Bound Information

Search of a Classical Analog to
Bound Entanglement

Luca Dolfi
Advisor: Prof. Stefan Wolf
Tutor: Arne Hansen

A thesis presented for the degree of
BSc in Informatics

Department of Informatics
Università della Svizzera Italiana
Spring 2018

Abstract

There is a correspondence between entanglement distillation in quantum mechanics and classical key agreement in information theory. In the quantum-mechanical framework there are, furthermore, non-distillable, but entangled quantum states — that is, states sharing bound entanglement. So, considering the above analogy, does there exists some notion of bound information? As of today this remains an open question. In this project we follow the intuition from bound entanglement, the related measures and their connections to concepts of classical key agreement, as well as related information-theoretical concepts, in order to further investigate this open question. We also look at a candidate probability distribution for bound information and perform numerical simulations in search for new, possibly better, candidates for bound information.

The structure of the report is as follows: after an explanation of the motivation of the search, chapter 2 explains the basics of key exchange in both classical and quantum mechanical frameworks. A comparison between methods is presented. Chapters 3 and 4 give the foundations for information theoretical concepts needed to understand and work with theoretical security. Chapter 5 summarizes the state of research on bound information and finally chapter 6 presents the numerical analysis conducted on probability distributions.

Contents

Chapter 1

Motivation

The goal of key exchange is to allow Alice and Bob to establish a secure, private channel for communication. For two parties to communicate confidentially, it is first needed to share some secret key between them, so that each party can encrypt and decrypt the communication. If two parties could not establish a secure — as in information theoretic secure — initial key exchange, they cannot communicate with absolute security without the risk of an eavesdropper Eve listening to them. The ultimate goal of Alice and Bob is to achieve a level of privacy, such that no eavesdropper could have information about the communication, even partially.

It has been noticed that these concepts of privacy also appear in nature and the strongest analogy comes from quantum mechanics.[1]From this theory arises the famous *quantum entanglement* that appears to be the equivalent of privacy in many ways. Both phenomena are composed of correlations between known parties that no other person can access or copy. As summed in [17] "If systems are in pure entangled state then at the same time (i) systems are correlated and (ii) no other system is correlated with them." This can be seen as Alice and Bob holding a secret that Eve cannot get to know.

quantum theory	**classical information**
(pure) quantum entanglement	secret classical correlations
quantum communication	secret classical communication
classical communication	public classical communication
entanglement distillation	classical key agreement (CKA)
local actions	local actions
bound entanglement	bound information ?

Table 1.1: Table showing key QM concepts and their analog in classical key agreement, following [5].

[1]While those analogies are present in many sources, they can be found summed up in

From table 1.1 we see that some of the resources and operations of QM have a bijective analog in classical information theory. Such a (close) relation suggests that the two theories can be viewed together and to use one to better understand the other. It is important however to point out that quantum entanglement and its effects *are not* a quantum manifestation of classical effects and one theory does not prove the other. There are limitations to the correspondences. For example there is no known instance — and it is believed to not exist – of a classical correspondence to super-dense coding (a quantum effect). Other entities like a classical correspondence to bound entanglement, *bound information*, are not excluded a priori and remain yet to be observed or disproved.

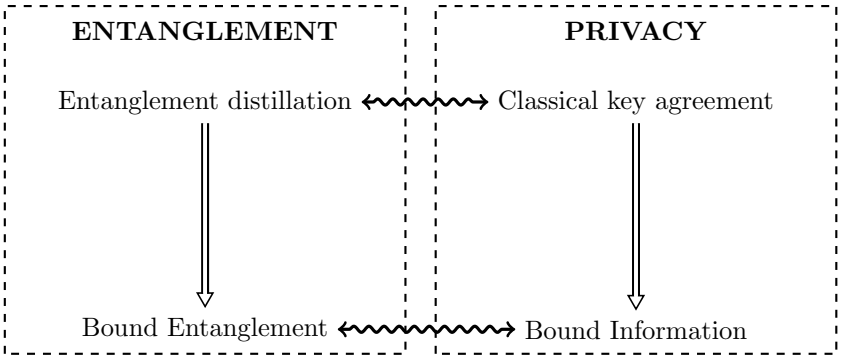


Figure 1.1: Certain aspects of quantum mechanics can be mapped to classical information theory.

An open question has remained over the years asking whether bound information exists in the classical regime. Should this resource exists, it would be — by definition — unusable to generate any key from it. Nevertheless the existence of a resource with bound information might lead to interesting bounds on information theoretical key exchange. To summarize, we are interested in the following question:

The Question

> Is there a tripartite probability P_{ABE}, corresponding to Alice and Bob wanting to establish a key unknown to Eve, that has some *cost* associated to it to create it, but has 0 possible key bits extractable from it?

the paper by Collins and Popescu [5], which also shortly addresses the question of bound information.

Chapter 2

A Common Key Exchange Problem

2.1 What is a shared key?

The first step towards understanding *bound information* is looking at the end product of a key exchange. The secret key is what we want to obtain from a protocol, so we must understand what we are after. What is then a shared key? How do we define a common secret shared between Alice and Bob than can be used formally later on?

Intuitively a common secret is a piece of information (i.e. *bits* of information) known to trusted parties — for example Alice and Bob — and to none else. In an environment where we allow the presence of an eavesdropper Eve that makes observation on the communication reaching such state is not always trivial. There exist methods and protocols to generate such secrets, even from nothing, although they reach different levels of secrecy. A notable one is the famous Diffie-Hellman method to generate a common cryptographic key [8] . We discuss in section 2.4, while still secure, it is not *information theoretical secure*. Here we provide a mathematical definition of a common secret that makes use of concepts that will be explained later in chapter 4.

Definition 1. Let X, Y, Z, S be random variables on the same range $\mathcal{X}$. Let X be owned by Alice, Y by Bob and Z by Eve. Then if

$$P[X = Y = S] > 1 - \epsilon \qquad \text{(common)}$$

$$\mathrm{I}(X; Z) = 0 \ \wedge \ \mathrm{I}(Y; Z) = 0 \qquad \text{(secret)}$$

for all $\epsilon > 0$ we say Alice and Bob share a common secret.

The first part defines the *common* property: X and Y — Alice and Bob's variables in the system — must be asymptotically the same, i.e. the probability that they are the same comes arbitrarily close to 1 for an arbitrarily large number of realization. The second part states that the amount of information Eve can gather about X and Y, through it's realization of Z, is zero.

