Programs: From Monads to the Quantum Computer From Contemporary CS to Contemporary Physics

Cem Bozşahin, Cognitive Science, METU

for a Course on Philosophy of Computer Science

April 14, 2022

- We have seen that algorithms are nice and succint ways to express ideas to other people.
- We can leave some bits to the interpreter, because, after all, they can independently operate to see for themselves.
- You would be amazed to find out how much of so-called 'formal notation' leaves a lot to the interpreter, see Hadamard (1945), Ganesalingam (2013).
- But it is at the level of a program that a computer scientist puts herself in computer's shoes.
  - We can talk about a list structure at the level of an algorithm without needing details.
  - We can talk about a conditional at the level of an algorithm without being specific about how it is carried out.
  - In a program, we can do neither. We need to be specific.

- This shoe is designed by us.
- Therefore we are trying to see what kind of control and data structures can be passed on to the computer for itself to independently operate.
- There is no homunculi inside to interpret things which the designer has not thought of.
- When it operates, it is attempting a human problem. At least today's computers do so (see Bozşahin 2018 for discussion.)

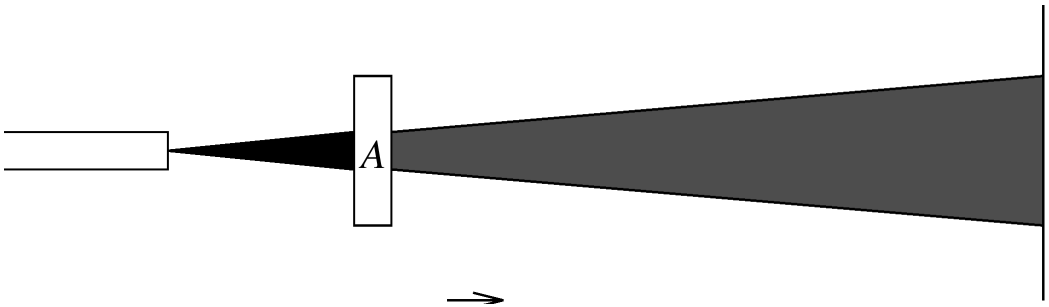
- We have seen that a digital computer has to be designed to operate within certain limits (encoding, decoding, instruction set, etc.)
- Everything in a digital computer has to translate to its native instruction set for it to operate.
- The instruction set is designed by us, with careful engineering.
- so that a programmer can know what is wrong if something goes wrong.

- The same goes for the analog computer. They have to be designed to interpret the analog device (e.g. a conducting foam) within certain limits.
- Otherwise, an analog program (usually called an analog, rather than program) cannot be fixed if there's something wrong with it. See Rubel (1993), Mills (2008).

- What about the quantum computer? Is it designed, or is it 'the quantum nature computes'?
- I am not the right person to talk about the quantum computer in detail, but here we go about the 'kitchen view',
- I am summarizing from Rieffel and Polak (2000), Arora and Barak (2009).

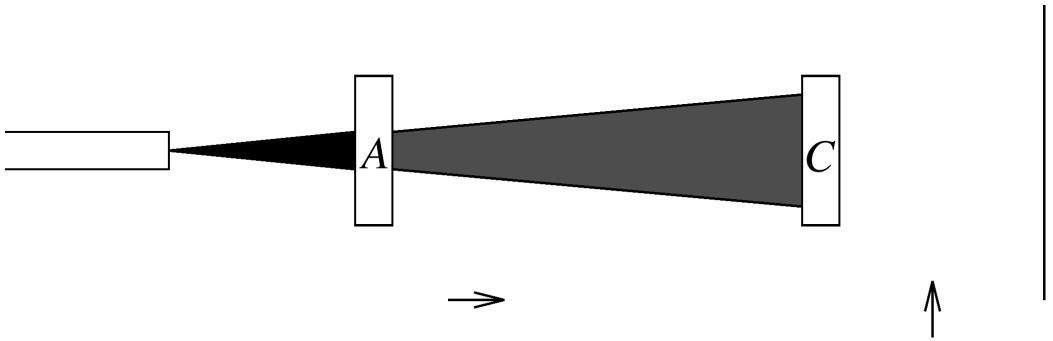
Photon polarization

- Photons are the only particles we can observe directly.
- Polarizers are optical filters which let light waves of certain polarization to pass through, blocking others.
- One experiment: a strong light source (e.g. laser pointer), three polaroids (filters): Filters A, B and C.
- A: horizontal polarizer, B: 45 degrees, C: vertical
- First, insert Filter A between the laser source and a projection screen.



