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

André Chailloux
SECRET Project Team, INRIA Paris-Rocquencourt

Giannicola Scarpa
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 Alice and Bob receive all the inputs at the same time and must 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 dimensions of the input and output space. From this result, we show that for any entangled game G, $\omega^*(G^n) = (1-\varepsilon^2)^{\Omega(\frac{n}{Q^4 \log(Q\cdot|O|)} - |\log(\varepsilon/Q)|)}$ where p is the input distribution of G and $Q = \max(\lceil \frac{1}{\min_{xy:p_{xy}\neq 0}(\sqrt{p_{xy}})} \rceil, |I|)$.

This is the first time exponential decay is shown for the parallel repetition of any entangled game. 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 in I^2 and a result function $V : O^2 \times I^2 \to \{0, 1\}$. 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 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 n inputs respectively $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$. Each (x_i, y_i) is taken according to p. They output respectively $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$. They win the game iff $\forall i,\ V(a_i, b_i|x_i, y_i) = 1$. In order to win the n-fold repetition, Alice and Bob can just use the best strategy for G and use it in 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, we know some games for which this does not hold. 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 [Raz98]. Afterwards, a series of works showed improved results for specific types of games [Hol07, Rao08, AKK$^+$08, Raz11]. Parallel repetition for games has many applications, from direct product theorems in communication complexity [PRW97] to hardness of amplification results [BGS98].

In the quantum setting, it is natural to consider entangled games where Alice and Bob are allowed to share some quantum state at the beginning of the game. Entangled games exhibit Bell violations which are a witness of quantum non-locality. 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 [CSUU08]. It was also shown that entangled unique games [KRT08] admit a parallel repetition with exponential decay. Finally, it was shown that any entangled game admits a parallel repetition [KV11]. 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, a new parallel repetition result with exponential decay has been shown for entangled projection games [DSV13].

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 dimension on the input and the output space.

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*

$$\omega^*(G^n) = (1-\varepsilon^2)^{\Omega(\frac{n}{Q^4 \log(Q\cdot|O|)} - |\log(\varepsilon/Q)|)},$$

where $|O|$ is the dimension of the output space of G and $Q = \max(\lceil \frac{1}{\min_{xy:p_{xy}\neq 0}(\sqrt{p_{xy}})} \rceil, |I|)$.

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

In order to prove this theorem, we introduce the concept of *Superposed Information Cost* of a game which is a very powerful concept and the cornerstone of our proof.

1.2 Superposed Information cost

This concept is derived from the notion of information cost widely used in communication complexity [CSWY01, BYJKS04, Bra12, KLL$^+$12]. 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 usually 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.

1.3 Properties of the information cost

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 (but 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 when considering 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 a first evidence that the game G^n is hard to win and that $\omega^*(G^n)$ decreases fast.

Using the superposed information cost 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

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

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*:

- Alice and Bob use the optimal strategy for G^n and win with probability $\omega^*(G^n) = 2^{-t}$.
- Alice sends $m = O(\frac{t \log(|I||O|)}{\varepsilon})$ 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 $t = \Omega(\frac{n\varepsilon^2}{\log(|I||O|)})$ or equivalently $\omega^*(G^n) = (1-\varepsilon^2)^{\Omega(\frac{n}{\log(|I|(|O|)})}$.

1.4 Organization of the paper

Section 2 contains preliminaries about measure distances on quantum states, quantum information theory and 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 Sections 6 and 7, we derive the upper and lower bounds of (1). Finally, in Section 8 we prove our main theorem.

2 Preliminaries

2.1 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 1 *For any two quantum states ρ, σ, the trace distance Δ between them is given by* $\Delta(\rho,\sigma) = \Delta(\sigma,\rho) = \frac{1}{2}\| \rho - \sigma \|_{\mathrm{tr}}$

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

Proposition 2 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, 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 3 *[Hel67] 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*

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

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

Proposition 4 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, 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 3 *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 $\mathrm{Tr}_{\mathcal{A}}(|\psi\rangle\langle\psi|) = \rho$.*

Proposition 5 (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 6 *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 7 ([SR01, NS03]) *For any two quantum states ρ, σ*

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

Proposition 8 ([FG99]) *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 7, we have

Proposition 9 *Let $|A\rangle, |B\rangle, |C\rangle$ three quantum states. We have*

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

and

Proposition 10 *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 7, we have

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

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 11 *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

$$F(\rho, \rho') = \sum_x \sqrt{p_x p_{x'}} ||\sqrt{\rho_x}\sqrt{\rho'_x}||_1 = \sum_x \sqrt{p_x p_{x'}} F(\rho_x, \rho_{x'})$$

■

2.2 Information Theory

For a quantum state ρ, the entropy of ρ is $H(\rho) = -tr(\rho \log(\rho))$. 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, $H(X)_\rho = H(\mathrm{Tr}_{\mathcal{Y}}(\rho))$.

