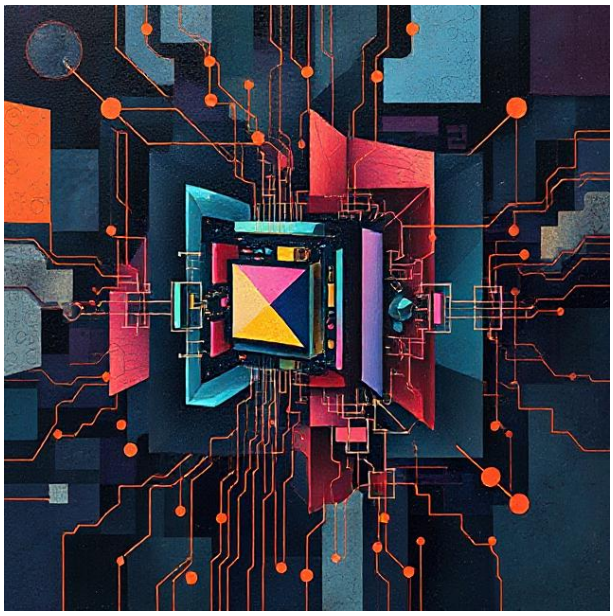
Quantum Hackathon Booklet

University of Colorado Boulder

Matthew Fox



Last Updated: October 6, 2025

Contents

Foreword

This is a set of four lectures and four readings on quantum information and quantum computation that was originally prepared for the 2025 - 2026 Quantum Hackathon at the University of Colorado Boulder (CU Boulder). They are intended for advanced undergraduate students who are enrolled in CU Boulder's Quantum Scholars program.

These notes cover several important topics in quantum information and quantum computing theory, including: the postulates of quantum mechanics, the Einstein–Podolsky–Rosen (EPR) paradox, Bell's theorem, the CHSH non-local game, the quantum circuit model of quantum computation, and Grover's algorithm.

It is assumed that readers are proficient in linear algebra. Ideal readers are also familiar with (but not necessarily proficient in) computability theory, quantum mechanics, probability theory, and a programming language such as Python. That said, the essential ideas from these topics are comprehensibly covered, so anyone lacking this "ideal" background can in principle follow along.

The four lecture notes are more or less verbatim what will be said in class, while the four readings are to be done "at home". That said, you are encouraged to discuss the readings with others in the course. Embedded in the readings are several problems, and readers should try their hand at these problems before moving past them, as the material only builds.

Please keep in mind that these notes were written on a tight schedule. In consequence, the notes are in no way a comprehensive treatment of the discussed topics, nor are they guaranteed to be error-free. Corrections by email to matthew.fox@colorado.edu are welcome.

List of Abbreviations and Symbols

iff	if and only if
$\in$	set containment ("in")
$\forall$	universal quantifier ("for all")
$\exists$	existential quantifier ("there exists")
$\mathbb{N}$	set of positive integers ($0 \notin \mathbb{N}$)
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{C}^N$	N-dimensional complex vector space
$\{0,1\}^n$	set of n-bit strings
$\{0,1\}^*$	set of finite length bit strings
$\mathrm{U}(N)$	set of $N \times N$ unitary matrices
$O(\cdot)$	big O notation
$\Pr[\cdot]$	probability
$\mathbb{E}[\cdot]$	expectation value
$\lfloor \cdot \rceil$	nearest integer function
$*$	complex conjugate
T	matrix transpose
$\dagger$	conjugate transpose (Hermitian conjugate)
$\lvert z \rvert$	length of z if $z \in \{0,1\}^*$, modulus of z if $z \in \mathbb{C}$
$\wedge$	logical AND
$\oplus$	logical exclusive OR (addition modulo 2)
$\otimes$	tensor product
$\lvert \psi \rangle$	ket vector
$\langle \psi \rvert$	bra vector
$\langle \psi \vert \phi \rangle$	bra-ket ("bracket") inner product
$\lvert \psi \rangle \langle \phi \rvert$	bra-ket ("bracket") outer product

Part I
A Most Incomprehensible Thing

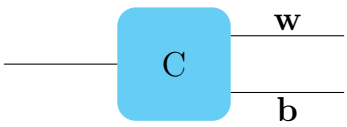
Lecture 1
A Most Incomprehensible Thing

In this first lecture, we will review the Stern–Gerlach experiment and a simplified version of Bell's theorem. Part of this presentation is based on David Albert's outstanding book *Quantum Mechanics and Experience*. The overarching point of this lecture is that quantum mechanics is inimitably bizarre. Perhaps, as we will explore at length in Parts III and IV of these notes, such bizarreness will manifest into a sort of "quantum computational advantage".

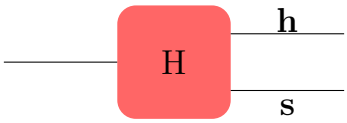
1.1. An Experimental Fact of Life: The Stern–Gerlach Experiment

Every quantum particle (an electron or silver atom, say) appears to have an intrinsic property that we call *color* and an intrinsic property that we call *hardness*. Whenever we look to see what the color of a particle is, we only ever see it to be either white (**w**) or black (**b**). Likewise, whenever we look to see what the hardness of a particle is, we only ever see it to be either hard (**h**) or soft (**s**). For decades, no other color or hardness has ever been seen, so we are confident that these are the only possible color and hardness values.

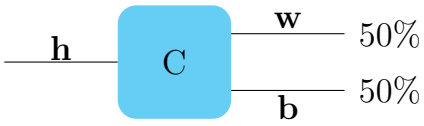
It is possible to build a *color box*, C, which resolves the color of a particle. It acts by taking in a particle on the left, whose color can be known or unknown, and then, after a short time, ejecting the same particle on the right on either the top track, if the color of the particle is white, or on the bottom track, if the color of the particle is black. Diagrammatically,



Similarly, we can build a *hardness box*, H, which resolves the hardness of a particle, akin to how a color box resolves the color of a particle. It looks like this:



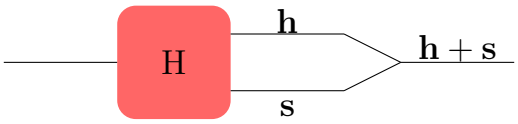
We may wonder if color and hardness are correlated. But, after many trials of feeding only hard particles into a color box, we conclude they are not because, in aggregate, 50% of the hard particles came out black and 50% came out white:



Exercise 1.1. How can we do this experiment without a source of hard particles?

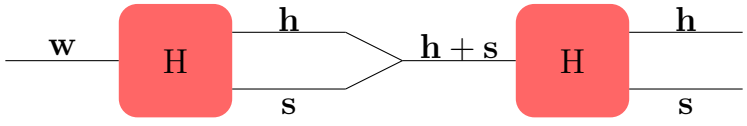
Interestingly, the same 50/50 statistics result if we instead feed soft particles into a color box, white particles into a hardness box, or, finally, black particles into a hardness box. These results only reaffirm our previous conclusion that hardness and color are not correlated.

Now consider the following apparatus, in which via a simple placement of mirrors, say, we merge the output paths into a single path:



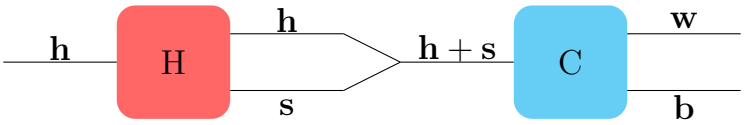
Specifically all we have done here directed the hard and soft beams into one, which experiments decidedly show do not affect the hardness or color of a particle.

Given this new apparatus, suppose we now we feed many white particles into it and then measure the hardness of the combined $\mathbf{h} + \mathbf{s}$ beam, as in:



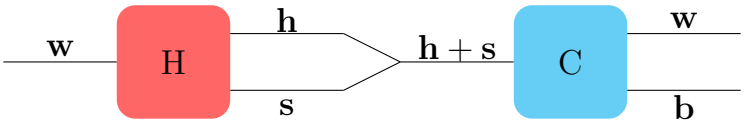
Exercise 1.2. Given what has been said so far, at the output of the first hardness box (left), what percentage of white particles do you expect to come out soft and what percentage do you expect to come out hard?

Now consider the simple variation below, where instead of inputting a white particle we input a hard particle, and instead of measuring its hardness after merging the beams, we measure its color:



Exercise 1.3. What statistics do you expect?

Now consider one final variation to this experiment. Suppose into this apparatus we input a *white* particle, as opposed to a hard particle, and then, after merging the two beams, we measure its color like in the previous experiment:



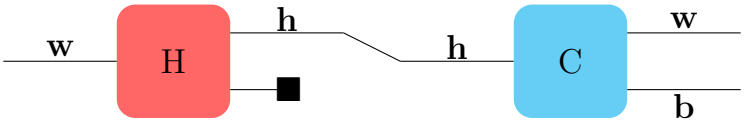
Given the reasoning we've used so far, there are two ways you might go here. On one hand, we input white particles, so it is natural to expect only white particles to emerge. On the other hand, at the output of the hardness box, we expect 50% of the white particles to be soft and 50% to be hard. Combining the beams does not change hardness or color, so these statistics should hold in the combined $\mathbf{h} + \mathbf{s}$ beam. We therefore expect 50% of the input to the color box to soft and 50% to be hard. Therefore, one could also expect 50% of the output to be white and 50% to be black.

Exercise 1.4. What statistics do you expect?

In fact, 100% of the output is white. No black particles ever emerge from this apparatus.

Let's look more closely at this experiment. Since the output of a color box is white if and only if the input is white, it must be that the $\mathbf{h} + \mathbf{s}$ beam is composed of only white particles. But the $\mathbf{h} + \mathbf{s}$ beam comes from combining the individual $\mathbf{h}$ and $\mathbf{s}$ beams, so the individual $\mathbf{h}$ and $\mathbf{s}$ beams must themselves be exclusively composed of white particles.

Let's test this hypothesis by blocking off the $\mathbf{s}$ path:



If the above hypothesis is correct, then 100% of the output ought to be white.

Exercise 1.5. What statistics do you expect?

In fact, instead of finding that the output is 100% white particles, the output goes back to 50% white and 50% black. The same thing happens if we instead blocked off the internal hard beam.

Now, in the context of this experiment, consider the following question:

*Along which internal path (**h** or **s**) did the inputted white particle go?*

Exercise 1.6. Discuss what you think the answer is with those around you.

In fact, in asking this question, we have ostensibly revealed that the present state of affairs is in tension with basic logic. To see why, consider the possibilities:

- If it took **h**, then blocking the **s** path should have no effect. But, as we just saw, blocking the **s** path *does* have an effect: the output statistics change.
- If it took **s**, then blocking the **h** path should have no effect. But, like in the last experiment, blocking the **h** path *does* have an effect: the output statistics change.
- Maybe it somehow took both? Suppose, then, that when the particle is traversing the internal path we closely scrutinize the two tracks. No matter how we look, we invariably see it on only *one* of the two paths, so it makes no sense to say that it took both!
- Maybe it took neither? But that's moonshine: if it takes neither, then blocking both the **h** and **s** paths should have no effect, yet doing that yields no output at all!

These exhaust the logical possibilities. Surely, then, something is amok with these color and hardness boxes. After all, what else could be responsible for this inscrutable behavior? However, after decades of R&D into wildly different color and hardness boxes, all of which function perfectly but via totally unrelated means, our credence that it is the experimental apparatus at fault nears zero.

Hence, with exceptionally high credence—higher credence than most other scientific exploits—we disconcertingly find ourselves with this:

> *Particles passing through this last apparatus, to the extent that we are able to understand them, do not take the internal route **h**, nor the internal route **s**, nor both, nor neither.*

These exhaust the logical possibilities. Therefore, if this is right—and again we have exceptionally good evidence that it is—then there can be no *fact* of what internal route the particle took. In other words, despite our ability to measure the hardness of a white particle and to obtain, in every instance of measuring, a demonstrable fact of the matter of what we measure the hardness of the white particle to be, before we measure the hardness, there is no fact of the hardness of a white particle. In the philosopher David Albert's words, "asking which internal path the particle took is like asking what is the marital status of the number 5." It is, in philosophical terms, a *category mistake*. There is simply no fact of the matter of the question we are asking.

All of this suggests that in this experiment, something new and extraordinary is happening pre-measurement. As we will come to study mathematically in Part II, that extraordinary thing is called *quantum superposition*.

Exercise 1.7. Discuss with your group how you feel/think about this. Is there anything in your day-to-day that resembles a quantum superposition?

Much of quantum computing rests on our ability to create quantum superpositions, and then, in some sense, to compute a bunch of things in parallel. We will see an example of this when we discuss Grover's algorithm in Part IV.

1.2. Another Experimental Fact of Life: Bell's Theorem

Yet another bizarre feature of quantum mechanics stems from something called *entanglement*, which we will formally introduce in Part II. In fact, this feature (called a *Bell inequality violation*) is arguably the most quantum thing about quantum mechanics.

Definition 1.1. Let S be a physical system with measurable properties A, B, and C, and let

$$\begin{aligned} N_S(A,B,C) &= \#\text{ times we see } S \text{ with } A, B, \text{ and } C \\ N_S(A,B,\bar{C}) &= \#\text{ times we see } S \text{ with } A, B, \text{ and NOT } C \\ N_S(A,B) &= \#\text{ times we see } S \text{ with } A \text{ and } B, \\ &\vdots \end{aligned}$$

Example 1.1.

- S is a car, A is "its speed is 42 mph relative to the road", B is "its GPS coordinates are $(45.97639, 7.65861)$", and C is "its color is blue".

- S is a star, A is "its mass is 1.5 times that of the Sun", B is "its luminosity is 1.1 times that of the Sun", and C is "its angular momentum is 0.4 times that of the Sun".
- S is an electron, A is "its color is black" (a.k.a. "its spin state is up along the x-axis"), B is "its hardness is hard" (a.k.a. "its spin state is up along the y-axis"), and C is "its spin state is up along the z-axis" (which we could give another fun name, e.g., whimsey).

Claim 1.1. *For all systems S with measurable properties A, B, and C,*

$$N_S(A, \bar{B}) + N_S(B, \bar{C}) \geq N_S(A, \bar{C}).$$

Proof. The right-hand side equals

$$\begin{aligned} \text{RHS} &= N_S(A, \bar{C}) \\ &= N_S(A, B, \bar{C}) + N_S(A, \bar{B}, \bar{C}). \end{aligned}$$

The left-hand side equals

$$\begin{aligned} \text{LHS} &= N_S(A, \bar{B}) + N_S(B, \bar{C}) \\ &= N_S(A, \bar{B}, C) + \underbrace{N_S(A, \bar{B}, \bar{C}) + N_S(A, B, \bar{C})}_{\text{RHS}} + N_S(\bar{A}, B, \bar{C}) \\ &= N_S(A, \bar{B}, C) + N_S(\bar{A}, B, \bar{C}) + \text{RHS} \\ &\geq \text{RHS}. \end{aligned}$$

■

Theorem 1.2 (A Version of Bell's Theorem)**.** *Let S be two qubits, e_A and e_B, in the Bell state $|\Phi^+\rangle$, and consider the measurable properties*

- *A = the state of e_A is up along the z-axis,*
- *B = the state of e_B is up along the θ-axis,*
- *C = the state of e_B is up along the 2θ-axis.*

Then, for sufficiently small $\theta > 0$,

$$N_S(A, \bar{B}) + N_S(B, \bar{C}) < N_S(A, \bar{C}).$$

What the heck is going on will have to wait. Interestingly, though, in certain models of quantum computation that exhibit a provable quantum advantage (e.g., quantum shallow circuits), their advantage is reducible to a Bell inequality violation like this.

Reading 1
Computation is Physical

Quantum computation, unsurprisingly, is about computation. But what *is* computation? In this reading, you will learn a few of the essential parts of the answer. For the full answer, I encourage you to take a course on computability theory in the computer science department. For us in the physics department, however, the key idea will be that computation—whatever it is—is governed by the laws of physics.

1.1. Binary Encodings

Computers compute. But what is it that they are computing? If you think hard about it, perhaps you'll convince yourself that computers compute functions. And in particular, I claim, they compute *boolean functions*, which are functions that map binary strings (a sequence of zeroes and ones) to binary strings.

But wait! A computer can compute the function that maps an integer (e.g., 42) to a list of integers consisting its prime decomposition (e.g., $[2, 3, 7]$). Where is the binary in that? Or what about the WolframAlpha-like function that maps a string of text and mathematical symbols (e.g., "What is $\int_0^1 x\, dx$?") to a rational number (e.g., $1/2$)? Where is the binary in that? Or, as one more example, what about the ChatGPT-like function that maps a string of text (e.g. "Write an essay about quantum computation in the style of Shakespeare") to a decent, human-like response to the input string (e.g., "O, what a marvel is this quantum computation, a realm where the very fabric of thought and matter doth intertwine! ..."). Where is the binary in that?

The answer to all of these questions is that both the input and output can be *encoded* in binary. We will show how this works for integers in a moment, but hopefully the more general claim is somewhat believable. After all, in your day-to-day, you only ever use a finite number of symbols to express yourself, to ask questions, to give answers, and so forth. This means that to each symbol you can associate a unique binary string (as in, for example, ASCII), so that text, numbers,

mathematical symbols, etc. can all be encoded in binary.

To understand how this works for integers, let $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ be the set of positive integers and, for every positive integer $n \in \mathbb{N}$, let $\{0,1\}^n$ be the set of all n-bit strings. For example,

$$\{0,1\}^1 = \{0,1\} \quad \text{and} \quad \{0,1\}^2 = \{00, 01, 10, 11\}.$$

Problem 1.1.

(a) Find $\{0,1\}^3$.

(b) Show that for all $n \in \mathbb{N}$, the set $\{0,1\}^n$ contains 2^n elements.

We will now describe the canonical encoding of integers as binary strings. We will not prove its correctness, but you are encouraged to think about it.

