A parallel repetition theorem for entangled two-player one-round games under product distributions

Rahul Jain[1] Attila Pereszlényi[2] Penghui Yao[2]

[1]Centre for Quantum Technologies and Department of Computer Science, National University of Singapore

[2]Centre for Quantum Technologies, National University of Singapore

Quantum Games and Protocols Workshop, Simons Institute, Berkeley

27th February, 2014

Centre for Quantum Technologies

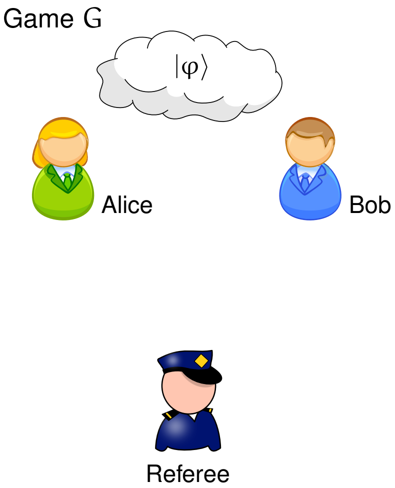
Outline

1. Introduction
   - The Model of Games
   - Parallel Repetition Theorems

Outline

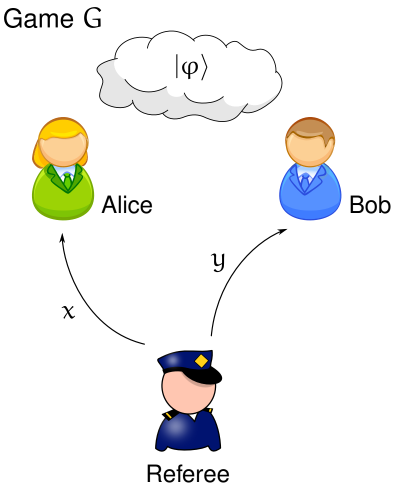
Outline

Two-Player One-Round Games



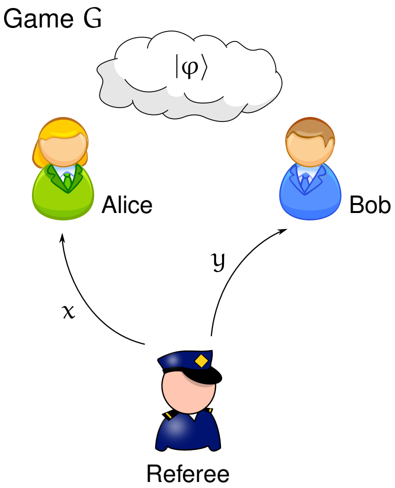
- Alice and Bob share an entangled state $|\varphi\rangle$.

Two-Player One-Round Games



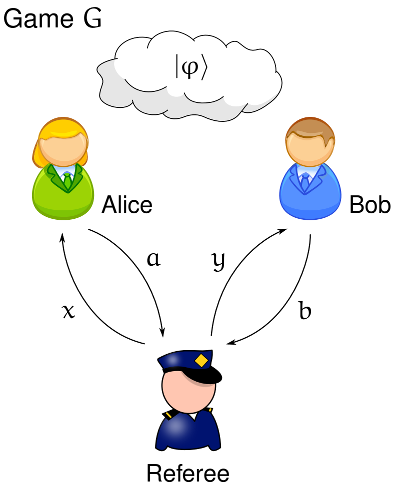
- Alice and Bob share an entangled state $|\varphi\rangle$.

Two-Player One-Round Games



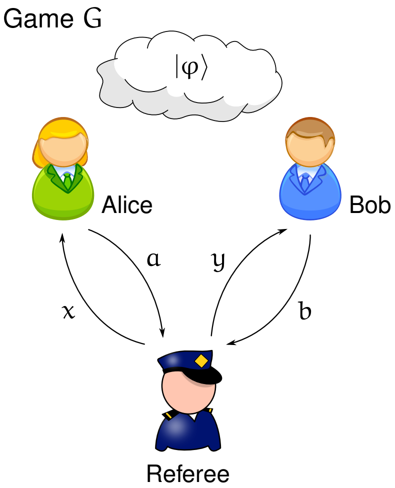
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.

Two-Player One-Round Games



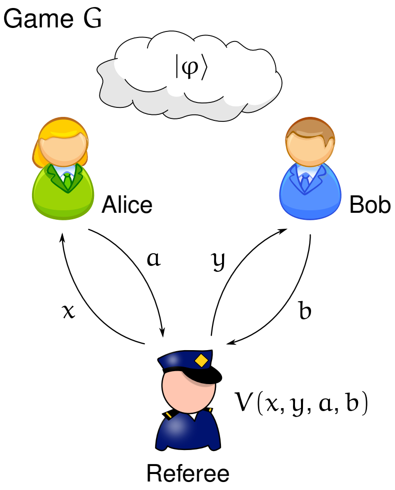
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.

Two-Player One-Round Games



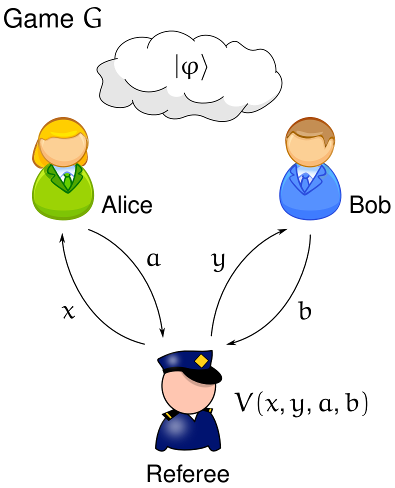
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.
- Alice and Bob answer $a \in \mathcal{A}$ and $b \in \mathcal{B}$ by performing measurements on $|\varphi\rangle$.

Two-Player One-Round Games



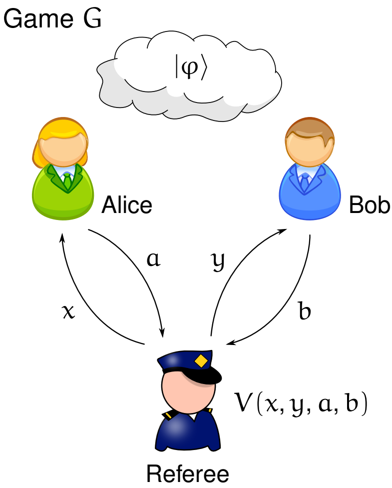
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.
- Alice and Bob answer $a \in \mathcal{A}$ and $b \in \mathcal{B}$ by performing measurements on $|\varphi\rangle$.

