8 Quantum cryptography using untrusted devices

In this chapter we introduce a variant of the BB'84 quantum key distribution protocol from the previous chapter. This variant is due to Ekert and is often referred to as the E'91 protocol for quantum key distribution. Since our protocol won't exactly follow Ekert's original proposal we will call it the "DIQKD protocol". The acronym DI stands for "device independent." What this means, informally, is that the new protocol's security doesn't rely on Alice and Bob performing trusted measurements on their qubit in each round — in fact, it doesn't even rely on the assumption that the system they measure in each round is a qubit! In other words, we partially drop assumption number 2 in Box **??**, thereby obtaining a higher level of security than the BB'84 protocol. As a counterpart the Ekert protocol is more difficult to implement as it requires the users to have the ability to distribute EPR pairs quickly and make rather accurate measurements on them.

The key difference between the DIQKD protocol and the BB'84 protocol is that in the DIQKD protocol we replace the "matching outcomes" test used in BB'84 by a different test. The new test is based on the CHSH game, which we introduced in Chapter **??**. Using the monogamous properties of entanglement the test will let us to show security in the more general DI setting. Let's see how this works.

8.1 The DIQKD protocol

Before we describe the protocol, let's see precisely what the notion of device-independent security covers — and does not cover.

8.1.1 Device-independent security

Week 7, Lecture 7.1,Lecture 1: Device-independent cryptography

The notion of device independence is motivated by the practical difficulty of characterizing the quantum mechanical devices, such as photon emitters or receptors, used in protocols such as BB'84. You remember that this protocol asks Alice to do things such as "prepare a qubit in the Hadamard basis", and Bob to "measure his qubit in the standard basis". When Alice prepares her qubit, and when Bob measures it, can they really trust their equipment to implement the task correctly? What if for example Alice's preparation device sometimes in fact creates *two* qubits, instead of a single one, without her noticing; could the additional qubit be intercepted by Eve and provide her with secret information, without Alice or Bob noticing? The following exercise shows that such misbehavior of Alice and Bob's equipment can indeed pose a serious security risk.

Example 8.1.1 *Consider the purified variant of the BB'84 protocol. Suppose that Eve prepares a*

state ρ_{ABE} of the following form:

$$\rho_{ABE} = \sum_{x,z=0}^{1} |x,z\rangle\langle x,z|_A \otimes |x,z\rangle\langle x,z|_B \otimes |x,z\rangle\langle x,z|_E . \tag{8.1}$$

Here A and B are each made of two qubits, instead of just one as required in the protocol. Nevertheless, suppose that Alice and Bob don't notice this: after all, a single photon isn't that easy to spot! Suppose further that their measurement devices, instead of measuring in the standard or Hadamard bases, as they think, in fact perform the following:

- *When the device is told to measure in the standard basis, it measures the first qubit of the two-qubit system associated with the device, A or B, in* (8.1) *in the standard basis;*
- *When the device is told to measure in the Hadamard basis, it measures the second qubit of the two-qubit system associated with the device in* (8.1) *in the standard basis.*

Such devices will perfectly pass all tests performed in the protocol: indeed, you can verify that for the state in (8.1) *when the basis choice is the same the outcome is the same, whereas when the bases are different the outcomes are perfectly uncorrelated. But any key extracted from ρ_{ABE} in* (8.1) *is completely insecure! (Exercise: Give an explicit attack for Eve.)* ∎

Although the example may look like a bit of a stretch, similar attacks have been implemented in practice. In fact one of the first real "attacks" on the BB'84 protocol is that the photon receptor used in an early experiment made a different clicking noise when it measured in one of Bob's bases, thereby "leaking" Bob's choice of measurement basis to any eavesdropper within earshot! (This is an example of a failure of the assumption "Bob's laboratory is safe" from Box **??**.) Many such attacks, often called *side-channel attacks*, have been demonstrated. Some of the most effective are called "detector blinding" attacks, in which the eavesdropper can take complete control of Bob's measurement device by shining a very bright laser right into it (without Bob noticing!). The problem is that while quantum information can in principle bring us great security, it is also very fragile and hence suceptible to unexpected attacks. Is there a way that we can better protect ourselves?

This is the goal of device-independent security. This notion aims to guarantee security even when there may be dramatic failures of Alice and Bob's equipment, and moreover that such failures could be exploited by an adversary. Now, we have to be careful about what we promise exactly. For example, as an extreme case we could imagine that Bob's device contains radio equipment that automatically transmits all its measurement results to Eve: in this case security is compromised, but there is no way for Bob to detect the radio transmitter unless he opens the device. Similarly, if the random number generator used by Alice to make her basis choices is biased, or controlled by Eve, then security cannot hold. The specific kinds of failures that are allowed by a device-independent proof of security have to be specified on a case-by-case basis. For quantum key distribution we will make the following assumptions, which refine item 2 from Box **??**:

2.a Alice and Bob's labs are perfectly isolated: once the protocol starts no information enters or exits their respective labs unless specified by the protocol.

2.b Alice and Bob's random number generators are perfect.

2.c The measurement devices used by Alice and Bob to perform measurements are arbitrary. These devices are initialized in a state ρ_{ABE} that may be chosen by the adversary. At each step of the protocol, each of Alice and Bob's devices makes a measurement when instructed, and always produces an outcome $x \in \{0,1\}$. The measurement that is performed is arbitrary. In particular, the device may have memory and behave differently in each round.

2.d At the end of the protocol the devices are discarded and will never be re-used. They will never fall in Eve's hands.

As you can see the main novelty in device-independence is assumption 2.c, which allows the devices to perform any kind of measurement, on any state; both may have been decided by Eve as part of her "attack". In the analysis of the BB'84 protocol in the previous chapter we allowed Eve to prepare any state for the devices, *but* Alice and Bob still had to receive a single qubit, and they could trust the way that measurements were made on that qubit (indeed, this was instrumental to the use of uncertainty relations). Here we remove that assumption.

We mention that the last assumption, while not crucial in our context, is important when we think about the problem of *composition*, which arises when trying to combine different cryptographic protocols, in sequence or even simultaneously and involving overlapping sets of users: this is because in the DIQKD protocol the devices themselves know Alice and Bob's raw key,[1] and could potentially store it in memory. So it is important that the devices are not re-used in another protocol where Alice and Bob might want to use the key produced with those devices.