Example 1.2. Given a positive integer $N \in \mathbb{N}$, let $n \in \mathbb{N}$ be the smallest positive integer such that $N \leq 2^n$. Then, there exists a unique list of n bits $x_1, x_2, \dots, x_n \in \{0,1\}$, or equivalently a unique string $x = x_1 x_2 \dots x_n \in \{0,1\}^n$, such that

$$N = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0.$$

Notice that in this encoding scheme, x_n (the last bit in the string x) is the least significant bit and x_1 (the first bit in the string x) is the most significant bit. Also, since by definition n is the smallest positive integer such that $N \leq 2^n$, it holds that $n \approx \log N$, where the logarithm is taken base 2.[1] In this way, we can encode integers as binary strings, and also interpret binary strings as integers.

Consequently, binary strings have both the necessary and sufficient amount of expressibility to talk about the positive integers. A simple corollary of this is that there are as many positive integers as there are binary strings. This fact is paramount to the theory of computation, so in the next problem you are asked to think about it some more.

Problem 1.2. Let $\{0,1\}^*$ be the set of all finite binary strings,

$$\{0,1\}^* = \bigcup_{n \in \mathbb{N}} \{0,1\}^n.$$

Use the encoding scheme discussed in Example 1.2 to argue (or if you are mathematically inclined, formally prove) that there are as many elements in the set $\{0,1\}^*$ as there are positive integers. In other words, argue that $\{0,1\}^*$ is countably infinite (as opposed to *un*countably infinite, like the real number line $\mathbb{R}$). Conclude that $\{0,1\}^*$ and $\mathbb{N}$ are bijective sets, which implies that every positive integer can be *uniquely* encoded as a binary string and vice versa.

[1] In fact, $n = \lfloor \log(N-1) \rfloor + 1$, where $\lfloor \cdot \rfloor$ is the floor function.

1.2. How Many Boolean Functions Are There?

In the last section, we introduced the idea that computers (including quantum computers) compute functions. In particular, computers compute *boolean* functions, which are maps from bit strings to bit strings. In functional notation, a boolean function f is expressed as follows,[2]

$$f : \{0,1\}^* \to \{0,1\}^*.$$

In this and the next section, we will study some of the basic properties of boolean functions. Ultimately, we are working toward a proof that there are boolean functions that no computer—quantum or not—can compute. That is rather interesting, for it suggests that perhaps what is so exciting about quantum computers is *not* that quantum computers can compute more functions than classical computers, but rather something more nuanced. Indeed, as we will discuss later, that is the case: classical computers can compute every function that a quantum computer can compute, and vice versa.

Claim 1.3. *There are uncountably many boolean functions. In other words, there are as many boolean functions as there are numbers on the real number line* $\mathbb{R}$.

Proof. Since $\{0,1\}^*$ and $\mathbb{N}$ are bijective sets (Problem 1.2), the number of functions $f : \{0,1\}^* \to \{0,1\}^*$ is equal to the number of functions $f : \mathbb{N} \to \mathbb{N}$. Therefore, it suffices to analyze how many functions there are that map $\mathbb{N}$ to $\mathbb{N}$. To obtain a contradiction, suppose there are only countably many functions $f : \mathbb{N} \to \mathbb{N}$. Then, there are as many such functions as there are positive integers, which implies that we can enumerate these functions by the positive integers: f_1, f_2, f_3, and so forth.

We will now define a new function that we will prove is not on this list. This proves the claim, for it contradictc our assumption that there are only countably many functions $f : \mathbb{N} \to \mathbb{N}$.[3]

Let $h(n) = f_n(n) + 1$. Clearly h maps positive integers to positive integers, i.e., $h : \mathbb{N} \to \mathbb{N}$. Thus, by assumption, h is one of the functions on the list $f_1, f_2, f_3, \ldots$. In other words, there exists a positive integer k such that $h(n) = f_k(n)$ for all $n \in \mathbb{N}$. Therefore, on one hand,

$$h(k) = f_k(k).$$

[2] If you have not seen functional notation before, it is merely a notational tool to quickly convey the domain and codomain of a function. A more general function f that maps elements of a set X (the domain of f) to a set Y (the codomain of f) is expressed as $f : X \to Y$.

[3] This proof technique is called *diagonalization*, and it is ubiquitous in computability theory.

But, on the other hand, it holds by the definition of h that

$$h(k) = f_k(k) + 1.$$

Therefore, $f_k(k) + 1 = f_k(k)$, which implies $1 = 0$. That is as good as contradictions get. Hence, our assumption that there are only countably many functions $f : \mathbb{N} \to \mathbb{N}$ is false, so there must be *un*countably many. Since the number of functions $f : \mathbb{N} \to \mathbb{N}$ is the same as the number of boolean functions $f : \{0,1\}^* \to \{0,1\}^*$, it follows that there are uncountably many boolean functions as well. ■

Okay, there are uncountably many boolean functions, but so what? That doesn't seem to get us any closer to the claim that perhaps there are functions that no computer—no matter how powerful—can compute.

At this point, that is true, because we do not have a formal idea of what it even means to "compute". For that, we need the Church–Turing thesis.

1.3. The Church–Turing Thesis

Among the uncountably many boolean functions, we are particularly interested in those that we can "compute" in some sense. To get at this, consider the following informal idea.

Definition 1.2. Say $f : \{0,1\}^* \to \{0,1\}^*$ is *effectively calculable* iff ("if and only if") there exists a finite, pen-and-paper procedure whereby a rote worker can deduce $f(x)$ for any given $x \in \{0,1\}^*$.

Effective calculability gets at what is hopefully an agreeable notion of what it means "to compute", namely, that there is some finite, mechanical (and physical!) process to evaluate the function f on any input. However, this notion is awkwardly informal (what is a "pen-and-paper procedure" mathematically?). Ultimately, it is the purpose of the Church–Turing thesis to formally explicate these ideas.

Thesis 1.4 (Church–Turing Thesis)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is effectively calculable iff it is computable by a Python program, i.e., iff there exists a Python program M such that for all inputs $x \in \{0,1\}^*$, $M(x) = f(x)$.*[4]

Crucially, the Church–Turing thesis is not a statement that one can prove. Instead, it is a postulate about computability theory that makes an hitherto

[4]Note, one can replace "Python program" with "deterministic Turing machine", for example, because Python is a Turing-complete programming language (as is PowerPoint, by the way).

informal idea (effective calculability) mathematically rigorous. It is generally accepted as correct, as all reasonable models of computation (Turing machines, circuits, random-access machines, and even all reasonable models of quantum computers) are provably equivalent in power to Python programs, and so they do not challenge the Church–Turing thesis. We will return to this point in the next section. Here, we want to establish that there are, in fact, *un*computable functions, and we are now in a position to show this.

Problem 1.3.

(a) Use the fact that there are uncountably many boolean functions (Claim 1.3) to prove that there exists a boolean function that no Python program can compute. Together with the Church–Turing thesis (Thesis 1.4), conclude that there are *uncomputable* functions. (*Hint:* It suffices to prove that there are only countably many Python programs. Why is that true? At the end of the day, what is a Python program but a finite string of symbols that has been typed out on a keyboard with finitely many keys?)

(b) Argue that, in fact, *most* boolean functions are uncomputable, in the same sense that most real numbers are not integers.

(c) Say a real number $x \in \mathbb{R}$ is *computable* iff there is a Python program M that on input $n \in \mathbb{N}$, outputs the first n digits of x. For example, π is computable, because there are algorithms that output the first n digits of π for any $n \in \mathbb{N}$ (e.g., an algorithm that uses the Taylor series for the arctangent function and computes $4 \arctan 1 = \pi$). Use part (b) to argue that most real numbers are not computable.[5]

1.4. The Church–Turing–Deutsch Thesis

In quantum computing, we take the perspective that computers are physical devices that evolve according to the laws of physics. This, of course, is motivated by the Church–Turing thesis, since the picture of someone working tirelessly with pen-and-paper, deducing on pain of irrationality $f(x)$ for any given x, is manifestly physical.

Problem 1.4. Is computational physical? Are computers constrained by physical law? Write a few sentences explaining how you feel about this.

[5]For an entertaining discussion of this fact, and how it more or less implies that we humans are privy to but a negligible fraction of $\mathbb{R}$, see this Numberphile video featuring Matt Parker.

This motivates the following, highly informal "definition" that is akin to the notion of effective calculability.

Definition 1.3. Say $f : \{0,1\}^* \to \{0,1\}^*$ is *physically calculable* iff there exists a finite, physical system whose mere physical evolution computes $f(x)$ for any given $x \in \{0,1\}^*$.

Again, this is awkwardly informal. Moreover, physical calculability comes across as substantially less anthropomorphic than effective calculability, as there is no mention of a "worker" here. That said, the effective calculability picture is nevertheless physical, so physical calculability subsumes the notion of effective calculability. Together with the Church–Turing thesis, this intuition suggests the following claim.

Claim 1.5. *If $f : \{0,1\}^* \to \{0,1\}^*$ is computable by a Python program, then f is physically calculable.*

Problem 1.5.

(a) Do you think this is reasonable?

(b) What about the converse? Do you think there is a physically calculable function $f : \{0,1\}^* \to \{0,1\}^*$ (computed, perhaps by the interactions of a bunch of electrons or, more exotically, the Hawking radiation from a Schwarzschild black hole) that is *not* computable by any Python program?

In fact, it is generally believed that every physically calculable function is computable. This is largely based on two ideas: (1) that quantum systems can be simulated by classical computers and (2) *reductionism*, i.e., that quantum mechanics underlies everything there is in the universe.[6] Put together, this belief constitutes its own thesis:

Thesis 1.6 (Church–Turing–Deutsch Thesis)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is physically calculable iff it is computable by a Python program.*

Again, like the Church–Turing thesis, this statement is not something that one can prove. Instead, its purpose is to make mathematically precise an hitherto informal idea (physical calculability). Note also that this thesis is no longer just a

[6]That said, a result in quantum field theory known as the *Nielsen–Ninomiya Theorem* suggests that the Standard Model of particle physics cannot be simulated on a classical computer. This, however, is up for debate as there are some workarounds.

postulate about computability theory, but is also a postulate about the physical world. In my opinion, this elevates the set of all computable functions to the level of a fundamental constant of nature, on a par with the speed of light c, Plank's constant $\hbar$, and Newton's gravitational constant G.

At this point, we can make the following conclusion: quantum systems (and quantum computers in particular) cannot compute functions that no classical computer can. In other words, for every quantum computer, there exists a classical computer that can simulate it, and vice versa.

But wait! If that's the case, then what are we doing here? If classical computers compute the same set of boolean functions as quantum computers, then what is so exciting about quantum computing?

1.5. Feynman's Vision

In 1981, the physics Nobel laureate Richard Feynman wrote a famous paper entitled *Simulating Physics with Computers*, available here. There, he notes that a faithful description of an n-state quantum system (typically denoted using Paul Dirac's ket notation, $|\psi\rangle$) seems to require at least 2^n complex numbers. Therefore, to accurately simulate the evolution of $|\psi\rangle$ on a classical computer would require storing an exponential number of parameters, so that the overall simulation will take a *very* long time (as a function of n). The quantum system, however, merely evolves its state $|\psi\rangle$ with ease according to something called the Schrödinger equation. In this way, while a quantum system cannot compute a function that no classical computer can compute (Thesis 1.6), it sure seems that a quantum system ought to be able to compute a function *faster* than any classical computer. Indeed, *this* is what is so exciting about quantum computing. Its not to do with what is and what is not computable; its to do with what is and what is not computable *efficiently*. Overall, the suspicion of most folks in the quantum computing world is the following.

Conjecture 1.7. *There exists a boolean function f that a quantum computer can compute in so-called "polynomial time", but any classical computer that computes f takes "exponential time".*[7]

Ultimately, we expect this "quantum advantage" or "quantum speedup" to come from the inimitable bizarreness of the quantum world. Next lecture, we will start our study of the essential mathematics that underlies quantum computing.

[7] If you've heard of the complexity class NP, note that Conjecture 1.7 does not imply that we think quantum computers can solve all the problems in NP because the function f in the conjecture need not correspond to an NP-complete problem (e.g. factoring integers).

Part II
The Postulates of Quantum Mechanics

Lecture 2
The Description and Evolution of Quantum Systems

Discussion 2.1. Discuss with your group what you took away from Part I.

In Part I, we discussed at a high level two bizarre features of quantum mechanics, namely, superposition and entanglement, which together enable a so-called "Bell inequality violation". We also discussed what is means for a computer to compute, the fact that not all functions are computable, and the fact that quantum computers—whatever they are—cannot compute more functions than classical computers. That said, we learned Feynman's insight that quantum computers *might* be able to compute certain functions *faster* than any classical computer.

In this lecture and the associated reading, we will learn the basic mathematics that underlie quantum computing. This will include a discussion of the postulates of quantum mechanics, their mathematical formalism, and the all-important notion of a qubit.

2.1. The States of Quantum Systems

Every physical theory has physical primitives that do not have a totally agreeable definition. For example, a "particle" is a primitive in Newtonian mechanics and in Einstein's relativity. In quantum mechanics, the physical primitive is a "quantum system". It is a "you know it when you see it" sort of thing that exists in the real world. If you like reductionism, then most likely every physical system is a quantum system, although that position is contended by some. Ultimately, though, we will not define what a "quantum system" is, in the same way that in Newtonian mechanics we do not define what a "particle" is.

Postulate 2.8.

- *To every quantum system S, there corresponds a complex-valued vector space*

(a.k.a. a Hilbert space*)*

$$\mathcal{H} = \mathbb{C}^N = \left\{ \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix} : \psi_1, \psi_2, \ldots, \psi_N \in \mathbb{C} \right\},$$

where N is the dimension *of $\mathcal{H}$.*

- *Vectors in $\mathcal{H}$ are called* ket vectors*. They are denoted using Paul Dirac's "ket notation",*

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix}.$$

- *For all $|\psi\rangle \in \mathcal{H}$, there exists a* dual vector $\langle\psi|$*, known as a* bra vector*, which formally is in the dual space of $\mathcal{H}$. For our purposes, the bra vector $\langle\psi|$ can be thought of as a row vector that is the conjugate transpose (or dagger, †) of $|\psi\rangle$:*

$$\begin{aligned} \langle\psi| &= |\psi\rangle^\dagger \\ &= (|\psi\rangle^*)^T \\ &= \begin{pmatrix} \psi_1^* & \psi_2^* & \cdots & \psi_N^* \end{pmatrix}. \end{aligned}$$

- *There exists an inner product on $\mathcal{H}$, called the* bra-ket ("bracket") inner product*, given by:*

$$\begin{aligned} \langle\psi|\phi\rangle &= \langle\psi||\phi\rangle \\ &= \begin{pmatrix} \psi_1^* & \psi_2^* & \cdots & \psi_N^* \end{pmatrix} \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_N \end{pmatrix} \\ &= \sum_{i=1}^{N} \psi_i^* \phi_i. \end{aligned}$$

- *The bra-ket inner product induces a norm on $\mathcal{H}$:*

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} = \sqrt{\sum_{i=1}^{N} \psi_i^* \psi_i}.$$

- *A* unit-vector *(a.k.a. a* normalized vector*) is* $|\psi\rangle \in \mathcal{H}$ *such that*

$$\||\psi\rangle\| = 1.$$

- *A* quantum state *(or just* state*) of the system* S *is a unit-vector in* $\mathcal{H}$*.*

For us, the most important example of a quantum system is that of a *qubit*.

Example 2.3 (Qubit)**.**

- A *quantum bit* (or *qubit* for short), a.k.a. a *two-state system*, is any quantum system S whose Hilbert space is two-dimensional:

$$\mathcal{H}_S = \mathbb{C}^2 = \left\{ \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} : \psi_1, \psi_2 \in \mathbb{C} \right\}.$$

- The two most important states of a qubit are the *computational basis states*, which are just the Cartesian basis vectors of $\mathbb{C}^2$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Exercise 2.8. Do you know a quantum system whose Hilbert space is $\mathbb{C}^4$? $\mathbb{C}^{2^n}$?

Postulate 2.8, and in particular the vector space structure underlying quantum systems, naturally entails the notion of superposition that we alluded to in Part I.

Fact 2.9 (Superposition)**.** *If* $|\psi\rangle$ *and* $|\phi\rangle$ *are quantum states, then so is*

$$\alpha|\psi\rangle + \beta|\phi\rangle$$

for all $\alpha, \beta \in \mathbb{C}$ *such that* $|\alpha|^2 + |\beta|^2 = 1$*, where* $|\alpha|^2 = \alpha^*\alpha$ *and* $|\beta|^2 = \beta^*\beta$*.*

In Part III, we will discuss how to encode classical data into a quantum state. Already, however, we can guess how this will go, given the notation used to label the computational basis states of a qubit:

$$0 \longleftrightarrow |0\rangle \quad \text{and} \quad 1 \longleftrightarrow |1\rangle.$$

This association constitutes a very natural classical-quantum encoding scheme. What's more, though, is that not only are the bit values 0 and 1 faithfully represented quantumly, but a whole new host of "intermediate values" are as well. In particular,

thanks to superposition, we can sensibly talk about the state $\alpha|0\rangle + \beta|1\rangle$ as a valid encoding of quantum data. Per our discussion in Part I, this has no classical counterpart. Thus, quantum mechanics allows quantum computers to have more complex representations of data than classical computers, and this is one of many popular arguments for why quantum computers are potentially more powerful that classical computers.[8]

Exercise 2.9. Given our discussion of the Stern–Gerlach experiment in Part I, what would you say the difference is between the states $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$? Discuss with those around you.

2.2. The Evolution of Quantum Systems

We will now discuss how quantum systems evolve in time. This is essentially the $F = ma$ postulate of quantum mechanics.