Two-Player One-Round Games



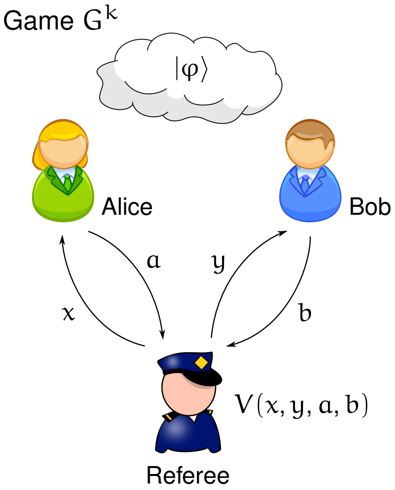
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.
- Alice and Bob answer $a \in \mathcal{A}$ and $b \in \mathcal{B}$ by performing measurements on $|\varphi\rangle$.
- They win if $V(x, y, a, b) = 1$.

Two-Player One-Round Games



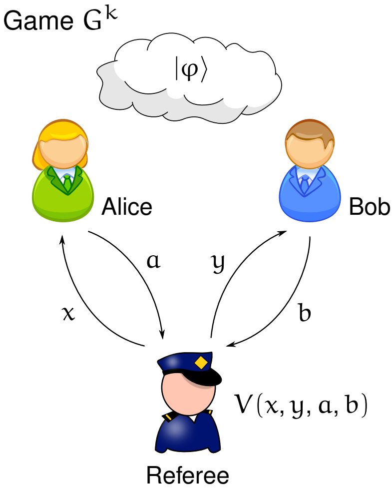
- Alice and Bob share an entangled state $|\varphi\rangle$.
- The referee selects questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to distribution μ.
- Alice and Bob answer $a \in \mathcal{A}$ and $b \in \mathcal{B}$ by performing measurements on $|\varphi\rangle$.
- They win if $V(x, y, a, b) = 1$.
- The value of G, denoted by $\omega^*(G)$, is the supremum of the achievable winning probability.

Parallel Repetition of Games



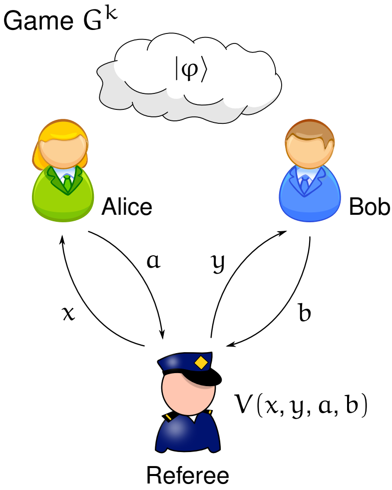
- G^k is the game where k copies of G are played in parallel.

Parallel Repetition of Games



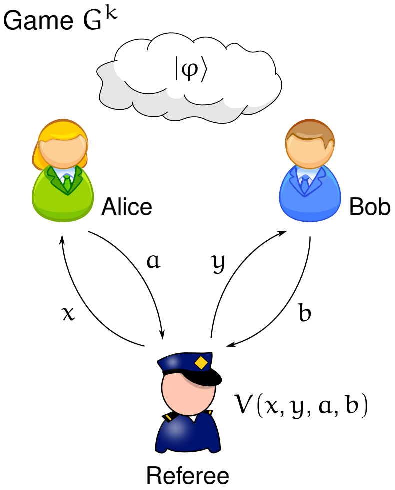
- G^k is the game where k copies of G are played in parallel.
- $x = (x_1, x_2, \dots, x_k) \in \mathcal{X}^{\times k}$, $y \in \mathcal{Y}^{\times k}$, $a \in \mathcal{A}^{\times k}$, $b \in \mathcal{B}^{\times k}$

Parallel Repetition of Games



- G^k is the game where k copies of G are played in parallel.
- $x = (x_1, x_2, \ldots, x_k) \in \mathcal{X}^{\times k}$, $y \in \mathcal{Y}^{\times k}$, $a \in \mathcal{A}^{\times k}$, $b \in \mathcal{B}^{\times k}$
- (x, y) is distributed according to $\mu^{\otimes k}$, where $\mu^{\otimes k}$ denotes k independent copies of μ.

Parallel Repetition of Games



- G^k is the game where k copies of G are played in parallel.
- $x = (x_1, x_2, \ldots, x_k) \in \mathcal{X}^{\times k}$, $y \in \mathcal{Y}^{\times k}$, $a \in \mathcal{A}^{\times k}$, $b \in \mathcal{B}^{\times k}$
- (x, y) is distributed according to $\mu^{\otimes k}$, where $\mu^{\otimes k}$ denotes k independent copies of μ.
- $V(x, y, a, b) = 1$ if the players win all the instances.

Outline

1. Introduction
   - The Model of Games
   - Parallel Repetition Theorems
2. Proof of the Main Theorem
   - Idea Behind the Proof
   - Some Details

The Basic Question

Skip this part

The Basic Question

How does $\omega^*\left(G^k\right)$ scale with k?

The Basic Question

How does $\omega^*(G^k)$ scale with k?

- Trivially, $\omega^*(G^k) \geqslant \omega^*(G)^k$.

The Basic Question

How does $\omega^*(G^k)$ scale with k?

- Trivially, $\omega^*(G^k) \geqslant \omega^*(G)^k$.
- The reverse direction doesn't hold but we can still hope to show that $\omega^*(G^k) \approx \omega^*(G)^k$.

The Basic Question

How does $\omega^*(G^k)$ scale with k?

- Trivially, $\omega^*(G^k) \geqslant \omega^*(G)^k$.
- The reverse direction doesn't hold but we can still hope to show that $\omega^*(G^k) \approx \omega^*(G)^k$.

Analogous result holds for the classical value (denoted by $\omega(G)$):

Theorem ([Raz '95] and [Holenstein '07])

$\exists$ *constant* C *s.t.*

$$\omega(G^k) \leqslant \left(1 - C(1 - \omega(G))^3\right)^{\frac{k}{\log(|\mathcal{A}| \cdot |\mathcal{B}|)}}$$

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

- Perfect parallel repetition holds for XOR games. [Cleve, Slofstra, Unger, Upadhyay ’08]

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

- Perfect parallel repetition holds for XOR games. [Cleve, Slofstra, Unger, Upadhyay ’08]
- Parallel repetition holds for the more general class of unique games [Kempe, Regev, Toner ’10]

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

- Perfect parallel repetition holds for XOR games. [Cleve, Slofstra, Unger, Upadhyay '08]
- Parallel repetition holds for the more general class of unique games [Kempe, Regev, Toner '10]
- and the even more general class of projection games [Dinur, Steurer, Vidick '13].