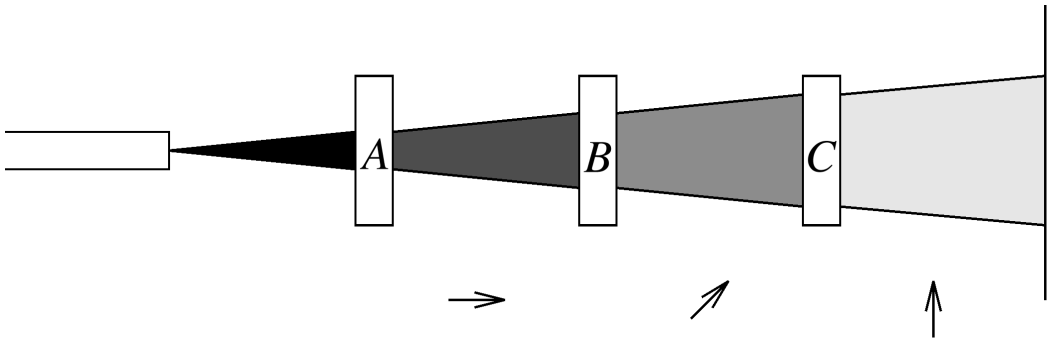
- Assuming that incoming light is randomly polarized, the intensity of the output (i.e. number of photons passed) will be half the intensity of incoming light.
- All outgoing photons are horizontally polarized.
- Filter A cannot be a simple sieve, letting only already horizontally polarized photons.
- Because, if that were the case, only a few of the randomly polarized incoming electrons would be horizontally polarized.
- We would expect much larger attenuation (cutoff) if that were the case. The filter is DOING something. Or nature does something to the filter.

Now insert Filter C (vertical polarizer)



- The intensity of the output drops to zero. The output of A is all horizontally polarized, all blocked by C.
- So far not much of a surprise.

Now insert Filter B between A and C:

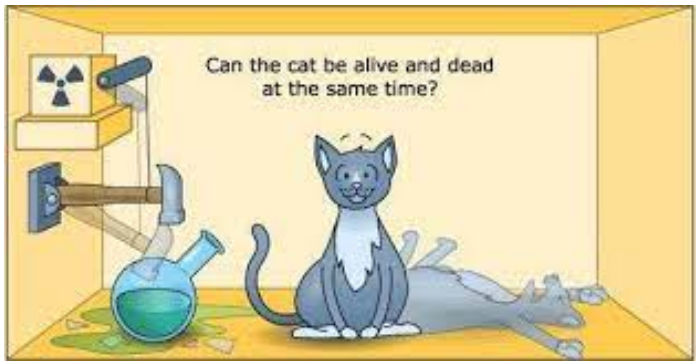


- The output intensity is NOT zero. What is going on?
- It turns out that the intensity of output is 1/8th of the incoming light.
- This is a counterintuitive result. We would expect intensity to decrease, not increase, if we add more filters.
- To understand the quantum computer, we need to understand the representational potential of this counterintuitive result.

Representation in quantum mechanics

- The state space of a quantum system, consisting of positions, momentums, polarization, spin, angular momentum etc. is modeled by Hilbert space of wave functions. These are not finite dimensional.
- Let's look at finite-dimensional complex vector spaces for the purpose of quantum computing.
- Dirac's bra-ket notation for quantum states is a very asymmetric notation which continues to horrify some computer scientists.

- The abstract wave function is represented as a ket, e.g.: $|\rightarrow\rangle$ for the horizontal polarizer A. You make up the vector name.
- Schrödinger was very creative, he had $|alive\rangle$ and $|dead\rangle$ for cats.



