Chapter 5

Towards Quantum Safety

5.1 Introduction

In Chapter 4, we proved composition theorems for two-prover commitment schemes. Those theorems crucially rely on the assumption that dishonest provers can *only* use classical shared randomness, and not entangled quantum states: The definition of our (strong) binding property does not apply if the provers use quantum entanglement instead of classical randomness. While the weak binding property is well-defined for adversaries with quantum capabilities, our proof of the composition theorem for this binding property, i.e., Theorem 4.13, still requires that we can assume without loss of generality that the adversaries' strategy is deterministic. This is not true if we consider adversaries with quantum capabilities.

In this chapter, we take some steps towards arguing that the Lunghi *et al.* scheme is binding for provers with quantum capabilities.

In Section 5.4, we show that $\mathcal{CHSH}^q$ satisfies the fairly-weak-binding definition as a string-commitment scheme even when the adversaries can share entangled quantum states. Our intuitive argument in Chapter 4 thus suggests that $\mathcal{CHSH}^q_m$ also satisfies the binding property with parameter linear in m for such adversaries. However, since our composition theorem only applies to classical provers, this intuition remains without a rigorous proof.

Approaching the problem from another direction, we introduce an analogue of the strong binding definition for the quantum case, and prove a composition theorem using this definition which applies to quantum provers. However, we currently do not know if $\mathcal{CHSH}^q$ (or any other scheme) satisfies this stronger definition. Thus, the question whether there exists a multi-round scheme binding for quantum adversaries remains open.

5.2 Quantum Information Theory

We start with a very brief introduction to quantum information theory where we fix our notation. We refer readers who are not familiar with the subject to introductory textbooks such as [NC00] or [Wil13]. Quantum information theory is based on quantum mechanics, but takes a somewhat different point of view. While quantum mechanics is about the evolution of quantum systems over time, quantum information theory views them as static carriers of information which only change when acted upon by an experimenter.

We begin with defining the required mathematical concepts and then introduce quantum states, measurements, and entanglement. Many properties that are taken for granted in classical information do not apply to quantum information: in particular, it is generally not possible to extract information from a quantum state without changing it, or to make a perfect copy of a quantum state. However, we also show how to express classical information and computation in the formalism of quantum information theory. Thus, quantum information can be viewed as an *extension* of classical information.

5.2.1 Definitions

In this section, we recall the mathematical concepts that are used to describe quantum information. We let $\mathcal{H}$ be a *finite-dimensional complex Hilbert space*, i.e., a complex vector space with an inner product $\langle\cdot|\cdot\rangle$ that is conjugate-symmetric and linear in the second argument. We write vectors in $\mathcal{H}$ using the *bra-ket notation* introduced by Paul Dirac [Dir39]: A vector in $\mathcal{H}$ is written as a *ket-vector* $|\phi\rangle$. Every ket-vector $|\phi\rangle$ has a corresponding *bra-vector* $\langle\phi|$ in the dual space $\mathcal{H}^*$:

$$\langle\phi| : \mathcal{H} \to \mathbb{C}, \quad |\psi\rangle \mapsto \langle\phi|\psi\rangle .$$

Thus, a bra- and a ket-vector "fit together" notationally to form the inner product: $\langle\phi|\,|\psi\rangle = \langle\phi|\psi\rangle$.

Definition 5.1. *A vector $|\phi\rangle \in \mathcal{H}$ is called a* state vector *if $\| \, |\phi\rangle \, \| := \sqrt{\langle\phi|\phi\rangle} = 1$.*

Definition 5.2. *Let $\{|i\rangle\}_{i\in I}$ be a basis of $\mathcal{H}$. It is called an* orthonormal basis *if all vectors have norm 1 and are mutually orthogonal. That is, for all $i, j \in I$:*

$$\langle i|j\rangle \;=\; \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

We write $\mathcal{L}(\mathcal{H})$ to denote the vector space of linear operators on $\mathcal{H}$. For any pair of vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, the *outer product* is defined as the linear operator $|\phi\rangle\langle\psi| : \mathcal{H} \to \mathcal{H}, |\delta\rangle \mapsto |\phi\rangle\langle\psi|\delta\rangle = \langle\psi|\delta\rangle\,|\phi\rangle$. The space $\mathcal{L}(\mathcal{H})$ is spanned by the set of outer products. In fact, if $\{|i\rangle\}_{i\in I}$ is a basis of $\mathcal{H}$, then $\{|i\rangle\langle j|\}_{i,j\in I}$ is a basis of $\mathcal{L}(\mathcal{H})$. We recall the following two linear operators acting on $\mathcal{L}(\mathcal{H})$:

Definition 5.3. *The* conjugate transpose *is the linear operator* $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ *that maps* $|\phi\rangle\langle\psi|$ *to* $|\phi\rangle\langle\psi|^\dagger := |\psi\rangle\langle\phi|$ *for all* $|\phi\rangle, |\psi\rangle \in \mathcal{H}$.

Definition 5.4. *The* trace *is the linear operator* $\mathrm{Tr} : \mathcal{L}(\mathcal{H}) \to \mathbb{C}$ *defined by* $\mathrm{Tr}(|\phi\rangle\langle\psi|) = \langle\psi|\phi\rangle$ *for all* $|\phi\rangle, |\psi\rangle \in \mathcal{H}$.

