

Early days with quantum tasks

Alex May^a

^a*The University of British Columbia*

E-mail: alexmay28@gmail.com

ABSTRACT: I relate my experiences doing research as a second and third year undergrad. The story is told at both a technical and personal level, drawing on my personal recollections and journal, emails from that time, and records I keep in my research notebooks.

Contents

1	Introduction	1
2	Second year - Quantum tasks	1
2.1	May, June and Quantum mechanics	1
2.1.1	Stern-Gerlach experiments	2
2.1.2	The quantum formalism	7
2.1.3	Problems on quantum mechanics	9
2.1.4	Back to the story...	10
2.2	July, August and Quantum Tasks	11
2.3	Moving upward to three diamonds	18
3	Third year - Keeping at it	24
4	After the proof and some reflections	24
5	Additional problems	27

1 Introduction

I'm anticipating that many of you, given that you come to physics circle, are interested in pursuing an undergraduate degree in physics, or maybe another science. During your undergraduate degrees you will most likely take part in some kind of research, and this will be even more true if you go on to graduate school. Working on my own research project was probably the most exciting and rewarding thing for me about my undergrad, although I don't think I would have guessed that if you'd asked me while I was in high school. I became a graduate student so that I could keep doing research for a few more years.

Given my experiences with research as an undergrad and your almost inevitable future encounter with research, I thought I would use this opportunity to tell you the story behind the research I did as an undergrad. Occasionally I'll pause to give you advice, which will always be things I wish someone had told me when I was in your position, but mainly I will just tell the story, so that you become familiar with what undergrad research looks like.

2 Second year - Quantum tasks

2.1 May, June and Quantum mechanics

I did my undergraduate degree at McGill University, in a joint math and physics program. It was in the summer of my second year of undergrad that I first became involved in research. In my mechanics course I had a TA, Igor Kozlov, whom I went to often to talk to for help.

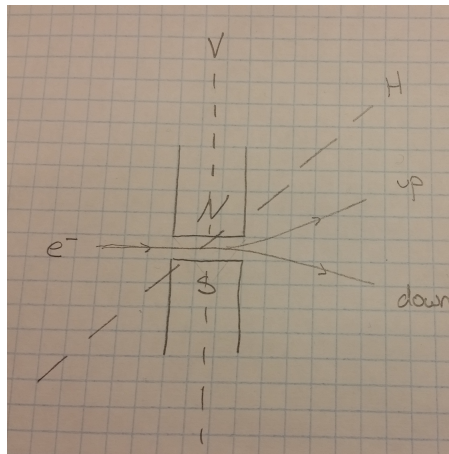
When the summer came around I asked him if he had any suggestions of who I might talk to about a research position for the summer. He connected me with a professor, Keshav Dasgupta, and he agreed to help me learn quantum mechanics that summer.

I got a desk in the Rutherford physics building, which was very exciting to me. Keshav and I would meet every week or so. He set a goal for me for the first month, to be able to explain the Bell inequalities to him. Bell inequalities were somewhere towards the back of the quantum mechanics textbook he'd suggested, so I opened to chapter one and got going. Keshav talked to me about entanglement, and how he felt that was the core of what quantum mechanics meant, and told me there were some other researchers at the university who studied entanglement very closely.

To understand entanglement, I first of all had to understand the basic structure of how quantum mechanics works. While I was working with Keshav I learned this from the book by Townsend [1], who borrowed their explanation largely from Feynman [2]. I'll only give you enough of a description of quantum mechanics as you'll need to follow the research I did later, but you can look at those references for details.

2.1.1 Stern-Gerlach experiments

I want to start getting you at least familiar with the quantum world by considering a series of experiments. The experiments involve sending single electrons through pairs of magnets, like I show below. I'm always going to have my electrons coming in from the left, and traveling horizontally. The electrons can pass through two different arrangements of magnets. Here we have electrons going through a vertical pair of magnets:



And here we have an electron going through a horizontal pairs of magnets:

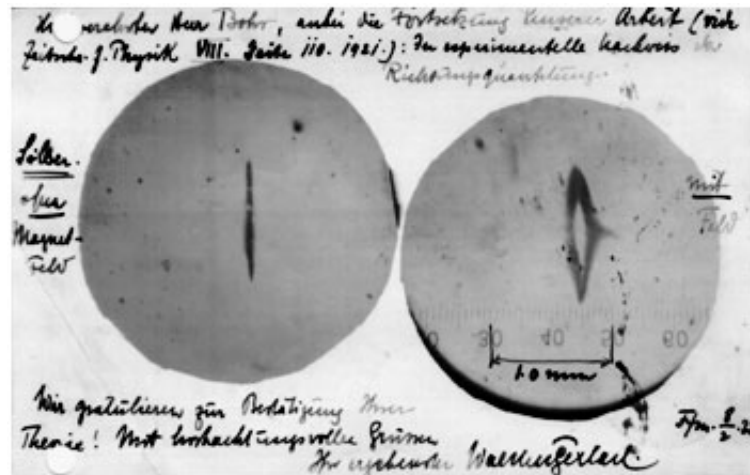
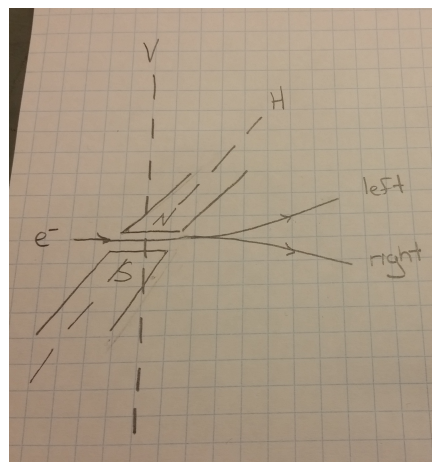
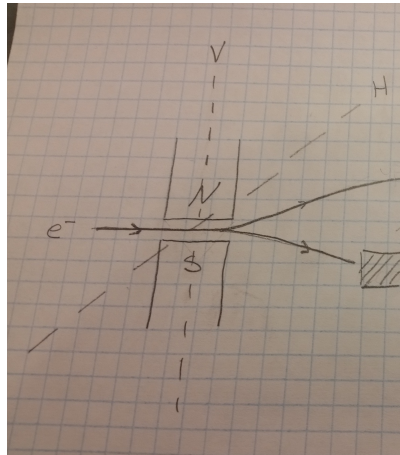


Figure 1. Picture of the photographic plates used in the original Stern-Gerlach experiments. The plate at left is with no magnets in place, the picture at right is with magnets. We see that the electrons are split into two beams, one on the left and one on the right.

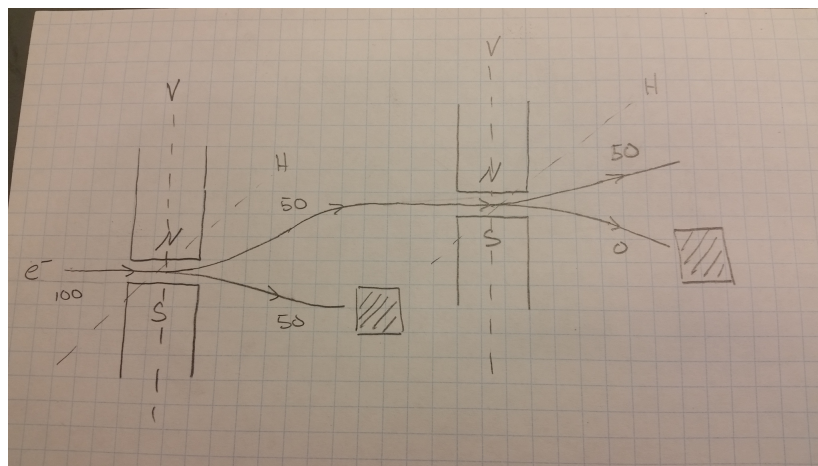


Of course, I could also consider putting my magnets at different angles, sending the electrons in from different directions, and so on, but we focus on this simplified scenario to cut out unnecessary details and make clear the key ideas.

