Towards Proving the Existence of "Bound" Information

Renato Renner * Stefan Wolf †

Abstract

In order to communicate secretly in the strong sense of information theory, two parties have to share a secret key about which a possible adversary has (virtually) no information. Such a key can be generated based on correlated classical or quantum information shared between the parties. The relationship that has recently been shown between these two models suggests that the concept of bound entanglement, i.e., shared quantum information between the parties which can, however, not be used to generate a quantum key, has a classical counterpart, called "bound information." Such information is a classical correlation between the players' pieces of information (from a possible adversary's viewpoint) that can, however, not be used to generate a secret key. The existence of such information, which could not be proven so far, would be somewhat surprising from the purely classical perspective. In this paper we take a step towards proving the existence of bound information. More specifically, a bidirectional correspondence between quantum and classical key bits (of a certain quality, called fidelity) is shown. Here, the connection between quantum and classical information is established by measuring the quantum system in a fixed basis.

1 Introduction

The separability problem, i.e., the the question whether a state of a composite quantum system contains quantum correlation or entanglement, as well as the distillability problem, i.e., the question whether a state of a composite quantum system can be transformed to an entangled pure state using local operations, are fundamental and well studied, but still unresolved problems of quantum information theory [1]. Recently, it turned out that both of these questions are closely related to classical information-theoretic notions, namely the intrinsic information and the secret-key rate, which are basic quantities in the theory of information-theoretic secret key agreement from common information.

The intrinsic information as well as the secret-key rate are measures on probability distributions: While the former quantifies some kind of correlation between random variables having a certain distribution, the latter is a measure for the maximal rate at which two parties, connected by an insecure (but authentic) channel, can generate common secret bits, if they have access to some correlated information specified by a probability distribution.

The link between these information-theoretic measures and the properties of a quantum state is mainly motivated by the fact that any probability distribution can be considered as resulting from the measurement of a certain quantum state. In [4], and later in [2], it has been shown that the inseparability of a mixed quantum state implies that the intrinsic information of a corresponding probability distribution is positive, and vice versa. On the other hand, evidence has been given in

*Computer Science Department, ETH Zürich, CH-8092 Zürich, Switzerland. Email: renner@inf.ethz.ch.

†Département d'Informatique et R.O., Université de Montréal, Montréal, QC, Canada H3C 3J7. Email: wolf@iro.umontreal.ca. Supported by Canada's NSERC.

the same papers that a similar relation holds between the distillability of a mixed quantum state and the secret-key rate of a corresponding distribution.

In this work we will focus on this latter relation, that is, the parallels between distillability and secret key agreement. We enlighten the close link between the outcome of quantum distillation protocols, i.e., almost perfect qubit pairs, and the outcome of classical secret key agreement protocols, i.e., two classical bits which are equal with high probability and on which an adversary only has negligible information. Our result is a step towards a proof for the existence of bound information, the classical counterpart of bound entanglement.

2 Classical Secret Key Agreement and Quantum Distillation

In [7], Maurer proposed the following setting for information-theoretically secure secret key agreement. Consider two parties (called Alice and Bob), connected by an authentic, but otherwise fully insecure communication channel, such that a possible adversary (Eve) learns the whole communication between them. Additionally, the players (including the adversary) have access to some correlated information which is given by repeated realizations of random variables X (for Alice), Y (Bob) and Z (Eve) jointly distributed according to P_{XYZ}. The goal of Alice and Bob is to generate a common secret key, meaning that they each end up with an identical random bit-string on which Eve has virtually no information.

Similarly, quantum distillation can be described as a game between two players in a quantum system who are connected by a classical communication channel and who can perform arbitrary local quantum operations on their respective subsystems. Additionally, the players have access to mixed quantum states ρ lying in a product space $\mathcal{H}_A \otimes \mathcal{H}_B$ where Alice controls $\mathcal{H}_A$ and Bob $\mathcal{H}_B$. The goal of them is to generate fully entangled qubit pairs.

In [3], it has been shown that for a given probability distribution P_{XYZ}, secret key agreement is possible if and only if there exists a so called *binarization* thereof such that the resulting distribution corresponds to a correlated secret bit pair. This will be made more precise by the following definition and theorem.

