

Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost

André Chailloux, Giannicola Scarpa

► **To cite this version:**

André Chailloux, Giannicola Scarpa. Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost. ICALP 2014, Jun 2014, Copenhagen, Denmark. pp.296 - 307, 2014, <10.1007/978-3-662-43948-7_25>. <hal-01094111>

HAL Id: hal-01094111

<https://hal.inria.fr/hal-01094111>

Submitted on 22 Dec 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost

André Chailloux¹ and Giannicola Scarpa²

¹ SECRET Project Team, INRIA Paris-Rocquencourt

² CWI, Amsterdam

Abstract. In a two-player game, two cooperating but non communicating players, Alice and Bob, receive inputs taken from a probability distribution. Each of them produces an output and they win the game if they satisfy some predicate on their inputs/outputs. The entangled value $\omega^*(G)$ of a game G is the maximum probability that Alice and Bob can win the game if they are allowed to share an entangled state prior to receiving their inputs.

The n -fold parallel repetition G^n of G consists of n instances of G where the players receive all the inputs at the same time and produce all the outputs at the same time. They win G^n if they win each instance of G .

In this paper we show that for any game G such that $\omega^*(G) = 1 - \varepsilon < 1$, $\omega^*(G^n)$ decreases exponentially in n . First, for any game G on the uniform distribution, we show that $\omega^*(G^n) = (1 - \varepsilon^2)^{\Omega\left(\frac{n}{\log(|I||O|)} - |\log(\varepsilon)|\right)}$, where $|I|$ and $|O|$ are the sizes of the input and output sets. From this result, we show that for any entangled game G , $\omega^*(G^n) \leq (1 - \varepsilon^2)^{\Omega\left(\frac{n}{Q \log(|I||O|)} - \frac{|\log(\varepsilon)|}{Q}\right)}$ where p is the input distribution of G and $Q = \frac{|I|^2 \max_{x,y} p_{xy}^2}{\min_{x,y} p_{xy}}$. This implies parallel repetition with exponential decay as long as $\min_{x,y} \{p_{xy}\} \neq 0$ for general games. To prove this parallel repetition, we introduce the concept of *Superposed Information Cost* for entangled games which is inspired from the information cost used in communication complexity.

1 Introduction

A *two-player (nonlocal) game* is played between two cooperating parties Alice and Bob which are not allowed to communicate. This game G is characterized by an input set I , an output set O , a probability distribution p on I^2 and a result function $V : O^2 \times I^2 \rightarrow \{0, 1\}$. The game proceeds as follows: Alice receives $x \in I$, Bob receives $y \in I$ where (x, y) is taken according to p . Alice outputs $a \in O$ and Bob outputs $b \in O$. They win the game if $V(a, b|x, y) = 1$. The value of the game $\omega(G)$ is the maximum probability, over all strategies, with which Alice and Bob can win the game.

The n -fold parallel repetition G^n of G consists of the following. Alice and Bob get inputs x_1, \dots, x_n and y_1, \dots, y_n , respectively. Each (x_i, y_i) is taken independently according to p . They output a_1, \dots, a_n and b_1, \dots, b_n , respectively. They win the game if and only if $\forall i, V(a_i, b_i|x_i, y_i) = 1$. In order to win the n -fold repetition, Alice and Bob can just take the best strategy for G and use it n times. If they do so, they will win G^n with probability $(\omega(G))^n$ which shows that $\omega(G^n) \geq (\omega(G))^n$.

Parallel repetition of games studies how the quantity $\omega(G^n)$ behaves. For example, if $\omega(G^n) = (\omega(G))^n$ for each n then we say that G admits perfect parallel repetition. However, there are some games for which this does not hold, for example the CHSH game [7] repeated two times. It was a long-standing open question to determine whether the value of $\omega(G^n)$ decreases exponentially in n . This was first shown by Raz [24]. Afterwards, a series of works showed improved results for specific types of games [14,23,1]. Parallel repetition for games has many applications, from direct product theorems in communication complexity [22] to hardness of approximation results [3,10,12].

In the quantum setting, it is natural to consider games where Alice and Bob are allowed to share some entangled state at the beginning of the game. In this case we talk about entangled strategies. The maximum probability that Alice and Bob can win a game G , over all the entangled strategies, is the entangled value $\omega^*(G)$. Some entangled games are witnesses for the phenomenon of quantum non-locality, as they are special

cases of the so-called Bell inequality violations. (We have a Bell inequality violation whenever $\omega^*(G) > \omega(G)$.) The study of entangled games is also greatly related to our understanding of quantum entanglement.

Perfect parallel repetition has been shown for entangled XOR games [8]. It was also shown that entangled unique games [16] admit parallel repetition with exponential decay. Finally, it was shown that any entangled game admits (a variant of) parallel repetition [17]. However, this last parallel repetition only shows a polynomial decay of $\omega^*(G^n)$. It was unknown for a large class of games whether this decay is exponential or not. Very recently two more works have been presented: a parallel repetition result with exponential decay for entangled projection games [9] and an independent work [15] similar to this one.

1.1 Contribution

The main contribution of this paper is the following theorem.

Theorem 1. *For any game G on the uniform distribution with $\omega^*(G) \leq 1 - \varepsilon$, we have:*

$$\omega^*(G^n) = (1 - \varepsilon^2)^{\Omega\left(\frac{n}{\log(|I||O|)} - |\log(\varepsilon)|\right)}.$$

where $|I|$ and $|O|$ are respectively the size of the input and the output sets.

The class of entangled games with a uniform distribution is a large class of entangled games for which such parallel repetition was unknown. We can extend this result to any entangled game.

Corollary 1. *For any game G such that $\omega^*(G) \leq 1 - \varepsilon$, we have that*

$$\omega^*(G^n) \leq (1 - \varepsilon^2)^{\Omega\left(\frac{n}{Q \log(|I||O|)} - \frac{|\log(\varepsilon)|}{Q}\right)},$$

where I and O are respectively the input and output sets and $Q = \frac{k^2 \max_{xy} p_{xy}^2}{\min_{xy} p_{xy}}$.

This corollary can be obtained directly from the previous theorem. It is not as strong as usual parallel repetition theorems with exponential decay because of this dependency on Q . Notice however that Q depends only on the game G and not on n .

Remark: In a previous version of this paper, we had a different claim which had a flaw in the proof. We replaced it by the above Corollary which is weaker in the sense that it gives non trivial bounds only for the case where $\min_{xy} \{p_{xy}\} \neq 0$.

1.2 Superposed Information cost

In order to prove the main theorem, we introduce the concept of *Superposed Information Cost* of a game, an insightful concept and the cornerstone of our proof.

This concept is derived from the notion of information cost widely used in communication complexity [6,2,4,18]. In the setting of communication complexity, we consider a function $f(x, y)$ and suppose that Alice has some input x and Bob some input y . They want to determine the outcome of $f(x, y)$ for a certain function f with the minimal amount of communication. The interactive information cost IC of f describes the least amount of information that Alice and Bob need to have about each other's inputs in order to compute $f(x, y)$.

We want to follow a similar approach for entangled games. In entangled games, the quantum state Alice and Bob share is independent of the inputs x, y . We now give extra resources to Alice and Bob: advice states. Alice and Bob are given an advice state $|\phi_{xy}\rangle$ that can depend on their inputs. This can greatly increase their winning probability. For example, Alice could have perfect knowledge of Bob's input y , and vice-versa.

We define (informally) the information cost of a game as follows:

Information Cost for entangled games

Alice and Bob are given advice states $|\phi_{xy}\rangle$ to share that can depend on their inputs. What is the minimal amount of information that these states have to give Alice and Bob about each other's input, in order to allow them to win the game with probability 1?

This is a natural extension of the information cost to entangled games. However, it is a limited notion since we cannot relate it to the entangled value of the game. (A simple counterexample can be obtained from the CHSH game.) Therefore, we extended this notion to the case where we allow the players to be *in a superposition of their inputs*.

Superposed Information Cost (SIC) for entangled games

We extend the notion of information cost by allowing the players to have a superposition of their inputs. We then consider the amount of information that advice states have to give Alice and Bob about each other's input, in order to allow them to win with probability 1.

These notions are defined precisely in Section 3.1.

Lower bounding the value of entangled games using the superposed information cost. The reason we introduce the superposed information cost for entangled games is that we want to have an information theoretic characterization of the value of entangled games. The next theorem states that the value of any entangled game on the uniform distribution can be lower bounded by the superposed information cost (this does not hold for the non-superposed one).

Theorem 2. *For any game G with a uniform input distribution, we have $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$ or equivalently $\omega^*(G) \geq 1 - 32 \ln(2) \cdot SIC(G)$.*

The Superposed information cost is additive under parallel repetition:

Proposition 1. $SIC(G^n) = nSIC(G)$.

Putting these two results together, we have $SIC(G^n) \geq \frac{n(1-\omega^*(G))}{32 \ln(2)}$. This result shows that $SIC(G^n)$ is large when n increases and can be seen as evidence that the game G^n is hard to win and that $\omega^*(G^n)$ decreases fast.

Using SIC to show our parallel repetition theorem. We fix a game G with $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$ for some t . In order to prove our theorem, we consider a quantity S which is strongly related to $SIC(G^n)$. We show that

$$\Omega(n\varepsilon) \leq S \leq O\left(\frac{t \log(|I||O|)}{\varepsilon}\right). \quad (1)$$

The lower bound is a natural extension of the above argument about the additivity of SIC. The ingredient we need to show the upper bound is the following *communication task*:

- The players use an optimal strategy for G^n and win with probability $\omega^*(G^n) = 2^{-t}$.
- Alice sends $m = O\left(\frac{t \log(|I||O|)}{\varepsilon}\right)$ bits to Bob.
- Using this message, Bob's goal is to determine with high probability whether they won most of the games or not.

Switching to a communication task and to a related quantity S seems much weaker than showing directly an upper bound on $SIC(G^n)$, but it will be enough for us. Combining these two results, we conclude that $t = \Omega\left(\frac{n\varepsilon^2}{\log(|I||O|)}\right)$ or equivalently, for ε close to 0, $\omega^*(G^n) = (1 - \varepsilon^2)^{\Omega\left(\frac{n}{\log(|I||O|)}\right)}$.

1.3 Organization of the paper

Section 2 contains preliminaries about entangled games. In Section 3, we define the key concept of the superposed information cost for a game and show that this quantity is additive when repeating games in parallel. In Section 4, we provide a brief organization of the main proof. In Section 5, we show Theorem 2 and some generalizations. In Section 6 we derive the upper bound of (1) (the lower bound is proven in the main paper). Finally, in Section 7 we prove our main theorem. Many proofs are deferred to the Appendix.

2 Entangled Games

The value of an entangled game

Definition 1. An entangled game $G = (I, O, V, p)$ is defined by finite input and output sets I and O as well as an accepting function $V : O^2 \times I^2 \rightarrow \{0, 1\}$ and a probability distribution $p : I^2 \rightarrow [0, 1]$.

A strategy for the game proceeds as follows. Alice and Bob can share any quantum state. Then, Alice receives an input $x \in I$ and Bob receives an input $y \in I$ where these inputs are sampled according to p . They can perform any quantum operation but are not allowed to communicate. Alice outputs $a \in O$ and Bob outputs $b \in O$. They win the game if $V(a, b|x, y) = 1$.

The *entangled value* of a game G is the maximal probability with which Alice and Bob can win the game. From standard purification techniques, we have that w.l.o.g., Alice and Bob share a pure state $|\phi\rangle$ and their optimal strategy consists of projective measurements $A^x = \{A_a^x\}_{a \in O}$ and $B^y = \{B_b^y\}_{b \in O}$ on $|\phi\rangle$. This means that after receiving their inputs, they share a state of the form $\rho = \sum_{x, y \in I} p_{xy} |x\rangle\langle x| \otimes |\phi\rangle\langle\phi| \otimes |y\rangle\langle y|$, for some state $|\phi\rangle$.

Definition 2. The entangled value of a game G is

$$\omega^*(G) = \sup_{|\phi\rangle, A^x, B^y} \sum_{x, y, a, b} p_{xy} V(a, b|x, y) \langle\phi| A_a^x \otimes B_b^y |\phi\rangle.$$

Definition 3. A game $G = (I, O, V, p)$ is on the uniform distribution if $I = [k]$ for some k and $\forall x, y \in [k]$, $p_{xy} = \frac{1}{k^2}$. We write $p = \text{Unif.}$ when this is the case.

Value of a game with advice states Consider a game $G = (I, O, V, p)$. We are interested in the value of the game when the two players share an advice state $|\phi_{xy}\rangle$ additionally to their inputs x, y . This means that Alice and Bob share a state of the form $\rho = \sum_{x, y, a, b} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$.

Definition 4. The entangled value of G , given that Alice and Bob share the above state ρ is

$$\omega^*(G|\rho) = \max_{A^x, B^y} \sum_{x, y} p_{xy} V(a, b|x, y) \langle\phi_{xy}| A_a^x \otimes B_b^y |\phi_{xy}\rangle.$$

Repetition of entangled games In the n -fold parallel repetition of a game G , each player gets n inputs from I and must produce n outputs from O . Each instance of the game will be evaluated as usual by the function V . The players win the parallel repetition game if they win *all* the instances. More formally, for a game $G = (I, O, V, p)$ we define $G^n = (I', O', V', q)$, where $I' = I^{\times n}$, $O' = O^{\times n}$, $q_{xy} = \prod_{i \in [n]} p_{x_i, y_i}$ and $V'(a, b|x, y) = \prod_{i \in [n]} V(a_i, b_i|x_i, y_i)$. While playing G^n , we say that Alice and Bob win game i if $V(a_i, b_i|x_i, y_i) = 1$.

Majority game For a game $G = (I, O, V, p)$ and a real number $\alpha \in [0, 1]$ we define $G_\alpha^n = (I', O', V', p')$ as follows: $I' = I^{\times n}$, $O' = O^{\times n}$, $p'_{xy} = \prod_{i \in [n]} p_{x_i, y_i}$ as in G^n . We define $V'(a, b|x, y) = 1 \Leftrightarrow \#\{i : V(a_i, b_i|x_i, y_i) = 1\} \geq \alpha n$.

3 Advice states, superposed players and information cost

The notion of information cost has been very useful for communication complexity. Here we derive a similar notion for entangled games.