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

- Perfect parallel repetition holds for XOR games. [Cleve, Slofstra, Unger, Upadhyay '08]
- Parallel repetition holds for the more general class of unique games [Kempe, Regev, Toner '10]
- and the even more general class of projection games [Dinur, Steurer, Vidick '13].
- For general games, [Kempe and Vidick '11] showed a theorem where the rate of decay is inverse-polynomial. (Although not for G^k.)

Parallel Repetition Theorems for the Quantum Value

Parallel repetition theorems for the quantum value were shown for some classes of games.

- Perfect parallel repetition holds for XOR games. [Cleve, Slofstra, Unger, Upadhyay '08]
- Parallel repetition holds for the more general class of unique games [Kempe, Regev, Toner '10]
- and the even more general class of projection games [Dinur, Steurer, Vidick '13].
- For general games, [Kempe and Vidick '11] showed a theorem where the rate of decay is inverse-polynomial. (Although not for G^k.)
- [Chailloux and Scarpa '13] showed it for games where the input distribution is uniform.

Our Contribution

Theorem (Main Theorem)

For any game G, where the input distribution μ is product on $\mathcal{X} \times \mathcal{Y}$, it holds that

$$\omega^*(G^k) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{k}{\log(|\mathcal{A}| \cdot |\mathcal{B}|)}\right)} .$$

Outline

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.
- Otherwise, we show that there exists a $j \in \overline{\mathcal{C}} = [k] \setminus \mathcal{C}$ s.t. success in the j-th coordinate is bounded away from 1.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.
- Otherwise, we show that there exists a $j \in \overline{\mathcal{C}} = [k] \setminus \mathcal{C}$ s.t. success in the j-th coordinate is bounded away from 1.
  - Doing this $\Omega(k)$ times, the success probability will be exponentially small in k.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.
- Otherwise, we show that there exists a $j \in \overline{\mathcal{C}} = [k] \setminus \mathcal{C}$ s.t. success in the j-th coordinate is bounded away from 1.
  - Doing this $\Omega(k)$ times, the success probability will be exponentially small in k.
  - Let $(x', y') \in \mathcal{X} \times \mathcal{Y}$ be distributed according to μ.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.
- Otherwise, we show that there exists a $j \in \overline{\mathcal{C}} = [k] \setminus \mathcal{C}$ s.t. success in the j-th coordinate is bounded away from 1.
  - Doing this $\Omega(k)$ times, the success probability will be exponentially small in k.
  - Let $(x', y') \in \mathcal{X} \times \mathcal{Y}$ be distributed according to μ.
  - We show that the players can embed (x', y') into the j-th coordinate and generate the state of the whole system in G^k.

Broad Idea

In G^k, let us condition on success on a set $\mathcal{C} \subseteq [k]$ of coordinates.

- If the success probability is small enough then we are done.
- Otherwise, we show that there exists a $j \in \overline{\mathcal{C}} = [k] \setminus \mathcal{C}$ s.t. success in the j-th coordinate is bounded away from 1.
  - Doing this $\Omega(k)$ times, the success probability will be exponentially small in k.
  - Let $(x', y') \in \mathcal{X} \times \mathcal{Y}$ be distributed according to μ.
  - We show that the players can embed (x', y') into the j-th coordinate and generate the state of the whole system in G^k.
  - If they could win the j-th instance with high probability then they would be able to win G with high probability.

Some Simplifications

Without loss of generality:

- Let the questions and answers be part of the whole (classical-)quantum state.

Some Simplifications

Without loss of generality:

- Let the questions and answers be part of the whole (classical-)quantum state.
- Upon receiving the questions, the players apply unitaries on their parts, measure registers A and B, in the standard basis, and send the outcomes to the referee.

Some Simplifications

Without loss of generality:

- Let the questions and answers be part of the whole (classical-)quantum state.
- Upon receiving the questions, the players apply unitaries on their parts, measure registers A and B, in the standard basis, and send the outcomes to the referee.

The global state, conditioned on success in $\mathcal{C}$, after the unitaries is of the form

$$\sigma = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \mu^{\otimes k}(x, y) \, |xy\rangle\langle xy|^{\mathsf{XY}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|$$

Some Simplifications

Without loss of generality:

- Let the questions and answers be part of the whole (classical-)quantum state.
- Upon receiving the questions, the players apply unitaries on their parts, measure registers A and B, in the standard basis, and send the outcomes to the referee.

The global state, conditioned on success in $\mathcal{C}$, after the unitaries is of the form

$$\sigma = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \mu^{\otimes k}(x, y) \, |xy\rangle\langle xy|^{XY} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|$$

where (unnormalized) $|\phi_{xy}\rangle$ is shared between Alice and Bob.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x, y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle .$$

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle \,.$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}} \otimes \tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x, y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle .$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}} \otimes \tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.
- Alice and Bob get questions $(x', y') \in \mathcal{X} \times \mathcal{Y}$.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle \,.$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}} \otimes \tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.
- Alice and Bob get questions $(x', y') \in \mathcal{X} \times \mathcal{Y}$.
- Suppose they measure registers X_j and Y_j.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x\in\mathcal{X}^{\times k}, y\in\mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle\,.$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}}\otimes\tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.
- Alice and Bob get questions $(x', y') \in \mathcal{X} \times \mathcal{Y}$.
- Suppose they measure registers X_j and Y_j.
- If the outcomes of the measurements are x' and y' then they can further measure A_j and B_j and reply to the referee.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle \,.$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}} \otimes \tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.
- Alice and Bob get questions $(x', y') \in \mathcal{X} \times \mathcal{Y}$.
- Suppose they measure registers X_j and Y_j.
- If the outcomes of the measurements are x' and y' then they can further measure A_j and B_j and reply to the referee.
- This way, we embedded a single instance of G into G^k, with being conditioned on success in $\mathcal{C}$.

How to generate the state in G^k?

Let us take a strategy for G where the players share

$$|\varphi\rangle = \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x, y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\phi_{xy}\rangle .$$

- $\mathrm{Tr}_{\tilde{\mathcal{X}} \otimes \tilde{\mathcal{Y}}}(|\varphi\rangle\langle\varphi|) = \sigma$.
- Alice and Bob get questions $(x', y') \in \mathcal{X} \times \mathcal{Y}$.
- Suppose they measure registers X_j and Y_j.
- If the outcomes of the measurements are x' and y' then they can further measure A_j and B_j and reply to the referee.
- This way, we embedded a single instance of G into G^k, with being conditioned on success in $\mathcal{C}$.
  - If $\omega^*(G)$ is bounded away from 1 then success in the j-th instance is also bounded away from 1.

Generate the state without measurements?

The previous argument doesn't work because the probability of getting (x', y'), when measuring X_j and Y_j, can be very small.

