A New Measure for Conditional Mutual Information and its Properties

Renato Renner [*] Juraj Skripsky [†] Stefan Wolf [‡]

Abstract

We propose a new measure for conditional mutual information, called the reduced intrinsic information. Given a tripartite probability distribution P_{XYZ}, the new measure is an upper bound on the rate $S(X;Y||Z)$ at which two parties, knowing realizations of X and Y, respectively, can generate secret key bits unknown to a third party having access to Z. Moreover, the new bound on S is strictly stronger than the best bound known previously, namely the intrinsic information shared by the parties. In fact, we show that since the new measure takes into account a greater class of potential adversarial strategies for minimizing the secret correlation between the legitimate partners, it can be smaller than the old bound by an arbitrarily large factor.

1 The Reduced Intrinsic Information

In the context of information-theoretic secret key agreement from common information [6], it is a central problem to measure the extractable secret correlation of a tripartite probability distribution. More precisely, assume that two parties Alice and Bob have access to repeated independent realizations of random variables X and Y, respectively, whereas an adversary Eve knows the realizations of Z. Assume further that Alice and Bob are connected by an noiseless and authentic but otherwise completely insecure channel. For this setting, the *secret-key rate* $S(X;Y||Z)$ has been defined as the maximal rate at which Alice and Bob can generate a mutual and highly secret key [6]. It is a fundamental problem to express $S(X;Y||Z)$ in terms of the distribution P_{XYZ}, in particular, to find upper bounds on S or to characterize distributions with $S > 0$. The best upper bound known so far that is expressible in terms of basic information-theoretic quantities of the distribution P_{XYZ} is the *intrinsic information* $I(X;Y{\downarrow}Z)$ [7], which is derived from the facts that the conditional information $I(X;Y|Z)$ is an upper bound on S [6], and that it is one possible strategy of Eve, trying to minimize the mutual information shared by the legitimate partners, to process her data, i.e., send Z through a channel $P_{\overline{Z}|Z}$:[1]

$$I(X;Y{\downarrow}Z) = \inf_{P_{\overline{Z}|Z}} \left(I(X;Y|\overline{Z})\right) . \tag{1}$$

We have [7]

$$S(X;Y||Z) \leq I(X;Y{\downarrow}Z) ,$$

and it has been an open problem whether the two quantities are always equal (or, if not, at least non-zero simultaneously).

The following observation made in [8] shows, however, that $S(X;Y||Z) = I(X;Y{\downarrow}Z)$ cannot always hold since the two quantities have different properties. For four random variables X, Y, Z, and U, we always have

$$S(X;Y||ZU) \geq S(X;Y||Z) - H(U) ; \tag{2}$$

[*] Computer Science Department, Swiss Federal Institute of Technology (ETH Zürich), CH-8092 Zurich, Switzerland. E-mail: renner@inf.ethz.ch

[†] Computer Science Department, Swiss Federal Institute of Technology (ETH Zürich), CH-8092 Zurich, Switzerland. E-mail: jskripsky@stud.ethz.ch

[‡] Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: wolf@iro.umontreal.ca

[1] A recent result [2] states that the infimum in (1) can be replaced by a minimum, where in addition the range of $\overline{Z}$ can be assumed to be equal to the range of Z.

on the other hand,

$$I(X;Y\downarrow ZU) < I(X;Y\downarrow Z) - H(U) \tag{3}$$

is possible.

The proof of property (2) is based on so-called *privacy amplification* [1], often described as the final step of a key-agreement protocol necessary when Alice and Bob already share a common key which is, however, only partially secret. The fact is used that in the special case where this raw key consists of many parts about which the adversary has independent information, the length of the extractable fully-secret key is roughly equal to the Shannon entropy of the original key from Eve's point of view. (A full proof of (2) is given in [8].) On the other hand, an example showing that inequality (3) can hold is given below.

Inequality (2), together with the fact that it can be violated by the intrinsic information, motivates the definition of a new measure which is, first of all, a strictly stronger upper bound on $S(X;Y||Z)$. Its definition is based on the observation that we have for any distribution P_{XYZ}

$$\begin{aligned} S(X;Y||Z) &\leq \inf_{P_{U|XYZ}} (S(X;Y||ZU) + H(U)) \\ &\leq \inf_{P_{U|XYZ}} (I(X;Y\downarrow ZU) + H(U)) \\ &=: I(X;Y\downarrow\downarrow Z) , \end{aligned}$$

where we call the latter the *reduced intrinsic information between X and Y, given Z*. The new measure is an upper bound on $S(X;Y||Z)$, and, as mentioned, we will show later that it is strictly stronger than the previous one, i.e., that

$$I(X;Y\downarrow\downarrow Z) < I(X;Y\downarrow Z)$$

can hold.