For any $A \in \mathcal{L}(\mathcal{H})$ and any orthonormal basis $\{|i\rangle\}_{i\in I}$, $\sum_{i\in I} \langle i| A |i\rangle = \sum_{i\in I} \mathrm{Tr}(A |i\rangle\langle i|) = \mathrm{Tr}(A)$, using the equality $\sum_{i\in I} |i\rangle\langle i| = \mathbb{I}$. Thus, the above definition of the trace coincides with the more usual one where $\mathrm{Tr}(A)$ is defined as the sum of the diagonal elements of a matrix representation of A.

Definition 5.5. *A linear operator* $\rho : \mathcal{H} \to \mathcal{H}$ *is called a* density matrix *if* ρ *is positive semi-definite (i.e.,* $\langle\phi| \rho |\phi\rangle \geq 0$ *for all* $|\phi\rangle \in \mathcal{H}$*) and* $\mathrm{Tr}(\rho) = 1$.

Definition 5.6. *An operator* $U \in \mathcal{L}(\mathcal{H})$ *is called* unitary *if* $U^\dagger U = \mathbb{I}$.

An equivalent characterization of unitaries is that they map an orthonormal basis to an orthonormal basis, i.e., U is unitary if and only if there are orthonormal bases $\{|i\rangle\}_{i\in I}$ and $\{|\phi_i\rangle\}_{i\in I}$ such that $U = \sum_{i\in I} |\phi_i\rangle\langle i|$.

Definition 5.7. *Let* $P : \mathcal{H} \to \mathcal{H}$ *be a linear operator. We say that* P *is a projector if* $P^2 = P$ *and* $P^\dagger = P$. *We say that two projectors* P *and* Q *are* (mutually) orthogonal *if* $PQ = 0$.[1]

Definition 5.8. *Suppose that* $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. *The* partial trace *is defined as the linear operator*

$$\mathrm{Tr}_A : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}_B),\ \rho_A \otimes \rho_B \mapsto \mathrm{Tr}(\rho_A)\rho_B$$

The partial trace Tr_B *is defined symmetrically.*

5.2.2 Quantum States and Measurements

A (finite-dimensional) quantum system A is associated with a *state space* $\mathcal{H}_A$, which is a finite-dimensional, complex Hilbert space. The *state* of a quantum system is represented as a density matrix ρ over $\mathcal{H}_A$. We identify the state of a quantum system with the density matrix that describes it and also call ρ a quantum state.

A quantum state can be acted on in the following two ways: The first is to *apply a unitary* U, transforming the state ρ into $U\rho U^\dagger$. The second way is to *perform a measurement*, which is the only way to extract classical information from a quantum state. A (projective) measurement is described by a collection $\{P_i\}_{i\in I}$ of mutually orthogonal projectors such that $\sum_{i\in I} P_i = \mathbb{I}$,

[1] Usually, projectors are defined just by the property $P^2 = P$. If they also satisfy $P^\dagger = P$, they are usually called *orthogonal projectors*. However, since all projectors we consider are orthogonal projectors, we reserve the term *orthogonal* for mutually orthogonal pairs of projectors.

where I is some finite index set. The measurement produces outcome i with probability $p_i := \mathrm{Tr}(P_i \rho P_i^\dagger) = \mathrm{Tr}(P_i \rho)$. If the state is measured and outcome i is observed, the state *collapses* to $\frac{1}{p_i} P_i \rho P_i$. There are more general formalisms for measurements, but we can restrict to projective measurements without loss of generality (see *Naimark's Dilation Theorem*).

If we can write $\rho = |\phi\rangle\langle\phi|$, ρ is called a *pure* state and we can use $|\phi\rangle$ as a representation of the quantum state. In this representation, applying a unitary U maps $|\phi\rangle$ to $U|\phi\rangle$. When performing a measurement, we observe outcome i with probability $p_i = \| P_i |\phi\rangle \|^2$ and obtain post-measurement state $\frac{1}{p_i} P_i |\phi\rangle$. If a quantum system is in the pure state $|\phi_i\rangle$ with probability p_i, it is represented by the density matrix $\sum_i p_i |\phi_i\rangle\langle\phi_i|$.

For every orthonormal basis $B = \{|i\rangle\}_{i \in I}$ of $\mathcal{H}$, $\{|i\rangle\langle i|\}_{i \in I}$ is a projective measurement, called the *total projective measurement* with respect to B or simply the measurement in basis B.

5.2.3 Bi-partite Quantum States and Entanglement

A crucial concept for this chapter is *quantum entanglement* shared between two parties. Let A and B be two quantum systems with respective state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. We may consider the two systems together as a single joint quantum system AB. The state space of AB is $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$. If A and B are prepared independently in states ρ_A and ρ_B, respectively, the state of the joint system is $\rho_A \otimes \rho_B$. If the state of the joint system is a pure tensor like this, we say that it is *in product state*. A product state can be seen as an analogue to a pair of independent random variables. A state is called *separable* if it can be written as $\rho_{AB} = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$ where the $\rho_{A,i}$ and $\rho_{B,i}$ are density matrices, $p_i \geq 0$ and $\sum_i p_i = 1$. A separable state is analogous to a pair of possibly correlated random variables. Finally, states that are not separable are called *entangled* and do not have any classical analogue.

If we perform an action on system A, the joint system AB is affected as follows: If a unitary U_A is applied on A, it acts as $U_A \otimes \mathbb{I}_B$ on the whole system. A measurement $\{P_i\}_{i \in I}$ on A acts as $\{P_i \otimes \mathbb{I}_B\}_{i \in I}$ on the joint system. Symmetrically, applying a unitary U_B on system B acts as $\mathbb{I}_A \otimes U_B$ and a measurement $\{P_i\}_{i \in I}$ on B acts as $\{\mathbb{I}_A \otimes P_i\}_{i \in I}$ on AB.

