

or...

$$\mathcal{N}_2 \otimes \mathcal{N}_1 \otimes \mathcal{N}_3 \otimes \mathcal{N}_2$$

???

$\in \mathcal{H}^{\otimes 4} \otimes \mathcal{H}^{\otimes 4}$

???

AVQC $\mathfrak{J} = \{\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3\}$

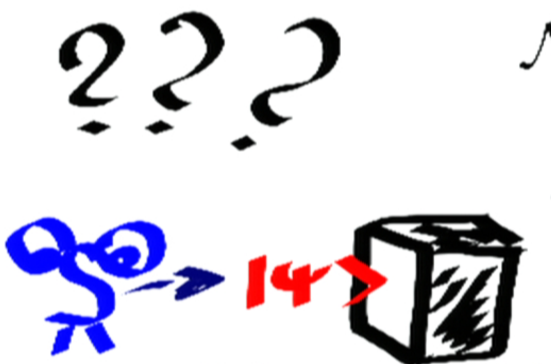
$$\mathcal{N}_1 \otimes \mathcal{N}_3 \otimes \mathcal{N}_1 \otimes \mathcal{N}_3$$

or...

$$\mathcal{N}_2 \otimes \mathcal{N}_1 \otimes \mathcal{N}_3 \otimes \mathcal{N}_2$$

or...

$$\mathcal{N}_2 \otimes \mathcal{N}_2 \otimes \mathcal{N}_2 \otimes \mathcal{N}_2$$



$\in \mathcal{H}^{\otimes 4} \otimes \mathcal{H}^{\otimes 4}$

AVQC $\mathfrak{J} = \{\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3\}$

Codes and Capacity for AVQC

- A random (m, k_m)-code for the finite AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ is a probability measure μ_m on $(CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m), \Sigma_m)$, where Σ_m is any σ-algebra on $CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m)$ containing all singleton sets and

$$k_m = \dim \mathcal{F}_m.$$

- $R \in \mathbb{R}_+$ is a randomly achievable rate for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ if there is a sequence of random (m, k_m)-codes with
  - $\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R$,
  - $\lim_{m\to\infty} \inf_{s^m\in\mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1.$
- The random entanglement transmission capacity $\mathcal{A}_{\mathrm{random}}(\mathfrak{I})$ of $\mathfrak{I}$ is defined by

$$\mathcal{A}_{\mathrm{random}}(\mathfrak{I}) := \sup\{R \in \mathbb{R}_+ : R \text{ is randomly achievable rate}\}.$$

Codes and Capacity for AVQC

- A deterministic (m, k_m)-code for the finite AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ is a probability measure μ_m on $(CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m), \Sigma_m)$, where Σ_m is any σ-algebra on $CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}_m)$ containing all singleton sets and

$$k_m = \dim \mathcal{F}_m, \quad \exists\ (\mathcal{P}^m, \mathcal{R}^m) \text{ s.t. } \mu_m(\{(\mathcal{P}^m, \mathcal{R}^m)\}) = 1.$$

- $R \in \mathbb{R}_+$ is a deterministically achievable rate for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ if there is a sequence of deterministic (m, k_m)-codes with
  - $\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R$,
  - $\lim_{m\to\infty} \inf_{s^m\in\mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1.$
- The deterministic entanglement transmission capacity $\mathcal{A}_{\text{det}}(\mathfrak{I})$ of $\mathfrak{I}$ is defined by

$$\mathcal{A}_{\text{det}}(\mathfrak{I}) := \sup\{R \in \mathbb{R}_+ : R \text{ is a deterministically achievable rate}\}.$$

Quantum Ahlswede Dichotomy

For a finite set of CPTP maps $\mathfrak{I} = \{\mathcal{N}_s\}_{s \in \mathbf{S}}$ we define $conv(\mathfrak{I})$ to be its convex hull:

$$conv(\mathfrak{I}) := \left\{ \mathcal{N}_{\mathfrak{q}} \in CPTPM(\mathcal{H}, \mathcal{K}) : \mathcal{N}_{\mathfrak{q}} = \sum_{s \in \mathbf{S}} \mathfrak{q}(s) \mathcal{N}_s, \ \mathfrak{q} \in \mathfrak{P}(\mathbf{S}) \right\}.$$