Quiz 8.1.1 *In the device-independent setting, attacks by Eve can be modeled by specifying what kinds of devices she gives to Alice and Bob. Which of the following attacks do we hope our device-independent protocol to protect against?*

a) Alice's devices communicate with Bob's devices during the protocol.
b) Eve gets to examine Alice and Bob's devices at the end of the protocol.
c) Alice's devices send information to Eve during the protocol.
d) $\longrightarrow$ ***Eve's laboratory is arbitrarily entangled with Alice and Bob's laboratory at the beginning of the protocol.***

8.1.2 The protocol

Week 7, Lecture 7.3,Lecture 1: A protocol for device-independent QKD
Week 7, Lecture 7.3,Lecture 2: The CHSH guessing game

We are almost ready to describe the DIQKD protocol. As already mentioned the protocol is based on the CHSH game. However, we need to make a small modification to the game in order to make it useful for quantum key distribution. (If you don't remember the CHSH game, now is a good time to check the rules again.) Indeed, in the honest optimal strategy for the CHSH game (Box **??**) Alice and Bob never use the same basis, and thus they never obtain perfectly correlated outcomes. However in order to produce a key it will be convenient for them to obtain (almost) perfectly correlated outcomes for at least one choice of a pair of bases. To make this possible in the protocol we think of Bob's device as having three, instead of two, possible measurement settings. Since in the device independent setting we don't assume that we know what measurements are made, we will label them using a value $\theta \in \{0, 1\}$ for Alice, where $\theta = 0$ means that Alice is asking for a standard basis measurement and $\theta = 1$ means a Hadamard basis measurement, and $\tilde{\theta} \in \{0, 1, 2\}$ for Bob, where $\tilde{\theta} \in \{0, 1\}$ correspond to the usual CHSH inputs (for which the ideal device would measure in the basis described in Box **??**), and the additional value $\tilde{\theta} = 2$ instructs the device to measure in the standard basis. We refer to the values of $\theta, \tilde{\theta}$ as *inputs* that the user introduces into their device, asking for a measurement outcome to be returned. Since Alice's device also measures in the standard basis on input 0, and since the honest devices share an EPR pair, this means that on inputs $(\theta, \tilde{\theta}) = (0, 2)$ the devices are expected to produce matching outcomes.

[1] Recall that the *raw key* is the string of bits obtained by each user as a result of their measurements in the protocol, and before the classical post-processing steps of information reconciliation and privacy amplification.

Protocol 1 (DIQKD protocol) *The protocol depends on a large integer n and a small parameter $\delta_{\max} > 0$ publicly chosen by the users (intuitively n is the number of bits of key that they expect to generate at the end and $\delta_{\max}$ is an error tolerance). Let $N = 12(1 + C\delta_{\max})n$, where C is a large constant that can be determined from the security analysis. Alice and Bob execute the following:*

1 *Alice chooses a uniformly random basis string $\theta = \theta_1, \ldots, \theta_N \in \{0,1\}^N$ and sequentially instructs her measurement device to measure in the bases θ. The device returns a string of outcomes $x = x_1, \ldots, x_N \in \{0,1\}^N$.*
2 *Bob chooses a uniformly random basis string $\tilde{\theta} = \tilde{\theta}_1, \ldots, \tilde{\theta}_N \in \{0,1,2\}^N$ and sequentially instructs his measurement device to measure in the bases $\tilde{\theta}$. The device returns a string of outcomes $\tilde{x} = \tilde{x}_1, \ldots, \tilde{x}_N \in \{0,1\}^N$.*
3 *Alice and Bob tell each other their basis strings θ and $\tilde{\theta}$ respectively over the CAC.*
4 *Alice picks a random subset $T \subseteq \{1, \ldots, N\}$ by flipping a fair coin for each $i \in \{1, \ldots, N\}$ to decide if it is selected in T. Alice tells Bob what T is over the CAC. They each set $T' = \{j \in T, \tilde{\theta}_j \in \{0,1\}\}$, $T'' = \{j \in T, \theta_j = 0 \wedge \tilde{\theta}_j = 2\}$, and $R = \{j \notin T, \theta_j = 0 \wedge \tilde{\theta}_j = 2\}$.*
5 *Alice and Bob announce x_T and $\tilde{x}_T$ to each other over the CAC. They compute the success probabilities $p_{\text{win}} = |\{j \in T', x_j \oplus \tilde{x}_j = \theta_j \wedge \tilde{\theta}_j\}|/|T'|$ and $p_{\text{match}} = |\{j \in T'', x_j = \tilde{x}_j\}|/|T''|$. If $p_{\text{win}} < \cos^2 \pi/8 - \delta_{max}$ or $p_{\text{match}} < 1 - \delta_{\max}$ they abort.*
6 *Let x_{remain} and $\tilde{x}_{\text{remain}}$ be Alice and Bob's outcomes restricted to indices in R. Alice and Bob perform information reconciliation and privacy amplification on x_{remain} and $\tilde{x}_{\text{remain}}$.*

In the protocol description we have not fleshed out the last step in full detail, because it is identical to the last steps of the BB'84 protocol with noise presented in the previous chapter. The important difference here is step 5, which plays the role of step 7 from the purified BB'84 protocol.

Before we proceed let's check the expected length of key produced by this protocol. Because the values $\theta_i, \tilde{\theta}_i$ are chosen uniformly at random we expect that

$$|R| \approx \frac{1}{6}|\{1, \ldots, N\} \backslash T| \approx \frac{1}{6}\frac{N}{2} = (1 + C\delta_{max})n \ .$$

As we will see, the steps of information reconciliation and privacy amplification lead to a moderate loss in the raw keys x_{remain} and $\tilde{x}_{\text{remain}}$, so that if the constant C is chosen large enough we can count on obtaining roughly n bits of final key.

How can we show security of this protocol? Based on the work done in the previous chapters we already know that it is sufficient to show two things. First of all, we need to show that the entropy $H_{\text{min}}(X_{\text{remain}}|E)$, evaluated on the state of the users at step 6 in the protocol conditioned on not aborting in step 5, is large. Second, we also need to make sure that $X_{\text{remain}} \approx \tilde{X}_{\text{remain}}$, as this will allow us to bound how much information is leaked to Eve in the step of information reconciliation.

If we make the i.i.d. assumption (Box **??**) then using the condition $p_{\text{match}} < 1 - \delta_{max}$ from step 5 and a similar analysis as in Section **??** in the previous chapter it is possible to show that leakage from information reconciliation is of order $h(\delta_{max})|R|$, which can be made arbitrarily small by taking $\delta_{\max}$ small enough. Therefore we focus on the first condition, guaranteeing uncertainty from Eve. In the previous chapter we saw how this condition, which was summarized in Eq. (**??**), can be achieved using three different methods: a direct method based on interpreting the matching outcomes game as an "entanglement projection test," a method based on guessing games, and a method based on uncertainty relations. Here we focus on the method that generalizes best to the device-independent setting, the use of guessing games, and introduce a new guessing game adapted to the CHSH test used in the protocol. (We will see we also use ideas from the method based on uncertainty relations.) The first method, which characterizes the entanglement shared by the users, can also be extended, and we will give the main ideas for taking this route in Section 8.3.

