# Coding Theorem and Strong Converse for Quantum Channels

Andreas Winter*
SFB 343, Fakultät für Mathematik
Universität Bielefeld, Postfach 100131, 33501 Bielefeld

September 7, 1998

**Abstract**

In this communication we present a new proof of Holevo's channel coding theorem for quantum channels, and its strong converse. The technique is largely inspired by Wolfowitz's combinatorial approach using types of sequences.

## 1 Introduction

After the recent achievements in quantum information theory, most notably Schumacher's quantum data compression [16], and the determination of the quantum channel capacity by Holevo [12] (and independently by Schumacher and Westmoreland [17]) building on ideas of Hausladen et.al. [7], we feel that one should try to convert other and stronger techniques of classical information theory than those used in the cited works to the quantum case. The present work will do this for the method of types, as it is called in [3] (and which constitutes a manifestly combinatorial approach to information theory), by rephrasing it in the operator language of quantum theory. This we apply to the coding problem for discrete memoryless quantum channels: we will give a new proof of the quantum channel coding theorem, and prove the strong converse. We point out that our techique is also suited to the situations of encoding under linear constraints, and with arbitrary signal states.

*Electronic address: winter@mathematik.uni-bielefeld.de

## 2 Prerequisites and notational conventions

We will use the definitions and notation of [18], in particular finite sets will be $\mathcal{A}$, $\mathcal{B}$, $\mathcal{M}$, $\mathcal{X}$, ..., quantum states (density operators) $\rho$, $\sigma$, ..., probability distributions $P$, $Q$, ..., and classical–quantum operations $V$, $W$, ... (also stochastic matrices), whereas general quantum operations (trace preserving, and completely positive maps) of C$^*$–algebras $\mathfrak{X}$, $\mathfrak{Y}$, ... are denoted as adjoint maps $\varphi_*$, $\psi_*$, ... Our algebras will be of finite dimension, and apart from commutative ones we will confine ourselves to the C$^*$–algebra $\mathfrak{L}(\mathcal{H})$, the algebra of (bounded) linear operators of the complex Hilbert space $\mathcal{H}$, even though everything works equally well for the general case.

The exponential function exp is always understood to basis 2, as well as the logarithm log. The same symbol $H$ denotes the Shannon and the von Neumann entropy (as Shannon's is the commutative case of von Neumann's).

We will use two different norms on operators: the supremum norm $\|\cdot\|_\infty$ which is the largest absolute value of an eigenvalue, and (for states etc.) the trace norm $\|\cdot\|_1$ which is the sum of the absolute values of the eigenvalues. It is known (and not difficult to prove, using the polar decomposition of $\alpha$, see Arveson [1]) that

$$\|\alpha\|_1 = \sup_{B:\|B\|_\infty\leq 1} |\mathrm{Tr}\,(\alpha B)|$$

If $\alpha$ is selfadjoint we may write it as the difference $\alpha_+ - \alpha_-$ of its positive and its negative part. Observe that then

$$\|\alpha\|_1 = \mathrm{Tr}\,(\alpha_+) + \mathrm{Tr}\,(\alpha_-) = \sup_{-\mathbb{1}\leq B\leq \mathbb{1}} \mathrm{Tr}\,(\alpha B)$$

Another useful formula is

$$\mathrm{Tr}\,(\alpha_+) = \sup_{0\leq B\leq \mathbb{1}} \mathrm{Tr}\,(\alpha B)$$

## 3 Quantum sources and channels

The following definition is from [9]: a (discrete memoryless) *classical–quantum channel* (cq–DMC) is a mapping $W$ from a finite set $\mathcal{X}$ into the states on a Hilbert space $\mathcal{H}$, taking $x\in\mathcal{X}$ to $W_x$ (by linear extension we may view this as a quantum operation from $(\mathbb{C}\mathcal{X})_*$ to $\mathfrak{L}(\mathcal{H})_*$).

From [18] we recall: for a probability distribution $P$ on $\mathcal{X}$ let $PW = \sum_{x\in\mathcal{X}} P(x)W_x$