Week 13 - Day 2

Secure Quantum Communication

Concept 1: Secure Quantum Communication

Concept 2: More two-level systems and no-cloning theorem

Quantum computation (Week 13)

Reference:

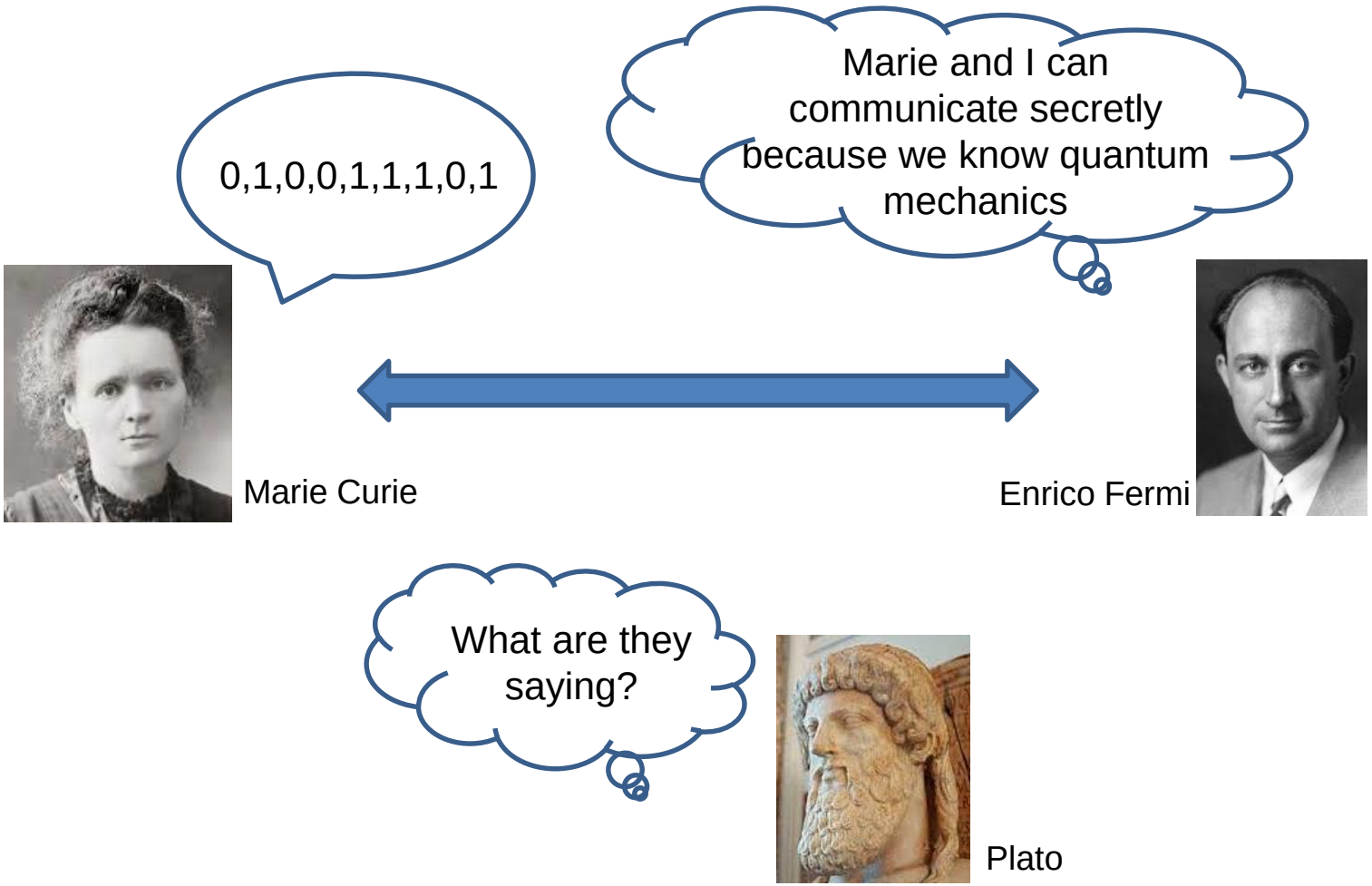
Six Quantum Pieces: A First Course in Quantum Physics

Chaper 1 section 1.3 and Chapter 2 sections 2.1, 2.2 and 2.3

Concept 1: Secure Quantum Communication

Secure quantum communication

Suppose Marie (M) wants to send a message to Enrico (E), but she wants to make sure that nobody else knows what the message is, especially the “classic” Plato.



The simplest way to communicate is to use the language of computers, i.e. 0s and 1s.

Secure quantum communication

The message between Marie and Enrico can always be written as a combination of 0s and 1s. For example the 255 different characters below correspond to an equal number of numbers, and any number between 0 to 255 can be associated to a combination of eight 0s or 1s by converting decimal to binary numbers.

Examples:

10 -> 00001010

126 -> 01111110

254-> 11111110

One drawback to this method is that it takes 8*L bits of memory (0 or 1) to write just L characters … but this is not an issue with current memories TB, e.g. 8×10^{12} bits (crazy number if you think about it).

ASCII table

DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII
1	☺	32	space	64	@	96	`	128	Ç	160	á	192	└	224	Ó
2	☻	33	!	65	A	97	a	129	ü	161	í	193	┴	225	ß
3	♥	34	"	66	B	98	b	130	è	162	ó	194	┬	226	Ô
4	♦	35	#	67	C	99	c	131	â	163	ú	195	├	227	Ò
5	♣	36	$	68	D	100	d	132	ä	164	ñ	196	─	228	õ
6	♠	37	%	69	E	101	e	133	à	165	Ñ	197	┼	229	Õ
7	•	38	&	70	F	102	f	134	å	166	ª	198	ã	230	µ
8	◘	39	'	71	G	103	g	135	ç	167	º	199	Ã	231	þ
9	○	40	(	72	H	104	h	136	ê	168	¿	200	╚	232	Þ
10	◙	41	)	73	I	105	i	137	ë	169	®	201	╔	233	Ú
11	♂	42	*	74	J	106	j	138	è	170	¬	202	╩	234	Û
12	♀	43	+	75	K	107	k	139	ï	171	½	203	╦	235	Ù
13	♪	44	,	76	L	108	l	140	î	172	¼	204	╠	236	ý
14	♫	45	-	77	M	109	m	141	ì	173	¡	205	═	237	Ý
15	☼	46	.	78	N	110	n	142	Ä	174	«	206	╬	238	¯
16	►	47	/	79	O	111	o	143	Å	175	»	207	¤	239	´
17	◄	48	0	80	P	112	p	144	È	176	░	208	ð	240	-
18	↕	49	1	81	Q	113	q	145	æ	177	▒	209	Ð	241	±
19	‼	50	2	82	R	114	r	146	Æ	178	▓	210	Ê	242	‗
20	¶	51	3	83	S	115	s	147	ô	179	│	211	Ë	243	¾
21	§	52	4	84	T	116	t	148	ö	180	┤	212	È	244	¶
22	▬	53	5	85	U	117	u	149	ò	181	Á	213	ı	245	§
23	↨	54	6	86	V	118	v	150	û	182	Â	214	Í	246	÷
24	↑	55	7	87	W	119	t	151	ù	183	À	215	Î	247	¸
25	↓	56	8	88	X	120	x	152	ÿ	184	©	216	Ï	248	°
26	→	57	9	89	Y	121	y	153	Ö	185	╣	217	┘	249	¨
27	←	58	:	90	Z	122	z	154	Ü	186	║	218	┌	250	·
28	∟	59	;	91	[	123	{	155	ø	187	╗	219	█	251	¹
29	↔	60	<	92	\	124	|	156	£	188	╝	220	▄	252	³
30	▲	61	=	93	]	125	}	157	Ø	189	¢	221	¦	253	²
31	▼	62	>	94	^	126	~	158	×	190	¥	222	Ì	254	■
		63	?	95	_	127	⌂	159	ƒ	191	┐	223	▀	255	space

Secure quantum communication

To communicate secretly, Marie and Enrico do not need to send each bit of information over a secure communication channel, which is a good thing because, as we will see, sending information secretly can be very time consuming and require much resources.