A final operation that can be performed on a joint system is to *remove* a part of it. When we have a joint system AB in state ρ_{AB}, the state of the subsystem B on its own is described by the *partial trace* $\mathrm{Tr}_A(\rho_{AB})$.

The above generalizes to tripartite (and, more generally, n-partite) states. Entanglement does not depend on physical proximity. Two agents that are far apart – like the provers in a relativistic bit-commitment scheme – can each keep one part of an entangled quantum state and apply unitaries and measurements to their part. Sharing an entangled quantum state allows two parties to correlate their behavior without communicating in a way that is not possible classically. We give an example of this phenomenon in the next

section.

5.2.4 Example: A Strategy for CHSH

To illustrate the effects of quantum entanglement, we now describe a strategy for the CHSH game using an entangled quantum state, which has a better success probability than any strategy that relies solely on shared randomness. Recall that the CHSH game works as follows [CHSH69]: The players Alice and Bob each receive an input bit a and b, respectively, and they each have to output a bit x and y, respectively, without communicating. They win if $x+y = a \cdot b$. In other words, if $a = b = 1$, they have to output *different* bits, and in all other cases, they have to output *identical* bits. It is easy to see that the maximal success probability for strategies using shared classical randomness is 0.75. However, there is a strategy that uses quantum entanglement and achieves a success probability of $\cos(\pi/8)^2 \approx 0.85$.

Let A and B be quantum systems with state spaces $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. We write the standard basis as $\{|0\rangle, |1\rangle\}$ and define the following vectors:

$$
\begin{aligned}
|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|\phi_0\rangle &= \cos(\pi/8)\,|0\rangle + \sin(\pi/8)\,|1\rangle \\
|\phi_1\rangle &= \sin(\pi/8)\,|0\rangle - \cos(\pi/8)\,|1\rangle \\
|\psi_0\rangle &= \cos(\pi/8)\,|0\rangle - \sin(\pi/8)\,|1\rangle \\
|\psi_1\rangle &= \sin(\pi/8)\,|0\rangle + \cos(\pi/8)\,|1\rangle
\end{aligned}
$$

$\{|+\rangle, |-\rangle\}$, $\{|\phi_0\rangle, |\phi_1\rangle\}$, and $\{|\psi_0\rangle, |\psi_1\rangle\}$ are orthonormal bases of $\mathbb{C}^2$. The measurements in the standard basis and each of those bases are defined as follows.

$$
\begin{aligned}
M_0^A &= \{|0\rangle\langle 0|, |1\rangle\langle 1|\} \\
M_1^A &= \{|+\rangle\langle +|, |-\rangle\langle -|\} \\
M_0^B &= \{|\phi_0\rangle\langle \phi_0|, |\phi_1\rangle\langle \phi_1|\} \\
M_1^B &= \{|\psi_0\rangle\langle \psi_0|, |\psi_1\rangle\langle \psi_1|\}
\end{aligned}
$$

The system AB is prepared in state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Alice keeps system A and Bob keeps system B. The strategy now works as follows. The players apply the measurement M_a^A or M_b^B, respectively, on their part of the quantum state. Their outputs are their respective measurement outcomes.

First, let us consider the case $a = 0$, $b = 0$. Alice applies the measurement M_0^A, which results in a uniformly random outcome $x \in \{0, 1\}$ with post-measurement state $|x\rangle \otimes |x\rangle$. Bob applies M_0^B. In order to win the game, he needs to output the same bit as Alice, and thus the winning probability is

$$\|(\mathbb{I}_A \otimes |\phi_x\rangle \langle\phi_x|)(|x\rangle \otimes |x\rangle)\|^2 = |\langle\phi_x|x\rangle|^2 = \cos(\pi/8)^2 \approx 0.85$$

If $a = 0$, $b = 1$, the two players again need to output the same bit. Thus, the probability that Bob produces the correct output is $|\langle\psi_x|x\rangle|^2 = \cos(\pi/8)^2 \approx 0.85$. If $a = 1$, $b = 0$, Alice outputs a uniformly random $x \in \{0, 1\}$, and the post-measurement state is $|+\rangle \otimes |+\rangle$ if $x = 0$ and $|-\rangle \otimes |-\rangle$ if $x = 1$. They need to output the same bit again, and thus the success probability is

$$\begin{aligned} |\langle +|\phi_0\rangle|^2 = |\langle -|\phi_1\rangle|^2 &= \left(\frac{1}{\sqrt{2}}(\sin(\pi/8) + \cos(\pi/8))\right)^2 \\ &= (\cos(\pi/4)\cos(\pi/8) + \sin(\pi/4)\sin(\pi/8))^2 \\ &= \cos(\pi/8)^2 \approx 0.85 \end{aligned}$$

Finally, we consider the case $a = 1$, $b = 1$. Here, the provers win if they produce *different* outputs. The winning probability is

$$|\langle +|\psi_1\rangle|^2 = |\langle -|\psi_0\rangle|^2 = \left(\frac{1}{\sqrt{2}}(\sin(\pi/8) + \cos(\pi/8))\right)^2 = \cos(\pi/8)^2 \approx 0.85$$

and thus, for all possible inputs a and b, the players can win with probability $\cos(\pi/8)^2 \approx 0.85$, without communicating.

