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

Chapter 1

Introduction

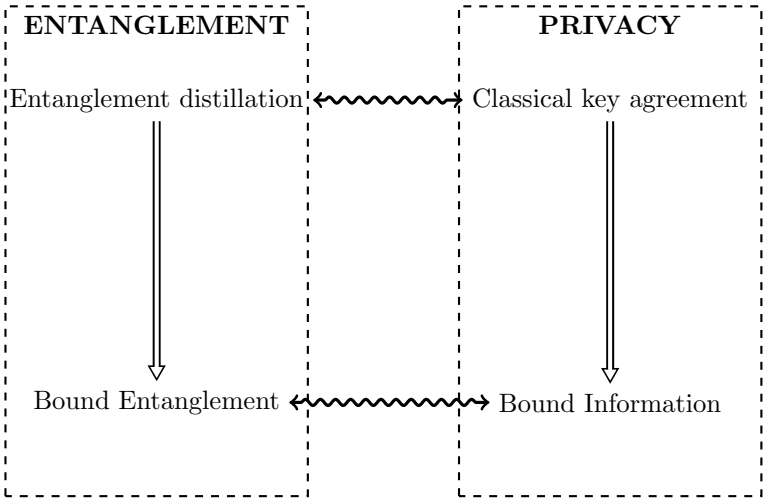

Figure 1.1: the big picture that represents how QM and Information Theory can relate to each other

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]

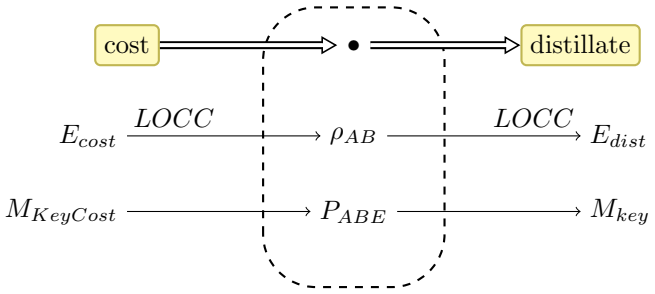

Figure 1.2: Sort of how and why the intuition is constructed from previous knowledge of concepts of QM

[...] 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]

[1] Hor+07.
[2] Hor+07.

1.2 Linear Algebra and Notation

In order to understand subsequent sections of this thesis a basic knowledge of the mathematical framework behind quantum mechanics is needed. The whole theory is constructed on a (mostly) straightforward linear theory, thus a basic knowledge of linear algebra plus some addendum is enough. It is important, however, to specify a standard notation as used in literature.

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

Dirac's bra-ket notation and Hilbert spaces

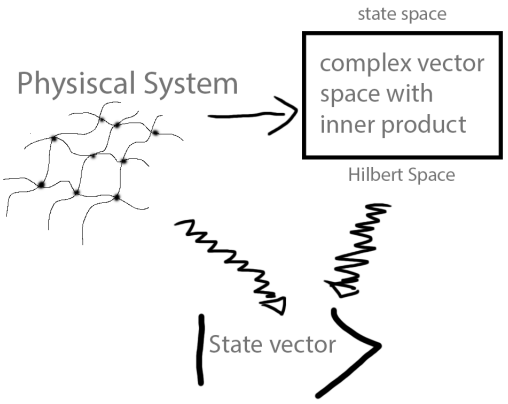

Figure 1.3: how a physical state is represented

The bra-ket notation is a handy notation introduced by physicist Paul Dirac to deal with the vector representation of quantum states linear functionals.

$$|\varphi\rangle = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \end{pmatrix} \text{ is a coloumn vector over } \mathcal{H}$$

$$\langle\psi| = \begin{pmatrix}\psi_1 & \psi_2 & \dots\end{pmatrix} \text{ is a row vector over } \mathcal{H}$$

Furthermore the conjugate transpose of a *bra* vector is the corresponding *ket* vector, and vice versa.[con18]

$$\langle\varphi|^\dagger = |\varphi\rangle,\ |\varphi\rangle^\dagger = \langle\varphi|$$

More specifically, for a complex vector space as $\mathcal{H}$, the components of $\langle\varphi|$ are each the complex conjugate of the components of $|\varphi\rangle$.
It is worth noting that in quantum information we will consider only vectors of finite dimensions, and more often than not, the standard basis for qubits represented by

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

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

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

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 matrix[3] $A = |w\rangle\langle v|$ 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.