If you pass an electron through a set of vertical magnets you find that some electrons go up and some go down (none go straight). One way we can see this is by putting a photographic plate that changes colour when an electron hits it. You find that there are two splotches of color on the plate after you've sent a number of electrons through, like we show in figure 1. If I block off one of the paths,

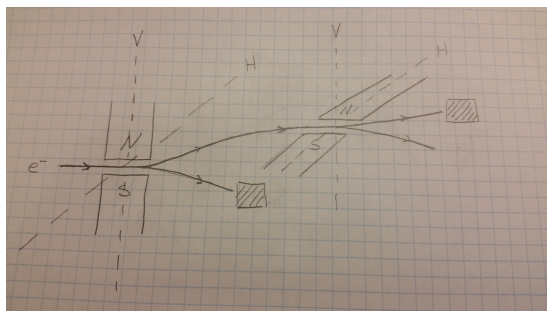


only a fraction of the electrons I shoot into the magnets will come out the other end. We can call the electrons that get through this up-type electrons. If we place a second set of vertical magnets right after the first, we find that every electron that goes into the second set of magnets will always come out. This makes sense - up-type electrons will go up again:

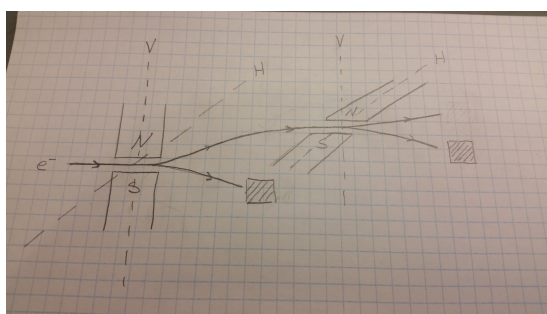


Similarly, electrons that went left when passed through horizontal magnets will go left again when you pass them immediately through a second set of horizontal magnets. For these reasons, it makes sense that we should think of electrons as coming in the four types “up-left”, “up-right”, “down-left”, “down-right”. We will call this the classical model of the electron, and give the different types labels that look like (\uparrow, \leftarrow) , (\uparrow, \rightarrow) , etc. We say that these labels describe the *state* of the electron; they tell me about all the information that the electron carries. At this point you should keep in mind that actually this classical model is going to turn out to be wrong, as I’ll get to shortly.

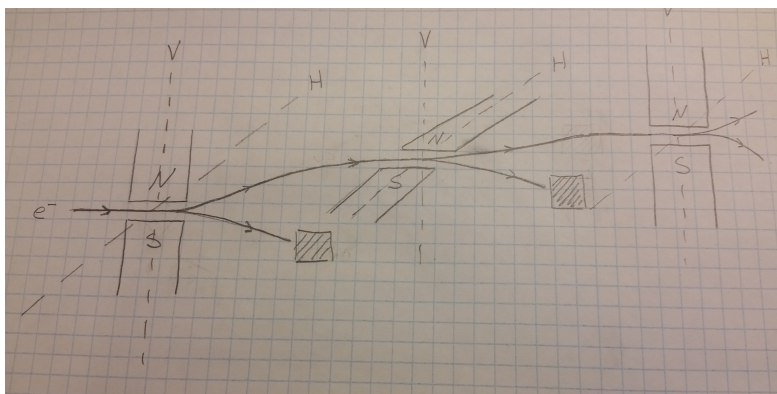
According to our classical model, if I want to pick out the (\uparrow, \rightarrow) type electrons I should set up the magnets:



while if I want to pick out the (\uparrow, \leftarrow) electrons I should set up:

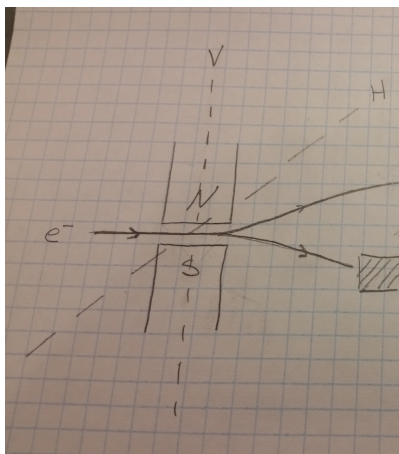


So far so good. But now let's put this model to the test. Apparently my magnets above select out the (\uparrow, \leftarrow) type electrons. What happens if I pass my electrons through another set of vertical magnets? The setup looks like this:

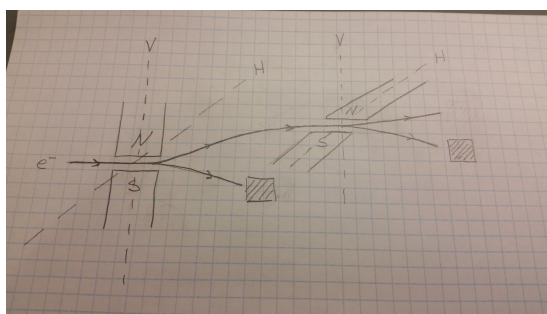


The classical model tells me that all my electrons should go up, but *that is not what happens!* Instead, half my electrons go up and half go down - it's like they've completely forgotten about the first set of magnets that selected only up-type.

There are two questions you can ask here: 1) What is going on? How did the electron forget that it passed a vertical magnet and went up? and 2) How do I change my model to describe this? We are only concerned with the second question, but when you study quantum mechanics more formally you can ponder the first one. What this experiment tells me I should do is only keep track of up-ness OR down-ness, and that it doesn't make sense to keep track of both. So now an electron coming out of



will be described by $|\uparrow\rangle$. Further, electrons that pass through several sets of magnets are only described by the last one they passed through, so



will just be described by $|\leftarrow\rangle$.

The symbol $|\leftarrow\rangle$ also describes the state of the electron - it tells me everything there is to know about what the electron will do when it passes through a set of magnets. This $|\leftarrow\rangle$ is not like the (\uparrow, \leftarrow) description of the electron though, since as we argued that description says too much about the electron. It would say that the electron will definitely go up, when really it has a 50% chance of going up and 50% chance of going down. While we called the (\leftarrow, \uparrow) type description a classical state, we call the $|\leftarrow\rangle$ a quantum state. The above experiments give you some idea of how quantum states behave.

$|\leftarrow\rangle$ has a 50-50 chance of going up or down when passed through a vertical set of magnets, which suggests $|\leftarrow\rangle$ is made from some kind of an equal mixture of up and down types. To represent this we write

$$|\leftarrow\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle). \quad (2.1)$$

The type of “mixture” here, a superposition, isn’t like anything you’ve seen before. It doesn’t for instance mean the left arrow is maybe an up type and maybe a down type but you just don’t know yet. Instead, it means that the electron is really neither, until you measure it, and the measurement pushes it into being one or the other. That will sound a bit mysterious, and indeed it is given only what I’ve said here, but you’ll just have to run with it for now.

2.1.2 The quantum formalism

At this point I'm going to offer up whole the way that quantum mechanics works. From the last section you know what a quantum state is, and you know that certain measurements of a quantum system involve probabilities rather than definite outcomes. We've introduced the idea of superposition a little bit. Hopefully this gives some justification for the rules I'll outline below. For a fuller justification you'll need to look at the references I mentioned earlier [1, 2].

Quantum states: A general quantum state is described by a superposition of basis states:

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \quad (2.2)$$

The basis states correspond to the outcomes of a measurements. For an electron, we can choose the bases states to be either up and down

$$|\uparrow\rangle, |\downarrow\rangle \quad (2.3)$$

or left and right

$$|\leftarrow\rangle, |\rightarrow\rangle \quad (2.4)$$

because it is possible to measure whether the electron is an up-spin or a down-spin, or to measure if it is a left spin or a right spin, but not to do both measurements (i.e. there's no such thing as a up-left electron).

A left state is an equal mixture of up and down states,

$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle \quad (2.5)$$

while a right state is an equal mixture of up and down as well, but with a minus sign,

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle. \quad (2.6)$$

Exercise 1 Express an up state as a superposition of a left and right state. That is, find numbers α and β such that

$$|\uparrow\rangle = \alpha|\leftarrow\rangle + \beta|\rightarrow\rangle. \quad (2.7)$$

Exercise 2 Express a down state as a superposition of a left and right state. That is, find numbers α' and β' such that

$$|\downarrow\rangle = \alpha'|\leftarrow\rangle + \beta'|\rightarrow\rangle. \quad (2.8)$$

Multiple systems and entanglement: The above description of quantum states is for a single system, for example of one electron. How do we describe the state of two electrons?

The state of one electron is written as a superposition of up and down states. The state of two electrons is written as the sum of four possible states: electron 1 is up and electron 2 is up, electron 1 is up and electron 2 is down, etc. So

$$|\Psi\rangle_{12} = \alpha|\uparrow\rangle|\uparrow\rangle + \beta|\uparrow\rangle|\downarrow\rangle + \gamma|\downarrow\rangle|\uparrow\rangle + \delta|\downarrow\rangle|\downarrow\rangle \quad (2.9)$$

If I give you a first electron that is described by

$$|\psi\rangle_1 = x|\uparrow\rangle_1 + y|\downarrow\rangle_1 \quad (2.10)$$

and a second electron described by

$$|\phi\rangle_2 = a|\uparrow\rangle_2 + b|\downarrow\rangle_2 \quad (2.11)$$

Then if I want to described the both of them together I write

$$\begin{aligned} |\psi\rangle_1|\phi\rangle_2 &= (x|\uparrow\rangle_1 + y|\downarrow\rangle_1)(a|\uparrow\rangle_2 + b|\downarrow\rangle_2) \\ &= xa|\uparrow\rangle_1|\uparrow\rangle_2 + xb|\uparrow\rangle_1|\downarrow\rangle_2 + ya|\downarrow\rangle_1|\uparrow\rangle_2 + yb|\downarrow\rangle_1|\downarrow\rangle_2 \end{aligned} \quad (2.12)$$

That is, I can factor out the brackets. If there are states $|\psi\rangle_1$, $|\phi\rangle_2$ such that

$$|\Psi\rangle_{12} = |\psi\rangle_1|\phi\rangle_2 \quad (2.13)$$

then we say $|\Psi\rangle_{12}$ is a product state. Otherwise we say it is entangled.

