Chapter 1

Introduction

0000

Part I

Preliminaries

0002

1.1 Introduction

In this chapter we give an introduction. [edit test 17]

0003

1.2 Notation

This is an equation:

0004

$$|\phi_d\rangle \;=\; \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle \;. \tag{1.2.0.1}$$

Part II

Background

Chapter 2

Nonlocal games

0006 We introduce definitions associated with nonlocal games and strategies that will be used throughout.
0007

2.1 Games and strategies

0008 **Definition 2.1.1** (Two-player one-round games)**.** A *two-player one-round game* $\mathfrak{G}$ is specified by a tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ where

1. $\mathcal{X}$ and $\mathcal{Y}$ are finite sets (called the *question alphabets*),
2. $\mathcal{A}$ and $\mathcal{B}$ are finite sets (called the *answer alphabets*),
3. μ is a probability distribution over $\mathcal{X} \times \mathcal{Y}$ (called the *question distribution*), and
4. $D : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$ is a function (called the *decision predicate*).

0009 **Definition 2.1.2** (Tensor product strategies)**.** A *tensor product strategy* S for a game $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ is a tuple $(|\psi\rangle, A, B)$ where

- $|\psi\rangle$ is a pure quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B$ for finite dimensional complex Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$,
- A is a set $\{A^x\}$ such that for every $x \in \mathcal{X}$, $A^x = \{A^x_a\}_{a \in \mathcal{A}}$ is a POVM over $\mathcal{H}_A$, and
- B is a set $\{B^y\}$ such that for every $y \in \mathcal{Y}$, $B^y = \{B^y_b\}_{b \in \mathcal{B}}$ is a POVM over $\mathcal{H}_B$.

000A **Definition 2.1.3** (Tensor product value)**.** The *tensor product value* of a tensor product strategy $S = (|\psi\rangle, A, B)$ with respect to a game $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ is defined as

$$\mathrm{val}^*(\mathfrak{G}, S) = \sum_{x,\, y,\, a,\, b} \mu(x, y)\, D(x, y, a, b)\, \langle\psi| A^x_a \otimes B^y_b\, |\psi\rangle \ .$$

For $v \in [0,1]$ we say that the strategy S *passes (or wins)* $\mathfrak{G}$ *with probability* v *if* $\mathrm{val}^*(\mathfrak{G}, S) \geq v$. The *tensor product value* of $\mathfrak{G}$ is defined as

$$\mathrm{val}^*(\mathfrak{G}) = \sup_S \mathrm{val}^*(\mathfrak{G}, S) \ ,$$

where the supremum is taken over all tensor product strategies S for $\mathfrak{G}$.

Remark 2.1.4. Unless specified otherwise, all strategies considered in this paper are tensor product strategies, and we simply call them *strategies*. Similarly, we refer to $\mathrm{val}^*(\mathfrak{G})$ as the *value* of the game $\mathfrak{G}$.

Definition 2.1.5 (Projective strategies)**.** We say that a strategy $S = (|\psi\rangle, A, B)$ is *projective* if all the measurements $\{A_a^x\}_a$ and $\{B_b^y\}_b$ are projective. 000B

Remark 2.1.6. A game $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ is *symmetric* if the question and answer alphabets are the same for both players (i.e. $\mathcal{X} = \mathcal{Y}$ and $\mathcal{A} = \mathcal{B}$), the distribution μ is symmetric (i.e. $\mu(x,y) = \mu(y,x)$), and the decision predicate D treats both players symmetrically (i.e. for all x, y, a, b, $D(x,y,a,b) = D(y,x,b,a)$). Furthermore, we call a strategy $S = (|\psi\rangle, A, B)$ *symmetric* if $|\psi\rangle$ is a state in $\mathcal{H} \otimes \mathcal{H}$, for some Hilbert space $\mathcal{H}$, that is invariant under permutation of the two factors, and the measurement operators of both players are identical. We specify symmetric games $\mathfrak{G}$ and symmetric strategies S using a more compact notation: we write $\mathfrak{G} = (\mathcal{X}, \mathcal{A}, \mu, D)$ and $S = (|\psi\rangle, M)$ where M denotes the set of measurement operators for both players. 000C

