Beware of Greeks bearing entanglement? Quantum covert channels, information flow and non-local games

David Mestel
University of Luxembourg
david.mestel@uni.lu

2022 IEEE 35th Computer Security Foundations Symposium (CSF) | 978-1-6654-8417-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSF54842.2022.9919683

***Abstract*—Can quantum entanglement increase the capacity of (classical) covert channels? To one familiar with Holevo's Theorem it is tempting to think that the answer is obviously no. However, in this work we show: quantum entanglement can in fact increase the capacity of a classical covert channel, in the presence of an active adversary; on the other hand, a zero-capacity channel is not improved by entanglement, so entanglement cannot create 'purely quantum' covert channels; the problem of determining the capacity of a given channel in the presence of entanglement is undecidable; but there is an algorithm to bound the entangled capacity of a channel from above, adapted from the semi-definite hierarchy from the theory of non-local games, whose close connection to channel capacity is at the core of all of our results.**

***Index Terms*—covert channels, information flow, quantum information**

I. Introduction

Suppose that you are processing sensitive data using a computer. How do you know that your computer was not given to you in a state of quantum entanglement with an eavesdropping adversary? This is a situation that (unlike the presence of Greek soldiers) cannot be detected by any local experiment. It does not require the victim to be using any kind of quantum technology.[1]

Fortunately, the presence of entanglement does not of itself jeopardise the privacy of one's data. This is due to the 'non-signalling' property of entanglement: although the adversary is able to obtain non-classical correlations with the victim's measurement outcomes, this does not allow him to deduce anything about what those measurements were (otherwise distant entanglement would enable faster-than-light communication). But what if the adversary *also* has access to some legitimate interaction with the victim, such as use of a shared resource? Is it possible for entanglement to create a covert channel where none would otherwise exist, or to increase the power of an existing channel? The purpose of the present work is to address this question.

Holevo's Theorem [1] states (in relevant part) that entanglement cannot increase the classical Shannon capacity of a purely classical discrete memoryless channel. It is therefore tempting to assume that this means the answer to the above question is 'no'; however, as we shall see, in fact the picture is rather more complex.

An abstracted representation of a system which may or may not give rise to a covert channel is shown in Figure 1. A victim, Alice, interacts with some system $\mathcal{C}$, to which access is also given to an eavesdropper, Bob. Bob may only receive messages from the system (a passive adversary), or he may also be able to send messages (an active adversary). We say that a covert channel exists if Bob is able to learn something about Alice's actions from his observations; this is set out formally in the classic paper of Goguen and Meseguer [2]. Note that we make the assumption that Alice is actively trying to convey information to Bob. This may be because she (perhaps a malicious process) is trying to exfiltrate data across what should be an information flow barrier. Alternatively she may be an innocent victim (in this situation the covert channel is often called a 'side-channel'), but if her behaviour is not specified then a conservative analysis must assume that she could behave as if trying to exfiltrate data.

It may be, however, that the question just of whether Bob can learn *anything* is too crude, and we may be interested in *how much* information can reach Bob from Alice; this is the subject of the field of 'Quantitative Information Flow' (QIF). The original approach [3] was to compute the Shannon mutual information between Alice's actions and Bob's observations, but it was pointed out by Smith [4] that this is usually inappropriate. This has given rise to extensive study of various possible measures of information flow; see the recent book [5]. However, in this work we will mainly (with the exception of Section VI) be agnostic as to the choice of measure, subject to mild reasonableness conditions.

The goal of QIF is essentially to analyse Figure 1 in quantitative fashion. The goal of this paper is to extend this analysis to the situation where Alice and Bob may share entanglement. We define information flow in this setting and then address some fundamental questions. Can entanglement make any difference? Can we tell how much? Can entanglement introduce covert channels where none existed before?

The author is supported by FNR under grant INTER FNRS/15/11106658/SeVoTe.

[1] Although we must acknowledge that it would require the adversary to have technical capabilities beyond those publicly known, since holding systems in superposition is currently a sensitive, fragile and usually short-lived affair.

DOI 10.1109/CSF54842.2022.00017

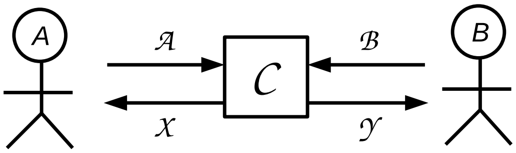

Fig. 1. An abstracted system

Overview

The structure of this paper is as follows. In Section II we set out basic concepts and definitions, for both classical information flow and quantum entanglement. In Section III we define an entangled version of information flow. We then introduce the reader to 'non-local games', an important concept from Quantum Information Theory that provides the technical machinery for many of our results, and show by a simple reduction from a certain game (the 'CHSH game') that it is possible for entangled capacity to exceed classical capacity (Theorem 10). In Section IV, on the other hand, we show that if a channel has zero classical capacity then it also has zero entangled capacity (Corollary 14), and so it is not possible for entanglement to introduce 'purely quantum' covert channels. In Section V, we consider the problem of computing the entangled capacity of a given channel, and show using the very recent breakthrough result MIP* = RE [6] that the problem of computing this capacity, even to within a constant factor approximation, is undecidable (Theorem 18). More positively, in Section VI we show that the Semi-Definite Programming (SDP) methods [7] for bounding the value of non-local games can be adapted to give upper bounds for entangled channel capacity. Finally in Section VII we reflect on the connection between covert channel capacity and non-local games, and consider future directions for quantum QIF.

Related work

As far as we are aware, the only work which has attempted to extend QIF into the quantum realm is the paper of Américo and Malacaria [8]. This studies a rather different setting, in which Alice sends to Bob a quantum state ρ^x which is a (specified) function of the secret value $x \in \mathcal{X}$; Bob is then allowed to apply a single measurement of his choice from a fixed set of allowed measurements, and the question is how much Bob can learn about the secret x according to various measures of information flow. This is of course only relevant to a network in which quantum states can be passed around.

The question of communication channels and their capacity is of course central to information theory, and quantum information theory is a huge topic in modern physics (see for instance [9]). However, perhaps surprisingly the present setting of the classical capacity of a classical fully interactive multi-round channel assisted by entanglement has not as far as we can tell been previously studied (see also the more recent survey [10]). This may be because physicists are generally more interested in quantum channels (which allow quantum states to be sent and received), or in the effect of entanglement on the quantum capacity of classical channels (which surprisingly can be positive due to the technique of 'quantum teleportation'). Additionally, the idea of a fully interactive channel may not seem particularly 'physical', since it is fairly far from the classic setting of a noisy communication medium; on the other hand such a situation is common in the setting of covert channels or side-channels arising from use of a shared resource or interaction with a common system.

II. Preliminaries

A. Classical information flow

Although many different models (at varying levels of abstraction) have been used in other works to represent the behaviour of the system, for this paper we will adopt a simple abstract model, a finite-round version of the model from the author's prior work [11] (and a multi-round version of the model used in [12]). We assume that Alice and Bob interact with the system over k rounds, at each round sending a message drawn from finite sets $\mathcal{A}$ and $\mathcal{B}$ respectively, and receiving in return messages from finite sets $\mathcal{X}$ and $\mathcal{Y}$ respectively. The behaviour of the system is then specified just by functions determining the probability distribution on output messages, based on the actions that have occurred up to that point:

Definition 1. *An* n-round abstract interactive channel *(n-IC) is given by finite sets* $\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}$ *and an* n*-tuple* $(f_1, \dots, f_n)$ *of functions*

$$f_i : (\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y})^{i-1} \times (\mathcal{A} \times \mathcal{B}) \to \mathbb{D}(\mathcal{X} \times \mathcal{Y}).$$

Note that $\mathbb{D}(\mathcal{X} \times \mathcal{Y})$ denotes the space of probability distributions on the set $\mathcal{X} \times \mathcal{Y}$. Note also that no generality is lost by using the same finite sets for each round of interaction: to represent a system using sets $\mathcal{A}_i, \mathcal{B}_i, \mathcal{X}_i, \mathcal{Y}_i$ at round i, take $\mathcal{A} = \sqcup_i \mathcal{A}_i$ (the disjoint union of the $\mathcal{A}_i$), and similarly for $\mathcal{B}, \mathcal{X}$ and $\mathcal{Y}$. Choose arbitrary $a_i \in \mathcal{A}_i$ and $b_i \in \mathcal{B}_i$, and set the images of the f_i to be supported only on $\mathcal{X}_i \times \mathcal{Y}_i$ and treat inputs at round i which are not in $\mathcal{A}_i$ (respectively $\mathcal{B}_i$) as though they were a_i (respectively b_i).

A simple example of such a system is a fair resource scheduler, which receives requests from Alice and Bob and (if both ask to use the resource) allocates the resource to whichever has received it fewer times in the past (breaking ties randomly). This has $\mathcal{A} = \mathcal{B} = \mathcal{X} = \mathcal{Y} = \{0, 1\}$, and $f_i(t, (1, 0)) = (1, 0), f_i(t, (0, 1)) = (0, 1), f_i(t, (0, 0)) = (0, 0)$, and

$$f_i(t, (1, 1)) = \begin{cases} (1, 0), & \text{if } \#_{\mathcal{X}}(t) < \#_{\mathcal{Y}}(t) \\ (0, 1), & \text{if } \#_{\mathcal{X}}(t) > \#_{\mathcal{Y}}(t)) \\ \frac{1}{2}(1, 0) + \frac{1}{2}(0, 1), & \text{if } \#_{\mathcal{X}}(t) = \#_{\mathcal{Y}}(t), \end{cases}$$

where $\#_{\mathcal{X}}(t)$ and $\#_{\mathcal{Y}}(t)$ denote the number of positions in t where the third (respectively fourth) co-ordinate is 1, and $(x, y) \in \mathbb{D}(\mathcal{X} \times \mathcal{Y})$ denotes the point distribution supported at (x, y). This system clearly does give rise to information leakage, because by always requesting use of the resource

Bob is able to (imperfectly) learn about whether Alice has requested it.

Given the specification of a channel $\mathcal{C}$, we are interested in the possible ways Alice and Bob may interact with the system, which we denote by their *strategies*. Clearly Alice is unable to see the messages passing between the system and Bob, and so her strategy at each step is represented by a function on the transcript of her interaction so far; similarly for Bob.

Definition 2. *Let $\mathcal{C} = (\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, (f_1, \dots, f_n))$ be an n-IC. A* classical $\mathcal{A}$-strategy *(respectively $\mathcal{B}$-strategy) for $\mathcal{C}$ is a tuple $(g_1, \dots, g_n)$ of functions*

$$g_i : (\mathcal{A} \times \mathcal{X})^{i-1} \to \mathbb{D}(\mathcal{A}),$$

respectively $h_i : (\mathcal{B} \times \mathcal{Y})^{i-1} \to \mathbb{D}(\mathcal{B})$. Denote the sets of such strategies by $\mathcal{S}_\mathcal{A}$ and $\mathcal{S}_\mathcal{B}$ respectively.