2.2 The analogy with entanglement

A fascinating feature that arises from quantum mechanics is quantum entanglement. As Einstein, Podolsky and Rosen pointed out almost a century ago [10], the measurement of entangled states defies the classical understanding of a state. They concluded that the theory is incomplete and has to be replaced. Bell responded to that with *non-locality*[2]: there are probability distributions for which there is no local hidden variable model, i.e. exactly what EPR are chasing for. As quantum mechanics gives rise to such non-local probability distributions we cannot hope to find a "local hidden variable model" replacing quantum mechanics.

For a quantum system to exhibit non-locality, entanglement is necessary. Consider two pure quantum states $|\psi\rangle_A$ and $|\phi\rangle_B$. The composite system of the two states is

$$|\psi\rangle_A \otimes |\phi\rangle_B = |\psi\phi\rangle_{AB} \tag{2.1}$$

States that can be represented as in Eq. 2.1 are called *separable*. Not all states are separable. Non-separable states are called *entangled*. Consider now the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right) = |\Psi^-\rangle_{AB} \tag{2.2}$$

for it there is no decomposition into (indices are omitted)

$$\begin{aligned}\frac{1}{\sqrt{2}}&\left((\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)\right) \\ &= \frac{1}{\sqrt{2}}\left(\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\right)\end{aligned} \tag{2.3}$$

that satisfies

$$\alpha_0\beta_0 = \alpha_1\beta_1 = 0 \tag{2.4}$$

$$\alpha_0\beta_1 = 1 \tag{2.5}$$

$$\alpha_1\beta_0 = -1 \tag{2.6}$$

This is an entangled state[1].

Furthermore, if Alice measures to have $|0\rangle$ on her part of the system, then Bob, using the same measurement basis, by non-locality, will measure $|1\rangle$. The other option of measuring $|1\rangle$ for Alice and $|0\rangle$ for Bob is also equally probable. Alice and Bob's values are always (anti-)correlated, regardless of which of the measurements is obtained (which is random).

Quantum entanglement possesses one more feature that classical correlation does not have: the monogamy of entanglement [18]. As Koashi and Winter state in their paper a fundamental difference is that classical correlation can be shared, while quantum entanglement can not. This translates to the case where an eavesdropper Eve listens to the message exchange between Alice and Bob:

[1] This particular state is called "singlet" and is one of the four Bell's basis presented in [2]

in the classical communication there is no direct way for Alice nor Bob to know that Eve is listening (i.e. *shares the correlation*), while in the second case Eve breaks the existing correlation between Alice and Bob. These two aspects of quantum entanglement — correlation and monogamy — give a valid framework for the establishment of a private channel between parties.

2.3 Examples of key exchange

Exchanging keys for encryption was once done *physically*, requiring the parties to meet and assure that no eavesdropper was present. Modern cryptographic systems make use of protocols over telecommunication channels. In both cases the result at the end is that the trusted parties leave (or terminate the protocol) with a bit of information that they know it will be known only to them. Here we present examples for both classical and quantum mechanical channels and compare them. The intention is to compare them and discuss on the different level of security – computational, physical and information theoretical — one might achieve with the correct implementation of one of those.

2.3.1 The Diffie-Hellman key exchange

A famous and widely used method for the exchange of cryptographic keys is the Diffie-Hellman (DH) key-exchange method. The whole process can be summarized in five basic steps [8]:

1. Alice and Bob *publicly* communicate and agree on two numbers, that will serve as basis for the computations.

2. Each party generates *locally* a personal and distinct secret (s_A and s_B) without ever communicating it .

3. They mix their own secret with the common agreed basis, producing a result R_A and R_B. The mathematical properties of this operation make it so it is computational infeasible to go back and retrieve the secrets s from R.

4. Both parties exchange *publicly* their result. Each party now know both the result of the other and their own.

5. Each party applies their secret to the received R. The outputs are equal for Alice and Bob so they can use this result as a common secret to create a key.

[1] A quantum state in quantum mechanics describes a single and isolated quantum system. This can be for example an electron or a photon. For our purposes, a quantum state is always abstracted as a *qubit* or multiple qubits, as described in appendix B

[1] There are known protocols that achieve that, for example in [11] or [3]

The parts exchanged over the public channel — the ones that Eve knows — are only the mutually agreed base and the two partial mixtures. It can be proven that those two elements alone give no information about the complete shared secret and that it is virtually impossible (within reasonable amount of time and use of resources) to obtain the correct final product with only those two.

2.3.2 The BB84 protocol

Protocols for the exchange of keys over a quantum channel have been invented [3, 11]. These protocols work on the underlying physics of quantum mechanics. Alice and Bob need then to have access to a quantum channel to exchange quantum states [2]. Here follows the BB84 protocol as described in [22] :

1. Alice chooses $(4 + \delta)n$ data bits.
2. Alice chooses a random $(4 + \delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or with the diagonal basis $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ if b is 1.
3. Alice sends the resulting state to Bob.
4. Bob receives the $(4+\delta)n$, announces *publicly* this fact, and measures each qubit in the X or Z basis at random.
5. Alice announces *publicly* b.
6. Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol and restart). They keep $2n$ bits.
7. Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which basis she selected.
8. Alice and Bob announce *publicly* and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9. Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

2.3.3 The one-time Pad

The one-time pad is not a key exchange method, but a technique to encrypt a message once the key is obtained. Here is presented as an example of utilization of a key previously exchanged with some other secure algorithm. The message obtained from the OTP is as secure as the method that produced the key. This

[2] A quantum channel is anything that can carry quantum states between two points. For example an optical fiber that carries photons.

means that if the key is provided to be information theoretical secure, then Eve is *completely factored out* from the information contained in the message. Shannon proved in [24] the perfect security of OTP. Figure 2.1 illustrates an example over a 5-bits string. It is important to notice that in order for to OTP to function correctly the key has to be perfectly random and at least of the same size of the message.