- Kets are column vectors. For example $|0\rangle$ can be $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle$ can be $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Other representations are possible, as long as we are consistent. E.g. we can swap definitions of $|0\rangle$ and $|1\rangle$.

- Bras are conjugate transposes of kets. For example $\langle 0| = (1 \;\; 0)$ and $\langle 1| = (0 \;\; 1)$
- They are row vectors
- We can multiply bras and kets as in matrix algebra, e.g.
  $|0\rangle \langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0 \;\; 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\langle 0||0\rangle = (1 \;\; 0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$
- $\langle 0| \, |1\rangle = (1 \;\; 0) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$ also written $\langle 0|1\rangle$
- $\langle 1| \, |1\rangle = (0 \;\; 1) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1$ $\langle 1|1\rangle$
- ket-bra is a matrix, bra-ket is a number. Ket and bra are vectors. Ket-ket is tensor product ($\otimes$). Bra-bra is not tensor-unique. (lessons for CS: what to encode/decode)

- Any matrix-vector algebra is fine, e.g. $|0\rangle \langle 0|1\rangle = |0\rangle 0$, which we write by convention as vector with a coefficient 0: $0\,|0\rangle$
- $0\,|0\rangle = 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
- Representation and numbers: Coefficients (e.g. 0 above) can be complex numbers. That seems to be required given our current understanding of real and complex numbers, and, nature, with them.
- NB. Bras are not simply transposes, they are conjugate transposes.
- Why do we need the conjugate transpose? The imaginary coefficient of a complex number corresponds to circular polarization. (i.e. it is there in the input light).
- We are here studying what we must encode and decode.

Complex coefficients and real results

- Let $|a\rangle = \begin{pmatrix} 2+3i \\ 6-5i \\ 9+i \end{pmatrix}$ $\langle a|$ is complex conjugate, transposed
- then $\langle a|a\rangle = (2-3i \;\; 6+5i \;\; 9-i) \begin{pmatrix} 2+3i \\ 6-5i \\ 9+i \end{pmatrix} =$

  $(2-3i)(2+3i) + (6+5i)(6-5i) + (9-i)(9+i) =$

  $4+6i-6i-9i^2+36-30i+30i-25i^2+81+9i-9i-i^2 =$

  $4+9+36+25+81+1 \qquad (i^2=-1)$
- More lessons for CS: intensions (e.g. i) are nice. Extensions are what we interpret.

- A quantum system consists of one particle: states of the system are wave functions (vectors), and observables are operators (matrices).
- There are infinitely many states, and arbitrarily largely many are computable.
- Multiple systems (bits, particles) need one more representational support: tensor product of matrices-vectors

Tensor product

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}_A^{m\times n} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}_B^{p\times q} = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}_{A\otimes B}^{mp\times nq}$$

$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

This is an idealization. We are assuming that quantum systems are closed, and continue to be closed when combined.

Engineering of that is a huge challenge in computer engineering.

We assume it holds in nature. Maybe it doesn't.

- ket-ket example: we get another ket, with combined dimension

$$|0\rangle\,|1\rangle = |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

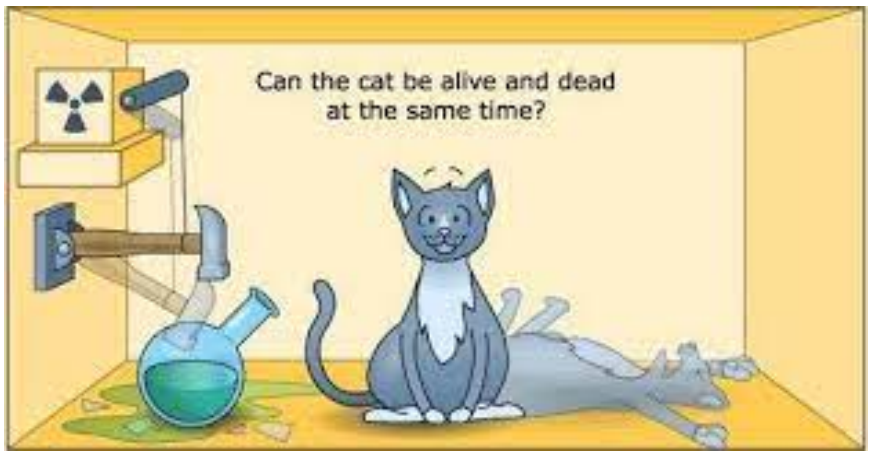
- bra-bra is not tensor-unique:
  $\langle 0|\,\langle 1| =? \langle 0| \otimes \langle 1| =? \langle 01| =??(1 \;\; 0) \otimes (0 \;\; 1) =??(0 \;\; 1 \;\; 0 \;\; 0)$
  $??(0 \;\; 0 \;\; 1 \;\; 0)$
- Unless we interpret tensor product as Kronecker product.
- Puritans take note: That's because a tensor product is an equivalence class over matrices, whereas the Kronecker product always yields a unique matrix.
- So, we've been doing Kronecker product when we said tensor product. Welcome to math confusion.

