Unique Informations and Deficiencies

by

Pradeep Kumar Banerjee, Eckehard Olbrich, Jürgen Jost, and Johannes Rauh

Preprint no.: 103 2019
Unique Informations and Deficiencies

Pradeep Kr. Banerjee*, Eckehard Olbrich, Jürgen Jost, and Johannes Rauh

Abstract

Given two channels that convey information about the same random variable, we introduce two measures of the unique information of one channel with respect to the other. The two quantities are based on the notion of generalized weighted Le Cam deficiencies and differ on whether one channel can approximate the other by a randomization at either its input or output. We relate the proposed quantities to an existing measure of unique information which we call the minimum-synergy unique information. We give an operational interpretation of the latter in terms of an upper bound on the one-way secret key rate and discuss the role of the unique informations in the context of nonnegative mutual information decompositions into unique, redundant and synergistic components.

Index Terms

Synergy, redundancy, unique information, Le Cam deficiency, degradation preorder, input-degradedness preorder, Secret key rate.

Note: The material in this manuscript has been presented at the Allerton conference 2018 [1].

This manuscript contains some corrections: most notably, Lemma 18 was removed and Proposition 28 was corrected. The numbering of equations and results in this file agrees with the numbering of the published version.

I. INTRODUCTION

Consider three random variables $S$, $Y$, $Z$ with finite alphabets. Suppose that we want to know the value of $S$, but we can only observe $Y$ and $Z$. The mutual information between $S$ and $Y$ can be decomposed into information that $S$ has about $Y$ that is unknown to $Z$ (we call this the unique or exclusive information of $Y$ w.r.t. $Z$) and information that $Y$ has about $S$ that is known to $Z$ (we call this the shared or redundant information).

$$I(S;Y) = \text{UI}(S;Y\|Z) + \text{SI}(S;Y,Z).$$

(1)

Conditioning on $Z$ annihilates the shared information but creates complementary or synergistic information from the interaction of $Y$ and $Z$.

$$I(S;Y|Z) = \text{UI}(S;Y\|Z) + \text{CI}(S;Y,Z).$$

(2)

Using the chain rule, the total information that the pair $(Y,Z)$ conveys about $S$ can be decomposed into four terms.

$$I(S;YZ) = I(S;Y) + I(S;Z|Y)$$

$$= \text{UI}(S;Y\|Z) + \text{SI}(S;Y,Z) + \text{UI}(S;Z\|Y) + \text{CI}(S;Y,Z),$$

(3)

where $\text{UI}$, $\text{SI}$, and $\text{CI}$ are nonnegative functions that depend continuously on the joint distribution of $(S,Y,Z)$. Nonnegative information decompositions of this form have been considered in [2]–[5].

Any definition of the function $\text{UI}$ fixes two of the terms in (3) which in turn also determines the other terms by (1) and (2). This gives rise to the consistency condition:

$$I(S;Y) + \text{UI}(S;Z\|Y) = I(S;Z) + \text{UI}(S;Y\|Z).$$

(4)

One can thus interpret the unique information as either the conditional mutual information without the synergy, or as the mutual information without the redundancy. The difference of the redundant and synergistic information is called the coinformation $\text{CoI}(S;Y;Z)$ which is symmetric in its arguments and can be negative: $\text{CoI}(S;Y;Z) = \text{SI}(S;Y,Z) - \text{CI}(S;Y;Z) = I(S;Y) - I(S;Y\|Z)$ [6]. Coinformation is a widely used measure in the neurosciences [7], [8] with negative values being interpreted as synergy [9] and positive values as redundancy [7]. If the interactions induce redundancy and synergy in equal measure, then the coinformation cannot detect it. Correlational importance, a nonnegative measure introduced in [8] (see also [10]) to quantify the importance of correlations in neural coding is

*The authors are with the Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany.

Email: {pradeep, olbrich, jjost, jrauh}@mis.mpg.de
similar in spirit to the synergistic information. However, examples are known\(^1\) when it can exceed the total mutual information.

The notions of synergy, redundancy and unique information also appear implicitly in information-theoretic cryptography\(^2\)–\(^5\). Consider the source model for secret key agreement between distant Alice and Bob against an adversary, Eve\(^6\), Alice, Bob and Eve observe i.i.d. copies of random variables \(S, Y, Z\) where \((S, Y, Z) \sim P_{SYZ}\). Alice and Bob want to compute a secret key by communicating messages over a noiseless but insecure (public) channel transparent to Eve such that Eve’s total information \((Z)\) and the entire public communication) about the key is negligibly small. The maximum (asymptotic) rate at which Alice and Bob can compute a key is called the two-way secret key rate \(S_{\rightarrow}(S; Y | Z)\). If Alice is allowed to use the public channel only once and Bob does not transmit, then the corresponding quantity is called the one-way secret key rate \(S \rightarrow \rightarrow(S; Y | Z)\).

An instance of a purely synergistic interaction is the XOR distribution: \(Y, Z\) are independent binary random variables and \(S = Y + Z \mod 2\). Here \(I(S; Y Z) = CI(S; Y, Z) = 1\) bit. Clearly, if Alice can only see \(S\) and Bob \(Y\), then they cannot realize a secret key. However if Alice can also see \(Z\), then she can compute \(Y\) which can be used as a key perfectly secret from Eve since Eve’s variable \(Z\) is independent of the key \(Y\).

An instance of a purely redundant interaction is the RDN distribution: \(S, Y, Z\) are uniformly distributed binary random variables with \(S = Y = Z\). Here \(I(S; Y Z) = SI(S; Y, Z) = 1\) bit. Alice and Bob cannot share a secret since Eve knows the exact values of \(S\) and \(Y\).

Intuitively, if Bob has some unique information about Alice’s variable \(S\) (that is not known to Eve), then there must be a situation where Bob can exploit this information to his advantage. A distribution combining the XOR and RDN exemplifies such an advantage.

**Example 1**\(^{4, 17}\). Consider the joint distribution

\[
\begin{array}{c|ccc}
S & 0 & 1 & 2 & 3 \\
\hline
0 & \frac{1}{8} (0) & \frac{1}{8} (1) & . & . \\
1 & \frac{1}{8} (1) & \frac{1}{8} (0) & . & . \\
2 & . & . & \frac{1}{4} (2) & . \\
3 & . & . & . & \frac{1}{4} (3) \\
\end{array}
\]

where \(Z\)’s value is shown in parentheses. For instance, the first entry of the table is read as \(P_{SYZ}(0, 0, 0) = \frac{1}{8}\). Here \(I(S; Y Z) = 2, SI(S; Y, Z) = 1.5, CI(S; Y, Z) = 0.5\) and \(UI(S; Y | Z) = 1\). If Eve sees 2 or 3, she knows the exact values of \(S\) and \(Y\). When she sees 0 or 1, she can infer that Alice and Bob’s values are in \(\{0, 1\}\), but in this range, their observations are independent. Hence, no secret key agreement is possible.