$H(X|Y)_\rho = H(XY)_\rho - H(Y)_\rho$ 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 $\lambda_{\max}$ is the maximum eigenvalue of ρ. For ρ in $\mathcal{X} \otimes \mathcal{Y}$, we define

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

We have $H_{min}(X|Y)_\rho \leq H(X|Y)_\rho$ [MDS$^+$13]. 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 1 (Subadditivity of the conditional entropy)

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

Claim 2 ([KNTSZ07])

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

where $\rho_A = Tr_{\mathcal{B}}(\rho)$ and $\rho_B = Tr_{\mathcal{A}}(\rho)$

Claim 3 (from [Vad99]) *For any distribution p on a universe U, If $H(p) \geq \log(|U|) - \varepsilon$ then $\Delta(p, Unif.) \leq \varepsilon$, where Unif. is the uniform distribution.*

2.3 Entangled Games

2.3.1 The value of an entangled game

We now define the notion of an entangled game and its value.

Definition 4 *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 $V : O^2 \times I^2 \to \{0, 1\}$ and a probability distribution $p : I^2 \to [0, 1]$.*

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 can assume that w.l.o.g., Alice and Bob can share a pure state $|\phi\rangle$. Moreover, their optimal strategy can be described as projective measurements $A^x = \{A^x_a\}_{a\in O}$ and $B^y = \{B^y_b\}_{b\in O}$.

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 5 *The entangled value of a game G is*

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

Definition 6 *We say that 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 will write $p = Unif.$ when this is the case.*

2.3.2 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 7 *The entangled value of G, given that Alice and Bob share the above state ρ is*

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

2.3.3 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 $I' = I^{\times n}, O' = O^{\times n}, q_{xy} = \Pi_{i\in[n]} p_{x_i,y_i}$ and $V'(a, b|x, y) = \Pi_{i\in[n]} V(a_i, b_i|x_i, y_i)$. While playing G^n, we say that Alice and Bob win game i if $V(a_i, b_i|x_i, y_i) = 1$.

2.3.4 Majority game

For a game $G = (I, O, V, p)$, we define $G^n_\alpha = (I', O', V', p')$ as follows: $I' = I^{\times n}$, $O' = O^{\times n}$, $p'_{xy} = \Pi_{i\in[n]} p_{x_i,y_i}$ as in G^n. We define V' as follows:

$$V'(a, b|x, y) = 1 \Leftrightarrow \#\{i : V(a_i, b_i|x_i, y_i) = 1\} \geq \alpha n.$$

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 2.3.2. 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 in 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 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 side, 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 that Bob has about x when he has a coherent superposition of his inputs.

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 any state $\rho = \sum_{xy\in[k]} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$. Let $p_{x\cdot} = \sum_y p_{xy}$ and $p_{\cdot y} = \sum_x p_{xy}$.

Let $|L^B_x\rangle = \frac{1}{\sqrt{p_{x\cdot}}} \sum_y \sqrt{p_{xy}}|\phi_{xy}\rangle|y\rangle$ and $|L^A_y\rangle = \frac{1}{\sqrt{p_{\cdot y}}} \sum_x \sqrt{p_{xy}}|x\rangle|\phi_{xy}\rangle$. Consider the two superposed states:

$$\sigma^A = \sum_{y\in[k]} p_{\cdot y}|L^A_y\rangle\langle L^A_y|_{\mathcal{XAB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$$
$$\sigma^B = \sum_{x\in[k]} p_{x\cdot}|x\rangle\langle x|_{\mathcal{X}} \otimes |L^B_x\rangle\langle L^B_x|_{\mathcal{ABY}}.$$

σ^A (resp. σ^B) corresponds to ρ where Alice's input (resp. Bob's input) is put in a coherent superposition.

Remark: The above definition is not uniquely defined for ρ since it depends on the phases applied on $|\phi_{xy}\rangle$. When we fix a state ρ, we also fix a description of the states $|\phi_{xy}\rangle$ in all the definitions we use.

We first define the superposed information cost of a state ρ of the above form.

Definition 8 *The superposed information cost $SIC(\rho)$ of ρ is defined as*

$$SIC(\rho)^1 = I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B}.$$

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

Definition 9 *For any entangled game $G = (I, O, V, p)$, we define $SIC(G) = \inf_\rho SIC(\rho)$ where the infimum is taken over all ρ of the form $\rho = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G|\rho) = 1$.*

3.2 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 $x = x_1, \ldots, x_n \in I^n$, 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 $q_{xy} = \Pi_j p_{x_j,y_j}$. We define $q_{xy}^{-i} = \Pi_{j \neq i} p_{x_j,y_j}$. 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

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

Let $\rho_i = \sum_{x_i,y_i \in I} p_{x_i,y_i}|x_i\rangle\langle x_i| \otimes |Z^i_{x_i,y_i}\rangle\langle Z^i_{x_i,y_i}| \otimes |y_i\rangle\langle y_i|$. 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 $\omega^*(G|\rho_i) = 1$.