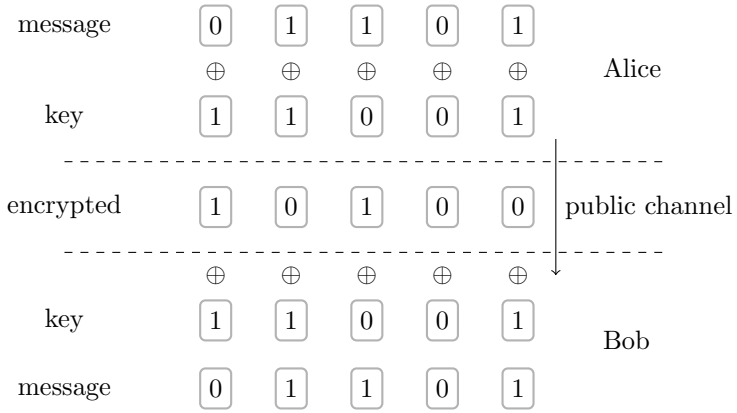


Figure 2.1: The one-time pad. In order to get true security the key should change each time for each message.

2.4 A comparison between securities

A point can be made comparing these different way of establishing privacy. The majority of cryptographic systems used are built on computational complexity security. When Shannon laid out the basis of information theory in [24] in 1949, he affirmed that the highest level of security (information theoretical security) can only be achieved by sharing a secret key from the beginning. Maurer later expanded this concept saying that it is not possible to obtain an information theoretical secure key from just a protocol through local operations and public communications[19]. A starting initial correlation must be provided.

Even though the Diffie-Hellman method does start from nothing, it does not violates Maurer's statement. The key produced by DH is not information theoretical secure. Step 3 enumerated above relies on computational complexity. The difficulty of breaking this step — thus accessing the correlation between Alice and Bob — is bounded only by the length of the number chosen one one side and the computational power available to the adversary on the other. This means, for example, that one cannot use a key obtained through Diffie-Hellman (DH) to generate an information theoretical secure key: as DH starts from nothing, a protocol R constructed to start as DH and producing information

theoretical secure key with LOPC will violate the statement that no key can be crated by LOPC alone. The BB84 protocol works differently, but also does not violate Maurer. Albeit Alice and Bob share, at the end of the protocol, a key starting from nothing, and the secret is in theory information theoretical secure — it can be arbitrarily close —, it does not so with public (classical) communication. Alice utilizes a quantum channel to pass the states to Bob, which is not public because of the monogamy of entanglement. The communication part in BB84 over a classical channel serves only to check for the presence of an enemy Eve, not to modify the secret — which is already transferred at this point. Thus the key is created only through a quantum channel, which is not covered by Maurer's claim.

2.5 The equivalent of CKA in QM

What we were trying to do was to factor out Eve from Alice and Bob's point of view. The goal of classical key agreement (CKA) is also to create a private correlation between Alice and Bob, from one that also includes Eve. We already stated that entangled states can provide this level of privacy [11]. However pure entangled states are very fragile and do not occur in nature. The more general quantum state is a mixed state. A mixed state is a convex mixture of pure states with their probability. A mixed state is represented by a density matrix, defined as a positive, trace-1 operator. By the spectral theorem they can then be wrote in the form of

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad |\psi_i\rangle : \text{ state with probability } p_i \tag{2.7}$$

and interpreted as a statistical Assume that Alice and Bob start with a state $|\psi_{ABE}\rangle$, which is also mixed with a part owned by Eve. Is there a way to factor her out the state, so that they obtain

$$\rho_{AB} = \mathrm{Tr}_E \, |\psi_{ABE}\rangle\langle\psi_{ABE}| \tag{2.8}$$

with

$$\rho_{AB} \otimes \rho_E \tag{2.9}$$

after a series of local operations and classical communication (LOCC)? Quantum distillation is a process that allows that. If Alice and Bob have maximally entangled states after distillation then they know — by the monogamy of entanglement — that Eve is factored out. In other words, the state Alice and Bob have is product with the environment and entangled among them. The joint probability distribution P_{ABE} falls similarly into a product $P_{AB} \cdot P_E$ after a CKA protocol. However from within P_{AB} we cannot decide whether Eve is factored out or not in classical key agreement.

To measure entanglement one might consider the least number of maximally entangled bipartite quantum states required to prepare a density matrix ρ_{AB} by local operations and classical communication. Similarly one might measure

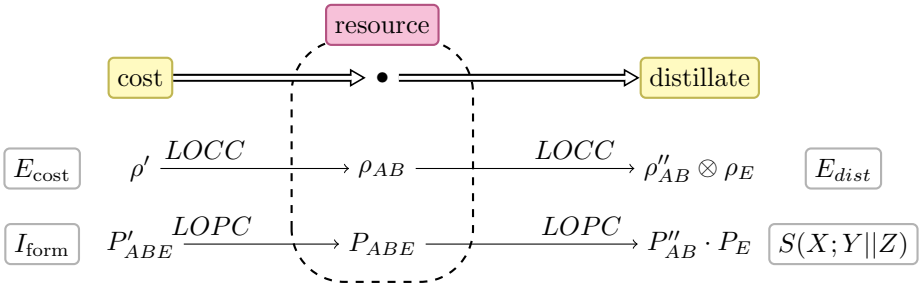


Figure 2.2: Entanglement distillation and CKA utilize a resource (mixed state or probability distribution) to produce a distillate that factors out Eve.

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. The first is called *entanglement cost* or *entanglement of formation*; the second describes the *distillate entanglement*. We will discuss the classical counterparts, namely the *information of formation* and the *secret-key rate*. Figure 2.2 illustrates the analogy between the resource, distillate and cost. This is part of the intuition that leads to bound information.

Chapter 3

Information Theoretical Model of Cryptography: Random Variables

3.1 The abstraction through random variables

We have mentioned many times the idea of *factoring out* the enemy in the previous chapter, but we never actually expressed formally what we meant with that for CKA. In order to make reasoning like this it is needed to model the concepts of *message* and *information* in a computation-able way. Shannon studied this problem and published his results in [24] which is now the foundation of modern information theory and cryptography.

Let us suppose that over a certain alphabet there exist messages $M_1, M_2, \ldots M_n$ and each message has a probability $P(M_i)$ to be chosen (i.e. transmitted). Each message M_i is encrypted into its counterpart E_i. An enemy intercepts E_i and can therefore calculate the probability of message M_i corresponding to the received encrypted version; namely the conditional probability $P(M_i|E_i)$. Shannon states that to obtain perfect secrecy of the message $P(M|E)$ must equal $P(M)$ for all E and all M. From Bayes' formula

$$P(M|E) = \frac{P(M)P(E|M)}{P(E)} \tag{3.1}$$

it follows that $P(E|M) = P(E)$ is an equivalent condition for perfect secrecy. That is, the probability of the cipher-text E must be independent of knowing the message M. This translates into the case where intercepting the encrypted message gives the enemy no information.