Consider now the modified distribution

\[
\begin{array}{c|ccc}
S & 0 & 1 & 2 & 3 \\
\hline
0 & \frac{1}{8} (0) & \frac{1}{8} (1) & . & . \\
1 & \frac{1}{8} (1) & \frac{1}{8} (0) & . & . \\
2 & . & . & \frac{1}{4} (0) & . \\
3 & . & . & . & \frac{1}{4} (1) \\
\end{array}
\]

where Eve’s variable \(Z\) can only assume binary values. For this distribution, \(I(S; Y Z) = 2, SI(S; Y, Z) = 0.5, CI(S; Y, Z) = 0.5\) and \(UI(S; Y | Z) = 1\). Now Bob has unique information about Alice’s values w.r.t. Eve (namely, the ability to distinguish whether Alice sees values in the XOR or the RDN quadrant) which he can use to agree on 1 bit of secret. The intrinsic information\(^2\) \(\tilde{I}(S; Y | Z) := \min_{P_{Z|S}} I(S; Y | Z')\), a well-known upper bound on the two-way secret key rate \(\tilde{I}(S; Y | Z)\) is not tight in this toy example. It evaluates to 1.5 bits.

How can we decide if \(Y\) has some unique information about \(S\) (that is not known to \(Z\))? Consider the channels \(\kappa\) and \(\mu\) with the common input alphabet \(S\) in Fig.\(^{16}\). If \(\mu\) reduces to \(\kappa\) by adding a post-channel \(\lambda\) at its output, then \(\mu\) may be said to include \(\kappa\). One can draw the same conclusion for the channels \(\kappa\) and \(\bar{\mu}\) with the common output alphabet \(S\) in Fig.\(^{16}\) if \(\bar{\mu}\) reduces to \(\bar{\kappa}\) by adding a pre-channel \(\lambda\) at its input. These are special cases of a channel inclusion preorder first studied by Shannon\(^{19}\). In both these situations, one would expect that \(Y\) provides no unique information about \(S\) w.r.t. \(Z\). A nonvanishing unique information would then quantify how far is one channel from being an inclusion or randomization of the other.

\(^1\)We compute the decomposition using a definition of the function \(\tilde{I}\) proposed in \(^2\). An efficient algorithm was recently proposed in \(^{13}\).

\(^2\)The intrinsic information violates the consistency condition\(^{19}\) and cannot be interpreted as unique information in our sense.
Depending on whether such a randomization is applied at the output or the input, two different ways of quantifying the unique information arise. Utilizing tools from statistical decision theory, [2] defined the function $\bar{U}$ based on the idea of approximating one channel from the other by a randomization at the input (see Fig. 1a). $\bar{U}$ defined the function $\bar{U}I$ as a difference of two Kullback-Leibler divergence terms where one of the terms implicitly uses a randomization at the output (see Fig. 1b). In both cases, the induced decompositions of the total mutual information are nonnegative and satisfy equations (1)-(3). While quantitative differences between the two decompositions have been studied earlier (see, e.g., [2, Figure 1]), the aforementioned distinction seems to have largely gone unnoticed in the literature. Also, as Example 1, it seems to suggest, the unique information is an interesting quantity in its own right that might play a role in bounding the secret key rate. An objective study relating the two quantities is missing.

In this minimum, there always exist deterministic optimal strategies. So it suffices to consider deterministic strategies.

In this paper, we bridge these little gaps and make the following contributions:

- Given two channels that convey information about the same random variable, we propose two measures of unique information of one channel w.r.t. the other. They are both based on a generalized version of Le Cam’s notion of weighted deficiency [20]–[22] of one channel w.r.t. another. Weighted deficiencies measure the cost of approximating one channel from the other via randomizations. Depending on whether the randomization is applied at the output or the input, two different notions of weighted deficiency arise. We call the respective quantities the weighted output and weighted input deficiencies. The new quantities induce nonnegative decompositions of the mutual information. Interestingly, the decomposition induced by the weighted input deficiency coincides with the one proposed in [3].

- We show that the definition of the unique information proposed in [2] shares some intuitive and basic properties of the secret key rate [13]. We give an operational interpretation of this quantity in terms of an upper bound on the one-way secret key rate. Theorem 37 is our main result in this part. As a minor side note, for secret key agreement against active adversaries, we restate Maurer’s impossibility result [23] in terms of vanishing unique informations in Theorem 39.

Proofs are collected in Appendix V-A.

II. UNIQUE INFORMATIONS AND LE CAM DEFICIENCIES

Suppose that an agent has a finite set of actions $A$. Each action $a \in A$ incurs a bounded loss $\ell(s, a)$ that depends on the chosen action $a$ and the state $s \in S$ of a finite random variable $S$. Let $\pi_S$ encode the agents’ uncertainty about the true state $s$. Then, the triple $(\pi_S, A, \ell)$ is called a decision problem. In the sequel, we assume that $\pi_S$ has full support. Before choosing her action, the agent is allowed to observe a finite random variable $Z$ through a channel from $S$ to $Z$ which is a family $\mu = \{\mu_s\}_{s \in S}$ of probability distributions on $Z$, one for each possible input $s \in S$. Let $M(S; Z)$ denote the space of all channels from $S$ to $Z$ which is the set of all (row) stochastic matrices $[0, 1]^{S \times Z}$. The goal of a rational agent is to choose a strategy $\rho \in M(Z; A)$ that minimizes her expected loss or risk

$$R(\pi_S, \mu, \rho, \ell) := \sum_{s \in S} \pi_S(s) \sum_{a \in A} \rho \circ \mu(s)(a)\ell(s, a),$$

where $\rho \circ \mu$ (read $\rho$ after $\mu$) denotes the composition of the channels $\rho$ and $\mu$. Writing $A_\mu = \{\rho \circ \mu : \rho \in M(Z; A)\}$, the optimal risk when using the channel $\mu$ is

$$R(\pi_S, \mu, \ell) := \min_{\sigma \in A_\mu} \sum_{s \in S} \pi_S(s) \sum_{a \in A} \sigma_s(a)\ell(s, a).$$

In this minimum, there always exist deterministic optimal strategies. So it suffices to consider deterministic strategies.

Suppose now that the agent is allowed to observe another finite random variable $Y$ through a second channel $\kappa \in M(S; Y)$ with the same input alphabet $S$. When will she always prefer $Z$ to $Y$? She can rank the variables by comparing her optimal risks: she will always prefer $Z$ over $Y$ if her optimal risk when using $Z$ is at most that when using $Y$ for any decision problem. We have the following definition.

\[ \begin{align*}
S &\xrightarrow{\kappa} Y \\
\bar{S} &\xrightarrow{\bar{\mu}} Y \\
S &\xrightarrow{\mu} Z \\
\bar{\bar{S}} &\xrightarrow{\bar{\bar{\mu}}} Z
\end{align*} \]
Problem of interest.

