

Bound Entanglement and Bound Information

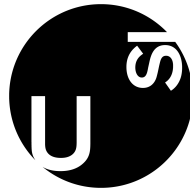
Thesis Subtitle

Luca Dolfi

Advisor: Prof. Dr. Stefan Wolf

Tutor: MSc Arne Hansen

A thesis presented for the degree of
BSc in Informatics



Department of Informatics
Università della Svizzera Italiana
Spring 2018

Contents

1	Introduction	2
1.1	Motivation	3
1.2	Linear Algebra and Notation	4
1.3	Basics of QM	5
1.3.1	Quantum Entanglement	5
1.4	Basics of Information Theory	5
1.4.1	Classical Key Agreement	5

Chapter 1

Introduction

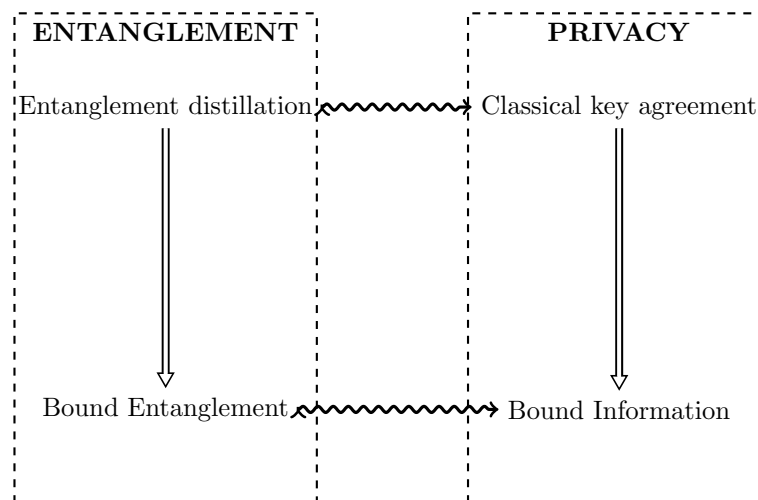


Figure 1.1: the big picture that represents how QM and Information Theory can relate to each other

entanglement theory	key agreement
quantum entanglement	secret classical correlations
quantum communication	secret classical communication
classical communication	public classical communication
local actions	local actions

Table 1.1: Table taken from [Hor+07]

1.1 Motivation

Why doing it.

from where does the intuition come from → explain intuition

why it may be useful

Looking at QM → WHY

Utilities in real world.

Computational security (RSA) < security through physical laws (BB84) < information theoretical security (??)

It is interesting, that entanglement, which is originally quantum concept, corresponds to privacy in general - not only in the context of quantum protocols.¹

The task of Alice and Bob is to obtain via local (classical) operations and public communication (LOPC) the longest bit-string which is almost perfectly correlated and about which Eve (who can listen to the public discussion) knows a negligible amount of information.²

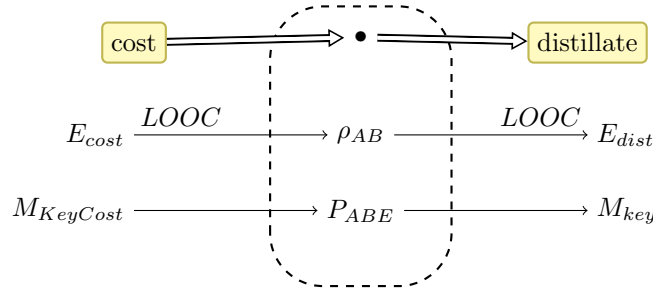


Figure 1.2: Sort of how and why the intuition is constructed from previous knowledge of concepts of QM

[...] an analogue of the necessary and sufficient condition for entanglement distillation was found. As in the quantum case the state is distillable iff there exists a projection (acting on n copies of a state for some n) onto 2-qubit subspace which is entangled, in the classical case, the key is distillable iff there exists a binary channel (acting on n copies of a distribution for some n) which outputs Alice's and Bob's variables, such that the resulting distribution has nonzero key. [Hor+07]

¹Hor+07.

²Hor+07.

1.2 Linear Algebra and Notation

1. Dirac's bracket notation
2. Inner/Outer product
3. Linear operator
4. Adjoints and Hermitian operators
5. Pauli matrices
6. Tensor Product and tensor space

Inner/outer product

The inner product of two vectors $|v\rangle$ and $|w\rangle$ is

$$(|v\rangle, |w\rangle) = \langle v|w\rangle = (|w\rangle, |v\rangle)^* = \langle w|v\rangle^*$$

Where $*$ represents the transpose, and because we are dealing with complex number, we also intend the conjugate transpose, which produces a scalar (complex) value.