- Lessons for CS: The representational support is there to facilitate encoding and decoding.
- Hmm. Is $\langle 01|01\rangle$ bad then, if $\langle 01|$ is weird?
- Didn't we just say we have $\langle a|$ and $\langle a|a\rangle$, for any a, if we have $|a\rangle$?
- And physicists and mathematicians do talk about stuff like $\langle 01|$: Nannicini (2020).
- $\langle 01|$ is actually the Kronecker product $\odot$, not tensor product $\otimes$.
- $\langle 01| = \langle 0| \odot \langle 1| = (1 \;\; 0) \odot (0 \;\; 1) = (0 \;\; 1 \;\; 0 \;\; 0)$

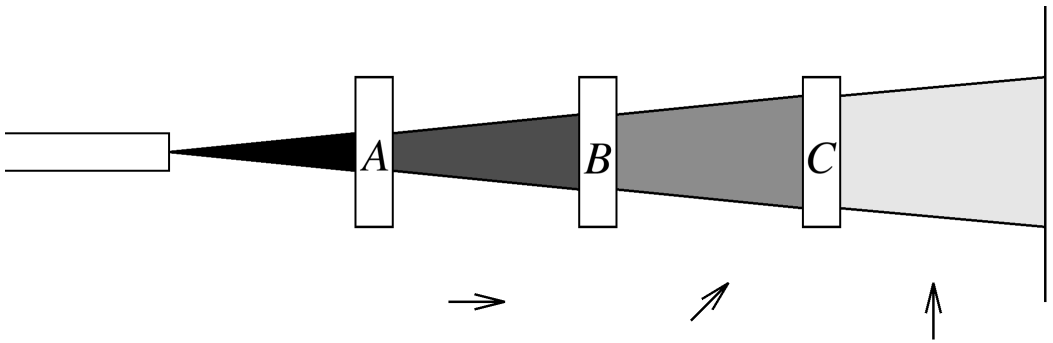
- $\otimes$ and $\odot$ are related but different, both increasing dimension (unlike matrix and Hadamard products).
- Both are compositional.
- Kronecker gives a unique result.
- Write $\otimes$ when we mean $\odot$? Better not write anything to baffle future generations. CS nitpicking;)
- And, KroneckerFarm won't catch on but TensorFarm is cool.
- Just like Schönfinkeling is unheard of (except in secret sects of CS) but Currying is very popular.