Having thus fixed the strategies followed by Alice and Bob, we obtain a probability distribution on traces of the system execution: writing $s_A = (g_1, \dots, g_n)$ and $s_B = (h_1, \dots, h_n)$ we have that the trace $t = ((a_1, b_1, x_1, y_1), \dots, (a_n, b_n, x_n, y_n))$ occurs with probability

$$\prod_{i=1}^{n} g_i(\pi_A(t_{i-1}))(a_i) h_i(\pi_B(t_{i-1}))(b_i) f_i(t_{i-1}, (a_i, b_i))(x_i, y_i),$$

writing t_i for the ith prefix of t and π_A and π_B for the projections onto $(\mathcal{A} \times \mathcal{X})^*$ and $(\mathcal{B} \times \mathcal{Y})^*$ respectively representing Alice and Bob's views of the system. We denote the trace produced by strategies s_A and s_B by the random variable T_{s_A, s_B}.

Now that we have defined the behaviour of the system and the parties, we are able to talk about information flow. We assume there is some secret about which Bob wishes to learn, which we will denote by the random variable K; Alice's strategy may depend in some way on the value of K. The question is, how much more does Bob know about K after the interaction than before? As outlined in Section I there are various possible ways to measure this, so our definition (essentially the formalism of [13]) is parameterised by a 'vulnerability measure' $\mathbb{V}$ on probability distributions.

Before he and Alice interact with the system, Bob's knowledge of the secret will be limited to the prior distribution of the random variable K; we quantify this knowledge by the vulnerability of this distribution according to the vulnerability measure $\mathbb{V}$, which we denote by $\mathbb{V}(K)$.

On the other hand, after the interaction Bob will have observed some trace t consisting of the messages passing between him and the system, and this allows him to update his beliefs about the secret to the *posterior* distribution $K|\pi_B(T) = t$ (recall that Bob is only able to observe the projection of the whole system trace T onto $(\mathcal{B} \times \mathcal{Y})^n$, since he does not see the messages passing between the system and Alice). In quantitative terms his knowledge of the secret is given by $\mathbb{V}(K|\pi_B(T) = t)$; we call the expected value of this quantitiy the 'posterior $\mathbb{V}$-vulnerability' and the expected difference between prior and posterior $\mathbb{V}$-vulnerability (that is the expected amount of information gained by Bob) the '$\mathbb{V}$-leakage' of the channel with the given prior distribution on K.

Definition 3. *Let $\mathcal{C}$ be an n-IC, and K a random variable taking values on the set $\mathcal{K}$. Let $\phi_A : \mathcal{K} \to \mathcal{S}_\mathcal{A}$ and $s_B \in \mathcal{S}_\mathcal{B}$. Let $\mathbb{V}$ be any vulnerability measure. The* posterior $\mathbb{V}$-vulnerability of K under *$(\mathcal{C}, \phi_A, s_B)$ is given by*

$$\begin{aligned}\mathcal{V}_\mathbb{V}(K, (\mathcal{C}, &\phi_A, s_B)) \\ &= \mathbb{E}_{t \sim \pi_B(T_{\phi_A(K), s_B})} \mathbb{V}\left(K | \pi_B(T_{\phi_A(K), s_B}) = t\right).\end{aligned}$$

The $\mathbb{V}$-leakage of K under *$(\mathcal{C}, \phi_A, s_B)$ is given by*

$$\mathcal{L}_\mathbb{V}(K, (\mathcal{C}, \phi_A, s_B)) = \mathcal{V}_\mathbb{V}(K, (\mathcal{C}, \phi_A, s_B)) - \mathbb{V}(K).$$

Note that the posterior distribution $K|\pi_B(T_{\phi_A(K), s_B}) = t$ is straightforwardly given by Bayes' theorem

$$p_{K|\pi_B(T_{\phi_A(K), s_B})}(k|t) = \frac{p_{\pi_B(T_{\phi_A(K), s_B})|K}(t|k) p_K(k)}{p_{\pi_B(T_{\phi_A(K), s_B})}(t)}.$$

Some important examples of vulnerability measures:

- Shannon entropy: $\mathbb{V}(K) = -H_1(K) = \sum_k p_K(k) \log(p_K(k))$. This gives a measure of leakage corresponding to mutual information.
- Min-entropy [4]: $\mathbb{V}(K) = -H_\infty(K) = \log \max_k p_K(k)$. This has a natural operational interpretation, as (log of) the multiplicative improvement in Bob's probability of guessing the value of K in one try.
- g-vulnerability [14]: this is a family of vulnerability measures, parameterised by a finite set of guesses $\mathcal{W}$ Bob can make, and a 'gain function' $g : \mathcal{W} \times \mathcal{K} \to [0, 1]$ giving the reward to Bob for making guess w if the true value was k. Then the expected value of Bob's multiplicative gain is given by $\mathbb{V}$-leakage with $\mathbb{V}(K) = \log \max_w p_K(k) g(w, k)$. We may also be interested in Bob's additive gain, which is given by $\mathbb{V}(K) = \max_w p_K(k) g(w, k)$ (omitting the log).

The definition of $\mathbb{V}$-leakage can be expressed more concisely using an analogue of Shannon mutual information (which gives the asymptotic capacity of a binary symmetric channel), parametrised by the vulnerability measure $\mathbb{V}$: if we define

$$I_\mathbb{V}(X; Y) = \mathbb{E}_{y \sim Y} \mathbb{V}(X | Y = y) - \mathbb{V}(X)$$

then we have that

$$\mathcal{L}_\mathbb{V}(K, (\mathcal{C}, \phi_A, s_B)) = I_\mathbb{V}(K; \pi_B(T_{\phi_A(K), s_B})).$$

Note that if $\mathbb{V}$ is Shannon entropy then $I_\mathbb{V}$ is Shannon mutual information; this is symmetric in X and Y but $I_\mathbb{V}$ is not in general symmetric for other vulnerability measures.

We then define the $\mathbb{V}$-capacity of the channel to be the maximum possible $\mathbb{V}$-leakage over all possible secrets K and all possible behaviours for Alice and Bob.

Definition 4. *Let $\mathcal{C}$ be an n-IC. The* classical $\mathbb{V}$-capacity of *$\mathcal{C}$ is given by*

$$\mathcal{L}_\mathbb{V}(\mathcal{C}) = \sup_K \sup_{\phi_A : K \to \mathcal{S}_\mathcal{A}, s_B \in \mathcal{S}_\mathcal{B}} \mathcal{L}_\mathbb{V}(K, (\mathcal{C}, \phi_A, s_B)).$$

Throughout this paper, we will consider only vulnerability measures satisfying three healthiness conditions, which hold for all reasonable measures and which we will need to use in order to prove some of our results later on (in particular for the proof of Theorem 17). The first healthiness condition we will call the *composition inequality*. Informally, this says that if we have a composition of channels $X \to Y \to Z$ then the capacity of the channel from X to Z is not greater than that of those from X to Y and from Y to Z. Clearly this is a property that any sensible vulnerability measure should have.

More formally, for random variables X, Y, Z, we say that they form a *Markov chain*, and write $X \to Y \to Z$ if we have $p_{X,Y,Z}(x, y, z) = p_X(x)p_{Y|X}(y|x)p_{Z|Y}(z|y)$ (note that this property is symmetric, so that $X \to Y \to Z$ if and only if $Z \to Y \to X$; see [15] Section 2.8). We say that a vulnerability measure $\mathbb{V}$ satisfies the composition inequality if for every Markov chain $X \to Y \to Z$ we have

$$I_{\mathbb{V}}(X;Z) \leq \sup_{Y'|X'=Y|X} I_{\mathbb{V}}(X';Y')$$

and

$$I_{\mathbb{V}}(X;Z) \leq \sup_{Z'|Y'=Z|Y} I_{\mathbb{V}}(Y';Z').$$

This fact for Shannon entropy vulnerability follows from the data-processing inequality ([15], Theorem 2.8.1), and for min-entropy is Theorem 6 of [16]. Note that the first inequality without the supremum (which would bound information flow rather than capacity) can fail for min-entropy vulnerability (see Example 7 of [16]), but both hold for Shannon entropy.

The second healthiness condition we will require is that the vulnerability of a Bernoulli random variable is (strictly) less if it is closer to uniform. That is, if $\rho, \rho' \in [0, 1]$ with $|\rho - 1/2| < |\rho' - 1/2|$ then we have

$$\mathbb{V}(\mathrm{Ber}(\rho)) < \mathbb{V}(\mathrm{Ber}(\rho')),$$

where $\mathrm{Ber}(\rho)$ is the Bernoulli distribution with parameter ρ.

The third and final assumption we make about $\mathbb{V}$ is that if we have a binary symmetric channel then the best way to use it is to send a uniformly random bit. More concretely, we assume that if (X, Y) is a binary symmetric channel with error probability p then $I_{\mathbb{V}}(X;Y)$ maximised when $X \sim \mathrm{Ber}(1/2)$, in which case the posterior is $\mathrm{Ber}(1 - p)$, so we assume

$$I_{\mathbb{V}}(X;Y) \leq \mathbb{V}(\mathrm{Ber}(1-p)) - \mathbb{V}(1/2).$$

A consequence of the composition inequality is that without loss of generality we may assume that Alice employs a deterministic strategy: indeed, we may consider her source of randomness to be a random variable X (so that she employs a deterministic strategy on $K \times X$), and then we have that $K \to K \times X \to \pi_B(T)$ is a Markov chain, so the capacity of the channel given by her deterministic strategy on $K \times X$ is at least that of the original strategy. Once we have that Alice uses a deterministic strategy we may assume that $|\mathcal{K}|$ is at most the size of the set of functions $(\mathcal{A} \times \mathcal{X})^{<n} \to \mathcal{A}$, which in particular is bounded. We can similarly show that Bob can be assumed to use a deterministic strategy (assume his randomness is resolved before the interaction and pick the value of the seed leading to the greatest leakage), and so the set of possible strategies is finite and the classical capacity of a given channel is computable.

Returning to the toy example of the fair scheduler described near the beginning of this section, we can easily see that this has postive $\mathbb{V}$-capacity under any vulnerability measure $\mathbb{V}$ satisfying the healthiness conditions. Indeed, let $K \sim U(\{0, 1\})$, and let Bob's strategy s_B be given by $h_i(t) = 1$ for all i, t (that is, Bob always asks to use the resource). Define strategy s_0 for Alice by $g_i(t) = 0$ for all i, t (never asking for the resource) and strategy s_1 by $g_i(t) = 1$ for all i, t (always asking for the resource). For $k \in \{0, 1\}$, let $\phi_A(k) = s_k$.