8.2 Security of device-independent quantum key distribution

Week 7, Lecture 7.4,Lecture 1: Security against collective attacks
Week 7, Lecture 7.4,Lecture 2: A candidate attack on DIQKD
Week 7, Lecture 7.5,Lecture 1: Security against general attacks
Week 7, Lecture 7.5,Lecture 2: Playing games in parallel

We start our security argument by focusing on a single round of the protocol, and analyze the adversary's power to gain information about Alice's output using a new tripartite guessing game.

8.2.1 A CHSH-based guessing game

Week 7, Lecture 7.2,Lecture 1: Testing entanglement using the CHSH game

Let's consider the following guessing game. By studying this game we will be able to show a bound on Eve's uncertainty in the DIQKD protocol. In the game there are three players, Alice, Bob and Eve. Alice receives an input $\theta \in \{0,1\}$, Bob receives $\tilde{\theta} \in \{0,1,2\}$, and Eve receives no input (if you prefer you can think that her input is always the same). The players have to produce answers $x, \tilde{x}, z \in \{0,1\}$ respectively. They win the game if and only if both of the following conditions hold:

- If $\tilde{\theta} \in \{0,1\}$ then $x \oplus \tilde{x} = \theta \wedge \tilde{\theta}$.
- If $\theta = 0$ and $\tilde{\theta} = 2$ then $x = z$.

Note that the two conditions never apply simultaneously. However, Alice in general doesn't know which condition is going to be checked (because if her input is $\theta = 0$ then both could in principle apply), and this is what makes the game hard: on the one hand, Alice wants to play the CHSH game the best she can with Bob, but on the other hand she wants to make sure that Eve has a way of knowing what outcome she'll get. If this sounds impossible, indeed it is! The following exercise asks you to show a bound on the maximum winning probability in the game.

Exercise 8.2.1 Suppose that Alice and Bob play the game according to the optimal CHSH strategy, and Eve always returns a uniformly random $z \in \{0,1\}$. Show that this strategy succeeds with probability

$$p_{\min} = \frac{2}{3}\cos^2\frac{\pi}{8} + \frac{1}{6} + \frac{1}{6}\cdot\frac{1}{2}$$

in the game. *[Hint: consider all* 6 *possible cases for the questions]*

Exercise 8.2.2 Show that it is impossible to win in this game with probability larger than

$$p_{\max} = \frac{2}{3}\cos^2\frac{\pi}{8} + \frac{1}{6} + \frac{1}{6}\,.$$

[Hint: What is the maximum probability for winning in the CHSH game?]

There is a gap between $p_{\min}$ and $p_{\max}$ obtained in the exercises. What is the right answer? As it turns out, the correct maximum is exactly $p_{\min}$. Intuitively this is because in order to win with probability close to $\cos^2 \pi/8$ in the CHSH part of the game Alice *has* to measure an EPR pair and hence return random outcomes that Eve couldn't possibly predict with probability more than $\frac{1}{2}$. This is a version of the phenomenon of *monogamy* which we already encountered in Section **??** in Chapter **??**. Concretely, it is possible to show the following trade-off.

Lemma 8.2.1 (CHSH guessing lemma) *Consider an arbitrary strategy for the players in the* CHSH *guessing game. Let ω be the probability that the first test passes (conditioned on $\tilde{\theta} \in \{0,1\}$) and γ the probability that the second test passes (conditioned on $\theta = 0$ and $\tilde{\theta} = 2$). Suppose that $\omega \geq \cos^2 \pi/8 - \delta$ for some $0 \leq \delta \leq 1/2$. Then $\gamma \leq 1/2 + 2\sqrt{\delta}$.*

We leave the proof of the lemma as an exercise. There are different possible ways to approach it. We indicate one possible proof strategy, which formalizes the intuition described earlier. The first step is to characterize the state shared by Alice and Bob as being close to an EPR pair using the condition $\omega \geq \cos^2 \pi/8 - \delta$. This can be done by building on the contents of Section 8.3 below. The second step, which is easier, uses that if Alice and Bob share a perfect EPR pair, then Eve has no information about Bob's outcomes.

From the lemma we get that the maximum winning probability in the game is the maximum over all possible $0 \leq \delta \leq 1/2$ of the expression

$$p_{\text{win}} \leq \frac{2}{3}\big(\cos^2 \frac{\pi}{8} - \delta\big) + \frac{1}{6} + \frac{1}{6}\Big(\frac{1}{2} + 2\sqrt{\delta}\Big).$$

You can easily verify that the right-hand side is always less than $p_{\min}$, as claimed. This bound is the analogue of the bound $p_{\text{win}} \leq \frac{1}{2} + \frac{1}{2\sqrt{2}}$ shown on the tripartite guessing game from Chapter **??**.

8.2.2 Security under the i.i.d. assumption

Let's move on to show security of the DIQKD protocol in the i.i.d. setting (Box **??**). As we saw in the previous chapter, under the i.i.d. assumption in order to get a bound on the final uncertainty $H_{\min}(X_{\text{remain}}|E)$ it suffices to show a bound on the uncertainty in each round of the protocol as measured by the conditional von Neumann entropy $H(X_i|E\Theta_i = 0)$, where Θ_i is Alice's choice of basis and X_i her measurement outcome in the i-th round of the protocol. In this expression we condition on $\Theta_i = 0$, because this is the only case which is used to create the raw key. Let's see how we can get such a bound using Lemma 8.2.1. First of all, we always have

$$H(X_i|E\Theta_i = 0) \geq H_{\min}(X_i|E\Theta_i = 0)\ , \tag{8.2}$$

because the min-entropy is the "smallest" entropy measure.[2] We also know that $H_{\min}(X_i|E\Theta_i = 0)$ has an interpretation as the maximum probability with which Eve, given access to the quantum system E, can guess the outcome X_i (when $\Theta_i = 0$). This is exactly the quantity γ that is estimated in Lemma 8.2.1. Precisely, from the lemma we get that

$$P_{guess}(X_i|E\Theta_i = 0) \leq \frac{1}{2} + 2\sqrt{\cos^2 \frac{\pi}{8} - \omega_i}\ ,$$

where ω_i is the probability that Alice and Bob's outputs in the i-th round satisfy the CHSH conditions, conditioned on their inputs being chosen in $\{0,1\}$. Taking the logarithm and using (8.2) we get

$$H(X_i|E\Theta_i = 0) \geq -\log\Big(\frac{1}{2} + 2\sqrt{\cos^2 \frac{\pi}{8} - \omega_i}\Big) = 1 - O(\sqrt{\delta_i})\ , \tag{8.3}$$

where $\delta_i = \cos^2 \pi/8 - \omega_i$. Eq. (8.3) shows that, as expected, the closer the winning probability is to the CHSH optimum, the more uncertainty there is in Alice's outcomes. Eq. (8.3) gives the right order asymptotically (for very small δ), and if we don't care too much about parameters, e.g. the number of