2 Properties of the Reduced Intrinsic Information

2.1 Basic Inequalities

The reduced intrinsic information can be written as

$$I(X;Y\downarrow\downarrow Z) = \inf_{P_{U|XYZ}} \left(\inf_{P_{\overline{Z}|ZU}} (I(X;Y|\overline{Z})) + H(U) \right) .$$

It has the following properties.

Theorem 1. *Let X, X', Y, Y', Z, and U be arbitrary random variables. Then we have*

1. $I(XX';YY'\downarrow\downarrow Z) \geq I(X;Y\downarrow\downarrow Z)$
2. $I(X;Y\downarrow\downarrow Z) \leq I(X;Y\downarrow Z) \leq \min\left(I(X;Y) , I(X;Y|Z)\right)$
3. $I(X;Y\downarrow\downarrow Z) \geq S(X;Y||Z) \geq I(X;Y) - I(X;Z)$
4. $I(X;Y\downarrow\downarrow ZU) \leq I(X;Y\downarrow\downarrow Z)$
5. $I(X;Y\downarrow\downarrow ZU) \geq I(X;Y\downarrow\downarrow Z) - H(U)$
6. $I(X;Y\downarrow\downarrow Z) = \inf_{P_{\overline{Z}|Z}} (I(X;Y\downarrow\downarrow \overline{Z}))$.

Proof.

1. Follows from the corresponding property of the conditional mutual information $I(X;Y|Z)$.
2. For the first inequality, choose U such that $H(U) = 0$; for the second, let $P_{\overline{Z}|Z}$ be such that $H(\overline{Z}) = 0$ and such that $\text{Prob}[\overline{Z} = Z] = 1$, respectively.
3. The first inequality was shown in the previous section, the second one follows from a result by Csiszár and Körner [3] (see [6]).

4. We have

$$\begin{aligned} I(X;Y\downarrow\downarrow ZU) &= \inf_{P_{U'|XYZU}} (I(X;Y\downarrow ZUU') + H(U')) \\ &\leq \inf_{P_{U'|XYZU}} (I(X;Y\downarrow ZU') + H(U')) \\ &= \inf_{P_{U'|XYZ}} (I(X;Y\downarrow ZU') + H(U')) \\ &= I(X;Y\downarrow\downarrow Z) \ . \end{aligned}$$

5. We have

$$\begin{aligned} I(X;Y\downarrow\downarrow Z) &= \inf_{P_{V|XYZ}} (I(X;Y\downarrow ZV) + H(V)) \\ &\leq \inf_{P_{U'|XY(Z,U)}} (I(X;Y\downarrow ZUU') + H(UU')) \\ &\leq \inf_{P_{U'|XY(Z,U)}} (I(X;Y\downarrow ZUU') + H(U') + H(U|U')) \\ &\leq I(X;Y\downarrow\downarrow ZU) + H(U) \ . \end{aligned}$$

   The first inequality holds since the minimization is restricted to random variables V containing U (i.e., $V = UU'$).

6. Let $P_{\overline{Z}|Z}$ be a conditional probability distribution. Then

$$I(X;Y\downarrow\downarrow Z) = I(X;Y\downarrow\downarrow Z\overline{Z}) \leq I(X;Y\downarrow\downarrow \overline{Z})$$

   holds because of 4.

□

The properties 5. and 6. of Theorem 1 imply that the reduced intrinsic information cannot be further reduced by the same techniques that led to the reduction of $I(X;Y|Z)$ to $I(X;Y\downarrow Z)$ and to $I(X;Y\downarrow\downarrow Z)$.

Let us now address the question whether $I(X;Y\downarrow\downarrow Z)$ is a better bound on $S(X;Y||Z)$ than $I(X;Y\downarrow Z)$, i.e., under which circumstances $I(X;Y\downarrow\downarrow Z) < I(X;Y\downarrow Z)$ holds.