Output deficiency is sufficient to ensure that the difference in the optimal risks is also bounded for any decision problems when using the channel $\mu$ small, then

$$
\max_{\pi_S, \kappa, \ell} \mathbb{E}_{\pi_S} \mathcal{L}(Y|S) - \mathbb{E}_{\kappa(S)} \mathcal{L}(Y|S) 
$$

Definition 7. The weighted output deficiency of $\mu$ w.r.t. $\kappa$ is

$$
\delta_o^S(\mu, \kappa) := \min_{\lambda \in \mathcal{M}(Z;Y)} D(\kappa || \mu \circ \pi_S),
$$

where $D$ is the Kullback-Leibler divergence and the subscript $o$ in $\delta_o^S$ emphasizes the fact that the randomization is at the output of the channel $\mu$ (see Fig. 1a).

As an immediate consequence, $\delta_o^S(\mu, \kappa) = 0$ if and only if $Z \subseteq_S Y$, which captures the intuition that if $\delta_o^S(\mu, \kappa)$ is small, then $Z$ is approximately Blackwell sufficient for $Y$.

Le Cam’s randomization criterion [20] shows that deficiencies quantify the maximal gap in the optimal risks of decision problems when using the channel $\mu$ rather than $\kappa$. The next proposition states that bounding the weighted output deficiency is sufficient to ensure that the differences in the optimal risks is also bounded for any decision problem of interest.

Proposition 8. Fix $\mu \in \mathcal{M}(S;Z)$, $\kappa \in \mathcal{M}(S;Y)$ and a prior probability distribution $\pi_S$ on $S$ and write $\|\ell\|_\infty = \max_{s,a} \ell(s,a)$. For every $\epsilon > 0$, if $\delta_o^S(\mu, \kappa) \leq \epsilon$, then $R(\pi_S, \mu, \ell) - R(\pi_S, \kappa, \ell) \leq \sqrt{\epsilon \ln(2)} \|\ell\|_\infty$ for any set of actions $\mathcal{A}$ and any bounded loss function $\ell$.

Another ordering that has been studied recently is the input-degradedness preorder [26] based on whether one channel can be simulated from the other by randomization at the input.

Definition 9. Let $\bar{\kappa} \in \mathcal{M}(Y;S)$, $\bar{\mu} \in \mathcal{M}(Z;S)$ be two channels with a common output alphabet. We say that $\bar{\kappa}$ is input-degraded from $\bar{\mu}$ and write $\bar{\mu} \succeq_S \bar{\kappa}$ if $\bar{\kappa} = \bar{\mu} \circ \bar{\lambda}$ for some $\bar{\lambda} \in \mathcal{M}(Y;Z)$.

[26] gave a characterization of input-degradedness that is similar to Blackwell’s theorem. The weighted deficiency counterpart of Definition 7 is as follows.
**Definition 10.** The weighted input deficiency of $\bar{\mu}$ w.r.t. $\bar{\kappa}$ is

$$\delta_i^\mu(\bar{\mu}, \bar{\kappa}) := \min_{\lambda \in M(Y; Z)} D(\bar{\kappa} \circ \lambda | \pi_Y),$$

where the subscript $i$ in $\delta_i^\mu$ emphasizes the fact that the randomization is at the input of the channel $\bar{\mu}$ (see Fig. 15).

### III. NONNEGATIVE MUTUAL INFORMATION DECOMPOSITIONS

We propose two nonnegative decompositions of the mutual information between the pair $(Y, Z)$ and $S$ based on Definition 10 and Definition 11 of the weighted output and input deficiencies.

**A. Nonnegative decomposition based on weighted output deficiencies**

Consider the following functions on the simplex $\mathbb{P}_{S \times Y \times Z}$.

**Definition 11.** Let $(S, Y, Z) \sim \mathcal{P}$.

$$UI_o(S; Y \mid Z) = \max \{\delta_o^\mu(\mu, \kappa), \delta_o^\mu(\kappa, \mu) + I(S; Y) - I(S; Z)\},$$

$$SL_o(S; Y, Z) = \min \{I(S; Y) - \delta_o^\mu(\mu, \kappa), I(S; Z) - \delta_o^\mu(\kappa, \mu)\},$$

$$CI_o(S; Y, Z) = \min \{I(S; Y | Z) - \delta_o^\mu(\mu, \kappa), I(S; Z | Y) - \delta_o^\mu(\kappa, \mu)\}.$$ **Proposition 13** (Nonnegativity). $SI_o, UI_o$ and $CI_o$ are nonnegative functions.

**Lemma 14.** $UI_o(S; Y \mid Z)$ vanishes if and only if $Y$ has no unique information about $S$ w.r.t. $Z$ (according to Definition 10).

**B. Nonnegative decomposition based on weighted input deficiencies**

Consider the following functions on the simplex $\mathbb{P}_{S \times Y \times Z}$.

**Definition 15.** Let $(S, Y, Z) \sim \mathcal{P}$.

$$UI_i(S; Y \mid Z) = \max \{\delta_i^\mu(\bar{\mu}, \bar{\kappa}), \delta_i^\mu(\bar{\kappa}, \bar{\mu}) + I(S; Y) - I(S; Z)\},$$

$$SI_i(S; Y, Z) = \min \{I(S; Y) - \delta_i^\mu(\bar{\mu}, \bar{\kappa}), I(S; Z) - \delta_i^\mu(\bar{\kappa}, \bar{\mu})\},$$

$$CI_i(S; Y, Z) = \min \{I(S; Y | Z) - \delta_i^\mu(\bar{\mu}, \bar{\kappa}), I(S; Z | Y) - \delta_i^\mu(\bar{\kappa}, \bar{\mu})\}.$$ **Remark 15.** The functions $UI_i$ and $SI_i$ depend only on the tuple $(\pi_Y, \pi_Z, \bar{\mu}, \bar{\kappa})$. $CI_i$ depends on the full joint $P$.

It is easy to see that the functions (9) satisfy the information decomposition equations (11)-(13). **Proposition 17** (Nonnegativity). $SI_i, UI_i$ and $CI_i$ are nonnegative functions.

**Definition 19.** For $C \subset \mathbb{P}_S$, let $\text{conv}(C)$ denote the convex hull of $C$. Let

$$Q_{y \sim Z}(S) \in \arg \min_{Q \in \text{conv}(\{\bar{\mu}_z\}_{z \in Z}) \subset \mathbb{P}_S} D(\bar{\kappa}_y \| Q)$$

be the reverse $I$-projection of $\bar{\kappa}_y$ onto the convex hull of the points $\{\bar{\mu}_z\}_{z \in Z} \in \mathbb{P}_S$. Define the projected information of $Y$ onto $Z$ w.r.t. $S$ as

$$I_S(Y \searrow Z) := \mathbb{E}_{(s, y) \sim \bar{\kappa} \times \pi_Y} \log \frac{Q_{y \sim Z}(s)}{Q_{y \sim Z}(s)}.$$ **Proposition 21** defined a measure of shared information based on reverse information projections to a convex set of probability measures.