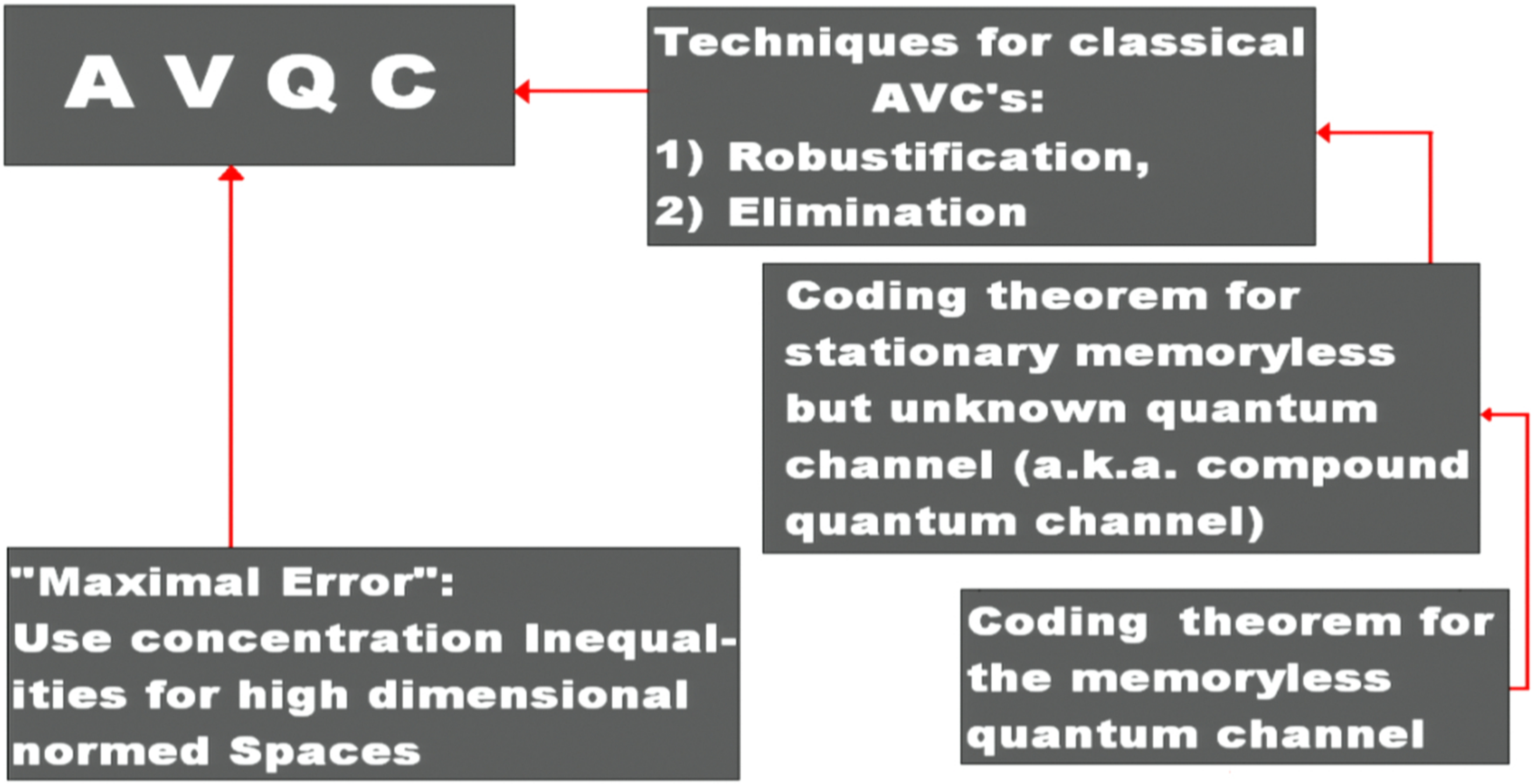
Our main result, a quantum mechanical version of Ahlswede's dichotomy for finite AVQCs, can be formulated as follows:

Theorem (Quantum Ahlswede Dichotomy)

Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s \in \mathbf{S}}$ be a finite AVQC. Then

$$\mathcal{A}_{\mathrm{random}}(\mathfrak{I}) = \lim_{m \to \infty} \frac{1}{m} \max_{\rho \in \mathcal{S}(\mathcal{H}^{\otimes m})} \inf_{\mathcal{N} \in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes m})$$

Either $\mathcal{A}_{\mathrm{det}}(\mathfrak{I}) = 0$ *or else* $\mathcal{A}_{\mathrm{det}}(\mathfrak{I}) = \mathcal{A}_{\mathrm{random}}(\mathfrak{I})$.


