Towards Proving the Existence of "Bound" Information

Renato Renner [1] Stefan Wolf [2]

Abstract — **We show that information-theoretically secure key agreement and quantum distillation are strongly related. This leads to new evidence for the existence of bound information, i.e., correlated information not useful for the generation of a secret key.**

I. Key Agreement and Quantum Distillation

Consider the *classical secret-key-agreement scenario* [5]: Two parties, Alice and Bob, have access to some correlated information given by repeated realizations of random variables X and Y, respectively, on which an adversary might have some knowledge Z. The goal of Alice and Bob is to generate a common secret key by only communicating over an authentic, but otherwise insecure channel. For a given distribution P_{XYZ}, the *secret-key rate* quantifies the number of secret key bits that can be generated (per realization of the random variables). On the other hand, the *intrinsic information* of P_{XYZ} measures the amount of "secret" correlation between X and Y and is an upper bound on the secret-key rate.

Quantum distillation can be described similarly: Alice and Bob (controlling the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively) initially share some instances of a correlated quantum state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ (where $\mathcal{H}_E$ is the environment). Their goal is to generate fully entangled qubit pairs, only performing local operations and communicating classically. For a given state $|\Psi\rangle$, one may ask whether it can be used for quantum distillation, i.e., whether it is *distillable*. Another question is whether it contains quantum entanglement, i.e., whether it is *inseparable*, which is a necessary condition for distillability.

II. The Link

It was demonstrated recently [3, 2, 1] that classical secret-key agreement and quantum distillation are closely related. In particular, there is a link between intrinsic information and inseparability, as well as between the secret-key rate and distillability. However, in order to compare the two concepts, the probability distribution P_{XYZ} has to be set into relation with the quantum state $|\Psi\rangle$. This can be done in a natural way by defining P_{XYZ} as the distribution of the outcomes of a quantum measurement M of $|\Psi\rangle$ with respect to some fixed basis. We assume that the space of quantum states is restricted such that the mapping M is bijective, and we denote its inverse by Q ("quantization"). $P_{XYZ} = M(|\Psi\rangle)$ is then called the distribution *corresponding to* $|\Psi\rangle$.

Inseparability of a quantum state implies that the intrinsic information of the corresponding probability distribution is positive, and vice versa [3, 1]. On the other hand, it seems that a similar relation exists between the distillability of a state and the secret-key rate of a corresponding distribution. In the following, we will focus on this latter relation.

It has been shown [2] that for a given distribution P_{XYZ}, secret key agreement is possible if and only if for some $N \in \mathbf{N}$, there exists a *binarization* of $P_{XYZ}^N = P_{X^N Y^N Z^N}$, i.e., binary-output channels $P_{\overline{X}|X^N}$ and $P_{\overline{Y}|Y^N}$, such that the resulting probability distribution $P_{\overline{XY}U}$ (where we set $U = Z^N$) is arbitrarily close to a *common secret-bit pair distribution (CSBD)*, i.e., corresponds (up to some small error) to the distribution of a perfect secret-bit pair.

Interestingly, this result has a quantum analogue [4]: A state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is distillable if and only if for some $N \in \mathbf{N}$, there exists a *quantum binarization* $|\overline{\Psi}\rangle$ of $|\Psi\rangle^{\otimes N}$ which is arbitrarily close to a Bell-state, i.e., a maximally entangled qubit pair. Such a quantum binarization is a projection of $|\Psi\rangle^{\otimes N}$ to $\overline{\mathcal{H}_A} \otimes \overline{\mathcal{H}_B} \otimes \mathcal{H}_E^{\otimes N}$, where $\overline{\mathcal{H}_A}$ and $\overline{\mathcal{H}_B}$ are two-dimensional subspaces of $\mathcal{H}_A^{\otimes N}$ and $\mathcal{H}_B^{\otimes N}$, respectively.

The following theorem states that CSBD and entangled qubit pairs are strongly related.

Theorem 1 *Let $|\Psi_n\rangle$ be a sequence of qubit pairs and $P_{\overline{XY}U,\,n} = M(|\Psi_n\rangle)$ the sequence of the corresponding distributions. Then $|\Psi_n\rangle$ converges to a Bell state if and only if $P_{\overline{XY}U,\,n}$ converges to a CSBD.*

III. "Bound" Information

Inseparable quantum states $|\Psi\rangle$ that are not distillable are called *bound entangled*. In analogy, probability distributions P_{XYZ} with positive intrinsic information which can not be used for secret key agreement are said to have *bound information*. Whereas bound entanglement is proven to exist, it is an open question whether there exist probability distributions having bound information. The following corollary of Theorem 1, however, provides some evidence for the existence of bound information: it does exist if every classical binarization has its quantum translation.

Corollary 2 *Let $|\Psi\rangle$ be a bound entangled quantum state such that the corresponding probability distribution P_{XYZ} has positive intrinsic information. If for all $N \in \mathbf{N}$ and all (classical) binarizations B^{cl} there exists a quantum binarization B^{qu} such that the following diagram is commutative, then P_{XYZ} is bound.*

$$\begin{array}{ccccc} P_{XYZ} & \longrightarrow & P_{XYZ}^N & \xrightarrow{B^{cl}} & P_{\overline{XY}Z^N} \\ \uparrow{\scriptstyle M} & & & & \downarrow{\scriptstyle Q:=M^{-1}} \\ |\Psi\rangle & \longrightarrow & |\Psi\rangle^{\otimes N} & \xrightarrow{B^{qu}} & |\overline{\Psi}\rangle \end{array}$$

Acknowledgments

The authors thank Gilles Brassard and Nicolas Gisin for interesting discussions.

References

[1] 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*, 2002.

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

[3] N. Gisin, S. Wolf, Linking classical and quantum key agreement: is there "bound information"?, in *Proceedings of CRYPTO 2000*, vol. 1880, 2000, pp. 482–500.

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

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

[1] Institute of Theoretical Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland. Email: renner@inf.ethz.ch. Supported by the Swiss National Science Foundation (SNF).

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