Exercise 3 Consider the state $|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle + |\uparrow\rangle_1|\downarrow\rangle_2)$. Is this product or entangled?

Exercise 4 Consider the state $|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)$. Is this product or entangled?

Measurements: To determine the probability of getting a certain measurement outcome when you start with a specific quantum state $|\psi\rangle$, you hit the “ket” $|\psi\rangle$ with the “bra” $\langle\uparrow|$, then square the resulting “braket” to give you the probability. For example,

$$\text{probability of getting up when measuring state } |\psi\rangle = |\langle\uparrow|\psi\rangle|^2 \quad (2.14)$$

Since measuring the up-downness of an up electron always gives outcome “up”, we have

$$\langle\uparrow|\uparrow\rangle = 1 \quad (2.15)$$

and a measurement of a down electron always gives outcome “down” we get

$$\langle\downarrow|\uparrow\rangle = 0 \quad (2.16)$$

“bra”s move over superpositions of kets in a linear way,

$$\langle\uparrow|(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) = \alpha\langle\uparrow|\uparrow\rangle + \beta\langle\uparrow|\downarrow\rangle = \alpha \quad (2.17)$$

Exercise 5 Determine the probability of measuring up when you pass a left electron $|\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$ through a vertical magnet.

Exercise 6 Determine the probability of measuring up when you pass an electron in the state $|\leftarrow\rangle = \sqrt{\frac{1}{3}}|\uparrow\rangle + \sqrt{\frac{2}{3}}|\downarrow\rangle$ through a vertical magnet.

Exercise 7 Any quantum state $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$ will have $|\alpha|^2 + |\beta|^2 = 1$. Why should this be the case? What would go wrong if $|\alpha|^2 + |\beta|^2$ was bigger than 1?

Operations: An operator is a thing that changes a quantum state. It is represented by a sum of “ketbras”. For example

$$A = |\uparrow\rangle\langle\downarrow| + |\downarrow\rangle\langle\uparrow| \quad (2.18)$$

The bra part of the ketbras acts in the same way as they do for measurements,

$$(|\uparrow\rangle\langle\downarrow| + |\downarrow\rangle\langle\uparrow|)|\uparrow\rangle = |\uparrow\rangle\langle\downarrow|\uparrow\rangle + |\downarrow\rangle\langle\uparrow|\uparrow\rangle = |\downarrow\rangle \quad (2.19)$$

Operators that change quantum states are always linear over superpositions, which means

$$A(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) = \alpha A|\uparrow\rangle + \beta A|\downarrow\rangle \quad (2.20)$$

Exercise 8 Consider the operator $|\uparrow\rangle\langle\downarrow| + |\downarrow\rangle\langle\uparrow|$ introduced above. What is $A|\uparrow\rangle$? How about $A|\downarrow\rangle$?

Exercise 9 What is $A|\leftarrow\rangle$? How about $A|\rightarrow\rangle$?

Exercise 10 How would you write down $A^2 = AA$ as a sum of ketbras? How would you describe (in words) what A^2 does to quantum states?

2.1.3 Problems on quantum mechanics

A quantum state is one of our objects $|\psi\rangle$, which we’ve described in terms of the Stern-Gerlach experiments and given the rules for working with above. We pointed out that the quantum state describes all the information there is to know about, in our example, the electrons spin. We often say that the quantum state $|\psi\rangle$ represents some *quantum information*.

We can contrast quantum information with classical information. Classical information is the stuff you usually think of when you think of information: the words of these notes constitute classical information, the voice over the radio constitutes classical information, and so on. The smallest unit of classical information is a bit, which is a symbol that can take on one of two possible different values. Ie a bit b can be 0 or 1. This contrasts with our quantum information $|\psi\rangle$ which can be in a superposition of two states, which we described as up and down.

An important feature of classical information is that it can be copied. If you tell me a bit, say 0, I can repeat 0 back to you three times: 000. Quantum information is different, as the next problem shows.

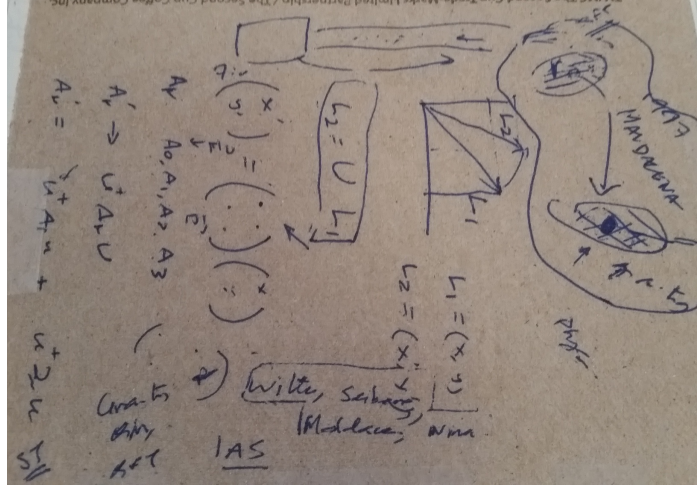


Figure 2. AdS/CFT explained to me on a napkin.

Problem 11 The no-cloning theorem: We have talked about the idea of quantum states, and of operations that change states always being linear operations. In this problem we'll use that operators act linearly (see equation 2.20) on states to prove a theorem known as no-cloning, which says that there is operation U that takes $|\uparrow\rangle_1|\psi\rangle_2$ to $|\psi\rangle_1|\psi\rangle_2$ for all choices of $|\psi\rangle$.

We'll start by imagining that there is such an operator that "clones" quantum states, then we'll show that such an operator would have to be non-linear. We can then conclude that no such operator can exist in quantum mechanics. Call our cloning operator U . By assumption we have that

$$U|\uparrow\rangle|\psi\rangle = |\psi\rangle|\psi\rangle \quad (2.21)$$

1. Let's suppose that $|\psi\rangle = |\rightarrow\rangle$. Since we're assuming U is an operator that can clone any state, we can do this. Then what is

$$U|\uparrow\rangle|\rightarrow\rangle? \quad (2.22)$$

2. Now use that $|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$ and ask again what $U|\uparrow\rangle|\rightarrow\rangle$ is.
3. Does your answer from parts 1 and 2 agree? Use these two results to argue that there can never be such a cloning operator U .

2.1.4 Back to the story...

Eventually Keshav and I moved on from quantum mechanics, and he started having me learn about quantum field theory. I was excited to tackle quantum field theory, which is the core framework in which current physics research is done. He wanted me to learn a little quantum field theory and to do a project with me on supersymmetry.

One day Keshav invited me to go to a coffee shop with him to chat. I thought that was pretty exciting, and Keshav even bought me a slice of chocolate cake while we were there.

I can't remember a ton of what we talked about, but I know I asked him what the Institute for Advanced Study was like and that he tried to explain something called "AdS/CFT" to me. I was pretty confused, but it all sounded very cool. I still have the napkin he drew on while he was trying to explain to me (figure 2). Nowadays I actually work on AdS/CFT, so I did end up understanding what Keshav was talking about that day in the coffee shop, it just took me 5 years to do.

Around that time I contacted someone who was studying entanglement more closely, specifically Patrick Hayden, as Keshav had encouraged me to do. I remember emailing him and sweating over the details of my email, being very nervous to knock on his door when I went to meet him, and trying to rehearse in my head what I'd say to try and convince him I was clever enough that he should work with me. I don't think it was any of the things I thought would impress him that actually did, but for whatever reason he decided we should work together.

2.2 July, August and Quantum Tasks

Patrick told me he'd heard an interesting talk while visiting the Perimeter Institute in Waterloo (<https://www.perimeterinstitute.ca/>), and thought there might be something in that direction we could work on. So he sent me off with a paper to read, and a plan to meet in a week or so to discuss project ideas.