Lemma 2.1.7. *Let* $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ *be a symmetric game such that* $\mathrm{val}^*(\mathfrak{G}) = 1 - \varepsilon$ *for some* $\varepsilon \geq 0$*. Then there exists a symmetric and projective strategy* $S = (|\psi\rangle, M)$ *such that* $\mathrm{val}^*(\mathfrak{G}, S) \geq 1 - 2\varepsilon$. 000D

Proof. By definition there exists a strategy $S' = (|\psi'\rangle, A, B)$ such that $\mathrm{val}^*(\mathfrak{G}, S') \geq 1 - 2\varepsilon$. Using Naimark's theorem (for example as formulated in [**?**, Theorem 4.2]) we can assume without loss of generality that $|\psi'\rangle \in \mathbb{C}^d_{A'} \otimes \mathbb{C}^d_{B'}$ for some integer d and that for every x and y, A^x and B^y is a projective measurement. Let

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_A|1\rangle_B|\psi'\rangle_{A'B'} + |1\rangle_A|0\rangle_B|\psi'_\tau\rangle_{A'B'}\big) \in (\mathbb{C}^2_A \otimes \mathbb{C}^d_{A'}) \otimes (\mathbb{C}^2_B \otimes \mathbb{C}^d_{B'}) \ ,$$

where $|\psi'_\tau\rangle$ is obtained from $|\psi\rangle$ by permuting the two players' registers. Observe that $|\psi\rangle$ is invariant under permutation of AA' and BB'.

For any question $x \in \mathcal{X} = \mathcal{Y}$, define the measurement $M^x = \{M_a^x\}_{a \in \mathcal{A}}$ acting on the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^d$ as follows:

$$M_a^x = |0\rangle\langle 0| \otimes A_a^x + |1\rangle\langle 1| \otimes B_a^x \ .$$

When Alice receives question x, she measures M^x on registers AA', and when Bob receives question y, he measures M^y on registers BB'. Using that by assumption the decision predicate D for $\mathfrak{G}$ is symmetric, it is not hard to verify that $\mathrm{val}^*(\mathfrak{G}, S) = \mathrm{val}^*(\mathfrak{G}, S')$. □

000E **Definition 2.1.8.** Let $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ be a game, and let $S = (|\psi\rangle, A, B)$ be a strategy for $\mathfrak{G}$ such that the spaces $\mathcal{H}_A \simeq \mathcal{H}_B$ canonically. Let $S \subseteq \mathcal{X} \times \mathcal{Y}$ denote the support of the question distribution μ, i.e. the set of (x, y) such that $\mu(x, y) > 0$. We say that S is a *commuting strategy for* $\mathfrak{G}$ if for all question pairs $(x, y) \in S$, we have $[A_a^x, B_b^y] = 0$ for all $a \in \mathcal{A}, b \in \mathcal{B}$, where $[A, B] = AB - BA$ denotes the commutator.

000F **Definition 2.1.9** (Consistent measurements)**.** Let $\mathcal{A}$ be a finite set, let $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ a state, and $\{M_a\}_{a\in\mathcal{A}}$ a projective measurement on $\mathcal{H}$. We say that $\{M_a\}_{a\in\mathcal{A}}$ *is consistent on* $|\psi\rangle$ if and only if

$$\forall a \in \mathcal{A}\ , \quad M_a \otimes \mathrm{Id}_B\ |\psi\rangle = \mathrm{Id}_A \otimes M_a\, |\psi\rangle\ .$$

000G **Definition 2.1.10** (Consistent strategies)**.** Let $S = (|\psi\rangle, A, B)$ be a projective strategy with state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$, for some Hilbert space $\mathcal{H}$, which is defined on question alphabets $\mathcal{X}$ and $\mathcal{Y}$ and answer alphabets $\mathcal{A}$ and $\mathcal{B}$, respectively. We say that the strategy S is *consistent* if for all $x \in \mathcal{X}$, the measurement $\{A_a^x\}_{a\in\mathcal{A}}$ is consistent on $|\psi\rangle$ and if for all $y \in \mathcal{Y}$, the measurement $\{B_b^y\}_{b\in\mathcal{B}}$ is consistent on $|\psi\rangle$.

000H **Definition 2.1.11.** We say that a strategy S for a game $\mathfrak{G}$ is *PCC* if it is projective, consistent, and commuting for $\mathfrak{G}$. Additionally, we say that a PCC strategy S is *SPCC* if it is furthermore symmetric.