[1] This definition is suitable when the input distribution of is a product distribution or close to a product distribution. One may want to consider a more general definition when considering any distributions

We define

$$|L^B_{x_i}(i)\rangle = \frac{1}{\sqrt{p_{x_i\cdot}}} \sum_{y_i \in I} \sqrt{p_{x_i,y_i}} |Z^i_{x_i,y_i}\rangle |y_i\rangle$$
$$|L^A_{y_i}(i)\rangle = \frac{1}{\sqrt{p_{\cdot y_i}}} \sum_{x_i \in I} \sqrt{p_{x_i,y_i}} |x_i\rangle |Z^i_{x_i,y_i}\rangle.$$

We now also define the two new superposed states of ρ_i

$$\sigma^B_i = \sum_{x_i \in I} p_{x_i\cdot} |x_i\rangle\langle x_i|_{\mathcal{X}_i} \otimes |L^B_{x_i}(i)\rangle\langle L^B_{x_i}(i)|_{\mathcal{X}_{-i}\mathcal{A}\mathcal{B}\mathcal{Y}}$$
$$\sigma^A_i = \sum_{y_i \in I} p_{\cdot y_i} |L^A_{y_i}(i)\rangle\langle L^A_{y_i}(i)|_{\mathcal{X}\mathcal{A}\mathcal{B}\mathcal{Y}_{-i}} \otimes |y_i\rangle\langle y_i|_{\mathcal{Y}_i}.$$

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

$$I(Y_i : XA)_{\sigma^A_i} + I(X_i : BY)_{\sigma^B_i} \geq SIC(G).$$

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

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

■

We can now prove our proposition:

Proposition 12 $SIC(G^n) = nSIC(G)$.

Proof: We have:

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

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 $SIC(G^n) = nSIC(G)$. ■

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

We will 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 $\rho = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ such that $\omega^*(G'|\rho) \geq 1 - \frac{\varepsilon}{4}$, we have that $SIC(\rho) = \Omega(\varepsilon)$.*

If $\omega^*(G) = 1-\varepsilon$, the 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 $G^n_{1-\varepsilon/32} = (I^n, O^n, V', Unif.)$ as defined in Section 2.3.4. There exists a game $G' = (I^n, O^n, V', p)$ and a state $\xi = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ 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 $G^n_{1-\varepsilon/32}$. 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 Section 7, we prove a 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 $t \leq \frac{c_0\varepsilon n}{4} - 1$ where c_0 is the absolute constant of Theorem 3. Let also $G^n_{1-\varepsilon/32} = (I^n = [k^n], O^n, V', Unif.)$ as defined in Section 2.3.4. 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 $SIC(\rho) \geq \Omega(n\varepsilon)$.

The way we prove this theorem is very similar to the proof of the additivity of the superposed information cost, but we use Theorem 3 instead of Theorem 2. In Section 8, we show how to use the two above theorems to conclude and show the following:

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

5 Relating the superposed information cost and the value of entangled games

5.1 Overview

The goal of this Section is to show the following theorem:

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

The proof goes 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).

1. First we show that $SIC(\rho) \geq \frac{1}{4\ln(2)}(1-\frac{1}{k^2}\sum_{y,y'} F^2(\rho_y^A, \rho_{y'}^A)+1-\frac{1}{k^2}\sum_{x,x'} F^2(\rho_x^B, \rho_{x'}^B))$ (Proposition 13).

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 unitaries $\{U_x\}_x, \{V_y\}_y$ (Proposition 14).

3. Finally, we show that $(1 - \max_{|\Omega\rangle} \sum_{x,y\in[k]} \frac{1}{k^2}|\langle\Omega|U_x \otimes V_y|\phi_{xy}\rangle|^2) \geq 1 - \omega^*(G)$ (Corollary 2 of Proposition 15).

   Putting the three inequalities together, we get

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

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

We then extend Theorem 2 as follows.

Theorem 3 *There exists a small constant c_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 $SIC(\rho) = \Omega(\varepsilon)$.*

5.2 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 $\rho_y^A = \mathrm{Tr}_{\mathcal{B}}|L_y^A\rangle\langle L_y^A|$ and $\rho_x^B = \mathrm{Tr}_{\mathcal{A}}|L_x^B\rangle\langle L_x^B|$. 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 13 $SIC(\rho) \geq \frac{1}{4\ln(2)}(1 - \sum_{y,y'} p_{\cdot y}p_{\cdot y'}F^2(\rho_y^A, \rho_{y'}^A) + 1 - \sum_{x,x'} p_{x\cdot}p_{x'\cdot}.F^2(\rho_x^B, \rho_{x'}^B))$.