Postulate 2.10 (The Schrödinger Equation)**.** *Let S be a quantum system with Hilbert space $\mathcal{H}_S = \mathbb{C}^N$. Absent any "measurements" of the system, if at time t_1 the state of S is $|\psi(t_1)\rangle$ and if at time $t_2 \neq t_1$ the state of S is $|\psi(t_2)\rangle$, then there exists an $N \times N$* unitary *matrix U such that*

$$|\psi(t_2)\rangle = U|\psi(t_1)\rangle.$$

In other words, with no measurements, every quantum state $|\psi\rangle \in \mathcal{H}_S$ evolves in time unitarily*. This is one form of the* Schrödinger equation.[9]

What does this mean?

Definition 2.4.

- An $N \times N$ matrix U is *unitary* iff $U^{-1} = U^\dagger = (U^*)^T$.
- $\mathrm{U}(N) = \{N \times N \text{ unitary matrices } U\}$. With matrix multiplication, $\mathrm{U}(N)$ forms a group (in fact, a Lie group) called the *unitary group of order N*.[10]

[8] See, for example, former Canadian Prime Minister Justin Tredeau explaining it here.

[9] Notice here that t_2 is not necessarily greater than t_1. Therefore, the evolution of quantum systems—at least according to the Schrödinger equation—is always *reversible*.

[10] Recall, a *group* is a pair $(G, \cdot)$, where G is a set and $\cdot : G \times G \to G$ is a binary operation, such that the operation is associative, G has an identity element, and G is closed under inverses. A *Lie group* is a group that is simultaneously another mathematical structure called a *manifold*.

Example 2.4. The following matrices are unitary:

- I_N (the $N \times N$ identity matrix),
- the T or $\pi/8$ *gate*:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \qquad T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix},$$

- the H or *Hadamard gate*:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H^\dagger,$$

- the S or *phase gate*:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix},$$

- the X, Y, *and* Z *Pauli matrices*:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X^\dagger, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y^\dagger, \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z^\dagger,$$

- the SWAP *gate*:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \text{SWAP}^\dagger,$$

- and the *controlled*-NOT or CNOT *gate*:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \text{CNOT}^\dagger.$$

Exercise 2.10.

(1) What is U(1) geometrically?

(2) Let $U \in \mathrm{U}(N)$ and $|\psi_1\rangle, |\phi_1\rangle \in \mathbb{C}^N$. If $|\psi_2\rangle = U|\psi_1\rangle$ and $|\phi_2\rangle = U|\phi_1\rangle$, prove that $\langle\phi_2|\psi_2\rangle = \langle\phi_1|\psi_1\rangle$.

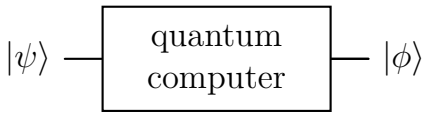
This last exercise is important. It reveals that unitary maps *preserve* the bra-ket inner product. Therefore, unitary maps are the *structure-preserving* maps on Hilbert spaces, in the same way that bijective maps are the structure-preserving maps on sets, homeomorphisms are the structure-preserving maps on topological spaces, homomorphisms are the structure-preserving maps on groups, and so forth. This is the mathematical reason why unitary operators are so important in quantum mechanics. A related fact is the following.

Fact 2.11. *If λ is an eigenvalue of $U \in \mathrm{U}(N)$, then $\lambda = e^{i\theta}$ for some $\theta \in [0, 2\pi)$.*

Therefore, unitary operators do not "scale" the vectors they act on.[11] Of course, given Postulate 2.10, such behavior is expected, for otherwise unitary operators would not be norm-preserving, so they would not map quantum states to quantum states.

2.3. Application: Quantum Computers

We are now in a position to formally discuss what a quantum computer actually is, at least at a high level. Simply put, a quantum computer is a map that takes as input a high-dimensional quantum state $|\psi\rangle \in \mathbb{C}^{2^n}$, and then outputs another state $|\phi\rangle$ in the same Hilbert space $\mathbb{C}^{2^n}$. Pictorially,



where time flows from left to right. Therefore, a quantum computer time-evolves a state $|\psi\rangle$ to a different state $|\phi\rangle$. By Postulate 2.10, there exists a unitary operator $U_{\mathrm{QC}} \in \mathrm{U}(2^n)$ that implements this transformation:

$$|\phi\rangle = U_{\mathrm{QC}}|\psi\rangle.$$

Consequently, *every quantum computer is a unitary operator.* Exactly what unitary operator depends on the algorithm the computer implements. We will see an example of this when we discuss Grover's algorithm in Part IV.

[11] Technically to reach this conclusion one must study the *singular values* of the unitary matrix in question. However, unitary matrices are examples of *normal matrices*, and the singular values of normal matrices are the (absolute values of the) eigenvalues.

In Postulate 2.10, there was an important qualification to the effect of "quantum states evolve in time unitarily provided the system is not being *measured*." Here, we discuss what it means "to measure" a quantum system, at least mathematically. Unfortunately, we can't do much better than afford a mathematical description because, at least at the moment, there is no consensus in the physics community what it *really* means to measure a quantum system, as nobody knows what the correct interpretation of quantum mechanics is.[12]

Postulate 2.12 (The Collapse Postulate)**.** *Let S be a quantum system with Hilbert space $\mathcal{H}_S = \mathbb{C}^N$ and let $B = \{|b_1\rangle, |b_2\rangle, \ldots, |b_N\rangle\}$ be an orthonormal basis of $\mathcal{H}_S$.*

- *Mathematically, to "measure S in the basis B" means to project the state of S to one of the B basis vectors with a certain probability. In particular, if S is in the state $|\psi\rangle$, then the probability of measuring S to be in the state $|b_i\rangle$ is got by the* Born rule*:*

$$\Pr\left[\textit{state of } S \textit{ is } |b_i\rangle\right] = \langle\psi|\Pi_{b_i}|\psi\rangle,$$

  where $\Pi_{b_i} = |b_i\rangle\langle b_i|$ is the outer product of $|b_i\rangle$ with $\langle b_i|$*, which is just the matrix you get when you multiply the column vector $|b_i\rangle$ by the row vector $\langle b_i|$. This matrix is also called the* projection matrix onto the state $|b_i\rangle$*.*

- *Immediately after the measurement, the state of S "collapses" to $|b_i\rangle$, which is to say that the measurement induces the (generally non-unitary) state evolution $|\psi\rangle \mapsto |b_i\rangle$.*

Exercise 2.11. Consider a qubit S in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. If one measures S in the computational basis, then what is the probability of measuring $|0\rangle$? $|1\rangle$?

This exercise reveals the meaning of the coefficients or "amplitudes" in a quantum state vector. In particular, they correspond to the *probability density* of seeing the quantum system in a particular basis state. Since, by the Born rule, we square these amplitudes to get the probability, it follows that the probability of obtaining a particular state is actually independent of any sort of "phase" that multiplies it. For example, the probability of measuring $|0\rangle$ in the states $|0\rangle$ and $e^{i\theta}|0\rangle$ is the same, no matter what θ is. For this reason, we say that $|0\rangle$ and $e^{i\theta}|0\rangle$ are *operationally*

[12] For more on this and other foundational issues in quantum mechanics, I recommend Adam Becker's book *What is Real?: The Unfinished Quest for the Meaning of Quantum Physics*.

equivalent because there is no measurement that one can do to distinguish them. The complete definition is below.

Definition 2.5. Two states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ are *operationally equivalent* iff there exists $\theta \in [0, 2\pi)$ such that $|\psi\rangle = e^{i\theta}|\phi\rangle$.

The importance of operational equivalence becomes apparent in the following fact, which shows that an experiment can in principle distinguish two quantum states iff they are not operationally equivalent.

Fact 2.13 (Corollary of the *Helstrom–Holevo Bound*)**.** *Let S be a quantum system that is either in state $|\psi\rangle$ or $|\phi\rangle$. There exists a series of measurements that can in principle determine which state S is in iff $|\psi\rangle$ and $|\phi\rangle$ are operationally inequivalent.*

For this reason, quantum states that differ by an overall phase factor $e^{i\theta}$ are equivalent, because no experiment—not even in principle—can distinguish them. This fact appears all over quantum mechanics, and it will be relevant when we study Bell's theorem in Part III.[13]

[13]Incidentally, a more Noetherian interpretation of operational equivalence is that quantum mechanics exhibits a *local* U(1) *symmetry*. This is one of many redundancies in the laws of physics. For more, consider learning *gauge theory*.

Reading 2

Composite Systems and Entanglement

In the last lecture, we discussed three of the four postulates of quantum mechanics, namely, the mathematical representation of states of quantum systems, the unitary evolution of quantum systems, and the non-unitary "collapse postulate", which has to do with the action of measuring or, more anthropomorphically, "looking at" quantum systems.

In this reading, you will learn the final postulate of quantum mechanics, namely, the mathematical representation of *composite* quantum systems. This is important for quantum computation because only by combining many qubits together will a quantum computer be able to perform computations on bit *strings*.

As you will see, the key to talking about composite quantum systems lies in understanding a single mathematical operation on matrices known as the *tensor product*. The tensor product is associated with the cool but intimidating-looking mathematical symbol $\otimes$. I promise, though, that this operation is actually quite simple. Like normal matrix multiplication, all it takes is a little getting used to.

2.1. The Tensor Product

Definition 2.6. Let A and B be $N_A \times M_A$- and $N_B \times M_B$-dimensional matrices, respectively. The *tensor product of A and B*, denoted $A \otimes B$, is the $N_A N_B \times M_A M_B$-dimensional matrix[14]

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1M_A}B \\ a_{21}B & a_{22}B & \cdots & a_{2M_A}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{N_A1}B & a_{N_A2}B & \cdots & a_{N_AM_A}B \end{pmatrix},$$

where a_{ij} is the entry in the ith row and jth column of A.

[14]The mathematician would point out that technically this is the *Kronecker product*, which is a special case of the tensor product. It is also known as the *direct product of matrices*.

Below are several examples.

Example 2.5.

- Let
$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}.$$
Then,
$$\begin{aligned} A \otimes B &= \begin{pmatrix} B & 2B \\ 3B & 4B \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} & 2\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} \\ 3\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} & 4\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 4 & 3 & 8 & 6 \\ 2 & 1 & 4 & 2 \\ 12 & 9 & 16 & 12 \\ 6 & 3 & 8 & 4 \end{pmatrix}. \end{aligned}$$

- Similarly,
$$\begin{aligned} B \otimes A &= \begin{pmatrix} 4A & 3A \\ 2A & A \end{pmatrix} \\ &= \begin{pmatrix} 4\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & 3\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\ 2\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 4 & 8 & 3 & 6 \\ 12 & 16 & 9 & 12 \\ 2 & 4 & 1 & 2 \\ 6 & 8 & 3 & 4 \end{pmatrix}. \end{aligned}$$
Consequently, $A \otimes B \neq B \otimes A$, so like the usual matrix product, the tensor product is generally not commutative.

- Let I_N and I_M be the $N \times N$ and $M \times M$ identity matrices, respectively. Then $I_N \otimes I_M$ equals the $NM \times NM$ identity matrix I_{NM}. Thus, in this special case, the tensor product *is* commutative because
$$I_N \otimes I_M = I_{NM} = I_{MN} = I_M \otimes I_N.$$

- Quantum states are represented by ket and bra vectors. Since these are column and row vectors, which are just $N \times 1$ and $1 \times N$ matrices, respectively, it makes sense to take the tensor product of quantum states. To see how this works, suppose

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_{N_A} \end{pmatrix} \in \mathbb{C}^{N_A} \quad \text{and} \quad |\phi\rangle = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{N_B} \end{pmatrix} \in \mathbb{C}^{N_B}.$$

  Then,

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \psi_1|\phi\rangle \\ \psi_2|\phi\rangle \\ \vdots \\ \psi_{N_A}|\phi\rangle \end{pmatrix} = \begin{pmatrix} \psi_1 \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{N_B} \end{pmatrix} \\ \psi_2 \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{N_B} \end{pmatrix} \\ \vdots \\ \psi_{N_A} \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{N_B} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \psi_1\phi_1 \\ \psi_1\phi_2 \\ \vdots \\ \psi_1\phi_{N_B} \\ \psi_2\phi_1 \\ \psi_2\phi_2 \\ \vdots \\ \psi_2\phi_{N_B} \\ \vdots \\ \psi_{N_A}\phi_1 \\ \psi_{N_A}\phi_2 \\ \vdots \\ \psi_{N_A}\phi_{N_B} \end{pmatrix} \in \mathbb{C}^{N_A N_B}.$$

  Similarly,

$$\langle\psi| \otimes \langle\phi| = \begin{pmatrix} \psi_1^*\langle\phi| & \psi_2^*\langle\phi| & \cdots & \psi_{N_A}^*\langle\phi| \end{pmatrix}.$$

  In this context, it is often tedious to keep track of all the tensor product symbols. For this reason, I (and others) will often omit the tensor product symbol $\otimes$ when talking about states and instead adopt the notational shorthand

$$|\psi\rangle|\phi\rangle = |\psi\rangle \otimes |\phi\rangle \quad \text{and} \quad \langle\psi|\langle\phi| = \langle\psi| \otimes \langle\phi|.$$

  However, you should not use this shorthand for more general matrices because it could easily be confused with matrix multiplication.

You should try your hand at the following problem before continuing.

Problem 2.1.

(a) Find the column vector associated with $|0\rangle|0\rangle = |0\rangle \otimes |0\rangle$. What 2-bit string would you say this state encodes?

(b) Find the column vector associated with $|1\rangle|0\rangle|0\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle$. What 3-bit string would you say this state encodes?

(c) Find $A \otimes B$, where

$$A = \begin{pmatrix} 2 & 42 \\ -5 & i \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 5 & 1 \\ -1 & 2 \end{pmatrix}.$$

Despite not being commutative, the tensor product still enjoys a number of nice properties.

Fact 2.14 (Useful Properties of the Tensor Product)**.**

(1) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ *whenever the matrix products are well-defined.*

(2) $(A + B) \otimes C = A \otimes C + B \otimes C$.

(3) $A \otimes (B + C) = A \otimes B + A \otimes C$.

(4) $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Here are some more problems to help you get familiar with the tensor product. I encourage you to do these before moving on.

Problem 2.2. Use Fact 2.14 to prove the four statements below. In particular, do *not* solve these problems by writing the matrices and vectors out in some basis.

(a) If $A \in \mathrm{U}(N)$ and $B \in \mathrm{U}(M)$, then $A \otimes B \in \mathrm{U}(NM)$. Therefore, the tensor product of two unitary matrices is itself a unitary matrix.

(b) If $A \in \mathrm{U}(N)$, $B \in \mathrm{U}(M)$, $|\psi\rangle \in \mathbb{C}^N$, and $|\phi\rangle \in \mathbb{C}^M$, then

$$(A \otimes B)|\psi\rangle|\phi\rangle = (A|\psi\rangle) \otimes (B|\phi\rangle).$$

Therefore, a tensor product of matrices acts on a tensor product of states in a very natural way.

(c) If $|\psi_A\rangle, |\phi_A\rangle \in \mathbb{C}^{N_A}$ and $|\psi_B\rangle, |\phi_B\rangle \in \mathbb{C}^{N_B}$, then

$$(\langle\psi_A|\langle\psi_B|)(|\phi_A\rangle|\phi_B\rangle) = \langle\psi_A|\phi_A\rangle \cdot \langle\psi_B|\phi_B\rangle.$$

Therefore, the bra-ket inner product of a tensor product of states is the product of the bra-ket inner products of the two states. (Note the similarity of this question to the question in (b).)

(d) Let

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big).$$

As we will discuss shortly, this is one of the four so-called *Bell states*. Show that

$$\langle\Phi^+|(|0\rangle\langle 0| \otimes I_2)|\Phi^+\rangle = \frac{1}{2},$$

where I_2 is the 2×2 identity matrix. (*Hint:* Use Fact 2.14 as well as parts (b) and (c).) As you may have guessed, this calculation corresponds to computing the probability that a *subsystem* computational measurement of $|\Phi^+\rangle$ returns $|0\rangle$. This type of calculation underlies both the EPR paradox and Bell's theorem in Part III, so do try to get this one!

2.2. Composite Systems

We now have everything we need to understand how to describe two or more quantum systems as one.

Postulate 2.15. *Let A and B be quantum systems with Hilbert spaces $\mathcal{H}_A = \mathbb{C}^{N_A}$ and $\mathcal{H}_B = \mathbb{C}^{N_B}$, respectively, and let $\{|a_1\rangle, \ldots, |a_{N_A}\rangle\}$ and $\{|b_1\rangle, \ldots, |b_{N_B}\rangle\}$ be bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The combined quantum system $A + B$ is described by the Hilbert space*

$$\mathcal{H}_{A+B} = \mathcal{H}_A \otimes \mathcal{H}_B = \text{span}\Big\{|a_i\rangle \otimes |b_j\rangle : i \in \{1, \ldots, N_A\}, j \in \{1, \ldots, N_B\}\Big\}.$$

In fact, $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^{N_A N_B}$.[15]

Problem 2.3. What is the Hilbert space for a quantum system composed of n qubits? In other words, if S is a quantum system consisting of n qubits, then $\mathcal{H}_S = \mathbb{C}^N$ for some positive integer N. What is N in terms of n?

[15] One way to prove this is to use the Cartesian bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, evaluate the tensor product between the various Cartesian basis elements, and then see that the resulting "tensored" basis is just the Cartesian basis of $\mathbb{C}^{N_A N_B}$.

2.3. Quantum Encodings

In quantum computing, we want to manipulate mathematical objects on a quantum computer. Because of this, we need a way to encode the mathematical object into a quantum state, so that the quantum computer can act on it. To do this, we will exploit the following observation.

Fact 2.16. *The set* $\{0,1\}$ *is bijective to the computational basis over* $\mathbb{C}^2$, $\{|0\rangle, |1\rangle\}$. *The two possible bijections are*

$$\begin{array}{ccc} 0 & \longleftrightarrow & |0\rangle \\ 1 & \longleftrightarrow & |1\rangle \end{array} \quad \textit{and} \quad \begin{array}{ccc} 0 & \longleftrightarrow & |1\rangle \\ 1 & \longleftrightarrow & |0\rangle \end{array}.$$

From an information-encoding point of view, the former is the most natural, so that is what we adopt. This bijection implies that every bit can be encoded into the quantum state of a qubit.