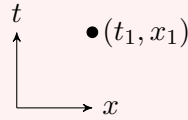
My intention was to work simultaneously on the project with Patrick and on the quantum field theory project with Keshav, but that's not how things ended up going. I drifted and spent a larger and larger portion of my time on the project with Patrick, and eventually officially let go of the other project. Keshav's project required I learn a lot more before I could get started, and I don't think I was ready for some of the more difficult material. It's important to take reasonably sized steps, and Patrick's project really was a better choice for me at the time. That said, I wish I'd kept in better touch with Keshav and followed up on his project, even if maybe that had to happen after I'd matured a bit and taken a few more classes. Nowadays I try and always to split my time between reading to advance what I know and working on whatever research project I have going on. It's important to do both, but for me at least I find the research more exciting and I tend to get out of balance.

The paper Patrick asked me to read was [3], and I also looked at the closely related paper [4], both by someone at Cambridge named Adrian Kent. It all sounded interesting, but I had no idea what a good project might be. Patrick did though, and in fact he chose what I think was an excellent project for me. It didn't have too much overhead, meaning I could get started reasonably quickly, but it was also meaningful, and I learned a lot in doing it. Sometimes beginning students are keen to start doing research on the biggest problems in the field, which usually involve some heavy physics to get too. It's great to be excited about those problems, but sometimes a more strategic approach is called for. Rather than the biggest problems, sometimes it's good to go after manageable smaller projects that you will learn a lot from and be more likely to contribute to.

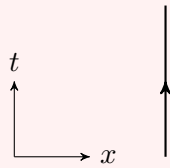
Before I get to describing the project, it's useful to introduce the idea of a spacetime diagram. A spacetime diagram is a map, but while a normal map describes places, which have a certain position, a spacetime diagram describes events, which have a position where

Spacetime diagrams

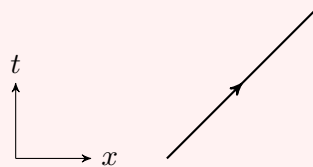
Spacetime diagrams are maps, but the points in the map don't correspond to positions in space: they correspond to positions in space and time. We usually label the space direction along the horizontal axis, and the time direction vertically:



The path an object traces out as it moves through spacetime is called a worldline. The worldline for an object at rest is just a straight, vertical, line.



As the line tilts further and further over, it corresponds to the object moving faster and faster. We usually choose our units of time and space to be such that light goes at 45 degrees:



Since nothing goes faster than light, no worldlines can be steeper than 45 degrees.

To choose the units correctly, we can take the horizontal axis to be marked in terms of meters. Then, the vertical axis should be marked in spacings of how long it takes light to go one meter, which is 1 meter divided by the speed of light, which is $0.33 \times 10^{-8} \text{ s}$.

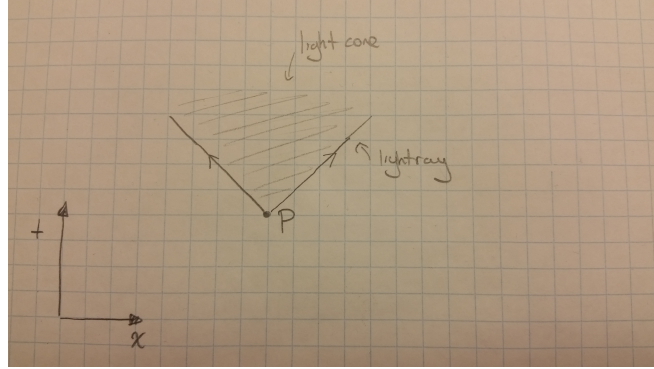
Figure 3. Spacetime diagrams

they occur and a time at which they occur. I've summarized some features of spacetime diagrams in box 3.

Exercise 12 *A car moves at $1/4$ the speed of light in the x direction, then after traveling a distance L stops and immediately proceeds in the opposite direction at $3/4$ the speed of light. Draw the cars world line on a spacetime diagram.*

Recall that, according to special relativity, nothing may travel faster than the speed of

light. Actually, the somewhat more precise way to say this is to say that no information may travel faster than the speed of light¹. In the language of a spacetime diagram, this means that information made available at a point p may travel only into the future light cone of p :



Recall that classical information, like a single bit b , can be copied an arbitrary number of times. Because of this a bit b initially located at point p can then be made available everywhere in p 's future light cone. As we learned in problem 11, quantum information is different: it cannot be copied, and so cannot be made to fill the future light cone of p . Quantum information moves through spacetime in a much more restricted fashion.

Adrian Kent, whose paper I was reading, had come up with an idea he called “summoning” that related to how quantum information can move through spacetime. To talk about what summoning is, it’s useful to introduce two people, Alice and Bob. In summoning, Bob gives to Alice a quantum state which we’ll label by $|\psi\rangle$. Then, sometime later and at some other place, he asks for the state back. He doesn’t ask for it back right away, but instead specifies another time and place where Alice should give it back. In general, there can be many times and places where Bob might request the state be returned.

Using the idea of a spacetime diagram, we can specify a summoning task more precisely. The place where Alice receives the quantum state from Bob we call the start point, s . Any point where Alice might have to return the state we label r_i , while any place that she might receive instructions on where to return the state we call c_i . To keep things simple, we specified that the instructions take a simple form: at each c_i Alice receives a single bit b_i which could be either 0 or 1. If it is 0, then it means the state does not need to be returned at r_i , while if it is 1 then it means the state does need to be returned at r_i . My research problem was to understand for which choices of $s, c_1, \dots, c_N, r_1, \dots, r_N$ could the task be completed with a perfect success rate by Alice.

Kent had thought about some summoning tasks, and actually proven a theorem saying that you couldn’t do certain ones. We’ll reproduce this theorem in the next problem.

Problem 13 *The no-summoning theorem:* Consider the summoning task shown in figure 5. In this problem we will argue that it is impossible to complete this task with a

¹This is more precise because, for example, an object’s shadow can travel faster than the speed of light, but the moving shadow cannot be used to convey information.

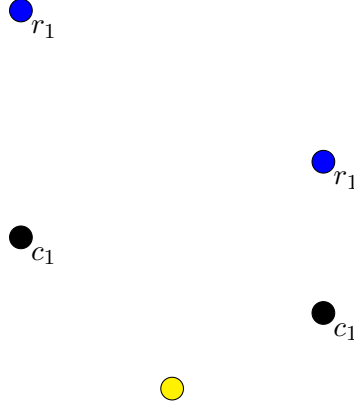


Figure 4. A simple example of a summoning task. At s Alice receives a quantum state $|\psi\rangle$. At each spacetime point c_i she receives a bit b_i which is either 0 or 1. Alice must return the state to the r_i such that $b_i = 1$. Alice is guaranteed that exactly one of the bits will be one.

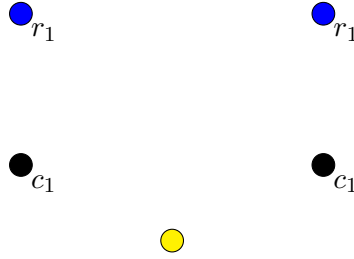


Figure 5. The type of summoning task that Kents “no-summoning” theorem says is impossible.

perfect success rate. To argue this, we will first assume that it is possible, and then show that this results in some kind of non-sense. We can then conclude that actually the task must be impossible.

Notice that the return point r_1 is outside of the light cone of the call point c_2 , and the return point r_2 is outside of the future light cone of the call point c_1 .

- 1. What classical information does Alice have available to her at r_1 ? What about at r_2 ?*
- 2. Usually, Alice gets a call at c_1 OR at c_2 . Imagine though that we played a trick on her, and asked for the state back at both c_1 AND c_2 . If Alice is running her perfect protocol that always completes the task, what happens when we play our trick?*
- 3. Use the results of a previous exercise or something you’ve learned in these notes to conclude this is nonsense, and so it must be that the task is impossible*

The no-summoning theorem deals only with a simple case. Specifically, it concerns the case where there are two “call-reveal” pairs. It already says something interesting though, specifically that the no-cloning theorem restricts how quantum information can move through spacetime.

The research problem Patrick gave to me was to understand exactly when an arbitrary summoning task can be completed. So we imagine now we have n call reveal pairs

$(c_1, r_1), \dots, (c_n, r_n)$, arranged arbitrarily in spacetime, and we want to know when we can successfully complete the task.

Problem 14 *Pause here and think about how you might go about starting to solve this problem. What would you try first? Who would you talk to? What resources would you make use of?*

One of the first things I did to try and understand this problem was to think through the case with just two pairs more carefully. The no-summoning theorem tells you it is impossible to complete the task under certain circumstances, but are those all of the circumstances where it's impossible? For example, do I need r_1 to be connected to r_2 ? Or that c_1 be connected to r_2 ? Or that c_1 be connected to c_2 ? As well, what about the start point s ? How does it fit in?