A V Q C
Techniques for classical AVC's:
1) Robustification,
2) Elimination
Coding theorem for stationary memoryless but unknown quantum channel (a.k.a. compound quantum channel)
Coding theorem for the memoryless quantum channel
"Maximal Error":
Use concentration Inequal-ities for high dimensional normed Spaces

Achievability 1: Ahlswede's Robustification Technique

We want to show the existence of good random codes for the AVQC $\mathfrak{I}$ or, equivalently,

$$\mathcal{A}_{\text{random}}(\mathfrak{I}) \geq \lim_{m\to\infty} \frac{1}{m} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes m})} \inf_{\mathcal{N}\in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes m}). \qquad (1)$$

- In order to do this we use a classic way to convert *compound* codes for $conv(\mathfrak{I})$ into random codes for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ which relies on Ahlswede's robustification technique.
- $\Rightarrow$ R. Ahlswede, Coloring Hypergraphs II, Journal of Combinatorics, Information & System Sciences Vol. 5, 220-268, 1980

Theorem (Ahlswede's robustification technique)

If a function $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0,1]$ *which is invariant under the action of* Perm_m *satisfies*

$$\sum_{s^m \in \mathbf{S}^m} f(p^*, s^m)\mathrm{q}(s_1) \cdot \ldots \cdot \mathrm{q}(s_m) \geq 1 - \gamma \tag{2}$$

for some $p^* \in \mathrm{Perm}_m$, *all* $\mathrm{q} \in T(m, \mathbf{S})$ *and some* $\gamma \in [0,1]$, *then*

$$\frac{1}{m!} \sum_{p \in \mathrm{Perm}_m} f(p, s^m) \geq 1 - 3\sqrt{\gamma}(m+1)^{|\mathbf{S}|} \qquad \forall s^m \in \mathbf{S}^m. \tag{3}$$

- Perm_m = set of permutations on $\{1, \ldots, m\}$.
- $T(m, \mathbf{S})$ =set of empirical distributions on $\mathbf{S}$ generated by $\mathbf{S}^m$.
- Invariance of f means that

$$f(p \circ p', p(s^m)) = f(p', s^m),$$

for all $p, p' \in \mathrm{Perm}_m$ and $s^m \in \mathbf{S}^m$.

Theorem (Ahlswede's robustification technique)

If a function $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0,1]$ *which is invariant under the action of* Perm_m *satisfies*

$$\sum_{s^m \in \mathbf{S}^m} f(p^*, s^m) q(s_1) \cdot \ldots \cdot q(s_m) \geq 1 - \gamma \tag{4}$$

for some $p^* \in \mathrm{Perm}_m$*, all* $q \in T(m, \mathbf{S})$ *and some* $\gamma \in [0,1]$*, then*

$$\frac{1}{m!} \sum_{p \in \mathrm{Perm}_m} f(p, s^m) \geq 1 - \gamma (m+1)^{|\mathbf{S}|} \qquad \forall s^m \in \mathbf{S}^m. \tag{5}$$

- Perm_m = set of permutations on $\{1, \ldots, m\}$.
- $T(m, \mathbf{S})$ =set of empirical distributions on $\mathbf{S}$ generated by $\mathbf{S}^m$.
- Invariance of f means that

$$f(p \circ p', p(s^m)) = f(p', s^m),$$

for all $p, p' \in \mathrm{Perm}_m$ and $s^m \in \mathbf{S}^m$.

- Using results of I. Bjelaković, H. Boche, J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Commun. Math. Phys.* 292, 55-97 (2009), we can find to any $\delta > 0$, $k \in \mathbb{N}$ and $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k})$ a sequence of (m, k_m) codes for the compound channel given by $conv(\mathfrak{I})$ such that
  - $$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq \inf_{\mathcal{N}\in conv(\mathfrak{I})} \frac{1}{k} I_c(\rho, \mathcal{N}^{\otimes k}) - \delta, \qquad (6)$$
  - $$\inf_{\mathcal{N}\in conv(\mathfrak{I})} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}^{\otimes m} \circ \mathcal{P}^m) \geq 1 - 2^{-mc}. \qquad (7)$$
- Define $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0,1]$ by

$$f(p, s^m) := F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{U}_{p,\mathcal{K}} \circ \mathcal{N}_{s^m} \circ \mathcal{U}_{p,\mathcal{H}} \circ \mathcal{P}^m),$$

  where $\mathcal{U}_{p,\mathcal{K}} : \mathcal{B}(\mathcal{K})^{\otimes m} \to \mathcal{B}(\mathcal{K})^{\otimes m}$ is the usual action of Perm_m on $\mathcal{B}(\mathcal{K})^{\otimes m}$ as permutations of tensor factors.
- f is invariant under the action of Perm_m.
- For application of the robustifiction technique, choose $p^* = id$