5.2.5 Representing Classical Information and Randomness

The formalism from the preceding sections can also be used to capture classical information. We can represent a single bit as a state of a *qubit* system, i.e., a quantum system with state space $\mathbb{C}^2$. We write $\{|0\rangle, |1\rangle\}$ for the standard basis of $\mathbb{C}^2$ and represent the bit b as the state vector $|b\rangle$. More generally, we can represent elements of a finite set S via a bijection mapping each element s to a standard basis vector $|s\rangle$ of $\mathbb{C}^{|S|}$. This representation can also be understood as an encoding, where decoding is done by measuring the quantum state in the standard basis. Note that because the quantum state itself is one of the basis vectors, performing this measurement has a deterministic outcome and does not alter the state. A distribution $p(s)$ over some set S is then naturally represented by the density matrix $\sum_{s\in S} p(s)\,|s\rangle\langle s|$. Shared randomness can be represented as the separable bipartite state $\sum_{s\in S} p(s)\,|s\rangle\langle s| \otimes |s\rangle\langle s|$.

It is possible to represent all classical computations as unitaries. Let $\mathcal{X}$ be a finite set and $\mathcal{Y}$ a finite group, where the group operation is denoted

by + and the neutral element by 0. Let $f : \mathcal{X} \to \mathcal{Y}$ be some function. Let $U_f : \mathbb{C}^{|X|} \otimes \mathbb{C}^{|Y|} \to \mathbb{C}^{|X|} \otimes \mathbb{C}^{|Y|}, |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$. It is easy to see that U_f is unitary because it maps an orthonormal basis to an orthonormal basis. We can represent the computation of $f(x)$ as follows in the quantum formalism: Given $|x\rangle$, we first append $|0\rangle \in \mathbb{C}^{|Y|}$ and then apply U_f. The second quantum system now holds the desired result.

5.3 Protocols

In this section, we adapt our formal definitions of interactive protocols from Section 2.2.1 to the quantum setting. We again consider protocols involving three parties, the provers P and Q and the verifier V. A protocol $\mathsf{prot}_{PQV} = (\mathsf{prot}_P, \mathsf{prot}_Q, \mathsf{prot}_V)$ consists of a triple of l-round interactive algorithms operating on a quantum state ρ_{PQV} over a Hilbert space $\mathcal{H}_{PQV} = \mathcal{H}_P \otimes \mathcal{H}_Q \otimes \mathcal{H}_V$. The subscripts P, Q and V indicate the player that controls the system. The players can perform the following actions on their respective parts of the quantum states:

- apply unitaries and perform measurements,
- prepare an additional quantum system in some initial state and add it to their system,
- discard a part of their quantum state,
- transmit part of their quantum state to another player, making them part of that player's state in the next round.

The outcome of this procedure is a quantum state ρ'_{PQV} over a Hilbert space $\mathcal{H}'_{PQV} = \mathcal{H}'_P \otimes \mathcal{H}'_Q \otimes \mathcal{H}'_V$. Note that the state spaces may change due to players exchanging parts of their states and preparing additional subsystems. We write

$$\rho'_{PQV} \leftarrow \mathsf{prot}_{PQV}(\rho_{PQV})$$

to denote an execution of the protocol on the input state ρ_{PQV}. As in the classical case, we can compose protocols by using the output state of one as the input for the other. We separate shared entanglement from the input: to denote shared entanglement between P and Q, we write $\mathsf{prot}_{PQV}[\sigma_{PQ}]$.

A commitment scheme with domain D consists of two interactive quantum algorithms: The first, $\mathsf{com}_{PQV}[\sigma_{PQ}] = (\mathsf{com}_P, \mathsf{com}_Q, \mathsf{com}_V)$ takes an input state $|s\rangle_P \otimes |s\rangle_Q \in \left(\mathbb{C}^{|D|}\right)^{\otimes 2}$ for P and Q, and V has no input. The output is some state ρ'_{PQV}. $\mathsf{open}_{PQV}[\sigma'_{PQ}]$ then takes the output of com_{PQV} as input and V produces a (quantum representation of a) single bit as output, indicating whether the commitment was opened correctly or not. P and Q produce no output.

Of particular interest is the security of a classical commitment scheme (i.e., one that requires only classical information processing on the part of the honest players) against dishonest provers with quantum capabilities. In this case, they can not send quantum information to the honest V. We may model this as V immediately measuring all quantum states he receives in the standard basis of their respective state space.

For classical commitment schemes, the definitions of soundness and the hiding property simply carry over. If the scheme requires the verifier to store quantum information, the hiding property needs to be adapted: we say that the scheme is δ-hiding if no measurement that V can perform on his quantum state allows him to distinguish between any pair of strings s_0 and s_1 with probability better than δ.[2]

5.4 Binding Properties

5.4.1 Definition

As we already mentioned, the weak-binding properties defined in Section 3.2.3 carry over to the quantum setting without change. We define the following strong binding property for the quantum case, essentially replacing the function $\hat{s}$ with a measurement. As usual, the binding property is defined with respect to some set of possible strategies for the dishonest players, e.g., strategies where they do not communicate.