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

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

where $\xi_{\mathcal{XA}}^A = \sum_y p_{\cdot y}\rho_y^A$ and $\xi_{\mathcal{Y}}^A = \sum_y p_{\cdot y}|y\rangle\langle y|$. Next, using Proposition 11, we have $F(\xi^A, \xi_{\mathcal{XA}}^A \otimes \xi_{\mathcal{Y}}^A) = \sum_y p_{\cdot y}F(\rho_y^A, \xi_{\mathcal{XA}}^A)$. From there, we have:

$$\begin{aligned}
1 - F(\xi^A, \xi_{\mathcal{XA}}^A \otimes \xi_{\mathcal{Y}}^A) &= 1 - \sum_{y\in[k]} p_{\cdot y}F(\rho_y^A, \xi_{\mathcal{XA}}^A) \\
&= \frac{1}{2}(1 - \sum_{y\in[k]} p_{\cdot y}F(\rho_y^A, \xi_{\mathcal{XA}}^A) + 1 - \sum_{y'\in[k]} p_{\cdot y'}F(\rho_{y'}^A, \xi_{\mathcal{XA}}^A)) \\
&= \frac{1}{2}\sum_{y,y'\in[k]} p_{\cdot y}p_{\cdot y'}[1 - F(\rho_y^A, \xi_{\mathcal{XA}}^A) + 1 - F(\rho_{y'}^A, \xi_{\mathcal{XA}}^A)] \\
&\geq \frac{1}{4}\sum_{y,y'\in[k]} p_{\cdot y}p_{\cdot y'}(1 - F(\rho_y^A, \rho_{y'}^A)) && \text{using Proposition 10} \\
&\geq \frac{1}{8}\sum_{y,y'\in[k]} p_{\cdot y}p_{\cdot y'}(1 - F^2(\rho_y^A, \rho_{y'}^A))
\end{aligned}$$

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

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

■

5.3 Second inequality

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

$$\varepsilon^A = 1 - \sum_{y,y'} \frac{1}{k^2}F^2(\rho_y^A, \rho_{y'}^A) = 1 - \mathop{\mathbb{E}}_{y,y'}[F^2(\rho_y^A, \rho_{y'}^A)]$$

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

The expectations will always be taken on 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 in $\mathcal{A}$ and $\mathcal{B}$ such that if we define $|\Omega_{xy}\rangle = (U_x \otimes V_y)|\phi_{xy}\rangle$, we have:*

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

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

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

For each y, consider the unitary U_y acting on $\mathcal{B}$ such that $|\langle L_j^A|(I_{\mathcal{XA}} \otimes U_y)|L_y^A\rangle| = F(\rho_j^A, \rho_y^A)$. 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 $(I_{\mathcal{XA}} \otimes U_y)$ acts only on space $\mathcal{B}$, we can write $(I_{\mathcal{XA}} \otimes U_y)|L_y^A\rangle = \frac{1}{\sqrt{k}} \sum_x |x\rangle|\xi_{xy}\rangle$ for some $|\xi_{xy}\rangle$. Therefore, we have:

$$F(\rho_j^A, \rho_y^A) = |\langle L_j^A|(I_{\mathcal{XA}} \otimes U_y)|L_y^A\rangle| = |\frac{1}{k}\sum_x \langle\xi_{xy}|\phi_{xj}\rangle| = |\mathop{\mathbb{E}}_x[\langle\xi_{xy}|\phi_{xj}\rangle]| \leq \mathop{\mathbb{E}}_x[|\langle\xi_{xy}|\phi_{xj}\rangle|].$$

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

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

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 $\nu_x^B = Tr_{\mathcal{A}}|M_x^B\rangle\langle M_x^B|$. 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

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

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

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

For each x, consider the unitary V_x acting on $\mathcal{A}$ such that $|\langle M_i^B|(V_x \otimes I_{\mathcal{BY}})|M_x^B\rangle| = F(\nu_i^B, \nu_x^B)$. 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 $(V_x \otimes I_{\mathcal{BY}})$ acts only on space $\mathcal{A}$, we can write $(V_x \otimes I_{\mathcal{BY}})|M_x^B\rangle = \frac{1}{\sqrt{k}} \sum_y |\Omega_{xy}\rangle|y\rangle$ for some $|\Omega_{xy}\rangle$. Therefore, we have:

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

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:

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

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, y $\langle\Omega_{xy}|\Omega_{xy'}\rangle = \langle\xi_{xy}|\xi_{xy'}\rangle$. Using Eq. 4, we have

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

Equations 7 and 8 give

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

Combining this with equations 3 and 6, we conclude

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

■

We can now prove the main proposition of this section.

