Quantum Computing: Foundations to Frontier Fall 2018

Lecture 2

Lecturer: Henry Yuen *Scribes: Motasem Suleiman, Chenyang Li Noah Fleming, Ian Mertz*

1 Overview

In this lecture we will first go over measuring in different bases, the Heisenberg Uncertainty Principle, and then explore quantum entanglement. We will talk about non-classical correlations that arise in the CHSH game, its relation to Bell's theorem and the EPR paradox, and conclude with applications of the CHSH game to the problem of certifying randomness generation.

2 Main Section

2.1 Measuring in Different Bases

Measurements are typically performed in the standard basis which is also known as the computational basis, $\{|0\rangle, |1\rangle\}$. In the single qubit case, we recall that a qubit is a complex vector $\alpha|0\rangle+\beta|1\rangle$. One can think of the measurement on this qubit is by projecting the vector on $|0\rangle$ or $|1\rangle$.

Let V be an orthonormal basis of $\mathbb{C}^d$ where $V = \{|u_1\rangle, |u_2\rangle, |u_3\rangle, \ldots, |u_d\rangle\}$. Let $|\psi\rangle \in \mathbb{C}^d$ be a d-dimensional quantun state. We can measure $|\psi\rangle$ in the basis V. If we associate basis vector $|u_i\rangle$ with outcome $i \in \{1, \ldots, d\}$, then we obtain outcome i with probability $|\langle\psi|u_i\rangle|^2$, and the post-measurement state is $|u_i\rangle$. In other words, we project the state $|\psi\rangle$ onto the basis vector $|u_i\rangle$.

Physically, what does "measuring in a non-standard basis" mean? There exists a unitary U that depends on the basis V such this non-standard basis measurement is equivalent to first applying U to the state $|\psi\rangle$, measuring in the standard basis, and then applying the inverse unitary $U^\dagger$ to the post-measurement state.

In other words, the probability of obtaining outcome $|u_i\rangle$ if we measured $|\psi\rangle$ in the V basis is the same as obtaining outcome $|i\rangle$ if we measured $|\psi'\rangle = U|\psi\rangle$ in the standard basis.

Partial measurement rule. What if we take a two-qubit state $|\psi\rangle = \sum \alpha_{ij}|i\rangle|j\rangle$ and measure the first qubit in a non-standard basis $V = \{|v_0\rangle, |v_1\rangle\}$?

Fix a $k \in \{0, 1\}$. We will calculate the probability of obtaining outcome $|v_k\rangle$. Consider the following vector:

$$|v\rangle = \sum_{ij} \alpha_{ij}\langle v_k|i\rangle\,|j\rangle.$$

Note that this is, in general, not a normalized state. Also note that $|v\rangle$ is a vector in $\mathbb{C}^2$ (not

$\mathbb{C}^2 \otimes \mathbb{C}^2$!). The probability of obtaining outcome $|v_k\rangle$ is the *norm squared* of $|v\rangle$:

$$\| |v\rangle \|^2 = \sum_j \left| \sum_i \alpha_{ij} \langle v_k | i \rangle \right|^2 .$$

The post-measurement state of both qubits is

$$|v_k\rangle \otimes \frac{1}{\| |v\rangle \|} |v\rangle.$$

You should check that this is a normalized state.

Example. Let $V = \{|+\rangle, |-\rangle\}$ where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Let $|\psi\rangle = \sqrt{\frac{2}{3}}|01\rangle + \sqrt{\frac{1}{3}}|10\rangle$. The probability of obtaining the $|-\rangle$ outcome when measuring the first qubit of $|\psi\rangle$ in the basis V is the following. We first calculate

$$\begin{aligned} |v\rangle &= \sqrt{\frac{2}{3}} \langle -|0\rangle \, |1\rangle + \sqrt{\frac{1}{3}} \langle -|1\rangle \, |0\rangle \\ &= \sqrt{\frac{2}{3}} \sqrt{\frac{1}{2}} \, |1\rangle + \sqrt{\frac{1}{3}} \left(-\sqrt{\frac{1}{2}} \right) |0\rangle \\ &= \sqrt{\frac{1}{3}} \, |1\rangle - \sqrt{\frac{1}{6}} \, |0\rangle. \end{aligned}$$