Now if $K = 0$ then Bob will always receive 1 from the system. If $n \geq 2$ then by fairness if $K = 1$ then Bob will always receive a 0 at least once, and so we have that $K|\pi_B(T_{\phi_A(K),s_B})$ is a point distribution for both $K = 0$ and $K = 1$, and so

$$\begin{aligned}\mathcal{L}_{\mathbb{V}}(\mathcal{C}) &\geq \mathcal{L}_{\mathbb{V}}(K, (\mathcal{C}, \phi_A, s_B)) \\ &= \mathbb{V}(\mathrm{Ber}(1)) - \mathbb{V}(\mathrm{Ber}(1/2)) \\ &> 0\end{aligned}$$

by the second healthiness condition.

If $n = 1$ then if $K = 1$ Bob will receive a 0 or a 1 uniformly at random. Hence if he receives a 0 he can deduce with certainty that $K = 1$, but if he receives a 1 then his posterior is that $K = 0$ with probability $\frac{1}{2}/(\frac{1}{2} + \frac{1}{4}) = \frac{2}{3}$ and $K = 1$ with probability $\frac{1}{3}$. Hence we have

$$\begin{aligned}\mathcal{L}_{\mathbb{V}}(\mathcal{C}) &\geq \mathcal{L}_{\mathbb{V}}(K, (\mathcal{C}, \phi_A, s_B)) \\ &= \big(\tfrac{1}{4}\mathrm{Ber}(1) + \tfrac{3}{4}\mathrm{Ber}(2/3)\big) - \mathbb{V}(\mathrm{Ber}(1/2) \\ &> 0,\end{aligned}$$

again by the second healthiness condition. Of course these lower bounds for $\mathcal{L}_{\mathbb{V}}(\mathcal{C})$ are not tight; the optimal strategy and maximum leakage will depend on the choice of vulnerability measure $\mathbb{V}$.

B. Entanglement

We give here a very brief introduction to the theory of quantum states and quantum measurements; a more detailed introduction can be found in [17].

A quantum system is represented by a complex Hilbert space $\mathcal{H}$ (that is, a complex inner product space such that the distance metric is continuous); for most of this work (except Section VI) we will assume that $\mathcal{H}$ is finite-dimensional, and so $\mathcal{H} \cong \mathbb{C}^n$ for some n. A *qubit* is a system $\mathcal{H} = \mathbb{C}^2$ and we write $\{|0\rangle, |1\rangle\}$ an orthonormal basis for $\mathcal{H}$ (the 'standard basis vectors').

A *state* of the system is a unit vector $|\psi\rangle \in \mathcal{H}$ (more precisely this is a 'pure state'; we will not need to consider mixed states in this work). If $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ then we say that $|\psi\rangle \in \mathcal{H}$ is *separable* if $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$; otherwise we say that $|\psi\rangle$ is *entangled*.

What does it mean to make a measurement on a system $\mathcal{H}$? In this work we will consider only *projective* measurements;

that is, measurements such that performing the measurement twice is the same as performing it once (this is without loss of generality since we will never care about the exact dimension of our Hilbert spaces and by the Naimark dilation theorem any measurement can be expressed as a projective measurement on a larger Hilbert space).

By an *orthogonal projective measurement* over $\mathcal{H}$ (hereafter just 'measurement') we mean a collection of Hermitian operators $\{E_i\}_{i\in\mathcal{I}}$ over $\mathcal{H}$, where $\mathcal{I}$ is the set of measurement outcomes, satisfying the following properties:

(i) for each i, $E_i^2 = E_i$ (each E_i is a projection),
(ii) $E_iE_j = 0$ for all $i \neq j$ (orthogonality), and
(iii) $\sum_{i\in\mathcal{I}} E_i = I$ the identity operator.

When we apply the measurement $\{E_i\}_{i\in\mathcal{I}}$ to state $|\psi\rangle$, we obtain result i with probability $\langle\psi|E_i|\psi\rangle$ (where $\langle\psi| = |\psi\rangle^* \in \mathcal{H}^*$ is the dual vector to $|\psi\rangle$); note that this is a probability distribution by condition (iii).

Some examples of measurements (on a single cubit) are measurement in the standard basis, $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, and measurement in the 'Hadamard basis', $\{(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)/2, (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)/2\}$, at an angle $\pi/4$ to the standard basis.

Note that measurements compose, so that if $\{E_i\}_{i\in\mathcal{I}}$ and $\{E_j\}_{j\in\mathcal{J}}$ are projective measurements then so is $\{E_iE_j\}_{(i,j)\in\mathcal{I}\times\mathcal{J}}$, corresponding to measuring $\mathcal{J}$ followed by $\mathcal{I}$. Note that measurements do *not* in general commute, so that $\{E_iE_j\}$ will give different results to $\{E_jE_i\}$. This is the essential difference between quantum and classical measurement, and gives rise to the famous 'uncertainty principle' in quantum mechanics.

III. Entangled channel capacity

A. Definition

We will now consider information flow in the situation in which Alice and Bob may share entanglement. This means that it is no longer possible to consider their strategies entirely separately: they share some entangled state $|\psi\rangle$, and at each step make measurements on their own part of the state (which may depend on the history of their own communication with the system up to that point), and choose a message to send to the system according the the result of the measurement. Alice's choice of measurements, but not Bob's, may also depend on the value of the secret K. Note that without loss of generality we may assume that each measurement consists of one projection for each element of $\mathcal{A}$ (respectively $\mathcal{B}$), since any post-processing of the measurement result into a (possibly random) choice of message can be incorporated into the measurement.

Definition 5. *Let $\mathcal{C}$ be an n-IC, and K a random variable taking values on the set $\mathcal{K}$. A* quantum joint strategy *for $\mathcal{C}$ is a pure state $|\psi\rangle$ in a finite-dimensional complex Hilbert space $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$, and sets $\{A^{k,t}\}$ and $\{B^{t'}\}$ such that*

(i) for every $k \in \mathcal{K}$ and every $t \in (\mathcal{A}\times\mathcal{X})^i$ with $0 \leq i < n$, $A^{k,t} = \{A^{k,t}_a\}_{a\in\mathcal{A}}$ is a measurement over $\mathcal{H}_\mathcal{A}$, and
(ii) for every $t' \in (\mathcal{B}\times\mathcal{Y})^i$ with $0 \leq i < n$, $B^{t'} = \{B^{t'}_b\}_{b\in\mathcal{B}}$ is a measurement over $\mathcal{H}_\mathcal{B}$.

Denote the space of such strategies by $\mathcal{S}^*_{\mathcal{C},K}$.

We again denote the trace produced by strategy s with secret k by the random variable $T_{s,k}$. What is the probability that $T_{s,k}$ takes the value $t = ((a_1, b_1, x_1, y_1), \ldots, (a_n, b_n, x_n, y_n))$? Whereas before in the classical case this was given by the product of the relevant classical probabilities corresponding to the execution t from the functions defining the strategies of Alice and Bob and the behaviour of the machine, now for Alice and Bob we must find the probability that the corresponding sequences of measurements result in the correct outcomes. This is given by the norm on $|\psi\rangle$ of the product of the corresponding projections; on the other hand, since the system itself is purely classical its probability is still given by multiplying the relevant probabilities.

Denote by A^k_t and B_t the projections corresponding to Alice and Bob taking the actions corresponding to trace t at each step; that is

$$\begin{aligned} A^k_t &= A^{k,((a_1,x_1),\ldots,(a_{n-1},x_{n-1}))}_{a_n} A^{k,((a_1,x_1),\ldots,(a_{n-2},x_{n-2}))}_{a_{n-1}} \\ &\qquad \ldots A^{k,((a_1,x_1))}_{a_2} A^{k,\emptyset}_{a_1} \\ B_t &= B^{((b_1,y_1),\ldots,(b_{n-1},y_{n-1}))}_{b_n} B^{((b_1,y_1),\ldots,(b_{n-2},y_{n-2}))}_{b_{n-1}} \\ &\qquad \ldots B^{((b_1,y_1))}_{b_2} B^{\emptyset}_{b_1}. \end{aligned}$$

Writing t_i for the ith prefix of t as before, we have that the probability that $T_{s,K}$ takes the value t is given by

$$\langle\psi|A^k_t \otimes B_t|\psi\rangle \prod_{i=1}^{n} f_i(t_i)(x_i, y_i),$$

where the f_i are the functions specifying the channel behaviour from Definition 1.

As in the classical case, we then say that the information leakage from Alice to Bob $\mathcal{L}_\mathbb{V}(K, (\mathcal{C}, s))$ is given by the increase in $\mathbb{V}$-vulnerability from the prior to Bob's posterior distribution after the interaction, for our preferred choice of vulnerability measure $\mathbb{V}$.

Definition 6. *Let $\mathcal{C}$ be an n-IC. The* entangled $\mathbb{V}$-capacity *of $\mathcal{C}$ is given by*

$$\mathcal{L}^*_\mathbb{V}(\mathcal{C}) = \sup_K \sup_{s\in\mathcal{S}^*_{\mathcal{C},K}} \mathcal{L}_\mathbb{V}(K, (\mathcal{C}, s)),$$

where $\mathcal{L}_\mathbb{V}(K, (\mathcal{C}, s))$ is defined equivalently to Definition 3.

Trivially $\mathcal{L}^*_\mathbb{V}(\mathcal{C}) \geq \mathcal{L}_\mathbb{V}(\mathcal{C})$ for any channel $\mathcal{C}$. We will write $\Delta^*_\mathbb{V}(\mathcal{C})$ for the 'quantum advantage'

$$\Delta^*_\mathbb{V}(\mathcal{C}) = \mathcal{L}^*_\mathbb{V}(\mathcal{C}) - \mathcal{L}_\mathbb{V}(\mathcal{C}).$$

We will say that $\mathcal{C}$ is a *purely quantum channel* if $\mathcal{L}^*_\mathbb{V}(\mathcal{C}) > \mathcal{L}_\mathbb{V}(\mathcal{C}) = 0$.

With this as our central definition, in the remainder of this paper we will investigate some of its fundamental questions, in particular: is it possible to have $\Delta^*_\mathbb{V}(\mathcal{C}) > 0$? Is it possible to have $\mathcal{L}_\mathbb{V}(\mathcal{C}) = 0$ but $\mathcal{L}^*_\mathbb{V}(\mathcal{C}) > 0$? Given a channel $\mathcal{C}$, can we compute $\mathcal{L}^*_{\mathbb{V}}(\mathcal{C})$? Given that (as we shall see) the answer to the previous question is ‘no’, can we at least get some bounds on it?

B. Non-local games

The key technical ingredient for many of the results of this paper is the observation that the entangled capacity of interactive channels has a close connection with the theory of *non-local games*. This is a formalism that highlights and in some sense allows us to measure the inherently ‘contextual’ nature of quantum mechanics: that is, that it is possible for two parties sharing entanglement to accomplish tasks that would be impossible for separated parties under any purely local theory of physics.