This conclusion is actually a particular case of a more general observation.

Fact 2.17. *For all* n, $\{0,1\}^n$ *contains* 2^n *elements (Problem 1.1), so* $\{0,1\}^n$ *is bijective to the Cartesian basis (a.k.a.* the computational basis*) over* $\mathbb{C}^{2^n}$,

$$\underbrace{\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}}_{2^n \textit{ elements}}.$$

Consequently, using any of the bijections between these two sets, one can encode n-bit classical data into a quantum system with Hilbert space $\mathbb{C}^{2^n}$. Unlike before, however, here there are *many* bijections from $\{0,1\}^n$ and the computational basis of $\mathbb{C}^{2^n}$ ($2^n!$ many, in fact[16]). Nevertheless, from an information-encoding point of view, the most natural is arguably

$$\begin{aligned} x = x_1 x_2 \ldots x_n \longleftrightarrow |x\rangle &= |x_1 x_2 \ldots x_n\rangle \\ &= |x_1\rangle |x_2\rangle \cdots |x_n\rangle, \end{aligned}$$

[16] *Proof:* For the first element in $\{0,1\}^n$, there are 2^n computational basis states to assign it to, for the second element in $\{0,1\}^n$, there are $2^n - 1$ computational basis states to assign it to, and so forth, for a total of $2^n!$ possible assignments.

where each $|x_i\rangle$ encodes x_i, the ith bit of x. We adopt this here.[17]

Problem 2.4.

(a) Let 0^n denote the n-bit, all zero string $00\ldots0$. What is $|0^n\rangle$ in terms of $|0\rangle$?

(b) Let S be a quantum system in the state

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle,$$

which represents a superposition over all n-bit strings. Given $y \in \{0,1\}^n$, what is the probability that one measures S in the state $|y\rangle$?

(c) Let H be the Hadamard gate (Example 2.4) and let $H^{\otimes n}$ denote the n-fold tensor product $H \otimes H \otimes \cdots \otimes H$. Show that

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle.$$

Conclude that if you measure $H^{\otimes n}|0^n\rangle$ in the computational basis, then you obtain $y \in \{0,1\}^n$ with the same probability had you uniformly drew y from $\{0,1\}^n$. Thus, acting $H^{\otimes n}$ on $|0^n\rangle$ and then measuring in the computational basis is an n-bit random number generator. This is a primitive example of a quantum algorithm.

Since all classical data can be represented in binary, this encoding scheme allows us to encode *semantic* classical data, such as integers.

Example 2.6. Let N be an integer with binary expansion

$$N = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0.$$

Then, the n-bit string $x_1 x_1 \ldots x_n$ encodes N in binary. One can then encode N into the state of a quantum system by encoding each of the n-bits of N into its own qubit, and then combining all of these n qubits together into one large, composite quantum system:

$$|N\rangle = |x_1\rangle|x_2\rangle\cdots|x_n\rangle.$$

Problem 2.5. Use the quantum encoding scheme in Exercise 2.6 to write $|42\rangle$ in terms of a tensor product of qubit states.

[17] We will not prove it here, but there exist unitary operators that implement the boolean AND, OR, and NOT operations. Thus, together with this encoding scheme, this fact allows one to prove that a quantum computer can do anything that a classical computer can do. In this way, quantum computers are at least as powerful as classical computers. For more on this, I recommend Nielson and Chuang's textbook *Quantum Information and Quantum Computation*.

2.4. Entanglement

In this final section, we will discuss what many argue is the most quintessentially quantum thing about quantum mechanics. This is *entanglement*, and it is only possible for composite quantum systems.

Fact 2.18 (Entanglement)**.** *By properties (2) and (3) in Fact 2.14, it is sometimes possible to factor superposed quantum states, for example:*

$$|\psi_1\rangle|\phi\rangle + |\psi_2\rangle|\phi\rangle = (|\psi_1\rangle + |\psi_2\rangle)|\phi\rangle.$$

In this case, the state is separable *because it can be written as a state from $\mathcal{H}_A$ times a state from $\mathcal{H}_B$. However, this is not always possible, for example:*

$$|0\rangle|0\rangle + |1\rangle|1\rangle.$$

Try as you might, this (unnormalized) state cannot be written as a state from $\mathcal{H}_A$ times a state from $\mathcal{H}_B$. Hence, this state is not separable, instead it is entangled.

Definition 2.7. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. A state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is *separable* iff there exist $|\phi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$ such that $|\psi\rangle = |\phi\rangle_A|\phi\rangle_B$. We say $|\psi\rangle$ is *entangled* iff it is not separable.

Problem 2.6. Determine whether the following (unnormalized) states are separable or entangled:

(a) $|0\rangle|0\rangle + |1\rangle|0\rangle$

(b) $|0\rangle|0\rangle|0\rangle - |0\rangle|0\rangle|1\rangle$

(c) $|0\rangle|0\rangle|0\rangle - |0\rangle|1\rangle|1\rangle$

(d) $|0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle$

(e) $|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle$

(f) $|0\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle$.

(g) Would you say the state in (f) is more or less entangled than the state in (e)? Explain your answer.

In fact, there is a whole zoo of "entanglement measures" out there, which allow one to make statements like "this state is more entangled than that state, at least with respect to this measure". While there are many subtleties in entanglement theory, it is the case that for so-called "pure and bipartite states" (which is what we are dealing with here), there are canonical *maximally entangled states*. The four most relevant to us are the so-called "Bell states".

Definition 2.8. The four *Bell states* are the maximally entangled states

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle - |1\rangle|1\rangle\big) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big).
\end{aligned}$$

As we will see in Part III, the Bell states are key to Bell's theorem and non-local games. They also underlie many quantum mechanical protocols, such as superdense coding and quantum teleportation. In addition to their entanglement properties, the Bell states form a basis of $\mathbb{C}^4$ known as the *Bell basis*. Because of this, they are sometimes used in place of the computational basis to talk about the state of 2-qubit quantum systems.

Problem 2.7. Show that $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is an orthonormal basis of $\mathbb{C}^4$.

Part III
Bell's Theorem and Non-Local Games

Lecture 3
The EPR Paradox and Bell's Theorem

Discussion 3.1. Discuss with your group what you took away from Part II.

In Part II, we discussed the mathematical foundations of quantum computation and quantum information. This included a discussion of the postulates of quantum mechanics, as well as a formal discussion of superposition and entanglement—two of the most esoteric features of quantum mechanics.

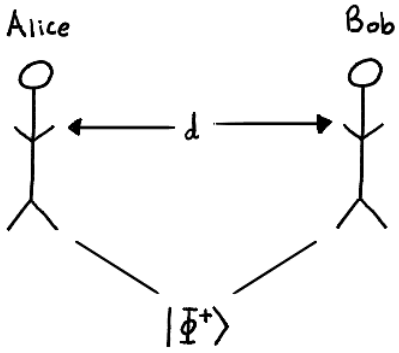
In this lecture and the associated reading, we will explore superpositions and entanglement in more detail. In particular, we will study two features of quantum mechanics that these phenomena entail, and we will discuss one way to think about them (which is in no way the "right" way, by the way; the "right" way, if there is one, is not presently known). In the reading, you will explore how one of these features (called a *Bell inequality violation*) can allow quantum systems to provably outperform any classical system at something called a non-local game. This is an example of a provable quantum computational advantage.

3.1. The Einstein–Podolsky–Rosen (EPR) Paradox

Consider two people, Alice and Bob, each with a qubit e_A and e_B in hand, that are spatially separated by a distance d. Suppose, further, that the joint state of their qubits is the (maximally entangled) Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big).$$

Here, the left ket in each term refers to Alice's qubit and the right ket refers to Bob's qubit. Pictorially, the situation is as follows:



Now, suppose Alice measures her qubit in the computational basis and Bob does nothing (which, formally, is to say that Bob applies the 2×2 identity operator I_2 to his qubit).

Claim 3.1. *The possible outcomes of Alice's measurement are* $|0\rangle$ *and* $|1\rangle$*. Moreover,*

$$\Pr\Big[\textit{Alice measures } |0\rangle\Big] = \frac{1}{2} \quad \textit{and} \quad \Pr\Big[\textit{Alice measures } |1\rangle\Big] = \frac{1}{2}.$$

Proof. Since Alice is measuring in the computational basis, she will obtain either $|0\rangle$ or $|1\rangle$ by Postulate 2.12. Moreover, by the Born rule,

$$\Pr\Big[\text{Alice measures } |0\rangle\Big] = \langle\Phi^+|(|0\rangle\langle 0| \otimes I_2)|\Phi^+\rangle.$$

You calculated this in Problem 2.2. For completeness, though, here's the answer:

$$\begin{aligned}
\Pr\Big[\text{Alice measures } |0\rangle\Big] &= \langle\Phi^+|(|0\rangle\langle 0| \otimes I_2)|\Phi^+\rangle \\
&= \left[\frac{1}{\sqrt{2}}(\langle 0|\langle 0| + \langle 1|\langle 1|)\right](|0\rangle\langle 0| \otimes I_2)\left[\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)\right] \\
&= \frac{1}{2}\left[\underbrace{\langle 0|0\rangle}_{=1}\langle 0| \otimes \langle 0|I_2 + \underbrace{\langle 1|0\rangle}_{=0}\langle 0| \otimes \langle 1|I_2\right]\Big[|0\rangle|0\rangle + |1\rangle|1\rangle\Big] \\
&= \frac{1}{2}\Big[\langle 0| \otimes \langle 0|\Big]\Big[|0\rangle|0\rangle + |1\rangle|1\rangle\Big] \\
&= \frac{1}{2}\left[\underbrace{\langle 0|0\rangle\langle 0|0\rangle}_{=1} + \underbrace{\langle 0|1\rangle\langle 0|1\rangle}_{=0}\right] \\
&= \frac{1}{2}.
\end{aligned}$$

A similar calculation establishes that $\Pr[\text{Alice measures } |1\rangle] = 1/2$.[18] ■

[18] Alternatively, by the law of total probability (i.e., the rule that all probabilities sum to one), $\Pr[\text{Alice measures } |1\rangle] = 1 - \Pr[\text{Alice measures } |0\rangle] = 1 - 1/2 = 1/2$.

Exercise 3.1. Given Claim 3.1—in particular that Alice will measure her qubit in either the state $|0\rangle$ or $|1\rangle$—argue that

- if Alice measures $|0\rangle$, then the joint state $|\Phi^+\rangle$ collapses to $|0\rangle|0\rangle$,
- if Alice measures $|1\rangle$, then the joint state $|\Phi^+\rangle$ collapses to $|1\rangle|1\rangle$.

Thus, the possible states of the composite system after Alice measures are

$$\begin{aligned} |0\rangle|0\rangle \quad &\text{with probability} \quad \frac{1}{2} \\ |1\rangle|1\rangle \quad &\text{with probability} \quad \frac{1}{2}. \end{aligned}$$

Consequently, *if* Alice measures $|0\rangle$, then she knowns with certainty that Bob, whenever he chooses to measure his side of the system, will see his qubit in state $|0\rangle$ as well. This implies that at the instant Alice measures, there becomes a definite fact of the matter of what state Bob has (either $|0\rangle$ or $|1\rangle$), and this is despite the two facts, but actually in no way in contradiction to them, that (1) Bob might be lightyears away (the distance d between Alice and Bob never showed up in this calculation) and (2) that before Alice measured, there was no fact of the matter of what Bob's state was!

To help get at what is so weird about this, it can be helpful to contrast the EPR experiment with a more classical version of the same experiment. To this end, suppose that instead of qubits, Alice and Bob each have a closed briefcase with either a red or blue card inside. Alice and Bob both know that they have the same colored card inside, but neither knows which. Thus, by the Bayesian *principle of indifference*, both would say that when they look inside their case, they will both see red with probability 1/2 and blue with probability 1/2. This is analogous to the situation in EPR, where, after either Alice or Bob measure their qubits, the final state of the two qubits is either $|00\rangle$ with probability 1/2 or $|11\rangle$ with probability 1/2.

Now suppose Alice and Bob are separated some distance d, and then Alice looks in her case and sees a red card. By the setup of the experiment, she can conclude with certainty that Bob also has a red card in his case. This inference, like EPR, is independent of the distance d, but that should not be surprising: the cards that Alice and Bob have are correlated. The difference in the card experiment, though, is that throughout the entire experiment, there was always a *fact* of what card Alice and Bob had in their cases: it was set when the two cases were closed. With the qubits in the EPR experiment, however, only through the act of either Alice or Bob measuring their qubit did there become a definite fact of what the state of

their and the other's qubit was. Thus, in some way, Alice's act of measuring her qubit *reified* Bob's qubit, and this occurred faster than the time it would take for light to go from Alice and Bob.

This is called the *EPR paradox* after physicists Albert Einstein, Boris Podolsky, and Nathan Rosen who described it in their famous 1935 paper *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, available here. Ostensibly, the EPR paradox demonstrates a sort of quantum mechanical non-locality, or, in Einstein's words, "spooky action at a distance".

Exercise 3.2. Discuss with those around you how you feel about this. Do you agree with Einstein that this behavior is "spooky" in that it is apparently at odds with the theory of relativity?

3.2. Bell's Theorem

The EPR paradox hints at a sort of non-locality in quantum mechanics. Ultimately, EPR argue that this is an insuperable problem for quantum mechanics as we have so far presented it. To fix it, they proposed that there must be so-called "hidden variable" that afford a more complete description of the quantum state $|\Phi^+\rangle$ that Alice and Bob share. In particular, there must be a *local* description of the state that Alice has and a local description of the state that Bob has, so that there can be no non-local reification of Bob's state when Alice measures her (or vice versa). This sort of idea says that there must be a fact of the state of Alice's qubit and the state of Bob's qubit before measuring, in the same way that in the card experiment from above, there was a fact of what color card Alice had and what color card Bob had before either looked in their case.

A question that naturally follows this discussion is whether such a local description of the EPR experiment is actually possible. If the answer is no, then we will have to accept the type of non-locality apparent in the EPR paradox as a property of our physical reality.[19]

In 1964, the physicist John Bell published his paper *On the Einstein–Podolsky–Rosen Paradox*, available here. There, he established that under the standard "Copenhagen" interpretation of quantum mechanics (which is the theory of quantum

[19]We note that the exact nature of this non-locality is somewhat philosophical, as it has to do with the *ontology* of the physical world, i.e., what is real and what is not. Of course, that we are teetering on philosophical ideas, as opposed to concrete physical ideas, is not, in my opinion, a good argument against the EPR paradox. Indeed, as the philosopher Daniel Dennett likes to say, "there is no such thing as philosophy-free science, only science whose philosophical baggage is taken on board without examination."

mechanics that we presented in Part II), there is indeed a genuine non-locality in quantum mechanics that is, vitally, experimentally testable. This is called *Bell's theorem*.

Here, we will describe a simplified version of his argument, which these days is called a *Bell inequality violation*. The rough idea is to establish a mathematical inequality of the form $a \geq b$ that all classical systems obey, and then to show that, nevertheless, there are quantum systems for which $a < b$. The relationship to non-locality comes from interpreting how the system violated the inequality.

Definition 3.1. We say the state of a qubit is *up along the θ-axis* iff its state is

$$|\uparrow_\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle.$$

Likewise, we say the state of a qubit is *down along the θ-axis* iff its state is

$$|\downarrow_\theta\rangle = \sin\theta\,|0\rangle - \cos\theta\,|1\rangle.$$

These names derive from a geometric way of thinking about qubit states known as the *Bloch sphere*, which you are encouraged to read about on your own time.

Exercise 3.3. Show that these states form an orthonormal basis of $\mathbb{C}^2$. Conclude that for all $\theta \in [0, 2\pi)$, the spin of a qubit along the θ-axis is a measurable property of a qubit, as one can measure it in the basis $\{|\uparrow_\theta\rangle, |\downarrow_\theta\rangle\}$.

Now, recall from Part I the following definition, example, and fact.

Definition 3.2. Let S be a physical system with measurable properties A, B, and C, and let

$$\begin{aligned} N_S(A, B, C) &= \#\text{ times we see } S \text{ with } A, B, \text{ and } C \\ N_S(A, B, \bar{C}) &= \#\text{ times we see } S \text{ with } A, B, \text{ and NOT } C \\ N_S(A, B) &= \#\text{ times we see } S \text{ with } A \text{ and } B, \\ &\vdots \end{aligned}$$

Example 3.1.

- S is a car, A is "its speed is 42 mph relative to the road", B is "its GPS coordinates are $(45.97639, 7.65861)$", and C is "its color is blue".
- S is a star, A is "its mass is 1.5 times that of the Sun", B is "its luminosity is 1.1 times that of the Sun", and C is "its angular momentum is 0.4 times that of the Sun".

- S is an electron, A is "its spin state is up along the x-axis", B is "its spin state is up along the y-axis", and C is "its spin state is up along the z-axis".

Fact 3.2 (Example of a *Bell Inequality*)**.** *For all systems S with measurable properties A, B, and C,*

$$N_S(A, \bar{B}) + N_S(B, \bar{C}) \geq N_S(A, \bar{C}).$$

This is the inequality that we can violate in quantum mechanics, as we shall now see. Such a violation is an example of a *Bell inequality violation*.

Theorem 3.3 (A Version of Bell's Theorem)**.** *Let S be two qubits, e_A and e_B, in the Bell state $|\Phi^+\rangle$, and consider the measurable properties*

- *$A =$ the state of e_A is up along the 0-axis (a.k.a. the z-axis, a.k.a. $|0\rangle$),*
- *$B =$ the state of e_B is up along the θ-axis,*
- *$C =$ the state of e_B is up along the 2θ-axis.*

Then, for sufficiently small $\theta > 0$,

$$N_S(A, \bar{B}) + N_S(B, \bar{C}) < N_S(A, \bar{C}).$$

You should think of the setup here as exactly the same as in the EPR experiment, where Alice and Bob each have a qubit in hand (e_A and e_B, respectively), and that they are spatially separated. The only difference here is that Alice and Bob are going to measure their qubits in bases other than the computational basis. Let's see what happens when they do this.