Generate the state without measurements?

The previous argument doesn't work because the probability of getting (x', y'), when measuring X_j and Y_j, can be very small.

Question

Is there a way to generate the post-measurement state (approximately) without measurements?

Generate the state without measurements?

The previous argument doesn't work because the probability of getting (x', y'), when measuring X_j and Y_j, can be very small.

Question

Is there a way to generate the post-measurement state (approximately) without measurements?

Answer

Yes, if the input distribution μ is product.

How to do it without measurements?

Let $\left|\varphi_{x_j'}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x_j'. States $\left|\varphi_{y_j'}\right\rangle$ and $\left|\varphi_{x_j' y_j'}\right\rangle$ are defined similarly.

How to do it without measurements?

Let $\left|\varphi_{x_j'}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x_j'. States $\left|\varphi_{y_j'}\right\rangle$ and $\left|\varphi_{x_j' y_j'}\right\rangle$ are defined similarly.

- We show that $I\left(X_j : \text{Bob}\right)_\varphi \approx 0$ and $I\left(Y_j : \text{Alice}\right)_\varphi \approx 0$.

How to do it without measurements?

Let $\left|\varphi_{x_j'}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x_j'. States $\left|\varphi_{y_j'}\right\rangle$ and $\left|\varphi_{x_j' y_j'}\right\rangle$ are defined similarly.

- We show that $I\left(X_j : \text{Bob}\right)_{\varphi} \approx 0$ and $I\left(Y_j : \text{Alice}\right)_{\varphi} \approx 0$.
- $I\left(X_j : \text{Bob}\right)_{\varphi} \approx 0$ implies that Bob's part of $\left|\varphi_{x_j'}\right\rangle$ is mostly independent of x_j'.

How to do it without measurements?

Let $\left|\varphi_{x_j'}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x_j'. States $\left|\varphi_{y_j'}\right\rangle$ and $\left|\varphi_{x_j' y_j'}\right\rangle$ are defined similarly.

- We show that $I\left(X_j : \text{Bob}\right)_\varphi \approx 0$ and $I\left(Y_j : \text{Alice}\right)_\varphi \approx 0$.
- $I\left(X_j : \text{Bob}\right)_\varphi \approx 0$ implies that Bob's part of $\left|\varphi_{x_j'}\right\rangle$ is mostly independent of x_j'.
- By the unitary equivalence of purifications, $\exists$ unitary $U_{x_j'}$ that Alice can apply to get $\left(U_{x_j'} \otimes \mathbb{1}_{\text{Bob}}\right)|\varphi\rangle \approx \left|\varphi_{x_j'}\right\rangle$.

How to do it without measurements?

Let $\left|\varphi_{x_j'}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x_j'. States $\left|\varphi_{y_j'}\right\rangle$ and $\left|\varphi_{x_j' y_j'}\right\rangle$ are defined similarly.

- We show that $I\left(X_j : \text{Bob}\right)_\varphi \approx 0$ and $I\left(Y_j : \text{Alice}\right)_\varphi \approx 0$.
- $I\left(X_j : \text{Bob}\right)_\varphi \approx 0$ implies that Bob's part of $\left|\varphi_{x_j'}\right\rangle$ is mostly independent of x_j'.
- By the unitary equivalence of purifications, $\exists$ unitary $\mathbf{U}_{x_j'}$ that Alice can apply to get $\left(\mathbf{U}_{x_j'} \otimes \mathbb{1}_{\text{Bob}}\right)|\varphi\rangle \approx \left|\varphi_{x_j'}\right\rangle$.
- Similarly, $\exists \mathbf{V}_{y_j'}$ s.t. $\left(\mathbb{1}_{\text{Alice}} \otimes \mathbf{V}_{y_j'}\right)|\varphi\rangle \approx \left|\varphi_{y_j'}\right\rangle$.

How to do it without measurements?

Let $\left|\varphi_{x'_j}\right\rangle$ be the resulting state after Alice measures X_j in $|\varphi\rangle$ and gets x'_j. States $\left|\varphi_{y'_j}\right\rangle$ and $\left|\varphi_{x'_j y'_j}\right\rangle$ are defined similarly.

- We show that $I\left(X_j : \mathrm{Bob}\right)_{\varphi} \approx 0$ and $I\left(Y_j : \mathrm{Alice}\right)_{\varphi} \approx 0$.
- $I\left(X_j : \mathrm{Bob}\right)_{\varphi} \approx 0$ implies that Bob's part of $\left|\varphi_{x'_j}\right\rangle$ is mostly independent of x'_j.
- By the unitary equivalence of purifications, $\exists$ unitary $U_{x'_j}$ that Alice can apply to get $\left(U_{x'_j} \otimes \mathbb{1}_{\mathrm{Bob}}\right)|\varphi\rangle \approx \left|\varphi_{x'_j}\right\rangle$.
- Similarly, $\exists V_{y'_j}$ s.t. $\left(\mathbb{1}_{\mathrm{Alice}} \otimes V_{y'_j}\right)|\varphi\rangle \approx \left|\varphi_{y'_j}\right\rangle$.
- By [Jain, Radhakrishnan, Sen '08], if the distribution of $\left(x'_j, y'_j\right)$ is product then
$$\left(U_{x'_j} \otimes V_{y'_j}\right)|\varphi\rangle \approx \left|\varphi_{x'_j y'_j}\right\rangle.$$

Outline

From Measurements to Unitaries (1 Sided)

Lemma

Let μ be a probability distribution on $\mathcal{X}$. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} \sqrt{\mu(x)}\, |xx\rangle^{X\tilde{X}} \otimes |\psi_x\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and the rest of $|\psi_x\rangle$ is with Bob.

From Measurements to Unitaries (1 Sided)

Lemma

Let μ be a probability distribution on $\mathcal{X}$. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} \sqrt{\mu(x)}\, |xx\rangle^{X\tilde{X}} \otimes |\psi_x\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and the rest of $|\psi_x\rangle$ is with Bob. Let $|\varphi_x\rangle \stackrel{\text{def}}{=} |xx\rangle \otimes |\psi_x\rangle$.