Let $P_{\bar{X}\bar{Y}Z}$ be a joint probability distribution of a triple of random variables $(\bar{X}, \bar{Y}, Z)$ where $\bar{X}$ and $\bar{Y}$ are binary, i.e., $\bar{\mathcal{X}} = \bar{\mathcal{Y}} = \{0, 1\}$.

Definition 2.1. *$P_{\bar{X}\bar{Y}Z}$ is said to be a* common secret bit pair distribution (CSBD) with fidelity f *if the random variables $\bar{X}$, $\bar{Y}$ and Z satisfy*

$$\begin{aligned} P[\bar{X} = \bar{Y}] &\geq f \\ |P[\bar{X} = \bar{Y} = 0] - P[\bar{X} = \bar{Y} = 1]| &\leq 1 - f \\ \min(H(\bar{X}|Z), H(\bar{Y}|Z)) &\geq f. \end{aligned}$$

Theorem 2.2. *A probability distribution P_{XYZ} allows for secret key agreement if and only if for each $\varepsilon > 0$ there exists a number N and a binarization, i.e., a pair of ternary-output channels $(P_{\bar{X}|X^N}, P_{\bar{Y}|Y^N})$ with ranges $\bar{\mathcal{X}} = \bar{\mathcal{Y}} = \{0, 1, \Delta\}$, such that $P[\bar{X} \neq \Delta \neq \bar{Y}] > 0$ and $P_{\bar{X}\bar{Y}Z^N|\bar{X}\neq\Delta\neq\bar{Y}}$ is a CSBD with fidelity $f = 1 - \varepsilon$.*

In [6], a similar statement has been proven for the quantum case. Here, fully entangled qubit pairs take the role of the correlated secret bit pairs in the classical setting. In order to use the same terminology, we will give a definition of fidelity for entangled qubits. Let therefore $\mathcal{H}_A$ and $\mathcal{H}_B$ be 2-dimensional Hilbert spaces with basis $\{|0\rangle, |1\rangle\}$ and

$$|\varphi\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

a Bell state in the product space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Since any mixed state in a Hilbert space $\mathcal{H}$ can be expressed as a pure state in a product space $\mathcal{H} \otimes \mathcal{H}_E$ where $\mathcal{H}_E$ has sufficiently large dimension, we will in the following consider pure states in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ instead of mixed states in $\mathcal{H}_A \otimes \mathcal{H}_B$.

Definition 2.3. *$|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is called* entangled qubit state with fidelity f *if*

$$\| |\Psi\rangle - |\varphi\rangle \otimes |\kappa\rangle \|^2 \leq 1 - f$$

for an appropriate state $|\kappa\rangle \in \mathcal{H}_E$.

Note that, expressed in terms of mixed states, the condition that $f \approx 1$ for a quantum state $|\Psi\rangle$ is equivalent to $\|\rho - P_{|\varphi\rangle}\| \approx 0$ for the density matrix $\rho := \mathrm{tr}_{\mathcal{H}_E}(P_{|\Psi\rangle})$.

Theorem 2.4. *A quantum state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is distillable if and only if for each $\varepsilon > 0$ there exists a number N and a pair of projectors (P_A, P_B) onto 2-dimensional subspaces of $\mathcal{H}_A^N$ and $\mathcal{H}_B^N$, respectively, such that $|\bar{\Psi}\rangle := P_A \otimes P_B \otimes \mathbf{1}_{\mathcal{H}_E}^N |\Psi\rangle^N$ is an entangled qubit state with fidelity $f = 1 - \varepsilon$.*

In the next section we will see that correlated secret bit pairs and fully entangled qubit pairs are closely connected. This, together with the above two theorems, suggests that there exists a strong relation between the possibility of secret key agreement for a certain probability distribution and the distillability of a corresponding quantum state.