The norm of $|v\rangle$ is $1/3 + 1/6 = 1/2$. Thus the probability of obtaining outcome $|-\rangle$ is $1/2$. The post-measurement state is then

$$|-\rangle \otimes \left(\sqrt{\frac{2}{3}}|1\rangle - \sqrt{\frac{1}{3}}|0\rangle \right).$$

2.2 Heisenberg Uncertainty Principle

The principle arises in physics and chemistry in which it states that one cannot tell the position and the momentum of a particle at the same time. In quantum information theory terms, this boils down to the following statement: it is not possible for a qubit $|\psi\rangle$ to be determined using both the standard basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis. In other words, if we measure $|\psi\rangle$ in the standard basis and get a deterministic outcome, then we cannot get a deterministic outcome when measuring $|\psi\rangle$ in the $\{|+\rangle, |-\rangle\}$ basis, and vice-versa. We say that these two bases are *incompatible*.

In physics, measuring the position or momentum of a particle is measuring in two incompatible bases.

2.3 Entanglement

In general, a two-qubit state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ cannot be represnted as $|\psi\rangle = |\phi\rangle \otimes |\theta\rangle$ for some $|\phi\rangle, |\theta\rangle \in \mathbb{C}^2$. Such states are called product or unentangled states. The equality holds when the two qubits act independently. i.e. measuring one does not affect the other one. However, general quantum states are entangled, which means that the two qubits show correlation between one another. This means that measuring one qubit influences the outcome measurement of the other one.

An example of two entangled two-qubit system is: $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ This is called the EPR pair (Bell state or maximally entangled state).

Let's explore some properties of the EPR pair. Suppose Alice gets one qubit and Bob gets the other qubit. When measuring in the standard basis, both Alice and Bob obtain the same outcome. Hence, they are correlated. This correlation is not special to the quantum world, it can also be done classically. Interestingly, with the EPR pair, the correlation might get more complicated, as we will see.

3 CHSH game

We will see that there can be interesting correlations between Alice and Bob's measurement outcomes that would not be possible in a classical world. These correlations can be illustrated by means of Clauser-Horne-Shimony-Holt (CHSH) game [CHSH69].

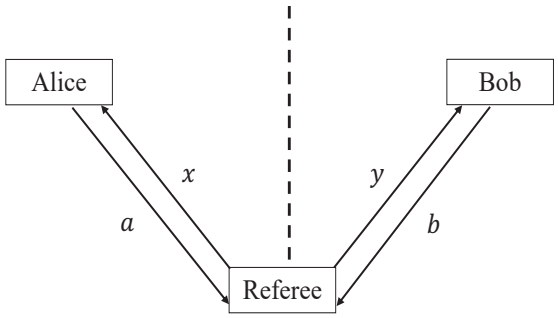

Figure 1: The CHSH game.

As depicted in Fig. 1 in the CHSH game, there are two players (Alice and Bob) who are viewed as cooperating with one another but cannot communicate directly with one another . A referee runs the game, and all communication in the game is between the players and the referee. The referee randomly selects and sends a question x to Alice and a question y to Bob. Each player sends an answer, say answer a for Alice wand b for Bob, back to the referee. All questions and answers, x, y, a, b, are single bits. Based on all of the questions and answers, the referee determines whether the players win or lose.

The winning condition is $a + b = xy \mod 2$. In other words, if $xy = 0$, then Alice and Bob have to output matching answers. If $xy = 1$, Alice and Bob have to output opposite answers.

What is the maximum winning probability for Alice and Bob in this game?

3.1 Classical strategy

Suppose Alice and Bob only use classical strategies, i.e., each player generate their answers as a deterministic function of their questions. It is easy to find a strategy with a wining probability of 3/4 and, i.e., they both answer 0 all the time. In fact, the maximum wining probability with a classical strategy is 3/4. One way of checking this is by trying all possible classical strategies (there aren't that many).

Furthermore, allowing randomized strategies can not help them to get a better success probability. This is because any classical randomized strategy for the CHSH game (where say Alice's answer is a function of the question x, as well as some random string r that might be possibly shared with Bob, and similarly for Bob's answer) can be converted into a deterministic strategy that has the same winning probability.