Remark 2.1.12. A strategy $S = (|\psi\rangle, A, B)$ for a symmetric game $\mathfrak{G} = (\mathcal{X}, \mathcal{X}, \mathcal{A}, \mathcal{A}, \mu, D)$ is called *synchronous* if it holds that for every $x \in \mathcal{X}$ and $a \neq b \in \mathcal{A}$, $\langle\psi|A_a^x \otimes B_b^x|\psi\rangle = 0$; in other words, the players never return different answers when simultaneously asked the same question. As shown in [**?**] the condition for a finite-dimensional strategy of being synchronous is equivalent to the condition that it is projective, consistent, and moreover $|\psi\rangle$ is a maximally entangled state. (The equivalence is extended to infinite-dimensional strategies, as well as correlations induced by limits of finite-dimensional strategies, in [**?**].)

000J **Definition 2.1.13** (Entanglement requirements of a game)**.** For all games $\mathfrak{G}$ and $\nu \in [0, 1]$, let $\mathcal{E}(\mathfrak{G}, \nu)$ denote the minimum integer d such that there exists a finite dimensional tensor product strategy S that achieves success probability at least ν in the game $\mathfrak{G}$ with a state $|\psi\rangle$ whose Schmidt rank is at most d. If there is no finite dimensional strategy that achieves success probability ν, then define $\mathcal{E}(\mathfrak{G}, \nu)$ to be ∞.

000K

2.2 Distance measures

We introduce several distance measures that are used throughout.

000L **Definition 2.2.1** (Distance between states)**.**

Let $\{|\psi_n\rangle\}_{n\in\mathbb{N}}$ and $\{|\psi'_n\rangle\}_{n\in\mathbb{N}}$ be two families of states in the same space $\mathcal{H}$. For some function $\delta : \mathbb{N} \to [0,1]$ we say that $\{|\psi_n\rangle\}$ and $\{|\psi'_n\rangle\}$ are δ-*close*, denoted as $|\psi\rangle \approx_\delta |\psi'\rangle$, if $\||\psi_n\rangle - |\psi'_n\rangle\|^2 = O(\delta(n))$. (For convenience we generally leave the dependence of the states and δ on the indexing parameter n implicit.)

Definition 2.2.2 (Consistency between POVMs)**.** Let $\mathcal{X}$ be a finite set and μ a distribution on $\mathcal{X}$. Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a quantum state, and for all $x \in \mathcal{X}$, $\{A_a^x\}$ and $\{B_a^x\}$ POVMs. We write 000M

$$A_a^x \otimes I_B \simeq_\delta I_A \otimes B_a^x$$

on state $|\psi\rangle$ and distribution μ if

$$\mathop{\mathbb{E}}_{x\sim\mu} \sum_{a\neq b} \langle\psi|A_a^x \otimes B_b^x|\psi\rangle \leq O(\delta) \ .$$

In this case, we say that $\{A_a^x\}$ and $\{B_a^x\}$ are δ-*consistent* on $|\psi\rangle$.

Note that a consistent measurement according to Definition **??** is 0-consistent with itself, under the singleton distribution, according to Definition **??** (and vice-versa).

Definition 2.2.3 (Distance between POVMs)**.** Let $\mathcal{X}$ be a finite set and μ a distribution on $\mathcal{X}$. Let $|\psi\rangle \in \mathcal{H}$ be a quantum state, and for all $x \in \mathcal{X}$, $\{M_a^x\}$ and $\{N_a^x\}$ two POVMs on $\mathcal{H}$. We say that $\{M_a^x\}$ *and* $\{N_a^x\}$ *are* δ*-close on state* $|\psi\rangle$ *and under distribution* μ if 000N

$$\mathop{\mathbb{E}}_{x\sim\mu} \sum_a \|(M_a^x - N_a^x)|\psi\rangle\|^2 \leq O(\delta) \ ,$$

and we write $M_a^x \approx_\delta N_a^x$ to denote this when the state $|\psi\rangle$ and distribution μ are clear from context. This distance is referred to as the *state-dependent* distance.