They only need to share a key to encrypt and decrypt their message.

For example, suppose the message is $m = 0011$ and the secret key is $k = 0101$, then Marie could send the encrypted message $c = m \oplus k$ where $\oplus$ stands for bit by bit binary sum

$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0$$

which gives $c = m \oplus k = 0110$

When Enrico receives the message, all he has to do to decrypt the message is

$$m = c \oplus k = 0110 \oplus 0101 = 0011$$

Only somebody with the same key can access the correct message.

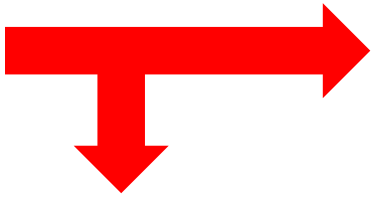
I will encrypt my message m with the key k, and send you the encrypted message c

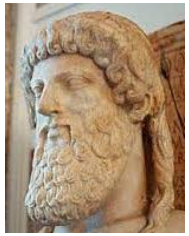
No worries, I will use the key to decrypt it and get back your message m.

Secure quantum communication

What can happen if Marie and Enrico cannot use quantum mechanics?

Marie Curie





Plato

Enrico Fermi

Plato can (in principle) intercept the message from Marie, make a copy for himself, and let the original message (or another copy) continue towards Enrico.

Two things are important to notice now:

1) it is impossible for Plato to make a copy of the message from Marie (we will see this later as the no-cloning theorem)
2) if Plato tries to eavesdrop, Marie and Enrico can (in principle) find out (as we will see soon)

Here comes one way in which Marie and Enrico can transfer this encryption key.

Secure quantum communication

I will send you one of these four photons chosen at random

Marie produces photons one by one. Each one is **randomly** prepared either in one of the four following states

$$|H\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |V\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \qquad |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

and she sends them one by one to Enrico. She will associate the value 1 to $|H\rangle$ and $|+\rangle$, and the value 0 to $|V\rangle$ and $|-\rangle$.

And I will measure in one of these two ways, also chosen at random

Enrico **randomly** chooses to measure either with the observable

$$\hat{A} = |H\rangle\langle H| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \; or \; \hat{B} = |+\rangle\langle +| = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

Secure quantum communication

What would be the outcome of the measurements by Enrico?

It depends on the photon sent by Marie and on the measurement chosen by Enrico.

How Marie can choose to send her photons

How Enrico can choose to measure the photons

	$\hat{A} = \|H\rangle\langle H\|$	$\hat{B} = \|+\rangle\langle +\|$
$\|H\rangle$	1	$1\ or\ 0\ each\ 50\%$
$\|V\rangle$	0	$1\ or\ 0\ each\ 50\%$
$\|+\rangle$	$1\ or\ 0\ each\ 50\%$	1
$\|-\rangle$	$1\ or\ 0\ each\ 50\%$	0

We'll refer to this as the "truth table".

Secure quantum communication

If Marie has sent a photon in the $|V\rangle$ or $|H\rangle$ state, and Enrico has measured with $\hat{A}$, then when Marie sent a 1, Enrico always measured a 1, and when Marie sent a 0, Enrico always measured a 0.

Similarly, if Marie has sent a photon in the $|+\rangle$ or $|-\rangle$ state, and Enrico has measured with $\hat{B}$, then when Marie sent a 1, Enrico always measured a 1, and when Marie sent a 0, Enrico always measured a 0.

But if Marie has sent a photon in the $|V\rangle$ or $|H\rangle$ state, and Enrico has measured with $\hat{B}$, or Marie has sent a photon in the $|+\rangle$ or $|-\rangle$ state, and Enrico has measured with $\hat{A}$ then their measurement and preparation would be completely random, not correlated. For instance, Marie could have sent a 0 but for 50% of the cases Enrico would be measuring 0 or 1.

Secure quantum communication

In order to make sure that the bit sent by Marie corresponds to what Enrico would measure they do this: Enrico tells Marie which observable he used to measure, and Marie tells Enrico whether he should trust that measurement or not.

Tell me which measurement you did for each photon and I will tell you which are the measurement results that would match what I planned to send.

Right, if you sent $|V\rangle, |H\rangle$ and I measured with $\hat{A}$, or if you send $|+\rangle, |-\rangle$ and I measure with $\hat{B}$, our results will match, Otherwise they will not be correlated.

For example:

Marie sends these 4 different photons in this order

$$|V\rangle, |H\rangle, |+\rangle, |-\rangle$$

and Enrico does the 4 following measurements

$$\hat{A}, \hat{B}, \hat{A}, \hat{B}$$

In this case Marie would tell Enrico to only consider the result of his measurement for the 1st and 4th photon only, because the 2nd and 3rd will not be correlated to what she sent.

Secure quantum communication

Is it true that Plato must leave a trace?

Suppose that Plato intercepts the photon sent by Marie. He does not know whether she sent in the $|V\rangle$, $|H\rangle$ or $|+\rangle$, $|-\rangle$ state. He will chose to measure with $\hat{A}$ or $\hat{B}$.

Suppose he chooses to use the $\hat{A}$ observable and he measures 1.

The state sent by Marie could be $|H\rangle$ or $|+\rangle$ or $|-\rangle$.

Plato cannot be sure.

From the truth table, he knows that there are 50% chances that Marie sent $|H\rangle$, 25% chances she sent $|+\rangle$ and 25% chances she sent $|-\rangle$.

So when he prepares a photon to send to Enrico, he has 50% chances of not sending the photon that Marie sent to Enrico. So Marie and Enrico have a chance of find out that Plato was spying.

Secure quantum communication

At this point Marie and Enrico should have a list of bits which, if nothing strange happened, it should be identical.

But how can they find out if anything bad happened?

They take a portion of the bits that they are confident that they should be equal, and they compare them.

For example Marie and Enrico have 7 photons that, by chance, were measured by Enrico in the correct basis, e.g. the 7 digits 0,1,0,0,1,0,1, and she tells Enrico "Cher Enrico, my first, third and fifth digits are respectively 0, 0 and 1. Do you think that our key is secure or compromised?"

If Enrico digits are indeed 0, 0 and 1 he can say: "Cher Madame Curie, they match perfectly. We can use the other digits as our key. Hurray for quantum mechanics!"

If Enrico digits do not match, then he would say: "Cher Madame Curie, I am afraid that something went wrong. Maybe Plato has tried to copy the message, but he does not know that he cannot do it without us finding out. Hurray for quantum mechanics! Let us do the whole process again."

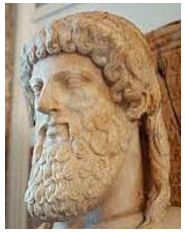
Independent of what happens, it is always: Hurray for quantum mechanics!