The basic setup is that we have two players, Alice and Bob, playing a (co-operative) game with a referee. The referee begins by sending Alice and Bob a message drawn (probabilistically) from finite sets $\mathcal{A}$ and $\mathcal{B}$ respectively. Alice and Bob must then respond with messages from sets $\mathcal{X}$ and $\mathcal{Y}$ respectively. The referee then determines according to a specified function D whether Alice and Bob have won or lost the game; we are interested in the highest probability with which Alice and Bob can win, which we call the ‘value’ of the game. (One could also consider games with more players or more rounds, but we will not need to for this work.)

Definition 7. *A* two-player one-round non-local game *is a tuple $\mathfrak{G} = (\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, D, \mu)$, where $\mathcal{A}, \mathcal{B}, \mathcal{X}$ and $\mathcal{Y}$ are finite sets, $\mu \in \mathbb{D}(\mathcal{A} \times \mathcal{B})$ is some probability distribution and $D : \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ is the* decision function*, determining whether Alice and Bob are considered to have won or lost the game.*

A classical *strategy s for $\mathfrak{G}$ comprises a pair of functions $f : \mathcal{A} \to \mathbb{D}(\mathcal{X})$ and $g : \mathcal{B} \to \mathbb{D}(\mathcal{Y})$. Write*

$$\mathit{val}(\mathfrak{G}, s) = \sum_{a,b,x,y} \mu(a, b) f(a, x) g(b, y) D(a, b, x, y)$$

for the win probability of strategy s, and

$$\mathit{val}(\mathfrak{G}) = \sup_s \mathit{val}(\mathfrak{G}, s),$$

the classical value *of $\mathfrak{G}$.*

It is easy to show that in fact Alice and Bob’s optimal win probability can be obtained with purely deterministic strategies, so that without loss of generality we may assume $f(a)(x), f(b)(y) \in \{0, 1\}$ for all a, b, x, y.

What if Alice and Bob are given access to entanglement? As for channels, we allow Alice and Bob to share some quantum state $|\psi\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. The strategy must specify a measurement taking values on $\mathcal{X}$ for each message Alice could receive; similarly for Bob.

Definition 8. *Let $\mathfrak{G} = (\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, D, \mu)$ be a game. A* quantum strategy *for $\mathfrak{G}$ is a pure state $|\psi\rangle$ in a finite-dimensional complex Hilbert space $\mathcal{H} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, and sets $\{A^a\}$ and $\{B^b\}$ such that for every $a \in \mathcal{A}$, $A^a = \{A^a_x\}_{x \in \mathcal{X}}$ is a measurement over $\mathcal{H}_{\mathcal{A}}$, and for every $b \in \mathcal{B}$, $B^b = \{B^b_y\}_{y \in \mathcal{Y}}$ is a measurement over $\mathcal{H}_{\mathcal{B}}$.*

For strategy s as above, let

$$\mathit{val}(\mathfrak{G}, s) = \sum_{a,b,x,y} \mu(a, b) \langle\psi| A^a_x \otimes B^b_y |\psi\rangle D(a, b, x, y).$$

Then the entangled value *of $\mathfrak{G}$ is given by*

$$\mathit{val}^*(\mathfrak{G}) = \sup_s \mathit{val}(\mathfrak{G}, s).$$

The original example of a non-local game is the *CHSH game* [18], which we denote $\mathfrak{G}_{CHSH}$. In this game, the messages sent and received by Alice and Bob each consist of a single bit. The judge sends each player a uniformly random bit a, b; they each reply with a single bit x, y. The players’ goal is to arrange that if $a = b = 1$ then x and y are *different*, and otherwise x and y are *equal*. Formally, we have $\mathcal{A} = \mathcal{B} = \mathcal{X} = \mathcal{Y} = \{0, 1\}$, $\mu = U(\mathcal{A} \times \mathcal{B})$ the uniform distribution and $D(a, b, x, y) = 1_{ab = x \oplus y}$.

It is fairly easy to see that if Alice and Bob are restricted to classical strategies then they cannot do better than just both always returning 0 (say). Since $a = b = 1$ occurs only with probability $1/4$, this means that they win with probability $3/4$.

On the other hand, as we see in Proposition 9, if Alice and Bob are given access to entangled strategies then they can win with probability $\cos^2(\pi/8) \approx 0.85 > 0.75$.

Proposition 9. *We have*

$$\mathit{val}^*(\mathfrak{G}_{CHSH}) \geq \cos^2(\pi/8) \approx 0.85 > \mathit{val}(\mathfrak{G}_{CHSH}) = 3/4.$$

Proof. It is easy to check that the optimal classical strategy is for Alice and Bob to always send 0, which has win probability 3/4. We exhibit an entangled strategy with win probability $\cos^2(\pi/8)$. Let $\mathcal{H}_{\mathcal{A}} = \mathcal{H}_{\mathcal{B}} = \mathbb{C}^2$ and $|\psi\rangle = (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$. For $\theta \in [-\pi, \pi]$ we will write $|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$, and $[\theta] = |\theta\rangle\langle\theta|$. Let $A^0_0 = [0]$, $A^0_1 = [\pi/2]$, $A^1_0 = [\pi/4]$, $A^1_1 = [3\pi/4]$, $B^0_0 = [\pi/8]$, $B^0_1 = [5\pi/8]$, $B^1_0 = [-\pi/8]$ and $B^1_1 = [3\pi/8]$. One can check that this strategy has win probability $\cos^2(\pi/8)$. □

This game (implemented with Alice and Bob sufficiently separated as to preclude communication between them) has been used to show experimentally that despite Einstein’s qualms the behaviour of the universe is in fact inherently non-local, since the players can obtain a winning strategy higher than that attainable in any purely local theory.

C. Quantum advantage

We now show, using a channel derived from the CHSH game, that it is possible for entanglement to increase channel capacity. Essentially we define a channel which plays the CHSH game with Alice and Bob, and if they win rewards them by transmitting a single bit of information. Since entanglement increases the probability with which they can win the game, it increases the capacity of the channel.

Concretely, define $\mathcal{C}_{CHSH}$ to be a two-round interactive channel with $\mathcal{A} = \{0, 1\} \times \{0, 1\}$ and $\mathcal{B} = \mathcal{X} = \mathcal{Y} = \{0, 1\}$.

Define $f_1(a,b) = U(\mathcal{X} \times \mathcal{Y})$ (that is, Alice and Bob's first round inputs are ignored), and

$$f_2((a_1,b_1,x,y),((a_2,a_2'),b_2)) \\ = \begin{cases} (0,a_2') & \text{if } a_2 \oplus b_2 = xy \\ (0,U(\{0,1\})) & \text{otherwise.} \end{cases}$$

Theorem 10. *Let $\mathbb{V}$ be a vulnerability measure. We have*

$$\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}_{CHSH}) \geq \mathbb{V}(\mathrm{Ber}((1+\cos^2(\pi/8))/2) - \mathbb{V}(\mathrm{Ber}(1/2)) \\ > \mathcal{L}_{\mathbb{V}}(\mathcal{C}_{CHSH}) = \mathbb{V}(\mathrm{Ber}(7/8)) - \mathbb{V}(\mathrm{Ber}(1/2)).$$

Proof. For the lower bound on $\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}_{CHSH})$, let $\mathcal{H}_{\mathcal{A}} = \mathcal{H}_{\mathcal{B}} = \mathbb{C}^2$ and $|\psi\rangle = (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$. Let K be uniformly distributed on $\{0,1\}$. Let $A^{k,()} = B^{()} = \{I,0,\ldots\}$. Let $A^{k,(a_1,x)}_{(a,k)} = A^x_a$ and $B^{(b_1,y)}_b = B^y_b$ from the proof of Proposition 9, and $A^{k,(a_1,x)}_{(a,1-k)} = 0$. Now since $a_2 \oplus b_2 = xy$ with probability $\cos^2(\pi/8)$ we have that $y_2 = k$ with probability $\cos^2(\pi/8) + (1-\cos^2(\pi/8))/2 = (1+\cos^2(\pi/8))/2$. Conditional on observing y_2, Bob's posterior probability that $k = y_2$ is $((1+\cos^2(\pi/8))/2) \cdot (1/2)/(1/2)$ by Bayes' theorem (see the formula immediately below Definition 3), so the posterior vulnerability is $\mathbb{V}(\mathrm{Ber}((1+\cos^2(\pi/8))/2))$, as required.

For the upper bound on $\mathcal{L}_{\mathbb{V}}(\mathcal{C}_{CHSH})$, we have that without loss of generality Alice and Bob employ deterministic strategies, and so it is a finite check to establish that their optimal strategy is $a_2 = b_2 = 0$ and $a_2' = k$ with $K \sim U(\{0,1\})$, giving leakage $\mathbb{V}(\mathrm{Ber}(7/8)) - \mathbb{V}(\mathrm{Ber}(1/2))$ as required. The strict inequality follows from the second healthiness condition on $\mathbb{V}$. □

IV. Purely quantum channels

In this section, we will show that it is not possible for entanglement to increase the capacity of a channel with zero classical capacity. In fact we do this by showing the slightly stronger result that a zero-classical-capacity channel has zero capacity even if Alice and Bob are allowed strategies involving *any* 'non-signalling' correlations—that is, such that Bob's choice at a particular stage does not in itself convey information for him, and similarly for Alice (recall that all correlations resulting from entanglement are non-signalling; but not all non-signaling correlations can be produced using entanglement). In mathematical terms this corresponds to saying that the marginal distribution on Bob's next action (respectively Alice's) is independent of the history of Alice's (respectively Bob's) part of the interaction.

Definition 11. *Let $\mathcal{C}$ be an n-IC, and K a random variable. A* generalised strategy *s for $\mathcal{C}$ is a tuple $(g_1,\ldots,g_n)$ of functions*

$$g_i : \mathcal{K} \times (\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y})^{i-1} \to \mathbb{D}(\mathcal{A} \times \mathcal{B}).$$

We say s is non-signalling *if*

(i) for every $k,k' \in \mathcal{K}$ and $t,t' \in (\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y})^n$ with $\pi_B(t) = \pi_B(t')$, we have $\forall b \in \mathcal{B}$

$$\sum_{a\in\mathcal{A}} g_i(k,t_i)(a,b) = \sum_{a\in\mathcal{A}} g_i(k',t_i')(a,b)$$

for every i, and

(ii) for every $k \in \mathcal{K}$ and $t,t' \in (\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y})^n$ with $\pi_A(t) = \pi_A(t')$, we have $\forall a \in \mathcal{A}$

$$\sum_{b\in\mathcal{B}} g_i(k,t_i)(a,b) = \sum_{b\in\mathcal{B}} g_i(k,t_i')(a,b)$$

for every i.