Definition 2.2.4 (Distance between strategies)**.** Let $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$ be a nonlocal game and let $S = (\psi, A, B)$, $S' = (\psi', A', B')$ be strategies for $\mathfrak{G}$. For $\delta \in [0,1]$ we say that S *is* δ*-close to* S' if the following conditions hold. 000P

1. The states $|\psi\rangle, |\psi'\rangle$ are states in the same Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and are δ-close.
2. For all $x \in \mathcal{X}, y \in \mathcal{Y}$, we have $A_a^x \approx_\delta (A')_a^x$ and $B_b^y \approx_\delta (B')_b^y$, with the approximations holding under the distribution μ, and on either $|\psi\rangle$ or $|\psi'\rangle$.

We record several useful facts about the consistency measure and the state-dependent distance without proof. Readers are referred to Sections 4.4 and 4.5 in [**?**] for additional discussion and proofs.

Fact 2.2.5 (Fact 4.13 and Fact 4.14 in [**?**])**.** *For POVMs* $\{A_a^x\}$ *and* $\{B_a^x\}$*, the following hold.* 000Q

000R 1. *If* $A_a^x \otimes I_B \simeq_\delta I_A \otimes B_a^x$ *then* $A_a^x \otimes I_B \approx_\delta I_A \otimes B_a^x$.

2. *If* $A_a^x \otimes I_B \approx_\delta I_A \otimes B_a^x$ and $\{A_a^x\}$ *and* $\{B_a^x\}$ *are projective measurements,*
000S *then* $A_a^x \otimes I_B \simeq_\delta I_A \otimes B_a^x$.

3. *If* $A_a^x \otimes I_B \approx_\delta I_A \otimes B_a^x$ *and either* $\{A_a^x\}$ *or* $\{B_a^x\}$ *is a projective measure-*
000T *ment, then* $A_a^x \otimes I_B \simeq_{\delta^{1/2}} I_A \otimes B_a^x$.

000U **Fact 2.2.6** (Fact 4.20 in [**?**])**.** *Let* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *be finite sets, and let* D *be a distribution over question pairs* (x, y)*. Let* $\{A_{a,b}^x\}$ *and* $\{B_{a,b}^x\}$ *be operators whose outcomes range over the product set* $\mathcal{A}\times\mathcal{B}$*. Suppose a set of operators* $\{C_{a,c}^y\}$*, whose outcomes range over the product set* $\mathcal{A}\times\mathcal{C}$*, satisfies the condition* $\sum_{a,c}(C_{a,c}^y)^\dagger C_{a,c}^y \leq$ Id *for all* y*. If* $A_{a,b}^x \approx_\delta B_{a,b}^x$ *on average over* x *sampled from the corresponding marginal of distribution* D*, then* $C_{a,c}^y A_{a,b}^x \approx_\delta C_{a,c}^y B_{a,b}^x$ *on average over* (x, y) *sampled from* D*.*

Proof. Fix questions x, y and answers $a \in \mathcal{A}, b \in \mathcal{B}$. We have then that

$$\sum_c \left\|(C_{a,c}^y A_{a,b}^x - C_{a,c}^y B_{a,b}^x)|\psi\rangle\right\|^2 = \sum_c \langle\psi|(A_{a,b}^x - B_{a,b}^x)^\dagger (C_{a,c}^y)^\dagger (C_{a,c}^y)(A_{a,b}^x - B_{a,b}^x)|\psi\rangle \tag{2.2.6.1}$$

$$\leq \langle\psi|(A_{a,b}^x - B_{a,b}^x)^\dagger (A_{a,b}^x - B_{a,b}^x)|\psi\rangle \tag{2.2.6.2}$$

$$= \left\|(A_{a,b}^x - B_{a,b}^x)|\psi\rangle\right\|^2 \tag{2.2.6.3}$$

where the inequality follows from the fact that $\sum_c (C_{a,c}^y)^\dagger C_{a,c}^y \leq \sum_{a,c}(C_{a,c}^y)^\dagger C_{a,c}^y \leq$ Id. Thus we obtain the desired conclusion

$$\mathop{\mathbb{E}}_{(x,y)\sim D} \sum_{a,b,c} \left\|(C_{a,c}^y A_{a,b}^x - C_{a,c}^y B_{a,b}^x)|\psi\rangle\right\|^2 \leq \mathop{\mathbb{E}}_{(x,y)\sim D} \sum_{a,b} \left\|(A_{a,b}^x - B_{a,b}^x)|\psi\rangle\right\|^2 \leq \delta.$$