Consider a game with advice state as defined in Section 2. The advice state can potentially greatly help the players. For example, Alice could know y and Bob could know x . We ask ourselves the following question:

For a game $G = (I = [k], O, V, p)$ such that $\omega^(G) = 1 - \varepsilon < 1$ and a state $\rho = \sum_{x,y \in [k]} p_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$, what is the minimum dependency that the states $\{|\phi_{xy}\rangle\}_{xy}$ must have on x, y to have $\omega^*(G|\rho) = 1$?*

There are different ways of characterizing this dependency on x, y . A first possibility would be to consider the information that Alice has about y and Bob has about x while sharing ρ . However, there are cases where Alice and Bob can win a game with probability 1 using an advice state while still not learning anything about each other's input. For example, take the CHSH game [7] and consider the states $|\phi_{00}\rangle = |\phi_{01}\rangle = |\phi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\mathcal{AB}}$ and $|\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. If the two players share the state $\rho = \sum_{x,y \in \{0,1\}} 1/4 |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$, Alice has no information about y and Bob has no information about x . On the other hand, if both players measure their registers \mathcal{A} and \mathcal{B} in the computational basis and output the results, they will win the CHSH game with probability 1 hence $\omega^*(CHSH|\rho) = 1$ while $\omega^*(CHSH) = \cos^2(\pi/8)$.

We must consider a slightly different scenario so that Alice or Bob can learn something about the other player's input. When considering the amount of information that Alice has about Bob's input y , we allow Alice to have a coherent superposition of her inputs. Similarly, we will be interested in the amount of information Bob has about x when he has a coherent superposition of his inputs.

This scenario is motivated as follows: if Alice and Bob have a common procedure to create $|\phi_{xy}\rangle$ from their respective inputs x and y , Alice can create a superposition of her inputs and they can perform the same procedure. This scenario has for example been in order to show optimal bounds for quantum bit commitment [5].

This approach leads to the definition of the superposed information cost of a game. In the next section, we give formal definitions of this notion.

3.1 The superposed information cost

Consider a family of states $\{|\phi_{xy}\rangle\}_{xy}$ and a probability distribution $\{p_{xy}\}_{xy}$. Let $p_x = \sum_y p_{xy}$ and $p_y = \sum_x p_{xy}$. Let $|L_x^B\rangle = \frac{1}{\sqrt{p_x}} \sum_y \sqrt{p_{xy}} |\phi_{xy}\rangle |y\rangle$ and $|L_y^A\rangle = \frac{1}{\sqrt{p_y}} \sum_x \sqrt{p_{xy}} |x\rangle |\phi_{xy}\rangle$. Consider the two superposed states:

$$\begin{aligned} \sigma^A &= \sum_{y \in [k]} p_y |L_y^A\rangle\langle L_y^A|_{\mathcal{XAB}} \otimes |y\rangle\langle y|_{\mathcal{Y}} \\ \sigma^B &= \sum_{x \in [k]} p_x |x\rangle\langle x|_{\mathcal{X}} \otimes |L_x^B\rangle\langle L_x^B|_{\mathcal{ABY}}. \end{aligned}$$

Here σ^A (resp. σ^B) corresponds to ρ where Alice's input (resp. Bob's input) is put in a coherent superposition. We first define the superposed information cost of a family of states with a probability distribution.

Definition 5. *The superposed information cost $SIC(\{|\phi_{xy}\rangle, p_{xy}\}_{xy})$ is defined as $SIC(\{|\phi_{xy}\rangle, p_{xy}\}_{xy}) = I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B}$.*

Remark: This definition has good properties when the input distribution is a product distribution or close to a product distribution. One may want to consider a more general definition when considering any distribution.

We also define the superposed information cost of a shared state ρ of the form $\rho = \sum_{x,y \in [k]} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$.

Definition 6. $SIC(\rho) = \inf\{SIC(\{|\phi_{xy}\rangle, p_{xy}\}_{xy})\}$ where the infimum is taken over all families $\{|\phi_{xy}\rangle, p_{xy}\}_{xy}$ s.t. $\rho = \sum_{x,y \in [k]} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$.

Remark: Notice that a state ρ doesn't uniquely define states $\{|\phi_{xy}\rangle, p_{xy}\}_{xy}$ because it doesn't capture the phases in the states $|\phi_{xy}\rangle$.

We now define the superposed information cost of an entangled game.

Definition 7. For any entangled game $G = (I, O, V, p)$, we define $SIC(G) = \inf\{SIC(\{|\phi_{xy}\rangle\}_{xy}, \{p_{xy}\}_{xy})\}$ where the infimum is taken over all $(\{|\phi_{xy}\rangle\}_{xy}, \{p_{xy}\}_{xy})$ such that the associated state $\rho = \sum_{x,y} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ satisfies $\omega^*(G|\rho) = 1$.

The superposed information cost behaves nicely under parallel repetition. In Appendix B, we show

Proposition 2. For any game G , we have $SIC(G^n) = n \cdot SIC(G)$.

4 Organisation of the proof of Theorem 1

In Section 5, we show how to use the *Superposed Information Cost* of a game G to bound its entangled value $\omega^*(G)$. We first show:

Theorem 2. For any game G on the uniform distribution, $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$.

We also extend this theorem as follows:

Theorem 3. There exists a small constant c_0 such that for any game $G = (I = [k], O, V, Unif.)$ satisfying $\omega^*(G) = 1 - \varepsilon$, for any game $G' = (I = [k], O, V, p)$ satisfying $\frac{1}{2} \sum_{x,y} |p_{xy} - \frac{1}{k^2}| \leq c_0 \varepsilon$ and any state $\rho = \sum_{x,y} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G'|\rho) \geq 1 - \frac{\varepsilon}{4}$, we have that $SIC(\rho) = \Omega(\varepsilon)$.

If $\omega^*(G) = 1 - \varepsilon$, Theorem 2 claims that $SIC(G) \geq \frac{\varepsilon}{32 \ln(2)}$ which gives by additivity of the superposed information cost that $SIC(G^n) \geq \frac{n\varepsilon}{32 \ln(2)}$. Ideally, we would like to upper bound $SIC(G^n)$ with a function of $\omega^*(G^n)$. Unfortunately, we are not able to do this directly. In Section 6, we show the following weaker statement:

Theorem 4. Consider a game $G = (I, O, V, Unif.)$ such that $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$. Let $G_{1-\varepsilon/32}^n = (I^n, O^n, V', Unif.)$ as defined in Section 2. There exists a game $G' = (I^n, O^n, V', p)$ and a state $\xi = \sum_{x,y} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ satisfying the following properties:

1. $H(XY)_\xi \geq 2n \log(k) - t - 1$
2. $\omega^*(G'|\xi) \geq 1 - \varepsilon/32$
3. $SIC(\xi) \leq \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5) + 2t + 2$.

The first condition states that p is in some sense close to the uniform distribution hence G' is close to $G_{1-\varepsilon/32}^n$. This theorem is weaker than an upper bound on $SIC(G')$ which itself is weaker than an upper bound on $SIC(G^n)$, but this kind of upper bound will be enough.

In Appendix E, we prove the following matching lower bound.

Theorem 5. Consider a game $G = (I = [k], O, V, Unif.)$ such that $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$ with $t = o(n\varepsilon)$. Let also $G_{1-\varepsilon/32}^n = (I^n = [k^n], O^n, V', Unif.)$ as defined in Section 2. For any game $G' = (I' = [k^n], O', V', p)$ and any state $\rho = \sum_{x,y \in [k^n]} p_{xy}|x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$, satisfying

1. $H(XY)_\rho \geq 2n \log(k) - t - 1$
2. $\omega^*(G'|\rho) \geq 1 - \varepsilon/32$

we have $SIC(\rho) \geq \Omega(n\varepsilon)$.

In Section 7, we show how to use the two above theorems to conclude:

Theorem 1. For any game $G = (I, O, V, Unif.)$ with $\omega^*(G) \leq 1 - \varepsilon$, we have $\omega^*(G^n) = (1 - \varepsilon^2)^{\Omega(\frac{n}{\log(|I||O|)} - |\log(\varepsilon)|)}$.

5 Overview of Theorem 2

Theorem 2. For any game G on the uniform distribution, $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$.

We sketch the proof as follows. We fix a game $G = (I = [k], O, V, \text{Unif.})$ and a state $\rho = \sum_{x,y} \frac{1}{k^2} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$ such that $\omega^*(G|\rho) = 1$. As in Section 3.1, we define $|L_y^A\rangle, |L_x^B\rangle, \sigma^A, \sigma^B$. Let $\rho_y^A = \text{Tr}_{\mathcal{B}} |L_y^A\rangle\langle L_y^A|$ and $\rho_x^B = \text{Tr}_{\mathcal{A}} |L_x^B\rangle\langle L_x^B|$. Intuitively, ρ_y^A (resp. ρ_x^B) corresponds to the input-superposed state that Alice (resp. Bob) has, conditioned on Bob getting y (resp. Alice getting x). Let F denote the fidelity of quantum states. We prove the following three inequalities.

1. First we show that $SIC(\rho) \geq \frac{1}{4 \ln(2)} (1 - \frac{1}{k^2} \sum_{y,y'} F^2(\rho_y^A, \rho_{y'}^A) + 1 - \frac{1}{k^2} \sum_{x,x'} F^2(\rho_x^B, \rho_{x'}^B))$
2. Then we show that

$$1 - \frac{1}{k^2} \sum_{y,y'} F^2(\rho_y^A, \rho_{y'}^A) + 1 - \frac{1}{k^2} \sum_{x,x'} F^2(\rho_x^B, \rho_{x'}^B) \geq \frac{1}{8} (1 - \max_{|\Omega\rangle} \sum_{x,y \in [k]} \frac{1}{k^2} |\langle \Omega | U_x \otimes V_y | \phi_{xy} \rangle|^2)$$

for some (sets of) unitaries $\{U_x\}_x, \{V_y\}_y$.

3. Finally, we show that $(1 - \max_{|\Omega\rangle} \sum_{x,y \in [k]} \frac{1}{k^2} |\langle \Omega | U_x \otimes V_y | \phi_{xy} \rangle|^2) \geq 1 - \omega^*(G)$.

Putting the three inequalities together, we get

$$\begin{aligned} SIC(\rho) &\geq \frac{1}{4 \ln(2)} (1 - \frac{1}{k^2} \sum_{y,y'} F^2(\rho_y^A, \rho_{y'}^A) + 1 - \frac{1}{k^2} \sum_{x,x'} F^2(\rho_x^B, \rho_{x'}^B)) \\ &\geq \frac{1}{32 \ln(2)} (1 - \max_{|\Omega\rangle} \sum_{x,y \in [k]} \frac{1}{k^2} |\langle \Omega | U_x \otimes V_y | \phi_{xy} \rangle|^2) \quad \text{for some } \{U_x\}_x \{V_y\}_y \\ &\geq \frac{1 - \omega^*(G)}{32 \ln(2)}. \end{aligned}$$

Since this holds for any ρ satisfying $\omega^*(G|\rho) = 1$, we have $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$.

6 Overview of Theorem 4

In this section we sketch the proof of Theorem 4. The construction of the state ξ will directly be inspired by a communication task that we now present.

The communication task Fix a game $G = (I, O, V, \text{Unif.})$ satisfying $\omega^*(G) = 1 - \varepsilon$. Let $G^n = (I^n, O^n, V_n, \text{Unif.})$ such that $\omega^*(G^n) = 2^{-t}$ for some t . We now consider the following task $H(p, m)$.

Task H(p, m)

- Alice and Bob are allowed to share any quantum state $|\phi\rangle$.
- Alice and Bob get inputs $x = x_1, \dots, x_n$ and $y = y_1, \dots, y_n$, with $x, y \in I^n$, following the uniform distribution.
- Alice is allowed to send m bits to Bob
- Then Alice outputs some value $a \in O^n$ and Bob outputs some value $b \in O^n$ or 'Abort'.

For each index i , we say that Alice and Bob win game i if Bob does not abort and $V(a_i, b_i | x_i, y_i) =$

1. We require the following

1. $Pr[\text{Bob does not abort}] \geq p$
2. $Pr[\text{Alice and Bob win} \geq (1 - \varepsilon/32)n \text{ games} \mid \text{Bob does not abort}] \geq (1 - \varepsilon/32)$.

Showing how to perform this task with a small amount of communication is a first step towards the construction of ξ . We consider the following protocol P that efficiently performs this task.

Protocol P for the task $H(p,m)$

1. Let $v \leq n$ be an integer, to be determined at the end of this section. Alice and Bob have shared randomness that correspond to v random (not necessarily different) indices $i_1, \dots, i_v \in [n]$ as well as a state $|\phi\rangle$ that allows them to win G^n with probability at least $\frac{\omega^*(G^n)}{2} = 2^{-(t+1)}$.
2. Alice and Bob receive uniform inputs x, y . They perform a strategy that wins all n games with probability $2^{-(t+1)}$ and have some outputs $a = a_1, \dots, a_n$ and $b = b_1, \dots, b_n$.
3. For each index $i \in \{i_1, \dots, i_v\}$, Alice sends x_i and a_i to Bob.
4. For each of these indices i , Bob looks at x_i, y_i, a_i, b_i and checks whether they win on all of these v games, *i.e.*, he checks that for all these indices, $V(a_i, b_i | x_i, y_i) = 1$.
5. If they do win on all of these games, Bob outputs b . Otherwise, Bob outputs 'Abort'.

Proposition 3. *The above protocol performs the task $H(p, m)$ with $p \geq 2^{-(t+1)}$ and $m = \frac{32 \log(|I||O|)}{\varepsilon} ((t+1) + |\log(\varepsilon)| + 5)$.*

Proof. We have:

$$\begin{aligned} \Pr[\text{Bob does not abort}] &= \Pr[\text{Alice and Bob win } G_i \forall i \in \{i_1, \dots, i_v\}] \\ &\geq \Pr[\text{Alice and Bob win } G_i \forall i \in [n]] = 2^{-(t+1)}, \end{aligned}$$

hence $p \geq 2^{-(t+1)}$. For a uniformly random index i , we have:

$$\Pr[\text{Alice and Bob win } G_i \mid \text{Alice and Bob win } \leq (1 - \varepsilon/32)n \text{ games}] \leq 1 - \varepsilon/32.$$

Since the indices in $\{i_1, \dots, i_v\}$ are independent random indices in $[n]$, we have

$$\begin{aligned} \Pr[\text{Bob does not abort} \mid \text{Alice and Bob win } \leq (1 - \varepsilon/32)n \text{ games}] \\ = \Pr[\text{Alice and Bob win } G_i \forall i \in \{i_1, \dots, i_v\} \mid \text{Alice and Bob win } \leq (1 - \varepsilon/32)n \text{ games}] \\ \leq (1 - \varepsilon/32)^v. \end{aligned}$$

Next, we have:

$$\begin{aligned} \Pr[\text{A and B win } \leq (1 - \varepsilon/32)n \text{ games} \mid \text{B does not abort}] \cdot \Pr[\text{B does not abort}] \\ = \Pr[\text{B does not abort} \mid \text{A and B win } \leq (1 - \varepsilon/32)n \text{ games}] \cdot \Pr[\text{A and B win } \leq (1 - \varepsilon/32)n \text{ games}] \\ \leq \Pr[\text{B does not abort} \mid \text{A and B win } \leq (1 - \varepsilon/32)n \text{ games}] \\ \leq (1 - \varepsilon/32)^v. \end{aligned}$$

This gives us:

$$\begin{aligned} \Pr[\text{A and B win } \leq (1 - \varepsilon/32)n \text{ games} \mid \text{B does not abort}] &\leq \frac{(1 - \varepsilon/32)^v}{\Pr[\text{B does not abort}]} \\ &\leq \frac{(1 - \varepsilon/32)^v}{2^{-(t+1)}}. \end{aligned}$$

We can take $v = \frac{32}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5)$, such that we have

$$\Pr[\text{A and B win } \leq (1 - \varepsilon/32)n \text{ games} \mid \text{B does not abort}] \leq \varepsilon/32.$$

Notice that $m = v \cdot \log(|I||O|)$. Therefore, if Alice sends $m = \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5)$ bits to Bob,

$$\Pr[\text{A and B win} \geq (1 - \varepsilon/32)n \text{ games} \mid \text{B does not abort}] \geq 1 - \varepsilon/32.$$

■

Using the communication task to prove Theorem 4

The idea is the following: Alice and Bob perform protocol P for the task $H(p, m)$ performing everything in superposition, including the messages and their shared randomness. The advice state we consider is the state ρ_{NA} Alice and Bob share conditioned on Bob not aborting. This state ρ_{NA} can be written as

$$\rho_{NA} = \sum_{xy} q_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|_{\mathcal{Y}}$$

To prove the theorem, we must show the following properties for ρ_{NA} .