Back to the counterintuitive result

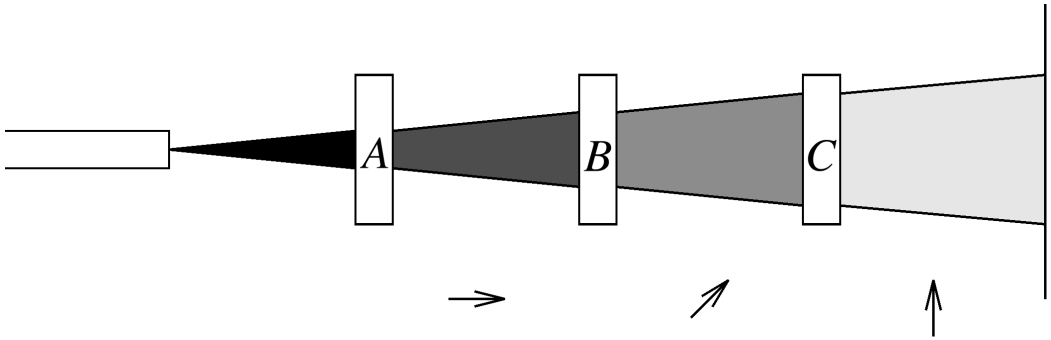
- We have done all this to make sense of the counterintuitive result.
- And I was kidding about vectors doing something by their names, cf. Schrödinger. What they do is determined by their interpretation.
- For the cat, we have $\frac{1}{\sqrt{2}}|dead\rangle + \frac{1}{\sqrt{2}}|alive\rangle$



What about photon polarization?



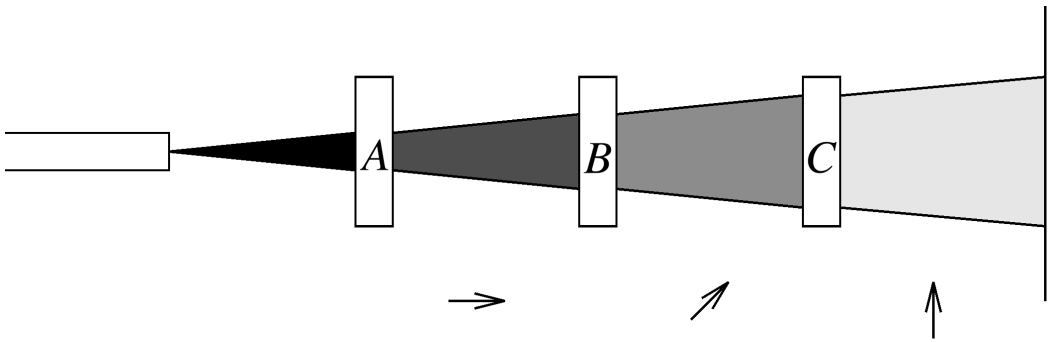
- Arbitrary input polarization, given A, B, C filters, requires measurement bases for them. After all, they are instruments with certain properties.



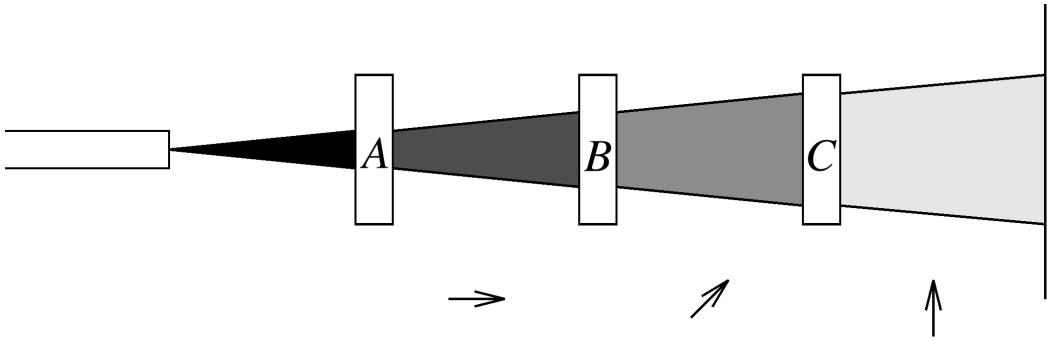
- Let's assume a polarizer measures the quantum state of photons in its (1) polarization direction; (2) and its orthogonal polarization, i.e.
- A is $a_1 |\rightarrow\rangle + a_2 |\uparrow\rangle$ recall: a_j, b_j, c_j are numbers
- B is $b_1 |\nearrow\rangle + b_2 |\nwarrow\rangle$
- C is $c_1 |\uparrow\rangle + c_2 |\rightarrow\rangle$
- We care about direction of polarization only, i.e.:

$$| a_1 |^2 + | a_2 |^2 = 1 \quad | b_1 |^2 + | b_2 |^2 = 1 \quad | c_1 |^2 + | c_2 |^2 = 1$$

for example $a_j, b_j, c_j = \frac{1}{\sqrt{2}}$



- Filter B's $|\nearrow\rangle$ and $|\nwarrow\rangle$ can be described using others, respectively as
- $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$ and $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$
- Check that the math adds up to 1. We have $\sum_{1}^{4}(\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}})^2$