Definition 5.9. *Let S be a commitment scheme. We say that S is* ε-binding *if for every dishonest opening strategy $\overline{\mathsf{com}}_P$ there exists a measurement $\mathsf{Eval} = \{M_{\hat{s}}\}_{\hat{s}}$ such that for every possible shared quantum states σ_{PQ} and every dishonest opening strategy $\overline{\mathsf{open}}_Q$ we have $p(s \neq \hat{s} \wedge s \neq \perp) \leq \varepsilon$ where s is the output of the verifier after the opening phase and $\hat{s}$ is the outcome of the measurement Eval applied to the state $\rho'_{PV} = \mathrm{Tr}_Q\left(\rho'_{PQV}\right)$ where ρ'_{PQV} is the state after the execution of $\overline{\mathsf{com}}_{PQV}[\sigma_{PQ}]$. We say that it is* fairly ε*-binding if $p(s \neq \hat{s} \wedge s = s_\circ) \leq \varepsilon$ holds for all $s_\circ$.*

In order to actually perform the measurement Eval, P needs to obtain (a copy of) V's quantum state. This is possible if only P communicates with V in the commit phase, V sends (a copy of) his initial state to P, and all the communication with V is classical, so P can simply store copies of all messages he sends to V. If only Q is active in the opening phase, the measurement can be performed without affecting the outcome of the protocol execution. These conditions are all satisfied in the $\mathcal{CHSH}^q$ scheme.

We do not currently know whether there exists a scheme that satisfies Definition 5.9. However, we were able to show that $\mathcal{CHSH}^q$ satisfies the weak-binding definition as a string-commitment scheme.

[2] To be more formal, one might use the *trace distance* here.

5.4.2 The Finite Field CHSH Game With Restricted Inputs

We now prove that $\mathcal{CHSH}^q$ is weak-binding with respect to quantum adversaries. Our proof is based on an analysis of the following CHSH-like game: Let $S \subseteq \mathbb{F}_q$ with $|S| = N$. In the game CHSH^q_S, the two players Alice and Bob receive uniformly random inputs $a \in \mathbb{F}_q$ and $b \in S$ and, without communicating, produce outputs x and y in $\mathbb{F}_q$. They win if $x + y = a \cdot b$.

Theorem 5.10. *The game CHSH^q_S with $|S| = N$ has quantum value*

$$\frac{1}{N} + \frac{N-1}{\sqrt{q}}.$$

We use the following lemma:

Lemma 5.11. *Let $\{\Pi_i\}_{i\in\mathcal{I}}$ be a collection of projectors on a Hilbert space $\mathcal{H}$ and let $|\phi\rangle$ be a unit vector in $\mathcal{H}$. For $i, j \in \mathcal{I}$, let $\varepsilon_{i,j} = \|\Pi_i\Pi_j |\phi\rangle\|$. Then, $\| \sum_{i\in\mathcal{I}} \Pi_i |\phi\rangle \| \leq 1 + \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} \varepsilon_{i,j}$.*

Proof. If $\| \sum_i \Pi_i |\phi\rangle \| \leq 1$, the conclusion obviously holds, so we assume that $\| \sum_i \Pi_i |\phi\rangle \| > 1$. We have

$$\begin{aligned}
\left\| \sum_i \Pi_i |\phi\rangle \right\|^2 &= \left| \sum_{i,j} \langle\phi| \Pi_i\Pi_j |\phi\rangle \right| \\
&\leq \sum_i \langle\phi| \Pi_i |\phi\rangle + \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} |\langle\phi| \Pi_i\Pi_j |\phi\rangle| \\
&\leq \left\| \sum_i \Pi_i |\phi\rangle \right\| + \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} \underbrace{\||\phi\rangle\|}_{=1} \cdot \|\Pi_i\Pi_j |\phi\rangle\| \text{ by Cauchy-Schwarz} \\
&= \left\| \sum_i \Pi_i |\phi\rangle \right\| + \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} \varepsilon_{i,j}
\end{aligned}$$

which implies that

$$\left\| \sum_i \Pi_i |\phi\rangle \right\| = 1 + \frac{\sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} \varepsilon_{i,j}}{\|\sum_i \Pi_i |\phi\rangle\|} \leq 1 + \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{I}\setminus\{i\}} \varepsilon_{i,j}$$

as we claimed. □

Proof of Theorem 5.10. A quantum strategy for Alice and Bob is (without loss of generality) described by a bipartite quantum state $|\phi\rangle \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, a projective measurement $\{P^a_x\}_{x\in\mathbb{F}_q}$ on $\mathcal{H}_A$ for every $a \in \mathbb{F}_q$, and a projective measurement $\{Q^b_y\}_{y\in\mathbb{F}_q}$ for every $b \in S$. The output distribution of Alice and

Bob on inputs a and b is $p(x,y|a,b) = \langle\phi| (P_x^a \otimes Q_y^b) |\phi\rangle$. Let win be the event that $x + y = a \cdot b$. The winning probability conditioned on Bob's input b is

$$p(\mathsf{win}|b) = \frac{1}{q} \sum_{a,x} \langle\phi| (P_x^a \otimes Q_{a\cdot b-x}^b) |\phi\rangle = \frac{1}{q} \sum_a \langle\phi| \Pi_{a,b} |\phi\rangle$$

where $\Pi_{a,b} = \sum_x P_x^a \otimes Q_{a\cdot b-x}^b$. Note that $\Pi_{a,b}$ is a projector since it is the sum of a set of mutually orthogonal projectors. In order to bound $p(\mathsf{win}|b)$, we consider an extended version of the game where Bob receives two distinct inputs b and b' and produces two outputs y and y'. Here, the players win if $x + y = a \cdot b$ *and* $x + y' = a \cdot b'$. We write win for the former event and win' for the latter. It is easy to see that if $b \neq b'$, then no matter what strategy the players use, $p(\mathsf{win}, \mathsf{win}'|b,b') = 1/q$: If both winning conditions are satisfied, then $y - y' = a \cdot (b - b')$, so $a = (y - y') \cdot (b - b')^{-1}$. Since Bob does not know a, this holds with probability $1/q$. One strategy for the extended game is that Bob first applies the measurement $\{Q_y^b\}_{y\in\mathbb{F}_q}$ and then the measurement $\{Q_{y'}^{b'}\}_{y'\in\mathbb{F}_q}$ on the post-measurement state. Thus,