Secure quantum communication

Let us go through a guided example of the exchanges between Marie and Enrico, and what Plato could also do.

(1)

I send Enrico the photon $|H\rangle$



(2)

I intercepted Marie's photon.

I used the $\hat{A}$ basis and got 1.

I don't know what Marie sent, but I know it is not $|V\rangle$.

I'll prepare the state $|+\rangle$ and send it to Enrico while he thinks it is from Marie.

(3)

I received a photon. Let us use the $\hat{A}$ basis this time.

Let us measure it.

Ok, I got a 0.

Secure quantum communication

Hi Marie, I used the observable $\hat{A}$. Should I keep this data point or discard it?

(4)

(good, with $\hat{A}$ he can get the correct data point).

Hi Enrico, you can keep that data point. You measured in the correct direction.

(5)

By the way Enrico, what did you actually measure for this photon?

(6)

Hi Marie, I got a 0.

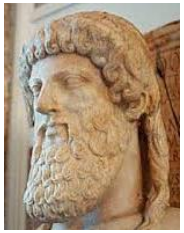
(7)

Oh no! Something is wrong.

Plato may have been spying on us.

Let us start again!

(8)



Oh no, I am too classic to compete with them!

(9)

As we have seen, Plato cannot try to measure what Marie has sent and resend it, because Marie and Enrico have a good chance to find out if they do their checks properly.

Maybe he could decide to make a copy of it instead?

We are going to show later that copying is not possible in quantum mechanics!

Secure quantum communication

What we just discussed is known as the BB84 protocol because it was invented in 1984 by Bennet and Brassard.

To summarize:

1) Marie sends Enrico photons in one of 4 different states chosen randomly
2) Enrico measures in one of 2 basis also chosen randomly
3) Enrico tells Marie which measurement he did
4) Marie tell Enrico which of the measurements he did he should consider and all the others are discarded
5) Of the data that is preserved, Enrico and Marie share a small portion, and they check that there is perfect match. If there is a match, they use the portion that they have not shared as their key. In case there is no match, it could be a sign that either their experimental apparatus has problems, or that Plato has tried to spy on them.

All of this is based on the fact that if Plato is not able to just copy the message; and if he tries to measure it, he may alter the state.

Fun Fact: After BB84, the most famous quantum cryptography protocol is E91, invented by Artur Ekert in 1991. Artur Ekert is a Prof in Oxford and at NUS, and has been the director of the Centre for Quantum Technologies in Singapore for more than 10 years.

Case Problem 1.1

Suppose Marie sends the following 10 photons $|H\rangle, |+\rangle, |V\rangle, |+\rangle, |-\rangle, |H\rangle, |H\rangle, |V\rangle, |-\rangle, |-\rangle$ and Enrico measures with the following observables $\hat{A}, \hat{A}, \hat{B}, \hat{A}, \hat{B}, \hat{B}, \hat{A}, \hat{B}, \hat{A}, \hat{A}$ and he obtains the following results $1,1,0,0,0,1,1,0,0,1$

1) After Enrico shares with Marie the measurements that he has done, what digits will Marie ask him to consider, and which ones to discard?

2) From the data, would you be able to detect an anomaly? If not, which is the key?

Case Problem 1.1: solution

Marie will ask Enrico to consider the measurements in a basis in which her photons give either 0 or 1 with 100% probability. If there are no anomalies, Enrico should measure 1 for $|H\rangle$ in basis $\hat{A}$ and for $|+\rangle$ in basis $\hat{B}$, and 0 for $|V\rangle$ in basis $\hat{A}$ and $|-\rangle$ in basis $\hat{B}$.

Let us make a table

Photon	Measurement	Keep?	Result of measurement	Anomaly?
$\|H\rangle$	$\hat{A}$	yes	1	no
$\|+\rangle$	$\hat{A}$	no		
$\|V\rangle$	$\hat{B}$	no		
$\|+\rangle$	$\hat{A}$	no		
$\|-\rangle$	$\hat{B}$	yes	0	no
$\|H\rangle$	$\hat{B}$	no		
$\|H\rangle$	$\hat{A}$	yes	1	no
$\|V\rangle$	$\hat{B}$	no		
$\|-\rangle$	$\hat{A}$	no		
$\|-\rangle$	$\hat{A}$	no		

There are no anomalies … so transmission may be secure.

Case Problem 1.2

Suppose Marie sends the following 10 photons $|H\rangle, |+\rangle, |+\rangle, |V\rangle, |H\rangle, |-\rangle, |H\rangle, |-\rangle, |V\rangle, |-\rangle$ and Enrico measures with the following observables $\hat{A}, \hat{A}, \hat{B}, \hat{A}, \hat{B}, \hat{B}, \hat{A}, \hat{B}, \hat{A}, \hat{A}$ and he obtains the following results $1,1,0,0,0,0,1,0,0,1$

1) After Enrico shares with Marie the measurements that he has done, what digits will Marie ask him to consider, and which ones to discard?

2) From the data, would you be able to detect an anomaly? If not, which is the key?

Case Problem 1.2: solution

Marie will ask Enrico to consider the measurements in a basis in which her photons give either 0 or 1 with 100% probability. If there are no anomalies, Enrico should measure 1 for $|H\rangle$ in basis $\hat{A}$ and for $|+\rangle$ in basis $\hat{B}$, and 0 for $|V\rangle$ in basis $\hat{A}$ and $|-\rangle$ in basis $\hat{B}$.

Let us make a table

Photon	Measurement	Keep?	Result of measurement	Anomaly?
$\|H\rangle$	$\hat{A}$	yes	1	no
$\|+\rangle$	$\hat{A}$	no		
$\|+\rangle$	$\hat{B}$	yes	0	**yes**
$\|V\rangle$	$\hat{A}$	yes	0	no
$\|H\rangle$	$\hat{B}$	no		no
$\|-\rangle$	$\hat{B}$	yes	0	no
$\|H\rangle$	$\hat{A}$	yes	1	no
$\|-\rangle$	$\hat{B}$	yes	0	no
$\|V\rangle$	$\hat{A}$	yes	0	no
$\|-\rangle$	$\hat{A}$	no		

There are 1 anomaly … so transmission may have been compromised.

More fun problems on quantum cryptography?

Head to

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html

and test yourself.

Note that here Marie and Enrico are (boringly) called Alice and Bob, and Plato is called (Eve).

Also they use Z and X basis instead of A and B (but they have the same meaning … so do not worry and jump on it!)

Concept 2: More two-level systems and no-cloning theorem

More two-level systems

So far we have considered single entities.

Some fantastic properties of quantum mechanics can only be addressed when discussing more than one two-level system.

Here we show you how to deal with few entities and it is not difficult to extend beyond that.

Here we are going to

1) Give an idea of why the capacity of quantum computer memories is very much larger than for classical computers
2) Give a derivation of the no cloning theorem

More two-level systems

The key is to study 2 two-level systems is to think of the 2 entities as a single one but larger, and figure out how to play with it.

To make things concrete we consider a source which produces 2 photons at the time.

One photon can be in the state $|H\rangle$ or $|V\rangle$, and the other as well.