- Now, the counterintuitive result of measuring 1/8th of incoming photons on screen is:
- Photons passing thru A are in state $|\rightarrow\rangle$. That's 1/2 of incoming photons.
- Photons passing thru B are in state $|\nearrow\rangle$. That's 1/2 of photons coming from A, or 1/4 of incoming photons.
- Photons passing thru C are in state $|\uparrow\rangle$. That's 1/2 of photons coming from B, or 1/8 of incoming photons.

Are we reasoning backwards?

- Did we just make up gadgets to match an observed result?
- Pessimists and agnostics: yes.
- Virtually all others: No.
  - We extended our theoretical vocabulary, and solidified our encoding/decoding (hopefully), to take on hitherto untackled problems. We can avoid overfitting the result, unless we cheat. Quantum healers beware!
- That's what good theories do.
- And it takes a bit of daredevil approach to science.

On to quantum computing

- We know that quantum computation is provably better than classical computation in some problems.
  - Uninformed search in a classical computer is $O(n)$, n being problem size.
  - Uninformed search in a quantum computer is $O(\sqrt{n})$, with Grover's algorithm.
  - That's a polynomial improvement in all polynomial problems, because the problem is P-complete.
- We don't know whether QC is provably better in all hard problems.
  - Schor's algorithm does not target an NP-complete problem.
- But it does solve one classically intractable problem polynomially.
- Where does the power come from?

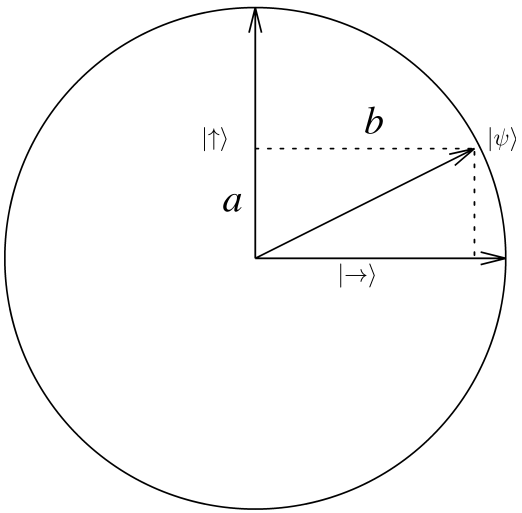


Fig. 1. Measurement is a projection onto the basis.

- Classical on-off bit can only be in state 0 or state 1.
- Quantum bit (qubit) is a superposition like $|\psi\rangle$ on the left.
- Think of $|\uparrow\rangle$ as $|1\rangle$, and $|\rightarrow\rangle$ as $|0\rangle$ we have $|\psi\rangle = a\,|1\rangle + b\,|0\rangle$
- such that they are bit-like, i.e. $|\ a\ |^2 + |\ b\ |^2 = 1$
- It can take any value in the rectangle.
- That's a lot more than just two values.
- Amazingly enough though, it is still digital, because any measuring device has finite orthonormal bases.

- That's the quantum advantage in a SINGLE system.
- Combined systems (multiple qubits) have one more advantage:
  - It is not always the case that their constituent states are separable.
  i. A separable state: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle = |0\rangle \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$
  ii. A non-separable state: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- Non-separable states are entangled. This is not expressible in classical computation.
- This intension has physical correlate, which we can manipulate in physics of computing.

- Extended expressivity with the quantum computer
  - Superposed qubit of the single system
  - Non-separable (entangled) qubits of the combined system
- These are not available in a classical computer
- Does that sound like 'quantum nature computes' to you?
- It doesn't sound like that at all to me
- Somebody has to harness these properties to be more expressive
- More expressive for what? To attempt solving more problems

How does a quantum computer operate?