[3]The 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.
Some well-known linear operators acting on single qubits that we will use later on are the *Pailu Matrices*

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

In particular it is safe to say that, unless stated otherwise, the operators that will be presented all have a set of properties and are called Hermitian operators, or self-adjoint operators.

$$A = A^{dagger} \quad \Longrightarrow (A|v\rangle)^\dagger = \langle v|A^\dagger$$

Operators have also to be positive, this means that it holds, for every $|v\rangle$: $\langle v|A|v\rangle$ is real non-negative. Any positive operator is also self-adjoint and therefore it has diagonal (spectral) representation $\sum_i \lambda_i |i\rangle\langle i|$ with non-negative eigenvalues λ_i.

Tensor product

The tensor product $V \otimes W$ is an operation between vector spaces that combines every element of the first vector space and every element of the second vector space in a bigger vector space. Tensor product is linear and from its properties emerges the famous phenomenon of quantum entanglement, which simply is that not all vectors in $\mathcal{H} = V \otimes W$ can be divided into $|v\rangle \otimes |w\rangle$ with $|v\rangle \in V,\ |w\rangle \in W$. This will later be explained in the next section.
Notation and abbreviation for the tensor product is

$$|v\rangle \otimes |w\rangle = |v\rangle|w\rangle = |v, w\rangle = |vw\rangle$$

It has the following properties:

$\forall |v\rangle \in V,\ \forall |w\rangle \in W,\ \forall z \in \mathbb{C}$
$\quad z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle$

$\forall |v_1\rangle, |v_2\rangle \in V,\ \forall |w\rangle \in W$
$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1 w\rangle + |v_2 w\rangle$

$\forall |v\rangle \in V,\ \forall |w\rangle \in W,\ A : V \to V'\ B : W \to W'$
$(A \otimes B)\left(\sum_i a_i |v_i w_i\rangle\right) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$

The inner product on V and W can be used to define (linearly) an inner product on $V \otimes W$.

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 superpositions 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]

Quantum mechanics is a very large and complex theory. For our purposes it is enough for us to only consider the quantum system called *qubit* and its rules of computation following from the tensor product algebra. ...

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 $|\psi_i\rangle\langle\psi_i|$ which makes $\rho \in \mathbf{P}(\mathcal{H})$ a projector itself on the the Hilbert space.

1.3.1 Quantum Measurements

To get an actual value out of a qubit one has to *measure* it. Measurement is, mathematically, a projection onto some chosen computational basis. The result

for each base vector projection is then interpreted as a *probability*. The state then changes after measurement, meaning for example that it will not retain it value as superposition any more.
...

If Alice has the state $|psi_i\rangle$ out of $i = 1..n$ and all states are orthonormal, then Bob can find out what the choice of i was. If the states are not orthonormal there is no quantum measurement capable of distinguishing the states.
From this follows that if the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, then $|\psi_2\rangle$ has a component orthogonal to $|\psi_1\rangle$ but also a component parallel to it which will give probability not 0 of measuring differently.

Example:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad P_{+1} = |0\rangle\langle 0|,\ P_{-1} = |1\rangle\langle 1|$$

Measurement on qubit $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ has probability
$p_{+1} = \langle\psi|P_{+1}|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \frac{1}{2}$ and similarly $p_{-1} = \frac{1}{2}$

1.3.2 Quantum Entanglement

There exist vectors in $V \otimes W$ that can not be represented by a single tensor product:

Given $v_1, v_2 \in V$ $w_1, w_2 \in W$ linear independent:

$v_1 \otimes w_1 + v_2 \otimes w_2 = v_1 w_1 + v_2 w_2 \in V \otimes W$ is *not* separable

this may be strange because on physical level tensor product is combination(merging) of quantum systems [Han13]

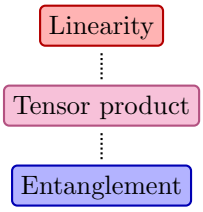

Figure 1.4: origin of entanglement via linearity

1.4 Basics of Information Theory

1.4.1 Classical Key Agreement

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.

[con18] Wikipedia contributors. *Bra–ket notation*. 2018. URL: `https://en.wikipedia.org/w/index.php?title=Bra%E2%80%93ket_notation&oldid=830232271`.

[Han13] Arne Hansen. "Swapped Bound Entanglement". Master Thesis. ETHZ, 2013.

[GW00] Nicolas Gisin and Stefan Wolf. "Linking clasical and quantum key agreement: is there "bound information"?" In: *Proceedings of CRYPTO 2000*. Ed. by Springer-Verlag. 2000.