- Using results of I. Bjelaković, H. Boche, J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Commun. Math. Phys.* 292, 55-97 (2009), we can find to any $\delta > 0$, $k \in \mathbb{N}$ and $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k})$ a sequence of (m, k_m) codes for the compound channel given by $conv(\mathfrak{I})$ such that
  - $$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq \inf_{\mathcal{N}\in conv(\mathfrak{I})} \frac{1}{k} I_c(\rho, \mathcal{N}^{\otimes k}) - \delta, \qquad (8)$$
  - $$\inf_{\mathcal{N}\in conv(\mathfrak{I})} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}^{\otimes m} \circ \mathcal{P}^m) \geq 1 - 2^{-mc}. \qquad (9)$$
- Define $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0, 1]$ by

$$f(p, s^m) := F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{U}_{p,\mathcal{K}} \circ \mathcal{N}_{s^m} \circ \mathcal{U}_{p,\mathcal{H}} \circ \mathcal{P}^m),$$

  where $\mathcal{U}_{p,\mathcal{K}} : \mathcal{B}(\mathcal{K})^{\otimes m} \to \mathcal{B}(\mathcal{K})^{\otimes m}$ is the usual action of Perm_m on $\mathcal{B}(\mathcal{K})^{\otimes m}$ as permutations of tensor factors.
- f is invariant under the action of Perm_m.
- For application of the robustifiction technique, choose $p^* = id$

- Using results of I. Bjelaković, H. Boche, J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Commun. Math. Phys.* 292, 55-97 (2009), we can find to any $\delta > 0$, $k \in \mathbb{N}$ and $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k})$ a sequence of (m, k_m) codes for the compound channel given by $conv(\mathfrak{I})$ such that
  - $$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq \inf_{\mathcal{N}\in conv(\mathfrak{I})} \frac{1}{k} I_c(\rho, \mathcal{N}^{\otimes k}) - \delta, \qquad (8)$$
  - $$\inf_{\mathcal{N}\in conv(\mathfrak{I})} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}^{\otimes m} \circ \mathcal{P}^m) \geq 1 - 2^{-mc}. \qquad (9)$$
- Define $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0,1]$ by

$$f(p, s^m) := F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{U}_{p,\mathcal{K}} \circ \mathcal{N}_{s^m} \circ \mathcal{U}_{p,\mathcal{H}} \circ \mathcal{P}^m),$$

  where $\mathcal{U}_{p,\mathcal{K}} : \mathcal{B}(\mathcal{K})^{\otimes m} \to \mathcal{B}(\mathcal{K})^{\otimes m}$ is the usual action of Perm_m on $\mathcal{B}(\mathcal{K})^{\otimes m}$ as permutations of tensor factors.
- f is invariant under the action of Perm_m.
- For application of the robustifiction technique, choose $p^* = id$

Theorem (Ahlswede's robustification technique)

If a function $f : \mathrm{Perm}_m \times \mathbf{S}^m \to [0,1]$ *which is invariant under the action of* Perm_m *satisfies*

$$\sum_{s^m \in \mathbf{S}^m} f(p^*, s^m) q(s_1) \cdot \ldots \cdot q(s_m) \geq 1 - \gamma \tag{4}$$

for some $p^* \in \mathrm{Perm}_m$, *all* $q \in T(m, \mathbf{S})$ *and some* $\gamma \in [0,1]$, *then*

$$\frac{1}{m!} \sum_{p \in \mathrm{Perm}_m} f(p, s^m) \geq 1 - \gamma (m+1)^{|\mathbf{S}|} \qquad \forall s^m \in \mathbf{S}^m. \tag{5}$$

- Perm_m = set of permutations on $\{1, \ldots, m\}$.
- $T(m, \mathbf{S})$ =set of empirical distributions on $\mathbf{S}$ generated by $\mathbf{S}^m$.
- Invariance of f means that

$$f(p \circ p', p(s^m)) = f(p', s^m),$$

for all $p, p' \in \mathrm{Perm}_m$ and $s^m \in \mathbf{S}^m$.

- It is easy to show that for *every* probability distribution $\mathfrak{q}$ on $\mathbf{S}$ we have with $\mathcal{N}_{\mathfrak{q}} := \sum_{s \in \mathbf{S}} \mathfrak{q}(s)\mathcal{N}_s \in conv(\mathfrak{I})$:

$$\sum_{s^m \in \mathbf{S}^m} f(p^*, s^m)\mathfrak{q}(s_1) \cdot \ldots \cdot \mathfrak{q}(s_m) = F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}_{\mathfrak{q}}^{\otimes m} \circ \mathcal{P}^m) \geq 1 - 2^{-mc}.$$

- Ahlswede's robustification thus gives, for any $s^m \in \mathbf{S}^m$, the estimate

$$\frac{1}{m!} \sum_{p \in \mathrm{Perm}_m} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{U}_{p,\mathcal{K}} \circ \mathcal{N}_{s^m} \circ \mathcal{U}_{p,\mathcal{H}} \circ \mathcal{P}^m)$$

$$= \frac{1}{m!} \sum_{p \in \mathrm{Perm}_m} f(p, s^m)$$

$$\geq 1 - \underbrace{2^{-mc}(m+1)^{|\mathbf{S}|}}_{\to 0 \text{ as } m \to \infty}$$

- This means that for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ the sequence of random codes $(\mu_m := \frac{1}{m!}\sum_{p\in\mathrm{Perm}_m}\delta_{(\mathcal{U}_{p,\mathcal{H}}\circ\mathcal{P}^m,\mathcal{R}^m\circ\mathcal{U}_{p,\mathcal{K}})})_{m\in\mathbb{N}}$ achieves

$$\inf_{\mathcal{N}\in conv(\mathfrak{I})}\frac{1}{k}I_c(\rho,\mathcal{N}^{\otimes k})-\delta,$$

where $\delta>0$, $k\in\mathbb{N}$ and $\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})$ are arbitrary.