Now imagine the message is transmitted by a satellite to Alice and Bob. Eve is also listening. This is an example of a public channel. We end up with three versions of the message[1]: Alice's version X, Bob's Y and Eve's version Z. To

express the whole space of combinations of possible messages, we need the joint probability P_{XYZ}. Then the idea of "factoring out Eve" takes the meaning of obtaining

$$P_{XYZ}(x, y, z) = P_{XY}(x, y) \cdot P_Z(z) \; \forall x, y, z \tag{3.2}$$

so that the marginal of P_{XYZ} over Z — i.e. the part of the distribution owned by Eve — is now product with variables X and Y. Z is independent from X and Y.

Information theory builds on probability theory, which provides us with useful measures and rules to operate on those probabilities. The most important to us are the marginal $P_X(x)$ of joint probabilities $P_{XY}(x, y)$, the entropy $\mathrm{H}(X)$, the correlation and mutual information $\mathrm{I}(X;Y)$ of random variables.

3.2 Local operations and public communication (LOPC)

By local operations and public communication we mean operations carried out on bit strings sampled from $P_{XYZ}(x, y, z)$ and can then be modeled as channels. We can mix different distributions together or trace out the marginal. Communication over an actual realization of a channel is noisy. That noise is also a form of operations on the probability distribution. Operations can also be carried out directly by the parties. This is of more interest because we have control over those operations.

Take for example the Diffie-Hellman method illustrated in section 2.3.1. steps 1 and 4 are *public communication* and steps 2,3 and 5 are *local operations*. Local operations are conducted privately, meaning that everything that happens is only accessible to the party conducting the operation. Other parties can not know what a local operation involved. Public communication is everything that is communicated in clear by parties, or that an eavesdropper can intercept. The totality of what an enemy knows from a protocol — apart from the functioning of the protocol itself — comes from public communication and the partial trace. Through public communication Alice and Bob can also send instructions on what to do in their local operations, like in BB84.

3.3 Secret-key rate

The secret-key rate $S(X;Y||Z)$ is roughly a quantification of the maximal amount of correlated bits between Alice and Bob extractable from an arbitrarily large number of independent realizations of a distribution P_{XYZ} that are not known to Eve. It was introduced by Maurer in [19] to prove lower bounds on the achievable size of a key shared by Alice and Bob in secrecy. It can be seen as a classical analog of the *distillable entanglement* in [4]. Formally the secret key rate is defined as follows.

[1] Ideally the three messages are identical, but just consider that the message is sent through a noisy channel: each receiver will have slight variations of the message, hence the distinction.

Definition 2. [19, 23] Let P_{XYZ} be a joint probability distribution. The secret-key rate $S(X;Y||Z)$ of X and Y with respect to Z is the largest $R \in \mathbb{R}$ such that for all $\epsilon > 0$ there exists a protocol, that involves a sufficiently large number N of realizations of X^N of X and Y^N of Y, that satisfies: Alice and Bob compute, at the end of the protocol, random variables S_A and S_B, respectively, with range $\mathcal{S}$ such that there exists a random variable S with the same range and

$$\mathrm{H}(S) = \log |S| \geq RN \ ,$$

$$P[S_A = S_B = S] > 1 - \epsilon \ ,$$

$$\mathrm{I}(S; CZ^N) < \epsilon$$

Here C is the totality of the protocol public communication; $\mathrm{I}(S; CZ^N)$ is the mutual information between the secret key and what the eavesdropper Eve knows (ref. 4.1).

The secret-key rate is a useful measure of the amount of extractable secrecy — hence, key bits — from a protocol with LOPC. It would be ideal to be able to express it as a function $S(X;Y||Z) = S(P_{XYZ})$. Instead, it can be bounded by two functions[19]

$$S(X;Y||Z) \leq \min[\mathrm{I}(X;Y),\, \mathrm{I}(X;Y|Z)] \tag{3.3}$$

$$S(X;Y||Z) \geq \max[\mathrm{I}(Y;X) - \mathrm{I}(Z;X),\, \mathrm{I}(X;Y) - \mathrm{I}(Z,Y)] \tag{3.4}$$

Those are not tight bounds. In fact in Eq. 3.4 the secret-key rate can be positive even when the right-hand side is negative.

Chapter 4

Measures of Correlation and Their Bounds

4.1 Mutual information

The mutual information measures the amount of information that X and Y *share*. It can be used as a measure of correlation (or dependency) between random variables. Intuitively we can use the mutual information — along with a check of privacy against Eve — to measure how much shared key two random variables X and Y can hold.

Definition 3. Let X and Y be two jointly distributed random variables. Then the mutual information of the random variables is the relative entropy — a measure of distance between probability distributions — between the joint distribution $P_{XY}(x, y)$ and the product distribution $P_X(x) \cdot P_Y(y)$.

$$\mathrm{I}(X;Y) = \sum_{y\in\mathcal{Y}} \sum_{x\in\mathcal{X}} p(x,y) \log\left(\frac{p(x,y)}{p(x)p(y)}\right) \tag{4.1}$$

or equivalently, showing its relation to the entropies of the random variables

$$\mathrm{I}(X;Y) = \mathrm{H}(X) - \mathrm{H}(X|Y) = \mathrm{H}(X,Y) - \mathrm{H}(X|Y) - \mathrm{H}(Y|X) = \mathrm{H}(Y) - \mathrm{H}(Y|X) \tag{4.2}$$

This relation can be seen more directly in Fig. 4.1.

Mutual information is nonnegative and bounded by the entropy of random variable X

$$0 \leq \mathrm{I}(X;Y) \leq \min\left(\mathrm{H}(X), \mathrm{H}(Y)\right) \tag{4.3}$$

In this sense the mutual information can also be interpreted as how much information X gives about Y, thus being bounded by its own entropy.