3.2 Quantum strategy

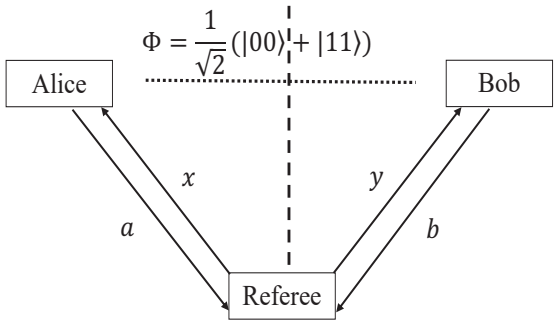

Figure 2: CHSH game with maximally entanglement states.

What if Alice and Bob use quantum strategy? They can get a better result if they can use entanglement. Suppose that before the game starts, as depicted in Fig.2, Alice and Bob get together in a lab and create an entangled two-qubit state:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1}$$

Alice takes one qubit and Bob takes the other one. When the game starts, Alice gets $x \in \{0, 1\}$ and Bob gets $y \in \{0, 1\}$. As depicted in Table 1, depending on their questions, they perform different measurements on their respective qubits.

(a)If Alice receives the question 0, she will measure her qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. Alice outputs 0 if the measurement result is $|0\rangle$, or 1 if the measurement result is $|1\rangle$.

(b)If Alice receives the question 1, she will measure her qubit with respect to the basis $\{|+\rangle, |-\rangle\}$, where$\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Alice outputs 0 if the measurement result is $|+\rangle$, or 1 if the measurement result is $|-\rangle$.

(c)If Bob receives the question 0, he will measure his qubit with respect to the basis $\{|a_0\rangle, |a_1\rangle\}$, where $\{|a_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, |a_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle\}$. Alice outputs 0 if the measurement result is $|a_0\rangle$, or 1 if the measurement result is $|a_1\rangle$.

(c)If Bob receives the question 1, he will measure his qubit with respect to the basis $\{|b_0\rangle, |b_1\rangle\}$,where $\{|b_0\rangle = \cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle, |b_1\rangle = \sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle\}$. Alice outputs 0 if the measurement result is $|b_0\rangle$, or 1 if the measurement result is $|b_1\rangle$.

Table 1: Alice's and Bob's quantum strategy

Alice			Bob		
Question x	Basis state	Output	Question y	Basis state	Output
x=0	$\|0\rangle$	0	y=0	$\|a_0\rangle$	0
	$\|1\rangle$	1		$\|a_1\rangle$	1
x=1	$\|+\rangle$	0	y=1	$\|b_0\rangle$	0
	$\|-\rangle$	1		$\|b_1\rangle$	1

Now, let us consider the winning probability. The total winning probability, $P(win)$, can be written as:

$$\begin{aligned}
&\Pr(win) \\
&= \Pr(a=0,b=0|x=0,y=0)\Pr(x=0,y=0) + \Pr(a=1,b=1|x=0,y=0)\Pr(x=0,y=0) \\
&+ \Pr(a=0,b=0|x=1,y=0)\Pr(x=1,y=0) + \Pr(a=1,b=1|x=1,y=0)\Pr(x=1,y=0) \\
&+ \Pr(a=0,b=0|x=0,y=1)\Pr(x=0,y=1) + \Pr(a=1,b=1|x=0,y=1)\Pr(x=0,y=1) \\
&+ \Pr(a=0,b=1|x=1,y=1)\Pr(x=1,y=1) + \Pr(a=1,b=0|x=1,y=1)\Pr(x=1,y=1).
\end{aligned} \tag{2}$$

Let's calculate probability that Alice and Bob win when their question pair is $(x, y) = (0, 0)$:

$$\begin{aligned}
\Pr(a=0,b=0|x=0,y=0) &= |(\langle 0| \otimes \langle a_0|)\,|\Phi\rangle|^2 \\
&= \left|(\langle 0| \otimes \langle a_0|)\,\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right|^2 \\
&= \left|\frac{1}{\sqrt{2}}\langle a_0|0\rangle\right|^2 \\
&= \frac{1}{2}\cos^2(\pi/8),
\end{aligned} \tag{3}$$

$$\begin{aligned}
\Pr(a=1,b=1|x=0,y=0) &= |(\langle 1| \otimes \langle a_1|)\,|\Phi\rangle|^2 \\
&= \left|(\langle 1| \otimes \langle a_1|)\,\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right|^2 \\
&= \left|\frac{1}{\sqrt{2}}\langle a_1|1\rangle\right|^2 \\
&= \frac{1}{2}\cos^2(\pi/8),
\end{aligned} \tag{4}$$

Thus, $\Pr(win|x=0,y=0) = \Pr(a=0,b=0|x=0,y=0) + \Pr(a=1,b=1|x=0,y=0) = \cos^2(\pi/8) \approx .854$. Similarity, we can compute the other conditional probabilities, $\Pr(a,b|x,y)$. In fact, it will turn out that $\Pr(win|x,y) = \cos^2(\pi/8)$ irrespective of the question pair (x,y). This

implies that $\Pr(win) = \cos^2(\pi/8) \approx .854$ which is strictly greater than 3/4, the maximum classical success probability.