From Measurements to Unitaries (1 Sided)

Lemma

Let μ be a probability distribution on $\mathcal{X}$. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} \sqrt{\mu(x)}\, |xx\rangle^{X\tilde{X}} \otimes |\psi_x\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and the rest of $|\psi_x\rangle$ is with Bob. Let $|\varphi_x\rangle \stackrel{\text{def}}{=} |xx\rangle \otimes |\psi_x\rangle$. If $I(X : \text{Bob})_\varphi \leqslant \varepsilon$ then there exist unitaries $\{U_x\}_{x \in \mathcal{X}}$ acting on Alice's space s.t.

$$\mathbb{E}_{x \leftarrow \mu}[\| |\varphi_x\rangle\langle\varphi_x| - (U_x \otimes \mathbb{1}_{\text{Bob}})\, |\varphi\rangle\langle\varphi|\, (U_x^* \otimes \mathbb{1}_{\text{Bob}}) \|_1] \leqslant 4\sqrt{\varepsilon}.$$

From Measurements to Unitaries (1 Sided)

Lemma

Let μ be a probability distribution on $\mathcal{X}$. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x\in\mathcal{X}} \sqrt{\mu(x)}\,|xx\rangle^{X\tilde{X}} \otimes |\psi_x\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and the rest of $|\psi_x\rangle$ is with Bob. Let $|\varphi_x\rangle \stackrel{\text{def}}{=} |xx\rangle \otimes |\psi_x\rangle$. If $I(X:\text{Bob})_\varphi \leqslant \varepsilon$ then there exist unitaries $\{U_x\}_{x\in\mathcal{X}}$ acting on Alice's space s.t.

$$\mathop{\mathbb{E}}_{x\leftarrow\mu}\left[\left\| |\varphi_x\rangle\langle\varphi_x| - (U_x \otimes \mathbb{1}_{\text{Bob}})\,|\varphi\rangle\langle\varphi|\,(U_x^* \otimes \mathbb{1}_{\text{Bob}}) \right\|_1\right] \leqslant 4\sqrt{\varepsilon}.$$

The proof easily follows from the unitary equivalence of purifications and Uhlmann's theorem.

From Measurements to Unitaries (2 Sided)

Lemma

Let μ be a prob. dist. on $\mathcal{X} \times \mathcal{Y}$ with marginals μ_X and μ_Y. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{\mu(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\psi_{x,y}\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and Y, $\tilde{Y}$, and the rest of $|\psi_x\rangle$ are with Bob.

From Measurements to Unitaries (2 Sided)

Lemma

Let μ be a prob. dist. on $\mathcal{X} \times \mathcal{Y}$ with marginals μ_X and μ_Y. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{\mu(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\psi_{x,y}\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and Y, $\tilde{Y}$, and the rest of $|\psi_x\rangle$ are with Bob. If $I(X : \text{Bob})_\varphi \leqslant \varepsilon$ and $I(Y : \text{Alice})_\varphi \leqslant \varepsilon$ then there exist unitaries $\{U_x\}_{x \in \mathcal{X}}$ on Alice's space and $\{V_y\}_{y \in \mathcal{Y}}$ on Bob's space

From Measurements to Unitaries (2 Sided)

Lemma

Let μ be a prob. dist. on $\mathcal{X} \times \mathcal{Y}$ with marginals μ_X and μ_Y. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} \sqrt{\mu(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\psi_{x,y}\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and Y, $\tilde{Y}$, and the rest of $|\psi_x\rangle$ are with Bob. If $\mathrm{I}(X:\mathrm{Bob})_\varphi \leqslant \varepsilon$ and $\mathrm{I}(Y:\mathrm{Alice})_\varphi \leqslant \varepsilon$ then there exist unitaries $\{\mathbf{U}_x\}_{x\in\mathcal{X}}$ on Alice's space and $\{\mathbf{V}_y\}_{y\in\mathcal{Y}}$ on Bob's space s.t.

$$\mathop{\mathbb{E}}_{(x,y)\leftarrow\mu}\left[\left\| |\varphi_{x,y}\rangle\langle\varphi_{x,y}| - (\mathbf{U}_x \otimes \mathbf{V}_y)\,|\varphi\rangle\langle\varphi|\,(\mathbf{U}_x^* \otimes \mathbf{V}_y^*)\right\|_1\right]$$

$$\leqslant 8\sqrt{\varepsilon} + 2\,\|\mu - \mu_X \otimes \mu_Y\|_1 .$$

From Measurements to Unitaries (2 Sided)

Lemma

Let μ be a prob. dist. on $\mathcal{X} \times \mathcal{Y}$ with marginals μ_X and μ_Y. Let

$$|\varphi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{\mu(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes |\psi_{x,y}\rangle$$

be shared by Alice and Bob, where X, $\tilde{X}$, and some part of $|\psi_x\rangle$ are with Alice and Y, $\tilde{Y}$, and the rest of $|\psi_x\rangle$ are with Bob. If $I(X : \mathrm{Bob})_\varphi \leqslant \varepsilon$ and $I(Y : \mathrm{Alice})_\varphi \leqslant \varepsilon$ then there exist unitaries $\{\mathbf{U}_x\}_{x \in \mathcal{X}}$ on Alice's space and $\{\mathbf{V}_y\}_{y \in \mathcal{Y}}$ on Bob's space s.t.

$$\mathop{\mathbb{E}}_{(x,y) \leftarrow \mu} \left[\left\| |\varphi_{x,y}\rangle\langle\varphi_{x,y}| - (\mathbf{U}_x \otimes \mathbf{V}_y)\, |\varphi\rangle\langle\varphi|\, (\mathbf{U}_x^* \otimes \mathbf{V}_y^*) \right\|_1 \right]$$
$$\leqslant 8\sqrt{\varepsilon} + 2 \left\| \mu - \mu_X \otimes \mu_Y \right\|_1 .$$

Proved by [Jain, Radhakrishnan, Sen '08].

Key Lemma

Our main theorem follows from the following lemma. Show theorem

Lemma (Key Lemma)

Let $1/10 > \delta_1, \delta_2, \delta_3 > 0$ *s.t.* $\delta_3 = \delta_2 + \delta_1 \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}|)$. *Let* $k' \stackrel{\text{def}}{=} \lfloor \delta_1 k \rfloor$.

Key Lemma

Our main theorem follows from the following lemma. ◂ Show theorem

Lemma (Key Lemma)

Let $1/10 > \delta_1, \delta_2, \delta_3 > 0$ *s.t.* $\delta_3 = \delta_2 + \delta_1 \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}|)$. *Let* $k' \stackrel{\text{def}}{=} \lfloor \delta_1 k \rfloor$. *Given any quantum strategy for* G^k, *there exists* $\{i_1, \ldots, i_{k'}\}$ *s.t. for each* $1 \leqslant l \leqslant k' - 1$, *either*

$$\Pr\left[T^{(l)} = 1\right] \leqslant 2^{-\delta_2 k}$$

where $T_i \in \{0, 1\}$ *indicates success in the* i*-th repetition and* $T^{(l)} \stackrel{\text{def}}{=} \prod_{j=1}^{l} T_{i_j}$.