**Definition 19.** For $C \subset \mathbb{P}_S$, let $\text{conv}(C)$ denote the convex hull of $C$. Let

$$Q_{y \sim Z}(S) \in \arg \min_{Q \in \text{conv}(\{\bar{\mu}_z\}_{z \in Z}) \subset \mathbb{P}_S} D(\bar{\kappa}_y \| Q)$$

be the reverse $I$-projection of $\bar{\kappa}_y$ onto the convex hull of the points $\{\bar{\mu}_z\}_{z \in Z} \in \mathbb{P}_S$. Define the projected information of $Y$ onto $Z$ w.r.t. $S$ as

$$I_S(Y \searrow Z) := \mathbb{E}_{(s, y) \sim \bar{\kappa} \times \pi_Y} \log \frac{Q_{y \sim Z}(s)}{Q_{y \sim Z}(s)}.$$ **Proposition 21** defined a measure of shared information based on reverse information projections to a convex set of probability measures.

**Definition 19.** For $C \subset \mathbb{P}_S$, let $\text{conv}(C)$ denote the convex hull of $C$. Let

$$Q_{y \sim Z}(S) \in \arg \min_{Q \in \text{conv}(\{\bar{\mu}_z\}_{z \in Z}) \subset \mathbb{P}_S} D(\bar{\kappa}_y \| Q)$$

be the reverse $I$-projection of $\bar{\kappa}_y$ onto the convex hull of the points $\{\bar{\mu}_z\}_{z \in Z} \in \mathbb{P}_S$. Define the projected information of $Y$ onto $Z$ w.r.t. $S$ as

$$I_S(Y \searrow Z) := \mathbb{E}_{(s, y) \sim \bar{\kappa} \times \pi_Y} \log \frac{Q_{y \sim Z}(s)}{Q_{y \sim Z}(s)}.$$ **Proposition 21** defined a measure of shared information based on reverse information projections to a convex set of probability measures.
For an account of some intuitive properties of the function $SI_{\text{red}}$ as a measure of shared information, see [3] Section II.B] and [5]. Proposition 20 states that implicit in the above construction is the weighted input deficiency $\delta^\pi_\mu(\bar{\kappa}, \bar{\mu})$.

**Proposition 20.** $I_S(Y \setminus Z) = I(S; Y) - \delta^\pi_\mu(\bar{\kappa}, \bar{\mu})$.

An immediate consequence of Proposition 20 is that the decomposition proposed in [3] and that in Definition 15 are equivalent.

**Proposition 21.** $SI_{\text{red}} = SI, UI_{\text{red}} = UI, CI_{\text{red}} = CI$, where $UI_{\text{red}}$ and $CI_{\text{red}}$ are the corresponding unique and complementary informations derived from [12] and satisfying equations (11)-(13).

### IV. Minimum-synergy Unique Information

[2] proposed a nonnegative decomposition of the mutual information based on the idea that the unique and shared information should depend only on the marginal distributions of the pairs $(S, Y)$ and $(S, Z)$.

**Definition 22.** Let $(S, Y, Z) \sim P$ and let $\kappa \in M(S; Y), \mu \in M(S; Z)$ be two channels with the same input alphabet such that $P_{SY}(s, y) = \pi_S(s)\kappa_y(y)$ and $P_{SZ}(s, z) = \pi_S(s)\mu_z(z)$. Define

\[
\Delta_P = \left\{ Q \in \mathbb{P}_{S \times Y \times Z} : Q_{SY}(s, y) = \pi_S(s)\kappa_y(y), \quad Q_{SZ}(s, z) = \pi_S(s)\mu_z(z) \right\},
\]

(14a)

\[
UI(S; Y \setminus Z) = \min_{Q \in \Delta_P} I_Q(S; Y | Z),
\]

(14b)

\[
UI(S; Z \setminus Y) = \min_{Q \in \Delta_P} I_Q(S; Z | Y),
\]

(14c)

\[
SI(S; Y, Z) = \max_{Q \in \Delta_P} CoI_Q(S; Y | Z),
\]

(14d)

\[
CI(S; Y, Z) = I(S; Y | Z) - UI(S; Y \setminus Z),
\]

(14e)

where $CoI$ is the coinformation and the subscript $Q$ in $CoI_Q$ and $I_Q$ denotes that joint distribution on which the quantities are computed.

In Appendix [V-B] we briefly comment on the optimization problems in Definitions 22, 10 and 7.

**Remark 23.** The functions $UI$ and $SI$ depend only on the triple $(\pi, \kappa, \mu)$. The function $CI$ depends on the full joint $P$.

**Lemma 24** ([2] Lemma 6). $UI(S; Y \setminus Z)$ vanishes if and only if $(S, Y)$ has no unique information about $Z$ w.r.t. $Z$ (according to Definition 5).

**Remark 25.** The following trivial bounds follow from (10)-(12).

\[
I(S; Y) - I(S; Z) \leq UI(S; Y \setminus Z) \leq \min\{I(S; Y), I(S; Y | Z)\}.
\]

(15)

These bounds are also valid for the functions $UI_o$ and $UI_i$. In the adversarial setting in Example 1 if either Eve has less information about $S$ than Bob or, by symmetry, less information about $Y$ than Alice, then Alice and Bob can exploit this difference to extract a secret key. In such a setting, bounds on the unique information common to $S$ and $Y$ w.r.t. $Z$ are useful.

\[
\max\{I(S; Y) - I(S; Z), I(Y; S) - I(Y; Z)\} \leq \max\{UI(S; Y \setminus Z), UI(Y; S \setminus Z)\} \leq \min\{I(S; Y), I(S; Y | Z)\}.
\]

(16)

An interesting observation is that these bounds match the trivial bounds on the two-way secret key rate [13] (see Section [V-A]).

\[
\max\{I(S; Y) - I(S; Z), I(Y; S) - I(Y; Z)\} \leq S_{\text{US}}(S; Y | Z) \leq \min\{I(S; Y), I(S; Y | Z)\}.
\]

(17)

The following lemma states that the quantities $UI, SI$ and $CI$ in Definition 22 bound the unique, shared and complementary components in any nonnegative decomposition of the mutual information under an assumption that is in keeping with the Blackwell ordering.

**Lemma 26** ([2] Lemma 3). Let $\tilde{UI}(S; Y \setminus Z), \tilde{SI}(S; Y \setminus Z), \tilde{SI}(S; Y, Z)$ and $\tilde{CI}(S; Y, Z)$ be nonnegative functions on $\mathbb{P}_{S \times Y \times Z}$ satisfying equations (11)-(13) and assume that the following holds:
Fig. 2: Distribution in Example 28b): (a) Concatenated erasure channels with a binary symmetric input distribution. (b) Equivalent erasure channel $P_{Z|S}$ with erasure probability $\epsilon = \frac{1}{3}$. (c) The “reverse” erasure channels $P_{S|Y}$ and $P_{S|Z}$.

(⇒) $\overline{UI}$ depends only on the triple $(\pi, \kappa, \mu)$.