It is not possible to do better than $\cos^2(\pi/8)$ with a quantum strategy for the CHSH game (although proving this is outside the scope of this lecture).

Thus, quantum entanglement gives rise to correlations that cannot be reproduced by classical randomness, and furthermore these correlations can help in playing this CHSH game.

4 Historical Perspective

The CHSH game is not just a cute demonstration of the advantage that using quantum entanglement can give in some esoteric game. In fact, the CHSH game arose naturally from one of the most important debates in Quantum Mechanics. In 1935, out of their great discomfort with the model of the real world that the theory of Quantum Mechanics presented, Einstein, Podolsky and Rosen (EPR), published a (now famous) paper titled "Can Quantum-Mechanical Description of Physical Reality be considered Complete?" [EPR35]. Their paper argued that although Quantum Mechanics may be remarkably good at predicting the outcome of experiments, it cannot be a complete description of nature.

Einstein, Podolsky and Rosen's grief with Quantum Mechanics can be summed up by the following experiment. Define the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

and imagine the following two thought experiments: Alice and Bob share $|\psi\rangle$ and are unable to communicate with each other. We will say that the first qubit belongs to Alice and the second belongs to Bob.

Experiment A: Alice measures her qubit in the standard basis $\{|0\rangle, |1\rangle\}$.

Experiment B: Alice measures her qubit in the Fourier basis $\{|+\rangle, |-\rangle\}$.

In Experiment A, Alices outcomes are as follows:

outcome: $|0\rangle$ with probability 1/2, with post measurement state $|00\rangle$,

outcome: $|1\rangle$ with probability 1/2, with post measurement state $|11\rangle$.

For, experiment B, the probability that

outcome: $|+\rangle$ with probability 1/2, with post measurement state $|++\rangle$,

outcome: $|-\rangle$ with probability 1/2, with post measurement state $|--\rangle$.

To see that this is correct for experiment B, observe that the probability of Alice measuring $|+\rangle$ is

$$\left\|(|+\rangle\langle+|\otimes I)\left(\frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle\right)\right\|^2 = \frac{1}{2}\left\|\langle+|0\rangle|0\rangle + \langle+|1\rangle|1\rangle\right\|^2 = \frac{1}{2}\left\|\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right\|^2 = 1/2.$$

The post-measurement state is then $|+\rangle \otimes (1/\sqrt{2}(|0\rangle + |1\rangle) = |+\rangle \otimes |+\rangle$. Similarly for the case when Alice measures $|-\rangle$.

Therefore, if Alice measures $|i\rangle$ for $i \in \{0, 1\}$, then she knows Bob's qubit must have collapsed to $|i\rangle$. Similarly, if Alice measures $|j\rangle$ for $j \in \{+, -\}$, then she knows Bob's must have collapsed to $|j\rangle$. Therefore, Bob's qubit is both in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis simultaneously. The punchline is that no matter what basis Alice chooses to measure in, and no matter what outcome she gets, Bob's state always collapses to that outcome simultaneously.

This is difficult to reconcile with Heisenberg uncertainty principle. Bob's qubit could be billions of light years away and yet Quantum Mechanics states that the state of the two particles collapsed in a way that make it appear that Bob's qubit knew what basis Alice chose to measure in, in the sense that after Alice performs one of the two experiments, she *knows* the state of Bob's qubit. But because of the locality of physics, Alice's choice of measurement couldn't have affected the intrinsic state of Bob's qubit (or so EPR's reasoning went).