So the two photons could be in the states

$$|H\rangle_1|H\rangle_2, \qquad |H\rangle_1|V\rangle_2, \qquad |V\rangle_1|H\rangle_2, \qquad |V\rangle_1|V\rangle_2$$

(where we have use the sub-index $|a\rangle_{1\ or\ 2}$ to denote which 2-level system is in state $|a\rangle$), or in any superpositions of these four states

$$|\psi\rangle = a_{HH}\,|H\rangle_1|H\rangle_2 + a_{HV}|H\rangle_1|V\rangle_2 + a_{VH}|V\rangle_1|H\rangle_2 + a_{VV}|V\rangle_1|V\rangle_2$$

(where a_{ij} is a complex number and $\sum_{i,j}\left|a_{ij}\right|^2 = 1$)

so now the state that represent 2 two-level systems is made of a basis with 4 states.

It is a effectively a four-level system.

More two-level systems

If the source would be producing three photons, then there would be $2^3 = 8$ possible configurations

$$|\psi\rangle = a_{HHH}|H\rangle_1|H\rangle_2|H\rangle_3 + a_{HHV}|H\rangle_1|H\rangle_2|V\rangle_3 + a_{HVH}|H\rangle_1|V\rangle_2|H\rangle_3 + a_{HVV}|H\rangle_1|V\rangle_2|V\rangle_3 + a_{VHH}|V\rangle_1|H\rangle_2|H\rangle_3 + a_{VHV}|V\rangle_1|H\rangle_2|V\rangle_3 + a_{VVH}|V\rangle_1|V\rangle_2|H\rangle_3 + a_{VVV}|V\rangle_1|V\rangle_2|V\rangle_3$$

Hence the state vector representing a collection of L two-level systems would have a dimension 2^L.

More two-level systems

The state vector of any collection of L two-level systems has a dimension of 2^L.

For example atoms in double wells (which we has seen before), but also double quantum dots etc….

Let us discuss the use of two-level systems for memory (when dealing with computing and information, a two-level system is referred to as qubit).

In classical computer, we have seen, one just needs to store a sequence of 0 and 1 to store information. In the computer, each bit of information is just a 0 or a 1.

So L bits only store one possible combination of 0 and 1.

For example give 8 bits you can only store a single combination like 01100101 or 10101001.

If we consider L qubits, they can represent a superposition with complex amplitudes of 2^L of the combinations of 0 and 1.

So in a quantum computer you can store something very different which contains a lot more information … you are actually storing the 2^L coefficients.

More two-level systems

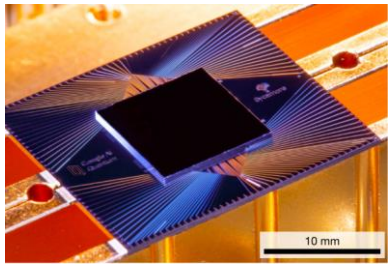
Suppose one takes a computer with 50 qubits and generates a state which is a combination of all these 2^{50} possible configurations … then there is just not enough RAM in any classical supercomputer to represent that state!!!

2^{50} is about the number of atoms on earth. It really is a huge number.

This indicates both how much more complex can quantum mechanics be compared to classical physics.

This also shows that a quantum computer with just 50 qubits could (ideally) do things that no other computer can do.

In 2019 Google made a quantum computation which no supercomputer had been able to perform yet, something people referred to as a first proof of Quantum Supremacy (what a fancy word!!). Very recently a classical computer was able to do the same computation … so quantum supremacy may have not been reached yet … but it is just a matter of time.

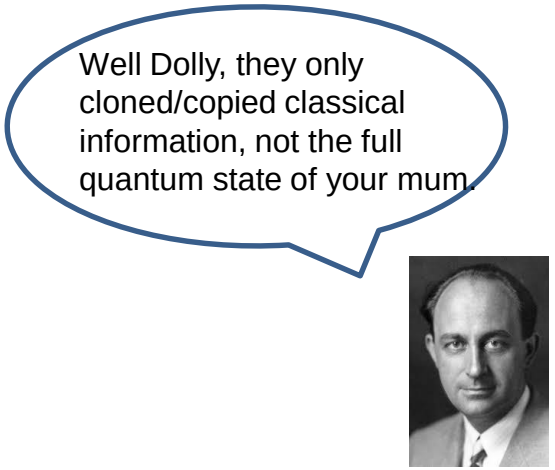


Google quantum computing processor with 54 qubits.

Warning: the computation done for quantum supremacy is completely useless … for a practically useful application of a quantum computer we have to wait between a few month to a few years (hopefully).

More two-level systems

Studying just 2 two-level systems one can also proof something we have mentioned earlier, i.e. that it is not possible to copy quantum states, also known as the no-cloning theorem.



We illustrate here a special case of the theorem.

Let us suppose that Marie prepared the photon in the superposition state

$$|\psi\rangle_M = \alpha|H\rangle_M + \beta|V\rangle_M$$

Plato has the state $|H\rangle_P$ and would like to turn it into the copy of Marie's state. More precisely he would like to do the operation $\hat{U}$ which does the following

$$\hat{U}\,|\psi\rangle_M|H\rangle_P = |\psi\rangle_M|\psi\rangle_P$$

The state of Marie has been copied on the state of Plato via the action of $\hat{U}$.

No-cloning theorem

Since $\hat{U}$ is linear (all operations in quantum mechanics, except for measurement are linear), one can do the copy in two different ways and they should give the same result.

1) Copy the whole state $|\psi\rangle_M$

$$\hat{U}\,|\psi\rangle_M|H\rangle_P = |\psi\rangle_M|\psi\rangle_P = (\alpha|H\rangle_M + \beta|V\rangle_M)(\alpha|H\rangle_P + \beta|V\rangle_P)$$
$$= \alpha^2\,|H\rangle_M\,|H\rangle_P + \alpha\beta\,|H\rangle_M\,|V\rangle_P + \alpha\beta|V\rangle_M\,|H\rangle_P + \beta^2\,|V\rangle_M\,|V\rangle_P$$

2) Copy each elements of the superposition $|\psi\rangle_M = \alpha|H\rangle_M + \beta|V\rangle_M$ one at the time

$$\hat{U}\,|\psi\rangle_M|H\rangle_P = \hat{U}(\alpha|H\rangle_M + \beta|V\rangle_M)|H\rangle_P$$
$$= \alpha\,\hat{U}|H\rangle_M|H\rangle_P + \beta\hat{U}|V\rangle_M|H\rangle_P$$
$$= \alpha\,|H\rangle_M|H\rangle_P + \beta|V\rangle_M|V\rangle_P$$

The results in 1) and 2) should be the same for any values of α and β, but the two states are the same only if $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ and $\beta = 1$.

Hence Plato cannot simply copy the key.

Case problem 2.1 (Extra problem)

Consider the state $|\psi\rangle_M\ |\psi\rangle_E$ where $|\psi\rangle_M = 1/2|V\rangle_M + \sqrt{3/4}|H\rangle_M$ and $|\psi\rangle_E = \sqrt{5/6}|V\rangle_E - 1/\sqrt{6}|H\rangle_E$.

What is the probability corresponding to each of the basis elements $|V\rangle_M|V\rangle_E$, $|H\rangle_M|V\rangle_E$, $|V\rangle_M|H\rangle_E$, $|H\rangle_M|H\rangle_E$?