For a vulnerability measure $\mathbb{V}$ we define $\mathbb{V}$-leakage under strategy s as before, and the supremum of such leakage under all non-signalling strategies as the non-signalling $\mathbb{V}$-capacity, which we denote $\mathcal{L}^{ns}_{\mathbb{V}}(\mathcal{C})$.

Every quantum joint strategy is a non-signalling strategy, with

$$g_i(k,t_i)(a,b) = \langle\psi|(A^{k,\pi_A(t_{i-1})}_a A^k_{t_{i-1}}) \otimes (B^{\pi_B(t_{i-1})}_b B_{t_{i-1}})|\psi\rangle\,.$$

Hence for any channel $\mathcal{C}$ we have

$$\mathcal{L}^{ns}_{\mathbb{V}}(\mathcal{C}) \geq \mathcal{L}^*_{\mathbb{V}}(\mathcal{C}) \geq \mathcal{L}_{\mathbb{V}}(\mathcal{C}). \tag{1}$$

Note that this inequality can be strict: for example, it is easy to show that non-signalling correlations allow Alice and Bob to win the CHSH game with probability 1, and so (as we will see in Theorem 17 in Section V below) we have $\mathcal{L}^{ns}_{\mathbb{V}}(\mathcal{C}_{CHSH}) \geq \mathbb{V}(\mathrm{Ber}(1)) - \mathbb{V}(Ber(1/2)) > \mathcal{L}^*_{\mathbb{V}}(\mathcal{C}_{CHSH})$.

The reason for considering this broader class of strategies is that they can be analysed in an abstract linear-algebraic manner. Define the set $\mathcal{D}_{\mathcal{A}} = [(\mathcal{A} \times \mathcal{X})^{<n} \to \mathcal{A}]$, the set of functions $(\mathcal{A}\times\mathcal{X})^{<n} \to \mathcal{A}$, and similarly $\mathcal{D}_{\mathcal{B}} = [(\mathcal{B}\times\mathcal{Y})^{<n} \to \mathcal{B}]$. A channel gives a map

$$c : \mathcal{D}_{\mathcal{A}} \times \mathcal{D}_B \to \mathbb{D}(\mathcal{B} \times \mathcal{Y})^n,$$

where $c(f,g)$ is the probability distribution on Bob's traces if Alice behaves according to f and Bob behaves according to g.

To accommodate probabilistic behaviour by Alice and Bob, we extend the function c by linearity to a linear map

$$\mathcal{C} : \mathbb{R}\mathcal{D}_{\mathcal{A}} \otimes_{\mathbb{R}} \mathbb{R}\mathcal{D}_{\mathcal{B}} \to \mathbb{R}(\mathcal{B} \times \mathcal{Y})^n,$$

where $\mathbb{R}X$ is the free real vector space over the set X.

Note that $\mathcal{C}$ is 'trace-preserving', where the trace of a vector v is the trace of the linear map $u \mapsto \langle u,v\rangle v$, or in more concrete terms $\mathrm{tr}(\sum_i c_i e_i) = \sum_i c_i$, where the e_i are the canonical basis vectors.

Observe that $\mathbb{R}\mathcal{D}_{\mathcal{A}}$ is canonically isomorphic to $[(\mathcal{A} \times \mathcal{X})^{<n} \to \mathbb{R}\mathcal{A}]$, and similarly $\mathbb{R}\mathcal{D}_{\mathcal{B}}$ to $[(\mathcal{B} \times \mathcal{Y})^{<n} \to \mathbb{R}\mathcal{B}]$, which extend to a canonical isomorphism between $\mathbb{R}\mathcal{D}_{\mathcal{A}} \otimes_{\mathbb{R}} \mathbb{R}\mathcal{D}_{\mathcal{B}}$ and $[(\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y})^{<n} \to \mathbb{R}(\mathcal{A} \times \mathcal{B})]$. By currying Definition 11 and observing that $\mathbb{D}(\mathcal{A} \times \mathcal{B}) \subset \mathbb{R}(\mathcal{A} \times \mathcal{B})$ we see that a generalised strategy corresponds to a map

$$s : \mathcal{K} \to \mathbb{R}\mathcal{D}_{\mathcal{A}} \otimes_{\mathbb{R}} \mathbb{R}\mathcal{D}_{\mathcal{B}}.$$

The payoff to all this is that we get a clean characterisation of the property that the marginal distribution on Bob's strategies cannot depend on the value of the secret, which turns out to suffice for the theorem.

Lemma 12. *Let s be a non-signalling generalised strategy. Then we have that $tr_{\mathcal{A}}(s(k))$ is constant for all k, where $tr_{\mathcal{A}}$ is the 'partial trace' function*

$$tr_{\mathcal{A}} : \mathbb{R}\mathcal{D}_{\mathcal{A}} \otimes_{\mathbb{R}} \mathbb{R}\mathcal{D}_{\mathcal{B}} \to \mathbb{R}\mathcal{D}_{\mathcal{B}},$$

the linear function generated by $f \otimes g \mapsto g$ for $f \in \mathcal{D}_{\mathcal{A}}, g \in \mathcal{D}_{\mathcal{B}}$.

Proof. Let $k, k' \in \mathcal{K}$. By condition (i) of Definition 11 we have for every trace prefix t_i and every $b \in \mathcal{B}$ that

$$\sum_{a\in\mathcal{A}} \langle s(k)(t_i), a \otimes b\rangle = \sum_{a\in\mathcal{A}} \langle s(k')(t_i), a \otimes b\rangle \qquad (2)$$

(where we define $(f \otimes g)(t_i) = f(\pi_A(t_i)) \otimes g(\pi_B(t_i))$ and extend by linearity).

Now trivially we have

$$s(k) = \sum_{f\in\mathcal{D}_{\mathcal{A}}, g\in\mathcal{D}_{\mathcal{B}}} \langle s(k), f \otimes g\rangle f \otimes g$$

and so

$$\begin{aligned} s(k)(t_i) &= \sum_{f,g} \langle s(k), f \otimes g\rangle (f \otimes g)(t_i) \\ &= \sum_{f,g} \langle s(k), f \otimes g\rangle f(t_i) \otimes g(t_i) \end{aligned}$$

(dropping the π_A and π_B for conciseness).

Hence

$$\begin{aligned} &\sum_{a\in\mathcal{A}} \langle s(k)(t_i), a \otimes b\rangle \\ &\qquad = \sum_{a} \sum_{f,g} \langle s(k), f \otimes g\rangle \langle f(t_i) \otimes g(t_i), a \otimes b\rangle \\ &\qquad = \sum_{f,g} \langle s(k), f \otimes g\rangle \langle f(t_i), \textstyle\sum_a a\rangle \langle g(t_i), b\rangle \\ &\qquad = \sum_{f,g} \langle s(k), f \otimes g\rangle \langle g(t_i), b\rangle, \qquad (3) \end{aligned}$$

since $f \in \mathcal{D}_{\mathcal{A}}$ and so $f(t_i) \in \mathcal{A}$ so $\langle f(t_i), \sum_a a\rangle = 1$.

Note that another characterisation of $\mathrm{tr}_{\mathcal{A}}$ is

$$\mathrm{tr}_{\mathcal{A}}(\xi) = \sum_{f,g} \langle \xi, f \otimes g\rangle g$$

(trivially true on the basis vectors $f' \otimes g'$ and hence by linearity true in general), and hence we have

$$\mathrm{tr}_{\mathcal{A}}(s(k))(t_i) = \sum_{f,g} \langle s(k), f \otimes g\rangle g(t_i).$$

Combining this with (3) and (2) gives that

$$\langle \mathrm{tr}_{\mathcal{A}}(s(k))(t_i), b\rangle = \langle \mathrm{tr}_{\mathcal{A}}(s(k'))(t_i), b\rangle$$

for all b, and hence that $\mathrm{tr}_{\mathcal{A}}(s(k))(t_i) = \mathrm{tr}_{\mathcal{A}}(s(k'))(t_i)$ for all t_i and so $\mathrm{tr}_{\mathcal{A}}(s(k)) = \mathrm{tr}_{\mathcal{A}}(s(k'))$, as required. □

Note that our 'partial trace' $\mathrm{tr}_{\mathcal{A}}$ is indeed a classical analogue of the familiar partial trace from quantum information theory.

We are now ready to prove the main theorem of this section, that non-signaling strategies cannot increase the capacity of a channel with zero classical capacity.

Theorem 13. *Let $\mathcal{C}$ be an n-IC and $\mathbb{V}$ a vulnerability measure. Then*

$$\mathcal{L}_{\mathbb{V}}(\mathcal{C}) = 0 \Rightarrow \mathcal{L}^{ns}_{\mathbb{V}}(\mathcal{C}) = 0.$$

Proof. Let $\mathcal{C}$ be an n-IC with $\mathcal{L}^{ns}_{\mathbb{V}}(\mathcal{C}) > 0$, so in particular there exists a non-signalling strategy $s : \{0,1\} \to \mathbb{R}\mathcal{D}_{\mathcal{A}} \otimes_{\mathbb{R}} \mathbb{R}\mathcal{D}_{\mathcal{B}}$ with $\mathcal{C}(s(0)) \neq \mathcal{C}(s(1))$.

We claim that there must exist $f, f' \in \mathcal{D}_{\mathcal{A}}$ and $g \in \mathcal{D}_{\mathcal{B}}$ such that $c(f,g) \neq c(f',g)$ (equivalently $\mathcal{C}(f \otimes g) \neq \mathcal{C}(f' \otimes g)$), and hence $\mathcal{C}$ has positive classical capacity.

Indeed, supposing the contrary for each $g \in \mathcal{D}_{\mathcal{B}}$ there exists $y_g \in \mathbb{D}(\mathcal{B} \times \mathcal{Y})^n$ such that $\mathcal{C}(f \otimes g) = y_g$ for all $f \in \mathcal{D}_{\mathcal{A}}$. Write

$$\begin{aligned} s(0) &= \sum_{f\in\mathcal{D}_{\mathcal{A}}, g\in\mathcal{D}_{\mathcal{B}}} c_{f,g} f \otimes g \\ s(1) &= \sum_{f\in\mathcal{D}_{\mathcal{A}}, g\in\mathcal{D}_{\mathcal{B}}} c'_{f,g} f \otimes g. \end{aligned}$$

Since s is non-signalling, by Lemma 12 for all $g \in \mathcal{D}_{\mathcal{B}}$ we have

$$\sum_{f\in\mathcal{D}_{\mathcal{A}}} c_{f,g} = \sum_{f\in\mathcal{D}_{\mathcal{A}}} c'_{f,g}.$$

But then

$$\begin{aligned} \mathcal{C}(s(0)) &= \mathcal{C}\left(\sum_{f,g} c_{f,g} f \otimes g\right) \\ &= \sum_{g} \left(\sum_{f} c_{f,g}\right) y_g \\ &= \sum_{g} \left(\sum_{f} c'_{f,g}\right) y_g \\ &= \mathcal{C}(s(1)), \end{aligned}$$

a contradiction. □

Combining Theorem 13 with inequality (1) gives the corresponding result for entangled capactiy.

