Bound Entanglement and Bound Information

Luca Dolfi

dolfil@usi.ch

Advisor: Prof. Stefan Wolf

Tutor: MSc Arne Hansen

Spring 2018

Motivation

Since the advent of quantum cryptography, i.e. cryptography based on the laws of physics rather than hard mathematics problem, there has been major interests in new possibilities to assure secure key distribution.
A secure key distribution between Alice and Bob is crucial to be sure that the key stays secret and can therefore be used to encrypt a message using a classical crypto system, for example a *one time pad*.
Protocols for the exchange of secret messages over quantum channels are already well known for the cases of local operations and classical communication, or for fully correlated states (fully entangled). This is not the same for the lesser forms of entanglement for which many open questions remain.

Goal

Is there a tripartite probability distribution, corresponding to Alice and Bob wanting to establish a key unknown to Eve, that has a non-zero key cost, while not allowing to distill any secret key?

The aim of this project is to build an understanding of bound entanglement, the related measures of entanglement and their connections to classical key agreement protocols, as well as related information-theoretic concepts, in order to approach this open question.

Project description

Entanglement -a consequence of the linear structure of the mathematical formalism of quantum mechanics- is one of the astounding aspects of quantum mechanics and a valuable resource for a number of computational tasks.
To measure entanglement one might consider the least number of maximally entangled bipartite quantum states -so-called singlets- required to prepare a density matrix ρ by local operations and classical communication. Similarly one might measure entanglement by the maximal number of

singlets that can be obtained form ρ by local operations and classical communication.
These measures are not the same. Particularly, there exists weakly entangled states -called bound-entangled- that require singlets for their preparation while they, in turn, do not allow to distill any singlets.

There are analogies to classical key agreement, for instance, entanglement distillation schemes based on protocols for classical key agreement.
Together with an information-theoretic analogue for the entanglement cost, the so-called **information of formation** or **key cost**, one can ask whether there exists an information-theoretic analogue to bound entanglement.

Plan

Possible tasks:

1. Build understanding of entanglement
   1.1. build understanding of bound entanglement
2. Build understanding of a channel in classical information theory
   2.1. build understanding of key agreement over a channel
3. Understand different measurements of entanglement and information-theoretic counterparts
   3.1. entanglement cost
   3.2. information of formation
   3.3.key cost
4. Understand the different QKD protocols and how they use entanglement
5. Look into tripartite probability distribution (classical probability)
   5.1.find a tripartite probability distribution between Alice, Bob and Eve that has a non-zero key cost, while not allowing to distill any secret key?
      5.1.1.Find the meaning of that.