Case problem 2.1 (Extra problem): solution

Considering the state $|\psi\rangle_M\,|\psi\rangle_E$ where $|\psi\rangle_M = 1/2|V\rangle_M + \sqrt{3/4}|H\rangle_M$ and $|\psi\rangle_E = \sqrt{5/6}|V\rangle_E - 1/\sqrt{6}|H\rangle_E$ we get

$$\left(1/2|V\rangle_M + \sqrt{3/4}|H\rangle_M\right)\left(\sqrt{5/6}|V\rangle_E - 1/\sqrt{6}|H\rangle_E\right)$$
$$= \sqrt{5/24}|V\rangle_M|V\rangle_E + \sqrt{5/8}|H\rangle_M|V\rangle_E - \sqrt{1/24}|V\rangle_M|H\rangle_E - \sqrt{1/8}|H\rangle_M|H\rangle_E$$

The probability is given by the modulus square of the coefficient multiplying the basis, hence we get

$5/24$ for $|V\rangle_M|V\rangle_E$
$5/8$ for $|H\rangle_M|V\rangle_E$
$1/24$ for $|V\rangle_M|H\rangle_E$
$1/8$ for $|H\rangle_M|H\rangle_E$

Case problem 2.2 (Extra problem)

Consider a pair of photons prepared in the state $|\psi\rangle = |+\rangle_M |V\rangle_E$ with $|+\rangle_M = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$ and $|V\rangle_E = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and the observable $\hat{A}_M = |H\rangle_M\langle H| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ acting only on Marie's photon, and the observable $\hat{B}_E = |-\rangle_E\langle -| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ only acting on the Enrico's photon.

What is the average output $\langle\psi|\hat{A}_M\hat{B}_E|\psi\rangle$?

Hint: for generic $|\psi\rangle = |\psi_1\rangle_1|\psi_2\rangle_2$, and observables $\hat{A}_1$ and $\hat{A}_2$, one gets

$$\langle\psi|\hat{A}_1\hat{A}_2|\psi\rangle = \langle\psi_1|_1\langle\psi_2|_2\hat{A}_1\hat{A}_2|\psi_1\rangle_1|\psi_2\rangle_2 = \langle\psi_1|\hat{A}_1|\psi_1\rangle_1\langle\psi_2|\hat{A}_2|\psi_2\rangle_2$$

Case problem 2.2 (Extra problem): solution

Using the hint we get

$$\langle\psi|\hat{A}_M\hat{B}_E|\psi\rangle = \langle +|\hat{A}_M|+\rangle_M\langle V|\hat{B}_E|V\rangle_E$$

$$= \left[\begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}\right] \times \left[\frac{1}{2}\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\right]$$

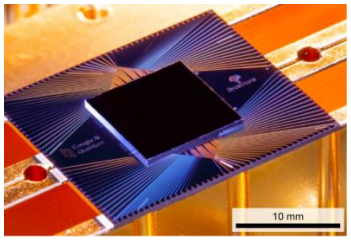
$$= \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

Application: Quantum computers

Quantum computers

We have already mentioned quantum computers.

We have seen that Google has been able to do a calculation that is extremely difficult for a classical computer.



Google quantum computing process with 54 qubits.

We shall mention now two other highlights of research on quantum computing:

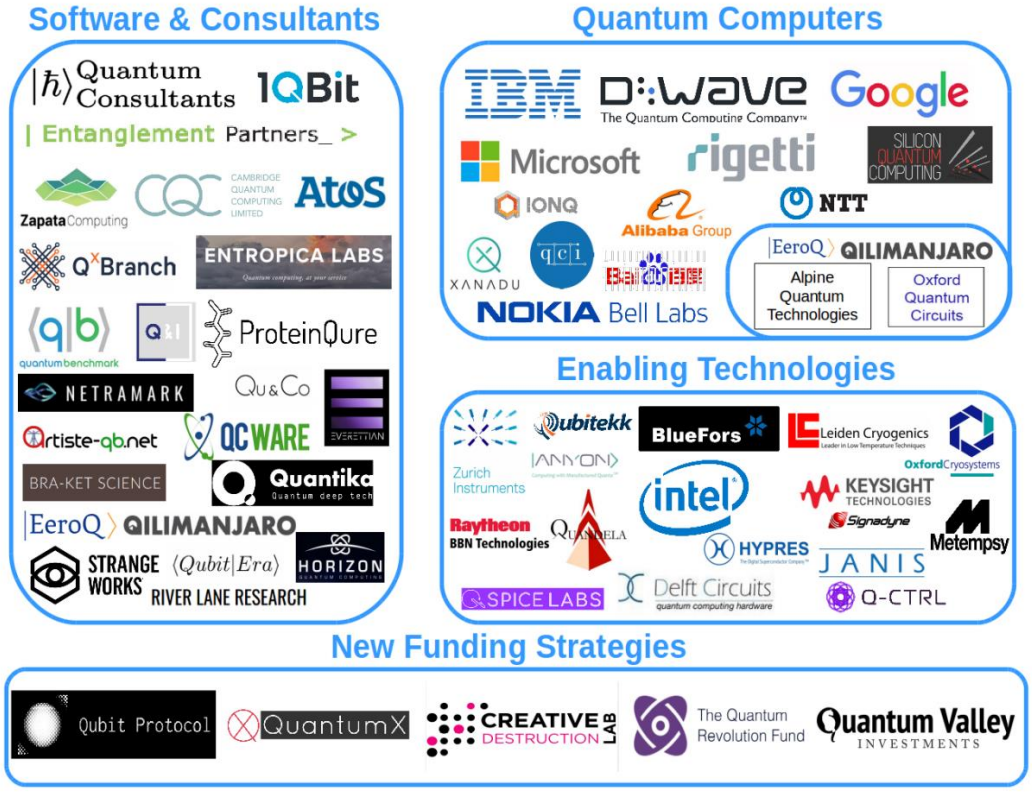
1) There exist some algorithms for quantum computer which, if they were implemented, would be able to do computation in a time which is exponentially faster than classical computers (for instance the Shor algorithm to find the prime factors of a number). Exponentially faster means that if a quantum computer takes a time t, a classical computer would take a time e^t
2) People have found new hybrid classical-quantum computers algorithms which can be exponentially faster than just classical algorithms. These algorithms have applications in chemistry, pharmacy, material science, finance etc.

More and better algorithms need to be found, and better and bigger quantum computers need to be built … for now you can play with IBM quantum computer on the cloud

https://quantum-computing.ibm.com/

Quantum computers

There are more and more quantum computing companies around the world. Join one of the companies facing these scientific and engineering/design challenges (also in Singapore)!!



The CEOs of these two local quantum computing companies were both in SUTD!

Quantum computers

There are more and more quantum computing companies around the world. Join one of the companies facing these scientific and engineering/design challenges (also in Singapore)!!