1. $H(XY)_{\rho_{NA}} \geq 2n \log(k) - t - 1$.
2. $\omega^*(G' | \rho_{NA}) \geq 1 - \varepsilon/32$ where $G'_{1-\varepsilon/32} = (I', O', V', \text{Unif.})$ and $G' = (I', O', V', q)$.
3. $SIC(\rho_{NA}) \leq \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5) + 2t + 2$.

The ideas behind the proofs of these three properties are as follows:

1. In task H(p,m), $\Pr[\text{Bob does not abort}] \geq p = 2^{-t}$, when conditioning on Bob winning, we remove at most t bits of entropy from the (uniform) inputs in X, Y , the 1 in the inequality is there for technical reasons.
2. In the task H(p,m), $\Pr[\text{Alice and Bob win} \geq (1 - \varepsilon/32)n \text{ games} \mid \text{Bob does not abort}] \geq (1 - \varepsilon/32)$. This directly implies the second property
3. In protocol P, before Alice sends her message, Bob has no information about x . Alice sends a message of size m , which gives m bits of information about Alice's input. Conditioning on Bob winning gives him an extra $2t$ bits of information. Since $m = \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5)$ from the previous Proposition, we can conclude.

7 Final Theorem

Theorem 1. *For any game $G = (I, O, V, \text{Unif.})$ with $\omega^*(G) \leq 1 - \varepsilon$, we have:*

$$\omega^*(G^n) = (1 - \varepsilon^2)^{\Omega\left(\frac{n}{\log(|I||O|)} - |\log(\varepsilon)|\right)}.$$

Proof. Let $G'_{1-\varepsilon/32} = (I^n = [k^n], O^n, V_n, \text{Unif.})$ as defined in Section 2. Using Theorem 4, we know there exists a state $\xi = \sum_{xy} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|$ and a game $G' = (I^n, O^n, V_n, p)$ satisfying

1. $H(XY)_{\xi} \geq 2n \log(k) - t - 1$
2. $\omega^*(G' | \xi) \geq 1 - \varepsilon/32$
3. $SIC(\xi) \leq \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5)$,

where $2^{-t} = \omega^*(G^n)$. We now distinguish two cases

- If $t = \Omega(\varepsilon n)$ then $\omega^*(G^n) = (1 - \varepsilon)^{\Omega(n)}$ and the theorem holds directly.
- If $t = o(\varepsilon n)$, we need the following argument. The state ξ satisfies all the properties of Theorem 5 which implies that $SIC(\xi) = \Omega(n\varepsilon)$. We combine the two inequalities and obtain

$$\Omega(n\varepsilon) \leq SIC(\xi) \leq \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5).$$

It follows that $t = \Omega\left(\frac{n\varepsilon^2}{\log(|T||O|)} - |\log(\varepsilon)|\right)$, which allows us to conclude

$$\omega^*(G^n) = 2^{-t} \leq (1 - \varepsilon^2)^{O\left(\frac{n}{\log(|T||O|)} - |\log(\varepsilon)|\right)}.$$

■

Finally, we extend the result to games with complete support (*i.e.*, games on distributions p such that $\mathbb{A}(x, y)$ for which $p_{xy} = 0$). This bound is weaker than the main result, because it depends also on p .

Corollary 1. *Let $G = (I, O, V, p)$ be a game with complete support and $\omega^*(G) = (1 - \varepsilon)$. Then,*

$$\omega^*(G^n) \leq (1 - \varepsilon^2)^{\Omega\left(\frac{n}{Q \log(|T||O|)} - \frac{|\log(\varepsilon)|}{Q}\right)},$$

where $Q = \frac{k^2 \max_{xy} p_{xy}^2}{\min_{xy} p_{xy}}$.

The proof of the above Corollary is in Appendix F.

Acknowledgments The authors thank Serge Fehr, Anthony Leverrier, Christian Schaffner and Ronald de Wolf for helpful suggestions. Part of the work was done while A.C. was at CWI, Amsterdam. A.C. was partially supported by the European Commission under the project QCS (Grant No. 255961). G.S. was supported by de Wolf’s Vidi grant 639.072.803 from the Netherlands Organization for Scientific Research (NWO).

References

1. Sanjeev Arora, Subhash A. Khot, Alexandra Kolla, David Steurer, Madhur Tulsiani, and Nisheeth K. Vishnoi. Unique games on expanding constraint graphs are easy: extended abstract. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, STOC ’08, pages 21–28, New York, NY, USA, 2008. ACM.
2. Z. Bar-Yossef, T. S. Jayram, R. Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *J. Comput. Syst. Sci.*, 68(4):702–732, June 2004.
3. Mihir Bellare, Oded Goldreich, and Madhu Sudan. Free bits, pcps, and nonapproximability—towards tight results. *SIAM J. Comput.*, 27(3):804–915, June 1998.
4. Mark Braverman. Interactive information complexity. In *Proceedings of the 44th symposium on Theory of Computing*, STOC ’12, pages 505–524, New York, NY, USA, 2012. ACM.
5. A. Chailloux and I. Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, volume 0, pages 354–362, October 2011.
6. Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd IEEE symposium on Foundations of Computer Science*, FOCS ’01, pages 270–, Washington, DC, USA, 2001. IEEE Computer Society.
7. John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.
8. Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. *Comput. Complex.*, 17(2):282–299, May 2008.
9. Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. 2013.
10. Uriel Feige. A threshold of $\ln n$ for approximating set cover. *J. ACM*, 45(4):634–652, July 1998.
11. Christopher A. Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory* 45. No, pages 45–1216, 1999.
12. Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, July 2001.
13. C. W. Helstrom. Detection theory and quantum mechanics. 10(3):254–291, 1967.
14. Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, STOC ’07, pages 411–419, New York, NY, USA, 2007. ACM.

15. Rahul Jain, Attila Pereszlyni, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. 2013.
16. Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. In *Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '08, pages 457–466, Washington, DC, USA, 2008. IEEE Computer Society.
17. Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 353–362, New York, NY, USA, 2011. ACM.
18. Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jeremie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, FOCS '12, pages 500–509, Washington, DC, USA, 2012. IEEE Computer Society.
19. H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman. Interaction in quantum communication. *Information Theory, IEEE Transactions on*, 53(6):1970–1982, 2007.
20. Martin Mller-Lennert, Frdric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. On quantum Renyi entropies: a new definition and some properties. *ArXiv e-prints*, June 2013.
21. Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67(1):012304, Jan 2003.
22. Itzhak Parnafes, Ran Raz, and Avi Wigderson. Direct product results and the gcd problem, in old and new communication models. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, STOC '97, pages 363–372, New York, NY, USA, 1997. ACM.
23. Anup Rao. Parallel repetition in projection games and a concentration bound. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, STOC '08, pages 1–10, New York, NY, USA, 2008. ACM.
24. Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, June 1998.
25. R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001.
26. Salil Pravin Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, 1999. Supervisor-Shafi Goldwasser.

A Preliminaries

A.1 Useful facts about the fidelity and trace distance of two quantum states.

We start by stating a few properties of the trace distance Δ and fidelity F between two quantum states. These two notions characterize how close two quantum states are.

Trace distance between two quantum states

Definition 8. For any two quantum states ρ, σ , the trace distance Δ between them is given by $\Delta(\rho, \sigma) = \Delta(\sigma, \rho) = \frac{1}{2} \|\rho - \sigma\|_{\text{tr}}$.

Here the used trace norm may be expressed as $\|X\|_{\text{tr}} = \sqrt{X^\dagger X} = \max_U |\text{tr}(XU)|$, where the maximization is taken over all unitaries of the appropriate size.

Proposition 4. For any two states ρ, σ , and a POVM $E = \{E_1, \dots, E_m\}$ with $p_i = \text{tr}(\rho E_i)$ and $q_i = \text{tr}(\sigma E_i)$, we have $\Delta(\rho, \sigma) \geq \frac{1}{2} \sum_i |p_i - q_i|$. There exists a POVM (even a projective measurement) for which this inequality is an equality.

Proposition 5. [13] Suppose Alice has a uniformly random bit $c \in \{0, 1\}$, unknown to Bob. She sends a quantum state ρ_c to Bob. We have

$$\Pr[\text{Bob guesses } c] \leq \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}.$$

There is a strategy for Bob that achieves the value $\frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$.

Fidelity of quantum states

Definition 9. For any two states ρ, σ , their fidelity F is given by $F(\rho, \sigma) = F(\sigma, \rho) = \text{tr}(\sqrt{\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}}})$

Proposition 6. For any two states ρ, σ , and a POVM $E = \{E_1, \dots, E_m\}$ with $p_i = \text{tr}(\rho E_i)$ and $q_i = \text{tr}(\sigma E_i)$, we have $F(\rho, \sigma) \leq \sum_i \sqrt{p_i q_i}$. There exists a POVM for which this inequality is an equality.

Definition 10. We say that a pure state $|\psi\rangle$ in $\mathcal{A} \otimes \mathcal{B}$ is a purification of some state ρ in \mathcal{B} if $\text{Tr}_{\mathcal{A}}(|\psi\rangle\langle\psi|) = \rho$.

Proposition 7 (Uhlmann's theorem). For any two quantum states ρ, σ , there exists a purification $|\phi\rangle$ of ρ and a purification $|\psi\rangle$ of σ such that $|\langle\phi|\psi\rangle| = F(\rho, \sigma)$.

Proposition 8. For any two quantum states ρ, σ and a completely positive trace preserving operation Q , we have $F(\rho, \sigma) \leq F(Q(\rho), Q(\sigma))$.

Proposition 9 ([25,21]). For any two quantum states ρ, σ

$$\max_{\xi} (F^2(\rho, \xi) + F^2(\xi, \sigma)) = 1 + F(\rho, \sigma).$$

Proposition 10 ([11]). For any quantum states ρ, σ , we have

$$1 - F(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{1 - F^2(\rho, \sigma)}.$$

As direct corollaries of Proposition 9, we have

Proposition 11. Let $|A\rangle, |B\rangle, |C\rangle$ be three quantum states. We have

$$|\langle A|C\rangle| \geq |\langle A|B\rangle|^2 + |\langle B|C\rangle|^2 - 1.$$

and

Proposition 12. For any 3 quantum states ρ_1, ρ_2, ρ_3 , we have

$$(1 - F(\rho_1, \rho_2)) + (1 - F(\rho_2, \rho_3)) \geq \frac{1}{2}(1 - F(\rho_1, \rho_3)),$$

or equivalently $F(\rho_1, \rho_3) \geq 1 - 2(1 - F(\rho_1, \rho_2) + 1 - F(\rho_2, \rho_3))$.

Proof. Using Proposition 9, we have

$$\begin{aligned} 1 + F(\rho_1, \rho_3) &= \max_{\xi} (F^2(\rho_1, \xi) + F^2(\xi, \rho_3)) \\ &\geq F^2(\rho_1, \rho_2) + F^2(\rho_2, \rho_3), \end{aligned}$$

which gives

$$1 - F(\rho_1, \rho_3) \leq 1 - F^2(\rho_1, \rho_2) + 1 - F^2(\rho_2, \rho_3) \leq 2(1 - F(\rho_1, \rho_2)) + 2(1 - F(\rho_2, \rho_3)).$$

Hence $1 - F(\rho_1, \rho_2) + 1 - F(\rho_2, \rho_3) \geq \frac{1}{2}(1 - F(\rho_1, \rho_3))$. ■

Proposition 13. For two quantum states $\rho = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$ and $\rho' = \sum_x p'_x |x\rangle\langle x| \otimes \rho'_x$, we have $F(\rho, \rho') = \sum_x \sqrt{p_x p'_x} F(\rho_x, \rho'_x)$.

Proof. We use the following definition of the fidelity: $F(\rho, \rho') = \|\sqrt{\rho}\sqrt{\rho'}\|_1$. From there, we immediately have that

$$F(\rho, \rho') = \sum_x \sqrt{p_x p'_x} \|\sqrt{\rho_x}\sqrt{\rho'_x}\|_1 = \sum_x \sqrt{p_x p'_x} F(\rho_x, \rho'_x).$$
■

A.2 Information Theory

For a quantum state ρ , the entropy of ρ is $H(\rho) = -\text{tr}(\rho \log(\rho))$. For a quantum state $\rho \in \mathcal{X} \otimes \mathcal{Y}$, $H(X)_\rho$ is the entropy of the quantum register in the space \mathcal{X} when the total underlying state is ρ . In other words, $H(X)_\rho = H(\text{Tr}_{\mathcal{Y}}(\rho))$.

$H(X|Y)_\rho = H(XY)_\rho - H(Y)_\rho$ is the conditional entropy of X given Y on ρ and $I(X : Y)_\rho = H(X)_\rho + H(Y)_\rho - H(XY)_\rho$ is the mutual information between X and Y on ρ .

We define $H_{\min}(\rho) = -\log(\lambda_{\max})$ where λ_{\max} is the maximum eigenvalue of ρ . For ρ in $\mathcal{X} \otimes \mathcal{Y}$, we define

$$H_{\min}(X|Y)_\rho = \max_{\sigma \in \mathcal{Y}} \sup\{\lambda : \rho \leq 2^{-\lambda} I_{\mathcal{X}} \otimes \sigma\}$$

We have $H_{\min}(X|Y)_\rho \leq H(X|Y)_\rho$ [20]. In the case where Alice and Bob share $\rho = \sum_x p_x |x\rangle\langle x|_{\mathcal{X}} \otimes \rho(x)_{\mathcal{Y}}$, where Alice has register \mathcal{X} and Bob has register \mathcal{Y} , we have $H_{\min}(X|Y)_\rho = -\log(\Pr[\text{Bob can guess } x])$.