Corollary 14. *Let $\mathcal{C}$ be an n-IC and $\mathbb{V}$ a vulnerability measure. Then*

$$\mathcal{L}_{\mathbb{V}}(\mathcal{C}) = 0 \Rightarrow \mathcal{L}^{*}_{\mathbb{V}}(\mathcal{C}) = 0.$$

V. Non-computability of entangled capacity

In this section we will show that the problem of computing the entangled capacity of a given channel, even approximately, is RE-complete—that is, as hard as the halting problem.

The key ingredient is Theorem 15, the recent breakthrough result of Ji, Natarajan, Vidick, Wright and Yuen which shows that computing the entangled value of a given non-local game is RE-complete. This was formerly a notorious open problem, because a proof of undecidability would resolve in the negative

Tsirelson's problem (asking whether the 'commuting operator' model—see Section VI—could produce the same correlations as the tensor product model described in Section III-B), which was known to be equivalent [19] to a famous open problem in the theory of operator algebras, the 'Connes embedding problem', open since 1976 [20].

Theorem 15 ([6], Theorem 12.7)**.** *The problem of approximating val*$^*(\mathfrak{G})$ *for a given* $\mathfrak{G}$ *is RE-complete. More precisely, the problem of determining whether a given* $\mathfrak{G}$ *has val*$^*(\mathfrak{G}) = 1$ *or val*$^*(\mathfrak{G}) \leq 1/2$*, given that one of these is the case, is RE-complete.*

In order to apply this to entangled channel capacity, we show how to associate to any non-local game $\mathfrak{G}$ a channel $\mathcal{C}_{\mathfrak{G}}$ such that the entangled capacity of $\mathcal{C}_{\mathfrak{G}}$ and the entangled value of $\mathfrak{G}$ are related by an explicit formula. This shows that the problem of computing entangled values of games is reducible to the problem of computing entangled capacity of channels, which shows that the latter is also RE-complete.

Informally, for a game $\mathfrak{G}$, we will define $\mathcal{C}_{\mathfrak{G}}$ as the channel that does the following:

1) Send messages $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ to Alice and Bob respectively, drawn according to the distribution μ
2) Receive messages $a \in \mathcal{A}$ and $b \in \mathcal{B}$ from Alice and Bob respectively, together with a bit $u \in \{0,1\}$ from Alice
3) If $D(x,y,a,b) = 1$ send the bit u to Bob; otherwise send Bob a uniformly random bit.

Definition 16. *For a game* $\mathfrak{G} = (\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, D, \mu)$*, define the 2-round abstract interactive channel* $\mathcal{C}_{\mathfrak{G}}$ *to comprise the tuple of finite sets* $(\mathcal{A} \times \{0,1\}, \mathcal{B}, \mathcal{X}, \mathcal{Y} \times \{0,1\})$ *and the functions* (f_1, f_2)*, where*

$$f_1((a,u),b)(x,(y,v)) = \mu(x,y)1_{v=0},$$

and

$$\begin{aligned} f_2(((a_1,u_1),b_1,&x_1,(y_1,v_1)),((a_2,u_2),b_2)) = \\ &(x_0,(y_0,u_1 \oplus X(1 - D(x_1,y_1,a_2,b_2)))), \end{aligned}$$

where $X \sim$ *Ber*$(1/2)$ *and* x_0 *and* y_0 *are arbitrary fixed elements of* $\mathcal{X}$ *and* $\mathcal{Y}$ *respectively.*

The main theorem of this section is that the entangled capacity of $\mathcal{C}_{\mathfrak{G}}$ is that given by the obvious strategy of setting u equal to the value of the secret and following an optimal strategy for $\mathfrak{G}$.[2]

Theorem 17. *Let* $\mathfrak{G}$ *be a game, and* $\mathbb{V}$ *a vulnerability measure. Then*

$$\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}_{\mathfrak{G}}) = \mathbb{V}(\mathrm{Ber}((1 + \mathit{val}^*(\mathfrak{G}))/2)) - \mathbb{V}(\mathrm{Ber}(1/2)).$$

Proof. We prove separately matching upper and lower bounds for $\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}_{\mathfrak{G}})$. The lower bound is trivial: given an entangled strategy for $\mathfrak{G}$ achieving win probability $p = \mathrm{val}^*(\mathfrak{G}) - \epsilon$, set $K \sim$ Ber(1/2) and have Alice and Bob execute the strategy for $\mathfrak{G}$, with Alice sending the value of K as her additional bit u.

Conditional on observing the value v, the posterior probability that $K = v$ is

$$\frac{p/2 + (1-p)/4}{p/2 + (1-p)/2} = (1+p)/2.$$

Hence the posterior vulnerability is $\mathbb{V}(\mathrm{Ber}((1+p)/2))$, and this strategy achieves leakage $\mathbb{V}(\mathrm{Ber}((1+p)/2)) - \mathbb{V}(\mathrm{Ber}(1/2))$, as required.

For the upper bound, let s be a strategy for $\mathcal{C}_{\mathfrak{G}}$ achieving leakage l. Let the random variable U be the bit sent by Alice, V the bit received by Bob and $W = D(x,y,a,b)$, the event that they 'win' the game.

By considering each $s(k)$ as a strategy for $\mathfrak{G}$, we have that

$$p = \max_k p_{W|K}(1|k) \leq \mathrm{val}^*(\mathfrak{G}).$$

Now, we have that $K \to (U,W) \to V$ is a Markov chain, but since the event that $W = 1$ may depend on K in an uncontrolled way we do not have that $K \to U \to V$ is a Markov chain. Our strategy will be to show that the dependence of V on K can be 'factored through' a random variable U' so that $K \to U' \to V$ is a Markov chain and (U', V) is a binary symmetric channel with error probability $(1-p)/2$.

Indeed, for $k \in \mathcal{K}$ we must have $V|K = k \sim \mathrm{Ber}(\rho_k)$ for some ρ_k (this follows just from that fact that $V|K = k$ is a $\{0,1\}$-valued random variable). In particular, we have

$$\begin{aligned} \rho_k &= p_{V|K}(1|k) \\ &= p_{W|K}(1|k)p_{U|K}(1|k) \\ &\qquad + p_{W|K}(0|k)\frac{p_{U|K}(1|k) + p_{U|K}(0|k)}{2} \\ &= p_{W|K}(1|k)p_{U|K}(1|k) + \frac{p_{W|K}(0|k)}{2} \\ &\in \left[\frac{p_{W|K}(0|k)}{2}, 1 - \frac{p_{W|K}(0|k)}{2}\right]. \end{aligned} \tag{4}$$

Now, putting

$$U'|K = k \sim \mathrm{Ber}\left(\frac{p + 2\rho_k - 1}{2p}\right)$$

and

$$V = U' \oplus \mathrm{Ber}\left(\frac{1-p}{2}\right)$$

independently of K, we have that $V|K = k \sim \mathrm{Ber}(\rho_k)$ for all k, as required (since one can check that the xor of Bernoulli random variables with parameters $(p + 2\rho_k - 1)/2p$ and $(1-p)/2$ is a Bernoulli random variable with parameter ρ_k). Note that by (4) and the fact that $p_{W|K}(0|k) = 1 - p_{W|K}(1|k) \geq 1 - p$, we have that $0 \leq (p + 2\rho_k - 1)/2p \leq 1$.

[2] Or rather strictly speaking the supremum of strategies corresponding to near-optimal strategies for $\mathfrak{G}$.

Now since $K \to U' \to V$ forms a Markov chain and (U', V) is a binary symmetric channel with error probability $(1-p)/2$, by the composition inequality for $\mathbb{V}$ we have that

$$\begin{aligned} l = I_{\mathbb{V}}(K;V) &\leq \sup_{V'|U''=V|U'} I_{\mathbb{V}}(U'';V') \\ &\leq \mathbb{V}(\mathrm{Ber}((1+p)/2)) - \mathbb{V}(\mathrm{Ber}(1/2)) \\ &\leq \mathbb{V}(\mathrm{Ber}((1+\mathrm{val}^*(\mathfrak{G}))/2)) - \mathbb{V}(\mathrm{Ber}(1/2)), \end{aligned}$$

as required. □

Note that Theorem 10 is a special case of the lower bound in Theorem 17, with $\mathfrak{G} = \mathfrak{G}_{CHSH}$.

Combining Theorem 17 with Theorem 15 gives the result that computing the entangled capacity of a given channel is undecidable. Note that the gapped problem is clearly in RE, because we can explicitly enumerate entangled strategies and accept if we find one with capacity above the lower threshold.

Theorem 18. *Let $\mathbb{V}$ be a vulnerability measure. The problem of determining whether a given channel $\mathcal{C}$ has $\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}) \geq \delta^+_{\mathbb{V}}$ or $\mathcal{L}^*_{\mathbb{V}}(\mathcal{C}) \leq \delta^-_{\mathbb{V}}$, given that one of these is the case, is RE-complete, where $\delta^+_{\mathbb{V}} > \delta^-_{\mathbb{V}}$ are the constants*

$$\begin{aligned} \delta^+_{\mathbb{V}} &= \mathbb{V}(\mathit{Ber}(1)) - \mathbb{V}(\mathit{Ber}(1/2)) \\ \delta^-_{\mathbb{V}} &= \mathbb{V}(\mathit{Ber}(3/4) - \mathbb{V}(\mathit{Ber}(1/2)). \end{aligned}$$

Note, for instance, that for min-entropy vulnerability we have $\delta^+_{\mathbb{V}} = \log_2 2 = 1$ and $\delta^-_{\mathbb{V}} = \log_2(3/2) \approx 0.58$, and for Shannon entropy vulnerability we have $\delta^+_{\mathbb{V}} = H_2(1/2) - H_2(1) = 1$ and $\delta^-_{\mathbb{V}} = H_2(1/2) - H_2(3/4) \approx 0.19$.

VI. SDP UPPER BOUNDS

In this section, we will show how upper bounds for entangled capacity, under the min-entropy vulnerability measure $\mathbb{V} = -H_\infty$, may be obtained using semidefinite programming. This is by analogy to a similar method [7] for non-local games. We first introduce semidefinite programming and outline the technique of [7], and then show how it may be adapted to obtain bounds on entangled min-entropy channel capacity.