Key Lemma

Our main theorem follows from the following lemma. ◂ Show theorem

Lemma (Key Lemma)

Let $1/10 > \delta_1, \delta_2, \delta_3 > 0$ *s.t.* $\delta_3 = \delta_2 + \delta_1 \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}|)$. *Let* $k' \stackrel{\text{def}}{=} \lfloor \delta_1 k \rfloor$. *Given any quantum strategy for* G^k, *there exists* $\{i_1, \ldots, i_{k'}\}$ *s.t. for each* $1 \leqslant l \leqslant k' - 1$, *either*

$$\Pr\left[T^{(l)} = 1\right] \leqslant 2^{-\delta_2 k} \qquad \textit{or}$$

$$\Pr\left[T_{i_{l+1}} = 1 \middle| T^{(l)} = 1\right] \leqslant \omega^*(G) + 12\sqrt{10\delta_3}$$

where $T_i \in \{0, 1\}$ *indicates success in the* i*-th repetition and* $T^{(l)} \stackrel{\text{def}}{=} \prod_{j=1}^{l} T_{i_j}$.

Proof of the Key Lemma

Skip the proof

Proof of the Key Lemma

Suppose that we already identified l coordinates and we want to find the $(l + 1)$-th coordinate with the given properties.

Proof of the Key Lemma

Suppose that we already identified l coordinates and we want to find the $(l+1)$-th coordinate with the given properties.

- Assume $q \stackrel{\text{def}}{=} \Pr\left[T^{(l)} = 1\right] > 2^{-\delta_2 k}$ as otherwise we are done.

Proof of the Key Lemma

Suppose that we already identified l coordinates and we want to find the $(l+1)$-th coordinate with the given properties.

- Assume $q \stackrel{\text{def}}{=} \Pr\left[T^{(l)} = 1\right] > 2^{-\delta_2 k}$ as otherwise we are done.
- Let $\mathcal{C} \stackrel{\text{def}}{=} \{i_1, \ldots, i_l\}$.

Proof of the Key Lemma

Suppose that we already identified l coordinates and we want to find the $(l+1)$-th coordinate with the given properties.

- Assume $q \stackrel{\text{def}}{=} \Pr\left[T^{(l)} = 1\right] > 2^{-\delta_2 k}$ as otherwise we are done.
- Let $\mathcal{C} \stackrel{\text{def}}{=} \{i_1, \ldots, i_l\}$.

The purified state after the unitaries is

$$|\theta\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |xxyy\rangle^{X\tilde{X}Y\tilde{Y}} \otimes \sum_{a_{\mathcal{C}} \in \mathcal{A}^{\times l}, b_{\mathcal{C}} \in \mathcal{B}^{\times l}} |a_{\mathcal{C}} b_{\mathcal{C}}\rangle^{A_{\mathcal{C}} B_{\mathcal{C}}} \otimes \left|\gamma_{x,y,a_{\mathcal{C}},b_{\mathcal{C}}}\right\rangle^{E_A E_B}.$$

Proof of the Key Lemma

Suppose that we already identified l coordinates and we want to find the $(l+1)$-th coordinate with the given properties.

- Assume $q \stackrel{\text{def}}{=} \Pr\left[T^{(l)} = 1\right] > 2^{-\delta_2 k}$ as otherwise we are done.
- Let $\mathcal{C} \stackrel{\text{def}}{=} \{i_1, \ldots, i_l\}$.

The purified state after the unitaries is

$$|\theta\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}^{\times k}, y \in \mathcal{Y}^{\times k}} \sqrt{\mu^{\otimes k}(x,y)}\, |x x y y\rangle^{X\tilde{X}Y\tilde{Y}} \otimes \sum_{a_\mathcal{C} \in \mathcal{A}^{\times l}, b_\mathcal{C} \in \mathcal{B}^{\times l}} |a_\mathcal{C} b_\mathcal{C}\rangle^{A_\mathcal{C} B_\mathcal{C}} \otimes \left|\gamma_{x,y,a_\mathcal{C},b_\mathcal{C}}\right\rangle^{E_A E_B}.$$

Conditioning on success in $\mathcal{C}$ gives us the state

$$|\varphi\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{q}} \sum_{x,y} \sqrt{\mu^{\otimes k}(x,y)}\, |x x y y\rangle \sum_{\substack{a_\mathcal{C}, b_\mathcal{C} \text{ s.t.} \\ \prod_{i \in \mathcal{C}} T_i = 1}} |a_\mathcal{C} b_\mathcal{C}\rangle \otimes \left|\gamma_{x,y,a_\mathcal{C},b_\mathcal{C}}\right\rangle.$$

Lemma about the Relative Entropy

From $q > 2^{-\delta_2 k}$, we show the following simple lemma.

Lemma

$$\mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \middle\| \theta_{x_{\mathcal{C}},y_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \right) \right] \leqslant \delta_3 k$$

Lemma about the Relative Entropy

From $q > 2^{-\delta_2 k}$, we show the following simple lemma.

Lemma

$$\mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \middle\| \theta_{x_{\mathcal{C}},y_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \right) \right] \leqslant \delta_3 k$$

Intuitively,

- going from θ to φ causes a difference of at most $-\log q < \delta_2 k$.

Lemma about the Relative Entropy

From $q > 2^{-\delta_2 k}$, we show the following simple lemma.

Lemma

$$\mathop{\mathbb{E}}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C} \leftarrow \varphi^{X_\mathcal{C} Y_\mathcal{C} A_\mathcal{C} B_\mathcal{C}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_\mathcal{C}, y_\mathcal{C}} \right) \right] \leqslant \delta_3 k$$

Intuitively,

- going from θ to φ causes a difference of at most $-\log q < \delta_2 k$.
- further measuring $A_\mathcal{C}$ and $B_\mathcal{C}$ results in a difference of at most $|\mathcal{C}| \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}|) \leqslant \delta_1 k \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}|)$.

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

Skip

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$\delta_3 k \geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}}, y_{\mathcal{C}}, a_{\mathcal{C}}, b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}} Y_{\mathcal{C}} A_{\mathcal{C}} B_{\mathcal{C}}}} \left[S\left(\varphi_{x_{\mathcal{C}}, y_{\mathcal{C}}, a_{\mathcal{C}}, b_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \middle\| \theta_{x_{\mathcal{C}}, y_{\mathcal{C}}}^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B} \right) \right]$$

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$\begin{aligned}\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\ &\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathsf{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{X(\mathsf{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right]\end{aligned}$$

where Bob $\stackrel{\text{def}}{=} Y\tilde{Y}_{\overline{\mathcal{C}}}E_B$.