[2] Among all Rényi entropies; we ask that the reader take the inequality on faith.

rounds of the protocol that are "wasted" for testing, then it is good enough for us. If we want the optimal trade-off, by using more refined optimization techniques it is possible to obtain a more precise bound

$$H(X_i|E\Theta_i) \geq 1 - h\Big(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i(\omega_i - 1) + 3}\Big) . \tag{8.4}$$

This bound is better in general because in contrast to (8.3) any value of ω_i larger than $\frac{3}{4}$ gives a positive lower bound on the conditional entropy. This means that as soon as Alice and Bob are able to observe outcomes that surpass the classical optimum winning probability in the CHSH game, they are able to certify that their raw key contains some uncertainty!

To conclude our analysis there are a couple more steps to make. First of all, how can we infer a bound on the quantity ω_i based on data that is collected in the protocol? Second, to measure the amount of key that will eventually be produced we need to be able to estimate the size of R, the set of indices from which the raw key is taken.

Since we are making the i.i.d. assumption, in principle the users' device has a well-defined success probability $\omega = \omega_i$ in the CHSH game. Moreover, this is precisely the quantity that is estimated at step 5 of the protocol. If we assume that the number of rounds selected for testing, $|T|$, is a constant fraction of n then the quality of the user's estimate for ω can be estimated using the same technique as in Section **??**. Let's explain how to do this in detail, without even making the untrue assumption that the number of test rounds is constant. To remove that assumption we need to estimate the chance that the number of test rounds deviates by too much from its expectation value. To model the situation we introduce binary random variables $Z_1, \ldots, Z_k$, where $k = |T'|$ (remember that T' is the subset of rounds tested for the CHSH condition), such that Z_j equals 1 if the CHSH condition in round j is satisfied. Then at step 5 of the protocol the users set $p_{\text{win}} = |T'|^{-1} \sum_{j \in T'} Z_j$. Note that this is an "observed" quantity, i.e. it may vary each time we run the protocol, even with the same devices. We would like to know the "true value" ω, i.e. the probability of success of the device in the CHSH game (instead of its average success in any particular run). How different can ω and p_{CHSH} be?

Let's first start by estimating the size of T'. We can think of the inputs for the rounds T' as being selected after the set of rounds T' itself is chosen by Alice: for instance, we could imagine Bob choosing rounds in which $\tilde{\theta}_J = 2$ at random, and Alice choosing a random set T; this defines the set T' but the players still have the freedom to choose specific inputs for those rounds. Since the probability of any given round lying in T is $1/2$, and independently the probability that Bob chooses $\tilde{\theta}_j = 2$ is $1/3$, the expected size of $|T'|$ is $n/6$. To show that the chance that the actual size differs from the expected size by too much is small we need a simple concentration inequality.

Theorem 8.2.2 (Chernoff bound [?]) *Let $X_1, \ldots, X_n$ be i.i.d. random variables taking values in $\{0, 1\}$, and $\mu = \mathrm{E}[X_i]$. Then for all $0 < \alpha < 1$,*

$$\Pr\Big(\Big|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\Big| > \alpha\mu\Big) \leq 2\, e^{-\frac{\alpha^2 \mu n}{3}} .$$

If we apply the proposition with $\mu = 1/6$ and $\alpha = 1/4$ we obtain that the probability that $|T'| < n/8$ is at most $e^{-n/(3\cdot 6\cdot 16)}$. Let's assume that this is not the case. Then we can apply the same bound once more, with some different α, to obtain

$$\Pr\Big(\sum_{j \in T'} Z_j > (1+\alpha)|T'|\omega\Big) \leq 2\, e^{-\frac{\alpha^2 \hat{p}_{\text{win}} |T'|}{3}} .$$

Hence, using our lower bound on the size of $|T'|$ as well as $\omega \geq 1/2 - \sqrt{2}/4$ (Exercise: why?),

$$\Pr\big(\omega < \frac{1}{1+\alpha} p_{\text{win}}\big) \leq 2\, e^{-\frac{\alpha^2 n}{C}}$$

for some large constant C.

So far we have managed to show that, except with probability exponentially small in n, provided the protocol does not abort in step 5. of the protocol it must be the case that $\omega \geq p_{\text{win}}/(1+\alpha) \geq \cos^2 \pi/8 - 2\delta$ (if we choose $\alpha = \delta$). Now is time to apply (8.4). Churning through the numbers we arrive at

$$H(X_j|E\Theta_j) \geq 1 - h\big(c\sqrt{\delta}\big) \ , \tag{8.5}$$

for some constant c. To conclude the last thing that we need to do is to estimate the size of R. Using Theorem 8.2.2 one last time it is easy to show that with very high probability R is almost $N/12$. Using a similar reasoning as in Section **??** in the previous chapter we arrive at the bound

$$H_{\min}(X_{\text{remain}}|E) \geq \big(1 - h\big(c\sqrt{\delta}\big)\big)|R| \gtrsim \big(1 - h\big(c\sqrt{\delta}\big)\big)\frac{N}{12} \ .$$

This is not an optimal bound. What is important for us is that it depends linearly on the total number of rounds N, and so we have the guarantee that the protocol generates a linear amount of key. (Remember that to get the final key length we'd also have to subtract the information exchanged for information reconciliation, which as mentioned earlier scales like $h(\delta)|R|$.) In practice various optimizations are possible to improve this rate. In particular, in a real implementation the users would bias their choice of measurement basis so that the pair $(0,2)$ happens most of the time, and only a comparatively small subset of the rounds are used for testing. This can help make $|R|$ very close to N, instead of $N/12$ here.

We note a final subtlety in the analysis that we have glossed over. Earlier we wrote things like "assuming this holds" when computing bounds on the size of T or the CHSH winning probability. What if these conditions do not hold? What we did show is that conditioned on not aborting both conditions hold, except with probability ε that is exponentially small. What this means is that in fact we have not quite obtained a lower bound on the conditional min-entropy, but what is known as the "smooth" conditional min-entropy, usually written as $\mathrm{H}^{\varepsilon}_{\min}(X_{\text{remain}}|E)$ (see Box **??**). What the ε means is that we are not bounding the entropy directly on the state ρ_{XE} from the protocol, but on a state that is very close—the state where all the conditions that "almost surely hold" *actually* hold. While this is a hypothetical state that never arises in practice, because it is so close to the real state it is sufficient to prove security on it: no adversary will ever be able to tell a real execution from an ideal one, except with advantage ε that is exponentially small.