This property is fundamental in the sense that it will allows us to go from a state space –that can be many dimensional– to a *measurement* space, which assumes real values.

In standard vector notation this is no different from

$$(\vec{v}, \vec{w}) = (\bar{v}_1 \quad \bar{v}_2) \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = (\bar{w}_1 \quad \bar{w}_2) \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = (\vec{w}, \vec{v})^*$$

It is important also to note that through the inner product of two vectors we also define the norm $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$.

The outer product of two vectors, on the other hand, produces a matrix, with very important properties. So if we define the matrix³ $A = |w\rangle\langle v|$ we observe that

$$|w\rangle\langle v|v'\rangle = \langle v|v'\rangle |w\rangle$$

which is a really convenient way of visualizing the action of matrix A . In particular if we divide it like $(|w\rangle\langle v|)(|v'\rangle)$ it is easy to interpret it as *matrix A acting on vector $|v'\rangle$* ; but the other equivalent form $(\langle v|v'\rangle)(|w\rangle)$ can also be seen as multiplying vector $|w\rangle$ by a value $\langle v|v'\rangle$.

The meaning of this is that $|w\rangle\langle v|$ can indeed be defined as a (linear) operator from the vector space of $|v\rangle$ and $|v'\rangle$ to the vector space of $|w\rangle$. This comes in very handy when we later use it to define operations and measurements on quantum states.

³The fact that the result of $|w\rangle\langle v|$ is indeed a matrix can be seen more directly if we remember that this is nothing less than a column-row vectors multiplication.

Linear operators

A linear operator between two vector spaces is defined as

$$\mathbf{A} : V \longrightarrow W, |v_i\rangle \mapsto A|v_i\rangle$$

$$\text{linear in all inputs, i.e. } A \left(\sum_i a_i |v_i\rangle \right) = \sum_i a_i A|v_i\rangle \text{ for all } i$$

Looking back at the definition of the matrix $A = |w\rangle\langle v|$ we can now refer to it as a linear operator from now on.

1.3 Basics of QM

The simplest quantum mechanical system, and the system which we will be most concerned with, is the *qubit*. A qubit has a two-dimensional state space. [...] The way a qubit differs from a bit is that superposition of these two states, of the form $a|0\rangle + b|1\rangle$, can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$, or definitely in the state $|1\rangle$. [NC10]

All pure states in QM are normalized vectors in \mathcal{H} .

$$|\psi\rangle \in \mathcal{H} \Rightarrow |\langle\psi|\psi\rangle| = 1$$

This is instrumental in seeing them as probability vectors. Every linear operator has then to be unitary to maintain this property.

A statistical mixture of states corresponds to a *density matrix*, which is itself a new state. It is important to note that a mixture of probability of states is not the same thing as superposition of states. In the latter we don't have a measure of uncertainty of the state, meaning also that in theory we are always able to find a measurement basis that will always output the same result for that state. In the former, however, this is not possible given by the direct intrinsic uncertainty of the state.

Density matrices have then the properties:

$$M = \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_i p_i P_{|\psi_i\rangle}, \text{ where state } |\psi_i\rangle \text{ has probability } p_i$$

ρ is a positive, trace-1 operator meaning that $Tr(\rho) = 1$ and all eigenvalues of ρ are positive. Moreover ρ is a linear combination of projectors $|i\rangle\langle i|$ which makes $\rho \in \mathbf{P}(\mathcal{H})$ a projector itself on the Hilbert space.

1.3.1 Quantum Entanglement

1.4 Basics of Information Theory

1.4.1 Classical Key Agreement

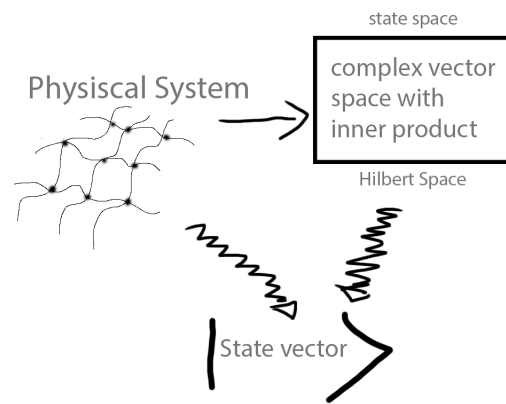


Figure 1.3: how a physical state is represented

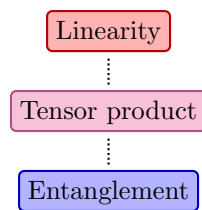


Figure 1.4: origin of entanglement via linearity

Bibliography

- [Hor+07] Ryszard Horodecki et al. “Quantum entanglement”. In: *Rev.Mod.Phys.*81:865-942,2009 (2007).
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2010.