- Python has a quantum library, called `qiskit`.
- Lisp, as usual, defines a new quantum language using its macro facility, called `qlisp`.
- In case you want to program it at the level like of a QTM:
- To compute function f on input x, that is, to do $f(x)$.
  - Input is prepared in a superposition, from $|0 \ldots 0\rangle$ to $|x0 \cdots 0\rangle$.
  - Once the quantum computer runs f, using its quantum gates etc. it ends in $|xf(x)0 \cdots 0r\rangle$. r is residue of quantum gates.
- Copy (not clone) result to unused bits by transformations, to get: $|xf(x)f(x)0 \cdots 0r\rangle$
- Run the gates in reverse, we get $|x0 \cdots 0f(x)0 \cdots 0\rangle$
- Run input transformation in reverse (Hadamard): $|0 \cdots 0f(x)0 \cdots 0\rangle$

- We have seen that intensions are important to describe to others what we have in mind about nature.
- If you are passing this knowledge to a human being, she is herself an interpreter. But, they tend to change over time.
- If you are passing it to a computer, you better not leave it to the interpreter to connect to it results, if you consider this to be your practice.
- So we must make a clear distinction between intensions on values and values themselves.
- That's what the monads symbolize. We use them sometimes without knowing, in fact in ALL data and program abstraction.

- The extensional view of computer programs: All programs have functionally equivalent lambda-terms.
  - Values: $1 = \lambda x.(x^2)1$. We also have $1{=}(\lambda x.1)a$ for any a.
  - Functions: $\lambda x.fx{=}f$ because e.g. $f1 = (\lambda x.fx)1{=}f1$
  - $f{=}\lambda f\,\lambda x.fx$ is eta conversion, assuming no free occurence of x in f.
  - The Halting Problem of TM : $(\lambda x.xx)(\lambda y.yy)$
- Turing's TM makes it evident that you need representational support for that.
- Monads: Programs are intensions on values, not values themselves. (Moggi, 1988, 1991)
- This is the intensional view of the computer program.

- Intension with 's', not 't'.

Two views of computing

- Lambda-calculus: Everything is a value, including functions.
- Monads: Everything is a function, including values.
- the TM: Either way, you need representation to be able to program.
- That's one reason everyone talks about the TM.
- Does the monadic view sound familiar?
- QM says all wave functions are vectors. The wave function characterizes a particle (a value), and observables are matrices operating over such vectors. They are functions too.
- We are treating everything as a function of kets and bras, including the scalars.

- Informally, a monad takes two values a and b and treats them as the latter dependent on the former, rather than as a single composite (a, b).
- If M is a monad, then Ma injects the intension of a (computation of a) into M. Then, Ma computes a inside, and this a constructs Mb, and result of Mb is returned.
- This is done by function composition. (Monads are monoids; see Mac Lane 1971)
- Essentially it says that two values must be dependent for computation to take place.

- The type of any Monad M is then $Ma \to ((a \to Mb) \to Mb) = Ma \to (a \to Mb) \to Mb$.
- Think about squaring 4.

1. $M4$ injects 4 into M as an intension. Extensionally, you can think of it as $(\lambda x.x)4$.
2. Inside M what is happening is extensionally $\lambda y.sq((\lambda z.z)y)((\lambda x.x)4)$

   All values are functions. We are composing sq with $(\lambda z.z)$
3. Ma to a is realized as $(\lambda x.x)4 = 4$
4. Then $a \to Mb$ is realized as $sq((\lambda z.z)4)$
5. Then Mb is realized as $sq(4)$. Think of sq as $\lambda w.w^2$

- Wait: We said two values. I see only one: 4.
- 16 is a value. THIS monad gives it as $sq(4)$.
- And why on earth can't we just write $(\lambda x.sq(x))4$?
- After all, this is what we CODE as a program, taking 4 as input.

  Compare the monadic version: $\lambda y.sq((\lambda z.z)y)((\lambda x.x)4)$
- In monadic view (and it is a view), all values operated on by computation are functions.
- Therefore, in monadic computation, we never have just the value, but intensions on the value.
- Even state change, that is, procedural programming, can be treated as a monad (Launchbury and Peyton Jones, 1994).