3 The Link Between Qubits and Classical Secret Bits

A measurement in a quantum system with respect to a fixed basis $\{|x\rangle\}_{x \in \mathcal{X}}$ can be considered as a mapping between the set of quantum states of the system to the set of probability distributions over all possible measurement outcomes, i.e.,

$$M : \quad |\psi\rangle \longmapsto P_X$$

with $P_X(x) = |\langle\psi|x\rangle|^2$ for all $x \in \mathcal{X}$. This function is not one-to-one. However, for an orthonormal basis $\{|x\rangle\}_{x \in \mathcal{X}}$ it is a bijection between the set of all states $|\psi\rangle = \sum_x a_x |x\rangle$ with real non-negative coefficients a_x and the set of all probability distributions over $\mathcal{X}$ with inverse

$$Q := M^{-1} : \quad P_X \longmapsto |\psi\rangle := \sum_x \sqrt{P_X(x)} \cdot |x\rangle.$$

In the previous section, we have seen that the question whether a given quantum state is distillable can be reduced to the question whether there exists some projection onto a fully entangled qubit pair. Moreover, a similar reduction holds for the problem of deciding whether secret key agreement for a given probability distribution is possible. In this case, a correlated secret bit pair takes the role of the fully entangled qubit pair. The two concepts are, however, strongly related. The following theorem states that the bijection Q maps classically correlated secret bit pairs to entangled qubit pairs.

Theorem 3.1. *If $P_{\bar{X}\bar{Y}Z}$ is a CSBD with fidelity $1 - \varepsilon$, then $|\Psi\rangle := Q(P_{\bar{X}\bar{Y}Z})$ is a entangled qubit pair with fidelity $1 - c \cdot \varepsilon$ (for some constant c).*

On the other hand, if a state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is an entangled qubit pair with fidelity $1 - \varepsilon^2$, then $P_{\bar{X}\bar{Y}Z} := M(\Psi)$ is a CSBD with fidelity $1 - c' \cdot \varepsilon$ (for some constant c').

The second part of this theorem (we will not give the proof of this part here due to space limitations) can be interpreted as the well-known fact that two parties can generate a secret key bit by measuring a fully entangled quantum bit pair of which each of them controls one subsystem. On the other hand, it is intuitively clear that the translation of a perfectly correlated secret bit pair (i.e., a CSBD with fidelity 1) to a quantum state leads to a Bell state. However, the interesting fact is that this also holds for a CSBD with fidelity smaller than 1, and that the fidelity of the resulting entangled quantum state is independent of the size of the range of the random variable Z (which in the classical setting specifies the knowledge of an adversary). This turns out to be important for proving relations between quantum distillation and classical secret-key agreement.

Proof. Let $P_{\bar{X}\bar{Y}Z}$ be a CSBD with fidelity $f = 1 - \varepsilon$, i.e.,

$$\begin{aligned} P[\bar{X} = \bar{Y}] &\geq 1 - \varepsilon & (1) \\ |P[\bar{X} = \bar{Y} = 0] - P[\bar{X} = \bar{Y} = 1]| &\leq \varepsilon & (2) \\ H(\bar{X}|Z) &\geq 1 - \varepsilon & (3) \\ H(\bar{Y}|Z) &\geq 1 - \varepsilon. & (4) \end{aligned}$$

Inequalities (1) and (2) directly imply that

$$|P[\bar{X} = 0] - P[\bar{X} = 1]| \leq 2\varepsilon. \tag{5}$$

In addition, assume without loss of generality that $P[\bar{X} = 0] \geq P[\bar{X} = 1]$, and let $\hat{X}$ be a binary random variable which only depends on $\bar{X}$ according to the conditional probability distribution

$$P_{\hat{X}|\bar{X}}(\hat{x}, \bar{x}) = \begin{cases} 1 - \delta & \text{if } \bar{x} = 0 \text{ and } \hat{x} = 0 \\ \delta & \text{if } \bar{x} = 0 \text{ and } \hat{x} = 1 \\ 1 & \text{if } \bar{x} = 1 \text{ and } \hat{x} = 1 \\ 0 & \text{otherwise} \end{cases}$$

where δ is chosen such that $P[\hat{X} = 0] = P[\hat{X} = 1]$. Note that from (5), $\delta \leq 2\varepsilon$. Using (3) we further find

$$\varepsilon \geq 1 - H(\bar{X}|Z) \geq H(\bar{X}) - H(\bar{X}|Z) = I(\bar{X}; Z) \geq I(\hat{X}; Z) \tag{6}$$