Because of this, Einstein, Podolsky and Rosen concluded that Bob's qubit has its answers for both the $\{|0\rangle, |1\rangle\}$ basis and the $\{|+\rangle, |-\rangle\}$ basis prepared ahead of time. This violates Heisenberg's uncertainty principle which states that the outcome of these two incompatible measurements cannot be determined. Therefore, something must be wrong. The conclusion of Einstein, Podolsky and Rosen was that Quantum Mechanics wasn't really describing reality. They posited that instead there was a deeper *classical* theory – consistent with the statistical predictions of Quantum Mechanics – but explains the paradox above by saying that in fact there are hidden variables that describe the intrinsic state of each particle. These variables describe different outcomes for each outcomes for each possible measurement you could make on them. But these variables would respect locality (i.e. signals cannot travel faster than the speed of light).

That is, they posited that there was an underlying classical theory called a *local hidden variable theory* that

1. Respects relativity/locality/causality, and
2. Reproduces the statistics of Quantum Mechanics.

To Einstein, this would be much more satisfactory, this would be the best of both worlds.

In 1964, a physicist named John Bell made an amazing contribution to quantum physics, that is at once incredibly simple but also profound. His contribution came in the form of (something similar to) the CHSH game. We make a modern reformulation of Bell's theorem here:

Theorem 1. *(Bell's Theorem [Bel64]) Any classical strategy for the CHSH game can win at most 3/4ths of the time, while there exists a quantum strategy for the CHSH game that wins at least a* $\cos^2(\pi/8) \geq .853$ *fraction of the time.*

If the universe truly followed Einstein's model of local hidden variables, then any strategy in particular would also be described using local hidden variables. But such a strategy is classical and so it cannot win more than 75% of the time. However, Quantum Mechanics predicts something different, and indeed this has been verified experimentally (See for example [CS78]). This says that no classical theory – such as a local hidden variable model – can ever reproduce all of the predictions of Quantum Mechanics and also be consistent with special relativity. The world is fundamentally non-classical.

5 Certifying randomness

We will now look at another, more practically motivated application of the CHSH game: generating random bits. When working with computers one never runs out of uses for truly random bits, both in computer science (cryptography, privacy randomized algorithms) and in general computer applications (gambling websites, your iTunes visualizer...). We don't yet have a full understanding of the power of randomness, but at the moment it's one of the workhorses keeping the internet afloat.

Pseudorandomness. Sometimes it's enough to get away with *pseudorandomness*, or bits that "look random enough" despite being generated deterministically. Of course it's enough to have your iTunes visualizer do something that looks sort of random to the naked eye, but pseudorandomness is a powerful tool in theoretical computer science with connections to both obtaining efficient algorithms and proving such algorithms don't exist.

However it would be a pretty big leap of faith to trust a deterministic procedure with protecting your credit card info, or shuffling the deck on your poker website. While it's true that these pseudorandom generators are given a *seed*—a small amount of randomness to get started—even these sources are hard enough to come by, and the hacks that most systems use are appallingly bad. Some of the most common seed sources come from the number of milliseconds since midnight, CPU temperature, inputs from your computer such as mouse movements or keyboard presses, and other physical mechanisms that are not particularly hard to predict[1]. Even the built in randomness function for most programming languages uses an algorithm called the Mersenne Twister, which can be infinitely determined with 624 consecutive samples [Wikb].

Certifying randomness. This suggests a question of testing whether or not a given string is random. Say you buy a random number generator on Amazon, a little black box that, for the low price of no less than $500 or so, promises that the string is actual true randomness, not based on some shady seeding method. Of course many companies have promised this in the past, and as we've already seen there's usually a smart computer scientist who breaks it by noticing the right pattern. But this could be the cleverest box we've seen yet, or more likely is using a novel way to generate terrible randomness.

As cryptographers, it is our job to certify that this box is actually putting out randomness beyond a shadow of a doubt. Because cryptography deals with transmitting messages in the presence of an adversary, cryptographers tend to be as paranoid as they come, and would never assume that their Amazon box has our best interest, ie outputting truly random bits, at heart. In fact given the NSA's history with exactly this issue [Wika], it's always better to assume the opposite. With that said, no one will get anywhere by just throwing the box away; we need to get our random bits eventually. So instead we ask the natural question:

Question: *Does there exist a deterministic test to determine whether or not your box is generating true randomness and not a deterministic procedure?*

[1] It would take days to go through all the hits on Google that come up for lottery and gambling sites that have been publically broken by bored cryptographers and even some notorious hackers. More many were based on sources coming from the timestamp, and were broken by people who learned the right time window in which they had to press the button [All17].