- This implies

$$\mathcal{A}_{random}(\mathfrak{I})\geq\lim_{k\to\infty}\frac{1}{k}\max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})}\inf_{\mathcal{N}\in conv(\mathfrak{I})}I_c(\rho,\mathcal{N}^{\otimes k}).$$

Achievability 2: Derandomization (Sketch)

Now we have a good *random* code with discrete support of size $\simeq m!$, but we want a *deterministic* one. Idea: Derandomize, following the ideas of Ahlswede in the classical case:

- If $\mathcal{A}_{\mathrm{det}}(\mathfrak{I}) > 0$, the sender can transmit entanglement to the receiver at positive rate using deterministic codes.
- Consequently, transmission of classical data at positive rate with deterministic codes is possible.
- Thus, we might try to send e.g. subexponentially many bits of classical information in order to first establish common randomness, then use a random code.

Problem: The number of branches in our code μ_m is $\simeq m!$, which is super-exponential!

A way out is given by a variant of Ahlswede's elimination technique (the original can be found in: ⇒ R. Ahlswede, Elimination of Correlations in Random Codes for Arbitrarily Varying Channels, Z. Wahrscheinlichkeitstheorie u. verw. Gebiete 44, 159-175 (1978))

The following lemma shows that only subexponentially many (in block length) branches are necessary.

Lemma (Random Code Reduction)

Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC, $m \in \mathbb{N}$, and μ_m an (m, k_m)-random code for the AVQC $\mathfrak{I}$ with

$$\min_{s^m\in\mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^l \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{P}^m, \mathcal{R}^m) \geq 1 - 2^{-ma} \quad (10)$$

for some positive constant $a \in \mathbb{R}$.
Let $\varepsilon \in (0, 1)$. There is an $M = M(a, \varepsilon, |\mathbf{S}|) \in \mathbb{N}$ such that, if $m \geq M$, there exist m^2 codes $\{(\mathcal{P}_i^m, \mathcal{R}_i^m) : i = 1, \dots, m^2\} \subset CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}'_m)$ with the property

$$\frac{1}{m^2} \sum_{i=1}^{m^2} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}_i^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}_i^m) > 1 - \varepsilon \qquad \forall s^m \in \mathbf{S}^m. \quad (11)$$

Definition

Let $\mathbf{S}$ be a finite set and $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ an AVQC.

1. $\mathfrak{I}$ is called m-symmetrizable, $m \in \mathbb{N}$, if for every finite set of states $\rho_1, \ldots, \rho_K \in \mathcal{S}(\mathcal{H}^{\otimes m})$, there are probability distributions $p_1, \ldots, p_K \in \mathfrak{P}(\mathbf{S}^m)$ such that for every $i, j \in \{1, \ldots, K\}$ the following holds:

$$\sum_{s^m\in\mathbf{S}^m} p_i(s^m)\mathcal{N}_{s^m}(\rho_j) = \sum_{s^m\in\mathbf{S}^m} p_j(s^m)\mathcal{N}_{s^m}(\rho_i). \tag{12}$$

2. We call $\mathfrak{I}$ symmetrizable if it is m-symmetrizable for all $m \in \mathbb{N}$.

Theorem

Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC. The following is true.

1. *$\mathfrak{I}$ is symmetrizable if and only if $C_{\mathrm{det}}(\mathfrak{I}) = 0$.*
2. *If $\mathfrak{I}$ is symmetrizable then $\mathcal{A}_{det}(\mathfrak{I}) = 0$.*

The following lemma shows that only subexponentially many (in block length) branches are necessary.