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$\begin{aligned}\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}\leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}}\left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}}\middle\|\theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}}}\right)\right]\\ &\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}}\middle\|\theta^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}}}\right)\right]\\ &= \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}}\middle\|\theta^{X}_{x_{\mathcal{C}},y_{\mathcal{C}}}\otimes\theta^{\mathrm{Bob}}_{x_{\mathcal{C}},y_{\mathcal{C}}}\right)\right]\end{aligned}$$

where Bob $\stackrel{\text{def}}{=} Y\tilde{Y}_{\overline{\mathcal{C}}}E_B$.

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$
\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C} \leftarrow \varphi^{X_\mathcal{C} Y_\mathcal{C} A_\mathcal{C} B_\mathcal{C}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_\mathcal{C}, y_\mathcal{C}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \middle\| \theta^{X(\mathrm{Bob})}_{x_\mathcal{C}, y_\mathcal{C}} \right) \right] \\
&= \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \middle\| \theta^{X}_{x_\mathcal{C}, y_\mathcal{C}} \otimes \theta^{\mathrm{Bob}}_{x_\mathcal{C}, y_\mathcal{C}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \middle\| \varphi^{X}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \otimes \varphi^{\mathrm{Bob}}_{x_\mathcal{C}, y_\mathcal{C}, a_\mathcal{C}, b_\mathcal{C}} \right) \right]
\end{aligned}
$$

where Bob $\stackrel{\text{def}}{=} Y\tilde{Y}_{\overline{\mathcal{C}}}E_B$.

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&= \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{X}_{x_{\mathcal{C}},y_{\mathcal{C}}} \otimes \theta^{\mathrm{Bob}}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \varphi^{X}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \otimes \varphi^{\mathrm{Bob}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \right) \right] \\
&= I(X : \mathrm{Bob} | X_{\mathcal{C}} Y_{\mathcal{C}} A_{\mathcal{C}} B_{\mathcal{C}})_{\varphi}
\end{aligned}$$

where $\mathrm{Bob} \stackrel{\mathrm{def}}{=} Y\tilde{Y}_{\overline{\mathcal{C}}}E_B$.

Upper Bound for the Mutual Information

Using the previous lemma, we can show the required upper bound for the mutual information.

$$
\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_AE_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&= \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{X}_{x_{\mathcal{C}},y_{\mathcal{C}}} \otimes \theta^{\mathrm{Bob}}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathbb{E}\left[S\left(\varphi^{X(\mathrm{Bob})}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \varphi^{X}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \otimes \varphi^{\mathrm{Bob}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \right) \right] \\
&= I(X : \mathrm{Bob} | X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}})_{\varphi} \\
&= \sum_{i \in \overline{\mathcal{C}}} I\left(X_i : \mathrm{Bob} \middle| X_{\mathcal{C}\cup[i-1]}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}\right)_{\varphi}
\end{aligned}
$$

where Bob $\stackrel{\text{def}}{=} Y\tilde{Y}_{\overline{\mathcal{C}}}E_B$.

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

Skip

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

$$\delta_3 k \geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}}, y_{\mathcal{C}}, a_{\mathcal{C}}, b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}} Y_{\mathcal{C}} A_{\mathcal{C}} B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}} E_A E_B}_{x_{\mathcal{C}}, y_{\mathcal{C}}, a_{\mathcal{C}}, b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}} E_A E_B}_{x_{\mathcal{C}}, y_{\mathcal{C}}} \right) \right]$$

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

$$\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right]
\end{aligned}$$

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

$$
\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&= \sum_{i \in \overline{\mathcal{C}}} \mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[S\left(\varphi^{X_i Y_i}_{r_i} \middle\| \theta^{X_i Y_i}_{x_{\mathcal{C}\cup[i-1]},y_{\mathcal{C}\cup[i-1]}} \right) \right]
\end{aligned}
$$

where $R_i \stackrel{\text{def}}{=} X_{\mathcal{C}\cup[i-1]} Y_{\mathcal{C}\cup[i-1]} A_{\mathcal{C}} B_{\mathcal{C}}$.

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

$$\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&= \sum_{i\in\overline{\mathcal{C}}} \mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[S\left(\varphi^{X_i Y_i}_{r_i} \middle\| \theta^{X_i Y_i}_{x_{\mathcal{C}\cup[i-1]},y_{\mathcal{C}\cup[i-1]}} \right) \right] \\
&\geqslant \sum_{i\in\overline{\mathcal{C}}} \mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[\left\| \varphi^{X_i Y_i}_{r_i} - \mu \right\|_1^2 \right]
\end{aligned}$$

where $R_i \stackrel{\text{def}}{=} X_{\mathcal{C}\cup[i-1]} Y_{\mathcal{C}\cup[i-1]} A_{\mathcal{C}} B_{\mathcal{C}}$.

Distribution of Questions

Using the same lemma, we show that for most of the coordinates in $\overline{\mathcal{C}}$ the distribution of questions is close to μ in $|\varphi\rangle$.

$$
\begin{aligned}
\delta_3 k &\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY\tilde{X}_{\overline{\mathcal{C}}}\tilde{Y}_{\overline{\mathcal{C}}}E_A E_B}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&\geqslant \mathop{\mathbb{E}}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}} \leftarrow \varphi^{X_{\mathcal{C}}Y_{\mathcal{C}}A_{\mathcal{C}}B_{\mathcal{C}}}} \left[S\left(\varphi^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}},a_{\mathcal{C}},b_{\mathcal{C}}} \middle\| \theta^{XY}_{x_{\mathcal{C}},y_{\mathcal{C}}} \right) \right] \\
&= \sum_{i \in \overline{\mathcal{C}}} \mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[S\left(\varphi^{X_i Y_i}_{r_i} \middle\| \theta^{X_i Y_i}_{x_{\mathcal{C}\cup[i-1]},y_{\mathcal{C}\cup[i-1]}} \right) \right] \\
&\geqslant \sum_{i \in \overline{\mathcal{C}}} \mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[\left\| \varphi^{X_i Y_i}_{r_i} - \mu \right\|_1^2 \right] \\
&\geqslant \sum_{i \in \overline{\mathcal{C}}} \left(\mathop{\mathbb{E}}_{r_i \leftarrow \varphi^{R_i}} \left[\left\| \varphi^{X_i Y_i}_{r_i} - \mu \right\|_1 \right] \right)^2
\end{aligned}
$$

where $R_i \stackrel{\text{def}}{=} X_{\mathcal{C}\cup[i-1]} Y_{\mathcal{C}\cup[i-1]} A_{\mathcal{C}} B_{\mathcal{C}}$.

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$I\left(X_j : \text{Bob}\middle|R_j\right)_{\varphi} \leqslant 10\delta_3$$

where $R_j = X_{\mathcal{C}\cup[j-1]}Y_{\mathcal{C}\cup[j-1]}A_{\mathcal{C}}B_{\mathcal{C}}$.