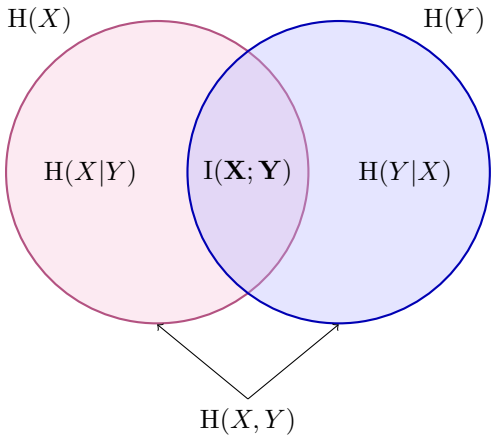


Figure 4.1: Representation of mutual information $\mathrm{I}(X;Y)$ in relation with entropies $\mathrm{H}(X)$ and $\mathrm{H}(Y)$ and joint entropy $\mathrm{H}(X,Y)$ of the random variables .

4.2 An eavesdropper that can choose the best channel to listen to

Additional information on a third random variable Z can increase or decrease the mutual information [7]. The *conditional mutual information* $\mathrm{I}(X;Y|Z)$ is the expected value of the mutual information of X and Y given a realization of a third variable Z. In a context of key exchange, we can interpret this as the remaining correlation between honest parties after the observations of an attacker Eve. What if Eve tried to minimize this, i.e. tried to find the best viewpoint possible over the communication between Alice and Bob?

Definition 4. [20, 23] Let P_{XYZ} be a discrete probability distribution. Then the intrinsic information between X and Y given Z is

$$\mathrm{I}(X;Y\downarrow Z) := \inf_{Z\to\bar{Z}} \mathrm{I}(X;Y|\bar{Z}) \tag{4.4}$$

The infimum is taken over all possible channels applied to Z (the choice of a channel can be seen as the choice of a point of view for Eve).

The intrinsic information is an upper bound to the secret-key rate, although not tight [23].

$$S(X;Y||Y) \leq \mathrm{I}(X;Y\downarrow Y) \tag{4.5}$$

Refer to the next chapter to see an analysis of the gap between the two measures. The amount of secret bits Alice and Bob can extract from the distribution is then bounded by how much the attacker Eve can disrupts their conditional mutual correlation. Intrinsic information is also a lower bound to another measure, *information of formation*, which is the amount of initial secret bits between Alice and Bob required to create the distribution P_{XYZ} with LOPC.

4.3 When correlation is unusable

Setting the bound in Eq. 4.5 we can see that not always factoring out the adversary can be enough to be able to produce a key. For example we could have

$$S(X;Y||Z) = 0$$
$$\mathrm{I}(X;Y\downarrow Z) > 0$$

meaning that there exists some sort of mutual correlation between Alice and Bob, but they share no key. Whether this case is possible is the question of bound information expressed at the beginning of this work.

Definition 5. [13, 23] Let P_{XYZ} be a joint probability distribution for parties Alice, Bob and Eve. For such distribution let

$$\mathrm{I}(X;Y\downarrow Z) > 0 \tag{4.6}$$

and

$$S(X;Y||Z) = 0 \tag{4.7}$$

hold. Then P_{XYZ} is said to have *bound information*.

Recalling the intuition from quantum mechanics, we now pose the case of the existence of bound entanglement. As stated before (section 2.5), quantum distillation extract from an entangled mixed state a set of quasi-pure entangled states. Pure entangled states can be used as a resource to produce a key for Alice and Bob [11]. There are, furthermore, entangled mixed states that are non-distillable, i.e. no pure entanglement can be extracted from them [15]. Bound entanglement is a kind of correlation between Alice and Bob — that can become inaccessible to Eve — but nevertheless of no use for generating a secret (quantum) key. So in the quantum regime this questions has already been answered.

Chapter 5

State of Research

The question of the existence of an analog to bound entanglement was firstly posed in [13] by Gisin and Wolf, where they analyzed comparisons and correspondences between quantum and classical protocols for key agreement. The question about bound information was a consequence of these correspondences. Since then the topic was picked up by the scientific community of quantum cryptography. A probability distribution that presents bound information has not been found yet.

5.1 Tripartite bound information

A later work by Acín et al. proposed the existence of bound information in a tripartite case [1]. They analyzed the probability distribution resulting from measurement of a known bound entangled state. Furthermore they also show that this distribution can be *activated*[1] the same way as in quantum entanglement. This result is different from what we want to achieve because the probability distribution is divided among parties Alice, Bob and Claire, with Eve being a fourth party in the distribution. In fact, their result of bound information is valid only when considering *pairs* of honest parties from the original distribution.

5.2 The gap between the bounds can be arbitrarily large

To distinguish and analyze the case of bound information some information theoretical measures are needed. We saw the secret key rate (section 3.3) and the intrinsic information (section 4.4) and we already presented the question of

[1] The activation of entanglement can be roughly described as the process through which entanglement can become a useful resource for nonclassical tasks. Horodecki *et al.* demonstrated the activation of bound entanglement in [16]

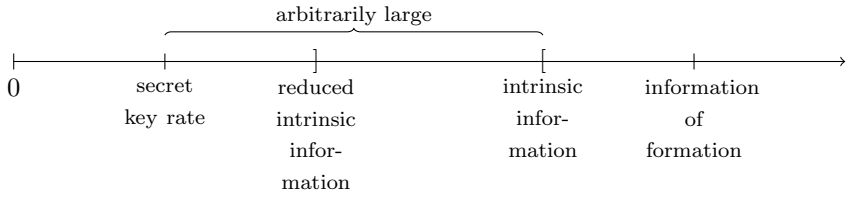


Figure 5.1: The different measures for P_{XYZ} and how they bound each other.

bound information in terms of such measures. In [23] a new measure of *reduced intrinsic information* $\mathrm{I}(X;Y \downdownarrows Z)$ is introduced as an upper bound on secret key rate, lower than the intrinsic information.

Definition 6. [23] Let P_{XYZ} be a a discrete probability distribution. The reduced intrinsic information of X and Y given Z is defined as

$$\mathrm{I}(X;Y \downdownarrows Z) := \inf_{P_{U|XYZ}} (\mathrm{I}(X;Y \downarrow ZU) + \mathrm{H}(U)) \tag{5.1}$$

and for every P_{XYZ} it holds

$$S(X;Y||Z) \leq \mathrm{I}(X;Y \downdownarrows Z) \leq \mathrm{I}(X;Y \downarrow Z) \tag{5.2}$$

Reduced intrinsic information is a stronger upper bound on secret key rate than intrinsic information. More importantly, Renner and Wolf proved that the gap between reduced and normal intrinsic information (hence also between the secret-key rate and intrinsic information) can be arbitrarily large for distributions where the range of X, Y and Z can be arbitrary large[23]. Considering then that the former is an upper bound to secret key rate, and the latter is a lower bound to information of formation, this implies then the existence of asymptotic bound information.