Lemma (Random Code Reduction)

Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC, $m \in \mathbb{N}$, and μ_m an (m, k_m)-random code for the AVQC $\mathfrak{I}$ with

$$\min_{s^m\in\mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^l \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{P}^m, \mathcal{R}^m) \geq 1 - 2^{-ma} \quad (10)$$

for some positive constant $a \in \mathbb{R}$.
Let $\varepsilon \in (0, 1)$. There is an $M = M(a, \varepsilon, |\mathbf{S}|) \in \mathbb{N}$ such that, if $m \geq M$, there exist m^2 codes $\{(\mathcal{P}_i^m, \mathcal{R}_i^m) : i = 1, \dots, m^2\} \subset CPTPM(\mathcal{F}_m, \mathcal{H}^{\otimes m}) \times CPTPM(\mathcal{K}^{\otimes m}, \mathcal{F}'_m)$ with the property

$$\frac{1}{m^2} \sum_{i=1}^{m^2} F_e(\pi_{\mathcal{F}_m}, \mathcal{R}_i^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}_i^m) > 1 - \varepsilon \qquad \forall s^m \in \mathbf{S}^m. \quad (11)$$

Definition

Let $\mathbf{S}$ be a finite set and $\mathfrak{J} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ an AVQC.

1. $\mathfrak{J}$ is called m-symmetrizable, $m \in \mathbb{N}$, if for every finite set of states $\rho_1, \ldots, \rho_K \in \mathcal{S}(\mathcal{H}^{\otimes m})$, there are probability distributions $p_1, \ldots, p_K \in \mathfrak{P}(\mathbf{S}^m)$ such that for every $i, j \in \{1, \ldots, K\}$ the following holds:

$$\sum_{s^m\in\mathbf{S}^m} p_i(s^m)\mathcal{N}_{s^m}(\rho_j) = \sum_{s^m\in\mathbf{S}^m} p_j(s^m)\mathcal{N}_{s^m}(\rho_i). \tag{12}$$

2. We call $\mathfrak{J}$ symmetrizable if it is m-symmetrizable for all $m \in \mathbb{N}$.

Theorem

Let $\mathfrak{J} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC. The following is true.

1. *$\mathfrak{J}$ is symmetrizable if and only if $C_{\mathrm{det}}(\mathfrak{J}) = 0$.*
2. *If $\mathfrak{J}$ is symmetrizable then $\mathcal{A}_{det}(\mathfrak{J}) = 0$.*

Maximal Error (Strong Subspace Transmission)

Application of one of the descendants of Levy's Lemma shows that the following are equivalent:

1. There is a sequence of (random or deterministic) (m, k_m)-codes for $\mathfrak{I}$ such that
   - $\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R$,
   - $\lim_{m\to\infty} \inf_{s^m \in \mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1$.
2. There is a sequence of (random or deterministic) (m, k_m)-codes for $\mathfrak{I}$ such that

$$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R,$$

$$\lim_{m\to\infty} \inf_{s^m \in \mathbf{S}^m} \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} \int F(\rho, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m(\rho)) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1,$$

where $F(\rho, \sigma) := \mathrm{tr}\{\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\}$ is the usual fidelity.

Theorem

For $\delta, \Theta > 0$ and an integer n let $k(\delta, \Theta, n) = \lfloor \delta^2(n-1)/(2\log(4/\Theta)) \rfloor$. Let $f : S(\mathbb{C}^n) \to \mathbb{R}$ be a continuous function and ν_k the uniform measure induced on the Grassmannian $G_{n,k}$ by the normalized Haar measure on the unitary group on $\mathbb{C}^n$ then, for all $\delta, \Theta > 0$, the measure of the set $E_k \subset G_{n,k}$ of all subspaces $E \subset \mathbb{C}^n$ satisfying the three conditions

1. $\dim E = k(\delta, \Theta, n)$
2. *There is a $\Theta-$net N in $S(E) = S(\mathbb{C}^n) \bigcap E$ such that $|f(x) - M_f| \le \omega_f(\delta)$ for all $x \in N$*
3. $|f(x) - M_f| \le \omega_f(\delta) + \omega_f(\Theta)$ *for all $x \in S(E)$*

satisfies $\nu_k(E_k) \ge 1 - \sqrt{2/\pi}\, e^{-\delta^2(n-1)/2}$.
$S(\mathbb{C}^n)$: unit sphere in $\mathbb{C}^n$,
$\omega_f(\delta) := \sup\{|f(x) - f(y)| : D(x,y) \le \delta\}$: modulus of continuity,
D: geodesic metric on $S(\mathbb{C}^n)$,
M_f: median of f (the number such that with ν the Haar measure on $S(\mathbb{C}^n)$ both $\nu(\{x : f(x) \le M_f\}) \ge 1/2$ and $\nu(\{x : f(x) \ge M_f\}) \ge 1/2$).