The previous arguments only handle the i.i.d. setting. Using a more technically involved argument it is possible to give bounds that apply in general. Such techniques lie beyond the scope of this book, but we give pointers in the chapter notes. For concreteness, and not insisting on actual parameters, we give a typical formulation for a complete security statement that can be shown about the DIQKD protocol.

Theorem 8.2.3 *The DIQKD protocol, Protocol 1, satisfies the following properties. There is a $0 < \kappa \leq 1$ and $C \geq 1$ (depending on the tolerance parameter δ) such that the following hold for $\ell = \kappa n$ and $\varepsilon \leq 2^{-Cn}$.*

First, there is an implementation of the devices such that the protocol does not abort with probability at least $1 - \varepsilon$.

Second, for any implementation of the devices, either the protocol aborts with probability larger than $1 - \varepsilon$, or conditioned on not aborting Alice and Bob each produces a key K_A of length ℓ such that $\Pr(K_A \neq K_B) \leq \varepsilon$ and

$$(1 - \Pr(\text{abort}))\left\|\rho_{KE} - \frac{\mathbb{I}_K}{2^\ell} \otimes \rho_E\right\|_1 \leq \varepsilon,$$

where ρ_{KE} is the joint state of the key K_A output by Alice and all the side information available to the eavesdropper at the end of the protocol, conditioned on the protocol not aborting.

Quiz 8.2.1 *Suppose that Alice and Bob perform the DIQKD protocol described in the chapter and succeed in 850 out of 1000 CHSH test rounds. What can we say about p_{win}, the probability that the CHSH test is passed on a future test round?*

a) $p_{win} = 0.85$ *with certainty.*
b) $p_{win} = 0.85$ *with high probability.*
c) $\longrightarrow$ $|p_{win} - 0.85|$ ***is small with high probability.***
d) $|p_{win} - 0.85|$ *is small with certainty.*

Quiz 8.2.2 *In the chapter we proved security for the collective setting, i.e. when Eve attacks each round of the protocol independently. Which of the following parts of the proof break when we move to the coherent setting, i.e. we no longer demand that ρ_{ABE} is the tensor product of $N \approx 12n$ identical states?*

a) The winning probability of the CHSH game on a random subset of rounds no longer predicts the winning probability on the rest of the rounds.
b) $\longrightarrow$ ***The entropy guarantees from individual rounds of the tripartite guessing game no longer gives an entropy guarantee on the whole key.***
c) Classical correlation inequalities fail when applied to random variables coming from measurements on entangled states.

8.3 Testing EPR pairs

We end the chapter with an optional section on a phenomenon called "rigidity" of the CHSH game. Remember that in the previous chapter (see Section **??**) we argued that the "matching outcomes" test has essentially the same effect as projecting the state ρ_{ABE} on an EPR pair between A and B. This, however, crucially relied on the fact that measurements made by Alice and Bob used in the protocol are fully characterized. To see where this played a role, see for example Exercise **??** and the formula for Π_1 and Π_2; these are only correct because we *know* which basis the users are measuring in.

Now we would like to argue that a similar effect is achieved by the test based on the CHSH game, *without* needing to assume anything about the user's measurements! To get started on this let's recall the standard version of the CHSH game (not the one with an extra input that we used for the DIQKD protocol). In the game the referee sends each of the two players, Alice and Bob, a uniformly random bit $x, y \in \{0, 1\}$ respectively. The players have to return outcomes $a, b \in \{0, 1\}$ such that the CHSH condition $a \oplus b = x \wedge y$ is satisfied. We saw that the maximum success probability of classical non-communicating players in this game is $p_{\text{win}} = 3/4$, while if Alice and Bob are quantum there is a strategy that allows them to succeed with probability $p^*_{\text{win}} = \cos^2 \pi/8 \approx 0.85$.

In the strategy described in Box **??** Alice and Bob share an EPR pair $|\text{EPR}\rangle_{AB}$ and make the following measurements. When $x = 0$, Alice measures her qubit in the standard basis $\{|0\rangle, |1\rangle\}$, and when $x = 1$ she measures in the Hadamard basis $\{|+\rangle, |-\rangle\}$. When $y = 0$, Bob measures his qubit in the basis

$$\{\cos(\pi/8)\,|0\rangle + \sin(\pi/8)\,|1\rangle\,, -\sin(\pi/8)\,|0\rangle + \cos(\pi/8)\,|1\rangle\}$$

and when $y = 1$, he measures in the basis

$$\{\cos(\pi/8)\,|0\rangle - \sin(\pi/8)\,|1\rangle\,, \sin(\pi/8)\,|0\rangle + \cos(\pi/8)\,|1\rangle\}\,.$$

Since these measurements are binary projective measurements, with POVM elements of the form $\{\Pi, \mathbb{I} -$

$\Pi\}$, we can equivalently describe them using the associated *observables* $O = 2\Pi - \mathbb{I}$. Note that O is a Hermitian operator which squares to identity. For Alice's measurements the observables are

$$A_0 = 2|0\rangle\langle 0| - \mathbb{I} = Z \ (x = 0) \quad \text{and} \quad A_1 = 2|+\rangle\langle +| - \mathbb{I} = X \ (x = 1).$$

For Bob we have

$$B_0 = H \ (y = 0) \quad \text{and} \quad B_1 = \tilde{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \ (y = 1).$$

We introduced this as a "good" strategy for the players: it certainly beats the classical bound $p_{\text{win}} = 3/4$, and achieves $p^*_{\text{win}} = \cos^2 \pi/8$. But could there be better strategies, achieving an even larger value? Or, even if they are not better, different strategies, based on using a different type of entangled state, for achieving the same success probability?

We're going to show that this is not the case: the maximum success probability of any quantum strategy in the CHSH game, as complicated as it may be, is p^*_{CHSH}. Moreover, any strategy achieving this value must be "equivalent" to the strategy described above. What do we mean by equivalent? We couldn't possibly hope to claim that the strategy is strictly unique. For example, if Alice and Bob were to rotate their basis choices by the same angle, then since the EPR pair is itself rotation invariant their success probability would remain unchanged. The next theorem shows that this local degree of freedom is essentially the only flexibility that the players have in designing an optimal strategy.