A. The SDP hierarchy

Semidefinite programming (SDP) [21] is a technique from numerical optimisation. A semidefinite progamming problem (for us; there are many equivalent formulations) is specified by an *objective* matrix A and *constraints* given by matrices $A_1, \ldots, A_n$ and scalars $a_1, \ldots, a_n$, and consists of the following optimisation:

$$\begin{aligned} &\text{maximise } A \bullet M \\ &\text{subject to } M \succcurlyeq 0 \\ &\qquad\qquad A_i \bullet M = a_i \qquad \forall i, \end{aligned}$$

where $\bullet$ is the Frobenius product $M \bullet N = \sum_{ij} M_{ij} N_{ij}$, and $M \succcurlyeq 0$ means that M is *positive semidefinite*—that is, M is Hermitian with all its eigenvalues non-negative; equivalently, M is Hermitian and we have $v^* M v \geq 0$ for any vector v. We say that a problem is *feasible* if there exists an M satisfying the constraints (ignoring the objective). The benefit of formulating a problem in this way is that the optimisation can be performed (to specified precision) in polynomial time, and indeed in a way which is usually efficient in practice. Note that it is easy to show that within this form we may introduce additional scalar variables together with arbitrary linear equality or inequality constraints with the entries of M, and we will allow ourselves to do this freely below.

The *SDP hierarchy*, introduced in the seminal paper [7], uses SDP to obtain an infinite sequence of stronger and stronger constraints on quantum behaviours, which importantly are tight in the limit: that is, if a behaviour is not quantum then this will be detected at some finite level of the hierarchy. The catch is that the notion of 'quantum' used is not the usual one of Alice and Bob having their own parts of the system, but rather that they share some infinite-dimensional Hilbert space, and the only constraint is that all of Alice's measurements should commute with all of Bob's. This is called the 'commuting operator' model, and is clearly a generalisation of the usual tensor product model (since if the system takes the form $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ with Alice and Bob's measurements being only on $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{H}_{\mathcal{B}}$ respectively then clearly their measurements commute); Tsirelson's conjecture asserted that the two models were equivalent, but this was refuted as a consequence of the recent result MIP* = RE [6].

More concretely, a *behaviour* means a collection of probability distributions $P(x,y) \in \mathbb{D}(\mathcal{A} \times \mathcal{B})$ for each $(x,y) \in (\mathcal{X} \times \mathcal{Y})$, for some finite sets $\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}$. We want to determine whether or not there exists some complex Hilbert space $\mathcal{H}$ (not necessarily finite-dimensional), a state $\psi \in \mathcal{H}$ and measurements $\{E^x_a\}_{a \in \mathcal{A}}$, $\{E^y_b\}_{b \in \mathcal{B}}$ for each $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ (for Alice and Bob respectively) such that E^x_a and E^y_b commute for every x, a, y, b, and such that we have

$$P(x,y)(a,b) = \langle \psi | E^x_a E^y_b | \psi \rangle \, .$$

Suppose that such a set of measurements does exist. Then we can consider a matrix Γ whose rows and columns are indexed by formal products of our operators E^x_a, E^y_b, and whose entries are given by

$$\Gamma_{S,T} = \langle \psi | S^\dagger T | \psi \rangle \, .$$

This matrix is positive semidefinite, since for any vector $v = \sum_S v_S e_S$ (with basis vectors e_S) we have

$$\begin{aligned} v^\dagger \Gamma v &= \sum_{S,T} v^*_S \, \langle \psi | S^\dagger T | \psi \rangle \, v_T \\ &= \langle \psi | (\textstyle\sum_S v_S S)^\dagger (\textstyle\sum_T v_T T) | \psi \rangle \\ &= \| \textstyle\sum_T v_T T \, | \psi \rangle \|^2 \\ &\geq 0. \end{aligned}$$

The matrix Γ is infinite, so to formulate a finitary SDP problem we must take a finite subset of its rows and columns: let the matrix Γ_i consist of those rows and columns of Γ corresponding to formal products of at most i operators. We consider the problem whose constraints are that $\Gamma_i \succcurlyeq 0$, together with additional constraints on the entries of Γ_i arising from the commutativity, orthogonality and idempotence properties of the operators, and also from the desired values of $P(x,y)(a,b) = \langle\psi|E^x_a E^y_b|\psi\rangle$. Clearly the Γ_i arising from a set of measurements realising the behaviour will be a feasible solution to this problem, but the highly non-trivial main theorem of [7] (Theorem 8) is that the converse is also true: if the problem is feasible for all i then a suitable set of measurements exists. Hence in particular if the behaviour is not quantum then we will find that the problem is infeasible for some i.

Instead of specifying a fixed behaviour, we can also formulate some objective as a function of the $\langle\psi|E^x_a E^y_b|\psi\rangle$ (or rather the corresponding entries of Γ_i), and then the optimal values for increasing i will give a sequence of tighter and tighter bounds, converging to the true optimum in the commuting operator model. This is the main technique for bounding the entangled value of non-local games (see Section III-B), and this is what we will adapt below to obtain bounds on entangled min-entropy capacity.

B. Bounds on min-entropy capacity

As discussed above, to apply SDP techniques we will need to consider min-entropy capacity in the commuting operator model, which is stronger than the entangled model (Definition 6) but weaker than the non-signalling model (Definition 11). Whereas in the entangled model we specified that the Hilbert space on which Alice and Bob made their measurements could be separated into a part $\mathcal{H}_\mathcal{A}$ held by Alice and a part $\mathcal{H}_\mathcal{B}$ held by Bob, we will now drop this assumption and assume only that the measurements made by Alice commute with those made by Bob.

Definition 19. *Let $\mathcal{C}$ be an n-IC, and K a random variable taking values on the set $\mathcal{K}$. A* commuting operator joint strategy *for $\mathcal{C}$ is a pure state $|\psi\rangle$ in a (possibly infinite-dimensional) complex Hilbert space $\mathcal{H}$, and sets $\{A^{k,t}\}$ and $\{B^{t'}\}$ such that*

(i) for every $k \in \mathcal{K}$ and every $t \in (\mathcal{A}\times\mathcal{X})^i$ with $0 \le i < n$, $A^{k,t} = \{A^{k,t}_a\}_{a\in\mathcal{A}}$ is a measurement over $\mathcal{H}_\mathcal{A}$,

(ii) for every $t' \in (\mathcal{B}\times\mathcal{Y})^i$ with $0 \le i < n$, $B^{t'} = \{B^{t'}_b\}_{b\in\mathcal{B}}$ is a measurement over $\mathcal{H}_\mathcal{B}$, and

(iii) for every k, t, t', a, b we have $A^{k,t}_a B^{t'}_b = B^{t'}_b A^{k,t}_a$.

Denote the space of such strategies by $\mathcal{S}^{co}_{\mathcal{C},K}$.

As usual we can define $\mathbb{V}$-leakage and $\mathbb{V}$-capacity $\mathcal{L}^{co}_\mathbb{V}(\mathcal{C})$. Note that any entangled strategy is trivially a commuting operator strategy; on the other hand a commuting operator strategy is still non-signalling and so we have

$$\mathcal{L}^{ns}_\mathbb{V}(\mathcal{C}) \ge \mathcal{L}^{co}_\mathbb{V}(\mathcal{C}) \ge \mathcal{L}^{*}_\mathbb{V}(\mathcal{C}) \ge \mathcal{L}_\mathbb{V}(\mathcal{C}). \tag{5}$$

The basic idea is that as before we consider a matrix Γ with entries $\langle\psi|S^\dagger T|\psi\rangle$, where S and T are formal products (of bounded length) of the operators defining our strategy. The additional ingredient is that we are able to express the objective of min-entropy capacity as a linear function of the entries of Γ, or rather more precisely as a linear function of additional scalar variables which are subject to linear constraints. This is done using the formula for min-entropy capacity given as Proposition 5.1 of [22].

This formula states that if we have a (non-interactive) channel defined by a conditional probability matrix $p_{Y|X}$ then we have

$$\sup_X I_{-H_\infty}(X;Y) = \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} p_{Y|X}(y|x), \tag{6}$$

where the supremum is over probability distributions for X, with Y obeying the conditional probabilities $p_{Y|X}(y|x)$.

Fixing strategies (i.e. sets of operators) for Alice and Bob fixes the conditional distribution $\pi_B(T_{\phi_A(K),s_B})|K$, whose values we will see can be expressed as linear functions of the entries of Γ. We then have that $\mathcal{L}^{co}_{-H_\infty}(\mathcal{C})$ is the supremum of $I_{-H_\infty}(K;\pi_B(T_{\phi_A(K),s_B})$ over all choices of strategies and all distributions for K, so in particular by (6) the capacity corresponding to a given choice of strategies is given by

$$\sum_{t\in(\mathcal{B}\times\mathcal{Y})^n} \max_k p_{\pi_B(T_{\phi_A(K),s_B})|K}(t|k).$$

Note that $\max$ is not a linear (or indeed convex) relation, and so this cannot be expressed directly in our SDP problem. However, since $\mathcal{K}$ and $(\mathcal{B}\times\mathcal{Y})^n$ are finite sets, we can just exhaust over 'guessing functions' $g : (\mathcal{B}\times\mathcal{Y})^n \to \mathcal{K}$, with the SDP for each maximising $\sum p(t|g(t))$.

Let $\mathcal{C}$ be an n-IC, $\mathcal{K}$ a finite set and $g : (\mathcal{B}\times\mathcal{Y})^n \to \mathcal{K}$. Define the semidefinite programming problem $\mathcal{P}_i(\mathcal{C},\mathcal{K},g)$ by the following variables:

- a matrix Γ, with entries $\Gamma_{S,T}$ for all strings S, T in symbols $A^{k,t}_a$, $B^{t'}_b$, 0 and 1 of length at most i; $\Gamma_{S,T}$ represents $\langle\psi|S^\dagger T|\psi\rangle$
- variables $p_{t|k}$ for each trace $t \in (\mathcal{B}\times\mathcal{Y})^n$ and each $k \in \mathcal{K}$, representing the probability of observing trace t conditional on the secret value $K = k$,

and objective

$$\text{maximise} \sum_{t\in(\mathcal{B}\times\mathcal{Y})^n} p_{t|g(t)}.$$

The first constraints arises from the fact that all of the $p_{t|k}$ represent probabilities, and as discussed above the matrix Γ is positive semidefinite.

- for all t, k, $0 \le p_{t|k} \le 1$
- $\Gamma \succcurlyeq 0$

The next constraints arise from the properties that Γ should have if it is the matrix arising from some set of operators: for instance we will have $\langle\psi|I|\psi\rangle = 1$ and $\langle\psi|0|\psi\rangle = 0$. More generally, if strings S, T and U, V are such that (interpreting the strings as products of operators) the orthogonality, idempotence and commutativity properties force $S^\dagger T = U^\dagger V$ then we should have $\Gamma_{S,T} = \Gamma_{U,V}$.