Claim (Subadditivity of the conditional entropy).

$$H(AB|C) \leq H(A|C) + H(B|C)$$

Claim ([19]).

$$I(A : B)_\rho \geq \frac{2}{\ln(2)}(1 - F(\rho, \rho_A \otimes \rho_B))$$

where $\rho_A = \text{Tr}_{\mathcal{B}}(\rho)$ and $\rho_B = \text{Tr}_{\mathcal{A}}(\rho)$

Claim (from [26]). For any distribution p on a universe U , if $H(p) \geq \log(|U|) - \varepsilon$ then $\Delta(p, \text{Unif.}) \leq \varepsilon$, where Unif. is the uniform distribution.

B Additivity of the superposed information cost

Our goal here is to prove the additivity of the superposed information cost, *i.e.* that $SIC(G^n) = nSIC(G)$. Before the proof, we introduce some notation and prove a lemma.

Let $G = (I, O, V, p)$ and let $G^n = (I^n, O^n, V_n, q)$. For a string $x = x_1, \dots, x_n \in I^n$, let x_{-i} be the string in I^{n-1} where we remove x_i from x . Let $\rho = \sum_{x,y \in I^n} q_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|$ satisfying $\omega^*(G^n|\rho) = 1$. As in Section 3.1, we define $|L_y^A\rangle, |L_x^B\rangle, \sigma^A, \sigma^B$ for ρ . We first prove the following Lemma:

Lemma 1. *For all $i \in [n]$ we have that*

$$I(Y_i : XA)_{\sigma^A} + I(X_i : YB)_{\sigma^B} \geq SIC(G).$$

Proof. By definition of G^n , we have $q_{xy} = \prod_j p_{x_j, y_j}$. We define $q_{xy}^{-i} = \prod_{j \neq i} p_{x_j, y_j}$. For each i , we can rewrite ρ as:

$$\rho = \sum_{x,y \in I^n} q_{xy} |x_i\rangle\langle x_i|_{\mathcal{X}_i} \otimes |x_{-i}\rangle\langle x_{-i}|_{\mathcal{X}_{-i}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}|_{AB} \otimes |y_{-i}\rangle\langle y_{-i}|_{\mathcal{Y}_{-i}} \otimes |y_i\rangle\langle y_i|_{\mathcal{Y}_i}.$$

We define

$$|Z_{x_i, y_i}^i\rangle = \sum_{x', y' \in I^n: x'_i = x_i, y'_i = y_i} \sqrt{q_{x' y'}^{-i}} |x'_{-i}\rangle \otimes |\phi_{x' y'}\rangle \otimes |y'_{-i}\rangle.$$

Let $\rho_i = \sum_{x_i, y_i \in I} p_{x_i, y_i} |x_i\rangle\langle x_i| \otimes |Z_{x_i, y_i}^i\rangle\langle Z_{x_i, y_i}^i| \otimes |y_i\rangle\langle y_i|$. ρ_i corresponds to ρ where the registers in $\mathcal{X}_{-i}, \mathcal{Y}_{-i}$ are put in superposition. Hence, Alice and Bob can go from ρ_i to ρ by measuring the registers \mathcal{X}_{-i} and \mathcal{Y}_{-i} in the computational basis. Using ρ , Alice and Bob can win the i^{th} instance of G with probability 1. This means that they can also win this i^{th} instance of G when sharing ρ_i and $\omega^*(G|\rho_i) = 1$.

We define

$$\begin{aligned} |L_{x_i}^B(i)\rangle &= \frac{1}{\sqrt{p_{x_i}}} \sum_{y_i \in I} \sqrt{p_{x_i, y_i}} |Z_{x_i, y_i}^i\rangle |y_i\rangle \\ |L_{y_i}^A(i)\rangle &= \frac{1}{\sqrt{p_{\cdot, y_i}}} \sum_{x_i \in I} \sqrt{p_{x_i, y_i}} |x_i\rangle |Z_{x_i, y_i}^i\rangle. \end{aligned}$$

We now also define the two new superposed states of ρ_i

$$\begin{aligned} \sigma_i^B &= \sum_{x_i \in I} p_{x_i} |x_i\rangle\langle x_i|_{\mathcal{X}_i} \otimes |L_{x_i}^B(i)\rangle\langle L_{x_i}^B(i)|_{\mathcal{X}_{-i} AB \mathcal{Y}} \\ \sigma_i^A &= \sum_{y_i \in I} p_{\cdot, y_i} |L_{y_i}^A(i)\rangle\langle L_{y_i}^A(i)|_{\mathcal{X} AB \mathcal{Y}_{-i}} \otimes |y_i\rangle\langle y_i|_{\mathcal{Y}_i}. \end{aligned}$$

$\omega^*(G|\rho_i) = 1$ implies $SIC(\rho_i) \geq SIC(G)$ hence

$$I(Y_i : XA)_{\sigma_i^A} + I(X_i : BY)_{\sigma_i^B} \geq SIC(G).$$

σ_i^A corresponds to σ^A where the input registers \mathcal{Y}_{-i} are put in a coherent superposition. From there, we have $Tr_{\mathcal{Y}_{-i}}(\sigma_i^A) = Tr_{\mathcal{Y}_{-i}}(\sigma^A)$ and $I(Y_i : XA)_{\sigma_i^A} = I(Y_i : XA)_{\sigma^A}$. Similarly, we have $I(X_i : BY)_{\sigma_i^B} = I(X_i : BY)_{\sigma^B}$, which gives

$$I(Y_i : XA)_{\sigma^A} + I(X_i : YB)_{\sigma^B} \geq SIC(G).$$

■

We can now prove our proposition:

Proposition 2. $SIC(G^n) = nSIC(G)$.

Proof. We have:

$$\begin{aligned}
SIC(\rho) &= I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B} \\
&= H(Y)_{\sigma^A} - H(Y|XA)_{\sigma^A} + H(X)_{\sigma^B} - H(X|BY)_{\sigma^B} \\
&= \sum_{i \in [n]} H(Y_i)_{\sigma^A} - H(Y|XA)_{\sigma^A} + \sum_{i \in [n]} H(X_i)_{\sigma^B} - H(X|BY)_{\sigma^B} \\
&\geq \sum_{i \in [n]} H(Y_i)_{\sigma^A} - \sum_{i \in [n]} H(Y_i|XA)_{\sigma^A} + \sum_{i \in [n]} H(X_i)_{\sigma^B} - \sum_{i \in [n]} H(X_i|BY)_{\sigma^B} \\
&= \sum_{i \in [n]} I(Y_i : XA)_{\sigma^A} + I(X_i : BY)_{\sigma^B} \\
&\geq nSIC(G),
\end{aligned}$$

where the first inequality comes from the subadditivity of the quantum conditional entropy and the last inequality comes from Lemma 1. Since this holds for any state ρ satisfying $\omega^*(G^n|\rho) = 1$, we conclude that $SIC(G^n) \geq nSIC(G)$.

We can also notice that $SIC(G^n) \leq nSIC(G)$. Indeed, consider a state ρ such that $\omega^*(G|\rho) = 1$. We have $\omega^*(G^n|\rho^{\otimes n}) = 1$. Moreover, $SIC(\rho^{\otimes n}) = nSIC(\rho)$. From there, we have $SIC(G^n) \leq nSIC(G)$. We conclude that $SIC(G^n) = nSIC(G)$. \blacksquare

C Proof of Theorems 2 and 3

The organisation and an overview of the proof can be found in Section 5.

C.1 First inequality

We will show this inequality for any input distribution. Let $\rho = \sum_{x,y \in [k]} p_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$. As in Section 3.1, we define $|L_y^A\rangle, |L_x^B\rangle, \sigma^A, \sigma^B$. Let $\rho_y^A = \text{Tr}_{\mathcal{B}} |L_y^A\rangle\langle L_y^A|$ and $\rho_x^B = \text{Tr}_{\mathcal{A}} |L_x^B\rangle\langle L_x^B|$. Intuitively, ρ_y^A (resp. ρ_x^B) corresponds to the input-superposed state that Alice (resp. Bob) has, conditioned on Bob getting y (resp. Alice getting x). We prove the following.

Proposition 14. $SIC(\rho) \geq \frac{1}{4 \ln(2)} (1 - \sum_{y,y'} p_{.y} p_{.y'} F^2(\rho_y^A, \rho_{y'}^A) + 1 - \sum_{x,x'} p_x p_{x'} F^2(\rho_x^B, \rho_{x'}^B))$.

Proof. Let $\xi^A = \text{Tr}_{\mathcal{B}}(\sigma^A)$ and $\xi^B = \text{Tr}_{\mathcal{A}}(\sigma^B)$. This means that $\xi^A = \sum_y p_{.y} \rho_y^A \otimes |y\rangle\langle y|$ and $\xi^B = \sum_x p_x |x\rangle\langle x| \otimes \rho_x^B$. We have $SIC(\rho) = I(XA : Y)_{\xi^A} + I(X : BY)_{\xi^B}$. Using Claim A.2, we get

$$SIC(\rho) \geq \frac{2}{\ln(2)} (1 - F(\xi^A, \xi_{\mathcal{X}^A}^A \otimes \xi_Y^A) + 1 - F(\xi^B, \xi_{\mathcal{X}^B}^B \otimes \xi_{\mathcal{Y}^B}^B)). \quad (2)$$

where $\xi_{\mathcal{X}\mathcal{A}}^A = \sum_y p_{\cdot y} \rho_y^A$ and $\xi_{\mathcal{Y}}^A = \sum_y p_{\cdot y} |y\rangle\langle y|$. Next, using Proposition 13, we have $F(\xi^A, \xi_{\mathcal{X}\mathcal{A}}^A \otimes \xi_{\mathcal{Y}}^A) = \sum_y p_{\cdot y} F(\rho_y^A, \xi_{\mathcal{X}\mathcal{A}}^A)$. From there, we have:

$$\begin{aligned}
1 - F(\xi^A, \xi_{\mathcal{X}\mathcal{A}}^A \otimes \xi_{\mathcal{Y}}^A) &= 1 - \sum_{y \in [k]} p_{\cdot y} F(\rho_y^A, \xi_{\mathcal{X}\mathcal{A}}^A) \\
&= \frac{1}{2} \left(1 - \sum_{y \in [k]} p_{\cdot y} F(\rho_y^A, \xi_{\mathcal{X}\mathcal{A}}^A) + 1 - \sum_{y' \in [k]} p_{\cdot y'} F(\rho_{y'}^A, \xi_{\mathcal{X}\mathcal{A}}^A) \right) \\
&= \frac{1}{2} \sum_{y, y' \in [k]} p_{\cdot y} p_{\cdot y'} [1 - F(\rho_y^A, \xi_{\mathcal{X}\mathcal{A}}^A) + 1 - F(\rho_{y'}^A, \xi_{\mathcal{X}\mathcal{A}}^A)] \\
&\geq \frac{1}{4} \sum_{y, y' \in [k]} p_{\cdot y} p_{\cdot y'} (1 - F(\rho_y^A, \rho_{y'}^A)) && \text{using Proposition 12} \\
&\geq \frac{1}{8} \sum_{y, y' \in [k]} p_{\cdot y} p_{\cdot y'} (1 - F^2(\rho_y^A, \rho_{y'}^A))
\end{aligned}$$

Similarly, we can show that $1 - F(\xi^B, \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{B}\mathcal{Y}}^B) \geq \frac{1}{8} \sum_{x, x' \in [k]} p_x \cdot p_{x'} (1 - F^2(\rho_x^B, \rho_{x'}^B))$. Combining these with Eq. 2, we conclude that

$$SIC(\rho) \geq \frac{1}{4 \ln(2)} \left(1 - \sum_{y, y'} p_{\cdot y} p_{\cdot y'} F^2(\rho_y^A, \rho_{y'}^A) + 1 - \sum_{x, x'} p_x \cdot p_{x'} F^2(\rho_x^B, \rho_{x'}^B) \right).$$

■

C.2 Second inequality

Let $\rho = \frac{1}{k^2} \sum_{x, y \in [k]} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}|_{\mathcal{A}\mathcal{B}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$. As in Section 3.1, we define $|L_y^A\rangle, |L_x^B\rangle, \sigma^A, \sigma^B$. Let $\rho_y^A = \text{Tr}_{\mathcal{B}} |L_y^A\rangle\langle L_y^A|$ and $\rho_x^B = \text{Tr}_{\mathcal{A}} |L_x^B\rangle\langle L_x^B|$. We define:

$$\begin{aligned}
\varepsilon^A &= 1 - \sum_{y, y'} \frac{1}{k^2} F^2(\rho_y^A, \rho_{y'}^A) = 1 - \mathbb{E}_{y, y'} [F^2(\rho_y^A, \rho_{y'}^A)] \\
\varepsilon^B &= 1 - \sum_{x, x'} \frac{1}{k^2} F^2(\rho_x^B, \rho_{x'}^B) = 1 - \mathbb{E}_{x, x'} [F^2(\rho_x^B, \rho_{x'}^B)].
\end{aligned}$$

The expectations will always be taken over the uniform distribution. We first show the following lemma.