Proof of Theorem 3.3. Suppose for contradiction that for all $\theta \in [0, 2\pi)$,

$$N_S(A, \bar{B}) + N_S(B, \bar{C}) \geq N_S(A, \bar{C}).$$

This, of course, is what we would expect classically. We will now make use of the fact that the two electrons are in the Bell state $|\Phi^+\rangle$, which exhibits the following property.

Exercise 3.4. Show that for all $\theta \in [0, 2\pi)$,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|\uparrow_\theta\rangle|\uparrow_\theta\rangle + |\downarrow_\theta\rangle|\downarrow_\theta\rangle\big).$$

Therefore, by a calculation similar to the one in the proof of Claim 3.1,

$$\begin{aligned}\Pr[B] &= \Pr\left[\text{state of } e_B \text{ is } |\uparrow_\theta\rangle\right] \\ &= \langle\Phi^+|(I_2 \otimes |\uparrow_\theta\rangle\langle\uparrow_\theta|)|\Phi^+\rangle \\ &= \frac{1}{2}.\end{aligned}$$

Thus, by the law of total probability (i.e., the rule that all probabilities add to one),

$$\begin{aligned}\Pr[\bar{B}] &= \Pr\left[\text{state of } e_B \text{ is NOT } |\uparrow_\theta\rangle\right] \\ &= 1 - \Pr[B] \\ &= \frac{1}{2}.\end{aligned}$$

Consequently, by the definition of conditional probability and supposing we were to run this experiment M times and collect statistics,

$$\begin{aligned}N_S(A, \bar{B}) &= M \Pr[A, \bar{B}] \\ &= M \Pr[A \mid \bar{B}] \Pr[\bar{B}] \\ &= \frac{M}{2} \Pr[A \mid \bar{B}].\end{aligned}$$

Now, by definition,

$$\begin{aligned}\Pr[A \mid \bar{B}] &= \Pr\left[\text{state of } e_B \text{ is } |0\rangle \text{ given state of } e_B \text{ is } |\downarrow_\theta\rangle = \sin\theta\,|0\rangle - \cos\theta\,|1\rangle\right] \\ &= \sin^2\theta.\end{aligned}$$

Consequently,

$$N_S(A, \bar{B}) = \frac{M}{2}\sin^2\theta.$$

Similar reasoning establishes that

$$N_S(B, \bar{C}) = \frac{M}{2}\sin^2\theta \quad \text{and} \quad N_S(A, \bar{C}) = \frac{M}{2}\sin^2 2\theta.$$

Altogether, then,

$$\begin{aligned}N_S(A, \bar{B}) + N_S(B, \bar{C}) \geq N_S(A, \bar{C}) &\implies \frac{M}{2}\sin^2\theta + \frac{M}{2}\sin^2\theta \geq \frac{M}{2}\sin^2 2\theta \\ &\implies 2\sin^2\theta \geq \sin^2 2\theta.\end{aligned}$$

We have not specified θ, so this should hold for all $\theta \in [0, 2\pi)$. However, if $0 < \theta \ll 1$ so that $\sin^2 \theta \approx \theta^2$, then

$$\begin{aligned} 2\sin^2\theta \geq \sin^2 2\theta &\implies 2\theta^2 \geq 4\theta^2 \\ &\implies 1 \geq 2, \end{aligned}$$

which is a contradiction! Therefore, quantum mechanics *violates* the Bell inequality in Fact 3.2. ■

What is going on here? There are at least two fundamental assumptions that went into the statement of the theorem. One is that a qubit can *simultaneously* have a definite state about two different axes, and the other is that when we measure the state of a qubit, there is only one outcome of the measurement. We will discuss the second point in the next section. For now, though, let's make the innocent-seeming assumption that, indeed, when we measure the state of a quantum system, we always obtain one measurement outcome.

If this is so, then we have to contend with the idea that a qubit (such as the spin of an electron) cannot *simultaneously* have a definite state about two different axes. This entails that, pre-measurement, there can be no fact of the matter of what each individual qubit state is about *any* axis. In other words, pre-measurement, it is impossible to give an accurate, *local* prescription of what the state of Alice and Bob's qubits are about the θ-, 2θ-, etc. axes, because if you could, then the Bell inequality in Fact 3.2 would be satisfied.

Consequently, as was suggested by the EPR paradox, it is genuinely the case that any measurement of Alice's qubit will necessarily and fundamentally change Bob's qubit. Because of this, we say that there are no "local hidden variables" that describe the states of the two qubits. Here, as in the EPR paradox, the word "local" is in reference to the fact that the two qubits in this experiment could be arbitrarily far apart, and that we cannot describe the states of the two qubits individually without contradicting the Bell inequality above. There is, therefore, a deep degree of *non-locality* in quantum mechanics, at least under its standard "Copenhagen" interpretation. That said, it is actually impossible to communicate information superluminally with this non-locality, so the postulates of relativity hold, despite this seeming in tension with them. For more on this, see Nielsen and Chuang's textbook *Quantum Information and Quantum Computation*.

But let's return to that second, innocuous-sounding assumption from before, namely, that in measuring any quantum mechanical system, we only ever obtain a single outcome of the measurement. Of course, experience tells us that this is *obviously* the case: when we measure the location of an electron, for example, we only ever see it "here"; we never see it both "here and there". That would not make sense! Similarly, when we measure the state of a qubit in the computational basis, for example, we only ever see it as $|0\rangle$ or $|1\rangle$; we never see it as both. This is all true, but, interestingly enough, that does not mean that only one measurement outcome was obtained!

To understand this, let us first take seriously the reductionist idea that every physical system is reducible to a finite number of quantum systems. This is essentially just the idea that tables, chairs, you, me, and so forth are but a vast soup of quarks, electrons, and other Standard Model matter put together in some complicated way. Yes, there are interesting things going on in some of these systems (e.g., consciousness), but at the end of the day, all of that is *emergent* from the more fundamental interactions of the Standard Model matter.

Okay, now consider an experiment where there is a qubit e, a "qubit state detector" D (which measures the state of a qubit in the computational basis, say), and a human H who is operating the detector. The reductionist hypothesis above, together with Postulates 2.8 and 2.15 of quantum mechanics, entail that there not only exists a Hilbert space $\mathcal{H}_e$ for the qubit, but also Hilbert spaces $\mathcal{H}_D$ and $\mathcal{H}_H$ for the detector and human, respectively, where

$$\mathcal{H}_D = \bigotimes_{\substack{\text{quantum systems } S \text{ that} \\ \text{comprise the detector}}} \mathcal{H}_S \qquad \text{and} \qquad \mathcal{H}_H = \bigotimes_{\substack{\text{quantum systems } S \text{ that} \\ \text{comprise the human}}} \mathcal{H}_S.$$

Consequently, there are several quantum states that the qubit, detector, and human can be in. For example, the qubit can be $|0\rangle$ or $|1\rangle$, as we have discussed before. Additionally, the detector has at least three physically distinguishable (i.e., orthogonal) states:

$$|\text{ready}\rangle, \quad |\text{qubit is } 0\rangle, \quad \text{and} \quad |\text{qubit is } 1\rangle.$$

These correspond to the detector being in the mode "ready to measure the qubit", "the detector has measured the qubit to be in the state $|0\rangle$ and is reporting it as such", and "the detector has measured the qubit to be in the state $|1\rangle$ and is reporting it

as such". Likewise, the human has at least three physically distinguishable states:

$$|\text{sees "ready"}\rangle, \quad |\text{sees "qubit is 0"}\rangle, \quad \text{and} \quad |\text{see "qubit is 1"}\rangle.$$

These correspond to the human seeing the detector being in mode "ready", "qubit is 0", and "qubit is 1", respectively.

How do these states interface with each other? Well, in the overall, qubit + detector + human composite system, which has Hilbert space $\mathcal{H}_e \otimes \mathcal{H}_D \otimes \mathcal{H}_H$, there are the obvious evolutions:

$$\begin{aligned} |0\rangle|\text{ready}\rangle|\text{sees "ready"}\rangle &\longmapsto |0\rangle|\text{qubit is 0}\rangle|\text{sees "qubit is 0"}\rangle \\ |1\rangle|\text{ready}\rangle|\text{sees "ready"}\rangle &\longmapsto |0\rangle|\text{qubit is 1}\rangle|\text{sees "qubit is 1"}\rangle. \end{aligned}$$

These correspond to the physical experiment of performing a computational basis measurement of a qubit that is in the state $|0\rangle$ or $|1\rangle$, respectively, and the detector and human getting a respective readout of the measurement result. Note, these transformations are necessarily unitary (and hence linear) by the Schrödinger evolution postulate of quantum mechanics (Postulate 2.10).

Now consider the same experiment, but where the initial state of the qubit is the superposition $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \neq 0$. Then, the composite qubit + detector + human system evolution is, by the linearity of the Schrödinger equation,

$$\begin{aligned} &(\alpha|0\rangle + \beta|1\rangle)|\text{ready}\rangle|\text{sees "ready"}\rangle \longmapsto \\ &\qquad \alpha|0\rangle|\text{qubit is 0}\rangle|\text{sees "qubit is 0"}\rangle + \beta|1\rangle|\text{qubit is 1}\rangle|\text{sees "qubit is 1"}\rangle. \end{aligned}$$

Contrary to the collapse postulate of quantum mechanics (Postulate 2.12), there is no state collapse here. Instead, there is simply a "larger", entangled superposition that includes the detector and human registering two different measurement outcomes.

This conclusion is known as the *measurement problem in quantum mechanics*. If you believe what we discussed in Part I, and in particular the conclusion that in a superposition there is no definitive fact of what the state of the system is, then what the measurement problem says is that under unitary evolution, *every* quantum system evolves into that sort of indeterminant state of affairs when it interacts with any other quantum system. This includes ourselves. Based on our everyday experience, however, we know that that cannot be right, because we find ourselves in determined states all the time.

In the textbook "Copenhagen" interpretation, one gets out of this situation by postulating the collapse postulate (Postulate 2.12). However, this tends to lead to a whole new set of questions like, what does it really *mean* to "measure" a quantum system? Interestingly, though, there is an out that doesn't invoke this Niels Bohr-inspired Copenhagen way of thinking at all.

3.4. A Different Way of Thinking About This

Note that under the reductionist hypothesis, one can continue the reasoning from before by including the lab, the earth, and, in fact, the whole universe into the mix as well. Doing this, one will find that for every quantum experiment in which one "measures" a quantum system (i.e., interacts a quantum system with another "larger" quantum systems like a detector), the whole universe will evolve into a big superposition of the possible outcomes of that experiment. In this way, there are "many worlds" created, each with a different outcome, and we become a part of this multiverse, with different versions of ourselves experiencing the different outcomes. Any single version of us, however, only experiences one such outcome, and this, some believe, explains our experience in the laboratory.

This is the germ of Hugh Everett's *many-worlds interpretation of quantum mechanics* (a.k.a. *the Everettian interpretation of quantum mechanics*). Note that it differs from the canonical interpretation in that it predicts that for any quantum experiment, there is generically more than one measurement outcome. In this way, the assumptions going into Bell's theorem (Theorem 3.3) are false, so it should not be surprising that one can violate a Bell inequality in quantum mechanics. Another way to say the same thing is that if your normative assumptions about the world include that the universe is local, then Bell's theorem should increase your credence that the many-worlds interpretation is the right way to think about quantum mechanics.

If you are interested in learning more about this interpretation, as well as other interpretations, I encourage you to read Adam Becker's outstanding book *What is Real?: The Unfinished Quest for the Meaning of Quantum Physics.*

Reading 3
The CHSH Game

In the last lecture, we discussed the EPR paradox and Bell's theorem. These are consequences of the postulates of quantum mechanics and demonstrate just how different quantum mechanics is from classical mechanics.

In this reading, you will see how we can exploit Bell's theorem—and in particular a violation of a Bell inequality called the *CHSH inequality*—to achieve a provable quantum advantage in a type of computational task known as a *non-local game*. Incidentally, the violation of the CHSH inequality was the subject of the 2022 Nobel Prize in Physics, so this stuff is really important in our understanding of physics.

3.1. Non-Local Games

The essential idea of a non-local game is to exploit a Bell inequality violation to achieve some sort of quantum computational advantage. These games are prisoner dilemma-type games in which there are two players, Alice and Bob, and a referee, Charlie, who asks Alice and Bob questions.

What makes the game "non-local" is that once the game starts, Alice and Bob are forbidden from communicating to each other. This could be achieve, for example, by placing each in a signal-impervious room so that no messages can get through, or by placing Alice and Bob so far away from each other that light could not travel between them during the course of the game. That said, Charlie is between Alice and Bob, and Alice and Bob can communicate with Charlie, at least in a controlled way. More on this below.

3.2. The Clauser–Horne–Shimony–Holt (CHSH) Game

We will now specialize to a particular non-local game known as the *CHSH game*, which is named after the physicists John Clauser, Michael Horne, Abner Shimony,

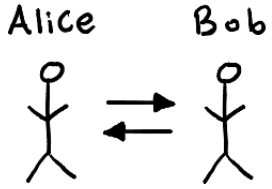
and Richard Holt. The CHSH game is an example of a more general class of games called *XOR games*, which are named after the logical exclusive OR operation $\oplus$ (a.k.a. addition modulo 2), which plays a fundamental role in such games.

Definition 3.3. The *CHSH game* is a non-local game that proceeds in four stages, starting at stage 0.

Stage 0: Alice and Bob can communicate at this stage, and together they develop a *strategy*. A strategy $\mathcal{S}$ is a set of four random variables,

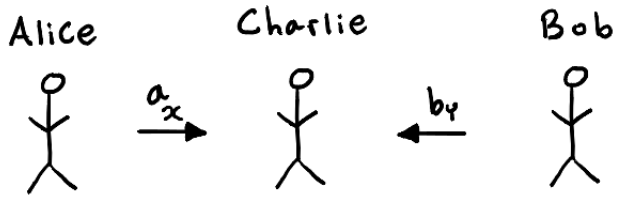
$$\mathcal{S} = \{a_0, a_1, b_0, b_1\},$$

such that all of the variables take values in the set $\{0, 1\}$. Consequently, for each of these random variables, there is a certain probability that it outputs 0 ($\Pr[a_0 = 0]$, $\Pr[a_1 = 0]$, etc.) and a certain probability that it outputs 1 ($\Pr[a_0 = 1]$, $\Pr[a_1 = 1]$, etc.). There are no other output options. Note, here the lower case a corresponds to Alice's "side" of the strategy and the lower case b corresponds to Bob's "side" of the strategy. A good picture for this stage is Alice and Bob talking and strategizing,



Stage 1: Alice and Bob are separated and forbidden from communicating for the remainder of the game. Charlie (the referee) independently generates two uniformly random bits $x, y \in \{0, 1\}$, which together as the 2-bit string $q = xy$ constitutes the *question*. Charlie sends Alice x (the first bit of the question) and sends Bob y (the second bit of the question). Pictorially,

Stage 2: Alice, who receives $x \in \{0, 1\}$ from Charlie, evaluates her random variable a_x and then sends the result back to Charlie. Similarly, Bob, who receives $y \in \{0, 1\}$ from Charlie, evaluates his random variable b_y and then sends the result back to Charlie. Pictorially,



Stage 3: Charlie checks if

$$a_x \oplus b_y = x \wedge y,$$

where $\wedge$ is the logical AND. If so, then Alice and Bob *win*. Otherwise, they *lose*.

That's the CHSH game. In summary, the game is this: if Charlie sends $q = xy \in \{00, 01, 10\}$, then to win, Alice and Bob must answer with the same bit. If, however, the question is $q = xy = 11$, then to win, they must answer with different bits. Due to their inability to communicate during the game, however, it is impossible for Alice and Bob to know with certainty the bit that the other received, so they cannot coordinate a direct response based on the other person's question. Rather, all they can do is strategize at the beginning knowing that they will not be able to communicate later. The question is how well can they do in this situation, and does quantum mechanics somehow let them do better than they could classically.

Before moving on, we will give an example of a strategy that Alice and Bob might employ. This example is a *deterministic strategy*, meaning $\Pr[a_0 = 0]$ is either 0 or 1, and similarly for a_1, b_0, and b_1. In other words, in a deterministic strategy, a_0, a_1, b_0, and b_1 are just bit values, as opposed to random variables in which they could be 0 or 1 with a non-trivial probability.

Example 3.2. Consider the deterministic strategy $\mathcal{S} = \{a_0, a_1, b_0, b_1\}$, where

$$a_0 = a_1 = b_0 = b_1 = 0.$$

Then,

- if $q = xy = 00$, then $x \wedge y = 0$ and $a_0 \oplus b_0 = 0$, so Alice and Bob win;
- if $q = xy = 01$, then $x \wedge y = 0$ and $a_0 \oplus b_1 = 0$, so Alice and Bob win;
- if $q = xy = 10$, then $x \wedge y = 0$ and $a_1 \oplus b_0 = 0$, so Alice and Bob win;
- if $q = xy = 11$, then $x \wedge y = 1$ and $a_1 \oplus b_1 = 0$, so Alice and Bob *lose*.

Thus, with this strategy, Alice and Bob win the CHSH game 75% of the time. As we will see in the next section, this strategy is actually optimal classically, even among non-deterministic classical strategies.

3.3. The Optimal Classical Strategy

To understand the optimal classical strategy, you will first prove that whatever the optimal classical strategy for Alice and Bob is, it necessarily fails some amount of the time. This means that there is no strategy $\mathcal{S}$ for which $\Pr_{\mathcal{S}}[\text{win}] = 1$, where[20]

$$\Pr_{\mathcal{S}}[\text{win}] = \Pr_{x,y\sim\{0,1\}}\left[a_x \oplus b_y = x \wedge y\right]$$

is the probability that Alice and Bob win using the strategy $\mathcal{S}$.