2.2 The Power of Multiple Local Information Minimization

Intuitively speaking, $I(X;Y\downarrow ZU)$ can potentially be smaller than $I(X;Y\downarrow Z)$ by *two* reasons: First, additional knowledge U is simply by itself an advantage for the adversary (who tries to minimize the correlation between Alice and Bob) and can lead to a reduction of intrinsic information by at most $H(U)$; secondly, however, it can have the *additional* advantage to provide information allowing for better processing the *previous* knowledge Z. Taken together, these two advantages (again, from the viewpoint of the adversary) can reduce the intrinsic information by more than $H(U)$; this fact justifies the new measure which takes this effect into account. In other words, the definition of $I(X;Y\downarrow\downarrow Z)$ considers multiple adaptive "local" minimizations instead of only one simple global minimization of mutual information (as in the definition of $I(X;Y\downarrow Z)$). It is important to note in this context that Eve, knowing Z but not U, cannot actually apply these strategies; their mere existence, however, allows for improving the bound on S.

Theorem 2. *Let P_{XYZ} be a distribution, and let $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_n$ be disjoint events with probabilities* $\mathrm{Prob}\,[\mathcal{E}_i] = p_i$ *such that* $\sum_i p_i = 1$. *Then*

$$I(X;Y\downarrow\downarrow Z) \leq \sum_{i=1}^{n} p_i I(X;Y\downarrow Z\,|\,\mathcal{E}_i) + H([p_1, p_2, \ldots, p_n]) \ .$$

Remark. One possibility of choosing the events $\mathcal{E}_i$ is by determining a partition of the range $\mathcal{X} \times \mathcal{Y}$ of XY into disjoint rectangles

$$\mathcal{X} \times \mathcal{Y} = \bigcup \mathcal{X}_i \times \mathcal{Y}_i$$

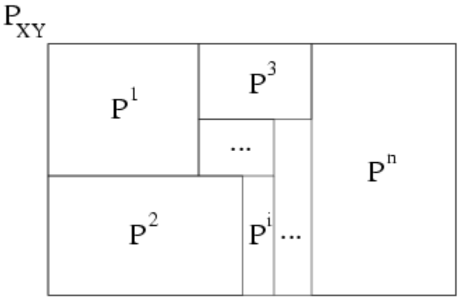

Figure 1: Partitioning a distribution P_{XYZ} into (conditional) distributions $P^i := P_{XYZ|X \in \mathcal{X}_i \times \mathcal{Y}_i}$: When knowing i, Eve can minimize the information shared by Alice and Bob in every rectangle separately.

(see Figure 1). Then, $I(X;Y{\downarrow}{\downarrow}Z)$ is achieved, roughly speaking, when Eve minimizes the information between Alice and Bob in every rectangle separately.

Proof of Theorem 2. Let U be the random variable indicating which of the (disjoint) events occurs, i.e., $U = i$ if and only if $\mathcal{E}_i$ occurs. Then

$$\begin{aligned}\sum_{i=1}^{n} p_i I(X;Y{\downarrow}Z \,|\, \mathcal{E}_i) + H([p_1,\ldots,p_n]) &= \sum_{i=1}^{n} P_U(i) \cdot \inf_{P_{\overline{Z}|Z}} (I(X;Y|\overline{Z}\,, U=i)) + H(U) \\ &\geq \inf_{P_{\overline{Z}|ZU}} (I(XU;YU|\overline{Z})) + H(U) \\ &\geq I(XU;YU{\downarrow}{\downarrow}Z) \\ &\geq I(X;Y{\downarrow}{\downarrow}Z)\ .\end{aligned}$$

□

In order to show the gap between $I(X;Y{\downarrow}{\downarrow}Z)$ and $I(X;Y{\downarrow}Z)$ explicitly, we now consider the special case where P_{XYZ} is composed by two distributions $P^0_{XYZ} = P_{XYZ|\mathcal{E}_0}$ and $P^1_{XYZ} = P_{XYZ|\mathcal{E}_1}$. If Eve's optimal information-minimizing channels are different for the two distributions P^0 and P^1, then $I(X;Y{\downarrow}{\downarrow}Z)$ is generally smaller than $I(X;Y{\downarrow}Z)$ since it takes into account strategies using two separate minimization channels instead of just one.