Lemma 2. *There exist $i, j \in [k]$ as well as unitaries $\{U_x\}_x$ and $\{V_y\}_y$ acting respectively on \mathcal{A} and \mathcal{B} such that if we define $|\Omega_{xy}\rangle = (U_x \otimes V_y)|\phi_{xy}\rangle$, we have:*

$$\begin{aligned}
\mathbb{E}_{xy} [|\langle \Omega_{xy} | \Omega_{xj} \rangle|^2] &\geq \mathbb{E}_{y, y'} [F^2(\rho_y^A, \rho_{y'}^A)] = 1 - \varepsilon^A \\
\mathbb{E}_{xy} [|\langle \Omega_{xy} | \Omega_{iy} \rangle|^2] &\geq \mathbb{E}_{x, x'} [F^2(\rho_x^B, \rho_{x'}^B)] = 1 - \varepsilon^B.
\end{aligned}$$

Proof. Let $j \in [k]$ that maximizes $\mathbb{E}_{y'} [F^2(\rho_j^A, \rho_{y'}^A)]$. We have

$$\mathbb{E}_{y'} [F^2(\rho_j^A, \rho_{y'}^A)] \geq \mathbb{E}_{y, y'} [F^2(\rho_y^A, \rho_{y'}^A)] \geq 1 - \varepsilon^A. \quad (3)$$

For each y , consider the unitary U_y acting on \mathcal{B} such that $|\langle L_j^A | (I_{\mathcal{X}\mathcal{A}} \otimes U_y) |L_y^A\rangle| = F(\rho_j^A, \rho_y^A)$. Such a unitary exists by Uhlmann's theorem. We also choose $U_j = I_{\mathcal{B}}$. Since $|L_j^A\rangle = \frac{1}{\sqrt{k}} \sum_x |x\rangle |\phi_{xj}\rangle$ and $(I_{\mathcal{X}\mathcal{A}} \otimes U_y)$ acts only on space \mathcal{B} , we can write $(I_{\mathcal{X}\mathcal{A}} \otimes U_y) |L_y^A\rangle = \frac{1}{\sqrt{k}} \sum_x |x\rangle |\xi_{xy}\rangle$ for some $|\xi_{xy}\rangle$. Therefore, we have:

$$F(\rho_j^A, \rho_y^A) = |\langle L_j^A | (I_{\mathcal{X}\mathcal{A}} \otimes U_y) |L_y^A\rangle| = \left| \frac{1}{k} \sum_x \langle \xi_{xy} | \phi_{xj} \rangle \right| = \left| \frac{1}{k} \sum_x \langle \xi_{xy} | \phi_{xj} \rangle \right| \leq \frac{1}{k} \sum_x |\langle \xi_{xy} | \phi_{xj} \rangle|.$$

Since we took $U_j = I_{\mathcal{B}}$, we have $|\xi_{xj}\rangle = |\phi_{xj}\rangle$ for all x . We can hence rewrite for all y

$$F(\rho_j^A, \rho_y^A) \leq \mathbb{E}_x[|\langle \xi_{xy} | \xi_{xj} \rangle|]. \quad (4)$$

We now analyze Bob's side of the state similarly. Let $|M_x^B\rangle = \sum_y \frac{1}{\sqrt{k}} |\xi_{xy}\rangle |y\rangle$. We have $|M_x^B\rangle = (\sum_y I_{\mathcal{A}} \otimes U_y \otimes |y\rangle\langle y|) |L_x^B\rangle$. Let $\nu_x^B = \text{Tr}_{\mathcal{A}} |M_x^B\rangle\langle M_x^B|$. We have $\nu_x^B = (\sum_y U_y^\dagger U_y \otimes |y\rangle\langle y|) \cdot \rho_x^B$. Hence for all x, x' , we have

$$F(\nu_x^B, \nu_{x'}^B) = F(\rho_x^B, \rho_{x'}^B). \quad (5)$$

Let $i \in [k]$ such that $\mathbb{E}_{x'}[F^2(\nu_i^B, \nu_{x'}^B)]$ is maximal. We have

$$\mathbb{E}_{x'}[F^2(\nu_i^B, \nu_{x'}^B)] \geq 1 - \varepsilon^B. \quad (6)$$

For each x , consider the unitary V_x acting on \mathcal{A} such that $|\langle M_i^B | (V_x \otimes I_{\mathcal{B}Y}) | M_x^B \rangle| = F(\nu_i^B, \nu_x^B)$. Such a unitary exists by Uhlmann's theorem. We take $V_i = I_{\mathcal{A}}$. Since $|M_x^B\rangle = \frac{1}{\sqrt{k}} \sum_y |\xi_{xy}\rangle |y\rangle$ and $(V_x \otimes I_{\mathcal{B}Y})$ acts only on space \mathcal{A} , we can write $(V_x \otimes I_{\mathcal{B}Y}) | M_x^B \rangle = \frac{1}{\sqrt{k}} \sum_y |\Omega_{xy}\rangle |y\rangle$ for some $|\Omega_{xy}\rangle$. Therefore, we have:

$$F(\nu_i^B, \nu_x^B) = |\langle M_i^B | (V_x \otimes I_{\mathcal{B}Y}) | M_x^B \rangle| = \left| \frac{1}{k} \sum_y \langle \xi_{iy} | \Omega_{xy} \rangle \right| = \left| \mathbb{E}_y[\langle \xi_{iy} | \Omega_{xy} \rangle] \right| \leq \mathbb{E}_y[|\langle \xi_{iy} | \Omega_{xy} \rangle|].$$

Using $F(\nu_i^B, \nu_i^B) = 1$, we have $|\xi_{iy}\rangle = |\Omega_{iy}\rangle$ for all y . Using Eq. 5, we can hence rewrite for all x :

$$F(\rho_i^B, \rho_x^B) = F(\nu_i^B, \nu_x^B) \leq \mathbb{E}_y[|\langle \Omega_{iy} | \Omega_{xy} \rangle|]. \quad (7)$$

Note finally that for all x , $(V_x \otimes I_{\mathcal{B}})(|\xi_{xy}\rangle) = |\Omega_{xy}\rangle$ hence we have for all x and for all y $\langle \Omega_{xy} | \Omega_{xy'} \rangle = \langle \xi_{xy} | \xi_{xy'} \rangle$. Using Eq. 4, we have

$$F(\rho_j^A, \rho_y^A) = \mathbb{E}_x[|\langle \xi_{xy} | \xi_{xj} \rangle|] = \mathbb{E}_x[|\langle \Omega_{xy} | \Omega_{xj} \rangle|]. \quad (8)$$

Equations 7 and 8 give

$$\begin{aligned} F^2(\rho_j^A, \rho_y^A) &= \mathbb{E}_x[|\langle \Omega_{xy} | \Omega_{xj} \rangle|^2] \leq \mathbb{E}_x[|\langle \Omega_{xy} | \Omega_{xj} \rangle|^2] \\ F^2(\rho_i^B, \rho_x^B) &= \mathbb{E}_y[|\langle \Omega_{xy} | \Omega_{iy} \rangle|^2] \leq \mathbb{E}_x[|\langle \Omega_{xy} | \Omega_{iy} \rangle|^2]. \end{aligned}$$

Combining this with equations 3 and 6, we conclude

$$\begin{aligned} 1 - \varepsilon^A &\leq \mathbb{E}_y[F^2(\rho_j^A, \rho_y^A)] \leq \mathbb{E}_{xy}[|\langle \Omega_{xy} | \Omega_{xj} \rangle|^2] \\ 1 - \varepsilon^B &\leq \mathbb{E}_x[F^2(\rho_i^B, \rho_x^B)] \leq \mathbb{E}_{xy}[|\langle \Omega_{xy} | \Omega_{iy} \rangle|^2]. \end{aligned}$$

■

We can now prove the main proposition of this section.

Proposition 15. *For any state $\rho = \frac{1}{k^2} \sum_{x,y \in [k]} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|$, there exist unitaries $\{U_x\}_x$ and $\{V_y\}_y$ such that*

$$\varepsilon^A + \varepsilon^B \geq \frac{1}{8} \left(1 - \max_{|\Omega\rangle} \sum_{x,y \in [k]} \frac{1}{k^2} |\langle \Omega | U_x \otimes V_y | \phi_{xy} \rangle|^2 \right),$$

where $\varepsilon^A = 1 - \sum_{y,y'} \frac{1}{k^2} F^2(\rho_y^A, \rho_{y'}^A)$ and $\varepsilon^B = 1 - \sum_{x,x'} \frac{1}{k^2} F^2(\rho_x^B, \rho_{x'}^B)$.

Proof. Fix $\rho = \frac{1}{k^2} \sum_{x,y \in [k]} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$. Using Lemma 2, let $\{U_x\}_x, \{V_y\}_y, i, j$ such that

$$\begin{aligned} \mathbb{E}_{xy} [|\langle\Omega_{xy}|\Omega_{xj}\rangle|^2] &\geq 1 - \varepsilon^A \\ \mathbb{E}_{xy} [|\langle\Omega_{xy}|\Omega_{iy}\rangle|^2] &\geq 1 - \varepsilon^B, \end{aligned}$$

with $|\Omega_{xy}\rangle = U_x \otimes V_y |\phi_{xy}\rangle$. Using Proposition 11, we have

$$\begin{aligned} \mathbb{E}_{x,y,y'} [|\langle\Omega_{xy}|\Omega_{xy'}\rangle|] &\geq \mathbb{E}_{x,y,y'} [|\langle\Omega_{xy}|\Omega_{xj}\rangle|^2 + |\langle\Omega_{xj}|\Omega_{xy'}\rangle|^2] - 1 \\ &\geq 1 - \varepsilon^A + 1 - \varepsilon^A - 1 = 1 - 2\varepsilon^A. \end{aligned}$$

It follows that

$$\mathbb{E}_{x,y,y'} [|\langle\Omega_{xy}|\Omega_{xy'}\rangle|^2] \geq \mathbb{E}_{x,y,y'} [|\langle\Omega_{xy}|\Omega_{xy'}\rangle|]^2 \geq (1 - 2\varepsilon^A)^2 \geq 1 - 4\varepsilon^A.$$

Similarly, we get $\mathbb{E}_{x,x',y} [|\langle\Omega_{xy}|\Omega_{x'y}\rangle|^2] \geq 1 - 4\varepsilon^B$. Using Proposition 11 again, we have

$$\begin{aligned} \mathbb{E}_{x,x',y,y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|] &\geq \mathbb{E}_{x,x',y,y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|^2 + |\langle\Omega_{x'y}|\Omega_{x'y'}\rangle|^2] - 1 \\ &\geq 1 - 4\varepsilon^A + 1 - 4\varepsilon^B - 1 = 1 - 4(\varepsilon^A + \varepsilon^B). \end{aligned}$$

This gives us

$$\mathbb{E}_{x,x',y,y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|^2] \geq \mathbb{E}_{x,x',y,y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|]^2 \geq (1 - 4\varepsilon^A - 4\varepsilon^B)^2 \geq 1 - 8\varepsilon^A - 8\varepsilon^B.$$

Using

$$\mathbb{E}_{x,y,x',y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|^2] \leq \max_{x',y'} \mathbb{E}_{x,y} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|^2] \leq \max_{|\Omega\rangle} \mathbb{E}_{x,y} [|\langle\Omega_{xy}|\Omega\rangle|^2],$$

we have

$$\max_{|\Omega\rangle} \mathbb{E}_{x,y} [|\langle\Omega|\Omega_{xy}\rangle|^2] \geq \mathbb{E}_{x,x',y,y'} [|\langle\Omega_{xy}|\Omega_{x'y'}\rangle|^2] \geq 1 - 8\varepsilon^A - 8\varepsilon^B,$$

hence

$$\varepsilon^A + \varepsilon^B \geq \frac{1}{8} (1 - \max_{|\Omega\rangle} \mathbb{E}_{x,y} [|\langle\Omega|\Omega_{xy}\rangle|^2]) = \frac{1}{8} (1 - \max_{|\Omega\rangle} \mathbb{E}_{x,y} [|\langle\Omega|U_x \otimes V_y|\phi_{xy}\rangle|^2]).$$

■

C.3 Last inequality

Proposition 16. Consider a game $G = (I, O, V, p)$ and a state

$$\rho = \sum_{x,y \in I} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$$

such that $\omega^*(G|\rho) = 1$. We have that $\max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle\Omega|\phi_{xy}\rangle|^2 \leq \omega^*(G)$.

Proof. Consider strategies $\{A_a^x\}_{x \in I, a \in O}$ and $\{B_b^y\}_{y \in I, b \in O}$ such that

$$\sum_{x,y,a,b} p_{xy} V(a, b|x, y) \langle\phi_{xy}|A_a^x \otimes B_b^y|\phi_{xy}\rangle = 1.$$

Let $|\Omega_0\rangle$ that maximizes $\sum_{x,y \in I} p_{xy} |\langle \Omega_0 | \phi_{xy} \rangle|^2$. For any x, y , since $\sum_{ab} V(a, b|x, y) \langle \phi_{xy} | A_a^x \otimes B_b^y | \phi_{xy} \rangle = 1$, we have:

$$\sum_{a,b} V(a, b|x, y) \langle \Omega_0 | A_a^x \otimes B_b^y | \Omega_0 \rangle \geq |\langle \Omega_0 | \phi_{xy} \rangle|^2.$$

From there, we have:

$$\begin{aligned} \omega^*(G) &\geq \sum_{xyab} p_{xy} V(a, b|x, y) \langle \Omega_0 | A_a^x \otimes B_b^y | \Omega_0 \rangle \\ &\geq \sum_{xy} p_{xy} |\langle \Omega_0 | \phi_{xy} \rangle|^2 = \max_{|\Omega\rangle} \sum_{xy} p_{xy} |\langle \Omega | \phi_{xy} \rangle|^2. \end{aligned}$$

■

This proposition has a useful corollary:

Corollary 2. Consider a game $G = (I, O, V, p)$ and a state

$$\rho = \sum_{x,y \in I} p_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$$

such that $\omega^*(G|\rho) = 1$. We have

$$\max_{|\Omega\rangle, \{U_x\}_x, \{V_y\}_y} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 \leq \omega^*(G),$$

for unitaries $\{U_x\}_x$ and $\{V_y\}_y$ acting respectively on \mathcal{A} and \mathcal{B} .

Proof. Let $\{U_x\}_x, \{V_y\}_y$ that maximize $\max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2$. Let $|\psi_{xy}\rangle = U_x \otimes V_y | \phi_{xy} \rangle$. Let $\eta = \sum_{xy} p_{xy} |x\rangle\langle x| \otimes |\psi_{xy}\rangle\langle \psi_{xy}| \otimes |y\rangle\langle y|$. Since Alice and Bob can go from η to ρ by applying respectively U_x^\dagger and V_y^\dagger , we conclude that $\omega^*(G|\eta) = \omega^*(G|\rho) = 1$. Using Proposition 16, we have $\max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 = \max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle \Omega | \psi_{xy} \rangle|^2 \leq \omega^*(G)$. ■

We now prove a similar statement in the case $\omega^*(G|\rho) < 1$.

Proposition 17. Consider a game $G = (I, O, V, p)$ and a state

$$\rho = \sum_{x,y \in I} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|.$$

If $\omega^*(G|\rho) \geq 1 - \gamma$ and $\max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle \Omega | \phi_{xy} \rangle|^2 \geq 1 - \gamma'$, then

$$\omega^*(G) \geq 1 - 2(\gamma + \gamma').$$

Proof. Consider strategies $\{A_a^x\}_{x \in I, a \in O}$ and $\{B_b^y\}_{y \in I, b \in O}$ such that

$$\sum_{x,y,a,b} p_{xy} V(a, b|x, y) \langle \phi_{xy} | A_a^x \otimes B_b^y | \phi_{xy} \rangle = 1 - \gamma.$$

Let $M^{xy} = \sum_{a,b} V(a, b|x, y) A_a^x \otimes B_b^y$ and let $|C_{xy}\rangle = \frac{M^{xy} | \phi_{xy} \rangle}{\|M^{xy} | \phi_{xy} \rangle\|}$. We have $\text{tr}(M^{xy} | \phi_{xy} \rangle \langle \phi_{xy} |) = |\langle C_{xy} | \phi_{xy} \rangle|^2$. Let $q_{xy} = |\langle C_{xy} | \phi_{xy} \rangle|^2$. This gives us immediately

$$\sum_{x,y} p_{xy} q_{xy} = 1 - \gamma.$$

Let $|\Omega\rangle$ such that $\sum_{x,y \in I} p_{xy} |\langle \Omega | \phi_{xy} \rangle|^2 \geq 1 - \gamma'$. Also, let $r_{xy} = |\langle \Omega | \phi_{xy} \rangle|^2$ and $s_{xy} = |\langle \Omega | C_{xy} \rangle|^2$. We have that

$$\sum_{xy} p_{xy} r_{xy} \geq 1 - \gamma',$$

as well as

$$\omega^*(G) \geq \sum_{xy} p_{xy} \text{tr}(M^{xy} |\Omega\rangle \langle \Omega|) \geq \sum_{xy} p_{xy} |\langle \Omega | C_{xy} \rangle|^2 = \sum_{xy} p_{xy} s_{xy}.$$

Using Proposition 11, we have that for all x, y $s_{xy} \geq (q_{xy} + r_{xy} - 1)^2$. Let $m_{xy} = 1 - q_{xy} + 1 - r_{xy}$. We have by definition that $\sum_{xy} p_{xy} m_{xy} \leq \gamma + \gamma'$. Moreover, we have:

$$\begin{aligned} \sum_{xy} p_{xy} s_{xy} &\geq \sum_{xy} p_{xy} (q_{xy} + r_{xy} - 1)^2 \\ &= \sum_{xy} p_{xy} (1 - m_{xy})^2 \\ &\geq \sum_{xy} p_{xy} (1 - 2m_{xy}) \geq 1 - 2(\gamma + \gamma'). \end{aligned}$$

We conclude that $\omega^*(G) \geq \sum_{xy} p_{xy} s_{xy} \geq 1 - 2(\gamma + \gamma')$. ■

We derive two corollaries from this proposition.