The answer, of course, is no. The first way to reject this idea is to note that every string of length n is equally likely to occur, so if your box outputs a particular string, say $r \in \{0,1\}^n$, there's no firm reason to reject even if r is the all zeroes string. An equivalent counterargument is by an *adversarial argument*: if you had such a test T, Amazon could send you a box that has a few strings your test T accepts and it simply prints them out when you press the button, no randomness involved.

5.1 Quantum randomness

In contrast to the deterministic setting, where true randomness is nigh impossible to come by, a quantum system is practically overflowing with it. Even a simple quantum procedure is enough to generate true randomness. We illustrate this using one of quantum computing's most important unitary gates, called the *Hadamard gate*, which in a word maps $|0\rangle \leftrightarrow |+\rangle$ and $|1\rangle \leftrightarrow |-\rangle$. We detail the procedure for completeness:

$$|\psi\rangle = |0\rangle$$

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$U|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

If we measure $U|\psi\rangle$ and return the result this is a uniformly random bit, as the coefficient on both $|0\rangle$ and $|1\rangle$ is $\sqrt{\frac{1}{2}}$.

Certifying quantum randomness. So all hope is not lost. For a number of years the hardware random number generators you see on the internet have been promising to use quantum sources to extract their randomness, with similar tricks to what we just saw. Unfortunately one could (and should) imagine the same box showing up at our house, even with "quantum" stamped across the top. We've already seen that it's hopeless to try and certify randomness just by looking at the output string in isolation, but there is one hope: we at least know how to check that stamp, in the form of the CHSH game.

Imagine the following scenario: you decide to shell out \$1000 instead of \$500 to get a hold of *two* boxes, both of which claim to use quantum mechanics to generate randomness. You put them on your desk, and wrap them up so they're free of generating any heat, sound, or anything else they might pick up from each other. You then play the CHSH game with these two boxes, randomly generating x and y and then pressing the button to get a and b. After running this game for a few hours their win rate is at 80%. With what we've seen in the lecture up until now we know that with almost perfect assurance this means there are quantum effects at play in these boxes, and in particular that the bits you're receiving have information-theoretic *entropy* (randomness) coming from quantum effects. Better yet, we've made *practically no assumptions* about the setting; the strongest thing we've assumed is that they aren't communicating, which can be easily fixed by just moving them to adjacent rooms, or shipping one off to China [Bil17].

There are two reasonable objections to come out of this test. The first is what to conclude when the win rate is close to (or even below) 75%. The short answer is that we can't conclude anything. Two

quantum players playing the CHSH game can easily underperform the best strategy, if their goal was to convince you that they weren't sharing any entanglement (remember, we're cryptographers, and we're as paranoid as it gets). The second objection is that we needed randomness to generate x and y, meaning that by all measures we've lost a treasure trove of random bits for the sake of testing that these boxes have *any* quantum randomness in them at all, possibly far less than the amount we put in.

5.2 Randomness expansion.

This problem was formalized in Roger Colbeck's Ph.D thesis [Col06], wherein he developed a procedure to not only certify quantum randomness when it's present, but to certify that the outputs of these two boxes[2] contains *more* randomness than the amount used to play the game.

Theorem 2 ([Col06], Section 5.2.3)**.** *For every constant $c > 1$ there exists a game which requires n bits of randomness where the boxes win the game iff there exist cn bits of randomness in their outputs.*

Even more, [Col06] also shows that it's possible to extract cn bits, not just certify them. This is an important distinction in theoretical computer science, where having a bitstring with entropy ω in no way guarantees a way to get ω purely random bits. This led to a line of work in quantum cryptography which we summarize now:

- Colbeck (2006)[Col06]: $n \to cn, c > 1$ (linear expansion)
- Pironio *et al* (2010) [PAM+10]: $n \to n^2$ (quadratic expansion)
- Vazirani, Vidick (2012) [VV12]: $n \to \exp(\Omega(n^{1/3}))$ (exponential expansion)

The central technique behind these expansion arguments is to play a protocol like the following. Let R denote the total number of rounds of CHSH being played.

1. The verifier (i.e. you) randomly chooses a small subset $S \subseteq \{1, \ldots, R\}$ of size $|S| = n$.
2. Play R rounds of the CHSH game in sequence with the two devices. In round j, if $j \in S$, then choose the questions x, y uniformly at random. If $j \notin S$, then set $x = 0, y = 0$.
3. Count how many of the CHSH games in the rounds S the boxes won. If the number is at least, say, $0.8n$, then accept. Otherwise, reject.