Maximal Error (Strong Subspace Transmission)

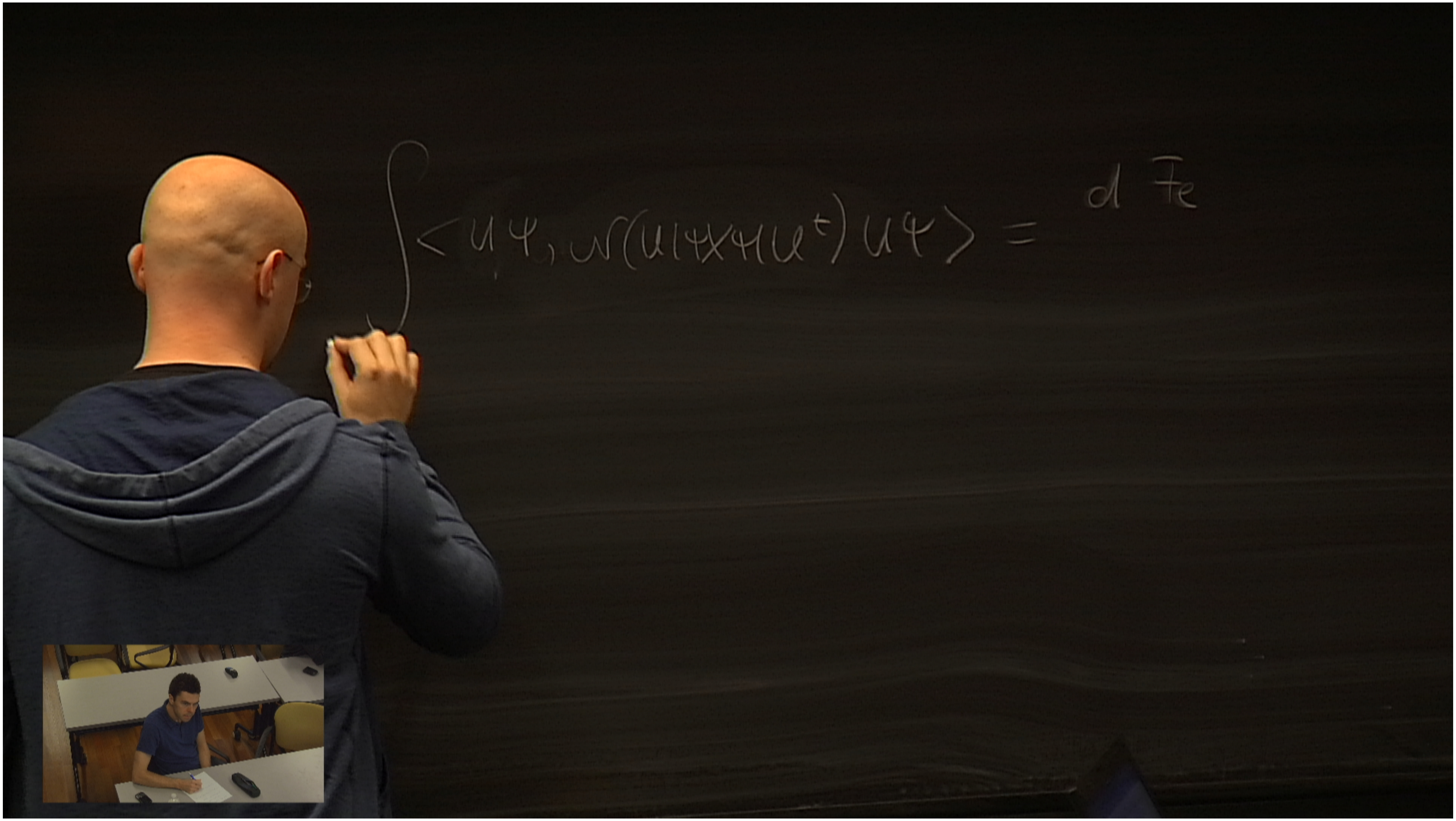
Application of one of the descendants of Levy's Lemma shows that the following are equivalent:

1. There is a sequence of (random or deterministic) (m, k_m)-codes for $\mathfrak{I}$ such that
   - $\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R$,
   - $\lim_{m\to\infty} \inf_{s^m \in \mathbf{S}^m} \int F_e(\pi_{\mathcal{F}_m}, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1$.
2. There is a sequence of (random or deterministic) (m, k_m)-codes for $\mathfrak{I}$ such that