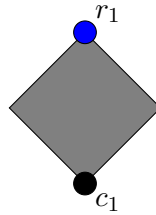
If we think through the proof of no-summoning again, we can work out that what was bad there is that neither of the call points connected to the other reveal points. So for a task to be possible we need at least one of $c_1 \rightarrow r_2$ or $c_2 \rightarrow r_1$. As well, if there was a reveal point r_i which is outside the future light cone of the start point s , then it'd be impossible to get the state from s to r_i , so the task would be impossible. We need then that $s \rightarrow r_i$ for all r_i .

To think about this another way, I constructed what I called the “causal diamonds”². The causal diamond D_i associated with a call-reveal pair (c_i, r_i) I defined as the intersection of the forward light cone of c_i with the backward light cone of r_i . That sounds a bit confusing, but the pictures make it obvious. For example the causal diamond of the call reveal pair:

 r_1

 c_1

is just the grey region



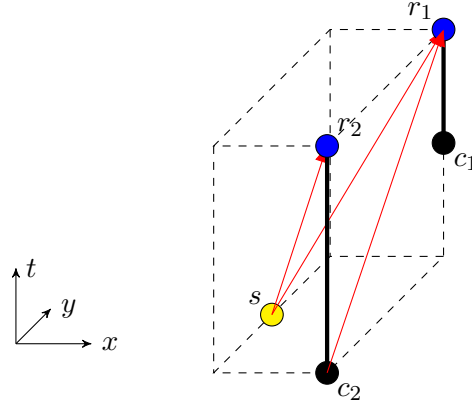
The causal diamond definition was useful in that it cleaned up my notation a bit: instead of talk about call-reveal pairs (c_i, r_i) I could just talk about diamonds D_i . The diamonds also had an important interpretation though: they represent the region where you both know

²By complete coincidence, this term was already standard in the field and used to denote the exact same thing, although people had defined it from a different starting point.

whether or not you're supposed to bring the state to that reveal point (because you're in the future light cone of the call point) and you can actually do something about it (because you're in the backward light cone of the reveal point).

Intuitively, it seems like you need to bring the state into each diamond, check if you need to return the state there, and then possibly move onto the next diamond. Consequently, I began to believe that was needed to complete a summoning task successfully was to bring the state into each diamond, and in turn I thought that meant there should be a path through spacetime that brings you through each diamond.

I didn't think this for long though, because I remembered an example Adrian had included in one of his papers [4]. He considered a summoning task with two diamonds, by in two spatial dimensions instead of the 1 I've been drawing,



Notice that the horizontal and into the page directions are space directions, and the time direction still runs up the page.

You can notice that the example above in $2+1$ dimensions has everything that we said we needed for a summoning task with two diamonds to be possible: it has both its reveal points in the future light cone of the start point, and it has one of its reveal points in the future light cone of one of its call points (in this case $c_2 \rightarrow r_1$). Nonetheless, it seems like I can't do this task: suppose I start with the quantum state near s . Starting at s , there's no path I can send the state on that will go through both diamonds.

In fact though, Adrian pointed out that you can do this task! Doing so requires a new tool called "quantum teleportation" that I haven't introduced to you yet, but it's not too hard to understand. Here I will just give you the functional description of what happens in quantum teleportation. Later, you can go on to understand teleportation at a deeper level, but it's an important skill to be able to work with a preliminary description of something.

So here's the basic picture of how quantum teleportation works. Alice, say here on Earth, holds a quantum state $|\psi\rangle_1$. There is also an entangled state $|\Psi\rangle_{23}$, with the 2 electron held by Alice and the 3 electron held by Bob. Alice's goal is to transfer the state $|\psi\rangle$ she holds on the 1 electron onto the 3 electron. To do this, she makes a certain measurement of the 1 and 2 electrons, which gives her a measurement outcome labeled by a, b, c or d . She then sends her measurement outcome, which is classical information, to Bob.

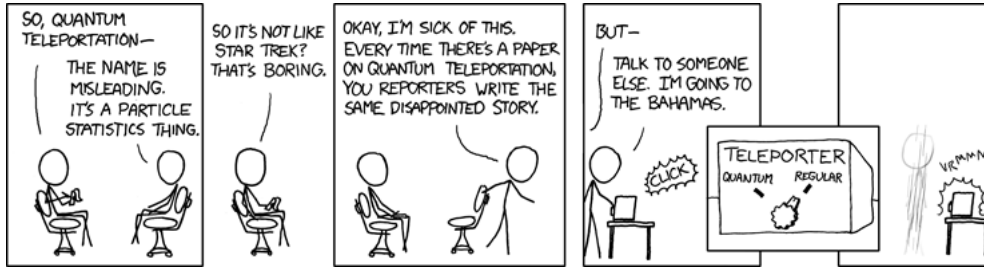
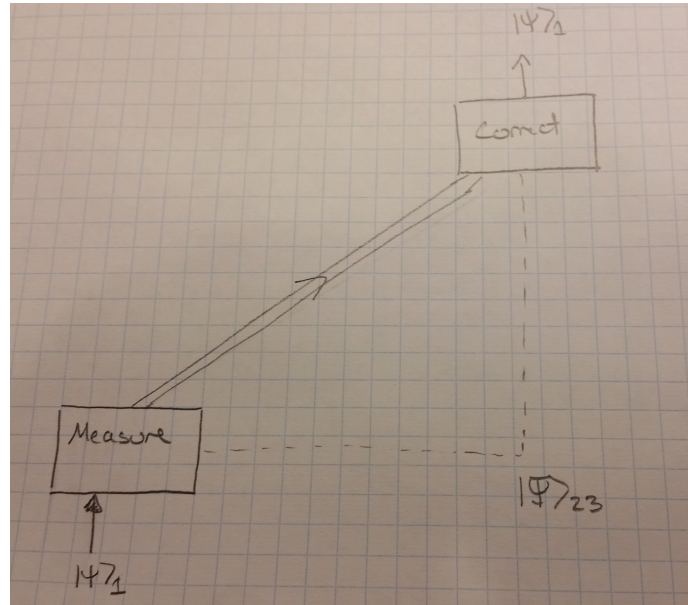


Figure 6. Comic reproduced from XKCD, see <https://xkcd.com/465/>.

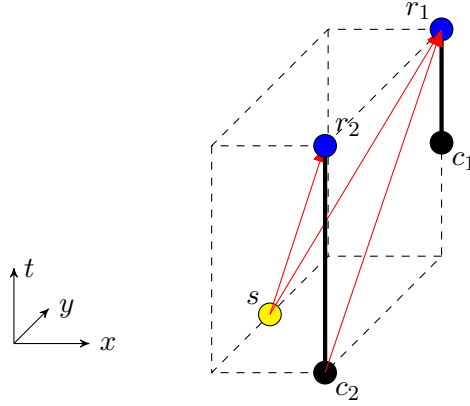
Bob then applies an operator to the 3 electron that depends on the measurement outcome he received, and after applying that operator he holds the state $|\psi\rangle_3$, as was desired.

We can also explain this in a picture:



Notice that in the teleportation procedure information never travels faster than the speed of light, and there already needs to be an entangled state distributed between where you are and where you want to go, so it's not quite the stuff of Star Trek fame (see figure 6). Nonetheless quantum teleportation is very useful for a variety of reasons. One reason, which was actually noted in the original paper introducing teleportation [5], is that Alice need not know where Bob is in order to send him her quantum state. Since what Bob needs to send to Alice, she can actually send it in all directions. Without teleportation Alice does need to know where Bob is, because she can't copy the state and naively can't send it in all directions.

This observation that teleportation lets Alice send her state without knowing where Bob is located is actually the key to completing the summoning task in 2 spatial dimensions I gave above. Recall that the task was



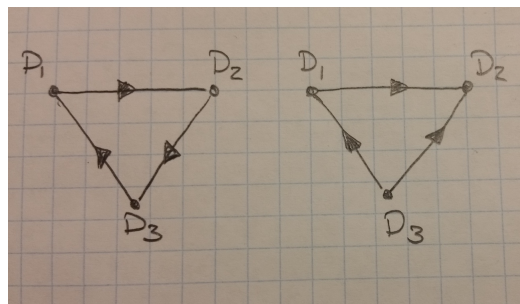
and we noted that the difficulty in completing it is that there is no path starting at s that passes through both diamonds.

To complete this task using teleportation, we do the following. Before the task starts, take an entangled state $|\Psi\rangle_{23}$ and share it between s and c_2 . Then, as soon as Alice receives the state, she teleports the state $|\psi\rangle_1$ that she receives by measuring the 1 and 2 electrons. She then sends her (classical) measurement outcome to both r_1 and r_2 . Meanwhile, over at c_2 , Alice looks at the call she gets. If the call is a 1, she send the 3 electron to r_2 . If the call is a 0, she sends the 3 electron up to r_1 . The end result is that both the measurement outcome from the teleportation and the 3 electron end up where ever the state is supposed to go. Since Alice can use the 3 electron and the measurement outcome to produce $|\psi\rangle$, she succeeds in completing the summoning task.