- $\Gamma_{1,1} = 1$ and $\Gamma_{0,0} = 0$
- $\Gamma_{S,T} = \Gamma_{U,V}$ whenever $S^\dagger T = U^\dagger V$ under the following relations: $(A^{k,t}_a)^\dagger = A^{k,t}_a = (A^{k,t}_a)^2$ and $(B^{t'}_b)^\dagger = B^{t'}_b = (B^{t'}_b)^2$; $A^{k,t}_a B^{t'}_b = B^{t'}_b A^{k,t}_a$; $A^{k,t}_a A^{k,t}_{a'} = 0$ for all $a' \neq a$

and $B^{t'}_b B^{t'}_{b'} = 0$ for all $b' \neq b$; and $S1 = S = 1S$ and $S0 = 0 = 0S$ for all S

The final constraints express that the $p_{t|k}$ are indeed the conditional probabilities according to the formula in Section III-A. Note that these are linear in the SDP variables, since the $f_i(t_i)(x_i, y_i)$ are fixed constants.

- for all $s \in (\mathcal{B} \times \mathcal{Y})^n$ and $k \in \mathcal{K}$, we have

$$p_{t|k} = \sum_{s:t=\pi_B(s)} \Gamma_{A^k_s, B_s} \prod_{i=1}^{n} f_i(s_i)(x_i, y_i),$$

with A^k_t and B_t the products as defined in Section III-A.

Write $\mathrm{opt}(\mathcal{P}_i(\mathcal{C}, \mathcal{K}, g))$ for the optimal value of $\mathcal{P}_i(\mathcal{C}, \mathcal{K}, g)$, and let $\mathrm{opt}_i(\mathcal{C}, \mathcal{K}) = \max_g \mathrm{opt}(\mathcal{P}_i(\mathcal{C}, \mathcal{K}, g)$. Then we have that this converges to the commuting operator min-entropy capacity of $\mathcal{C}$.

Theorem 20. *Let $\mathcal{C}$ be an n-IC. Then*

$$\mathcal{L}^{co}_{-H_\infty}(\mathcal{C}) = \lim_{i \to \infty} \log \mathrm{opt}_i(\mathcal{C}, (\mathcal{B} \times \mathcal{Y})^n).$$

Proof. First observe that without loss of generality we may take $\mathcal{K} = (\mathcal{B} \times \mathcal{Y})^n$: indeed, if $|\mathcal{K}| > |(\mathcal{B} \times \mathcal{Y})^n|$ then there will elements $k \in \mathcal{K}$ which are never Bob's optimal guess after the interaction, and assigning probability to these elements in the prior clearly cannot increase min-entropy leakage. The upper bound on $\mathcal{L}^{co}_{-H_\infty}(\mathcal{C})$ is then immediate, since a commuting operator strategy for $\mathcal{C}$ gives a feasible solution for $\mathcal{P}_i(\mathcal{C}, (\mathcal{B} \times \mathcal{Y})^n, g)$ for all i as described above (with $g(t) = \arg\max_k p_{\pi_B(T_{\phi_A(K), s_B})|K}(t|k)$).

The lower bound is more delicate. First note that there are only finitely many possible values for g and so by passing to a subsequence we may assume that g is fixed. We then proceed essentially by the proof of Theorem 8 of [7]. This shows that if we have a sequence of feasible solutions (say with optimal values v_i), whose Γ matrices we denote Γ^i, then (viewing the Γ^i as living in the space of infinite matrices whose entries are indexed by *all* strings S and T, extending Γ^i with zeros as necessary), there is a pointwise convergent subsequence whose limit is (say) the infinite matrix Γ^∞, and moreover there exists an (infinite-dimensional) Hilbert space $\mathcal{H}$, state $|\psi\rangle \in \mathcal{H}$ and collection of operators $A^{k,t}_a$ and $B^{t'}_b$ such that $\Gamma^\infty_{S,T} = \langle\psi|S^\dagger T|\psi\rangle$ for all S, T.

Now all of the $p_{t|k}$ are probabilities and so are contained in the compact set $[0, 1]$. Hence passing to a further subsequence we may assume that all the $p_{t|k}$ converge, and by continuity of the constraints we have that their limit, say $p^\infty_{t|k}$ is a valid set of conditional probabilites for the strategy corresponding to the operators obtained in the previous paragraph, with advantage $\sum_t p^\infty_{t|g(t)} = \lim_{i\to\infty} v_i$, as required. □

Note that for $j > i$ we have that any solution for $\mathrm{opt}(\mathcal{P}_j(\mathcal{C}, \mathcal{K}, g))$ restricts to a solution for $\mathrm{opt}(\mathcal{P}_i(\mathcal{C}, \mathcal{K}, g))$ with the same value of the objective, and so the $\log \mathrm{opt}_i(\mathcal{C}, (\mathcal{B} \times \mathcal{Y})^n)$ are a descending sequence of upper bounds for $\mathcal{L}^{co}_{-H_\infty}(\mathcal{C})$.

By (5), the $\log \mathrm{opt}_i(\mathcal{C}, (\mathcal{B} \times \mathcal{Y})^n)$ also give upper bounds for $\mathcal{L}^{*}_{-H_\infty}(\mathcal{C})$. By Theorem 18 there exist channels $\mathcal{C}$ such that $\mathcal{L}^{co}_{-H_\infty}(\mathcal{C}) > \mathcal{L}^{*}_{-H_\infty}(\mathcal{C})$ (since otherwise we could simultaneously enumerate upper bounds from above and entangled strategies from below) and so the upper bounds do not converge to the true value of $\mathcal{L}^{*}_{-H_\infty}(\mathcal{C})$, but since the question of whether such channels exist is equivalent to the Connes Embedding Problem which was open for more than 40 years, it seems reasonable to expect that this will not arise in practice.

VII. Conclusions

A. Interactive channels and non-local games

In this work we have shown that there is a close connection between the communication capacity of interactive channels and the value of non-local games. In particular in Theorem 17 we have shown that for every game there exists a channel such that the entangled capacity of the channel corresponds to the entangled value of the game (and the same argument would give corresponding results for other classes such as commuting operator or non-signalling strategies).

What about going the other way? For the particular case of min-entropy capacity, it does seem that one could transform a channel into a (multi-round) game, essentially by having Bob guess the value of the secret at the end (modulo the technical issue of the prior probability distribution over secrets not being specified *a priori*); one could do the same for other g-leakage measures, using randomness outside the control of Alice and Bob to represent rewards between 0 and 1. On the other hand it is difficult to see how to do this for general vulnerability measures, including in particular Shannon entropy—how can one express this as simple acceptance or rejection of a transcript?

It thus seems that interactive channel capacity is in some sense a generalisation of non-local games, where non-local games correspond specifically to capacity with respect to g-leakage measures. Since non-local games have given rise to such a beautiful and useful theory, it seems reasonable to wonder whether a similarly rich theory may be available for other leakage measures. A promising starting point would seem to be the Shannon entropy measure, which is on the one hand a natural measure but on the other not (so far as we can tell) encompassed by non-local games.

B. Quantum QIF

The formulation of quantitative measures of information flow was the beginning, not the end, of the subject of QIF. Similarly, although this paper formulates a definition of entangled information flow and addresses some fundamental theoretical questions, it certainly does not claim to answer all the questions which are necessary to assess to what extent information leakage assisted by entanglement may constitute a threat in practice. In particular, the systems we have considered have mainly been rather artificial, constructed from non-local games specifically to have the properties we want. In the future it will be necessary to analyse more realistic systems to determine whether they may be affected by entanglement. This is likely to require handling less abstracted models than that described in Section II-A, and finding pragmatic algorithms which are more efficient in practical cases than that described in Section VI.

Finally, we do not by any means intend to suggest that approaches in the style of [8], in which the channels themselves may be quantum, are anything other than equally important as future directions for QIF in the quantum realm. Quantum networks may well become extremely relevant in the near or medium-term future, and indeed quantum key distribution systems already exist. We hope that in the future it may be possible to extend the approach of this paper to that setting, perhaps by extending Fig 1 to allow quantum states as messages.

References

[1] A. S. Holevo, "Some estimates for the amount of information transmittable by a quantum communications channel," *Problemy Peredači Informacii*, vol. 9, no. 3, pp. 3–11, 1973.

[2] J. A. Goguen and J. Meseguer, "Security policies and security models," in *1982 IEEE Symposium on Security and Privacy*. IEEE, 1982, pp. 11–20.

[3] J. W. Gray, III, "Toward a mathematical foundation for information flow security," *J. Comput. Secur.*, vol. 1, no. 3-4, pp. 255–294, May 1992. [Online]. Available: http://dl.acm.org/citation.cfm?id=2699806.2699811

[4] G. Smith, "On the foundations of quantitative information flow," in *Proc. 12th Int. Conf. on Foundations of Software Science and Computational Structures (FOSSACS '09)*, 2009, pp. 288–302.

[5] M. Alvim, K. Chatzikokolakis, A. McIver, C. Morgan, C. Palamidessi, and G. Smith, *The Science of Quantitative Information Flow*, ser. Information Security and Cryptography. United States: Springer, Springer Nature, 2020.

[6] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "MIP*=RE," 2020. [Online]. Available: https://arxiv.org/abs/2001.04383

[7] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, no. 7, p. 073013, 2008.

[8] A. Américo and P. Malacaria, "QQIF: Quantum quantitative information flow," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 261–270.

[9] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[10] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.

[11] D. Mestel, "Quantifying information flow in interactive systems," in *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*. IEEE, 2019, pp. 414–427.

[12] M. S. Alvim, K. Chatzikokolakis, Y. Kawamoto, and C. Palamidessi, "Information leakage games," in *International Conference on Decision and Game Theory for Security*. Springer, 2017, pp. 437–457.

[13] M. S. Alvim, K. Chatzikokolakis, A. McIver, C. Morgan, C. Palamidessi, and G. Smith, "Axioms for information leakage," in *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*. IEEE, 2016, pp. 77–92.

[14] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *Proc. 25th IEEE Computer Security Foundations Symposium (CSF '12)*, June 2012, pp. 265–279.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. John Wiley & Sons, Inc., 2005.

[16] B. Espinoza and G. Smith, "Min-entropy as a resource," *Information and Computation*, vol. 226, pp. 57–75, 2013.

[17] M. Nielsen and I. Chuang, "Quantum computation and quantum information," 2000.

[18] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden variable theories." *Physical Review Letters*, vol. 23, pp. 880–884, 1969.

[19] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner, "Connes' embedding problem and tsirelson's problem," *Journal of Mathematical Physics*, vol. 52, no. 1, p. 012102, 2011.

[20] A. Connes, "Classification of injective factors cases II1, II∞, IIIλ, $\lambda \neq 1$," *Annals of Mathematics*, pp. 73–115, 1976.

[21] H. Wolkowicz, R. Saigal, and L. Vandenberghe, *Handbook of semidefinite programming: theory, algorithms, and applications*. Springer Science & Business Media, 2012, vol. 27.

[22] C. Braun, K. Chatzikokolakis, and C. Palamidessi, "Quantitative notions of leakage for one-try attacks," *Electronic Notes in Theoretical Computer Science*, vol. 249, pp. 75 – 91, 2009, proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1571066109003077