Languages of Quantum Information Theory

Andreas Winter[*]

SFB 343, Fakultät für Mathematik

Universität Bielefeld, Postfach 100131, 33501 Bielefeld

(September 8, 1998)

Abstract

This note will introduce some notation and definitions for information theoretic quantities in the context of quantum systems, such as (conditional) entropy and (conditional) mutual information. We will employ the natural C*–algebra formalism, and it turns out that one has an allover dualism of language: we can define everything for (compatible) observables, but also for (compatible) C*–subalgebras. The two approaches are unified in the formalism of quantum operations, and they are connected by a very satisfying inequality, generalizing the well known Holevo bound. Then we turn to communication via (discrete memoryless) quantum channels: we formulate the Fano inequality, bound the capacity region of quantum multiway channels, and comment on the quantum broadcast channel.

1998 PACS number(s): 03.67.-a, 03.67.Hk, 89.70.+c

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

I. INTRODUCTION

After the beginnings of quantum information theory in the sixties [1], and Holevo's now widely known investigations of the seventies [2–4] today there is again a tremendous interest in this field. This interest focuses on two areas which may be described, sightly abusing language introduced by Holevo twenty years ago [3], as *classical–quantum* problems on the one hand, and *quantum–quantum* problems on the other, and it mostly derives from the latter, as these include all problems of (quantum) information processing inside a quantum computer or memory. Whereas this area (which is charcterized by its attention to *entanglement*) poses many new and beautiful, and also very difficult problems, the present note is concerned wholly with the former area (though it is by now not altogether clear how to separate these two worlds, cf. e.g. opinion uttered by Adami and Cerf [5]). We take the view that classical–quantum problems are those in which classical information has to be stored in or sent trough some quantum system. Examples from recent work are the determination of the quantum channel capacity for fixed input states [6–8], quantum cryptographic protocols [9,10], and entanglement enhanced transmission (superdense coding) [11].

Our approach is somewhat reminiscent of "quantum probability" through its formulation in terms of C*–algebras and its emphasis on observable operators (which reflects our dwelling in the classical–quantum area), but we cannot respect the bounds of this field: we will use positive operator valued measures (instead of unbounded selfadjoint operators), and we will consider quantum operations, both quite uncommon in noncommutative probability. Finally it should be noted that we hardly present any new concepts or results — our contribution lies in introducing a reasonable and efficient calculus.

The outline of the paper is as follows: in section II we will basically recall the language of C*–algebras, completely positive maps, positive operator valued measures, and the notion of compatibility. In the following sections III and IV we will define various information theoretic quantities, first for observables, second for $*$–subalgebras. In section V we will unify these approaches using completely positive C*–algebra maps, and can give meaning