Problem 3.1. To prove that for all strategies $\mathcal{S}$, $\Pr_{\mathcal{S}}[\text{win}] < 1$, let us suppose for contradiction that there exists a strategy $\mathcal{S} = \{a_0, a_1, b_0, b_1\}$ for which $\Pr_{\mathcal{S}}[\text{win}] = 1$.

(a) Argue that this strategy is deterministic. In other words, argue that if $\Pr_{\mathcal{S}}[\text{win}] = 1$, then a_0, a_1, b_0, and b_1 are each either 0 or 1 with probability one.

(b) Argue that these bits must satisfy the following set of equations:

$$\begin{aligned} a_0 \oplus b_0 &= 0, \\ a_0 \oplus b_1 &= 0, \\ a_1 \oplus b_0 &= 0, \\ a_1 \oplus b_1 &= 1. \end{aligned}$$

(c) Show that this is impossible. (*Hint:* What happens when you sum modulo 2 the left and right sides of the above constraints?) Conclude that there is no strategy $\mathcal{S}$ for which $\Pr_{\mathcal{S}}[\text{win}] = 1$, as desired.

Consequently, no matter what strategy Alice and Bob use, they cannot win all the time. In other words, they must lose some amount of the time. To quantify by how much they will lose with the most optimal classical strategy, we perform a "change of variables" so that instead of talking about the bit values 0 and 1, we can talk about the signed values 1 and -1, respectively.

Specifically, for all $x, y \in \{0, 1\}$, let

$$A_x = (-1)^{a_x} \quad \text{and} \quad B_y = (-1)^{b_y}.$$

[20] Here, $x, y \sim \{0, 1\}$ means that x and y are drawn uniformly and independently from the set $\{0, 1\}$. In other words, this is notation that reflects Charlie drawing the two bits of the question uniformly and independently.

As desired, these are random variables that take values in the set $\{-1, 1\}$. Moreover, A_x and B_y have probabilities of being -1 and 1 commensurate with the probabilities that a_x and b_y are 1 and 0, respectively. This change of variables may seem like a pointless thing to do at this stage, however, as we will see shortly, it is this change of variables that ultimately allows us to non-trivially bound the success probability of *every* classical strategy. Before seeing how this is done, though, you should try your hand to see how the winning criterion for a_x and b_y carries over to the variables A_x and B_y.

Problem 3.2. Argue that for all strategies $\mathcal{S}$, Alice and Bob win the CHSH game iff $A_x B_y = (-1)^{x \wedge y}$. Conclude that

$$\Pr_{\mathcal{S}}[\text{win}] = \Pr_{x,y \sim \{0,1\}} \left[A_x B_y = (-1)^{x \wedge y} \right].$$

Now, for the remainder of this section, we will make use of the *conditional* probability that Alice and Bob win, denoted $\Pr_{\mathcal{S}}[\text{win} \mid xy]$. This is the probability that Alice and Bob win *given* that Charlie has asked the particular question $q = xy \in \{0, 1\}^2$. Why do we care about these probabilities? Well, as formalized in Claim 3.5 below, it turns out that to know these *conditional* probabilities is enough to determine the *un*conditional probability that Alice and Bob win. To understand this, let's first establish the following fact about these conditional probabilities.

Claim 3.4. *For all strategies $\mathcal{S}$,*

$$\begin{aligned}
\Pr_{\mathcal{S}}[\mathit{win} \mid q = 00] &= \Pr[A_0 B_0 = 1] \\
\Pr_{\mathcal{S}}[\mathit{win} \mid q = 01] &= \Pr[A_0 B_1 = 1] \\
\Pr_{\mathcal{S}}[\mathit{win} \mid q = 10] &= \Pr[A_1 B_0 = 1] \\
\Pr_{\mathcal{S}}[\mathit{win} \mid q = 11] &= \Pr[A_1 B_1 = -1].
\end{aligned}$$

Proof. By Problem 3.2, Alice and Bob win iff $A_x B_y = (-1)^{x \wedge y}$. Therefore, *given* that the question is $q = xy = 00$, then Alice and Bob win iff $A_0 B_0 = 1$. Consequently, given that the question is $q = 00$, Alice and Bob win with probability

$$\Pr_{\mathcal{S}}[\text{win} \mid q = 00] = \Pr[A_0 B_0 = 1],$$

as desired. A similar argument establishes the other three equations. ■

We can now use these conditional probabilities to derive a very useful expression for the (*un*conditional) probability that Alice and Bob win.

Claim 3.5. *For all strategies $\mathcal{S}$,*

$$\Pr_{\mathcal{S}}[win] = \frac{1}{4} \sum_{x,y \in \{0,1\}} \Pr_{\mathcal{S}}[win \mid q = xy].$$

Proof. To relate the *un*conditional probability of winning $\Pr_{\mathcal{S}}[\text{win}]$ to the *conditional* probabilities of winning $\Pr_{\mathcal{S}}[\text{win} \mid q = xy]$, note that by the law of total probability and Bayes' theorem,

$$\begin{aligned} \Pr_{\mathcal{S}}[\text{win}] &= \sum_{x,y \in \{0,1\}} \Pr_{\mathcal{S}}[\text{win}, q = xy] \\ &= \sum_{x,y \in \{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy] \Pr[q = xy]. \end{aligned}$$

Now, by the definition of the CHSH game, Charlie generates the question q uniformly, so each of the four questions in the set $\{0,1\}^2$ has an equal chance of being asked. Consequently, $\Pr[q = xy] = 1/4$ and so

$$\Pr_{\mathcal{S}}[\text{win}] = \frac{1}{4} \sum_{x,y \in \{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy],$$

as desired. ■

At this point, we just need one more notion from probability theory to prove the optimal classical strategy for the CHSH game.

Definition 3.4. For a given strategy $\mathcal{S}$ and for all $x, y \in \{0,1\}$, let $\mathbb{E}_{\mathcal{S}}[A_x B_y]$ be the *expectation value* of the random variable $A_x B_y$. In particular, for all $x, y \in \{0,1\}$,

$$\mathbb{E}_{\mathcal{S}}[A_x B_y] = \Pr[A_x B_y = 1] - \Pr[A_x B_y = -1].$$

To ensure you are comfortable with this notion, and in particular how it relates to the conditional probabilities discussed above, you should complete the following problem before moving on.

Problem 3.3. Show the following.

(a) If $q = xy \in \{00, 01, 10\}$, then $\mathbb{E}_{\mathcal{S}}[A_x B_y] = 2 \Pr_{\mathcal{S}}[\text{win} \mid q = xy] - 1$.

(b) If $q = xy = 11$, then $\mathbb{E}_{\mathcal{S}}[A_x B_y] = 1 - 2 \Pr_{\mathcal{S}}[\text{win} \mid q = xy]$.

We will now prove the first of two essential claims, both of which have to do with the random variable

$$C = A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1,$$

which is sometimes called the *CHSH quantity*.

Claim 3.6. *For all strategies $\mathcal{S}$, $\mathbb{E}_{\mathcal{S}}[C] = 8\Pr_{\mathcal{S}}[win] - 4$.*

Proof. By the linearity of the expectation value (a.k.a., *the linearity of expectation*),

$$\mathbb{E}_{\mathcal{S}}[C] = \mathbb{E}_{\mathcal{S}}[A_0B_0] + \mathbb{E}_{\mathcal{S}}[A_0B_1] + \mathbb{E}_{\mathcal{S}}[A_1B_0] - \mathbb{E}_{\mathcal{S}}[A_1B_1].$$

Thus, by the result in Problem 3.3,

$$\mathbb{E}_{\mathcal{S}}[C] = 2\left(\sum_{x,y\in\{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy]\right) - 4.$$

But by Claim 3.5,

$$\sum_{x,y\in\{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy] = 4\Pr_{\mathcal{S}}[\text{win}].$$

Put together, then, the above two equations imply that

$$\mathbb{E}_{\mathcal{S}}[C] = 8\Pr_{\mathcal{S}}[\text{win}] - 4,$$

as desired. ■

This result establishes that for all strategies $\mathcal{S}$, a bound on $\mathbb{E}_{\mathcal{S}}[C]$ implies a (potentially strategy-dependent) bound on the probability that Alice and Bob win, $\Pr_{\mathcal{S}}[\text{win}]$. In particular, if there exists a strategy-*independent* bound on $\mathbb{E}_{\mathcal{S}}[C]$, then this implies a strategy-*independent* bound on $\Pr_{\mathcal{S}}[\text{win}]$. Such a bound would act as an *absolute* bound on the probability that Alice and Bob can win, no matter their strategy. This is why the CHSH quantity is so interesting, and it is also why it was essential to perform the change of variables above.

As we will now see, obtaining a strategy-independent bound on $\mathbb{E}_{\mathcal{S}}[C]$, and hence hence on $\Pr_{\mathcal{S}}[\text{win}]$, is actually quite easy.

Claim 3.7 (The CHSH Inequality)**.** *For all strategies $\mathcal{S}$, $|\mathbb{E}_{\mathcal{S}}[C]| \leq 2$.*

Proof. To prove the claim, it suffices to recognize that the CHSH quantity C can be rearranged as follows:

$$\begin{aligned} C &= A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \\ &= B_0(A_0 + A_1) + B_1(A_0 - A_1). \end{aligned}$$

Since if $A_0 = A_1$, then $A_0 + A_1 = \pm 2$ and $A_0 - A_1 = 0$, and if $A_0 \neq A_1$, then $A_0 + A_1 = 0$ and $A_0 - A_1 = \pm 2$, it holds that $C = \pm 2$. Therefore, by the definition

of the expectation value of C and the fact that $|a+b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$ (the so-called *triangle inequality*),

$$\begin{aligned} |\mathbb{E}_{\mathcal{S}}[C]| &= |2\Pr[C=2] - 2\Pr[C=-2]| \\ &\leq 2\Pr[C=2] + 2\Pr[C=-2] \\ &= 2\underbrace{(\Pr[C=2] + \Pr[C=-2])}_{=1} \\ &= 2. \end{aligned}$$

This is the desired result.[21] ■

We are now in a position to prove that no classical strategy can win the CHSH game more than 75% of the time.

Problem 3.4. Use Claims 3.6 and 3.7 to show that $\Pr_{\mathcal{S}}[\text{win}] \leq 3/4$ for all strategies $\mathcal{S}$ for which $\Pr_{\mathcal{S}}[\text{win}] \geq 1/2$, i.e., for all strategies $\mathcal{S}$ that are better than just "flipping a coin". Conclude that no matter what strategy Alice and Bob choose, they cannot win the CHSH game more than 75% of the time.

This proves the upper bound on the winning probability for any classical strategy for the CHSH game. As a corollary, you have also shown that the deterministic strategy we discussed in Example 3.2 is classically optimal. In the next section, you will prove that in fact there are quantum strategies that can do considerably better. The reason, as we shall see, is because quantum mechanics can *violate* the CHSH inequality, which is exactly analogous to the phenomenon we saw with Bell's theorem in the last lecture.

3.4. A Better Quantum Strategy

We begin with the punchline of this reading, namely that there is a quantum strategy that *provably* outperforms every classical strategy in the CHSH game by quite a large margin.

Claim 3.8. *There exists a quantum strategy $\mathcal{S}$ for which*

$$\Pr_{\mathcal{S}}[\textit{win}] = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85.$$

Consequently, using a quantum strategy, Alice and Bob can win the CHSH game approximately 85% of the time.

[21] Another way to show this is to use the fact that for all random variables C, $|\mathbb{E}[C]| \leq \mathbb{E}[|C|]$.

To prove this, let's return to stage 0 in the CHSH game, where Alice and Bob can communicate and strategize. Their quantum strategy will consist of two main parts, both of which are highly quantum. The first part is that Alice and Bob will together generate the Bell state $|\Phi^+\rangle$ and share this between them at stage 0. As was briefly mentioned in the preceding lecture, they cannot use this resource to communicate during the game, so the rules of the game will still be respected. However, as this is now essentially the setup to the EPR experiment, they might be able to exploit the non-locality of quantum mechanics to do something non-classically (e.g., violate the CHSH inequality) at a later stage of the game.

The second part of their strategy details how they will generate the bits to send back to Charlie. These are the random variables a_x and b_y from before. This part of their strategy will first consist of them agreeing on a value of $\theta \in [0, 2\pi)$. (Ultimately, they will choose $\theta = \pi/8$, however keeping θ unspecified shows why $\theta = \pi/8$ is a good choice.) Next, to actually generate the values a_x and b_y, Alice and Bob will measurs their side of the state $|\Phi^+\rangle$ in a basis that depends on the question q and their choice of θ.

Specifically, upon receiving their part of the question $q = xy \in \{0,1\}^2$ from Charlie, Alice and Bob will do the following:

- If $x = 0$, then Alice measures her side of $|\Phi^+\rangle$ in the computational basis ($\{|0\rangle, |1\rangle\}$). She then sends a_0 to Charlie, where
$$a_0 = \begin{cases} 0 & \text{if she measures } |0\rangle \\ 1 & \text{if she measures } |1\rangle. \end{cases}$$
- If $x = 1$, then Alice measures her side of $|\Phi^+\rangle$ in the basis $\{|\uparrow_{2\theta}\rangle, |\downarrow_{2\theta}\rangle\}$. She then sends a_1 to Charlie, where
$$a_1 = \begin{cases} 0 & \text{if she measures } |\uparrow_{2\theta}\rangle \\ 1 & \text{if she measures } |\downarrow_{2\theta}\rangle. \end{cases}$$
- If $y = 0$, then Bob measures his side of $|\Phi^+\rangle$ in the basis $\{|\uparrow_\theta\rangle, |\downarrow_\theta\rangle\}$. He then sends b_0 to Charlie, where
$$b_0 = \begin{cases} 0 & \text{if he measures } |\uparrow_\theta\rangle \\ 1 & \text{if he measures } |\downarrow_\theta\rangle. \end{cases}$$
- If $y = 1$, then Bob measures his side of $|\Phi^+\rangle$ in the basis $\{|\uparrow_{-\theta}\rangle, |\downarrow_{-\theta}\rangle\}$. He then sends b_1 to Charlie, where
$$b_1 = \begin{cases} 0 & \text{if he measures } |\uparrow_{-\theta}\rangle \\ 1 & \text{if he measures } |\downarrow_{-\theta}\rangle. \end{cases}$$

Altogether, $\mathcal{S} = \{a_0, a_1, b_0, b_1\}$ constitutes their quantum strategy. The basic idea here is that if Alice and Bob both receive 1, then they rotate their qubits away from each other so that their measurement bases are 3θ away from each other. That is important in the CHSH game, because Alice and Bob must send Charlie different bits if $q = xy = 11$. If, however, only one or neither receives 1, then their bases are θ away from each other, and this increases the chance that they send back the same bit to Charlie (which they must do to win).

To see that this strategy not only works, but works better than any classical strategy, it suffices to do what we did before and analyze the *conditional* probabilities that Alice and Bob win on each of the four possible questions $q = xy \in \{0,1\}^2$, and then to take the average. In other words, to compute $\Pr_{\mathcal{S}}[\text{win}]$ for this strategy, we will again look at the *conditional* distributions $\Pr_{\mathcal{S}}[\text{win} \mid q = xy]$ and use Claim 3.5, which establishes that

$$\Pr_{\mathcal{S}}[\text{win}] = \frac{1}{4} \sum_{x,y \in \{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy].$$

We note that unlike in the case of the classical strategies, it is sufficient for this quantum strategy to reason at the level of the random variables a_x and b_x, not the variables $A_x = (-1)^{a_x}$ and $B_y = (-1)^{b_x}$. Because of this, it is useful to have an analogue of Claim 3.4 for the conditional probabilities $\Pr_{\mathcal{S}}[\text{win} \mid q = xy]$, but in terms of a_x and b_y as opposed to A_x and B_y.

Claim 3.9. *For all strategies $\mathcal{S}$,*

$$\begin{aligned}
\Pr_{\mathcal{S}}[\textit{win} \mid q = 00] &= \Pr[a_0 = 0, b_0 = 0] + \Pr[a_0 = 1, b_0 = 1], \\
\Pr_{\mathcal{S}}[\textit{win} \mid q = 01] &= \Pr[a_0 = 0, b_1 = 0] + \Pr[a_0 = 1, b_1 = 1], \\
\Pr_{\mathcal{S}}[\textit{win} \mid q = 10] &= \Pr[a_1 = 0, b_0 = 0] + \Pr[a_1 = 1, b_0 = 1], \\
\Pr_{\mathcal{S}}[\textit{win} \mid q = 11] &= \Pr[a_1 = 1, b_1 = 0] + \Pr[a_1 = 0, b_1 = 1].
\end{aligned}$$

Proof. By the definition of the CHSH game, Alice and Bob win iff $a_x \oplus b_y = x \wedge y$. Thus, *given* that the question $q = xy = 00$, then Alice and Bob win iff $a_0 \oplus b_0 = 0$. Consequently, given that the question is $q = 00$, Alice and Bob win with probability

$$\Pr_{\mathcal{S}}[\text{win} \mid q = 00] = \Pr[a_0 \oplus b_0 = 0].$$

Of course, $a_0 \oplus b_0 = 0$ iff $a_0 = b_0 = 0$ or $a_1 = b_1 = 1$. These are mutually exclusive events, so

$$\Pr[a_0 \oplus b_0 = 0] = \Pr[a_0 = 0, b_0 = 0] + \Pr[a_0 = 1, b_0 = 1].$$

Consequently,

$$\Pr_{\mathcal{S}}[\text{win} \mid q = 00] = \Pr[a_0 = 0, b_0 = 0] + \Pr[a_0 = 1, b_0 = 1],$$

as desired. A similar argument establishes the other three equations. ■

What are the values of these probabilities? Well, we can find them by analyzing Alice and Bob's quantum strategy! For example, to find $\Pr_{\mathcal{S}}[\text{win} \mid q = 00]$, note that if $q = xy = 00$, then, by the definition of their quantum strategy, Alice measures her side of $|\Phi^+\rangle$ in the computational basis and sets a_0 to her measurement result, whereas Bob measures his side of $|\Phi^+\rangle$ in the basis $\{|\uparrow_\theta\rangle, |\downarrow_\theta\rangle\}$, and he sets $b_0 = 0$ iff he measures $|\uparrow_\theta\rangle$. In other words,

$$\Pr[a_0 = 0, b_0 = 0] = \langle\Phi^+|\Big(|0\rangle\langle 0| \otimes |\uparrow_\theta\rangle\langle\uparrow_\theta|\Big)|\Phi^+\rangle,$$
$$\Pr[a_0 = 1, b_0 = 1] = \langle\Phi^+|\Big(|1\rangle\langle 1| \otimes |\downarrow_\theta\rangle\langle\downarrow_\theta|\Big)|\Phi^+\rangle.$$

By a calculation similar to the one in the proof of Claim 3.1, it is not difficult to show that both of these probabilities evaluate to $\frac{1}{2}\cos^2\theta$, so

$$\Pr_{\mathcal{S}}[\text{win} \mid q = 00] = \cos^2\theta.$$

You should now try to prove one or more of the remaining three conditional winning probabilities.