□

000V **Fact 2.2.7.** *Let* $\mathcal{X}, \mathcal{A}$ *denote finite sets, and let* $\mathcal{G}$ *denote a set of functions* $g : \mathcal{X} \to \mathcal{A}$*. Let* $\{A_a^x\}$*,* $\{B_a^x\}$ *be POVMs indexed by* $\mathcal{X}$ *and outcomes in* $\mathcal{A}$*. Let* $\{S_g^x\}$ *denote a set of operators such that for all* $x \in \mathcal{X}$*,* $\sum_g (S_g^x)^\dagger S_g^x \leq$ Id*. If* $A_a^x \approx_\delta B_a^x$ *on average over* x*, then* $S_g^x A_{g(x)}^x \approx_\delta S_g^x B_{g(x)}^x$.

Proof. We expand:

$$\begin{aligned}
\mathop{\mathbb{E}}_x \sum_g \left\|S_g^x (A_{g(x)}^x - B_{g(x)}^x)|\psi\rangle\right\|^2 &= \mathop{\mathbb{E}}_x \sum_g \langle\psi|(A_{g(x)}^x - B_{g(x)}^x)^\dagger (S_g^x)^\dagger S_g^x (A_{g(x)}^x - B_{g(x)}^x)|\psi\rangle \\
&= \mathop{\mathbb{E}}_x \sum_a \langle\psi|(A_a^x - B_a^x)^\dagger \Big(\sum_{g:g(x)=a} (S_g^x)^\dagger S_g^x\Big)(A_a^x - B_a^x)|\psi\rangle \\
&\leq \mathop{\mathbb{E}}_x \sum_a \langle\psi|(A_a^x - B_a^x)^\dagger (A_a^x - B_a^x)|\psi\rangle \\
&= \mathop{\mathbb{E}}_x \sum_a \left\|(A_a^x - B_a^x)|\psi\rangle\right\|^2.
\end{aligned}$$

The inequality follows from the fact that $\sum_{g:g(x)=a}(S_g^x)^\dagger S_g^x \leq \sum_g (S_g^x)^\dagger (S_g^x) \leq$ Id. The last line is at most δ by assumption, and we obtain the desired conclusion. □

Lemma 2.2.8. *Let $\mathcal{A}$ be a finite set. Let $\{A_a^x\}_{a\in\mathcal{A}}$ be a projective measurement and let $\{B_a^x\}_{a\in\mathcal{A}}$ be a set of matrices. If $A_a^x \approx_\delta B_a^x$, then for all subsets $S \subseteq \mathcal{A}$, we have* 000W

$$\sum_{a\in S} A_a^x \approx_\delta \sum_{a\in S} A_a^x \cdot B_a^x.$$

Proof. We expand:

$$\begin{aligned}\mathop{\mathbb{E}}_x \left\| \sum_{a\in S} \left(A_a^x - A_a^x \cdot B_a^x\right)|\psi\rangle \right\|^2 &= \mathop{\mathbb{E}}_x \left\| \sum_{a\in S} A_a^x \cdot \left(A_a^x - B_a^x\right)|\psi\rangle \right\|^2 \\ &= \mathop{\mathbb{E}}_x \sum_{a\in S} \langle\psi|(A_a^x - B_a^x)^\dagger A_a^x (A_a^x - B_a^x)|\psi\rangle \\ &\leq \mathop{\mathbb{E}}_x \sum_a \left\|(A_a^x - B_a^x)|\psi\rangle\right\|^2 .\end{aligned}$$

In the second line we used the projectivity of $\{A_a^x\}$, and in the third line we used that $A_a^x \leq \mathrm{Id}$. □

Fact 2.2.9 (Triangle inequality, Fact 4.28 in [**?**])**.** *If $A_a^x \approx_\delta B_a^x$ and $B_a^x \approx_\epsilon C_a^x$, then $A_a^x \approx_{\delta+\epsilon} C_a^x$.* 000X

Fact 2.2.10 (Triangle inequality for "$\simeq$", Proposition 4.29 in [**?**])**.** *If $A_a^x \otimes I_B \simeq_\varepsilon I_A \otimes B_a^x$, $C_a^x \otimes I_B \simeq_\delta I_A \otimes B_a^x$, and $C_a^x \otimes I_B \simeq_\gamma I_A \otimes D_a^x$, then $A_a^x \otimes I_B \simeq_{\varepsilon+2\sqrt{\delta+\gamma}} I_A \otimes D_a^x$.* 000Y

Fact 2.2.11 (Data processing, Fact 4.26 in [**?**])**.** *Suppose $A_a^x \otimes I_B \simeq_\delta I_A \otimes B_a^x$. Then $A_{[f(\cdot)=b]}^x \otimes I_B \simeq_\delta I_A \otimes B_{[f(\cdot)=b]}^x$.* 000Z

The state-dependent distance is the right tool for reasoning about the closeness of measurement operators in a strategy. The following lemma ensures that, when two families of measurements are close on a state, changing from one family of measurement to the other only introduces a small error to the value of the strategy.