$$\begin{aligned}
\frac{1}{q} = p(\mathsf{win}, \mathsf{win}'|b,b') &= \frac{1}{q} \sum_{a,x} \langle\phi| \left(P_x^a \otimes Q_{a\cdot b'-x}^{b'} Q_{a\cdot b-x}^b\right) |\phi\rangle \\
&= \frac{1}{q} \sum_a \langle\phi| \left(\sum_x P_x^a \otimes Q_{a\cdot b'-x}^{b'} Q_{a\cdot b-x}^b\right) |\phi\rangle \\
&= \frac{1}{q} \sum_a \left\| \sum_x \left(P_x^a \otimes Q_{a\cdot b'-x}^{b'} Q_{a\cdot b-x}^b\right) |\phi\rangle \right\|^2
\end{aligned}$$

where we use that the $\{P_x^a\}_x$ are mutually orthogonal projectors. Using that

$$\sum_x P_x^a \otimes Q_{a\cdot b'-x}^{b'} Q_{a\cdot b-x}^b = \sum_{x,x'} (P_x^a \otimes Q_{a\cdot b'-x}^{b'})(P_{x'}^a \otimes Q_{a\cdot b-x'}^b) = \Pi_{a,b}\Pi_{a,b'}$$

we conclude that $\sum_a \|\Pi_{a,b'}\Pi_{a,b} |\phi\rangle\|^2 = 1$. It follows that $\sum_a \|\Pi_{a,b'}\Pi_{a,b} |\phi\rangle\| \leq \sqrt{q}$.

It holds that

$$\begin{aligned}
p(\mathsf{win}) = \frac{1}{N}\sum_b p(\mathsf{win}|b) &= \frac{1}{qN}\sum_{a,b} \langle\phi|\,\Pi_{a,b}\,|\phi\rangle \\
&= \frac{1}{qN}\sum_a \langle\phi|\sum_b \Pi_{a,b}\,|\phi\rangle \\
&\leq \frac{1}{qN}\sum_a \left\|\sum_b \Pi_{a,b}\,|\phi\rangle\right\| \text{ by Cauchy-Schwarz} \\
&\leq \frac{1}{qN}\sum_a \left(1 + \sum_{b\neq b'} \|\Pi_{a,b}\Pi_{a,b'}\,|\phi\rangle\|\right) \text{ by Lemma 5.11} \\
&= \frac{1}{N} + \frac{1}{qN}\sum_{b\neq b'}\sum_a \|\Pi_{a,b}\Pi_{a,b'}\,|\phi\rangle\,\| \\
&\leq \frac{1}{N} + \frac{N(N-1)\sqrt{q}}{qN} \\
&\leq \frac{1}{N} + \frac{N-1}{\sqrt{q}}
\end{aligned}$$

□

5.4.3 Binding Property of the Commitment Scheme

Theorem 5.12. *The $\mathcal{CHSH}^q$ scheme is ε-fairly-weak-binding for $\varepsilon = 2/\sqrt[4]{q}$.*

Proof. Fix a commit strategy $\overline{\mathsf{com}}_{PQ}$ against the scheme. Enumerate the elements of $\mathbb{F}_q$ as $s_1, \ldots, s_q$, and for every $i \in \{1, \ldots, q\}$ let $\overline{\mathsf{open}}^i_{PQ}$ be an opening strategy maximizing $p_i := p(s = s_i)$, where s is the output of the verifier when P and Q use this strategy. We assume without loss of generality that the p_is are in descending order. We define $p(\hat{s})$ as follows. Let $N \geq 2$ be an integer which we will fix later. By Theorem 5.10, it holds that

$$\sum_{i=1}^{N} p_i \leq 1 + \frac{N(N-1)}{\sqrt{q}}$$

where we let $p_i = 0$ for $i > q$ in case $N > q$. To see that this inequality holds, consider the game CHSH^q_S with $S = \{s_1, \ldots, s_N\}$. We let Alice produce her output x using the strategy $\overline{\mathsf{com}}_{PQ}$ and we let Bob use the strategy $\overline{\mathsf{open}}^i_{PQ}$ on input s_i. Given that the input is s_i, this strategy succeeds with probability p_i. From our bound on the quantum value of this game, our bound on the sum of probabilities follows.

We would like to define $p(\hat{s})$ as $p(\hat{s} = s_i) := p_i - (N-1)/\sqrt{q}$ for all $i \leq N, q$; however, this is not always possible because $p_i - (N-1)/\sqrt{q}$ may be

negative. To deal with this, let N' be the largest integer such that $N' \leq N$ and $p_1, \ldots, p_{N'} \geq (N-1)/\sqrt{q}$. (We let $N' = 0$ if $p_1 < (N-1)/\sqrt{q}$.) It follows that

$$\sum_{i=1}^{N'} p_i \leq 1 + \frac{N'(N'-1)}{\sqrt{q}} \leq 1 + \frac{N'(N-1)}{\sqrt{q}} \quad \text{and thus} \quad \sum_{i=1}^{N'} p_i = 1 + N'(N-1)\cdot\varepsilon$$