Definition 7. [23] Let $P_{X_{(n)}Y_{(n)}Z_{(n)}}$ be a an arbitrary discrete n-ary probability distribution. Then the distribution is said to have *asymptotic bound information* when

$$\mathrm{I}(X_{(n)};Y_{(n)} \downarrow Z_{(n)}) \to c > 0 \tag{5.3}$$

and

$$S(X_{(n)};Y_{(n)}||Z_{(n)}) \to 0 \tag{5.4}$$

for $n \to \infty$.

5.3 A candidate probability distribution

Wolf and Renner proposed in [23] for the first time a probability distribution (Fig. 5.2) which is a valid candidate for the classical analogy of *bound entanglement*. In fact, they offer a probability distribution that asymptotically has

Y \ X	0	1	2	3
0	1/8	1/8	0	0
1	1/8	1/8	0	0
2	0	0	1/4	0
3	0	0	0	1/4

$$Z \equiv X + Y \ (mod\, 2) \ \text{ if } X, Y \in \{0, 1\}$$
$$Z \equiv X \ (mod\, 2) \ \text{ if } X \in \{2, 3\}$$
$$U \equiv \lfloor X/2 \rfloor$$

Figure 5.2: Probability distribution proposed by Renner, Wolf and Skripsky in [23] for which it holds that $S(X;Y||Z) \neq \mathrm{I}(X;Y\downarrow Z)$

bound information. This example did not come directly from a translation of bound entangled states. Moreover hey also show, for such a distribution, that

$$S(X;Y||Z) \neq \mathrm{I}(X;Y\downarrow Z) \tag{5.5}$$

and they emphasize that this is the first time that equality does not hold. This fact disproved the conjecture posed in [20], that the two measured were actually the same.

For this probability distribution we have

$$\mathrm{I}(X;Y\downarrow Z) = 3/2,\ S(X;Y||Z) = 1,\ \mathrm{I}(X;Y\downdownarrows Z) = 1$$

With the the fact that $\mathrm{I}(X;Y\downdownarrows Z) = S(X;Y||Z)$ does hold, and with the statements above, we can think of a model to later search for bound information in chapter 6. If the reduced intrinsic information is a useful measure, we can minimize it to find probability distributions that have no possible key extractable from it. A condition to be a useful measure is that it must have the same lower bound as the secret-key rate. As we will see in section 6.3 however, there are some conditions on the reduced intrinsic information that does not allow it to be a good measure.

More promising is a family of probabilities on a parameter $a > 0$ they mention at the end (Fig. 5.3) which is a slight modification of the first. Here Renner and Wolf conjecture that it might be possible to achieve bound information by different values of a. They also noted, however, that for a too big the correlation between Alice and Bob is lost, loosing also the key cost value (or information of formation).

Y \ X	0	1	2	3
0	1/8	1/8	a	a
1	1/8	1/8	a	a
2	a	a	1/4	0
3	a	a	0	1/4

$Z \equiv X + Y \ (mod\, 2)$ if $X, Y \in \{0, 1\}$
$Z \equiv X \ (mod\, 2)$ if $X, Y \in \{2, 3\}$
$Z = (X, Y)$ otherwise

Figure 5.3: A candidate probability distribution for bound information, for $a \geq 0$ (and renormalized).

Chapter 6

A Numerical Analysis of Candidate Distributions

Towards the end of the project we decided to implement a python module to do testing and analysis on some candidate probability distributions. The motivation for this was given mainly by the results showed again in [23].

6.1 Analysis design and goals

To visualize and motivate the scope of this analysis we expand Eq. 5.2 as follow

$$S(X;Y||Z) \leq \mathrm{I}(X;Y \downdownarrows Z) \leq \mathrm{I}(X;Y \downarrow Z) \leq I_{form}(X;Y|Z) \tag{6.1}$$

including also the information of formation. As mentioned before, obtaining a value for the secret-key rate and information of formation — the fundamental quantities for key agreement — requires a *possible* protocol. For their bounds (i.e. the central parts of the inequality) we can obtain direct numerical values from the probability distribution alone. The aim of this part of the project is then to take a candidate as given in Fig. 5.3 and trace the values of the reduced and normal intrinsic information for variation of the probability distribution.

A good result we hope to obtain is a probability distribution for which the reduced measure tends to 0, while the intrinsic information remains larger than 0, bounding also the information of formation to be greater than 0. Due to the tightness of the bounds, this will constrain the value for the secret key rate down to (possibly) 0, while keeping a non-zero key cost (I_{form}). This will lead to a new candidate for bound information.

In order to perform analysis on those measures we firstly had to implement a library of modules that dealt with the probability and information theory aspects. Following criteria for separability of quantum states, a quantum me-

chanics module was also implemented to translate and later tests the distributions from the quantum to classical regime. The intrinsic information (and its reduced counterpart) is defined as an *infimum* over the set of tripartite probability distributions. To find a correct value it would require to solve an optimization problem. The definition given in section 4.4 however does not allow us to formulate the problem as convex, or, at least, not a trivial one, since the mutual information is only convex for a fixed term. We decided then to adopt a Monte-Carlo method to estimate them.

For each step — i.e. for each variation — of the candidate base probability, the values of

- mutual information
- intrinsic information
- reduced intrinsic information
- trace over quantum state witness given in [9]

are estimated.

6.2 Different noises analysis

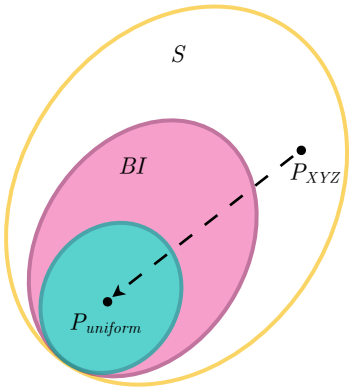


Figure 6.1: From the set S of tripartite distributions we create a "path" towards distributions with zero key cost (cyan), going through the ones without extractable key (magenta). The distributions that holds bound information reside in the cyan\magenta part.

The variations of the distribution mentioned above are linear steps toward a noise distribution we define. The first and obvious noise function we tested is the uniform distribution, which acts on all values of P_{XYZ}. Following the idea of the candidate distribution showed in Fig. 5.3 we also utilized a noise function that operates on the non-correlated part for Alice and Bob.