Then $\overline{UI} \leq UI, \overline{SI} \geq SI$ and $\overline{CI} \geq CI$ with equality if and only if there exists $Q \in \Delta_P$ such that $\overline{CI}_Q(S : Y ; Z) = 0$.

Lemma 26 is consistent with our interpretation of the function $UI$ as the minimum-synergy unique information.

Corollary 27.

$$\delta^\pi_0(\mu, \kappa) \leq UI_0(S ; Y | Z) \leq UI(S ; Y | Z),$$

$$\delta^\pi_1(\mu, \kappa) \leq UI_1(S ; Y | Z) \leq UI(S ; Y | Z).$$

Proposition 28 follows from Lemmas 14 and 24 and Definition 7.

Proposition 28. $\delta^\pi_0(\mu, \kappa) = 0 \iff UI_0(S ; Y | Z) = 0 \iff UI(S ; Y | Z) = 0$.

In [2], it was claimed that the vanishing sets of $UI_{red} = UI_0$ and $UI$ agree. In the published version of this paper [1], this was used to show that the vanishing sets of $UI_i$ and $\delta^\pi_i$ agree with that of $UI$. As the following example shows, this is not correct:

Example 28b). Consider the distribution depicted in Figure 2a). $P_S$ is a binary symmetric distribution and $P_{Y|S}$ and $P_{Z|Y}$ are symmetric erasure channels with erasure probabilities $\epsilon_1 = \frac{1}{6}$ and $\epsilon_2 = \frac{1}{3}$, resp. We have:

- $S - Y - Z$ is a Markov chain by construction. The erasure probability of the induced erasure channel $P_{Z|S}$ shown in Figure 2b) is greater than that of $P_{Y|S}$, whence $UI(S ; Y | Z) = I(S ; Y | Z) = \frac{1}{6} > 0$.
- On the other hand, the induced “reverse” erasure channels $P_{S|Y}$ and $P_{S|Z}$ are identical (see Figure 2c)). Thus, $\delta^\pi_1 = 0$.

A. $UI$ is an upper bound on the one-way secret key rate

In this section, we show that the function $UI$ has a meaningful operational interpretation in a task where the goal is to extract a secret key from shared randomness and public communication.

In a two-way secret key agreement protocol for the source model [12], [13], [16], Alice, Bob and Eve observe $n$ i.i.d. copies of random variables $S$, $Y$ and $Z$ respectively, where $(S, Y, Z)$ is distributed according to some joint distribution $P$ assumed to be known to all parties. The protocol proceeds in rounds: In each round either Alice or Bob can transmit a message over an insecure but authenticated public discussion channel. If Alice (resp., Bob) transmits message $C_i$ in round $i$, then $C_i$ is a function of $S^n$ (resp., $Y^n$) and all the messages received so far. After $r$ rounds, Alice (resp., Bob) computes a key $K_{A}^n \in K^n$ for $K = \{0, 1\}$ (resp., $K_{B}^n \in K^n$) as a function of $S^n$ (resp., $Y^n$) and $C := (C_1, C_2, \ldots, C_r)$, the collection of messages sent over the public channel. The protocol is one-way if Alice is allowed to use the public channel only once and Bob cannot transmit at all: Alice computes a key $K_{A}^n$ and a
message $C$ for Bob as a function of $S^n$. Bob computes a key $K^n_B$ as a function of $Y^n$ and $C$. In the limit $n \to \infty$, the secret key must satisfy the following conditions:

$$\Pr[K^n_A \neq K^n_B] = 0, \quad \log |K^n| - H(K^n|Z^nC) = 0. \quad (18)$$

The largest achievable rate $\lim_{n \to \infty} \frac{1}{n}$ at which Alice and Bob can distill a key in the two-way and the one-way communication scenarios are resp. called, the two-way secret key rate $S_\rightarrow(S;Y|Z)$ and the one-way secret key rate $S_\rightarrow(S;Y|Z)$.

An exact expression for the one-way secret key rate is known.

**Theorem 29** ([12 Theorem 1]). The one-way secret key rate $S_\rightarrow(S;Y|Z)$ for the source model is

$$S_\rightarrow(S;Y|Z) = \max_{P_{UY|SYZ}} I(U;Y|V) - I(U;Z|V)$$

for random variables $U$, $V$ such that $YZ - S - UV$ is a Markov chain, and where both $U$ and $V$ have range of size at most $|S| + 1$.

The one-way secret key rate is a lower bound on the two-way secret key rate.

General properties of upper bounds on the secret key rates have been investigated under the rubric of protocol monotones—nonnegative real-valued functionals of joint distributions that can never increase during protocol execution (see e.g., [28]–[31]). For example, the intrinsic information, an upper bound on the two-way secret key rate is a protocol monotone [17].

We show that the function $UI$ shares some intuitive and basic properties of the secret key rate. Lemma [20] states that if Alice and Bob discard certain realizations of their random variables by restricting their ranges, then the $UI$ can never increase. See [13 Lemma 3] for a counterpart of this property for the two-way secret key rate.

**Lemma 30** (Monotonicity under range restrictions [32]). $UI((S,S');(Y,Y')|Z) \geq UI(S;Y|Z)$.

The following Lemma states that $UI$ can never increase under local operations of Alice and Bob. The counterpart of this lemma for the secret key rate is [13 Lemma 4].

**Lemma 31** (Monotonicity under Local Operations). $UI$ cannot increase under local operations of $S$ or $Y$.

Lemma [32] states that if Eve is allowed access to some additional side information, then the $UI$ can only decrease. See [13 Lemma 5] for a counterpart of this property for the two-way secret key rate.

**Lemma 32** (Monotonicity under adversarial side information [32]). $UI(S;Y|(Z,Z')) \leq UI(S;Y|Z)$.

Suppose Alice publicly announces the value of a random variable. Then Lemma [33] states that $UI$ can never increase.

**Lemma 33** (Monotonicity under one-way public communication). $UI(S;(Y,f(S))|(Z,f(S))) \leq UI(S;Y|Z)$ for all functions $f$ over the support of $S$.

The following two properties, additivity and asymptotic continuity are important if the function $UI$ is to furnish an upper bound on the asymptotic rate of transforming a given joint distribution into a secret key.

**Lemma 34** (Additivity under tensor products. [2 Lemma 19]). For independent pairs of jointly distributed random variables $(S_1,Y_1,Z_1)$ and $(S_2,Y_2,Z_2)$,

$$UI((S_1,S_2);(Y_1,Y_2)|(Z_1,Z_2)) = UI(S_1;Y_1|Z_1) + UI(S_2;Y_2|Z_2).$$

We also have asymptotic continuity for the $UI$.

**Theorem 35** (Asymptotic continuity). $UI$ is asymptotically continuous.

The following theorem gives sufficient conditions for a function to be an upper bound for the secret key rate.