where the last inequality follows from the fact that $Z \longrightarrow \bar{X} \longrightarrow \hat{X}$ is a Markov chain. This mutual information can be written as a sum over the ranges of $\hat{X}$ and Z, i.e., the sets $\{0,1\}$ and $\mathcal{Z}$, respectively,

$$\begin{aligned} I(\hat{X}; Z) &= H(Z) - H(Z|\hat{X}) \\ &= \sum_{x \in \{0,1\}} P[\hat{X} = x]\big(H(Z) - H(Z|\hat{X} = x)\big) \\ &= \sum_{x \in \{0,1\}} \sum_{z \in \mathcal{Z}} \frac{1}{2}\big(-P[Z = z]\log_2 P[Z = z] + P[Z = z|\hat{X} = x]\log_2 P[Z = z|\hat{X} = x]\big), \end{aligned}$$

where in the last line we have used that both $P[\hat{X} = 0]$ and $P[\hat{X} = 1]$ are equal to $\frac{1}{2}$. Hence, with

$$\begin{aligned} p_z &:= P[Z = z] = P[\hat{X} = 0, Z = z] + P[\hat{X} = 1, Z = z] \\ \varepsilon_z &:= P[\hat{X} = 0, Z = z] - P[\hat{X} = 1, Z = z] \end{aligned}$$

inequality (6) gets

$$\frac{1}{2}\sum_{z \in \mathcal{Z}} \big(-p_z \log_2 p_z + (p_z + \varepsilon_z)\log_2(p_z + \varepsilon_z)\big) + \big(-p_z \log_2 p_z + (p_z - \varepsilon_z)\log_2(p_z - \varepsilon_z)\big) \leq \varepsilon.$$

A simple calculation shows that the terms in this sum can be lower bounded by a quadratic expression in ε_z,

$$\frac{\varepsilon_z^2}{p_z \ln 2} \leq \big(-p_z \log_2 p_z + (p_z + \varepsilon_z) \log_2(p_z + \varepsilon_z)\big) + \big(-p_z \log_2 p_z + (p_z - \varepsilon_z) \log_2(p_z - \varepsilon_z)\big)$$

for all $z \in \mathcal{Z}$, and hence

$$\frac{1}{2} \sum_{z \in \mathcal{Z}} \frac{\varepsilon_z^2}{p_z \ln 2} \leq \varepsilon.$$

In terms of probabilities, we thus have

$$\sum_{z \in \mathcal{Z}} k_z \cdot \big(\sqrt{P[\hat{X}=0, Z=z]} - \sqrt{P[\hat{X}=1, Z=z]}\big)^2 \leq 4\varepsilon \ln 2$$

with

$$k_z := \frac{\big(\sqrt{P[\hat{X}=0, Z=z]} + \sqrt{P[\hat{X}=1, Z=z]}\big)^2}{P[\hat{X}=0, Z=z] + P[\hat{X}=1, Z=z]}$$

and, since $k_z \geq 1$ for all $z \in \mathcal{Z}$,

$$\sum_{z \in \mathcal{Z}} (\sqrt{P[\hat{X}=0, Z=z]} - \sqrt{P[\hat{X}=1, Z=z]})^2 \leq 4\varepsilon \ln 2. \tag{7}$$

Let us define a vector $|\Psi'\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$,

$$|\Psi'\rangle := |0,0\rangle \otimes \sum_{z \in \mathcal{Z}} \sqrt{P[\hat{X}=0, Z=z]} |z\rangle + |1,1\rangle \otimes \sum_{z \in \mathcal{Z}} \sqrt{P[\hat{X}=1, Z=z]} |z\rangle.$$

Then, setting

$$|\kappa\rangle := \sum_{z \in \mathcal{Z}} \frac{1}{\sqrt{2}} (\sqrt{P[\hat{X}=0, Z=z]} + \sqrt{P[\hat{X}=1, Z=z]}) \cdot |z\rangle,$$

and making use of inequality (7) results in an upper bound for the distance between the Bell state and the state $|\Psi'\rangle$,

$$\| |\Psi'\rangle - |\varphi\rangle \otimes |\kappa\rangle \|^2 \leq 2 \ln 2 \cdot \varepsilon. \tag{8}$$

On the other hand, starting from (1) and $\delta \leq 2\varepsilon$, a straightforward calculation (which is however omitted in this extended abstract) leads to

$$\| |\Psi\rangle - |\Psi'\rangle \|^2 \leq 12\varepsilon. \tag{9}$$

Combining (8) and (9) concludes the proof.