Theorem 8.3.1 (CHSH rigidity) *Suppose given an entangled state $|\psi\rangle_{AB} \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and observables A_0, A_1 for Alice and B_0, B_1 for Bob such that the corresponding strategy has a success probability $p^*_{\text{CHSH}} = \cos^2 \pi/8$ in the CHSH game. Then there exist isometries $U_A : \mathbb{C}^{d_A} \to \mathbb{C}^2 \otimes \mathbb{C}^{d_{A'}}$ and $V_B : \mathbb{C}^{d_B} \to \mathbb{C}^2 \otimes \mathbb{C}^{d_{B'}}$ such that*

$$U_A \otimes V_B \, |\psi\rangle_{AB} = |\text{EPR}\rangle \otimes |\text{junk}\rangle_{A'B'}$$

and

$$\begin{aligned}
(U_A \otimes V_B)(A_0 \otimes \mathbb{I}_B) \, |\psi\rangle &= ((Z \otimes \mathbb{I}) \, |\text{EPR}\rangle) \otimes |\text{junk}\rangle \, , \\
(U_A \otimes V_B)(A_1 \otimes \mathbb{I}_B) \, |\psi\rangle &= ((X \otimes \mathbb{I}) \, |\text{EPR}\rangle) \otimes |\text{junk}\rangle \, , \\
(U_A \otimes V_B)(\mathbb{I}_A \otimes B_0) \, |\psi\rangle &= ((\mathbb{I} \otimes H) \, |\text{EPR}\rangle) \otimes |\text{junk}\rangle \, , \\
(U_A \otimes V_B)(\mathbb{I}_A \otimes B_1) \, |\psi\rangle &= ((\mathbb{I} \otimes \tilde{H}) \, |\text{EPR}\rangle) \otimes |\text{junk}\rangle \, .
\end{aligned}$$

In words, the theorem says that if a strategy achieves the optimal value in CHSH then up to some local rotations on Alice and Bob's spaces it looks exactly as the strategy described above. We called the rotations "isometries" because their range might not be the whole space; in particular it is not necessarily the case that d_A or d_B are even.[3] The state $|\text{junk}\rangle$ can be any state: it does not matter for analyzing the strategy, because as the last equations show the strategy only acts on the "EPR" part of the state. We had to include the $|\text{junk}\rangle$ state ibecause any strategy can always be made more complicated by extending the entangled state arbitrarily, and making the players' measurements act as identity on the extended space.

Note that the theorem assumes that the players' strategy can be described by observables, or equivalently binary projective measurements. More generally we may consider players that apply a non-projective POVM. However, as described in Box **??** a POVM can always be simulated with a projective measurement acting on a larger space, so the assumption is without loss of generality.

Remark 8.3.2 *In practice we cannot expect to verify that some players achieve the optimal success probability in the CHSH game: at best, by repeatedly playing the game we can verify that they succeed*

[3] An isometry is a linear map that preserves distances, but need not be invertible. A unitary is an isometry which is also invertible.

with probability at least $p^*_{\text{win}} - \delta$, where $\delta > 0$ is a quantity depending on the quality of the players' strategy and on the accuracy of the verification (i.e. the number of repetitions of the game). To handle this scenario we need "robust" analogues of Theorem 8.3.1, that have similar conclusions under the weaker assumption of near-optimal success. Such results are known, where the exact equalities in Theorem 8.3.1 are replaced by approximations in trace distance with an error scaling as $O(\sqrt{\delta})$.

Before we get to the proof of the theorem we make a small detour and explore the notion of angle between a pair of projection operators. This will be an important tool in the proof.

8.3.1 Principal angles and Jordan's lemma

Consider two lines through the origin in the complex plane $\mathbb{C}^2$. Each line is described by a unit vector $|u\rangle$, $|v\rangle$, and (ignoring any orientation) the angle between the two lines is the unique $\theta \in [0, \pi/2)$ such that $\cos^2\theta = |\langle u|\, v\rangle|^2$. Up to a change of basis we can always consider that $|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and (up to an irrelevant phase) $|v\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$. A more convoluted way to describe the angle between the two lines is through the associated rank-1 projections $P = |u\rangle\langle u|$ and $Q = |v\rangle\langle v|$: there will always exist a choice of basis for $\mathbb{C}^2$ in which

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad Q = \begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix},$$

for some $\theta \in [0, \pi/2)$.

How do we generalize the notion of angle to higher dimensional subspaces? The notion of principal angle gives an inductive definition. Suppose P and Q are two orthogonal projections in $\mathbb{C}^d$. (We identify the projections with the space on which they project.) The smallest principal angle between P and Q is defined as $\theta_1 \in [0, \pi/2)$ such that

$$\cos^2\theta_1 = \sup_{|u\rangle \in P, |v\rangle \in Q} |\langle u|\, v\rangle|^2,$$

where by $|u\rangle \in P$ we mean any unit vector in the range of P, i.e. such that $P|u\rangle = |u\rangle$. This is a natural definition: we are finding the lines lying in P and Q that form the smallest possible angle. If P and Q intersect, then they share a vector and $\theta_1 = 0$.

We define principal angles $\theta_2, \ldots, \theta_d$, where $d = \min(\operatorname{rank} P, \operatorname{rank} Q)$, inductively via

$$\cos^2\theta_i = \sup_{\substack{|u_i\rangle \in P,\, |u_i\rangle \perp \operatorname{Span}\{|u_1\rangle, \ldots, |u_{i-1}\rangle\} \\ |v_i\rangle \in Q,\, |v_i\rangle \perp \operatorname{Span}\{|v_1\rangle, \ldots, |v_{i-1}\rangle\}}} |\langle u_i|\, v_i\rangle|^2,$$

where $|u_1\rangle, \ldots, |u_{i-1}\rangle$ are unit vectors in P that achieve the optimum in the definition of $\theta_1, \ldots, \theta_{i-1}$ respectively, and similarly for the $|v_j\rangle$ and Q.

Jordan's lemma states that associated with the principal angles comes a very convenient simultaneous block decomposition of P and Q.