Problem 3.5. Show at least one of the following.[22]

(a) $\Pr_{\mathcal{S}}[\text{win} \mid q = 01] = \cos^2\theta$.

(b) $\Pr_{\mathcal{S}}[\text{win} \mid q = 10] = \cos^2\theta$.

(c) $\Pr_{\mathcal{S}}[\text{win} \mid q = 11] = \sin^2 3\theta$.

Consequently, by Claim 3.5,

$$\begin{aligned}\Pr_{\mathcal{S}}[\text{win}] &= \frac{1}{4}\sum_{x,y\in\{0,1\}} \Pr_{\mathcal{S}}[\text{win} \mid q = xy] \\ &= \frac{1}{4}\left(3\cos^2\theta + \sin^2 3\theta\right).\end{aligned}$$

[22] To show (b) and (c), use the trigonometric identities $\cos(-\theta) = \cos(\theta)$, $\sin(-\theta) = -\sin\theta$, $\cos(a+b) = \cos a\cos b - \sin a\sin b$, and $\sin(a+b) = \sin a\cos b + \cos a\sin b$. These imply, for instance, that $\cos\theta = \cos 2\theta\cos\theta + \sin 2\theta\sin\theta$ and $\sin 3\theta = \sin 2\theta\cos\theta + \cos 2\theta\sin\theta$.

Using a bit of calculus, one can show that this quantity is maximized when $\theta = \pi/8$. The remarkable thing is that for this choice of θ,

$$\Pr_{\mathcal{S}}[\text{win}] = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85.$$

Therefore, the above quantum strategy with $\theta = \pi/8$ provably outperforms *all* classical strategies by quite a considerable margin. This establishes Claim 3.8.

But *why* does this quantum strategy work? Well, it's the same reason for the bizarre behavior we saw when discussing Bell's theorem: a Bell inequality violation (and hence the non-locality of quantum mechanics)! In particular, this quantum strategy violates the CHSH inequality (Claim 3.7). To see this, simply plug the above winning probability into the formula of Claim 3.6 to obtain that

$$\begin{aligned}\mathbb{E}_{\mathcal{S}}[C] &\approx 8(0.85) - 4 \\ &= 2.8 \\ &> 2.\end{aligned}$$

Thus, $|\mathbb{E}_{\mathcal{S}}[C]| > 2$, so quantum mechanics violates the CHSH inequality! Incidentally, this inequality violation was shown experimentally in the 1980s by physicists Alain Aspect, John Clauser, and Anton Zeilinger, and for this work they were awarded the 2022 Nobel Prize in Physics.

Also, the winning bound of about 85% is optimal *quantumly*. This follows from a very famous result in quantum information theory known as *Tsirelson's bound*, after the physicist Boris Tsirelson.

Part IV
Grover's Algorithm

Lecture 4

The Circuit Model of Quantum Computation

Discussion 4.1. Discuss with your group what you took away from Part III.

In Part III, we discussed Bell's theorem, one of the most profound consequences of entanglement. We then saw in the associated reading that a version of Bell's theorem can manifest into a sort of "quantum computational advantage" in the sense that there exists a quantum strategy to the CHSH game that provably outperforms all classical strategies.

In this lecture, we will introduce the circuit model of quantum computation. By the end of the lecture, you will know how to formally define a "quantum computer". In the associated reading, you will apply this definition and learn about *Grover's algorithm*, which is an example of a quantum algorithm that provably outperforms all classical algorithms for a computational problem known as *unstructured search*.

4.1. Gate Sets and Universality

In Part II, we saw several important examples of unitary matrices. I repeat some of those examples here, together with their *circuit representations*:

- the 1-qubit T or $\pi/8$ *gate*:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \qquad \text{—}\boxed{T}\text{—}$$

- the 1-qubit H or *Hadamard gate*:

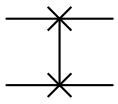
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \text{—}\boxed{H}\text{—}$$

- the 1-qubit S or *phase gate*:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad \text{—}\boxed{S}\text{—}$$

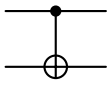
- the 2-qubit SWAP *gate*:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad$$



- and the 2-qubit *controlled*-NOT or CNOT *gate*:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad$$



In the circuit model of quantum computation, unitary matrices like these take the role of the fundamental classical operations like AND, OR, and NOT.

Definition 4.1. A finite set of unitary matrices $\mathcal{G}$ is called a *gate set*, and the elements of $\mathcal{G}$ are called *quantum gates*.

Example 4.1.

- The *Clifford gate set*, $\mathcal{G}_{\text{Clifford}} = \{H, S, \text{CNOT}\}$.
- The *Clifford + T gate set*, $\mathcal{G}_{\text{Clifford}+T} = \{T, H, S, \text{CNOT}\}$.

Importantly, not all gate sets are created equal. Some have a very important property known as *universality*.

Definition 4.2 (Informal)**.** A gate set $\mathcal{G}$ is *universal* iff for all unitary matrices $U \in \text{U}(2)$, one can approximate U to arbitrary precision by a finite product of gates $g_1 g_2 \dots g_\ell$ from $\mathcal{G}$.[23]

Importantly, the Clifford gate set $\mathcal{G}_{\text{Clifford}}$ is not universal, but the Clifford + T gate set is. Also, thanks to a result known as the *Solovay–Kitaev theorem*, all universal gate sets are equivalent to each other, but not just in the sense that they can approximate each other (they can), but also in the more surprising sense that they can approximate each other using a small number of gates in the product.

Exercise 4.1. The Clifford + T gate set is important from both the theoretical and experimental points of view. Now, if $S = T^2$, then there is no reason to include S in the gate set, at least theoretically. I claim, however, that including S is crucial experimentally. Why do you think that might be so?

[23] To properly formalize this statement requires introducing the topological notion of *density* and the linear algebraic notion of *operator distance*. If you are interested in these ideas, check out Nielsen and Chuang's textbook *Quantum Information and Quantum Computation*.

4.2. Quantum Circuits

Given a gate set, we can define quantum circuits over it.

Definition 4.3.

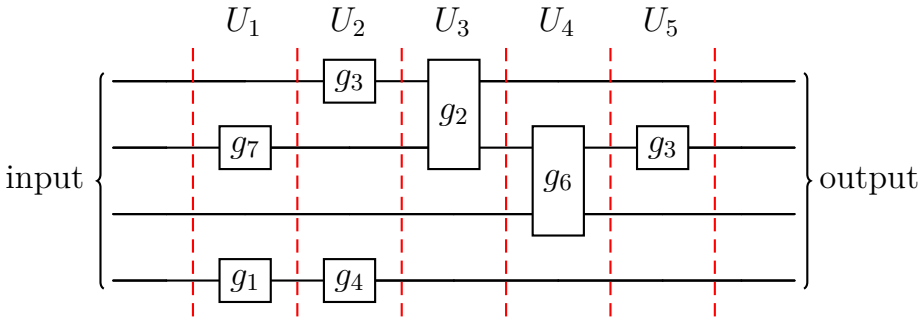
- An *n-qubit quantum circuit Q over a gate set $\mathcal{G}$* is an operator in $\mathrm{U}(2^n)$ that admits the matrix product decomposition

$$Q = U_d U_{d-1} \cdots U_1,$$

where each $U_j \in \mathrm{U}(2^n)$ admits the tensor product decomposition

$$U_j = \bigotimes_{k=1}^{m_j} g_k, \qquad g_k \in \mathcal{G} \cup \{I_2\},$$

where $m_j \leq n$ (as U_j is an n-qubit unitary) and I_2 is the 2×2 identity matrix. Pictorially, every quantum circuit can be represented as a directed acyclic graph, where the directedness is left to right, e.g.,



This representation also explicates the tensor product decomposition of the individual layers U_j in terms of the gates in $\mathcal{G}$. For example:

$$U_2 = g_3 \otimes I_2 \otimes I_2 \otimes g_4, \quad U_4 = I_2 \otimes g_6 \otimes I_2, \quad \text{and} \quad U_5 = I_2 \otimes g_3 \otimes I_2 \otimes I_2,$$

where the identity I_2 is represented in the diagram by a solid black line.

- Above, d denotes the *depth of Q* (the number of "layers" of Q), and the number of non-identity gates that comprise Q is the *size of Q*.
- On input $x \in \{0,1\}^n$, the *output of Q* is the quantum state

$$Q(x) = Q|x\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle.$$

- On input $x \in \{0,1\}^n$, the *probability that Q outputs $y \in \{0,1\}^n$*, denoted $\Pr[Q(x) = |y\rangle]$, is the probability that a computational basis measurement of $Q|x\rangle$ is $|y\rangle$. In particular, by the Born rule,

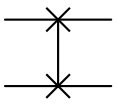
$$\begin{aligned}\Pr\left[Q(x) = |y\rangle\right] &= \langle x|Q^\dagger(|y\rangle\langle y|)Q|x\rangle \\ &= (\langle x|Q^\dagger|y\rangle)(\langle y|Q|x\rangle) \\ &= (\langle y|Q|x\rangle)^*(\langle y|Q|x\rangle) \\ &= |\langle y|Q|x\rangle|^2.\end{aligned}$$

- We say Q *computes* $f : \{0,1\}^n \to \{0,1\}^n$ iff for all $x \in \{0,1\}^n$,

$$\Pr\left[Q(x) = |f(x)\rangle\right] \geq \frac{2}{3}.$$

Let's see a concrete example.

Example 4.2. Let $Q = \text{SWAP}$. This is a 2-qubit quantum circuit over $\mathcal{G} = \{\text{SWAP}\}$:



Though primitive, this is a valid quantum circuit whose size and depth are both 1. This circuit computes the 2-bit permutation function $\text{PERM} : x_1x_2 \mapsto x_2x_1$. This can be seen by evaluating the effect of Q on the computational basis states (which is tantamount to a *truth table* for the unitary operation SWAP):

$$\begin{aligned}Q(00) &= \text{SWAP}|0\rangle|0\rangle = |0\rangle|0\rangle \\ Q(01) &= \text{SWAP}|0\rangle|1\rangle = |1\rangle|0\rangle \\ Q(10) &= \text{SWAP}|1\rangle|0\rangle = |0\rangle|1\rangle \\ Q(11) &= \text{SWAP}|1\rangle|1\rangle = |1\rangle|1\rangle.\end{aligned}$$

Therefore,

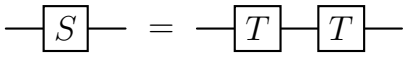
$$Q(x_1x_2) = |x_2\rangle|x_1\rangle = |\text{PERM}(x_1x_2)\rangle.$$

Consequently, on input x_1x_2, Q outputs x_2x_1 with probability one. In this case, we say that Q computes PERM *exactly*.

Now it's your turn. Try one or more of the following problems.

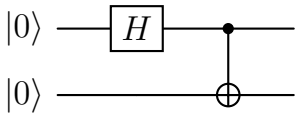
Exercise 4.2.

(1) Prove the circuit identity:

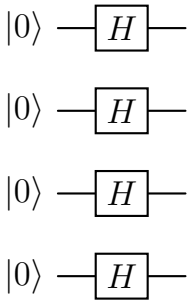


What does this mean in plain matrix multiplication language?

(2) Quantum circuits can do more than just compute functions. In particular, they can be used to generate certain quantum states from computational states, which can then be used for quantum information tasks (e.g., quantum protocols such as *superdense coding* or *quantum teleportation*). As a particular instance of this, show that the following quantum circuit generates the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$:



(3) Argue that the following circuit is a 4-bit random number generator:



4.3. Circuit Families and Uniformity

As we discussed in Part I, in computation we are ultimately interested in functions $f : \{0,1\}^* \to \{0,1\}^*$. In particular, we are interested in functions where the input size is *not fixed*. For example, we care about the function PRIME : $\{0,1\}^* \to \{0,1\}^*$, which on *any* input x—no matter how large—outputs 1 if x encodes a prime and 0 otherwise. To this end, we want a way for a circuit to compute a function whose input size can vary.

Definition 4.4.

- A *quantum circuit family* Q *over a gate set* $\mathcal{G}$ is a pair $(Q, \mathcal{G})$, where $Q = \{Q_n : n \in \mathbb{N}\}$ is a collection of n-qubit quantum circuits $\mathcal{G}$ (one for each $n \in \mathbb{N}$).
- On input $x \in \{0,1\}^*$, the *output of* Q is the state $Q(x) = Q_{|x|}|x\rangle$. Therefore, on input $x \in \{0,1\}^*$, the probability that Q outputs $y \in \{0,1\}^*$ is the same as in Definition 4.3, namely

$$\Pr\left[Q(x) = |y\rangle\right] = |\langle y|Q_{|x|}|x\rangle|^2.$$

  Here, $|x|$ is the length of the string x, i.e., the number of bits that comprise x.
- We say Q *computes* $f : \{0,1\}^* \to \{0,1\}^*$ iff for all $x \in \{0,1\}^*$,

$$\Pr\left[Q(x) = |f(x)\rangle\right] \geq \frac{2}{3}.$$

Interestingly, quantum circuit families (as well as classical circuit families) can compute "hard" functions.

Fact 4.1. *For all universal gate sets* $\mathcal{G}$*, there exists a quantum circuit family over* $\mathcal{G}$ *that computes an uncomputable function.*[24]

This implies that quantum circuit families on their own are too powerful to be a good model of computation. To reduce their power to a more reasonable level, we will impose what is known as a "uniformity condition" on the circuit family. The most basic type of uniformity condition enforces that in a quantum circuit family $Q = \{Q_n : n \in \mathbb{N}\}$, the map $n \mapsto C_n$ is computable. This implies that there is a Python program M such that for all $n \in \mathbb{N}$, $M(n)$ outputs a description of the circuit Q_n. Interestingly, by imposing this condition, uniform circuit families exactly characterize the set of computable functions.

Fact 4.2. *$f : \{0,1\}^* \to \{0,1\}^*$ is computable iff there exists a quantum circuit family $Q = \{Q_n : n \in \mathbb{N}\}$ over a universal gate set $\mathcal{G}$ such that:*

(i) Q computes f,

(ii) the map $n \mapsto C_n$ is computable, i.e., the family Q is uniform.

Because of this, uniform circuit families constitute a reasonable model of computation because it agrees with the Church–Turing–Deutsch thesis. Ultimately, this means that we can use uniform families of quantum circuits as a definition of a "quantum computer". This is what we will do in the next section.

[24] The basic idea is that you can encode a difficult (even uncomputable) function into the map $n \mapsto Q_n$. If you are interested in this idea, check out the complexity class P/poly.

Definition 4.5.

- A *quantum computer* is a pair $(Q, \mathcal{G})$, where Q is a uniform family of quantum circuits over a gate set $\mathcal{G}$.
- We say $(Q, \mathcal{G})$ is *efficient* (a.k.a. *polynomial time*) iff every $Q_n \in Q$ is a polynomial size quantum circuit and the uniformity map $n \mapsto Q_n$ is computable in polynomial time by a Python program.[25]
- On input $x \in \{0,1\}^*$, the *output of* $(Q, \mathcal{G})$ is the quantum state
$$Q(x) = Q_{|x|}(x).$$
- We say $(Q, \mathcal{G})$ *computes* $f : \{0,1\}^* \to \{0,1\}^*$ iff for all $x \in \{0,1\}^*$,
$$\Pr\left[Q(x) = |f(x)\rangle\right] \geq \frac{2}{3}.$$

Importantly, quantum computers cannot compute uncomputable functions.

Fact 4.3 (Corollary of Fact 4.2)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is computable (in the sense of the Church–Turing thesis, Thesis 1.4) iff it is computable by a quantum computer.*

Moreover, *efficient* or *polynomial time* quantum computers can compute anything that efficient classical computers can.

Fact 4.4. *If $f : \{0,1\}^* \to \{0,1\}^*$ is computable by an efficient classical computer, then f is computable by an efficient quantum computer.*

However, it is expected that efficient quantum computers can compute functions that no efficient classical computer can (recall Conjecture 1.7).

Conjecture 4.5. *There exists $f : \{0,1\}^* \to \{0,1\}^*$ computable by an efficient quantum computer but not computable by any efficient classical computer.*

In computational complexity theory, this conjecture is summed up in a single line: $\mathsf{BPP} \neq \mathsf{BQP}$. Of course, to fully understand what this means requires introducing some complexity theory notions, which we do not have time for. That said, if you are interested in this beautiful theory, then I encourage you to check out Arora and Barak's outstanding textbook *Computational Complexity: A Modern Approach*.

[25] This means that given n, one can *efficiently* describe the circuit Q_n. This stronger uniformity condition is called P*-unifomity*.