Theorem 3. *Let P_{XYZ} be a distribution, let $\mathcal{X}$ and $\mathcal{Y}$ be the ranges of X and Y, respectively, let $\mathcal{X} = \mathcal{X}_0 \cup \mathcal{X}_1$ (where $\mathcal{X}_0$ and $\mathcal{X}_1$ are disjoint) and analogously $\mathcal{Y} = \mathcal{Y}_0 \cup \mathcal{Y}_1$, such that $P_{XYZ}(x,y,z) = 0$ if $x \in \mathcal{X}_0$ and $y \in \mathcal{Y}_1$ or vice versa, and let $p = \mathrm{Prob}\,[x \in \mathcal{X}_0]$. We denote by $P^0_{XYZ} = P_{X^0Y^0Z^0}$ the distribution $P_{XYZ|\mathcal{E}_0}$, and analogously for $\mathcal{E}_1$. (See Figure 2.) Then we have*

$$I(X;Y{\downarrow}{\downarrow}Z) \leq p \cdot \inf_{P_{\overline{Z}^0|Z^0}} \left(I(X^0;Y^0|\overline{Z}^0)\right) + (1-p) \cdot \inf_{P_{\overline{Z}^1|Z^1}} \left(I(X^1;Y^1|\overline{Z}^1)\right) + h(p)$$

and

$$I(X;Y{\downarrow}Z) \geq \inf_{P_{\overline{Z}|Z}} \left(p \cdot I(X^0;Y^0|\overline{Z}) + (1-p) \cdot I(X^1;Y^1|\overline{Z})\right)\ .$$

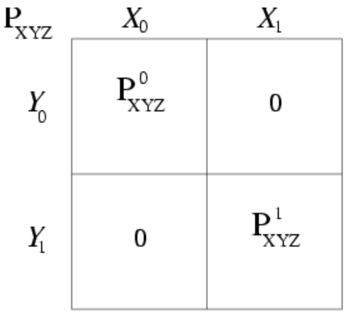

Figure 2: The distribution P_{XYZ} as a product of two distributions P^0_{XYZ} and P^1_{XYZ}.

Proof. The first statement follows directly from Theorem 2. For the second part, let again $U \in \{0,1\}$ be the random variable indicating whether $x \in \mathcal{X}_0$ or $x \in \mathcal{X}_1$ holds. Then

$$\begin{aligned}
I(X;Y{\downarrow}Z) &= \inf_{P_{\overline{Z}|Z}} (I(X;Y|\overline{Z})) \\
&\geq \inf_{P_{\overline{Z}|Z}} (I(XU;YU|\overline{Z}U)) \\
&= \inf_{P_{\overline{Z}|Z}} (P_U(0) \cdot I(X;Y|\overline{Z}, U=0) + P_U(1) \cdot I(X;Y|\overline{Z}, U=1)) \\
&= \inf_{P_{\overline{Z}|Z}} \left(p \cdot I(X^0;Y^0|\overline{Z}) + (1-p) \cdot I(X^1;Y^1|\overline{Z})\right) \ .
\end{aligned}$$

□

Theorem 3 allows for separating $I(X;Y{\downarrow\downarrow}Z)$ from $I(X;Y{\downarrow}Z)$ as follows. Consider for instance the following special case of a distribution composed by two distributions with different minimizing channels $P_{\overline{Z}|Z}$.

Let $p = 1/2$, $\mathcal{X}_0 = \mathcal{Y}_0 = \{0,1,\ldots,n-1\}$, $\mathcal{X}_1 = \mathcal{Y}_1 = \{n, n+1, \ldots, 2n-1\}$, $\mathcal{Z} = \{0,1,\ldots,n-1\}$. For $x \in \mathcal{X}_0$ and $y \in \mathcal{Y}_0$ let

$$P_{XYZ}(x,y,z) = \frac{1}{2} P^0_{XYZ}(x,y,z) = \begin{cases} 1/2n^2 & \text{if } \ z \equiv x+y \pmod{n} \\ 0 & \text{otherwise} \end{cases}$$

and for $x \in \mathcal{X}_1$ and $y \in \mathcal{Y}_1$, let

$$P_{XYZ}(x,y,z) = \frac{1}{2} P^1_{XYZ}(x,y,z) = 1/2n \qquad \text{if } x \equiv y \equiv z \pmod{n}$$

and $P_{XYZ}(x,y,z) = 0$ otherwise. The marginal distribution P_{XY} is represented in the following table.