Lemma 2.2.12. *Let $\{A_{a,b}^x\}$, $\{B_{a,b,c}^x\}$, $\{C_{a,c}^x\}$ be POVMs. Suppose $\{B_{a,b,c}^x\}$ is projective, and* 0010

$$\begin{aligned} A_{a,b}^x \otimes \mathrm{Id}_B &\approx_\delta \mathrm{Id}_A \otimes B_{a,b}^x , \\ C_{a,c}^x \otimes \mathrm{Id}_B &\approx_\delta \mathrm{Id}_A \otimes B_{a,c}^x . \end{aligned}$$

Then the following approximate commutation relation holds:

$$[A_{a,b}^x, C_{a,c}^x] \otimes I_B \approx_\delta 0 .$$

Proof. Applying Fact **??** to $C^x_{a,\,c}\otimes \mathrm{Id}_B \approx_\delta \mathrm{Id}_A \otimes B^x_{a,\,c}$ and $\{A^x_{a,b}\otimes \mathrm{Id}_B\}$, we have

$$A^x_{a,\,b}C^x_{a,\,c}\otimes \mathrm{Id}_B \approx_\delta A^x_{a,\,b}\otimes B^x_{a,\,c}\,. \tag{2.2.12.1}$$

Similarly, applying Fact **??** to $A^x_{a,\,b}\otimes \mathrm{Id}_B \approx_\delta \mathrm{Id}_A \otimes B^x_{a,\,b}$ and $\{\mathrm{Id}_A \otimes B^x_{a,c}\}$, and using the fact that $\{B^x_{a,b,c}\}$ is projective, we have

$$\begin{aligned} A^x_{a,\,b}\otimes B^x_{a,\,c} &\approx_\delta \mathrm{Id}_A \otimes B^x_{a,\,c}B^x_{a,\,b} \\ &= \mathrm{Id}_A \otimes B^x_{a,\,b,\,c}\,. \end{aligned} \tag{2.2.12.2}$$

Combining Equations (**??**) and (**??**), we have

$$A^x_{a,\,b}C^x_{a,\,c}\otimes \mathrm{Id}_B \approx_\delta \mathrm{Id}_A \otimes B^x_{a,\,b,\,c}\,. \tag{2.2.12.3}$$

A similar argument gives

$$C^x_{a,\,c}A^x_{a,\,b}\otimes \mathrm{Id}_B \approx_\delta \mathrm{Id}_A \otimes B^x_{a,\,b,\,c}\,. \tag{2.2.12.4}$$

The claim follows from Equations (**??**) and (**??**). □

The following lemma is a slightly modified version of [**?**, Fact 4.34].

Lemma 2.2.13. *Let $k \geq 0$ be an integer and let $\varepsilon > 0$. Let $\mathcal{X}$ be a finite set and μ a distribution over $\mathcal{X}$. For each $1 \leq i \leq k$ let $\mathcal{G}_i$ be a set of functions $g_i : \mathcal{Y} \to \mathcal{R}_i$ and for each $x \in \mathcal{X}$ let $\{G^{i,\,x}_g\}_{g\in\mathcal{G}_i}$ be a projective measurement. Suppose that for all $i \in \{1,\ldots,k\}$, $\mathcal{G}_i$ satisfies the following property: for any two $g_i \neq g'_i \in \mathcal{G}_i$, the probability that $g_i(y) = g'_i(y)$ over a uniformly random $y \in \mathcal{Y}$ is at most ε.*