**Theorem 36** ([30 Theorem 3.1], [28 Lemma 2.10]). Let $M$ be a nonnegative real-valued function of the joint distribution of the triple $(S,Y,Z)$ such that the following holds:

1. **Local operations (LO) of Alice or Bob cannot increase $M$:** For all jointly distributed RVs $(S,Y,Z,S')$ such that $YZ - S - S'$ is a Markov chain, $M(S,Y,Z) \geq M(S',Y,Z)$ (and likewise for $Y$).
2. **Public communication (PC) by Alice cannot increase $M$:** $M((S,f(S)),(Y,f(S)),(Z,f(S))) \leq M(S,Y,Z)$ for all functions $f$ over the support of $S$. 


3. Normalization: For a perfect secret bit \( P_{SS\Delta}(0,0,\delta) = P_{SS\Delta}(1,1,\delta) = \frac{1}{2} \). \( M(S,S,\Delta) = 1 \).

4. Asymptotic continuity: \( M \) is an asymptotically continuous function of \((S,Y,Z)\).

5. Additivity: \( M \) is additive on tensor products.

Then \( M \) is an upper bound for the one-way secret key rate.

If, in addition, \( M \) does not increase under public communication by Bob (property 2., with \( f(S) \) replaced by \( g(Y) \) for some function \( g \) over the support of \( Y \)), then \( M \) is an upper bound for the two-way secret key rate.

Theorem 37 is our main result in this Section.

**Theorem 37.** \( UI \) is an upper bound for the one-way secret key rate.

**B. Vanishing unique informations and secret key agreement against active adversaries**

The secret key agreement scenario in Section IV-A assumes that the public discussion channel is authenticated, i.e., Eve is only a passive adversary. When this assumption is no longer valid and Eve has both read and write access to the public channel, an all-or-nothing result is known [23]: Either the same secret key rate can be achieved as in the authentic channel case, or nothing at all. Maurer defined the following property of a distribution to characterize the impossibility of secret key agreement against active adversaries.

**Definition 38.** Given \((S,Y,Z) \sim P\), we say that \( Y \) is simulatable by \( Z \) w.r.t. \( S \) and write \( \text{sim}_S(Z \rightarrow Y) \) if there exists a random variable \( Y' \) such that the pairs \((S,Y)\) and \((S,Y')\) are statistically indistinguishable, and \( S - Z - Y' \) is a Markov chain.

One would immediately recognize that \( \text{sim}_S(Z \rightarrow Y) \) and \( Z \xrightarrow{\text{g}} Y \) in Definition 2 are equivalent. Let \( S^*_{\leftrightarrow}(S;Y|Z) \) denote the secret key rate in the active adversary scenario. We restate Maurer’s impossibility result (Theorem 11 in [23]) in terms of the function \( UI \).

**Theorem 39** ([23, Theorem 11]). Let \((S,Y,Z) \sim P\) be a distribution with \( S^*_{\leftrightarrow}(S;Y|Z) > 0 \). If either \( UI(S;Y|Z) = 0 \) or \( UI(Y;S|Z) = 0 \), then \( S^*_{\leftrightarrow}(S;Y|Z) = 0 \), else \( S^*_{\leftrightarrow}(S;Y|Z) = S^*_{\leftrightarrow}(S;Y|Z) \).

**Remark 40.** Theorem 39 gives an operational significance to the vanishing \( UI \), namely, if either \( S \) or \( Y \) possess no unique information about each other w.r.t. \( Z \), then Alice and Bob have no advantage in a secret key agreement task against an active Eve. By Proposition 28 the same is true for \( UI_0 \).

**Example 41** shows a distribution for which \( S^*_{\leftrightarrow}(S;Y|Z) > 0 \) but \( S^*_{\leftrightarrow}(S;Y|Z) = 0 \).

**Example 41** ([33, Example 4]). Consider the distribution

| \( S \) | \( Y \) | \( Z \) |
|---|---|---|
| \( S \) | 0 \( \frac{1}{2} \) \( \frac{1}{2} \) | 0 (0) |
| \( S \) | 1 \( \frac{1}{2} \) \( 0 \) | 0 (1) |

where \( Z \)’s value is shown in parentheses. This distribution has \( I(S;Y|Z) = \tilde{I}(S;Y,Z) = 0.02 \) and \( CI(S;Y,Z) = 0.55 \). [33] showed that a secret key agreement protocol exists such that \( S^*_{\leftrightarrow}(S;Y|Z) > 0 \). However since the pairwise marginal distributions of \((S,Y)\), \((S,Z)\) and \((Y,Z)\) are all identical, all the unique informations vanish. Hence \( S^*_{\leftrightarrow}(S;Y|Z) = 0 \).

**V. Conclusion**

The information decomposition framework extends earlier ideas to define information measures that make it possible to do a finer analysis than is possible with Shannon’s mutual information alone. For example, measures of redundancy and synergy have long been sought in the neural sciences [7], [8], [11].

In this paper, we proposed two new quantities that can be interpreted as unique informations in the context of nonnegative mutual information decompositions. The quantities are derived using a generalized version of weighted Le Cam deficiencies that have a rich heritage in the theory of comparison of statistical experiments [21]. We related the proposed quantities to the function \( UI \) proposed in [2]. We gave an operational interpretation of the latter in terms of an upper bound on the number of secret key bits extractable per copy of a given joint distribution using local operations and one-way public communication. It might be of independent interest to characterize the set of distributions for which two-way secret key agreement is possible at a rate given by the unique information.
APPENDIX

A. Proofs

Proof of Proposition 8 If \( \delta_{\alpha}^\pi(\mu, \kappa) \leq \epsilon \), then we can find some \( \lambda \in M(\mathcal{Z}; \mathcal{Y}) \) such that \( D(\kappa||\lambda \circ \mu|\mathcal{P}_S) \leq \epsilon \). Let \( \rho' \in M(\mathcal{Y}; \mathcal{A}) \) and let \( \rho = \rho' \circ \lambda \). Then

\[
\begin{align*}
R(\pi_S, \mu, \rho, \ell) - R(\pi_S, \kappa, \rho', \ell) &= E_{s \sim \pi_S}[E_{a \sim \rho_S}(s, a) - E_{a \sim \rho' \circ \kappa_S}(s, a)] \\
&\leq E_{s \sim \pi_S}[\|\rho \circ \mu_S - \rho' \circ \kappa_S\|_{TV} \ell] \\
&\leq E_{s \sim \pi_S}[\|\rho' \circ \lambda \circ \mu_S - \rho' \circ \kappa_S\|_{TV} \ell] \\
&\leq E_{s \sim \pi_S}[\|\lambda \circ \mu_S - \kappa_S\|_{TV} \ell] \\
&\leq E_{s \sim \pi_S} \left[ \sqrt{\ln(2)} D(\kappa \circ \mu|\mathcal{P}_S) \right] \ell
\end{align*}
\]

where we have used the data processing inequality for the total variation (TV) distance in the fourth step and Pinsker’s inequality in the fifth. The last step follows from the concavity of the square root function. Finally, take a minimum over \( \rho' \) and \( \rho \). This completes the proof.