Corollary 3. *Consider a game $G = (I, O, V, p)$ and a state*

$$\rho = \sum_{x,y \in I} p_{xy} |x\rangle \langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle \langle \phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle \langle y|_{\mathcal{Y}}.$$

If $\omega^*(G|\rho) \geq 1 - \gamma$ and

$$\max_{|\Omega\rangle, \{U_x\}, \{V_y\}} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 \geq 1 - \gamma',$$

for unitaries $\{U_x\}_x$ and $\{V_y\}_y$ acting respectively on \mathcal{A} and \mathcal{B} , then

$$\omega^*(G) \geq 1 - 2(\gamma + \gamma').$$

Proof. Let $\{U_x\}, \{V_y\}$ such that $\max_{|\Omega\rangle} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 = 1 - \gamma'$. Let $|\psi_{xy}\rangle = U_x \otimes V_y | \phi_{xy} \rangle$. Let $\eta = \sum_{xy} p_{xy} |x\rangle \langle x| \otimes |\psi_{xy}\rangle \langle \psi_{xy}| \otimes |y\rangle \langle y|$. Since Alice and Bob can go from η to ρ by applying respectively U_x^\dagger and V_y^\dagger , we conclude that $\omega^*(G|\eta) = \omega^*(G|\rho) \geq 1 - \gamma$. Using Proposition 17, we conclude that $\omega^*(G) \geq 1 - 2(\gamma + \gamma')$. ■

Taking a counterpositive of the above Corollary we get the following

Corollary 4. *Consider a game $G = (I, O, V, p)$ and a state*

$$\rho = \sum_{x,y \in I} p_{xy} |x\rangle \langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle \langle \phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle \langle y|_{\mathcal{Y}}.$$

If $\omega^*(G|\rho) \geq 1 - \gamma$ and $\omega^*(G) \leq 1 - \varepsilon$, then

$$\max_{|\Omega\rangle, \{U_x\}, \{V_y\}} \sum_{x,y \in I} p_{xy} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 \leq 1 - (\varepsilon/2 - \gamma),$$

for unitaries $\{U_x\}_x$ and $\{V_y\}_y$ acting respectively on \mathcal{A} and \mathcal{B} .

C.4 Putting it together

We can now show our theorems

Theorem 2. *For any game G with a uniform input distribution, we have $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$.*

Proof. Consider a game $G = (I = [k], O, V, \text{Unif.})$ and $\rho = \frac{1}{k^2} \sum_{x,y} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G|\rho) = 1$. Using Proposition 14 and Proposition 15, take $\{U_x\}_x$ and $\{V_y\}_y$ such that

$$SIC(\rho) \geq \frac{1}{32 \ln(2)} (1 - \max_{|\Omega\rangle} \sum_{xy} \frac{1}{k^2} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2).$$

Using Corollary 2, we have

$$\max_{|\Omega\rangle} \sum_{xy \in [k]} \frac{1}{k^2} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 \leq \omega^*(G).$$

From there, we have $SIC(\rho) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$. Since this holds for any ρ satisfying $\omega^*(G|\rho) = 1$, we can conclude that $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$. \blacksquare

We now proceed to prove a similar result for the case where $\omega^*(G|\rho) < 1$.

Proposition 18. *For any game G with a uniform input distribution, and any state ρ such that $\omega^*(G|\rho) = 1 - \gamma$, we have $SIC(\rho) \geq \frac{1}{32 \ln(2)} (\frac{\varepsilon}{2} - \gamma)$ where $\varepsilon = 1 - \omega^*(G)$.*

Proof. The proof will be similar to the previous one. Consider a game $G = (I = [k], O, V, \text{Unif.})$ and $\rho = \frac{1}{k^2} \sum_{x,y} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G|\rho) = 1 - \gamma$. Using Proposition 14 and Proposition 15, take $\{U_x\}$ and $\{V_y\}$ such that

$$SIC(\rho) \geq \frac{1}{32 \ln(2)} (1 - \max_{|\Omega\rangle} \sum_{xy} \frac{1}{k^2} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2).$$

Using Corollary 4, we have that

$$1 - \max_{|\Omega\rangle} \sum_{xy} \frac{1}{k^2} |\langle \Omega | (U_x \otimes V_y) | \phi_{xy} \rangle|^2 \geq \frac{\varepsilon}{2} - \gamma,$$

where $\varepsilon = 1 - \omega^*(G)$. From there, we have $SIC(\rho) \geq \frac{1}{32 \ln(2)} (\frac{\varepsilon}{2} - \gamma)$. Since this holds for any ρ satisfying $\omega^*(G|\rho) = 1 - \gamma$, we can conclude that $SIC(G) \geq \frac{1-\omega^*(G)}{32 \ln(2)}$. \blacksquare

Our last extension is the following theorem, which is the one we will use for parallel repetition.

Theorem 3. *There exists a constant $c_0 > 0$ such that for any game $G = (I = [k], O, V, \text{Unif.})$ satisfying $\omega^*(G) = 1 - \varepsilon$, for any game $G' = (I = [k], O, V, p)$ satisfying $\frac{1}{2} \sum_{x,y} |p_{xy} - \frac{1}{k^2}| \leq c_0 \varepsilon$ and any state $\rho = \sum_{xy} p_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G'|\rho) \geq 1 - \frac{\varepsilon}{4}$, we have that $SIC(\rho) = \Omega(\varepsilon)$.*

Proof. Fix any G, G', ρ . We also fix a small constant c_0 that will be specified later in the proof. Let $\rho(U) = \frac{1}{k^2} \sum_{xy} |x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$.

Let σ^A, σ^B the superposed states of ρ . As in Proposition 14, we define $\xi^B = \text{Tr}_{\mathcal{A}}(\sigma^B)$. This means that $\xi^B = \sum_x p_x |x\rangle\langle x| \otimes \rho_x^B$ for some ρ_x^B . Let also $\xi_{\mathcal{X}}^B = \text{Tr}_{BY}(\xi^B)$ and $\xi_{\mathcal{B}Y}^B = \text{Tr}_X(\xi^B)$.

Similarly, let $\sigma^A(U), \sigma^B(U)$ the superposed states of $\rho(U)$ and let $\xi^B(U) = \text{Tr}_{\mathcal{A}}(\sigma^B(U))$. This means that $\xi^B(U) = \frac{1}{k} \sum_x |x\rangle\langle x| \otimes \rho_x^B(U)$ for some $\rho_x^B(U)$. Let also $\xi_{\mathcal{X}}^B(U) = \text{Tr}_{BY}(\xi^B(U))$ and $\xi_{\mathcal{B}Y}^B(U) = \text{Tr}_X(\xi^B(U))$.

We want to upper bound $SIC(\rho) = I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B}$. Let $\delta = \frac{1}{2} \sum_{x,y} |p_{xy} - \frac{1}{k^2}| \leq c_0 \varepsilon$. We proceed as in Proposition 14. Using Claim A.2, we have $I(X : BY)_{\sigma^B} \geq \frac{2}{\ln(2)} (1 - F(\xi^B, \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{B}Y}^B))$. Notice

that $\Delta(\sigma^B, \sigma^B(U)) \leq \delta$ which implies $\Delta(\xi^B(U), \xi^B) \leq \delta$; $\Delta(\xi_{\mathcal{X}}^B(U), \xi_{\mathcal{X}}^B) \leq \delta$ and $\Delta(\xi_{\mathcal{BY}}^B(U), \xi_{\mathcal{BY}}^B) \leq \delta$. The two last inequalities give us $\Delta(\xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U), \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B) \leq 2\delta$. From there, by using Claim A.2 and Propositions 10 and 12, we have:

$$\begin{aligned} I(X : BY)_{\sigma^B} = I(X : BY)_{\xi^B} &\geq \frac{2}{\ln(2)}(1 - F(\xi^B, \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B)) \\ &\geq \frac{2}{\ln(2)}\left(\frac{1}{2}(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B)) - (1 - F(\xi^B, \xi^B(U)))\right) \\ &\geq \frac{2}{\ln(2)}\left(\frac{1}{2}(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B)) - \delta\right). \end{aligned}$$

Then, we have:

$$\begin{aligned} 1 - F(\xi^B(U), \xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B) &\geq \frac{1}{2}(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U))) - (1 - F(\xi_{\mathcal{X}}^B \otimes \xi_{\mathcal{BY}}^B, \xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U))) \\ &\geq \frac{1}{2}(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U))) - 2\delta, \end{aligned}$$

which gives us

$$I(X : BY)_{\sigma^B} \geq \frac{2}{\ln(2)}\left(\frac{1}{4}(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U))) - 2\delta\right).$$

Let $\varepsilon^B = 1 - \frac{1}{k^2} \sum_{x, x'} F^2(\rho_x^B(U), \rho_{x'}^B(U))$. As in Proposition 14, we can show that

$$(1 - F(\xi^B(U), \xi_{\mathcal{X}}^B(U) \otimes \xi_{\mathcal{BY}}^B(U))) \geq \frac{\varepsilon^B}{8},$$

hence $I(X : BY)_{\sigma^B} \geq \frac{2}{\ln(2)}\left(\frac{\varepsilon^B}{32} - 2\delta\right)$. Similarly, if we define $\varepsilon^A = 1 - \frac{1}{k^2} \sum_{y, y'} F^2(\rho_y^A(U), \rho_{y'}^A(U))$ we can show that $I(Y : XA)_{\sigma^A} \geq \frac{2}{\ln(2)}\left(\frac{\varepsilon^A}{32} - 2\delta\right)$, which gives

$$SIC(\rho) \geq \frac{2}{\ln(2)} \left(\frac{\varepsilon^A + \varepsilon^B}{32} - 4\delta \right).$$

Using Proposition 15, we have:

$$SIC(\rho) \geq \frac{2}{\ln(2)} \left(\frac{1}{256} \max_{|\Omega\rangle, \{U_x\}, \{V_y\}} \frac{1}{k^2} \sum_{x, y} |\langle \Omega | \phi_{xy} \rangle|^2 - 4\delta \right).$$

We have $\omega(G) = 1 - \varepsilon$ and $\omega(G|\rho(U)) \geq 1 - \varepsilon/4 - \delta$. Using Corollary 4, we have:

$$\max_{|\Omega\rangle, \{U_x\}, \{V_y\}} \frac{1}{k^2} \sum_{x, y} |\langle \Omega | \phi_{xy} \rangle|^2 \leq 1 - (\varepsilon/2 - \varepsilon/4 - \delta) = 1 - \varepsilon/4 + \delta.$$

From there, we conclude:

$$SIC(\rho) \geq \frac{2}{\ln(2)} \left(\frac{1}{256} (\varepsilon/4 - \delta) - 4\delta \right).$$

By taking $c_0 = \frac{1}{8092}$, which implies $\delta \leq \frac{\varepsilon}{8092}$, we obtain $SIC(\rho) = \Omega(\varepsilon)$. ■

D Proof of Theorem 4

We first present the actual construction of ξ and then show it has the desired properties required for Theorem 4.

- Alice and Bob perform protocol P where the inputs are classical but the randomness, the message and the outputs are left in a quantum superposition. To maintain the “classicality” of the message sent by Alice, we ask Alice to have a quantum register which acts as a copy of the message.
- We ask Bob to determine whether he aborts or not. The state ξ will be the state Alice and Bob share conditioned on Bob not aborting.
- Using Proposition 3, we prove that ξ has the desired properties

Procedure for constructing ξ

1. Alice and Bob pick random inputs $x, y \in_R I^n = [k^n]$. They also share a state $\sum_r \gamma_r |r\rangle_{\mathcal{R}_A} \otimes |\phi\rangle_{AB} \otimes |r\rangle_{\mathcal{R}_B}$ where $|\phi\rangle$ is the same as in protocol P and r corresponds to the shared randomness in protocol P .
2. Alice and Bob perform a strategy that allows them to win G^n with probability $2^{-(t+1)}$ but keep their outputs in a coherent superposition instead of measuring. They keep these outputs in registers \mathcal{O}_A and \mathcal{O}_B . They hence share the state $\rho_1 = \sum_{x,y} \frac{1}{k^{2n}} |x\rangle\langle x|_{\mathcal{X}} \otimes |\Omega_{xy}^1\rangle\langle\Omega_{xy}^1| \otimes |y\rangle\langle y|_{\mathcal{Y}}$, with

$$|\Omega_{xy}^1\rangle = \sum_{a,b,r} \gamma_{xyrab} |a\rangle_{\mathcal{O}_A} |r\rangle_{\mathcal{R}_A} |\phi_{ab}^{xy}\rangle_{AB} |r\rangle_{\mathcal{R}_B} |b\rangle_{\mathcal{O}_B},$$

for some states $|\phi_{ab}^{xy}\rangle$.