Proposition 14 *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*

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

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

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

with $|\Omega_{xy}\rangle = U_x \otimes V_y|\phi_{xy}\rangle$. Using Proposition 9, we have

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

It follows that

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

Similarly, we get $\mathbb{E}_{x,x',y}[|\langle\Omega_{xy}|\Omega_{x'y}\rangle|^2] \geq 1-4\varepsilon^B$. Using Proposition 9 again, we have

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

This gives us

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

Using

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

we have

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

hence

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

■

5.4 Last inequality

Proposition 15 *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

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

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 15, 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 16 *Consider a game $G = (I, O, V, p)$ and a state*

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

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: Consdier 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 $tr(M^{xy}|\phi_{xy}\rangle\langle\phi_{xy}|) = |\langle C_{xy}|\phi_{xy}\rangle|^2$. 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

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

Using Proposition 9, 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 defintion 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 16, we conclude that $\omega^*(G) \geq 1 - 2(\gamma + \gamma')$. ■

Taking a counterpostitive 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 $\mathcal{B}$.

5.5 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 13 and Proposition 14, 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 $SIC(G) \geq \frac{1-\omega^*(G)}{32\ln(2)}$. ■

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

Proposition 17 *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 13 and Proposition 14, 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 $\omega^*(G|\rho) = 1$, we can conclude that $SIC(G) \geq \frac{1-\omega^*(G)}{32\ln(2)}$. ■

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

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 $\rho = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ 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 13, we define $\xi^B = Tr_{\mathcal{A}}(\sigma^B)$. This means that $\xi^B = \sum_x p_{x\cdot}|x\rangle\langle x| \otimes \rho_x^B$ for some ρ_x^B. Let also $\xi^B_{\mathcal{X}} = \mathrm{Tr}_{BY}(\xi^B)$ and $\xi^B_{\mathcal{BY}} = \mathrm{Tr}_X(\xi^B)$.

Similarly, let $\sigma^A(U), \sigma^B(U)$ the superposed states of $\rho(U)$ and let $\xi^B(U) = Tr_{\mathcal{A}}(\sigma^B(U))$. 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 $\xi^B_{\mathcal{X}}(U) = \mathrm{Tr}_{BY}(\xi^B(U))$ and $\xi^B_{\mathcal{BY}}(U) = \mathrm{Tr}_X(\xi^B(U))$.

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 13. Using Claim 2, we have $I(X:BY)_{\sigma^B} \geq \frac{2}{\ln(2)}(1 - F(\xi^B, \xi^B_{\mathcal{X}} \otimes \xi^B_{\mathcal{BY}}))$. Notice that $\Delta(\sigma^B, \sigma^B(U)) \leq \delta$ which implies $\Delta(\xi^B(U), \xi^B) \leq \delta$; $\Delta(\xi^B_{\mathcal{X}}(U), \xi^B_{\mathcal{X}}) \leq \delta$ and $\Delta(\xi^B_{\mathcal{BY}}(U), \xi^B_{\mathcal{BY}}) \leq \delta$. The two last inequalities give us $\Delta(\xi^B_{\mathcal{X}}(U) \otimes \xi^B_{\mathcal{BY}}(U), \xi^B_{\mathcal{X}} \otimes \xi^B_{\mathcal{BY}}) \leq 2\delta$. From there, by using Claim 2 and Propositions 8 and 10, we have:

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

Then, we have:

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

which gives us

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

Let $\varepsilon^B = 1 - \frac{1}{k^2}\sum_{x,x'} F^2(\rho_x^B(U), \rho_{x'}^B(U))$. As in Proposition 13, we can show that

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

hence $I(X:BY)_{\sigma^B} \geq \frac{2}{\ln(2)}(\frac{\varepsilon^B}{32} - 2\delta)$. 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 $I(Y:XA)_{\sigma^A} \geq \frac{2}{\ln(2)}(\frac{\varepsilon^A}{32} - 2\delta)$, which gives

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

Using Proposition 14, we have:

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

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:

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

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

6 Upper Bound

In the previous section, we showed how the superposed information cost of a game G can be used to bound its entangled value $\omega^*(G)$. As we showed with Proposition 12, the superposed information cost of G^n grows linearly in n. If we could manage to upper bound $SIC(G^n)$ by a quantity involving $\omega^*(G^n)$, we could be able to lower bound $\omega^*(G^n)$ as a function of n. Unfortunately, we are not able to directly upper bound $SIC(G^n)$, but working on a slightly different game will be enough for us. The goal of this Section is to prove the following weaker upper bound:

Theorem 4 *Consider a game $G = (I, O, V, Unif.)$ such that $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$. Let $G^n_{1-\varepsilon/32} = (I^n, O^n, V', Unif.)$ as defined in Section 2.3.4. There exists a game $G' = (I^n, O^n, V', p)$ and a state $\xi = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}| \otimes |y\rangle\langle y|$ 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 $G^n_{1-\varepsilon/32}$. The above 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.