Proof of Proposition 13 Let \( (S, Y, Z) \sim P \). Consider first the case when \( UI_o(S; Y \setminus Z) = \delta_{\alpha}^\pi(\mu, \kappa) \). Then \( UI_o \) is nonnegative by definition. Let \( \lambda^* \in M(\mathcal{Z}; \mathcal{Y}) \) achieve the minimum in (7). Then \( CI_o \) is nonnegative since

\[
I_o(S; Y|Z) = \sum_s P(s) \sum_z P(y|s) D(P(y|s, z)||P(y|z))
\]

where the first inequality follows from the convexity of the Kullback-Leibler divergence and the second inequality follows from the definition of \( \lambda^* \).

\[
SI_o(S; Y, Z) = D(P_Y|S \parallel P_Y|P_S) - D(P_Y|S \parallel \lambda^*_Y|P_Y|S) \\
\geq D(P_Y|S \parallel P_Y|P_S) - D(P_Y|S \parallel P_Y|P_Z|S|P_S) = 0.
\]

The proof for the case when \( UI_o(S; Y \setminus Z) = \delta_{\alpha}^\pi(\kappa, \mu) + I(S; Y) - I(S; Z) \) or equivalently \( UI_o(S; Z \setminus Y) = \delta_{\alpha}^\pi(\kappa, \mu) \) by the consistency condition (4) is similar.

Proof of Lemma 14 If \( Y \) has no unique information about \( S \) w.r.t. \( Z \), then \( UI(S; Y \setminus Z) = 0 \). Thus, \( UI_o(S; Y \setminus Z) \) vanishes by Lemma 26. Conversely, assume that \( UI_o(S; Y \setminus Z) \) vanishes. By Definition 11 since \( \delta_{\alpha}^\pi(\mu, \kappa) \) is a nonnegative quantity, it follows that \( \delta_{\alpha}^\pi(\mu, \kappa) = 0 \). By definition, \( \kappa = \lambda \circ \mu \) for some \( \lambda \in M(\mathcal{Z}; \mathcal{Y}) \), whence \( Y \) has no unique information about \( S \) w.r.t. \( Z \).

Proof of Proposition 20 The proof is similar to that of Proposition 13 and is omitted.

Proof of Proposition 20 The proof is direct by noting that \( I(S; Y) - I_S(Y \setminus Z) = D(\kappa||Q_{Y \setminus Z}|\pi_Y) \) and the fact that

\[
D(\kappa||Q_{Y \setminus Z}|\pi_Y) = \sum_{y \in \mathcal{Y}} \pi_Y(y) \min_{Q \in \text{conv}(\{\mu_z \}_{z \in \mathcal{Z}})} D(\kappa_y||Q) \\
= \min_{\lambda \in M(\mathcal{Y}; \mathcal{Z})} \sum_{y \in \mathcal{Y}} \pi_Y(y) D(\kappa_y||\lambda_y) = \delta_{\alpha}^\pi(\mu, \kappa).
\]

Proof of Lemma 30 Let \( (S, S', Y, Y', Z) \sim P' \) and let \( P \) be the \( (S, Y, Z) \)-marginal of \( P' \). Let \( Q' \in \Delta_{P'} \), and let \( Q \) be the \( (S, Y, Z) \)-marginal of \( Q' \). Then \( Q \in \Delta_P \). Moreover,

\[
I_Q'(SS'; YY'|Z) \geq I_Q(S; Y|Z) = I_Q(S; Y|Z).
\]
The proof is complete by taking the minimum over $Q' \in \Delta_{P'\prime}$. \hfill \blacksquare

**Proof of Lemma 31.** Let $(S, Y, Z)$ be a Markov chain. Let $P'\prime$ be a marginal distribution of $(S', Y, Z)$, and let $P$ be the $(S, Y, Z)$-marginal. Let $Q^* = \arg\min_{Q \in \Delta_{P'}} I_Q(S; Y | Z)$, and let

$$Q''(s', y, z) = \sum_s P'(s' | s) Q^*(s, y, z).$$

Then $Q'' \in \Delta_{P'}$. By definition,

$$UI(S; Y \mid Z) = I_{Q'}(S; Y | Z) \geq I_{Q''}(S'; Y | Z) \geq \min_{Q' \in \Delta_{P'}} I_Q(S; Y | Z) = UI(S'; Y \mid Z),$$

where the conditional form of the data processing inequality was used. This chain of inequalities shows that $Q''$ increase under local operations of $Q$. Consequently, the proof is complete by taking the minimum over $Q \in \Delta_{P'}$. \hfill \blacksquare

**Proof of Lemma 32.** Let $(S, Y, Z)$ be a Markov chain. Let $P \in \Delta_{P'}$, and let $Q'(s, y, z, z') := Q(s, y, z) P'(z' | s)$. Then

$$I_Q(S; Y | Z) = I_Q(S; Y | Z) \geq I_{Q'}(S; Y | Z) + I_Q'(Z' | S, Y | Z) = I_{Q'}(S; Y | Z) = I_{Q'}(S; Y | Z).$$

The proof is complete by taking the minimum over $Q' \in \Delta_{P'}$.

**Proof of Lemma 33.** Write $S' = f(S)$. Let $(S, Y, Z)$ be a Markov chain. Let $P \in \Delta_{P'}$, and define $Q'(s, y, z, s') = Q(s, y, z) P'(s' | s)$ if $P(s) > 0$ and $Q'(s, y, z, s') = 0$ otherwise. Then $Q' \in \Delta_{P'}$. Moreover, $Q$ is the $(S, Y, Z)$-marginal of $Q'$, and $Q'$ is the $(S, Y, Z)$-marginal of $Q$. Therefore,

$$I_Q(S; Y | Z) = I_Q(S; Y | Z) \geq I_{Q'}(S; Y | Z) + I_Q'(Z' | S, Y | Z) = I_{Q'}(S; Y | Z) = I_{Q'}(S; Y | Z).$$

The proof is complete by taking the minimum over $Q \in \Delta_{P'}$. \hfill \blacksquare

To prove asymptotic continuity (Theorem 35), we need the following lemma.

**Lemma 42.** Let $P, P' \in \mathbb{P}_{S \times Y \times Z}$. For any $Q \in \Delta_{P'}$ there exists $Q' \in \Delta_{P'}$ with $||Q - Q'||_1 \leq 5 ||P - P'||_1$.