Software & Consultants

Quantum Computers

Enabling Technologies

New Funding Strategies

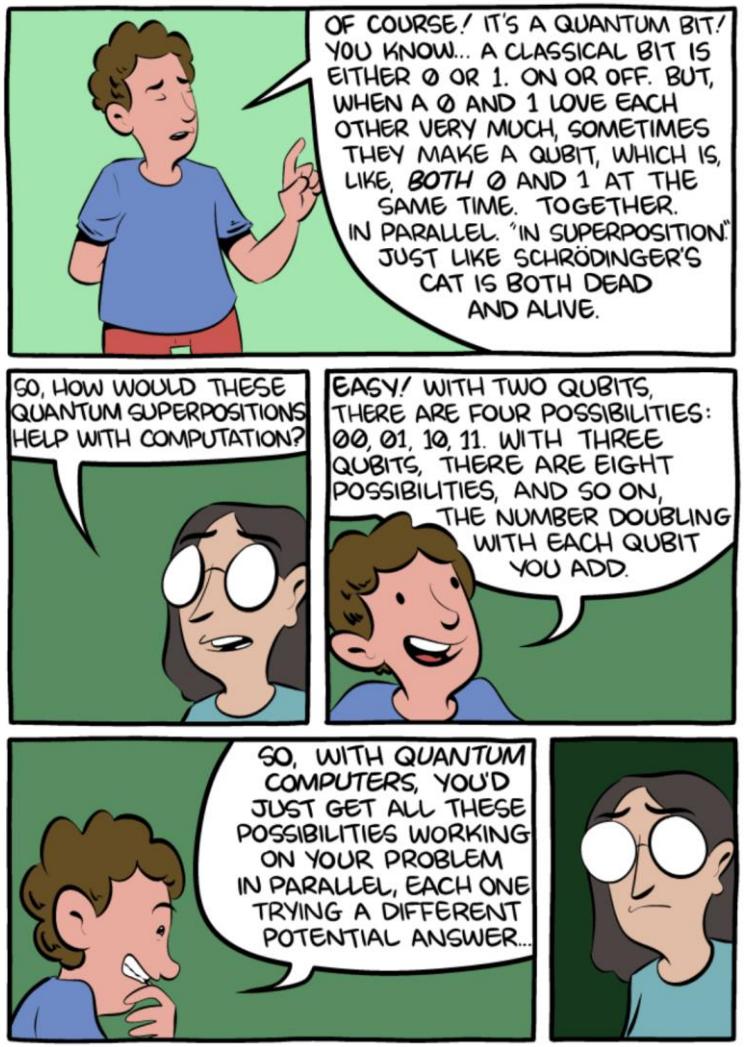
Numerous perspectives for engineers and computer scientists!

And architects: shape the future quantum data centres!!!

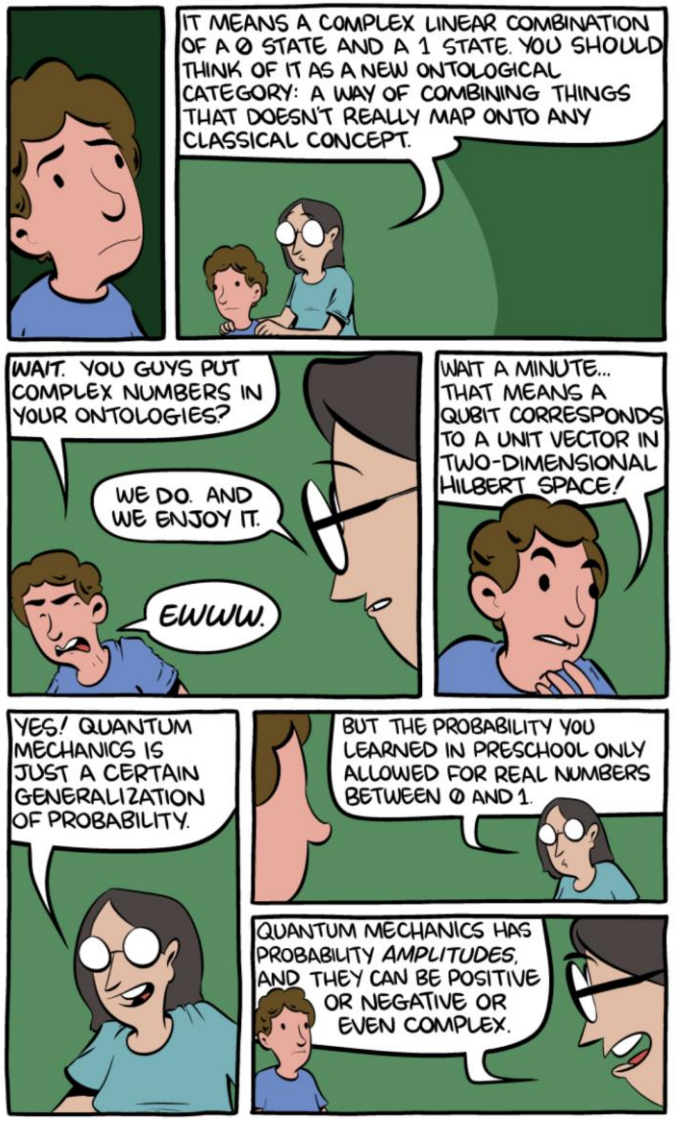
Quantum computers

We shall conclude with the quantum computing talk

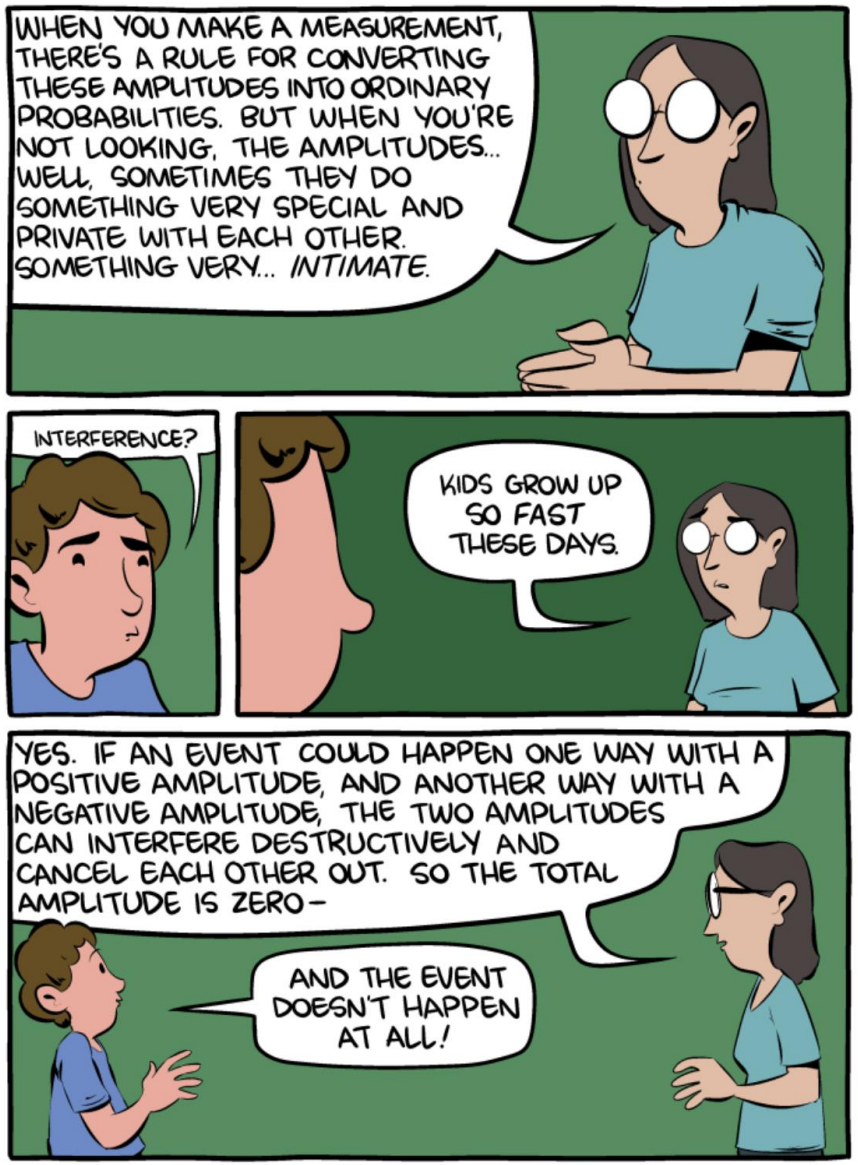
https://www.smbc-comics.com/comic/the-talk-3