We first present a construction of a state ξ and then we show that this state satisfies the above properties.

6.1 Constructing ξ

The construction of ξ will directly be inspired by a communication task that we now present.

6.1.1 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 random inputs $x = x_1, \ldots, x_n$ and $y = y_1, \ldots, y_n$, with $x, y \in I^n$.
- 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[Bob does not abort] $\geq p$
2. Pr[Alice and Bob win $\geq (1 - \varepsilon/32)n$ games | 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. Alice and Bob have some shared randomness that correspond to v random (not necessarily different) indices $i_1, \ldots, i_v \in [n]$ 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 random inputs x, y. They perform a strategy that wins all n games with probability $2^{-(t+1)}$ and have some outputs $a = a_1, \ldots, a_n$ and $b = b_1, \ldots, b_n$.
3. For each index $i \in \{i_1, \ldots, i_v\}$, 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 18 *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:

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

hence $p \geq 2^{-(t+1)}$.

For a random index i, we have:

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

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

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

Next, we have:

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

This gives us:

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

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

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

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,

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

■

6.1.2 Actually constructing ξ

- 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 18, we prove that ξ has the desired properties

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

Procedure for constructing ξ

1. Alice and Bob pick random inputs $x, y \in_R I^n = [k^n]$. They also share a state $\sum_r \gamma_r |r\rangle_{\mathcal{R}_A} \otimes |\phi\rangle_{\mathcal{AB}} \otimes |r\rangle_{\mathcal{R}_B}$ 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 $\rho_1 = \sum_{x,y} \frac{1}{k^{2n}} |x\rangle\langle x|_{\mathcal{X}} \otimes |\Omega^1_{xy}\rangle\langle\Omega^1_{xy}| \otimes |y\rangle\langle y|_{\mathcal{Y}}$, with

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

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

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 $\rho_2 = \sum_{x,y} \frac{1}{k^{2n}} |x\rangle\langle x| \otimes |\Omega^2_{xy}\rangle\langle\Omega^2_{xy}| \otimes |y\rangle\langle y|$, with

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

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

$$|\Omega^3_{xy}\rangle = \sum_{a,b,r,M} \gamma_{xyrabM} |a\rangle |M\rangle |r\rangle |\phi^{xy}_{ab}\rangle |r\rangle |M\rangle |b\rangle |NA\rangle_{\mathcal{Z}} +$$
$$\sum_{a,r,M} \gamma_{xyra,AB,M} |a\rangle |M\rangle |r\rangle |\phi^{xy}_{a,AB}\rangle |r\rangle |m\rangle |AB\rangle |AB\rangle_{\mathcal{Z}}.$$

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

Let $\rho_{-Z} = Tr_Z(\rho_3)$. 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 $\sum_{xy} q_{xy} |x\rangle\langle x| \otimes |Y^{NA}_{xy}\rangle\langle Y^{NA}_{xy}| \otimes |y\rangle\langle y|$. 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.

6.2 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 $Dim(XY) = k^{2n}$, 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 $H(XY)_{\rho_{NA}} \geq 2n\log(k) - t - 1$. ■

2) $\omega^*(G'|\xi) \geq 1 - \varepsilon/32$ where $G^n_{1-\varepsilon/32} = (I', O', V', \text{Unif.})$ 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 conditionned on Bob not aborting. We know that in this case, $Pr[\text{Alice and Bob win } \geq (1 - \varepsilon/32)n \text{ games} \mid \text{Bob does not abort}] \geq (1 - \varepsilon/32)$. From there, we have $\omega^*(G'|\xi) \geq (1 - \varepsilon/32)$ ■

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 $\sigma^A_{NA}, \sigma^B_{NA}$ of ξ as defined in Section 3.1. Recall that $\rho_{NA} = \sum_{xy} q_{xy}|x\rangle\langle x| \otimes |Y^{NA}_{xy}\rangle\langle Y^{NA}_{xy}| \otimes |y\rangle\langle y|$ 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 $SIC(\xi) = I(X : M_B B'Y)_{\sigma^B_{NA}} + I(Y : XA')_{\sigma^A_{NA}}$. Let also σ^A_2, σ^B_2 the superposed states of ρ_2.

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

Lemma 3 $I(X : M_B B'Y)_{\sigma^B_{NA}} \leq n\log(k) - H_{min}(X|M_B B'Y)_{\sigma^B_2} + t + 1$

Proof: We have:

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

By definition, we have $H_{min}(X|M_B B'Y)_{\sigma^B_2} = -\log(\Pr[\text{ Bob guesses x} \mid \text{Alice and Bob share } \sigma^B_2])$. When Alice and Bob share σ^B_2, if Bob tries to determine whether he aborts or not, the state he shares with Alice conditioned on not aborting is σ^B_{NA}. Since Bob doesn't abort with proability greater than 2^{-t+1}, we have

$\Pr[\text{ Bob guesses x} \mid \text{Alice and Bob share } \sigma^B_2]) \geq 2^{-(t+1)} \Pr[\text{ Bob guesses x} \mid \text{Alice and Bob share } \sigma^B_{NA}]$

From there, we have

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

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

We now prove the following:

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

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

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

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

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

Using Equations 9 and 10, we have:

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

By definition of H_{min}(Section 2.2), this gives $H_{min}(X|M_BB'Y)_{\sigma'_{XM_BB'Y}} \leq n\log(k) - m$. ■

We now put everything together and prove the following.