We argued earlier that we need, for the task to be possible, that 1) both the reveal points to be in the future light cone of the start points and 2) one of the reveal points to be in the future light cone of the other call point. Now we know that actually we can do the task whenever both of those conditions are true, since the teleportation style protocol will always work. This totally characterizes for us summoning tasks with two diamonds: we know exactly when they are possible and when they are impossible.

2.3 Moving upward to three diamonds

Next I moved on to the cases with three diamonds. The first thing you can notice is that whenever two diamonds are disconnected you can apply the no-summoning theorem again: the no-cloning theorem can be used to tell you that a task with any two diamonds being disconnected is impossible. Then it remained to think about the various ways you can connect up three diamonds. All the ways, at least up to relabeling what you call D_1, D_2 and D_3 are these:



The case on the right I could figure out how to do, so I knew that one was possible. The way to do it involves using the teleportation protocol again, and we’ve already seen something like that, so I won’t describe this case. The other case, the case where the connections go in a loop, I didn’t see any way to do. On the other hand the no-summoning theorem didn’t tell me it was impossible, so I was a bit confused with this one. One possibility I considered for a long time was that you could never actually get such an arrangement of diamonds by choosing call and reveal points in a spacetime. Instead, I thought that whenever you had a loop, one pair of diamonds in the loop would actually always be connected in both directions. I called this the “loop lemma”.

In fact, I could argue roughly that this was the case if I worked with only one spatial dimension. For some reason I didn’t really think too hard about whether or not that idea would still be true in two spatial dimensions. Probably that was because I had an exciting idea about how to solve the problem if the loop lemma was true, and I was busily pursuing that idea.

At that time I was organizing a series of talks for and by undergraduates. The talks were in math, physics and computer science, so we got an interesting mix of topics. Hosting the talks was also a useful way of getting a bit of a community going during the summer months. A lot of people were away, and the usual social circles were all disrupted, so giving everyone who was still there an excuse to get together was good and got us all talking. There were some good talks, but more useful was talking to people before and after, about the talks and about whatever else.

Since I was the organizer I’d written a talk that I could use to fill in any week that might come along where I couldn’t find a speaker, or if someone canceled. Such a week came around towards the end of the summer. Before I gave the talk I mentioned to Patrick that I was giving it, I think just in the context of asking him how I could best explain something. To my surprise he asked me when and where the talk would be. I told him, but pointed out that though he was super welcome to come, it’d otherwise just be undergrads. He said he didn’t mind and he’d see me there.

Before giving the talk I was kind of nervous. After all, I hadn’t actually solved my problem at this point. What was I supposed to tell them about? And this with my supervisor in the room! But I went ahead and gave the talk anyway. I explained (as best I understood it then) how quantum states worked, how teleportation worked, and much of what I’ve said above. Then I got to the point about three diamonds and diamonds with cycles of connections. I said that I thought that I thought everytime you had a cycle you’d

Observation

2 messages

Patrick Hayden <patrickh@mcgill.ca>
To: Alex May <alex.may@mail.mcgill.ca>

Wed, Aug 29, 2012 at 8:43 PM


I think I have a counterexample in 2+1 dimensions to the conjecture that a loop always implies a doubled edge.

Set p_0, p_1, p_2, p_3 at the vertices of a square with common time coordinate 0.

Set spatial coordinates of q_0, q_1, q_2, q_3 to the midpoints of the edges joining p_j and p_{j+1} and the common time coordinate is set so that q_j and q_{j+1} are lightlike to p_j .

See the attached diagram.

The example doesn't satisfy the condition of being a causal graph, however, because there are no edges between j and $j+2$. So, if the loop conjecture is true, we need additional hypotheses beyond what I wrote on the board today. (Namely, the fact that every pair of diamonds is connected by an edge in the graph.)

 counterexample.pdf
21K

Patrick Hayden <patrickh@mcgill.ca>
To: Alex May <alex.may@mail.mcgill.ca>

Thu, Aug 30, 2012 at 3:25 PM

FYI I think that I've checked all the cases and confirmed that the loop lemma is true in 1+1.

On 2012-08-30, at 2:42 PM, Alex May wrote:

> What if you do what you've described with four regions, but just with three? (have p_0, p_1, p_2 at same time coordinate, set spatial coordinates of q_0, q_1, q_2 to midpoints of the edges between the p 's) It looks like you still get a loop with no double edges, but now your graph has edges between every pair. So it looks to me like a counter example to the loop conjecture (and to my conjectured condition for the possibility of tasks). What do you think?

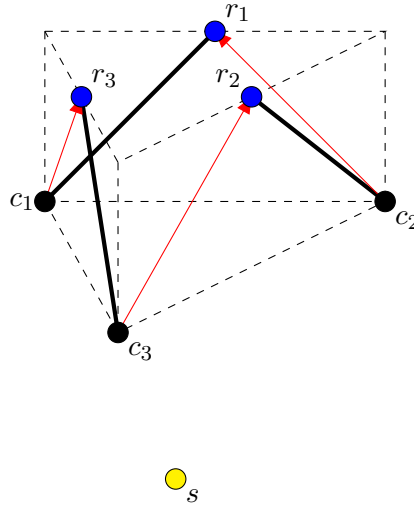
>

> Alex

Figure 7. The email Patrick sent me after he attended the talk I gave for my fellow undergrads. Patrick points out that the audience members disbelief of my loop lemma was correct - the loop lemma is false. I follow up by pointing out an example with just three diamonds. Reducing it to three diamonds means we have a problem that has a loop and has every diamond directly connected.

also get the extra connection, and argued you could never get one with only one spatial dimension, and started to go on to explain how I thought things would work if you assumed that. At that point though someone in the audience put up their hand and asked if I had a better reason to believe my loop lemma. I said no. He said he didn't believe me then.

Later that night Patrick emailed me (figure 7). He'd taken that guy in the rooms disbelief seriously, and actually figured out that you can get cycles! The picture he sent me was a cycle among four diamonds, but we quickly saw that you could actually do it with just three. The cycle on three looks like this:



This was a lesson to me. I'd gotten caught up in the path I was pursuing, and brushed under a rug an assumption I'd made earlier on that might have been wrong. It's definitely ok, and essential strategy even, to pretend for awhile that somethings true and see what the consequences would be, and then to come back later and check your assumption. It's just that while you do that you have to not get too swept up in what your doing. At the back of your mind you have to stay open to the possibility that the assumption you made way back when is wrong.

I learned a second lesson too, which was that even though Patrick, a very well respected expert in the field, had been at my talk, it had ended up being an undergrad who was just hearing about the problem for the first time that made the most useful contribution that day. And all he had to do was be a bit stubborn and push for a good reason for me to make my assumption!

So how could we deal with these summoning tasks that had loops in them? I tried using teleportation in various ways, but nothing seemed to work. It was possible they were just impossible to complete, but I didn't have any way I might prove that if it was true. I kept looking for ideas, either of how to prove it was impossible or of how to do it.

I recalled something I'd learned about quantum states that I thought might be useful. While they can't be copied, they can be split up into different parts in what is called an error correcting code. I can't actually recall, and nothing in my notes seems to hint at, how I first heard about quantum error correcting codes. Most likely though it was Patrick who suggested to me that they might be relevant and suggested I look into them. Certainly it's good to have someone with a broad expertise around who can point you towards these sorts of things!

I've introduced error correcting codes for classical information in the next problem. Afterwards I'll describe quantum error correcting codes.

Problem 15 *Error correcting codes* *An error correcting code is a way to store information in a way that protects against losses. For example, suppose I have some classical information, say a single bit b which can be 0 or 1, and suppose there is some probability*

that the thing I am storing this bit on might get lost or erased. What should I do? Well, the simplest thing I could do is copy the bit a few times,

$$\begin{aligned} 0 &\rightarrow 00 \\ 1 &\rightarrow 11 \end{aligned} \tag{2.23}$$

Then, if I lose any one bit, I can just look at the other one. The information we'd like to store we call your logical state, while the encoded, larger number of bits we call the physical state.

Design an error correcting code that stores two bits worth of logical information in three physical bits. That is, fill in the blanks of the table

$$00 \rightarrow _ _ _ \tag{2.24}$$

$$01 \rightarrow _ _ _ \tag{2.25}$$

$$10 \rightarrow _ _ _ \tag{2.26}$$

$$11 \rightarrow _ _ _ \tag{2.27}$$

and do so in a way that guards against erasing any one of the physical bits.