Y \ X	0	1	2	3
0	0	0	a	a
1	0	0	a	a
2	a	a	0	0
3	a	a	0	0

(a) Noise1

Y \ X	0	1	2	3
0	a	a	a	a
1	a	a	a	a
2	a	a	0	0
3	a	a	0	0

(b) Noise2

Figure 6.2: Different noises disturbs different parts of the correlation between X and Y

This method of simulating noise added to a known distribution takes also inspiration from the quantum world. A method to look for bound entangled states applies a noise channel to a known entangled state and then the new state is tested on different separability criteria. The intuition comes from the respectively enclosed convex sets of separable states.

6.3 The problem with the reduced intrinsic information

During the implementation of the module we were confronted with some issues on the measure of the reduced intrinsic information. Recalling Eq. 5.1, we first generate random channels $XYZ \to U$ to get the conditional probability $P_{U|XYZ}$. Then the intrinsic information is minimized over all possible channels $ZU \to \bar{Z}\bar{U}$. Ideally, we want to show how the reduced intrinsic information goes to 0, so that the secret key rate also falls to 0. Thus, $\mathrm{H}(U)$ is a lower bound on the value of the reduced intrinsic information. In order to minimize this lower bound, the marginal P_U should be deterministic and thus $\mathrm{H}(U) = 0$. However for the other term $\mathrm{I}(X;Y\downarrow ZU)$ a deterministic U will result in having the intrinsic information. Intuitively, minimizing on $\mathrm{H}(U)$ increases the value of $\mathrm{I}(X;Y\downarrow ZU)$ and vice versa.

Observing this, we questioned the usefulness of the reduced intrinsic information as a measure to demonstrate the existence of bound information, contrary to we thought at the beginning.

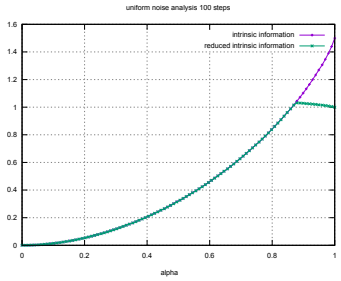
6.4 Results

Despite the difficulties encountered in implementing the code, we were able to produce some marginal results. When the noise functions were applied to the marginal P_{XYZ} of the distribution in Fig. 5.2 we were able to make the following observations

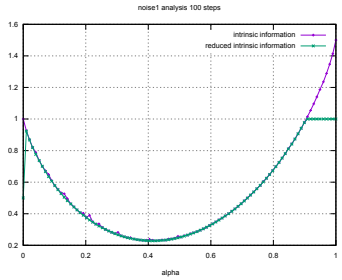
- For the uniform noise, as expected, the behavior presents no intrinsic information nor reduced intrinsic information. The two measures remain the same until around $\alpha = 1 - 1/8 = 0.875$. Around that point the reduced intrinsic information of the behavior *decreases* until reaching 1, as we already knew from [23].

- For the noise in Fig. 6.2a, we notice first of all that the intrinsic information is not monotonic along the path. It takes the form of a convex function with minimum for an α around 0.4. At both ends of the path the two measures diverge resulting in $\mathrm{I}(X; Y \downarrow Z) \approx 1$ and $\mathrm{I}(X; Y \downdownarrows Z) \approx 0.5$ for $\alpha = 0$, i.e. for just the noise function represented in the figure. On the other end we obtain again the results as before for the marginal of the candidate.

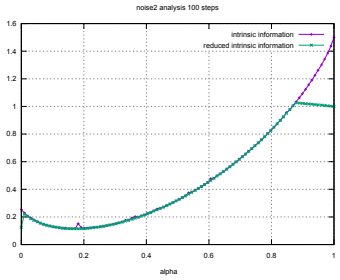
- Finally for the noise function in fig. 6.2b we observe the same general behavior as before. The observable minimum is around values $\alpha = 0.2$ and for just the noise function the reduced intrinsic information falls to about $\mathrm{I}(X; Y \downdownarrows Z) \approx 0.125$ and $\mathrm{I}(X; Y \downarrow Z) \approx 0.25$.



(a) Uniform noise



(b) Noise1



(c) Noise2

Figure 6.3: Results obtained from the application of the different noise functions of Fig. 6.2, applied to the marginal of Fig. 5.2. Each test is conducted over 100 steps between the two behaviors

Chapter 7

Conclusion

Throughout the project, topics of information theory and quantum mechanics were researched thoroughly. We have built an understanding why some aspects of quantum mechanics present an analog in classical key agreement and how they can be used as an intuition in research. Moreover, we have seen how and why the question of bound information remains yet an open question. We researched and understood the measures presented as bounds to define the amount of secrecy a probability distribution among parties can hold, and how much does it cost to build it. Lastly, the implementation of a python library to perform a numerical analysis of candidates was instrumental to observe how the measure of reduced intrinsic information is not a useful measure for the search of bound information.

As future work on the topic, more thought can be put into the usefulness of the reduced intrinsic information measure. The intuitions on the bounds on $\mathrm{H}(U)$ and the minimization of the term $\mathrm{I}(X;Y\downarrow ZU)$ have to be formally stated. The code produced during the project, while providing as a library of functions for the study, was not completed to the intended form, as it only tested the marginal of 5.2 and not the tripartite distribution 5.3. More development can be done in the library to be able to test other candidate tripartite distributions. More tests for separability criteria of the translated quantum states are already being added as a continuation of the work.

Appendix A

Mathematical Framework for QM

Unless stated otherwise, we consider each coefficient to be complex (as in elements of $\mathbb{C}$). Vectors have complex components.

A.1 Inner product spaces

In standard vector notation we define the inner (scalar) product of complex vectors as

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

Where † represents the conjugate transpose.

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

A.2 Tensor product spaces

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:

$$\forall |v\rangle \in V,\ \forall |w\rangle \in W,\ \forall z \in \mathbb{C}$$
$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle$$
$$\forall |v_1\rangle, |v_2\rangle \in V,\ \forall |w\rangle \in W$$
$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1 w\rangle + |v_2 w\rangle$$
$$\forall |v\rangle \in V,\ \forall |w\rangle \in W,\ A : V \to V'\ B : W \to W'$$
$$(A \otimes B)\left(\sum_i a_i |v_i w_i\rangle\right) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$$

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

Appendix B

Quantum Mechanics

"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 $|1\rangle$." [22]

B.0.1 The three postulates

[1]

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

Postulate 2: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle$$

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of *measurements operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occur is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \ ,$$

[1] 22.