The randomness expansion results above show that, for different tradeoffs between n and R, if the verifier accepts, then with high probability the answers of the devices (which forms an R-length string), will contain roughly $\Omega(R)$ bits of entropy (which is much more than the amount of randomness used by the verifier to select set S and also the randomness for the S-round questions).

The intuition for why this works is the following: while the rounds outside of the set S seem useless, recall that neither of the devices can communicate, and thus the first box receiving a 0 doesn't

[2]Colbeck's setup contained three boxes instead of two, and used a different game. A follow up work of Barrett, Colbeck, and Kent [BCK12] uses only two devices, as do all other follow-up works we discuss in this section.

guarantee that the other box did as well. Even if both boxes knew that there were only going to be an ϵ fraction of the games where either of them would see a 1, [Col06] argued that they can't do much with the information without knowing where those games would appear. Ultimately the randomness in both the actual CHSH rounds and in deciding when they would appear is much less than the amount of randomness the boxes have to generate in order to not fall below the 75% threshold. All follow-up works used the same basic strategy but primarily varied the number of rounds where the actual game would be played.

Infinite randomness expansion. While exponential expansion seems like a natural stopping point, one might ask if it's the last stop on our way to *infinite* randomness expansion. All other strategies for expansion used this sparsified game method, but in order to go to infinite expansion we clearly need a much different approach.

The only strategy that immediately comes to mind when discussing infinite expansion, and one that may have occurred to most readers as soon as we talked about expanding n bits to more than n bits, is to just feed this new pure randomness back into the same game. This does not immediately succeed, as the two boxes are allowed to keep their transcripts between rounds and thus know exactly what randomness the tester has pressed out of them. Thus they could easily switch to a deterministic strategy as soon as they see their own bits coming back.

After showing linear expansion, [Col06] made the (near trivial) observation that infinite randomness can be achieved by rigging up these pairs of boxes in parallel and using the same initial random string for all of them. This runs into the obvious problem of costing far more than $1000, but it suggests a similar strategy, namely using randomness from one instance of the game for a new instance, and then eventually looping back to the first set of boxes once the new randomness is independent enough from the bits that it generated. In fact, it turns out that $4000, or rather eight boxes, suffices.

Theorem 3 ([CY14], Theorem 2.1)**.** *For every k there exists a k-round protocol involving eight non-signalling quantum devices that, starting with n bit seed, can certify that an output string s is drawn from a distribution that is $\exp(-\Omega(n^{1/3}))$-close to uniform. Furthermore, the string s has length $g^{(k)}(n)$, where $g^{(k)}$ is the k-fold composition of the function $g(m) = \exp(\Omega(m^{1/3}))$,*

The current frontier is infinite randomness expansion using four boxes [MS16], a total of two instances of the CHSH game. It is still open whether it can be done using three or even two boxes, for some variant of CHSH. Note that while there may be room for improvement in the parameters of the argument, such as the probability of failure as a function of the seed length, the seed length itself must be greater than zero; information theory promises that even in the quantum setting we can't ever hope to get something from nothing.

Open problem. *Find the minimum number of non-signaling quantum devices needed in an infinite randomness expansion scheme.*

References

[All17] Willy Allison. Security & surveillance: Running the rng risk. *GGB Magazine*, 2017. Accessed: 2018-09-20.

[BCK12] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *CoRR*, abs/1209.0435, 2012.

[Bel64] John Stewart Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.

[Bil17] Lee Billings. China shatters "spooky action at a distance" record, preps for quantum internet. *Scientific American*, 2017. Accessed: 2018-09-20.

[CHSH69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[Col06] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *Ph.D thesis, University of Cambridge*, 2006.

[CS78] John F Clauser and Abner Shimony. Bell's theorem. experimental tests and implications. *Reports on Progress in Physics*, 41(12):1881, 1978.

[CY14] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 427–436, 2014.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[MS16] Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM (JACM)*, 63(4):33, 2016.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, Antoine Boyer de la Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Matthew Olmschenk, David Hayes, Le Luo, T. Andrew Manning, and Christopher R. Monroe. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[VV12] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: Or, true random number generation secure against quantum adversaries. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 61–76, 2012.

[Wika] Wikipedia. Dual_ec_drbg. Accessed: 2018-09-20.

[Wikb] Wikipedia. Mersenne twister. Accessed: 2018-09-20.