for some $\varepsilon \leq 1/\sqrt{q}$. We now set $p(\hat{s})$ to be $p(\hat{s} = s_i) := p_i - (N-1)\varepsilon \geq 0$ for all $i \leq N'$. Now consider an opening strategy $\overline{\mathsf{open}}_{PQ}$ and let $p(s)$ be the resulting output distribution. By definition of the p_i, it follows that $p(s = s_i) \leq p_i$ for all $i \leq q$, and $p_i \leq p(\hat{s} = s_i) + (N-1)/\sqrt{q}$ for all $i \leq N'$. It follows that there is a joint distribution $p(\hat{s}, s)$ with $p(\hat{s} = s = s_i) = \min\{p(s = s_i), p(\hat{s} = s_i)\} \geq p(s = s_i) - (N-1)/\sqrt{q}$ for all $i \leq N'$, and thus $p(\hat{s} \neq s = s_i) = p(s = s_i) - p(\hat{s} = s = s_i) \leq (N-1)/\sqrt{q}$ for all $i \leq N'$. Furthermore, when $N' < i \leq N$, we have $p(\hat{s} \neq s = s_i) = p(s = s_i) \leq p_i < (N-1)/\sqrt{q}$ by definition of N'. Since the p_i are sorted in descending order, it follows that for all $i > N$

$$p(\hat{s} \neq s = s_i) = p(s = s_i) \leq p_i \leq p_N \leq \frac{1}{N}\sum_{i=1}^{N} p_i \leq \frac{1}{N} + \frac{N-1}{\sqrt{q}}$$

and thus, we have shown for all $s_\circ \in \mathbb{F}_q$ that

$$p(\hat{s} \neq s = s_\circ) \leq \frac{1}{N} + \frac{N-1}{\sqrt{q}}.$$

We now select N so that this value is minimized: it is easy to verify that the function $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, $x \mapsto 1/x + (x-1)/\sqrt{q}$ has its global minimum in $\sqrt[4]{q}$; thus, we pick $N := \lceil \sqrt[4]{q} \rceil$, which gives us

$$p(\hat{s} \neq s = s_\circ) \leq \frac{1}{N} + \frac{N-1}{\sqrt{q}} \cdot \varepsilon \leq \frac{1}{\sqrt[4]{q}} + \frac{\sqrt[4]{q}}{\sqrt{q}} = \frac{2}{\sqrt[4]{q}}$$

for any $s_\circ \in \mathbb{F}_q$, as claimed. □

5.5 The Composition Theorem

5.5.1 The Composition Operation

Besides considering adversaries with quantum capabilities, this composition theorem also differs from the previous one in that it composes a weak-binding and binding scheme to produce a weak-binding scheme. The structure of the proof is somewhat different as well: In the proof of the classical composition theorem, we composed a "small" $\mathcal{S}$ (in the sense that only one prover communicates with the verifier in the commit phase and only the other in the

opening phase) with a "big" $\mathcal{S}'$. In the proof of our composition theorem for the quantum case, we instead compose a "big" $\mathcal{S}$ with a small $\mathcal{S}'$. This requires a slightly different definition of eligible pairs $(\mathcal{S}, \mathcal{S}')$ where some properties of $\mathcal{S}$ and $\mathcal{S}'$ are reversed:

Definition 5.13. *Let $\mathcal{S}$ and $\mathcal{S}'$ be two 2-prover string-commitment schemes with domains D and D', respectively. We call the pair $(\mathcal{S}, \mathcal{S}')$* eligible *if they are both classical (i.e., no quantum communication or computation is required on the part of the honest verifier and provers) and the following two properties hold, or they hold with the roles of P and Q exchanged.*

1. *The commit phase of $\mathcal{S}$ is a protocol com_{PQV} that involves communication between P and V only. The commit phase of $\mathcal{S}'$ is a protocol com'_{PQV} that involves communication between Q and V only and the opening phase is a protocol open'_{PQV} involving communication between P and V only.*

2. *The last round of open_{PQV} is of the following simple form: Q sends some $y \in D'$ to V who computes the output deterministically as $s = \mathsf{Extr}(y, \bar{c})$ where $\bar{c}$ consists of all communication in the previous rounds (including the commit phase). We call this message y the* final opening information*.*

Furthermore, we specify that the possible attacks on $\mathcal{S}$ are so that P and Q do not communicate during the course of the commit phase, but there may be some limited communication during the opening phase. The possible attacks on $\mathcal{S}'$ are so that P and Q do not communicate during the course of the entire execution of the scheme.

The composition operation $\mathcal{S} \star \mathcal{S}'$ is defined in the same way as in the classical setting: instead of sending the opening information y in the last round, the provers instead use $\mathcal{S}'$ to commit to y and then open the commitment. We define the possible attacks $(\overline{\mathsf{com}}_{PQ}, \overline{\mathsf{open}}''_{PQ})$ on $\mathcal{S} \star \mathcal{S}'$ to be those where $\overline{\mathsf{com}}_{PQ}$ is a commit strategy for $\mathcal{S}$ and $\overline{\mathsf{open}}''_{PQ}$ can be decomposed as $\overline{\mathsf{open}}'_{PQ} \circ \overline{\mathsf{com}}'_{PQ} \circ \mathsf{ptoq} \circ \overline{\mathsf{open}}^*_{PQ}$ where ptoq allows P to send a quantum state to Q, $\overline{\mathsf{open}}^*_{PQ}$ is an opening strategy for $\mathcal{S}$ excluding the last round. For any input state ρ_{PQ}, $\overline{\mathsf{com}}'_{PQ}(\rho_{PQ})$ is a commit strategy and $\overline{\mathsf{open}}'_{PQ}$ is an opening strategy for $\mathcal{S}'$.