As mentioned in the problem above, the most basic way to make a classical error correcting code is to copy the logical bit a few times, ie send $b \rightarrow bbb$. What if we want to make a quantum error correcting code? Specifically, I want to store the state on one electron, say $|\psi\rangle_1$, onto 3 electrons in some state $|\Psi\rangle_{123}$ in a way that protects against losing one electron. That is, I should be able to recover $|\psi\rangle$ by starting with electrons 1 and 2, or 2 and 3, or 1 and 3. The naive way to do this would be to send

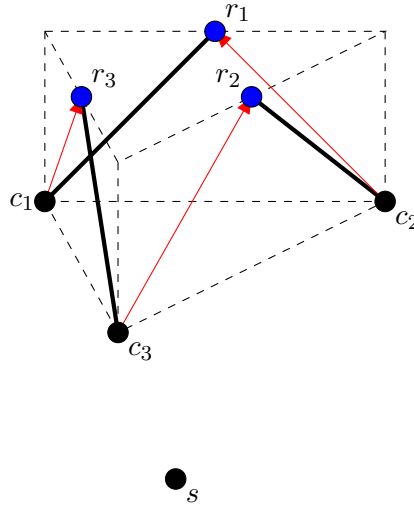
$$|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle|\psi\rangle \tag{2.28}$$

but as we learned earlier, this is impossible! We can't copy a quantum state.

What are we to do then? The trick is to store the quantum state in a way that allows you to lose one electron, but never allows more than one copy of the state to be produced. This at first seems impossible, but actually its not so hard to imagine: we encode the state $|\psi\rangle$ into the state of 3 electrons in a way that allows $|\psi\rangle$ to be recovered from electrons 1 and 2, or electrons 2 and 3, or electrons 1 and 3, but not from any one electron alone. Since you always need two electrons to make the original quantum state, and there are a total of three electrons, you can't make more than one copy.

Exercise 16 Quantum error correction Suppose that we encode a quantum state into n parts such that any k of them can be used to get $|\psi\rangle$ back - this is called a $((k,n))$ scheme. What is the smallest that k can be?

Now we are ready to come back to the case with three diamonds and a cycle,



We can use our error correcting code with three parts such that any two can be used to get the state back (our $((2,3))$ scheme) to complete this. I leave this for you to do!

Problem 17 We will use the $((2,3))$ scheme to design a protocol that successfully completes the cyclic task with three diamonds.

1. You've received the state at s and promptly turned it into three shares in a $((2,3))$ error correcting code. Now you need to decide where to send each share. Should you send one share to each diamond, or two shares to one diamond, or? Notice that each diamond is the same as every other: it connects to one diamond and is connected to from one other diamond. Use this fact to argue you should send one share to each diamond.
2. Now you've brought one share to each diamond. At the c_i you receive the information b_i , and you can use this information to decide where to send your share. There are two cases: $b = 0$ and $b = 1$. Decide where to send the share in the error correcting code in each case, and argue this always completes the summoning task.
3. **Bonus:** What happens in the protocol you've designed if two of the b 's are 1? If you know for sure you will get exactly two b 's with $b = 1$, is there a protocol that will always result in the state being handed over at one of the diamonds where $b = 1$? What if you're not sure if there will be 1 or 2 places where $b = 1$?

Now that I knew I could do this task, I understood exactly when you could do tasks for up to three diamonds: summoning was possible (for up to three diamonds) if and only if 1) all the reveal points are in the future light cone of the start point and 2) every diamond is connected (and which direction they're connected in doesn't matter). I remember feeling very excited when I realized this might be how it worked for all numbers of diamonds, because it would be such a nicely simple answer if it was true. I wrote down my conjecture:

Conjecture 18 A summoning task with any number of diamonds is possible if and only if the following two conditions hold

1. *All the reveal points are in the future light cone of the start point*
2. *Every diamond is connected to every other diamond*

I had what I thought was the right idea in hand, but I didn't know how to prove it for more than three diamonds and the end of the summer was coming near...

3 Third year - Keeping at it

The summer ended and I still hadn't proven my conjecture. It was disappointing. Patrick encouraged me to keep thinking about it during the semester, but I worried I wouldn't have the time given all the classes I'd be taking. I did keep thinking about it, even if I hadn't really intended to. I found I'd think about it in the metro, or in a boring lecture, or whenever, and sometimes I'd find a bit of time on a weekend to work on it. I had the bad habit too of thinking about it while trying to fall asleep, which kept me up.

I remember once thinking I'd figured out how to prove my theorem while sitting through a lengthy electricity and magnetism lecture. The excitement of thinking I'd had it and the disappointment of realizing I didn't wasn't honestly pretty serious emotional turmoil. I was deeply invested at that point. I think I had some amount of useful insight that time though, so I don't think that idea was a total loss.

I had another flash of insight riding home from my girlfriends on the metro one night. I remember alternately running and walking home from the metro station, trying to keep the somewhat vague (but, I was convinced, important) notion in my head until I could get to a sheet of paper and start writing. I worked at my kitchen table until 2 or 3 in the morning I think, trying get it to work out, and then when I did think I had it checking it and rechecking it. I wrote Patrick an email with my idea, but then went to bed without sending it. I didn't trust my tired self not to be making some embarrassing mistake. In the morning I checked it yet again and sent it off (see figure 8). I'd titled the email "I have it! (I think)" and written at the end of it "I'm excited, but I am remembering that even when I think I have it, it sometimes happens that I actually don't. Let me know what you think."

That night Patrick got back to me with a short email saying he'd have a look and that it seemed interesting. He was at a conference in Singapore at the time, so he was a bit occupied. While I waited for a reply I went into campus and found whoever I could and explained my (supposed) result to them, to see if they could find an error. No one did, so it was so far so good. The next morning Patrick got back to me: "Absolutely beautiful. It should work, as far as I can tell!"

4 After the proof and some reflections

After Patrick's email to me we still had to write up our result. Since Patrick could probably do a better job of it than I could, I let him do the writing, but he had me look over it and give him feedback. I also wrote my own version of the paper independently before I'd seen

```

>> From: Patrick Hayden [REDACTED]
>> Sent: Tuesday, September 11, 2012 10:48 AM
>> To: Alex May
>> Subject: Re: I have it! (I think)
>>
>> Absolutely beautiful. It should work, as far as I can tell!
>>
>> The efficiency is dreadful, but efficiency is a question for another day: for  $n$  pairs, there are  $n$ 
subsets of size  $n-1$  and it's necessary to solve the problem for each one. So if  $f(n)$  is the size of the
secret sharing state or the number of subproblems, then  $f(n) \sim n f(n-1) = n!$ .
>>
>> Congratulations! This is a real breakthrough.
>>
>> On 2012-09-11, at 9:35 AM, Alex May wrote:
>>

//outlook.office365.com/mail/inbox/id/AAQkAGU2MTQ4ZDI2LTA4ZTkxNDk5NC1hN2ExLTc4ZTU1YmE1NjNkOAAQAGf590MUwk1YhY6heYz4EaY%3D 2/

```

```

119
Mail - Alex May - Outlook

>>> Hey, so I think I found the general algorithm for completing any task satisfying the condition that
every pair of regions is causally related. I'd be awesome to come in tomorrow to show you, is there a
good time?
>>>
>>> What I'm thinking goes like this:
>>>
>>> Up to relabeling there are 2 distinct tasks with three regions, the cyclic case  $A \rightarrow B \rightarrow C \rightarrow A$ , and
the other one  $A \rightarrow B$ ,  $A \rightarrow C$ ,  $B \rightarrow C$ , which I'm calling the Tee (because in general you have to teleport
to complete it). We can do both of these, so we can do any three region task.
>>>
>>> Suppose we can do any task with  $k$  regions. Denote a secret sharing scheme where there are  $m$ 
shares, and any  $n$  of them can be used to reconstruct the secret as a  $[n, m]$  scheme. Create a  $[k, k+1]$ 
scheme. Because  $\binom{k+1}{k} = k+1$ , for every set of  $k$  vertices, we can associate to it one share.
Consider the vertex  $v$  where the call is received. There will be  $k = \binom{k}{k-1}$   $k$ -tasks which
include  $v$  (this requires we use the conjectured condition). We can complete each such task, giving
us  $k$  shares at  $v$ , which completes the  $k+1$ -task.
>>>
>>> I'm excited, but I am remembering that even when I think I have it, it sometimes happens that I
actually don't. Let me know what you think.
>>>
>>> Best,
>>> Alex

```

Figure 8. The “I have it!” email exchange between Patrick and I. The first email is the bottom one, the reply is above.

his, just to give it a try and learn. Comparing his version to mine was quite useful in learning how to communicate clearly.