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

Proof: Combining Lemma 3 and Lemma 4, we have

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

■

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

Putting this all together, we have:

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

To conclude the proof, recall from Section 6.1.1 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 satsfies all the desired properties of Theorem 4.

7 Lower Bound

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

Theorem 5 *Consider a game $G = (I = [k], O, V, Unif.)$ such that $\omega^*(G) = 1 - \varepsilon$ and $\omega^*(G^n) = 2^{-t}$ with $t \leq \frac{c_0\varepsilon n}{4}$ where c_0 is the absolute constant of Theorem 3. Let also $G^n_{1-\varepsilon/32} = (I^n = [k^n], O^n, V', Unif.)$ as defined in Section 2.3.4. 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 $SIC(\rho) \geq \Omega(n\varepsilon)$.

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 stratregy.

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 stratagy and $H(\mathcal{X}_i, \mathcal{Y}_i)_\rho$ is large.

Lemma 5 *Let $p_i = \Pr[$Alice and Bob win game i 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*

$$|K| \geq 3n/4, \qquad |L| \geq 3n/4, \qquad \textit{which implies} \quad |K \bigcap L| \geq n/2.$$

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:

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

Since $\sum_i H(X_iY_i)_\rho \geq H(XY)_\rho = 2n\log(k) - t$, 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 $|K \bigcap L| = |K| + |L| - |K \bigcup L| \geq |K| + |L| - n \geq n/2$. ■

The final step of the proof will be very similar to the proof of Proposition 12.

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

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

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

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

Now, let $\gamma_i = \sum_{x_i,y_i\in[k]} p^i_{x_i,y_i}|x_i\rangle\langle x_i| \otimes |Z^i_{x_i,y_i}\rangle\langle Z^i_{x_i,y_i}| \otimes |y_i\rangle\langle y_i|$. 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^A_i, σ^B_i 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 $\forall i \in K \bigcap L$, $I(Y_i : XA)_{\sigma^A_i} + I(X_i : BY)_{\sigma^B_i} = \Omega(\varepsilon)$.*

Proof: Consider $i \in K \bigcap L$. Since $i \in L$, we have $H(X_iY_i)_{\gamma_i} \geq 2\log(k) - 4t/n \geq 2\log(k) - c_0\varepsilon$. Using Claim 3, we have $\Delta(p^i, \text{Unif.}) \leq c_0\varepsilon$ or in other words that $\frac{1}{2}\sum_{x_i,y_i\in[k]} |p^i_{x_i,y_i} - \frac{1}{k^2}| \leq c_0\varepsilon$. 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 $SIC(\gamma_i) = I(Y_i : XA)_{\sigma^A_i} + I(X_i : BY)_{\sigma^B_i} = \Omega(\varepsilon)$. ■

We can now finish the proof. First notice that $Tr_{\mathcal{Y}_{-i}}(\sigma_i^A) = Tr_{\mathcal{Y}_{-i}}(\sigma^A)$ 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

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

To conclude, we write

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

■

8 Final Theorem and conclusion

We can now prove our main theorem.

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

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

Proof: Let $G^n_{1-\varepsilon/32} = (I^n = [k^n], O^n, V_n, \text{Unif.})$ as defined in Section 2.3.4. 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. $S(XY)_\xi \geq 2n\log(k) - t - 1$
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 $t \geq \frac{c_0\varepsilon n}{4}$, then $\omega^*(G^n) = (1-\varepsilon)^{\Omega(n)}$ and the theorem holds directly.

- If $t \leq \frac{c_0 \varepsilon n}{4}$, 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

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

Putting the two equations together, we have $t = \Omega\left(\frac{n\varepsilon^2}{\log(|I||O|)} - |\log(\varepsilon)|\right)$ which allows us to conclude

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

■

Finally, we extend this result to general games.

Corollary 1 *For any game $G = (I, O, V, p)$ such that $\omega^*(G) \leq 1 - \varepsilon$, we have that*

$$\omega^*(G^n) = (1-\varepsilon^2)^{\Omega(\frac{n}{Q^4 \log(Q \cdot |O|)} - |\log(\varepsilon/Q)|)},$$

where $|O|$ is the dimension of the output space of G and $Q = \max(\lceil \frac{1}{\min_{xy: p_{xy} \neq 0}(\sqrt{p_{xy}})} \rceil, |I|)$.