3. Alice sends the message M that depends on x, a, r corresponding to step 3 of protocol P to Bob and keeps a copy of M to herself in superposition, which means that they share a state $\rho_2 = \sum_{x,y} \frac{1}{k^{2n}} |x\rangle\langle x| \otimes |\Omega_{xy}^2\rangle\langle\Omega_{xy}^2| \otimes |y\rangle\langle y|$, with

$$|\Omega_{xy}^2\rangle = \sum_{a,b,r,M} \gamma_{xyrabM} |a\rangle_{\mathcal{O}_A} |M\rangle_{\mathcal{M}_A} |r\rangle_{\mathcal{R}_A} |\phi_{ab}^{xy}\rangle_{AB} |r\rangle_{\mathcal{R}_B} |M\rangle_{\mathcal{M}_B} |b\rangle_{\mathcal{O}_B}.$$

4. Bob copies in a new register \mathcal{Z} whether he aborts or not. This means that they share a state $\rho_3 = \sum_{x,y} \frac{1}{k^{2n}} |x\rangle\langle x| \otimes |\Omega_{xy}^3\rangle\langle\Omega_{xy}^3| \otimes |y\rangle\langle y|$, with

$$\begin{aligned} |\Omega_{xy}^3\rangle &= \sum_{a,b,r,M} \gamma_{xyrabM} |a\rangle |M\rangle |r\rangle |\phi_{ab}^{xy}\rangle |r\rangle |M\rangle |b\rangle |NA\rangle_{\mathcal{Z}} + \\ &\sum_{a,r,M} \gamma_{xyra,AB,M} |a\rangle |M\rangle |r\rangle |\phi_{a,AB}^{xy}\rangle |r\rangle |m\rangle |AB\rangle |AB\rangle_{\mathcal{Z}}. \end{aligned}$$

We can write $|\Omega_{xy}^3\rangle = \sqrt{\gamma'_{xy}} |Y_{xy}^{NA}\rangle |NA\rangle + \sqrt{1 - \gamma'_{xy}} |Y_{xy}^{AB}\rangle |AB\rangle$, for some $\{\gamma'_{xy}\}_{xy}$ and states $\{|Y_{xy}^{NA}\rangle\}_{xy}$ and $\{|Y_{xy}^{AB}\rangle\}_{xy}$.

Let $\rho_{-Z} = \text{Tr}_Z(\rho_3)$. Since the probability of Bob not aborting is p , we can write

$$\rho_{-Z} = p \cdot \rho_{NA} + (1 - p) \cdot \rho_{AB},$$

for some state ρ_{AB} . ρ_{NA} is of the form $\sum_{xy} q_{xy} |x\rangle\langle x| \otimes |Y_{xy}^{NA}\rangle\langle Y_{xy}^{NA}| \otimes |y\rangle\langle y|$. We choose $\xi = \rho_{NA}$.

In the above protocol, ρ_2 corresponds to the state Alice and Bob share after Step 3 of protocol P except that the randomness, message and outputs are kept in a quantum superposition in the way described above.

Similarly, $\xi = \rho_{NA}$ corresponds to the state at the end of protocol P , conditioned on Bob not aborting. Again, the randomness, message and outputs are kept in a quantum superposition in the way described above.

D.1 Showing the desired properties of $\xi = \rho_{NA}$

We now show that $\xi = \rho_{NA}$ has the desired properties of Theorem 4.

1) $H(XY)_\xi \geq 2n \log(k) - t - 1$.

Proof. $H(XY)_{\rho_{-Z}} = 2n \log(k)$. Since $\text{Dim}(XY) = k^{2n}$, this means that $H_{\min}(XY)_{\rho_{-Z}} = 2n \log(k)$. We have $p\rho_{NA} \leq \rho_{-Z}$ hence $H_{\min}(XY)_{\rho_{NA}} - \log(p) \geq H_{\min}(XY)_{\rho_{-Z}} = 2n \log(k)$. This gives us $H_{\min}(XY)_{\rho_{NA}} \geq 2n \log(k) + \log(p)$. Since $p \geq 2^{-(t+1)}$, we conclude that $H_{\min}(XY)_{\rho_{NA}} \geq 2n \log(k) - t - 1$, hence $H(XY)_{\rho_{NA}} \geq 2n \log(k) - t - 1$. \blacksquare

2) $\omega^*(G'|\xi) \geq 1 - \varepsilon/32$ where $G_{1-\varepsilon/32}^n = (I', O', V', \text{Unif.})$ and $G' = (I', O', V', q)$.

Proof. This holds by construction of ξ . Indeed, ξ is the superposed version of the state Alice and Bob share after protocol P conditioned on Bob not aborting. We know that in this case, $\Pr[\text{Alice and Bob win}] \geq (1 - \varepsilon/32)n$ games | Bob does not abort $\geq (1 - \varepsilon/32)$. From there, we have $\omega^*(G'|\xi) \geq (1 - \varepsilon/32)$ \blacksquare

3) $SIC(\xi) \leq \frac{32 \log(|I||O|)}{\varepsilon}((t+1) + |\log(\varepsilon)| + 5) + 2t + 2$.

Proof. We upper bound the superposed information cost of the state $\xi = \rho_{NA}$. We are interested in the superposed states $\sigma_{NA}^A, \sigma_{NA}^B$ of ξ as defined in Section 3.1. Recall that $\rho_{NA} = \sum_{xy} q_{xy} |x\rangle\langle x| \otimes |Y_{xy}^{NA}\rangle\langle Y_{xy}^{NA}| \otimes |y\rangle\langle y|$ for some q_{xy} . Let $\mathcal{A}' = \mathcal{O}_A \otimes \mathcal{M}_A \otimes \mathcal{R}_A \otimes A$ and $\mathcal{B}' = \mathcal{O}_B \otimes \mathcal{R}_B \otimes B$. We have $SIC(\xi) = I(X : M_B B' Y)_{\sigma_{NA}^B} + I(Y : X A')_{\sigma_{NA}^A}$. Let also σ_2^A, σ_2^B the superposed states of ρ_2 .

To proceed with the proof, we need the following lemmas and proposition.

Lemma 3. $I(X : M_B B' Y)_{\sigma_{NA}^B} \leq n \log(k) - H_{\min}(X | M_B B' Y)_{\sigma_2^B} + t + 1$

Proof. We have:

$$\begin{aligned} I(X : M_B B' Y)_{\sigma_{NA}^B} &= H(X)_{\sigma_{NA}^B} - H(X | M_B B' Y)_{\sigma_{NA}^B} \leq n \log(k) - H(X | M_B B' Y)_{\sigma_{NA}^B} \\ &\leq n \log(k) - H_{\min}(X | M_B B' Y)_{\sigma_{NA}^B}. \end{aligned}$$

By definition, we have $H_{\min}(X | M_B B' Y)_{\sigma_2^B} = -\log(\Pr[\text{Bob guesses } x \mid \text{Alice and Bob share } \sigma_2^B])$. When Alice and Bob share σ_2^B , if Bob tries to determine whether he aborts or not, the state he shares with Alice conditioned on not aborting is σ_{NA}^B . Since Bob doesn't abort with probability greater than 2^{-t+1} , we have

$$\Pr[\text{Bob guesses } x \mid \text{Alice and Bob share } \sigma_2^B] \geq 2^{-(t+1)} \Pr[\text{Bob guesses } x \mid \text{Alice and Bob share } \sigma_{NA}^B]$$

From there, we have

$$\begin{aligned} H_{\min}(X | M_B B' Y)_{\sigma_2^B} &= -\log(\Pr[\text{Bob guesses } x \mid \text{Alice and Bob share } \sigma_2^B]) \\ &\leq -\log(\Pr[\text{Bob guesses } x \mid \text{Alice and Bob share } \sigma_{NA}^B]) + t + 1 \\ &= H_{\min}(X | M_B B' Y)_{\sigma_{NA}^B} + t + 1. \end{aligned}$$

We conclude that $I(X : M_B B' Y)_{\sigma_{NA}^B} \leq n \log(k) - H_{\min}(X | M_B B' Y)_{\sigma_{NA}^B} \leq n \log(k) - H_{\min}(X | M_B B' Y)_{\sigma_2^B} + t + 1$. \blacksquare

We now prove the following:

Lemma 4. $H_{min}(X|M_B B'Y)_{\sigma_2^B} \leq n \log(k) - m.$

Proof. Let $\sigma'_{X M_B B'Y} = \text{Tr}_{\mathcal{A}'}(\sigma_2^B)$, $\sigma'_{X B'Y} = \text{Tr}_{\mathcal{A}' \mathcal{M}_B}(\sigma_2^B)$, and $\sigma'_{B'Y} = \text{Tr}_{\mathcal{X} \mathcal{A}' \mathcal{M}_B}(\sigma_2^B)$. We have $H_{min}(X|M_B B'Y)_{\sigma_2^B} = H_{min}(X|M_B B'Y)_{\sigma'_{X M_B B'Y}}$. First notice that

$$\sigma'_{X B'Y} = \frac{I_{\mathcal{X}}}{k^n} \otimes \sigma'_{B'Y}. \quad (9)$$

Moreover, we can write $\sigma'_{X M_B B'Y} = \sum_{M \in [m]} r_M |M\rangle\langle M| \otimes \eta(M)_{\mathcal{X} B'Y}$ for some states $\{\eta(M)\}_M$ and $\sum_M r_M = 1$. Notice that $\sigma'_{X B'Y} = \sum_M r_M \eta(M)$. We have:

$$\sigma'_{X M_B B'Y} = \sum_{M \in [m]} r_M |M\rangle\langle M| \otimes \eta(M)_{\mathcal{X} B'Y} \leq I_{\mathcal{M}_B} \otimes \sigma'_{X B'Y}. \quad (10)$$

Using Equations 9 and 10, we have:

$$\begin{aligned} \sigma'_{X M_B B'Y} &\leq I_{\mathcal{M}_B} \otimes \sigma'_{X B'Y} \leq \frac{1}{k^n} I_{\mathcal{X}} \otimes I_{\mathcal{M}_B} \otimes \sigma'_{B'Y} \\ &\leq \frac{2^m}{k^n} I_{\mathcal{X}} \otimes \left(\frac{I_{\mathcal{M}_B}}{2^{s_m}} \otimes \sigma'_{B'Y} \right). \end{aligned}$$

By definition of H_{min} (Section A.2), this gives $H_{min}(X|M_B B'Y)_{\sigma'_{X M_B B'Y}} \leq n \log(k) - m.$ ■

We now put everything together and prove the following.

Proposition 19. $I(X : M_B B'Y)_{\sigma_{N_A}^B} \leq m + t + 1.$

Proof. Combining Lemma 3 and Lemma 4, we have

$$I(X : M_B B'Y)_{\sigma_{N_A}^B} \leq n \log(k) - H_{min}(X|M_B B'Y)_{\sigma_2^B} + t + 1 \leq m + t + 1. \quad \blacksquare$$

Now let's analyze $\sigma_{N_A}^A$. Here, Alice does not receive any message from Bob hence $I(Y : X A')_{\sigma_2^A} = 0$. As in Lemma 3, we can show that $I(Y : X A')_{\sigma_{N_A}^A} \leq I(Y : X A')_{\sigma_2^A} + t + 1 = t + 1.$

Putting this all together, we have:

$$SIC(\xi) = I(Y : X A')_{\sigma_{N_A}^A} + I(X : M_B B'Y)_{\sigma_{N_A}^B} \leq m + 2t + 2.$$

To conclude the proof, recall from Section 6 that $m = \frac{32 \log(|I||O|)}{\varepsilon} ((t + 1) + |\log(\varepsilon)| + 5)$. From there, we conclude that

$$SIC(\xi) \leq \frac{32 \log(|I||O|)}{\varepsilon} ((t + 1) + |\log(\varepsilon)| + 5) + 2t + 2,$$

which concludes the proof. ■

We showed that ξ satisfies all the desired properties of Theorem 4.

E Proof of Theorem 5

We now give a lower bound complementary to the upper bound described in Theorem 4.

Theorem 5. Consider a game $G = (I = [k], O, V, \text{Unif.})$ such that $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$ with $t = o(n\varepsilon)$. Let also $G_{1-\varepsilon/32}^n = (I^n = [k^n], O^n, V', \text{Unif.})$ as defined in Section 2. For any game $G' = (I' = [k^n], O', V', p)$ and any state $\rho = \sum_{x,y \in [k^n]} p_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|_{\mathcal{Y}}$, satisfying

1. $H(XY)_\rho \geq 2n \log(k) - t$
2. $\omega^*(G'|\rho) \geq 1 - \varepsilon/32$

we have $\text{SIC}(\rho) \geq \Omega(n\varepsilon)$.

Proof. Fix any state ρ of the form

$$\rho = \sum_{x,y \in [k^n]} p_{xy} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle \phi_{xy}| \otimes |y\rangle\langle y|_{\mathcal{Y}},$$

satisfying properties 1. and 2. above. Property 2 tells us that there is strategy that allows Alice and Bob to win G' with high probability. We make them perform this strategy.

We first show that there is a large number of indices i such that Alice and Bob win game i with high probability with this strategy and $H(\mathcal{X}_i, \mathcal{Y}_i)_\rho$ is large.

Lemma 5. Let $p_i = \Pr[\text{Alice and Bob win game } i \text{ using } \rho]$. Let $K = \{i : p_i \geq 1 - \varepsilon/4\}$. Let $L = \{i : H(X_i, Y_i)_\rho \geq 2 \log(k) - \frac{4t}{n}\}$. We have

$$|K| \geq 3n/4, \quad |L| \geq 3n/4, \quad \text{which implies } |K \cap L| \geq n/2.$$

Proof. $\frac{1}{n} \sum_{i \in [n]} p_i$ corresponds to the average number of games won by Alice and Bob. They win G' if they win at least $(1 - \varepsilon/32)$ games. Since they can win G' with probability at least $1 - \varepsilon/32$, we know that $\frac{1}{n} \sum_{i \in [n]} p_i \geq (1 - \varepsilon/32)(1 - \varepsilon/32) \geq 1 - \varepsilon/16$. We have:

$$\sum_i p_i = \sum_{i \in K} p_i + \sum_{i \notin K} p_i \leq |K| + (n - |K|)(1 - \varepsilon/4) = n - (n - |K|)\varepsilon/4,$$

since $\sum_i p_i \geq n(1 - \varepsilon/16)$, we have $n - (n - |K|)\varepsilon/4 \geq n(1 - \varepsilon/16)$ and $|K| \geq \frac{3n}{4}$.

Similarly, we have:

$$\begin{aligned} \sum_i H(X_i Y_i)_\rho &= \sum_{i \in L} H(X_i Y_i)_\rho + \sum_{i \notin L} H(X_i Y_i)_\rho \\ &\leq 2|L| \log(k) + (n - |L|)(2 \log(k) - \frac{4t}{n}) \\ &= 2n \log(k) - (n - |L|)\frac{4t}{n}. \end{aligned}$$

Since $\sum_i H(X_i Y_i)_\rho \geq H(XY)_\rho = 2n \log(k) - t$, we have $2n \log(k) - (n - |L|)\frac{4t}{n} \geq 2n \log(k) - t$ which gives $|L| \geq \frac{3n}{4}$.

Putting this together, we have $|K \cap L| = |K| + |L| - |K \cup L| \geq |K| + |L| - n \geq n/2$. ■

The final step of the proof will be very similar to the proof of Proposition 2.