- What about constants? Are they monadic functions?
  - say: I want Ma to always give 4, whatever a is.
  - Even if I think of it as a function, I would say $\lambda x.4$

    here is the monadic version: $\lambda y.(\lambda w.4)((\lambda z.z)y)((\lambda x.x)a)$
  - We are still composing, this time $(\lambda w.4)$ with $(\lambda z.z)$
- But it says a bit more about being a constant, TO the interpreter: It is a function that no function can map to another value.

- What about many-argument functions? They have more than two values, at least two input and one output.
- Say we want to compute $5 - 4 = 1$
- Looks so easy in the extensional view: $(\lambda x \lambda y.x - y)5\ 4$
- It says: Give me 5, THEN give me 4, I give you $5 - 4$.
- Now try to explain the computation here to future generations five centuries from now.
- It suggests the following monadic view: give me 5, I give you $M_a 5$. Give me 4, I give you $M_b 4$, then I give you $M_c(M_b M_a)$. I am chaining TWO computations to do the THIRD one, because there are THREE intensional values, and the last one (M_c) is what YOU want to extensionalize.
- It is `Haskell`'s **do** monad, which can chain any number of computations.

-I used M_a and M_b because they can be more complex than doing the same thing, i.e. computationally echoing the value provided.
-An informal sketch of what happens in $M_c(M_bM_a)$ 'in the kitchen':

1. *Ma* sets up the M_b as follows: $\lambda y.M_b((\lambda z.z)y)((\lambda x.x)M_a)$
   This is function composition, composing M_b with $(\lambda z.z)$, giving M_bM_a
2. M_c is then: $\lambda y.M_c((\lambda z.z)y)((\lambda x.x)(M_bM_a))$
   This is also function composition, giving $M_c(M_bM_a)$

- Take M_c to be '$-$'. M_a got in there first. M_c has the last word.

- Every step has two intensions made explicit.
- Intensions are important to get across generations: Egyptians knew $2 > 1$. Did they know that atomic number of helium (2) is greater than atomic number of hydrogen (1)? Ajdukiewicz (1967)
- Not pretty, but future generations may appreciate the effort.

- Mathematicians take heed: If you want interpreters of later centuries to disambiguate your notation AND intention, it's time to think also like a computer scientist, because we must keep records of our encoding decoding.
- We can do that for humans too.
- If you don't believe a computer scientist, ask Ganesalingam (2013).
- I am not alone in this rant, at least for quantum notation: Fortnow (2003), Aaronson (2013).

Aaronson, S. (2013). *Quantum computing since Democritus*. Cambridge University Press.

Ajdukiewicz, K. (1967). Intensional expressions. *Studia Logica 20*(1), 63–86.

Arora, S. and B. Barak (2009). *Computational complexity: a modern approach*. Cambridge University Press.

Bozşahin, C. (2018). Computers aren't syntax all the way down or content all the way up. *Minds and Machines 28*(3), 543–567.

Fortnow, L. (2003). One complexity theorist's view of quantum computing. *Theoretical Computer Science 292*(3), 597–610.

Ganesalingam, M. (2013). *The language of mathematics*. Springer.

Hadamard, J. (1945). *An essay on the psychology of invention in the mathematical field*. Dover.

Launchbury, J. and S. L. Peyton Jones (1994). Lazy functional state threads. *ACM SIGPLAN Notices 29*(6), 24–35.

Mac Lane, S. (1971). *Categories for the Working Mathematician*. Berlin/New York: Springer.

Mills, J. W. (2008). The nature of the extended analog computer. *Physica D: Nonlinear Phenomena 237*(9), 1235–1256.

Moggi, E. (1988). *Computational Lambda-Calculus and Monads*. LFCS, University of Edinburgh.

Moggi, E. (1991). Notions of computation and monads. *Information and computation 93*(1), 55–92.

Nannicini, G. (2020). An introduction to quantum computing, without the physics. *SIAM Review 62*(4), 936–981.

Rieffel, E. and W. Polak (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys (CSUR) 32*(3), 300–335.

Rubel, L. A. (1993). The extended analog computer. *Advances in Applied Mathematics 14*(1), 39–50.