Lemma 8.3.3 (Jordan's lemma) *Let P and Q be two projection operators in $\mathbb{C}^d$. Then there exists a basis of $\mathbb{C}^d$ in which P and Q are simultaneously block diagonal, with blocks of size one or two such that either (for one-dimensional blocks)*

$$P, Q \in \{(0),\, (1)\},$$

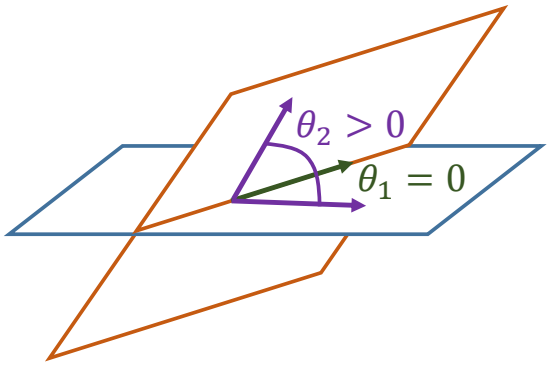

Fig. 8.1 Principal angles between two 2-dimensional subspaces in 3 dimensions. The subspaces intersect, and the smallest angle is $\theta_1 = 0$. The second principal angle is $\theta_2 > 0$.

or (for two-dimensional blocks)

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad Q = \begin{pmatrix} \cos\theta_i^2 & \cos\theta_i \sin\theta_i \\ \cos\theta_i \sin\theta_i & \sin\theta_i^2 \end{pmatrix},$$

with $\theta_1, \ldots, \theta_d \in (0, \pi/2]$, $d = \min(\operatorname{rank} P, \operatorname{rank} Q)$, *the principal angles between* P *and* Q.

The proof of the lemma is not very hard. It uses an alternative definition of the principal angles via the singular values of the operator PQ.

Quiz 8.3.1 *Suppose we have three projectors P_0, P_1, P_2 over a d-dimensional complex vector space. What does Jordan's lemma guarantee about a common diagonalization?*

a) $\longrightarrow$ ***For any*** i, j***, there is a basis in which*** P_i ***is diagonal and*** P_j ***is block diagonal with block size*** 2.
b) There is a basis in which P_0, P_1, P_2 are all block-diagonal with block size 2.
c) There is a basis in which P_0, P_1, P_2 are all diagonal.
d) If $\dim P_0 + \dim P_1 + \dim P_2 \leq d$, then there is a basis in which P_0, P_1, P_2 are all block-diagonal with block size 2.

8.3.2 Proof of the rigidity theorem

The proof of Theorem 8.3.1 has two steps. In the first step we use Jordan's lemma to reduce the case of general strategies to the case of "qubit strategies", for which the shared state is a two-qubit entangled states and the players' observables are single-qubit observables. In the second step we analyze qubit strategies in detail and show that they must take the form of Pauli measurements on an EPR pair.

A. Reduction to qubit strategies

Consider an arbitrary strategy $|\psi\rangle_{AB}$, A_0, A_1, B_0, B_1. Apply Jordan's lemma to the projections $P = \frac{1}{2}(\mathbb{I} + A_0)$ and $Q = \frac{1}{2}(\mathbb{I} + A_1)$. The lemma gives a basis for Alice's space $\mathbb{C}^{d_A}$ such that both P and Q are block-diagonal in that basis, with blocks of size at most 2×2. Then $A_0 = 2P - \mathbb{I}$ and $A_1 = 2Q - \mathbb{I}$ are block-diagonal in the same basis.

This block-diagonal decomposition lets us reformulate Alice's strategy as follows: each of her two-outcome projective measurements is equivalent to a measurement which (i) applies a multiple-outcome projective measurement that projects on the individual blocks of the decomposition, and (ii) depending on the block obtained as outcome performs the basis measurement associated with the restriction of A_0 (or A_1) to that block.

Exercise 8.3.1 Suppose that after application of Jordan's lemma we discover a basis

$$\{|u_1\rangle, |u_2\rangle, |u_3\rangle, |u_4\rangle, |u_5\rangle\} \tag{8.6}$$

of $\mathbb{C}^5$ in which

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Consider the two-outcome projective measurements associated with A_0 and A_1. Give an equivalent description of these measurements as the combination of a projective measurement $\{\Pi_0, \Pi_1, \Pi_2, \Pi_3\}$ followed by a basis measurement involving at most 2 basis elements. The projective measurement should be independent of Alice's input x, while the basis measurement should depend both on the outcome of the projective measurement and Alice's input.

The same argument can be applied to Bob's observables. The key point is that, since the block decomposition is the same for A_0 and A_1 (resp. B_0 and B_1), step (i) associated with projection on the blocks does not depend on the player's question. Thus the step could be performed even before the game even starts, without affecting their success probability! But then the players are really playing the game with a qubit strategy — whichever qubit strategy corresponds to the outcomes they obtained when applying the projective measurement from step (i).

This reformulation of an arbitrary strategy shows that it can always be reduced to a convex combination of qubit strategies, and it will be sufficient to analyze the latter.

B. Optimal qubit strategies

To prove the theorem we first express the success probability p^*_{win} of a given quantum strategy in terms of the observables A_x and B_y.

Exercise 8.3.2 Using the definition of the winning criterion $a \oplus b = x \wedge y$ and the relation between observables and binary measurements, show that

$$p^*_{\text{win}} = \frac{1}{2} + \frac{1}{8} \langle\psi| A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 |\psi\rangle . \tag{8.7}$$

Let's call the operator appearing inside the bra-ket in (8.7) the CHSH operator,

$$\text{CHSH} = \text{A}_0 \otimes \text{B}_0 + \text{A}_0 \otimes \text{B}_1 + \text{A}_1 \otimes \text{B}_0 - \text{A}_1 \otimes \text{B}_1 .$$

The main trick in the proof is to consider the square of this operator. Using $A_0^2 = A_1^2 = B_0^2 = B_1^2 = \mathbb{I}$,

we get

$$\begin{aligned}\mathrm{CHSH}^2 &= \big((A_0+A_1)\otimes B_0 + (A_0-A_1)\otimes B_1\big)^2 \\ &= (A_0+A_1)^2\otimes\mathbb{I} + (A_0-A_1)^2\otimes\mathbb{I} + (A_0+A_1)(A_0-A_1)\otimes B_0B_1 \\ &\quad + (A_0-A_1)(A_0+A_1)\otimes B_1B_0 \\ &= 4\mathbb{I} + [A_0,A_1]\otimes[B_1,B_0], \end{aligned} \tag{8.8}$$

where $[A_0,A_1] = A_0A_1 - A_1A_0$ and $[B_1,B_0] = B_1B_0 - B_0B_1$ are the commutators. Since the operator norm (the largest singular value) of $[A_0,A_1]$ and $[B_0,B_1]$ is each at most 2, the norm of CHSH^2 is at most 8. Plugging back into (8.7), even an optimal choice of $|\psi\rangle$ (i.e. an eigenvector of CHSH associated to its largest singular value) will give a value at most $p^*_{\mathrm{win}} \leq 1/2 + \sqrt{8}/8 = \cos^2\pi/8$. Thus $\cos^2\pi/8$ is indeed the maximum probability of success in the CHSH game.