Proof: Fix $G = (I, O, V, p)$. We consider a set I' such that $I \subseteq I'$ and $\forall x, y,\ st.\ p_{xy} \neq 0$, $p_{xy} \geq \frac{1}{|I'|^2}$. We can find such a set I' with $|I'| = Q$. Let $\Pi = \{(x,y) \in I^2 : p_{xy} \neq 0\}$. Let $H = (I', O, V', \text{Unif.})$ be the game defined as follows: $V'(a,b|x,y) = V(a,b|x,y)$ if $(x,y) \in \Pi$. $V'(a,b|x,y) = 1$ otherwise. We have:

$$\begin{aligned}
\omega^*(G) &= \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} p_{xy} V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle \\
&\leq \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} \frac{1}{Q^2} V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle + \sum_{a,b} \sum_{(x,y)\in\Pi} (p_{xy} - \frac{1}{Q^2}) V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle \\
&\leq \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} \frac{1}{Q^2} V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle + \sum_{(x,y)\in\Pi} (p_{xy} - \frac{1}{Q^2}) \cdot 1 \\
&= \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} \frac{1}{Q^2} V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle + 1 - \frac{|\Pi|}{Q^2}.
\end{aligned}$$

Moreover,

$$\begin{aligned}
\omega^*(H) &= \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{x,y\in I'} \frac{1}{Q^2} V'(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle \\
&= \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} \frac{1}{Q^2} V'(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle + \sum_{a,b} \sum_{x,y\notin\Pi} \frac{1}{Q^2} V'(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle \\
&= \sup_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{(x,y)\in\Pi} \frac{1}{Q^2} V(a,b|x,y) \langle \phi | A_a^x \otimes B_b^y | \phi \rangle + 1 - \frac{|\Pi|}{Q^2} \\
&\geq \omega^*(G).
\end{aligned}$$

Similarly, we have $\omega^*(G^n) \leq \omega^*(H^n)$. Moreover,

$$\begin{aligned}
1-\omega^*(H) &= \inf_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{x,y\in I'} \frac{1}{Q^2}(1-V'(a,b|x,y))\langle\phi|A_a^x \otimes B_b^y|\phi\rangle \\
&= \inf_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{x,y\in \Pi} \frac{1}{Q^2}(1-V(a,b|x,y))\langle\phi|A_a^x \otimes B_b^y|\phi\rangle \\
&\geq \frac{1}{Q^2} \inf_{|\phi\rangle, A^x, B^y} \sum_{a,b} \sum_{x,y\in \Pi} p_{xy}(1-V(a,b|x,y))\langle\phi|A_a^x \otimes B_b^y|\phi\rangle \\
&= \frac{\varepsilon}{Q^2},
\end{aligned}$$

from which we have $\omega^*(H) \leq 1 - \frac{\varepsilon}{Q^2}$. Using the parallel repetition theorem on the uniform distribution, we have that

$$\omega^*(G^n) \leq \omega^*(H^n) = (1-\frac{\varepsilon^2}{Q^4})^{\Omega(\frac{n}{\log(|I'||O|)} - |\log(\varepsilon/Q)|)}.$$

Therefore, we conclude that

$$\omega^*(G^n) = (1-\varepsilon^2)^{\Omega(\frac{n}{Q^4 \log(Q\cdot|O|)} - |\log(\varepsilon/Q)|)}.$$

■

Acknowledgments

The authors wish to thank Ronald de Wolf and Anthony Leverrier for helpful suggestions. Part of this 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 Ronald de Wolf's Vidi grant 639.072.803 from the Netherlands Organization for Scientific Research (NWO).

References

[AKK+08] 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.

[BGS98] Mihir Bellare, Oded Goldreich, and Madhu Sudan. Free bits, pcps, and nonapproximability—towards tight results. *SIAM J. Comput.*, 27(3):804–915, June 1998.

[Bra12] 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.

[BYJKS04] 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.

[CSUU08] 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.

[CSWY01] 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.

[DSV13] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. 2013.

[FG99] 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.

[Hel67] C. W. Helstrom. Detection theory and quantum mechanics. 10(3):254–291, 1967.

[Hol07] 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.

[KLL+12] 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.

[KNTSZ07] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman. Interaction in quantum communication. *Information Theory, IEEE Transactions on*, 53(6):1970–1982, 2007.

[KRT08] 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.

[KV11] 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.

[MDS+13] 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.

[NS03] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67(1):012304, Jan 2003.

[PRW97] 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.

[Rao08] 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.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, June 1998.

[Raz11] Ran Raz. A counterexample to strong parallel repetition. *SIAM J. Comput.*, 40(3):771–777, June 2011.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001.

[Vad99] Salil Pravin Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, 1999. Supervisor-Shafi Goldwasser.