**Proof.** The signed measure $M = Q + P' - P$ has the same pair margins as $P'$ for the pairs $(S, Y)$ and $(S, Z)$, and $M$ is normalized (that is, $\sum_{s, y, z} M(s, y, z) = 1$). If $M$ is nonnegative, the statement of the lemma is true, since $||M - Q||_1 = ||P - P'||_1$, with $Q' = M$. Otherwise there exist $s_0, y_0, z_0$ with $M(s_0, y_0, z_0) < 0$. Since $\sum_{s, y, z} M(s, y, z) = P'(s_0, z_0) \geq 0$ and $\sum_{s, y, z} M(s, y, z) = P'(s_0, z_0) \geq 0$ there exist $y_1 \neq y_0$ and $z_1 \neq z_0$ with $M(s_0, y_1, z_0) > 0$ and $M(s_0, y_0, z_1) > 0$. Let $\nu = \min \{ M(s_0, y_1, z_0), M(s_0, y_0, z_1), |M(s_0, y_0, z_0)| \} > 0$, and consider the measure $M'$ defined by

$$M'(s_0, y_0, z_0) = M(s_0, y_0, z_0) + \nu,$$

$$M'(s_0, y_1, z_0) = M(s_0, y_1, z_0) - \nu,$$

$$M'(s_0, y_0, z_1) = M(s_0, y_0, z_1) - \nu,$$

$$M'(s_0, y_1, z_1) = M(s_0, y_1, z_1) + \nu,$$

$$M'(s, y, z) = M(s, y, z), \quad \text{otherwise}.$$

Then $M'$ has the same pair margins as $M$ and $P'$ for the pairs $(S, Y)$ and $(S, Z)$, and $M$ is normalized. Moreover, the absolute sum over the negative entries decreases:

$$\sum_{s, y, z : M(s, y, z) < 0} |M(s, y, z)| \geq \sum_{s, y, z : M'(s, y, z) < 0} |M'(s, y, z)| + \nu > \sum_{s, y, z : M'(s, y, z) < 0} |M'(s, y, z)|.
Finally, \( \|M - M'\|_1 \leq 4\nu \). Iterating the procedure, one obtains a normalized measure \( M'' \) that has the same pair margins as \( M \) and \( P'' \) and that is non-negative. The triangle inequality shows
\[
\|M'' - M\|_1 \leq 4 \sum_{s,y,z:M(s,y,z)<0} |M(s,y,z)| \leq 4\|P - P'\|_1.
\]
Thus, \( \|M'' - Q\|_1 \leq \|M'' - M\|_1 + \|M - Q\|_1 \leq 5\|P - P'\|_1 \). Hence, the statement follows with \( Q' = M'' \).

**Proof of Theorem 35** Let \( P, P' \in \mathbb{P}_{S \times Y \times Z} \), let \( Q \in \arg \min_{Q \in \Delta_{P'}} I_Q(S; Y | Z) \). Choose \( Q' = \Delta_{P''} \) as in Lemma 42 and let \( Q^* \in \arg \min_{Q \in \Delta_{P''}} I_Q(S; Y | Z) \). Then
\[
I_{P'}(S; Y | Z) - I_{P'}(S; Y | Z) = I_{Q'}(S; Y | Z) - I_Q(S; Y | Z) \leq I_Q(S; Y | Z) - I_Q(S; Y | Z) \leq 2h'(\epsilon) + \frac{\epsilon}{2} \log \min\{|S|, |Y|\},
\]
where \( h'(\epsilon) = \max_{0 \leq x \leq \min\left(\frac{\epsilon}{M}, 1\right)} h(x), h(\cdot) \) is the binary entropy function and where we have used the fact that for any \( P, P' \in \mathbb{P}_{S \times Y \times Z} \), if \( \|P - P'\|_1 = 2\epsilon \) then \( I_{P'}(S; Y | Z) \leq I_P(S; Y | Z) + 2h(\epsilon) + \epsilon \log \min\{|S|, |Y|\} \) \( \square \).

**Proof of Theorem 37** The function \( UI \) satisfies additivity (see Lemma 34), asymptotic continuity (see Theorem 35) and the Normalization property. Furthermore, \( UI \) satisfies monotonicity under local operations of Alice and Bob (see Lemma 31) and monotonicity under one-way public communication by Alice (see Lemma 33). Hence, by Theorem 36 \( UI \) is an upper bound to the one-way secret key rate. \( \square \)

**B. Optimization problems**

The optimization problems in definitions 7, 10 and 22 of the functions \( \delta_\pi^\gamma \), \( \delta_\pi^x \), and \( UI \), respectively, are convex programs. Furthermore, the feasible sets in definitions 10 and 22 have a nice product structure in relation to the corresponding objective functions.

Given \( (S, Y, Z) \sim P \) and a value \( s \in S \), let \( A_s : \mathbb{P}_{Y \times Z} \to \mathbb{P}_Y \times \mathbb{P}_Z \) be the linear map that computes the marginal distributions of \( Y \) and \( Z \), given \( P_{Y|Z|s} \). Each \( Q \in \Delta_P \) in (14b) has the form \( Q = \pi S Y Z | S \in S \times s \in \Delta_{P,s} \), where
\[
\Delta_{P,s} := \{ Q_{YZ} \in \mathbb{P}_{Y \times Z} : Q_Y(y) = \kappa_s(y), Q_Z(z) = \mu_s(z) \}, \quad s \in S
\]
is a fiber of \( A_s \) passing through \( P_{Y|Z|s} \). Then \( \Delta_{P,s} = (P_{Y|Z|s} + \ker A_s) \cap \mathbb{P}_{Y \times Z} \). As an intersection of an affine space with the probability simplex, \( \Delta_{P,s} \) is a polytope. Using a variational representation of the conditional mutual information (a.k.a. the Golden formula), the objective in (14b) can be written as a double minimization.

\[
UI(S; Y | Z) = \min_{Q \in \Delta_P} I_Q(S; Y | Z) = \min_{Q_{YZ} \in \mathbb{P}_{Y \times Z} \Delta_{P,s} \lambda \in \mathbb{M}(Z; Y)} D(Q_{YZ} | S) \lambda \times \mu \| \pi S
\]
\[
= \min_{\lambda \in \mathbb{M}(Z; Y)} \sum_s \pi S(s) \min_{Q_{YZ} \in \Delta_{P,s}} D(Q_{YZ} | S) \lambda \times \mu.
\]

Proposed an efficient alternating minimization algorithm to solve (20). An alternating minimization algorithm recursively fixes one of the two free variables and minimizes the other. When \( \lambda \) is fixed, each summand involves computing an \( I \)-projection (27) to the linear family of probability distributions of \( (Y, Z) \) defined by \( \Delta_{P,s} \). The different summands can be optimized parallely for the different values of \( s \in S \).

For the weighted input deficiency (8),
\[
\delta_\pi^x(\bar{\mu}, \bar{\kappa}) = \min_{\lambda \in \mathbb{M}(\bar{\mu}; \bar{\kappa})} \sum_{y \in \mathcal{Y}} \pi_Y(y) D(\bar{\kappa}_y \| \bar{\mu})
\]
\[
= \sum_{y \in \mathcal{Y}} \pi_Y(y) \min_{Q \in \{ \bar{\mu} : s \in \mathcal{E} \} \mathcal{P}_S} D(\bar{\kappa}_y \| Q),
\]
each summand involves computing a \( rI \)-projection (27) to a convex set of probability distributions. Again, the summands can be optimized separately for the different values of \( y \in \mathcal{Y} \). This is useful in practice in parallelizing the computations.