	X		$\mathcal{X}_0$			$\mathcal{X}_1$		
Y		0	$\cdots$	$n-1$	n	$n+1$	$\cdots$	$2n-1$
	0	$\frac{1}{2n^2}$	$\cdots$	$\frac{1}{2n^2}$	0	0	$\cdots$	0
$\mathcal{Y}_0$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$
	$n-1$	$\frac{1}{2n^2}$	$\cdots$	$\frac{1}{2n^2}$	0	0	$\cdots$	0
	n	0	$\cdots$	0	$\frac{1}{2n}$	0	$\cdots$	0
	$n+1$	0	$\cdots$	0	0	$\frac{1}{2n}$		0
$\mathcal{Y}_1$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\ddots$	$\vdots$
	$2n-1$	0	$\cdots$	0	0	0	$\cdots$	$\frac{1}{2n}$

According to Theorem 3, we have for this distribution

$$I(X;Y{\downarrow\downarrow}Z) \leq 1 \tag{4}$$

whereas

$$I(X;Y{\downarrow}Z) \geq \frac{\log_2 n}{2} \ . \tag{5}$$

The first inequality (4) follows from the fact that both distributions P^0 and P^1 have vanishing intrinsic information: For P^0, the channel $P_{\overline{Z}|Z}$ forgetting Z completely brings the conditional information down to 0 (note that in this case, X and Y are independent) whereas for P^1, the channel which leaves Z unchanged achieves this. In fact, equality holds in (4) since $S(X;Y||Z) \geq 1$: One secret-key bit, namely the bit U, can be extracted from X and Y without any communication.

In order to prove the second inequality (5), let for a channel $P_{\overline{Z}|Z}$ be $\overline{z} \in \overline{\mathcal{Z}}$, $a_i := P_{\overline{Z}|Z}(\overline{z}, i)$, and $a := \sum a_i$. Then we have

$$\begin{aligned} I(X;Y|\overline{Z}=\overline{z}) &\geq \frac{1}{2}(I(X^0;Y^0|\overline{Z}=\overline{z}) + I(X^1;Y^1|\overline{Z}=\overline{z})) \\ &= \frac{1}{2}(\log_2 n - H([a_1/a, \ldots, a_{n-1}/a]) + H([a_1/a, \ldots, a_{n-1}/a])) \\ &= \frac{\log_2 n}{2} , \end{aligned}$$

which concludes the argument since $\overline{z}$ was an arbitrary value of $\overline{Z}$.

We have thus seen that $I(X;Y\downarrow\downarrow Z)$ is a new upper bound on $S(X;Y||Z)$ that can be smaller than the previous bound $I(X;Y\downarrow Z)$ by an arbitrarily large factor.

3 Concluding Remarks

We have defined a new measure for the conditional mutual information, the reduced intrinsic information. The measure proved useful for quantifying the secret correlation between two parties Alice and Bob in the presence of an adversary Eve: It is an upper bound on the rate at which secret-key bits are extractable from the correlation by a protocol using public communication. More specifically, the new measure is a strictly better bound than the (previously known) intrinsic information; this is of interest since the latter is shown in [8] to be a *lower* bound on the number of secret-key bits required to *generate* the correlation P_{XYZ} (or a better one from Alice and Bob's point of view) by public communication. This means that some distributions are wasteful with secret correlations in the sense that not all secret-key bits required to generate them are extractable.

This fact is not very surprising when seen in the light of the parallels pointed out in [5] between secret-key agreement from classical information (as studied in this article) on one hand and quantum distillation on the other: The gap between the rates at which secret-key bits can be *extracted* from a distribution and at which such bits are required to *generate* the same distribution is reflected by the gap between two important measures for entanglement of bipartite quantum states, namely between *entanglement of formation* and *distillable entanglement.* Moreover, the new measure can be used to prove, at least asymptotically, the classical analog to so-called *bound* (non-distillable) entanglement: intrinsic information shared by Alice and Bob useless for generating a secret key [8].

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, Generalized privacy amplification, *IEEE Transactions on Information Theory*, Vol. 41, no. 6, pp. 1915–1923, 1995.

[2] M. Christandl, R. Renner, and S. Wolf, A property of the intrinsic mutual information, manuscript, 2002.

[3] I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. IT-24, pp. 339–348, 1978.

[4] N. Gisin, R. Renner, and S. Wolf, Linking classical and quantum key agreement: is there a classical analog to bound entanglement?, in *Algorithmica*, vol. 34, pp. 389–412, 2002.

[5] N. Gisin and 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.

[6] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[7] U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.

[8] R. Renner and S. Wolf, New bounds in secret-key agreement: the gap between formation and secrecy extraction, manuscript, 2002.