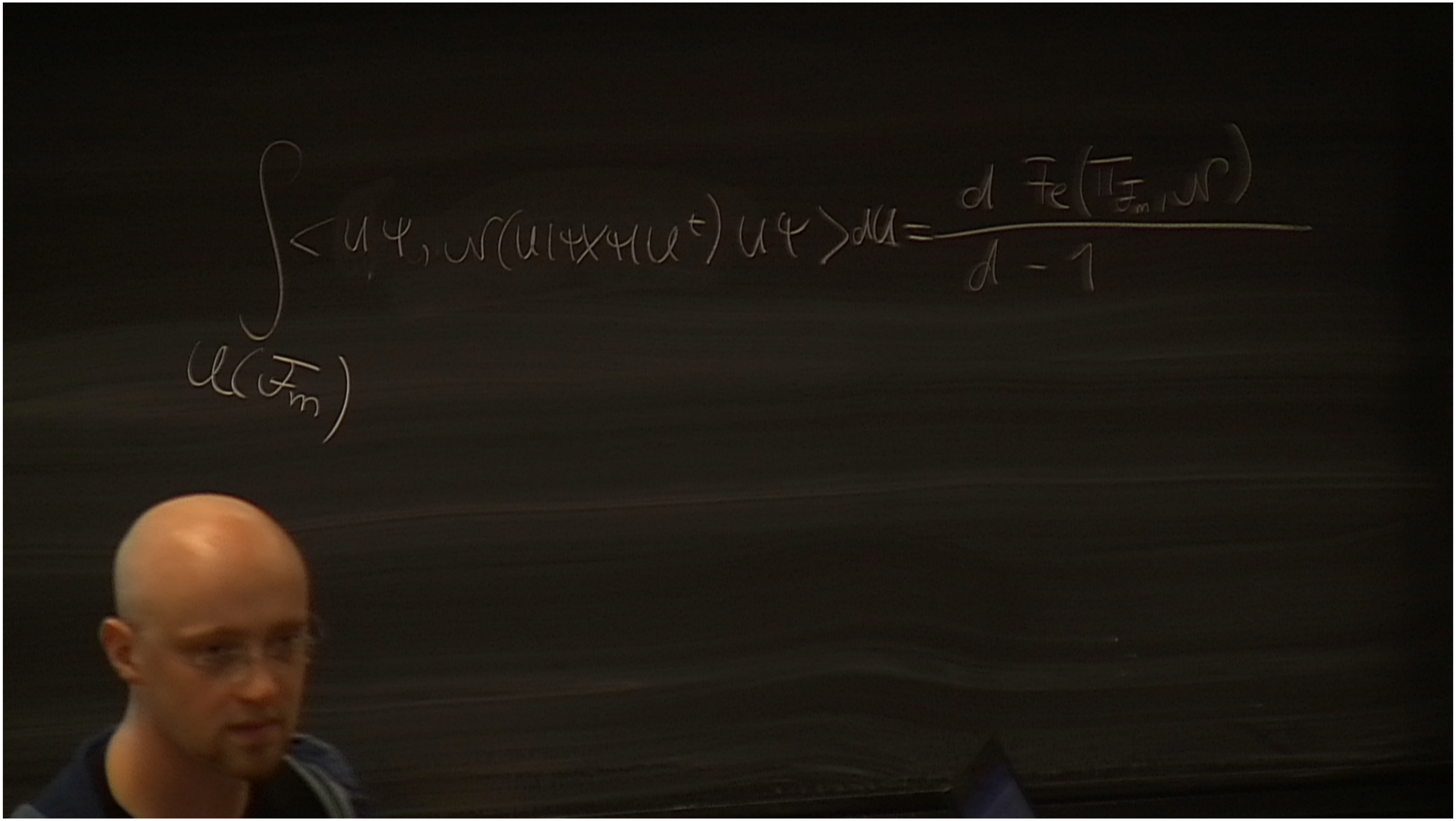
$$\liminf_{m\to\infty} \frac{1}{m} \log k_m \geq R,$$

$$\lim_{m\to\infty} \inf_{s^m \in \mathbf{S}^m} \min_{\rho \in \mathcal{S}(\mathcal{F}_m)} \int F(\rho, \mathcal{R}^m \circ \mathcal{N}_{s^m} \circ \mathcal{P}^m(\rho)) d\mu_m(\mathcal{R}^m, \mathcal{P}^m) = 1,$$

where $F(\rho, \sigma) := \mathrm{tr}\{\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\}$ is the usual fidelity.



$$\int_{\mathcal{U}(\mathcal{F}_m)} \langle U\psi, \mathcal{N}(U|\psi\rangle\langle\psi|U^{\dagger})\, U\psi \rangle = \frac{d\, F_e(\pi_{\mathcal{F}_m}, \mathcal{N})}{d - 1}$$


$\int_{U(\mathcal{F}_m)} \langle U\psi, W(U|\psi\rangle\langle\psi|U^\dagger)\, U\psi \rangle \, dU = \frac{d \, \mathrm{Tr}(\Pi_{\mathcal{F}_m} W)}{d-1}$

$$\int_{\mathcal{U}(\mathcal{F}_m)} \langle U\psi, \mathcal{N}(U|\psi\rangle\langle\psi|U^{\dagger})U\psi \rangle \, dU = \frac{d \; F_e(\Pi_{\mathcal{F}_m}, \mathcal{N})}{d - 1}$$

$$F_e(\Pi_{\mathcal{F}_{s^m}}, \; \mathcal{R}_{s^m}$$