Let $\left\{A^x_{g_1,\,g_2,\,\ldots\,,\,g_k}\right\}$ be a projective measurement with outcomes $(g_1,\ldots,g_k) \in \mathcal{G}_1 \times \cdots \times \mathcal{G}_k$. For each $1 \leq i \leq k$, suppose that on average over $x \sim \mu$ and $y \in \mathcal{Y}$ sampled uniformly at random,

$$A^x_{[\mathrm{eval}_y(\cdot)_i = a_i]} \otimes I_B \simeq_\delta I_A \otimes G^{i,\,x}_{[\mathrm{eval}_y(\cdot)=a_i]}\,. \tag{2.2.13.1}$$

Define the POVM family $\{C^x_{g_1,\,g_2,\,\ldots\,,\,g_k}\}$, for $x \in \mathcal{X}$, by

$$C^x_{g_1,\,g_2,\,\ldots\,,\,g_k} = G^{k,\,x}_{g_k}\cdots G^{2,\,x}_{g_2}\,G^{1,\,x}_{g_1}\,G^{2,\,x}_{g_2}\cdots G^{k,\,x}_{g_k}\,.$$

Then on average over $x \sim \mu$ and $y \in \mathcal{Y}$ sampled uniformly at random,

$$A^x_{[\mathrm{eval}_y(\cdot)=(a_1,\,a_2,\,\ldots,\,a_k)]} \otimes I_B \simeq_{k(\delta+\varepsilon)^{1/2}} I_A \otimes C^x_{[\mathrm{eval}_y(\cdot)=(a_1,\,a_2,\,\ldots,\,a_k)]}\,. \tag{2.2.13.2}$$

Proof. The proof is identical to the one given in [**?**, Fact 4.34], with the only modification needed to insert the dependence on x for all measurements considered. □

Lemma 2.2.14 (Fact 4.35 in [**?**])**.** *Let $\mathcal{D}$ be a distribution on $(x, y_1, y_2) \in \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$. For $i \in \{1, 2\}$ let $\mathcal{G}_i$ be a collection of functions $g_i : \mathcal{Y}_i \to \mathcal{R}_i$ and let $\{(G_i)^x_g\}_{g\in\mathcal{G}_i}$ be families of measurements such that $\{(G_2)^x_g\}_g$ is projective*

for every x. Suppose further that for every (x, y_1) it holds that for $g_2 \neq g_2' \in \mathcal{G}_2$ the probability, on average over y_2 chosen from $\mathcal{D}$ conditioned on (x, y_1), that $g_2(y_2) = g_2'(y_2)$ is at most η. Let $\{A^{x,y_1,y_2}_{a_1,a_2}\}$ be a family of projective measurements with outcomes $(a_1, a_2) \in \mathcal{R}_1 \times \mathcal{R}_2$ such that for $i \in \{1, 2\}$,

$$A^{x,y_1,y_2}_{a_i} \otimes \mathrm{Id} \simeq_\delta \mathrm{Id} \otimes (G_i)^x_{[\mathrm{eval}_{y_i}(\cdot)=a_i]} \tag{2.2.14.1}$$ 0019

and

$$A^{x,y_1,y_2}_{a_1,a_2} \otimes \mathrm{Id} \simeq_\delta \mathrm{Id} \otimes A^{x,y_1,y_2}_{a_1,a_2} \ . \tag{2.2.14.2}$$ 001A

Define a family of measurements $\{J^x_{g_1,g_2}\}$ as

$$J^x_{g_1,g_2} \ = \ (G_2)^x_{g_2} (G_1)^x_{g_1} (G_2)^x_{g_2} \ . \tag{2.2.14.3}$$ 001B

Then there is a

$$\delta_{pasting} \ = \ \delta_{pasting}(\eta, \delta) \ = \ \mathrm{poly}(\eta, \delta) \tag{2.2.14.4}$$ 001C

such that

$$A^{x,y_1,y_2}_{a_1,a_2} \otimes \mathrm{Id} \simeq_{\delta_p} \mathrm{Id} \otimes J^x_{[\mathrm{eval}_{y_1}(\cdot)=a_1, \mathrm{eval}_{y_2}(\cdot)=a_2]} \ . \tag{2.2.14.5}$$ 001D

Chapter 3

Complexity theory

001E

Chapter 4

Operator algebras

001F

Part III

Warm-up

Chapter 5

Pauli braiding

5.1 Multiplayer games

A multiplayer game is a single-round interaction between a *referee* and multiple *players*. The game specifies the actions of the referee: with what distribution she selects the questions to the players, and what tuples of answers are valid for each tuple of questions. The players, traditionally referred to as Alice, Bob, Charlie, etc., are always assumed to attempt to maximize their probability of winning (i.e. providing valid answers) in the game. The probability is over both the referee's and the players' randomness. This quantity, the players' maximum winning probability, is usually called the *value* of the game.