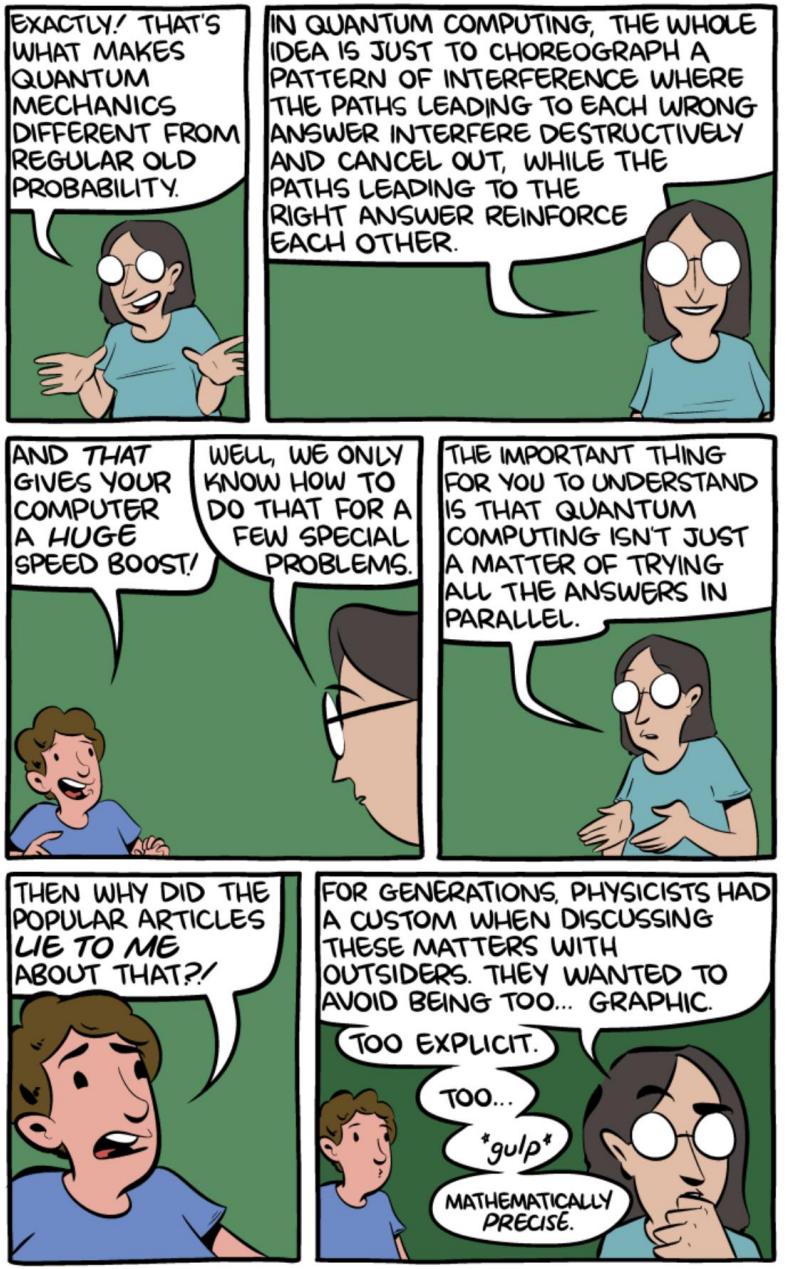


Quantum computers

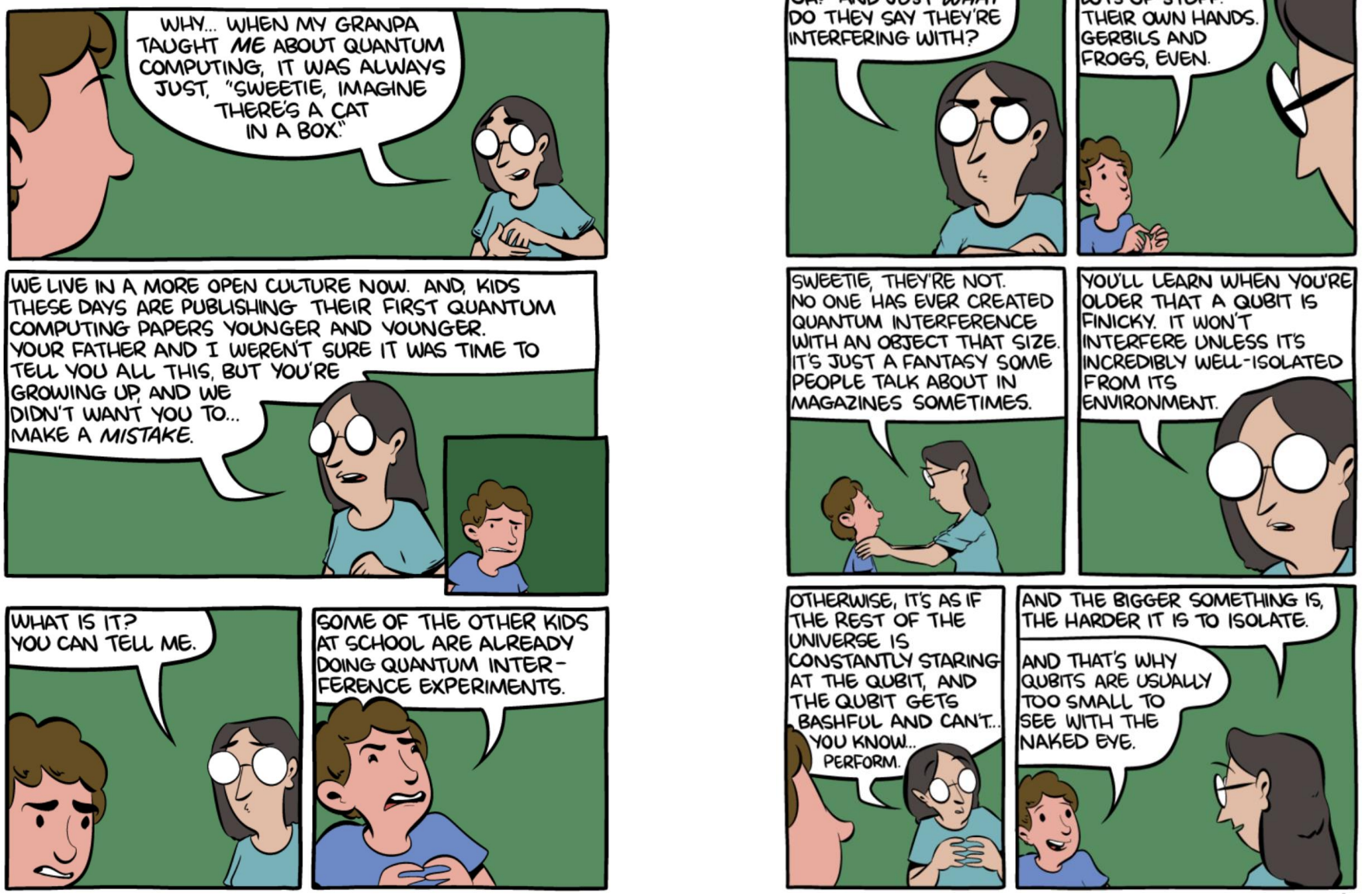


Quantum computers

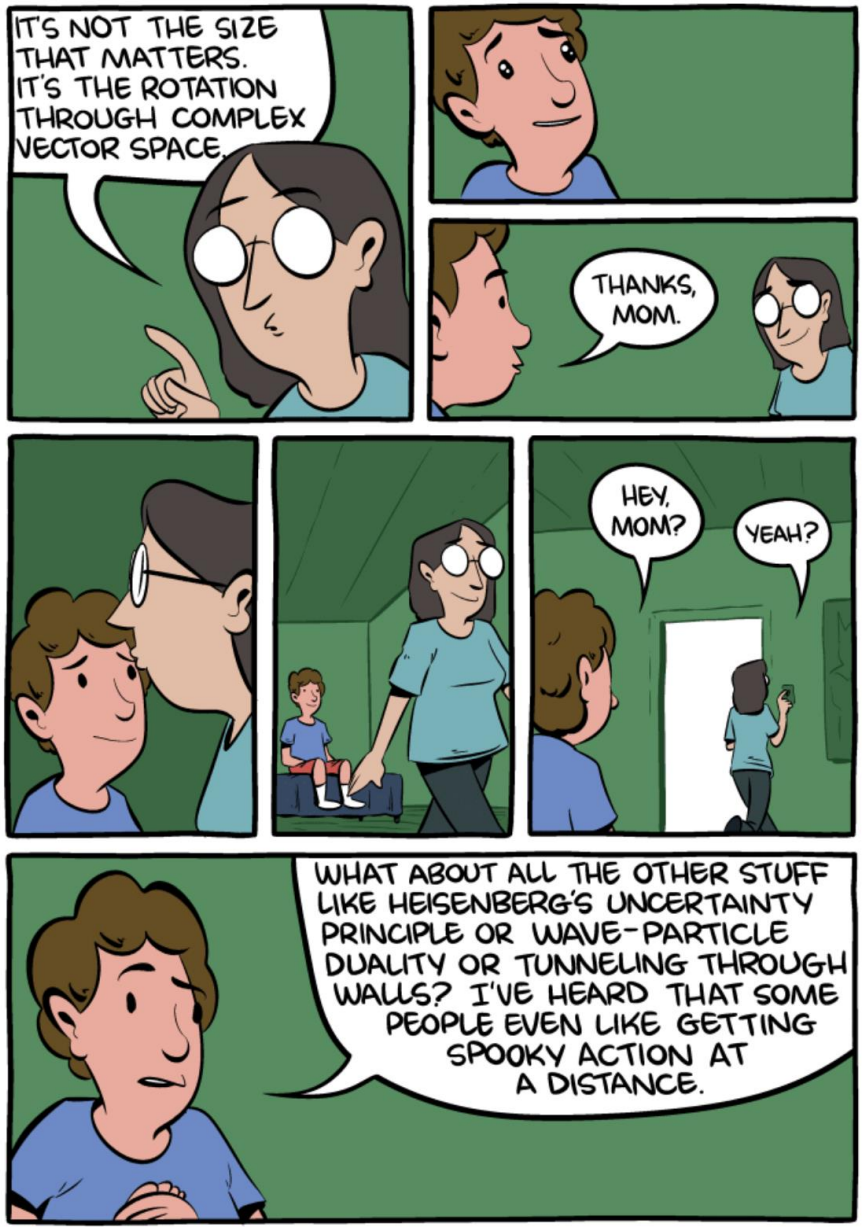




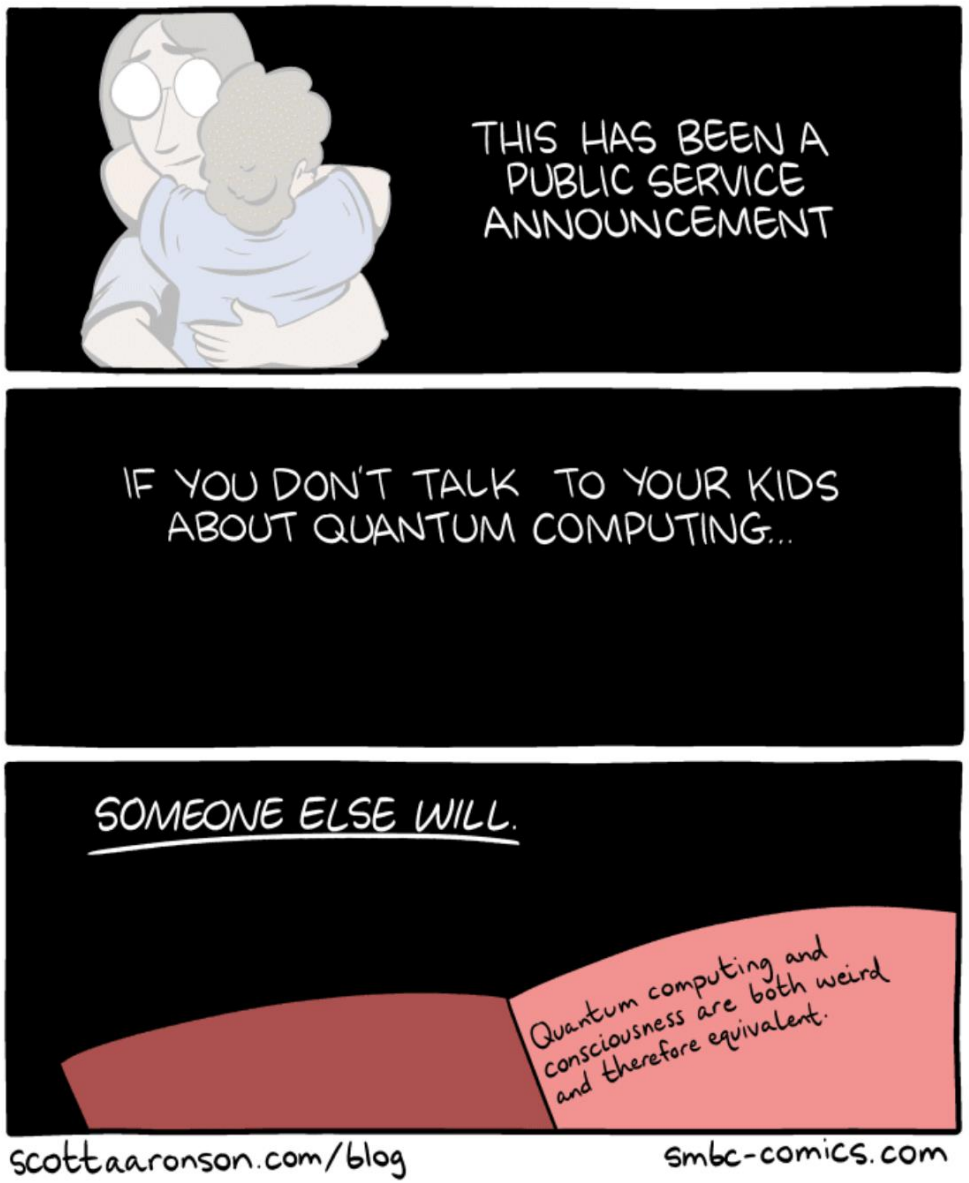
Quantum computers



Quantum computers



Quantum computers



Time to revise the quantum mechanics part

Some fun and good videos to watch

https://www.youtube.com/watch?v=ZuvK-od647c&feature=youtu.be

https://www.youtube.com/watch?v=zcqZHYo7ONs&feature=youtu.be

https://www.youtube.com/watch?v=MzRCDLre1b4