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} .$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I .$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle .$$

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.

B.1 Dirac's bra-ket notation

Every pure quantum state can be represented as vector in a vector space with inner product, i.e. a *Hilbert space*. A complex Hilbert space $\mathcal{H}$ of dimension n is isomorphic to $\mathbb{C}^n$ with the standard inner product. In $\mathbb{C}^n$ one can choose a basis and then represent vectors with coordinates with respect to this basis. The bra-ket notation is a handy notation introduced by physicist Paul Dirac to deal with such vector representation of quantum states. First of all we note that a state $\varphi' \in \mathcal{H}$ corresponds via the isomorphism to $\varphi \in \mathbb{C}^n$. It can be represented as a vector with respect of some basis as follows

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

$$\langle\varphi| = \begin{pmatrix} \varphi_1 & \varphi_2 & \dots \end{pmatrix} \text{ is a row "bra" vector over } \mathcal{H}$$

To be representative of a quantum state the vector has to have unitary length, $\|\varphi\| = 1$. Furthermore the conjugate transpose of a *bra* vector is the corresponding *ket* vector, and vice versa.

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

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

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

which are recognizable as the equivalent of $\vec{e_1}$ and $\vec{e_2}$ in $\mathbb{C}^2$.

To summarize then, $|\varphi\rangle$ represents a column vector on a complex vector space with inner product equivalent to $\mathbb{C}^n$ in some basis, and $\langle\varphi|$ is its complex conjugate.

So if we define the matrix[2] $A = |w\rangle\langle v|$ we observe that

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

which is a 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* $|v'\rangle$. 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 intuition of this is that $|w\rangle\langle v|$ can indeed be defined as a (linear) operator from the vector space of $|v\rangle$ to the vector space of $|w\rangle$.

B.2 Measurements on a basis

To get any information out of a state 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 its 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 — measuring with the same basis — find out what the choice of i was. If the states are not orthonormal there is no quantum measurement capable of distinguishing the states. If the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, then $|\psi_2\rangle$ has a component orthogonal to $|\psi_1\rangle$, and also a component parallel to it. This will lead to a non-zero probability of measuring a value on $|\psi_1\rangle$ for the state $|\psi_2\rangle$.

Example 1. [22]

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

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 $p_{-1} = \frac{1}{2}$

Linear operators

A linear operator between two vector spaces is defined as

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

[2]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.

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

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 *Pauli 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.

B.3 Mixed states

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

$$|\psi\rangle \text{ is a state vector } \Rightarrow |\psi\rangle \in \mathcal{H} \text{ and } |\langle\psi|\psi\rangle| = 1$$

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 because of the 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 $\mathrm{Tr}(\rho) = 1$ and all eigenvalues of ρ are positive. Moreover ρ is a linear combination of projectors $|\psi_i\rangle\langle\psi_i|$ which makes $\rho \in \mathbb{P}(\mathcal{H})$ a projector itself on the the Hilbert space.

Bibliography

[1] Antonio Acin, J Ignacio Cirac, and Ll Masanes. "Multipartite bound information exists and can be activated". In: *Physical review letters* 92.10 (2004), p. 107903.

[2] John S Bell. "Physics 1, 195 (1964)". In: *Google Scholar* (1966).

[3] H Bennett Ch and G Brassard. "Quantum cryptography: public key distribution and coin tossing Int". In: *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*. 1984, pp. 175–9.

[4] Charles H Bennett et al. "Mixed-state entanglement and quantum error correction". In: *Physical Review A* 54.5 (1996), p. 3824.

[5] Daniel Collins and Sandu Popescu. "Classical analog of entanglement". In: *Phys. Rev. A* 65 (3 Feb. 2002), p. 032321. DOI: 10.1103/PhysRevA.65.032321. URL: https://link.aps.org/doi/10.1103/PhysRevA.65.032321.

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

[7] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[8] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[9] Andrew C Doherty, Pablo A Parrilo, and Federico M Spedalieri. "Complete family of separability criteria". In: *Physical Review A* 69.2 (2004), p. 022308.

[10] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" In: *Physical review* 47.10 (1935), p. 777.

[11] Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical review letters* 67.6 (1991), p. 661.

[12] Nicolas Gisin, Renato Renner, and Stefan Wolf. "Bound Information: The Classical Analog to Bound Quantum Entanglemen". In: *European Congress of Mathematics*. Ed. by Carles Casacuberta et al. Basel: Birkhäuser Basel, 2001, pp. 439–447. ISBN: 978-3-0348-8266-8.

[13] Nicolas Gisin and Stefan Wolf. "Linking classical and quantum key agreement: is there "bound information"?" In: *Annual International Cryptology Conference*. Springer. 2000, pp. 482–500.

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

[15] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?" In: *Physical Review Letters* 80.24 (1998), p. 5239.

[16] Paweł Horodecki, Michał Horodecki, and Ryszard Horodecki. "Bound entanglement can be activated". In: *Physical review letters* 82.5 (1999), p. 1056.

[17] Ryszard Horodecki et al. "Quantum entanglement". In: *Reviews of modern physics* 81.2 (2009), p. 865.

[18] Masato Koashi and Andreas Winter. "Monogamy of quantum entanglement and other correlations". In: *Physical Review A* 69.2 (2004), p. 022309.

[19] Ueli M Maurer. "Secret key agreement by public discussion from common information". In: *IEEE transactions on information theory* 39.3 (1993), pp. 733–742.

[20] Ueli M Maurer and Stefan Wolf. "Unconditionally secure key agreement and the intrinsic conditional information". In: *IEEE Transactions on Information Theory* 45.2 (1999), pp. 499–514.

[21] Ueli Maurer and Stefan Wolf. "Towards characterizing when information-theoretic secret key agreement is possible". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 1996, pp. 196–209.

[22] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[23] Renato Renner and Stefan Wolf. "New bounds in secret-key agreement: The gap between formation and secrecy extraction". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2003, pp. 562–577.

[24] Claude E Shannon. "Communication theory of secrecy systems". In: *Bell Labs Technical Journal* 28.4 (1949), pp. 656–715.