Multiplayer games play an important role in theoretical computer science. Their study ca be motivated from at least two vantage points:

- *Hardness of approximation for constraint satisfaction problems.* The most famous game in this context is the 3SAT "clause-vs-variable" game. In this game there are two players, Alice and Bob. Both players and the referee are given access to the same 3SAT formula φ. Moreover, the players can agree on a strategy after having seen the formula and before the game starts. Once the game starts, the referee selects a clause $C = x \vee y \vee z$ (some of the variables may be negated) uniformly at random, as well as a variable $w \in \{x, y, z\}$ appearing in C, again uniformly at random. She sends the triple $\{x, y, z\}$ to Alice, and the single variable w to Bob. Each player is expected to return an assignment to the variables he or she was asked about. The players win if and only if Alice's assignment satisfies the clause C, and Bob's assignment is consistent with Alice's on the variable they were asked in common.
  It is not hard to verify that the maximum success probability in this game is directly related to the largest number of clauses of φ that can be simultaneously satisfied by any assignment. Since 3SAT is NP-hard, it follows that the value of a game specified explicitly (in matrix form, i.e. a table specifying explicitly the distribution on questions and the truth

table for valid answer tuples) is NP-hard to compute.
In fact, it follows from the PCP theorem that the value is not only hard to compute exactly, but even to approximate within a sufficiently small constant factor. The language of games plays an important role in Dinur's proof of the PCP theorem [**?**], and it has been instrumental in many reductions deriving hardness of approximation for combinatorial problems. It can also be a useful perspective when studying rounding techniques for linear programming (LP) or semidefinite programming (SDP) relaxations of constraint satisfaction problems.

- *Interactive protocols in cryptography.* In cryptography, games often play a role as building blocks in *interactive protocols*, where the players are usually referred to as *provers*. A famous game in this context is the two-prover commitment protocol by Ben-Or et al. [**?**]. This protocol was introduced to show that all languages in NP have two-prover interactive proofs with perfect zero-knowledge. Technically the protocol gives rise to a two-round game: the referee first interacts with the first prover (commit phase), and then with the second prover (reveal phase). Many kinds of games arise in cryptography, with the players sometimes exchanging messages between themselves, some players being trusted ("oracles") and others not, etc.

Quantum information introduces an exciting twist in the theory of multiplayer games: what if the players are allowed to use entanglement? The game is the same, but the set of allowed strategies has been broadened. While entanglement does not allow the players to communicate, it could in principle allow them to increase their odds of winning, and indeed this is the case: you already saw this in the example of the CHSH game, and we will see many more examples as we go.

Remark 5.1.1. One can ask, why stop at quantum? The most general strategies that respect the no-communication assumption are aptly called *non-signaling strategies*. We will not discuss them in this lecture, but aside from being a nice extension of quantum strategies they have recently become very relevant in designing efficient (single-prover) classical delegation protocols; see e.g. [**?**].

Interestingly, many games have the property that the optimal quantum strategy for the players is essentially unique. This property, called *rigidity*, can be leveraged to devise classical tests that verify that arbitrary quantum devices (the players) perform very specific operations. This opens up a whole new world of possibilities, from the certification of information-theoretic randomness to "device-independent" security proofs in cryptography to protocols for delegated computation; we will touch on some of these topics in a subsequent lecture.

Resources. A great introduction to complexity-theoretic questions about nonlocal games is the paper by Cleve et al. [**?**]. The lecture notes by Ji (see module 5 here) cover CHSH, the Magic Square game, linearity testing (using a slightly different analysis than the one we will give here), and graph-based games.

Notation. In this lecture we use the non-standard notation

001K
$$|\phi_d\rangle \;=\; \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle \tag{5.1.1.1}$$

for the maximally entangled state in d dimension. In particular, $|\phi_2\rangle$ denotes an EPR pair.

Part IV

Overview

Chapter 6

The argument

001M

Chapter 7

Question reduction

001N

Chapter 8

Answer reduction

001P

Chapter 9

Recursive Compression

001Q

Part V

Related tools

Chapter 10

Parallel repetition

001S