Note that so far we have not used the reduction to qubit strategies discussed in the previous section, and the preceding argument is completely general. Let's now assume we are working with a qubit strategy which achieves the optimal p^*_{win}. Then all inequalities discussed above must be tight. In particular, $|\psi\rangle$ must be an eigenvector of CHSH with eigenvalue $2\sqrt{2}$, and as a consequence of (8.8) $|\psi\rangle$ must also be an eigenvector of $[A_0,A_1]\otimes[B_0,B_1]$ with associated eigenvalue 4. Squaring this operator,

$$\big([A_0,A_1]^2\otimes[B_0,B_1]^2\big)\,|\psi\rangle = 16\,|\psi\rangle\,.$$

Using further that $[A_0,A_1]^2 \leq 4\mathbb{I}$ and $[B_0,B_1]^2 \leq 4\mathbb{I}$ we get that necessarily

$$\big([A_0,A_1]^2\otimes\mathbb{I}\big)\,|\psi\rangle = \big(\mathbb{I}\otimes[B_0,B_1]^2\big)\,|\psi\rangle = 4\,|\psi\rangle\,, \tag{8.9}$$

as neither operator can reduce the norm of $|\psi\rangle$. Assume $|\psi\rangle$ is not trivial, in the sense that its reduced density matrices on A and B have rank 2 (if this is not the case then it is easy to see that the strategy boils down to a classical strategy, which cannot achieve a success probability larger than $p_{\mathrm{CHSH}} = 3/4$). Tracing out the A or B qubits in (8.9) and inverting the reduced density matrix of $|\psi\rangle$ on the remaining qubit gives us the operator equalities $A_0A_1 = -A_1A_0$ and $B_1B_0 = -B_0B_1$: Alice's and Bob's observables pairwise anti-commute. It turns out that anti-commutation is a surprisingly strong constraint, as shown in the following exercise.

Exercise 8.3.3 Suppose that R and S are two observables on $\mathbb{C}^2$ such that $RS = -SR$. Then there exists a basis of $\mathbb{C}^2$ in which $R = Z$ and $S = X$. *[Hint: first show that we cannot have $R = \mathbb{I}$ or $R = -\mathbb{I}$, and deduce the eigenvalues of R. Use this to write R in a convenient form, and then use the anti-commutation relation to find the form of S.]*

Applying the results of the exercise to A_0 and A_1 we obtain a unitary U_A on Alice's qubit such that $U_AA_0U_A^\dagger = Z$ and $U_AA_1U_A^\dagger = X$. Similarly, for Bob's observables we may find a unitary U_B such that $U_BB_0U_B^\dagger = H$ and $U_BB_1U_B^\dagger = \tilde{H}$. Note that for Bob we are using H and $\tilde{H}$ in lieu of X and Z, but any pair of single-qubit observables will do. To conclude it remains to show the following.

Exercise 8.3.4 Show that the operator

$$Z\otimes H + X\otimes H + X\otimes\tilde{H} - Z\otimes\tilde{H}$$

has largest eigenvalue $2\sqrt{2}$, with a unique associated eigenvector equal to $|\mathrm{EPR}\rangle$.

C. Putting everything together

We are almost done with the proof of Theorem 8.3.1. To summarize, we start with an arbitrary strategy $|\psi\rangle_{AB}$, A_0, A_1, B_0, B_1 with success probability $p^*_{\mathrm{win}} = \cos^2\pi/8$ in the CHSH game. Using part A

this strategy can be decomposed in a convex combination of qubit strategies. More formally, there are projective measurements $\Pi^A = \{\Pi_1^A, \ldots, \Pi_{k_A}^A\}$ and $\Pi^B = \{\Pi_1^B, \ldots, \Pi_{k_B}^N\}$ for Alice and Bob, made of projectors with rank at most 2 each, such that $A_x = \sum_j \Pi_j^A A_x \Pi_j^A$ and $B_y = \sum_j \Pi_j^B B_y \Pi_j^B$. The associated block decomposition can be specified by a unitary changes of basis U_A' and U_B' on Alice and Bob's systems respectively.

Using the first steps of part B, we know that any strategy can have success probability at most p^*_{win}, therefore all the qubit strategies, given by $(\Pi_j^A \otimes \Pi_\ell^B |\psi\rangle, \Pi_j^A A_x \Pi_j^A, \Pi_\ell^B B_y \Pi_\ell^B)$ for any $j \in \{1, \ldots, k_A\}$ and $\ell \in \{1, \ldots, k_B\}$, must have success probability p^*_{CHSH} (otherwise the overall strategy wouldn't achieve the optimal success probability).

By the remainder of part B, for all of these qubit strategies there exists a local change of basis U_j^A and U_ℓ^B in which it is equivalent to the canonical optimal strategy. By combining the unitaries U_A (resp. U_B), which specify the blocks, with the unitaries U_j^A (resp. U_ℓ^B), which identify a basis for each block in which $\Pi_j^A A_0 \Pi_j^A = Z$, $\Pi_j^A A_1 \Pi_j^A = X$, and similarly for Bob and $H, \tilde{H}$, we obtain the isometries claimed in the theorem: the proof is complete!

8.4 Chapter notes

The idea for the DIQKD protocol, which is that entanglement between Alice and Bob can be tested using the phenomenon of non-locality, is due to Ekert [**?**].

Example 8.1.1 is taken from [**?**].

Regarding Lemma 8.2.1: there are many ways it can be shown, yielding bounds of varying quality. The simplest analysis would consider a relaxation of the problem where the three players are allowed any kind of *non-signaling strategy*: in this case a bound can be obtained via linear programming. The bound can then be strengthened by considering the fact that the players must be quantum, using a semidefinite relaxation of the problem. But the optimal bound can be obtained by a direct analytic calculation, using the fact that Alice only has two possible inputs to reduce to the two-dimensional case via an application of Jordan's lemma. This is done in [**?**], from which the bound given here, which is due to [**?**], can be derived.

For a proof of Jordan's lemma, see e.g. Exercise VII.1.10 of [**?**]. An error-tolerant version of Theorem 8.3.1 on rigidity of the CHSH game is shown in [**?**], with an earlier argument appearing in [**?**]. The use of these results for DIQKD is explored in [**?**]. In terms of parameters such as tolerance to errors and key rate this technique yields weaker results than the approaches using uncertainty relations and guessing games; however, it also proves a stronger characterization of the devices that can be useful in other scenario (see for example the problem of delegating computations in Chapter **??**). For a quantitatively stronger approach, based on the "entropy accumulation theorem (EAT)," see [**?**].