We start with a few notations. For a string $x = x_1, \dots, x_n \in [k^n]$, let x_{-i} be the string in $[k^{n-1}]$ where we remove x_i from x . As in Section 3.1, we define $|L_y^A\rangle, |L_x^B\rangle, \sigma^A, \sigma^B$. Also, let

$$p_{x\cdot} = \sum_{y \in [k^n]} p_{xy} \quad ; \quad p_{\cdot y} = \sum_{x \in [k^n]} p_{xy}$$

and

$$p_{x_i, y_i}^i = \sum_{x', y': x'_i = x_i, y'_i = y_i} p_{x' y'} \quad ; \quad p_{x_{-i}, y_{-i}}^{-i} = \sum_{x', y': x'_{-i} = x_{-i}, y'_{-i} = y_{-i}} p_{x' y'}$$

For each i , we rewrite ρ as:

$$\rho = \sum_{x, y \in [k^n]} p_{xy} |x_i\rangle \langle x_i|_{\mathcal{X}_i} \otimes |x_{-i}\rangle \langle x_{-i}|_{\mathcal{X}_{-i}} \otimes |\phi_{xy}\rangle \langle \phi_{xy}|_{AB} \otimes |y_{-i}\rangle \langle y_{-i}|_{\mathcal{Y}_{-i}} \otimes |y_i\rangle \langle y_i|_{\mathcal{Y}_i}.$$

We define

$$|Z_{x_i, y_i}^i\rangle = \sum_{x', y' \in [k^n]: x'_i = x_i, y'_i = y_i} \sqrt{p_{x'_i, y'_i}^{-i}} |x'_{-i}\rangle_{\mathcal{X}_{-i}} \otimes |\phi_{x' y'}\rangle \otimes |y'_{-i}\rangle_{\mathcal{Y}_{-i}}.$$

Now, let $\gamma_i = \sum_{x_i, y_i \in [k]} p_{x_i, y_i}^i |x_i\rangle \langle x_i| \otimes |Z_{x_i, y_i}^i\rangle \langle Z_{x_i, y_i}^i| \otimes |y_i\rangle \langle y_i|$. The state γ_i corresponds to ρ where the inputs in registers $\mathcal{X}_{-i}, \mathcal{Y}_{-i}$ are in coherent superposition. In particular, Alice and Bob can go from γ_i to ρ by measuring the registers \mathcal{X}_{-i} and \mathcal{Y}_{-i} in the computational basis.

Using ρ , Alice and Bob can win the i^{th} instance of G with probability p_i . This means that they can win this i^{th} instance of G when sharing γ_i with probability at least p_i .

Now, consider σ_i^A, σ_i^B the 2 superposed states of γ_i as defined in Section 3.1. We first show the following:

Lemma 6. *If $t \leq \frac{c_0 \varepsilon n}{4}$ then $\forall i \in K \cap L, I(Y_i : XA)_{\sigma_i^A} + I(X_i : BY)_{\sigma_i^B} = \Omega(\varepsilon)$.*

Proof. Consider $i \in K \cap L$. Since $i \in L$, we have $H(X_i Y_i)_{\gamma_i} \geq 2 \log(k) - 4t/n \geq 2 \log(k) - c_0 \varepsilon$. Using Claim A.2, we have $\Delta(p^i, \text{Unif.}) \leq c_0 \varepsilon$ or in other words that $\frac{1}{2} \sum_{x_i, y_i \in [k]} |p_{x_i, y_i}^i - \frac{1}{k^2}| \leq c_0 \varepsilon$. Since $i \in K$, we have $\omega^*(G'_i | \gamma_i) \geq 1 - \varepsilon/4$ for $G'_i = (I, O, V, p^i)$. Using Theorem 3, we conclude that $SIC(\gamma_i) = I(Y_i : XA)_{\sigma_i^A} + I(X_i : BY)_{\sigma_i^B} = \Omega(\varepsilon)$. \blacksquare

We can now finish the proof. The above lemma holds for our t since $t = o(\varepsilon n)$. First notice that $\text{Tr}_{\mathcal{Y}_{-i}}(\sigma_i^A) = \text{Tr}_{\mathcal{Y}_{-i}}(\sigma^A)$ hence $I(Y_i : XA)_{\sigma_i^A} = I(Y_i : XA)_{\sigma^A}$. Similarly, we have $I(X_i : BY)_{\sigma_i^B} = I(X_i : BY)_{\sigma^B}$ which gives

$$I(Y_i : XA)_{\sigma_i^A} + I(X_i : BY)_{\sigma_i^B} = I(X_i : BY)_{\sigma^A} + I(Y_i : XA)_{\sigma^B}$$

and hence

$$\forall i \in K \cap L, I(X_i : BY)_{\sigma^A} + I(Y_i : XA)_{\sigma^B} = \Omega(\varepsilon).$$

To conclude, first we write

$$\begin{aligned} SIC(\rho) &= I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B} \\ &= H(Y)_{\sigma^A} - H(Y|XA)_{\sigma^A} + H(X)_{\sigma^B} - H(X|BY)_{\sigma^B} \\ &\geq H(XY)_\rho - H(Y|XA)_{\sigma^A} - H(X|BY)_{\sigma^B} \\ &\geq 2n \log(k) - t - H(Y|XA)_{\sigma^A} - H(X|BY)_{\sigma^B} \\ &\geq \sum_{i \in [n]} H(Y_i)_{\sigma^A} - H(Y|XA)_{\sigma^A} + \sum_{i \in [n]} H(X_i)_{\sigma^B} - H(X|BY)_{\sigma^B} - t \\ &\geq \sum_{i \in [n]} H(Y_i)_{\sigma^A} - H(Y_i|XA)_{\sigma^A} + \sum_{i \in [n]} H(X_i)_{\sigma^B} - H(X_i|BY)_{\sigma^B} - t \\ &= \sum_{i \in [n]} I(Y_i : XA)_{\sigma^A} + I(X_i : BY)_{\sigma^B} - t \\ &\geq \sum_{i \in K \cap L} I(Y_i : XA)_{\sigma^A} + I(X_i : BY)_{\sigma^B} - t \\ &= \Omega(n\varepsilon) - t = \Omega(n\varepsilon) \quad \text{since } |K \cap L| \geq n/2 \text{ and } t = o(n\varepsilon). \end{aligned}$$

F Games with complete support

In this Appendix we prove Corollary 1. The idea is the following. Starting from any game G with complete support, we define a new game H that can be interpreted as follows:

- With some probability Alice and Bob play G_U , a variant of G on the uniform distribution
- If they are not in the previous case, they win no matter what they answer
- They know in which case they are thanks to an extra input bit
- If they ignore the extra bit of information, they play the original game.

In Lemma 7 we prove that H^n has a larger value than G^n , which intuitively follows from the fact that players can just ignore the extra bits. Since the difficulty of winning H^n comes from the indices where Alice and Bob must play G_U , in Lemma 8 we show that the winning probability of H^n is bounded by the winning probability of a parallel repetition of G_U . We have an exponential decay because G_U meets the requirements of Theorem 1. To finish, we relate $\omega^*(G)$ to $\omega^*(G_U)$ in Lemma 9 and we prove Corollary 1.

Let us start with some definitions. Let $G = (I, O, V, p)$ with $|I| = k$. Let $\alpha_{min} = \min_{xy} \{k^2 p_{xy}\}$ and $\alpha_{max} = \max_{xy} \{k^2 p_{xy}\}$. We have:

$$\forall (x, y) \in I^2 \quad \frac{\alpha_{min}}{k^2} \leq p_{xy} \leq \frac{\alpha_{max}}{k^2}.$$

Let U be the uniform distribution on I^2 . By seeing p and U as vectors indexed by (x, y) , we can rewrite the above as $\alpha_{min}U \leq p \leq \alpha_{max}U$. Let p' the probability distribution satisfying $p = \alpha_{min}U + (1 - \alpha_{min})p'$. Let $\tilde{I} = \{0, 1\} \times I$ and q be the distribution on \tilde{I}^2 such that $q_{0x0y} = \frac{\alpha_{min}}{k^2}$, $q_{1x1y} = (1 - \alpha_{min})p'_{xy}$ and $q_{0x1y} = q_{1x0y} = 0$. We have:

$$q_{0x0y} + q_{1x1y} = \frac{\alpha_{min}}{k^2} + (1 - \alpha_{min})p'_{xy} = p_{xy}.$$

We define the game $H = (\tilde{I}, O, \tilde{V}, q)$ with the following winning predicate:

- $\tilde{V}(ab|0x0y) = V(ab|xy)$ for all $a, b \in O^2$.
- $\tilde{V}(ab|1x1y) = 1$ for all $a, b \in O^2$.

This means that if Alice and Bob's extra bit is 0 the predicate is the same than the predicate of G , while if the extra bit is 1 they always win. Notice that for each $c \in \{0, 1\}$, we have $\tilde{V}(ab|cxcy) \geq V(ab|xy)$. Now consider the parallel repetition. Let $\tilde{x}, \tilde{y} \in \tilde{I}^n$, where we write $\tilde{x}_i = c_i x_i$ and $\tilde{y}_i = c_i y_i$ with $x_i, y_i \in I$ and c_i being the extra bit. Let \tilde{V}' and V' be the predicates for H^n and G^n , respectively. Then for all a, b , we have

$$\tilde{V}'(ab|\tilde{x}\tilde{y}) = \Pi_i(\tilde{V}(a_i b_i|\tilde{x}_i \tilde{y}_i)) \geq \Pi_i(V(a_i b_i|xy)) = V'(ab|xy). \quad (11)$$

Lemma 7. $\omega^*(G^n) \leq \omega^*(H^n)$.

Proof. Fix an optimal strategy for G^n . Let $P(ab|xy)$ the probability that Alice and Bob output $a, b \in O^n$ on inputs $x, y \in I^n$ when applying such strategy for G^n . We have

$$\omega^*(G^n) = \sum_{xyab} p_{xy} P(ab|xy) V'(ab|xy).$$

Define the following strategy for H^n . Alice and Bob, on inputs $\tilde{x}, \tilde{y} \in \tilde{I}^n$ according to q^n , ignore the extra bit and apply the above optimal strategy for G^n on inputs x, y . Let $\tilde{P}(ab|\tilde{x}\tilde{y})$ the probability of outputs a, b on

inputs $\tilde{x}\tilde{y}$ with this strategy. We have $\tilde{P}(ab|\tilde{x}\tilde{y}) = P(ab|xy)$. Also note that for all $x, y \in I^n$ and $c \in \{0, 1\}^n$ we can write $q_{cxy} = p_{xy}r_{xyc}$ where $r_{xyc} \geq 0$ and $\sum_c r_{xyc} = 1$. It follows from above and (11) that

$$\begin{aligned} \omega^*(H^n) &\geq \sum_{xyab} \sum_c q_{cxy} \tilde{P}(ab|\tilde{x}yc) V^n(ab|cxy) \\ &\geq \sum_{xyab} p_{xy} \sum_c r_{xyc} P(ab|xy) V^n(ab|cxy) \\ &\geq \sum_{xyab} p_{xy} \sum_c r_{xyc} P(ab|xy) V^n(ab|xy) \\ &= \sum_{xyab} p_{xy} P(ab|xy) V^n(ab|xy) = \omega^*(G^n). \end{aligned}$$

■

We now want to upper bound $\omega^*(H^n)$. Let G_U the game G on the uniform distribution and let $\varepsilon_U = 1 - \omega^*(G_U)$. We prove the following.

Lemma 8. $\omega^*(H^n) \leq (1 - \varepsilon_U^2)^{\Omega(\frac{n\alpha_{min}}{\log(|I||O|)} - \alpha_{min}|\log(\varepsilon)|)}$.

Proof. Thanks to the extra bit, we can interpret H as follows:

- With probability α_{min} , Alice and Bob play G_U
- With probability $1 - \alpha_{min}$, they win on any output
- They know in which case they are

If there are k instances of G_U , Alice and Bob win the whole game if and only if they win these k instances of G_U . The probability that i instances of G_U occur is equal to $\binom{n}{i} \alpha_{min}^i (1 - \alpha_{min})^{n-i}$. This gives

$$\omega^*(H^n) \leq \sum_{i=0}^n \binom{n}{i} \alpha_{min}^i (1 - \alpha_{min})^{n-i} \omega^*(G_U^i).$$

Since G_U is on the uniform distribution, we have that $\omega^*(G_U^i) \leq (1 - \varepsilon_U^2)^{\Omega(\frac{i}{\log(|I||O|)} - |\log(\varepsilon)|)}$ by Theorem 1. This gives

$$\omega^*(H^n) \leq \sum_{i=0}^n \binom{n}{i} \alpha_{min}^i (1 - \alpha_{min})^{n-i} (1 - \varepsilon_U^2)^{\Omega(\frac{i}{\log(|I||O|)} - |\log(\varepsilon)|)}.$$

We can show by analytic calculations that

$$\sum_{i=0}^n \binom{n}{i} \alpha_{min}^i (1 - \alpha_{min})^{n-i} Y^i = (\alpha_{min}(Y - 1) + 1)^n.$$

By plugging this in the above inequality, we obtain

$$\omega^*(H^n) \leq (1 - \varepsilon_U^2)^{\Omega(\frac{n\alpha_{min}}{\log(|I||O|)} - \alpha_{min}|\log(\varepsilon)|)}.$$

■

Now we relate the values of G and G_U . Let $\omega^*(G) = 1 - \varepsilon$.

Lemma 9. $\varepsilon \leq \alpha_{max} \varepsilon_U$.

Proof. Fix an optimal strategy for G_U and let $P(ab|xy)$ the probability of outputs a, b on inputs x, y for this strategy. We have

$$\begin{aligned}\varepsilon_U &= \sum_{xyab} \frac{1}{k^2} P(ab|xy)(1 - V(ab|xy)) \\ &\geq \sum_{xyab} \frac{p_{xy}}{\alpha_{max}} P(ab|xy)(1 - V(ab|xy)) \\ &\geq \frac{\varepsilon}{\alpha_{max}}.\end{aligned}$$

■

Finally, we combine all of the above in the final corollary

Corollary 1. *Let $G = (I, O, V, p)$ be a game with complete support and $\omega^*(G) = (1 - \varepsilon)$. Then,*

$$\omega^*(G^n) \leq (1 - \varepsilon^2)^{\Omega\left(\frac{n}{Q \log(|I||O|)} - \frac{|\log(\varepsilon)|}{Q}\right)},$$

where $Q = \frac{k^2 \max_{xy} p_{xy}^2}{\min_{xy} p_{xy}}$.

Proof. By chaining the previous lemmas, we obtain

$$\begin{aligned}\omega^*(G^n) &\leq \omega^*(H^n) \leq (1 - \varepsilon_U^2)^{\Omega\left(\frac{n\alpha_{min}}{\log(|I||O|)} - \alpha_{min} |\log(\varepsilon)|\right)} \\ &\leq (1 - \varepsilon^2)^{\Omega\left(\frac{n\alpha_{min}}{\alpha_{max}^2 \log(|I||O|)} - \frac{\alpha_{min} |\log(\varepsilon)|}{\alpha_{max}^2}\right)} \leq (1 - \varepsilon^2)^{\Omega\left(\frac{n}{Q \log(|I||O|)} - \frac{|\log(\varepsilon)|}{Q}\right)}.\end{aligned}$$

■