5.5.2 The Composition Theorem

In the following composition theorem, we take it as understood that the assumed respective binding properties of $\mathcal{S}$ and $\mathcal{S}'$ hold with respect to a well-defined respective classes of possible attacks.

Theorem 5.14. *Let $(\mathcal{S}, \mathcal{S}')$ be an eligible pair of 2-prover commitment schemes, and assume that $\mathcal{S}$ is ε-fairly-weak-binding and that $\mathcal{S}'$ is δ-fairly-binding. Then, their composition $\mathcal{S}'' = \mathcal{S} \star \mathcal{S}'$ is a $(\varepsilon + k(\mathcal{S}) \cdot \delta)$-fairly-weak-binding 2-prover commitment scheme.*

Proof. We first consider the case where $k(\mathcal{S}) = 1$. We fix an arbitrary possible strategy $(\overline{\mathsf{com}}_P, \overline{\mathsf{open}}''_{PQ})$ against $\mathcal{S}''$, where $\overline{\mathsf{open}}''_{PQ}$ is of the form $\overline{\mathsf{open}}''_{PQ} = \overline{\mathsf{open}}'_{PQ} \circ \overline{\mathsf{com}}'_{PQ} \circ \mathsf{ptoq} \circ \overline{\mathsf{open}}^*_{PQ}$. We decompose and reassemble the strategy into strategies against $\mathcal{S}$ and $\mathcal{S}'$. The strategy for $\mathcal{S}'$ uses a shared quantum state ρ_{PQ} of appropriate size and works by executing $\overline{\mathsf{com}}'_{PQ}(\rho_{PQ})$ and then $\overline{\mathsf{open}}'_{PQ}$. By the δ-fairly-binding property of $\mathcal{S}'$, there exists a measurement $\mathsf{Eval} = \{M_{\hat{y}}\}_{\hat{y}}$ depending only on $\overline{\mathsf{com}}'_{PQ}$ which Q can apply after $\overline{\mathsf{com}}$ such that $p(y \neq \hat{y} \wedge y = y_\circ) \leq \delta$ for every $y_\circ$, where y is the output of $\overline{\mathsf{open}}_{PQV}$. This holds for every possible shared quantum state ρ_{PQ}, and in particular for the ones generated as follows: Let σ_{PQV} be the quantum state after an execution of $\overline{\mathsf{com}}_{PQV}$ and $\overline{\mathsf{open}}^*_{PQV}$. This execution involves sending classical messages $\bar{c}$ between the provers and the verifier. Thus, we may write $\sigma_{PQV} = \sum_{\bar{c}} p(\bar{c})\sigma^{\bar{c}}_{PQV}$. Writing $p(y, \hat{y}|\bar{c})$ for the distribution of the output and the measurement outcome when using the shared quantum state $\rho_{PQ} = \sigma^{\bar{c}}_{PQ}$, it holds that $p(y \neq \hat{y} \wedge y = y_\circ|\bar{c}) \leq \delta$.

Note that $\overline{\mathsf{com}}_P$ is a commit strategy for $\mathcal{S}$. As such, by the weak-binding property of $\mathcal{S}$, there exists a distribution $p(\hat{s})$, only depending on $\overline{\mathsf{com}}_P$, so that Definition 3.9 is satisfied for every opening strategy $\overline{\mathsf{open}}_Q$ for $\mathcal{S}$. In particular, this holds for the following opening strategy:

1. The provers execute $\overline{\mathsf{open}}^*_{PQ}$.
2. Q simulates an execution of $\overline{\mathsf{com}}'_Q$ and performs the measurement Eval with result $\hat{y}$.
3. Q sends $\hat{y}$ to V.

By the ε-fairly-weak binding property of $\mathcal{S}$, there is a consistent joint distribution $p(s, \hat{s})$ such that for every $s_\circ$, $p(\tilde{s} \neq \hat{s} \wedge \tilde{s} = s_\circ) \leq \varepsilon$ where $\tilde{s} = \mathsf{Extr}(\hat{y}, \bar{c})$. Let $y_\circ(\bar{c})$ be such that $\mathsf{Extr}(y_\circ, \bar{c}) = s_\circ$ (or some default value if no such $y_\circ$ exists). Since we assume that $k(\mathcal{S}) = 1$, there is only one possible value for $y_\circ(\bar{c})$. Recalling that $s = \mathsf{Extr}(y, \bar{c})$, it holds that

$$\begin{aligned}
p(\hat{s} \neq s \wedge s = s_\circ) &= p(\hat{s} \neq s \wedge s = s_\circ \wedge s = \tilde{s}) + p(\hat{s} \neq s \wedge s = s_\circ \wedge s \neq \tilde{s}) \\
&\leq p(\hat{s} \neq \tilde{s} \wedge \tilde{s} = s_\circ) + p(\mathsf{Extr}(y, \bar{c}) \neq \mathsf{Extr}(\hat{y}, \bar{c}) \wedge \mathsf{Extr}(y, \bar{c}) = s_\circ) \\
&\leq p(\hat{s} \neq \tilde{s} \wedge \tilde{s} = s_\circ) + \sum_{\bar{c}} p(\bar{c}) p(y \neq \hat{y} \wedge y = y_\circ(\bar{c})|\bar{c}) \\
&\leq \varepsilon + \delta
\end{aligned}$$

and in the case that $k(\mathcal{S}) > 1$, it is easy to see that we can upper-bound this probability with $\varepsilon + k(\mathcal{S})\delta$. □