□

4 Bound Information

In the theory of information-theoretically secure secret-key agreement, it is an open problem whether for all probability distribution P_{XYZ} with positive intrinsic information secret-key agreement is possible. In analogy to bound entanglement, i.e., entanglement that can not be distilled, probability distributions having positive intrinsic information but which can not be used for secret key agreement are called bound.

In [2] and [4], some evidence for the existence of bound information has been given. In the following, we will discuss the consequences of Theorem 3.1 with respect to this question.

Let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ be a bound entangled quantum state and $P_{XYZ} := M(|\Psi\rangle)$ a probability distribution resulting from measurement of $|\Psi\rangle$ with respect to some basis. Moreover, for a given binarization $(P_{\bar{X}|X^N}, P_{\bar{Y}|Y^N})$ (where $n \in \mathbb{N}$) of this distribution, let $|\bar{\Psi}\rangle := Q(P_{\bar{X}\bar{Y}Z^N|\bar{X}\neq\Delta\neq\bar{Y}})$.

We now come to the main statement of this section. Consider the following diagram.

$$\begin{array}{ccc} P_{XYZ} & \xrightarrow{(P_{\bar{X}|X^N}, P_{\bar{Y}|Y^N})} & P_{\bar{X}\bar{Y}Z^N|\bar{X}\neq\Delta\neq\bar{Y}} \\ \uparrow{\scriptstyle M} & & \downarrow{\scriptstyle Q=M^{-1}} \\ |\Psi\rangle & \xrightarrow{(P_A, P_B)} & |\bar{\Psi}\rangle \end{array} \tag{10}$$

If for any binarization $(P_{\bar{X}|X^N}, P_{\bar{Y}|Y^N})$ there is a pair of 2-dimensional projectors (P_A, P_B) of $|\Psi\rangle^N$ such that (10) is commutative, then P_{XYZ} is bound.

To see this, assume by contradiction that secret key agreement is possible for P_{XYZ}. Then, from Theorem 2.2, for any $\varepsilon > 0$ there exists a number N and a binarization $(P_{\bar{X}|X^N}, P_{\bar{Y}|Y^N})$ such that $P_{\bar{X}\bar{Y}Z^N|\bar{X}\neq\Delta\neq\bar{Y}}$ is a CSBD with fidelity $1-\varepsilon$. Theorem 3.1 then states that $|\bar{\Psi}\rangle$ is an entangled qubit pair with fidelity $1 - c \cdot \varepsilon$. Since $|\bar{\Psi}\rangle$ is a projection of $|\Psi\rangle^N$ onto two 2-dimensional Hilbert spaces, this means, according to Theorem 2.4, that the state $|\Psi\rangle$ is distillable, which contradicts the assumption that $|\Psi\rangle$ is bound entangled.

References

[1] M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach, Separability and distillability in composite quantum systems — a primer, *Journal of Modern Optics*, Vol. 47, pp. 2481–2499, 2000. (quant-ph/0006064)

[2] N. Gisin, R. Renner, and S. Wolf, Linking classical and quantum key agreement: is there a classical analog to bound entanglement?, to appear in *Algorithmica*, 2001.

[3] N. Gisin, R. Renner, and S. Wolf, Bound information: the classical analog to bound entanglement, in *Proceedings of 3ecm*, Birkhäuser Verlag, 2000.

[4] N. Gisin, S. Wolf, Linking classical and quantum key agreement: is there "bound information"?, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, vol. 1880, pp. 482–500, Springer-Verlag, 2000.

[5] N. Gisin, S. Wolf, Quantum cryptography on noisy channels: quantum versus classical key agreement protocols, *Phys. Rev. Lett.*, Vol. 83, pp. 4200–4203, 1999.

[6] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?, *Phys. Rev. Lett.*, Vol. 80, pp. 5239–5242, 1998.

[7] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, pp. 733–742, 1993.