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$I\left(X_j : \text{Bob} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$
$$I\left(Y_j : \text{Alice} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$

where $R_j = X_{\mathcal{C}\cup[j-1]} Y_{\mathcal{C}\cup[j-1]} A_{\mathcal{C}} B_{\mathcal{C}}$.

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$I\left(X_j : \text{Bob} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$
$$I\left(Y_j : \text{Alice} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$
$$\left\| \varphi^{X_j Y_j} - \mu \right\|_1 \leqslant \mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}} \left[\left\| \varphi_{r_j}^{X_j Y_j} - \mu \right\|_1 \right] \leqslant \sqrt{10\delta_3}$$

where $R_j = X_{\mathcal{C}\cup[j-1]} Y_{\mathcal{C}\cup[j-1]} A_{\mathcal{C}} B_{\mathcal{C}}$.

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$\begin{aligned} I\left(X_j : \text{Bob} \middle| R_j\right)_{\varphi} &\leqslant 10\delta_3 \\ I\left(Y_j : \text{Alice} \middle| R_j\right)_{\varphi} &\leqslant 10\delta_3 \\ \left\|\varphi^{X_j Y_j} - \mu\right\|_1 \leqslant \mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}} \left[\left\|\varphi_{r_j}^{X_j Y_j} - \mu\right\|_1\right] &\leqslant \sqrt{10\delta_3} \end{aligned}$$

where $R_j = X_{\mathcal{C}\cup[j-1]} Y_{\mathcal{C}\cup[j-1]} A_{\mathcal{C}} B_{\mathcal{C}}$. By similar arguments as in the previous slide, we also have

$$\mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}} \left[\left\|\varphi_{r_j}^{X_j Y_j} - \varphi_{r_j}^{X_j} \otimes \varphi_{r_j}^{Y_j}\right\|_1\right] \leqslant \sqrt{10\delta_3}$$

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$\mathrm{I}\left(X_j : \text{Bob} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$
$$\mathrm{I}\left(Y_j : \text{Alice} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$
$$\left\|\varphi^{X_jY_j} - \mu\right\|_1 \leqslant \mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}}\left[\left\|\varphi^{X_jY_j}_{r_j} - \mu\right\|_1\right] \leqslant \sqrt{10\delta_3}$$

where $R_j = X_{\mathcal{C}\cup[j-1]}Y_{\mathcal{C}\cup[j-1]}A_{\mathcal{C}}B_{\mathcal{C}}$. By similar arguments as in the previous slide, we also have

$$\mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}}\left[\left\|\varphi^{X_jY_j}_{r_j} - \varphi^{X_j}_{r_j} \otimes \varphi^{Y_j}_{r_j}\right\|_1\right] \leqslant \sqrt{10\delta_3}$$
$$\mathop{\mathbb{E}}_{x_j,y_j \leftarrow \varphi^{X_jY_j}}\left[\left\|\varphi^{R_j}_{x_j,y_j} - \varphi^{R_j}\right\|_1\right] \leqslant \sqrt{10\delta_3}.$$

Final Upper Bounds

By Markov's inequality, there exists a $j \in \overline{\mathcal{C}}$ s.t.

$$I\left(X_j : \text{Bob} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$

$$I\left(Y_j : \text{Alice} \middle| R_j\right)_\varphi \leqslant 10\delta_3$$

$$\left\|\varphi^{X_j Y_j} - \mu\right\|_1 \leqslant \mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}} \left[\left\|\varphi_{r_j}^{X_j Y_j} - \mu\right\|_1\right] \leqslant \sqrt{10\delta_3}$$

where $R_j = X_{\mathcal{C}\cup[j-1]} Y_{\mathcal{C}\cup[j-1]} A_{\mathcal{C}} B_{\mathcal{C}}$. By similar arguments as in the previous slide, we also have

$$\mathop{\mathbb{E}}_{r_j \leftarrow \varphi^{R_j}} \left[\left\|\varphi_{r_j}^{X_j Y_j} - \varphi_{r_j}^{X_j} \otimes \varphi_{r_j}^{Y_j}\right\|_1\right] \leqslant \sqrt{10\delta_3}$$

$$\mathop{\mathbb{E}}_{x_j, y_j \leftarrow \varphi^{X_j Y_j}} \left[\left\|\varphi_{x_j, y_j}^{R_j} - \varphi^{R_j}\right\|_1\right] \leqslant \sqrt{10\delta_3}.$$

With these, and by treating R_j as public coins, it's easy to show that we can embed G into G^k.

Summary

We proved the following parallel repetition theorem.

Theorem (Main Theorem)

For any game G, where the input distribution μ is product on $\mathcal{X} \times \mathcal{Y}$, it holds that

$$\omega^*(G^k) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{k}{\log(|\mathcal{A}|\cdot|\mathcal{B}|)}\right)}.$$

Summary

We proved the following parallel repetition theorem.

Theorem (Main Theorem)

For any game G, where the input distribution μ is product on $\mathcal{X} \times \mathcal{Y}$, it holds that

$$\omega^*\left(G^k\right) = \left(1 - \left(1 - \omega^*(G)\right)^3\right)^{\Omega\left(\frac{k}{\log(|\mathcal{A}|\cdot|\mathcal{B}|)}\right)}.$$

It improves upon the result of [Chailloux and Scarpa '13] by

- generalizing it from uniform to product distributions

Summary

We proved the following parallel repetition theorem.

Theorem (Main Theorem)

For any game G, where the input distribution μ is product on $\mathcal{X} \times \mathcal{Y}$, it holds that

$$\omega^*(G^k) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{k}{\log(|\mathcal{A}|\cdot|\mathcal{B}|)}\right)}.$$

It improves upon the result of [Chailloux and Scarpa '13] by

- generalizing it from uniform to product distributions and by
- removing the dependence on $|\mathcal{X}|$ and $|\mathcal{Y}|$.

Summary

We proved the following parallel repetition theorem.

Theorem (Main Theorem)

For any game G, where the input distribution μ is product on $\mathcal{X} \times \mathcal{Y}$, it holds that

$$\omega^*(G^k) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{k}{\log(|\mathcal{A}| \cdot |\mathcal{B}|)}\right)}.$$

It improves upon the result of [Chailloux and Scarpa '13] by

- generalizing it from uniform to product distributions and by
- removing the dependence on $|\mathcal{X}|$ and $|\mathcal{Y}|$.

A parallel repetition theorem for arbitrary games where the exponent only depends on k and $|\mathcal{A}| \cdot |\mathcal{B}|$ is still unknown.

Thank you for your attention!

The manuscript is available at arXiv:1311.6309.