Reading 4
Grover's Algorithm

In the previous lecture, we discussed universal gate sets (and in particular the Clifford + T gate set) as well as the circuit model of quantum computation. At the end of the day, we formally defined what a quantum computer is, and we stated without proof that quantum computers cannot compute more functions than classical computers. This leaves open the possibility, however, that perhaps there are functions that a quantum computer can compute *faster* than any classical computer. Given the stuff we saw with the CHSH game in Part III, this is actually a pretty reasonable intuition.

In this final reading, you will be guided through a proof that, in fact, there is a function (or more properly, a computational task) that a quantum computer can do provably faster than any classical computer. The exact task is called *the unstructured search problem*, and the quantum algorithm that solves it faster than any classical algorithm is called *Grover's algorithm*, which is named after its founder, physicist Lov Grover.

4.1. Oracles and the Query Complexity Paradigm

To formally understand the unstructured search problem requires a quick discussion about *oracles*, which are essentially algorithmic subroutines that do not hinder the complexity of the larger algorithm of which they are a part.

Definition 4.6. Let $f : \{0,1\}^* \to \{0,1\}$ be a (not necessarily computable!) function. We call a (classical or quantum) operation $\mathcal{O}_f$ that computes f an *oracle for* f. Quantumly, $\mathcal{O}_f$ is a family of quantum circuits that acts on the computational

basis states in the following way:[26]

$$\mathcal{O}_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle.$$

Notice, in this definition we have not specified how difficult it is to compute f. This is on purpose, because it may, in fact, be very difficult (or impossible!) to compute f. This is the paradigm of *query complexity*, in which we assume we have some black box function (the oracle), and we do not care at all about how difficult it is to implement the black box. Instead, what we care about is minimizing the number of calls to the black box $\mathcal{O}_f$. As we will see with Grover's algorithm, quantum computers require provably fewer queries to the oracle than any classical computer.

4.2. The Unstructured Search Problem

Before we discuss Grover's algorithm, we need to introduce the computational problem that Grover's algorithm solves.

The Unstructured Search Problem

Input: A function $f : \{0,1\}^n \to \{0,1\}$ as an oracle such that

$$\begin{cases} f(x) = 1 & \text{if } x = x^\star \in \{0,1\}^n \\ f(x) = 0 & \text{otherwise.} \end{cases}$$

Output: $x^\star$ (the "needle in the haystack") by querying f.

Problem 4.1. Let $N = 2^n$. Argue that, on the average, every classical probabilistic algorithm that solves the unstructured search problem by querying f must make at least $N/2$ queries. In other words, argue that to find x^* by merely asking questions of the form "What is $f(x)$?" requires, on the average, $N/2$ such questions.

In the next section, we will see if we can do better quantumly.

[26] Typically, one defines a quantum oracle $\mathcal{O}_f$ as the map $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$. This is arguably more natural from a computational point of view, however, it turns out to be equivalent to the oracle definition we have given (which is formally known as a *phase oracle*). See Nielsen and Chuang's discussion of Grover's algorithm for more on this.

4.3. Grover's Algorithm

To solve unstructured search on a quantum computer, first recall the quantum oracle we have for f:

$$\mathcal{O}_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle.$$

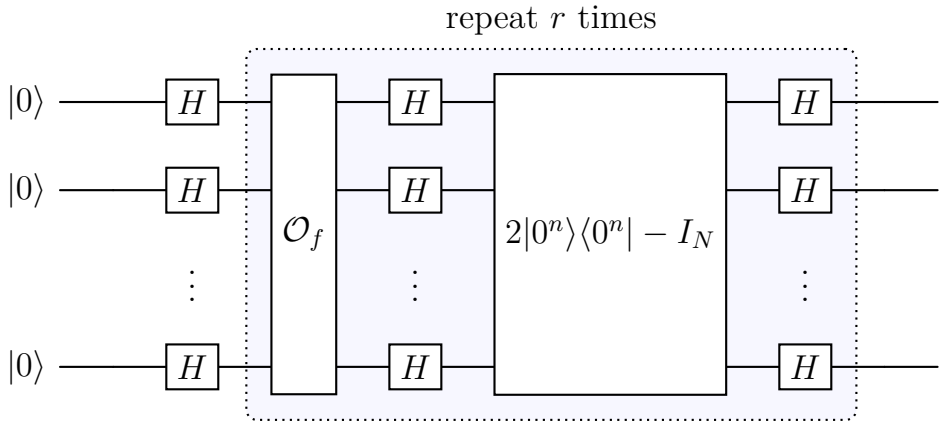
This is the black-box that we will ask questions to. In particular, we are interested in the number of questions of the form "What is $\mathcal{O}_f|x\rangle$?" that we need to ask to determine $x^\star$. We will see that this number is considerably smaller than the number of questions we have to ask in the classical case (Problem 4.1).

We are now ready to study Grover's algorithm.

Grover's Algorithm:

1. Prepare n qubits in the state $|0^n\rangle$.
2. Apply $H^{\otimes n}$ (the n-fold tensor product $H \otimes H \otimes \cdots \otimes H$).
3. Perform the following *Grover iteration* r times:
   (i) apply $\mathcal{O}_f$,
   (ii) apply $H^{\otimes n}$,
   (iii) apply the *Grover diffusion operator* $2|0^n\rangle\langle 0^n| - I_N$,[27]
   (iv) apply $H^{\otimes n}$.
4. Measure all n qubits in the computational basis.

As a circuit, Grover's algorithm is simply:



[27] Recall that $|0^n\rangle\langle 0^n|$ is the *outer product* of $|0^n\rangle$ and $\langle 0^n|$, which is the matrix multiplication of the column vector $|0^n\rangle$ with the row vector $\langle 0^n|$, and thus results in a $2^n \times 2^n$ (unitary) matrix.

In this algorithm, a single Grover iteration (step 3) corresponds to applying what is sometimes called the *Grover operator*,

$$\begin{aligned} G &= H^{\otimes n}(2|0^n\rangle\langle 0^n| - I_N)H^{\otimes n}\mathcal{O}_f \\ &= (2|\Phi\rangle\langle\Phi| - I_N)\mathcal{O}_f, \end{aligned}$$

where, by the result in question (c) of Problem 2.4,

$$\begin{aligned} |\Phi\rangle &= H^{\otimes n}|0^n\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle. \end{aligned}$$

Moreover, the number r parametrizes the number of times we call the oracle $\mathcal{O}_f$ (i.e., the number of questions "What is $\mathcal{O}_f|x\rangle$?"). Remarkably, r is considerably smaller in the quantum case than the classical value of $r = N/2$ (Problem 4.1).

Theorem 4.6. *Using an efficient quantum computer (namely, that specified by Grover's algorithm), it is possible to solve the unstructured search problem with probability* $1 - O(2^{-n})$ *using only* $r = O(\sqrt{N})$ *queries to* f*. This is quadratically fewer than the classical lower bound of* $N/2$ *queries (Problem 4.1).*

We prove this in the next section.

4.4. Correctness of Grover's Algorithm

To prove that Grover's algorithm does what it says, we will begin by building some geometric intuition behind the algorithm, which will assist in its analysis.

Problem 4.2.

(a) Let $|\psi_i\rangle$ be the state in Grover's algorithm at step i. Find $|\psi_1\rangle$ and $|\psi_2\rangle$. (*Hint:* Recall question (c) in Problem 2.4.)

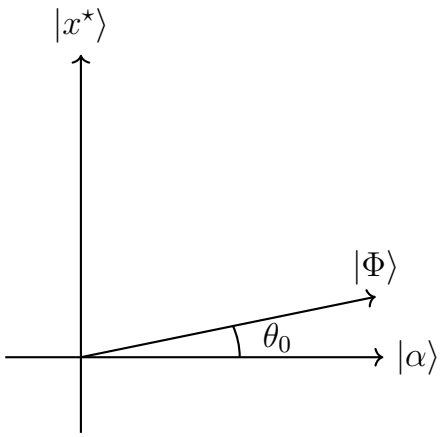
(b) If

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{x\in\{0,1\}^n \\ x\neq x^\star}} |x\rangle,$$

prove that

$$|\Phi\rangle = \sqrt{\frac{N-1}{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|x^\star\rangle.$$

Consequently, $|\Phi\rangle$ is a vector in the two-dimensional subspace of $\mathbb{C}^{2^n}$ that is spanned by $|\alpha\rangle$ and $|x^\star\rangle$. Thus, we can think of $|\Phi\rangle$ as a two-dimensional vector that mostly points in the direction of $|\alpha\rangle$:



Here, $\theta_0 \in [0, 2\pi)$ is such that

$$\cos\theta_0 = \sqrt{\frac{N-1}{N}}$$
$$\sin\theta_0 = \frac{1}{\sqrt{N}}.$$

Thus, using the formula you derived in question (b) of Problem 4.2, it holds that

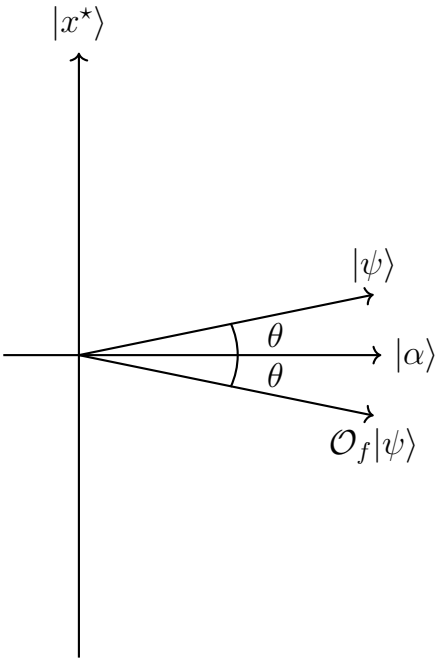
$$|\Phi\rangle = \cos\theta_0|\alpha\rangle + \sin\theta_0|x^\star\rangle.$$

You will now analyze what happens geometrically in step 3 of Grover's algorithm. From this, we will be able to deduce the ideal number of iterations r needed to find $|x^\star\rangle$ with high probability. We will start by understanding how the oracle $\mathcal{O}_f$ acts on the two-dimensional representation derived above.

Problem 4.3. Let $\theta \in [0, 2\pi)$. If $|\psi\rangle = \cos\theta|\alpha\rangle + \sin\theta|x^\star\rangle$, show that

$$\mathcal{O}_f|\psi\rangle = \cos\theta|\alpha\rangle - \sin\theta|x^\star\rangle.$$

Geometrically, you are being asked to show that the oracle $\mathcal{O}_f$ rotates $|\psi\rangle$ through the $|\alpha\rangle$ axis by an angle of 2θ, as in the picture below:



You will now prove one more geometric fact, but this time about the Grover operator G.

Problem 4.4. Let $G = (2|\Phi\rangle\langle\Phi| - I_N)\mathcal{O}_f$ be the Grover operator. Show that

$$\begin{aligned} G|x^\star\rangle &= \cos\omega|x^\star\rangle - \sin\omega|\alpha\rangle \\ G|\alpha\rangle &= \sin\omega|x^\star\rangle + \cos\omega|\alpha\rangle, \end{aligned}$$

where

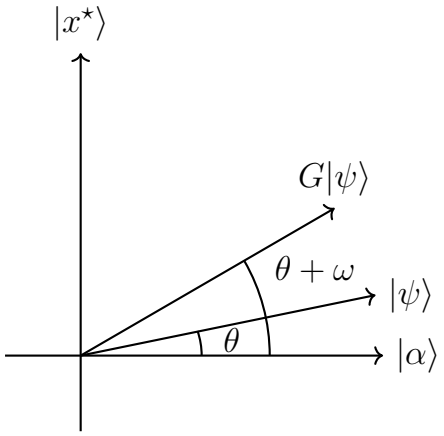
$$\sin\omega = \frac{2\sqrt{N-1}}{N} \quad \text{and} \quad \cos\omega = \sqrt{1-\sin^2\theta} = 1 - \frac{2}{N}.$$

(The geometric interpretation of this is shown in the next corollary.)

Corollary 4.7. *If* $|\psi\rangle = \cos\theta|\alpha\rangle + \sin\theta|x^\star\rangle$, *then*

$$G|\psi\rangle = \cos(\theta+\omega)|\alpha\rangle + \sin(\theta+\omega)|x^\star\rangle$$

Pictorially,



Proof. This follows from Problem 4.4 and elementary trigonometry:

$$\begin{aligned} G|\psi\rangle &= G(\cos\theta|\alpha\rangle + \sin\theta|x^\star\rangle) \\ &= \cos\theta(G|\alpha\rangle) + \sin\theta(G|x^\star\rangle) \\ &= \cos\theta(\sin\omega|x^\star\rangle + \cos\omega|\alpha\rangle) + \sin\theta(\cos\omega|x^\star\rangle - \sin\omega|\alpha\rangle) \\ &= (\cos\theta\cos\omega - \sin\theta\sin\omega)|\alpha\rangle + (\cos\theta\sin\omega + \sin\theta\cos\omega)|x^\star\rangle \\ &= \cos(\theta+\omega)|\alpha\rangle + \sin(\theta+\omega)|x^\star\rangle. \end{aligned}$$

■

Therefore, the Grover operation rotates a given state closer to the target state $|x^\star\rangle$ by an angle ω. We can use this to our advantage to now find $|x^\star\rangle$ with high probability.

Claim 4.8. *If* $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rceil$,[28] *then the probability that we measure* $G^r|\Phi\rangle$ *to be in state* $|x^\star\rangle$ *is* $1 - O(1/N) = 1 - O(2^{-n})$.

Proof. Since

$$|\Phi\rangle = \cos\theta_0|\alpha\rangle + \sin\theta_0|x^\star\rangle,$$

by the previous corollary

$$G^r|\Phi\rangle = \cos(\theta_0 + r\omega)|\alpha\rangle + \sin(\theta_0 + r\omega)|x^\star\rangle.$$

We want r such that $\cos(\theta_0 + r\omega) = 0$ because then when we measure the state, we will obtain $|x^\star\rangle$. Since

$$\cos(\theta_0 + r\omega) = 0 \quad \text{if} \quad \theta_0 + r\omega = \frac{\pi}{2},$$

[28] Here, $\lfloor x \rceil$ denotes the nearest integer to $x \in \mathbb{R}$.

we choose

$$r = \left\lfloor \frac{\frac{\pi}{2} - \theta_0}{\omega} \right\rfloor.$$

We will now show that this choice of r is $O(\sqrt{N})$. This requires quite a bit of algebra. First, using the Taylor series

$$\arcsin(x) = x + \frac{x^3}{6} + \cdots + \frac{(2n)!}{2^{2n}(n!)^2}\frac{x^{2n+1}}{2n+1} + \cdots,$$

it follow that

$$\begin{aligned}\theta_0 &= \arcsin \frac{1}{\sqrt{N}} \\ &= \frac{1}{\sqrt{N}} + O\left(\frac{1}{N^{3/2}}\right)\end{aligned}$$

and

$$\begin{aligned}\omega &= \arcsin \frac{2\sqrt{N-1}}{N} \\ &= \frac{2\sqrt{N-1}}{N} + O\left(\frac{1}{N^{3/2}}\right) \\ &= \frac{2}{\sqrt{N}} + O\left(\frac{1}{N}\right) \\ &= \frac{2}{\sqrt{N}}\left(1 + O\left(\frac{1}{\sqrt{N}}\right)\right).\end{aligned}$$

Consequently,[29]

$$\begin{aligned}r &= \left\lfloor \frac{\frac{\pi}{2} - \theta_0}{\omega} \right\rfloor \\ &= \left\lfloor \frac{\frac{\pi}{2} - \frac{1}{\sqrt{N}} + O\left(\frac{1}{N^{3/2}}\right)}{\frac{2}{\sqrt{N}}\left(1 + O\left(\frac{1}{\sqrt{N}}\right)\right)} \right\rfloor \\ &= \left\lfloor \frac{\frac{\pi}{2}\sqrt{N} - 1 + O\left(\frac{1}{\sqrt{N}}\right)}{2\left(1 + O\left(\frac{1}{\sqrt{N}}\right)\right)} \right\rfloor \\ &= \left\lfloor \frac{\pi\sqrt{N}}{4} - \frac{1}{2} + O\left(\frac{1}{\sqrt{N}}\right) \right\rfloor\end{aligned}$$

[29]Here, we use the fact that if $|x| < 1$, then $\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots$.

Therefore, with $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rceil$,[30]

$$\begin{aligned}
\Pr\left[\text{measure } G^r|\Phi\rangle \text{ in state } |x^\star\rangle\right] &= \sin^2(\theta_0 + r\omega) \\
&= \sin^2\left(\underbrace{\frac{1}{\sqrt{N}}}_{\theta_0} + \underbrace{\left(\frac{\pi}{4}\sqrt{N}\right)}_{r}\underbrace{\frac{2}{\sqrt{N}}}_{\omega} + \underbrace{O\left(\frac{1}{\sqrt{N}}\right)}_{\text{other terms}}\right) \\
&= \sin^2\left(\frac{\pi}{2} + O\left(\frac{1}{\sqrt{N}}\right)\right) \\
&= \cos^2\left(O\left(\frac{1}{\sqrt{N}}\right)\right) \\
&= \left(1 - O\left(\frac{1}{N}\right)\right)^2 \\
&= 1 - O\left(\frac{1}{N}\right).
\end{aligned}$$

■

Altogether, then, we have proven Theorem 4.6, as desired. Therefore, Grover's algorithm shows that quantum computers can provably outperform classical computers for the unstructured search problem.

It is natural to wonder if there is any quantum algorithm that could outperform Grover's algorithm. It turns out, however, that this is false.

Fact 4.9. *Any quantum algorithm that solves the unstructured search problem with probability at least $1/2 + \delta$, for any $\delta > 0$, must make at least $c\sqrt{N}$ queries to f, for some constant $c > 0$.*

Therefore, Grover's algorithm is the *optimal* quantum algorithm for the unstructured search problem.

[30] Here, we use the fact that $\sin\left(\frac{\pi}{2} + x\right) = \cos x$ and that $\cos x = 1 - O(x^2)$.