Writing the paper was more of a process than I realized it would be. There was a lot of back and forth, and while we wrote we thought about adding sections that we’d have to develop new results for. Writing the result can really clarify what’s missing, and it does often happen that you end up doing a lot of extra research while you try and write. In our case we ended up deciding that our result stood on its own and we wouldn’t add anything, so we actually got it out pretty quickly, within about one month of the “I have it!” email. Our paper appeared on the arXiv [6], and was published in a journal some time later.

Aside from writing the paper, there was a lot of other communicating of our result that we still had to do. Patrick was very generous with me in funding my travel to conferences to talk about our work. I went to the Canadian Association of Physicist Undergradu-

ate Conference (CUPC) (see <https://www.cap.ca/congress-conference/cupc/>), a local conference held for graduate students, and even to the core annual conference held in our field, which was in Beijing that year. I had another useful learning experience in preparing the talks for the CUPC and the grad student conference, and in watching Patrick give his talk in Beijing.

Every time I went to a conference to talk about my results I was nervous about something. At the undergrad and grad student conferences I was worried people would think my result wasn't important. At the Beijing conference I was worried I'd seem naive to all the profs there. The climate at the undergrad conference was maybe a little competitive, I felt sometimes like people were trying to show off and there were awards given for best poster and best talk, but at the grad student conference and the high level conference in Beijing there was really no competitive atmosphere (best poster and talk awards are purely undergrad phenomena). And the Profs didn't look down on me as naive, they *knew* I was naive (I was an undergrad!) and were impressed I'd been able to do some interesting work and expressed their hope for my future.

I've often reflected on the haphazard series of connections that led me to meet Patrick, and all the consequences that has had. In many ways the haphazardness makes it all feel very lucky, and indeed I do think I was very lucky to come across the people that I did and have the opportunities that I did. At the same time, there's a lot you can do to set up good connections in the academic world. In the context of being an undergrad who's interested in research, I think one thing my story shows is the importance of your TA's. It's the TA's that you'll interact with most often and most directly, and they can sometimes directly offer you research to do or connect you with professors. Igor helped me out tremendously when I was an undergrad, and now that I'm a grad student and a TA I've had the opportunity see things from the other side. I am definitely on the watch for good undergrads I can recruit. I like helping undergrads out, because I was one once and I know what it's like, but also because a good undergrad can be really useful to me!

Aside from the good luck, I also did work very hard that summer. I put in a lot of hours. And I benefited from a strong community of people around me. Giving that talk for instance pulled me out of a blind alley and got me unstuck. I also benefited from many small conversations with many different people that summer. Those could range from explaining things I'd learned from my quantum textbook to someone, to discussing approaches to my research problem, to seeking out help with bits of mathematics that I wasn't familiar with. All those conversations help keep things moving.

Another thing that strikes me looking back is the surprising interconnections in the topics of research I've worked on. For example, a paper I published in February of 2019 [7] is closely related to my first ever paper [6] from the fall of 2012. It's also closely related to a final project I did for a class in 2013. So you should certainly keep this in mind as you do research: every past project you work on is something that can potentially be connected to what you're working on now, and something that can potentially give you new ideas for what to do next.

As I go through my career, I keep being pleasantly surprised that I'm able to contribute meaningfully to the forefront of research. I worried as an undergrad and when I was in high

school that I wouldn't be able to, because I didn't think (and still don't think) I'm the smartest person around. What could I contribute that the smartest person in the room couldn't? It turns out though that this line of thinking is wrong. Hard work and lots of communication count for a lot. Another way contributions happen though is just from your own unique path. Sometimes it takes a person who, just by luck, happened to know about thing X that no-one would have guessed would be relevant. Sometimes it takes a quirk of someones personality or quirk in their take in how science should proceed. It's true I'm not the smartest guy in the room, but every once in a while there's a problem that requires my own weirdness to solve.

5 Additional problems

Problem 19 *More on classical error correcting codes* In problem 15 we began to study classical error correcting codes, which are ways of storing classical information that protect it against errors. Here we will study a somewhat more complex example of an error correcting code called the Hamming code. It will let us store 4 logical bits into 7 physical bits.

We will work up to designing and understanding this code.

1. Lets start by revisiting the code from problem 15 and thinking about it in a new way. Recall that we wrote

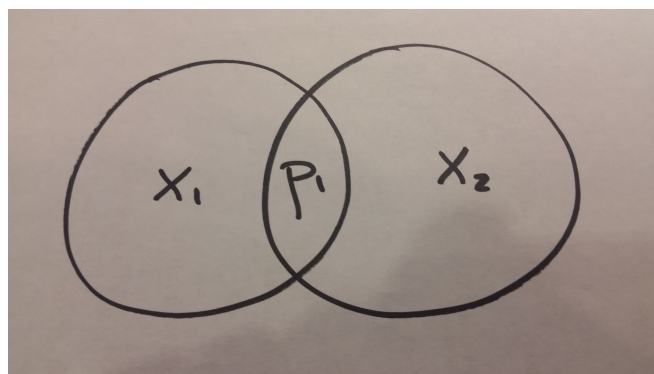
$$00 \rightarrow _ _ _ \quad (5.1)$$

$$01 \rightarrow _ _ _ \quad (5.2)$$

$$10 \rightarrow _ _ _ \quad (5.3)$$

$$11 \rightarrow _ _ _ \quad (5.4)$$

and found that we could fill in the table on the right always corrected for any single bit error. Although trial and error is a perfectly good way to solve this, there is actually another way. To see this, draw a Venn diagram with two circles:



Call the two logical bits x_1 and x_2 and put them into the center of the two circles. Then calculate the third bit that sits in the overlap of the two circles, according to

$x_1 \oplus x_2 = p_1$, where \oplus means you should follow the rule

$$0 \oplus 0 = 0$$

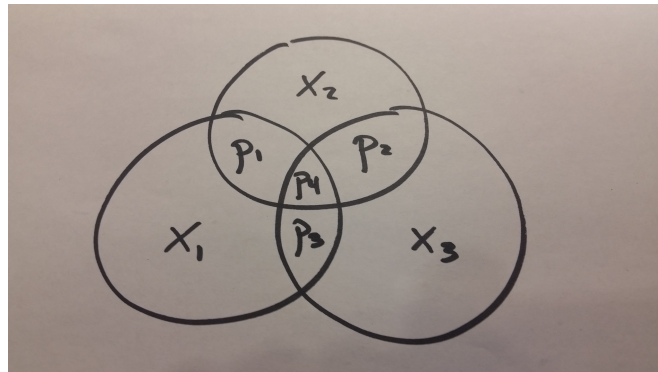
$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Notice that $1 \oplus 1 = 0$, not 1! This is called addition “mod” 2, because everytime your sum gets up to 2 you go back to zero.³ Use x_1, x_2, p_1 as your three physical bits and fill in the table above (this might be different than how you filled it in before).

2. Using your Venn diagram, how can you fill in the x_1 bit if you know p_1 and x_2 ? How about x_2 from p_1 and x_1 ?
3. Because its possible to get back x_1 and x_2 when any one bit is erased from the Venn diagram, this gives us an error correcting code that stores two logical bits into three physical ones, and corrects the erasure of one bit. Notice that we could also use our Venn diagram in a backwards way: we could call p_1 the logical bit. Then we notice that erasing any one of x_1, x_2, p_1 still allows us to construct p_1 again. So we can also view this as an error correcting code that stores 1 logical bit into 3 physical ones!
4. Now, use a Venn diagram with three circles and the \oplus rule to store 3 logical bits into 7 physical bits:



How should we determine p_4 from the x 's? Convince yourself that in your Venn diagram you can erase any bit and still recover x_1, x_2, x_3 .

5. Now use your Venn diagram with three circles in the backwards way: convince yourself you can construct any of the p 's even after any one bit has been erased. This means you can actually store 4 logical bits into 7 physical ones!

³You already know how to add mod 12: 3 hours past 11:00 is 2:00.

References

- [1] John S Townsend. *A modern approach to quantum mechanics*. University Science Books, 2000.
- [2] Richard P Feynman, Robert B Leighton, and Matthew Sands. The feynman lectures on physics; vol. i. *American Journal of Physics*, 33(9):750–752, 1965.
- [3] Adrian Kent. A no-summoning theorem in relativistic quantum theory. *Quantum information processing*, 12(2):1023–1032, 2013.
- [4] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.
- [5] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.
- [6] Patrick Hayden and Alex May. Summoning information in spacetime, or where and when can a qubit be? *Journal of Physics A: Mathematical and Theoretical*, 49(17):175304, 2016.
- [7] Alex May. Quantum tasks in holography. *arXiv preprint arXiv:1902.06845*, 2019.