CAMBRIDGE

Cambridge University Press
978-0-521-19956-8 - Quantum Computing since Democritus
Scott Aaronson
Excerpt
More information

1 Atoms and the void

I would rather discover a single cause than become king of the Persians.

– Democritus

So why Democritus? First of all, who *was* Democritus? He was this Ancient Greek dude. He was born around 450 BC in this podunk Greek town called Abdera, where people from Athens said that even the air causes stupidity. He was a disciple of Leucippus, according to my source, which is Wikipedia. He's called a "pre-Socratic," even though actually he was a contemporary of Socrates. That gives you a sense of how important he's considered: "Yeah, the *pre*-Socratics – maybe stick 'em in somewhere in the first week of class." Incidentally, there's a story that Democritus journeyed to Athens to meet Socrates, but then was too shy to introduce himself.

Almost none of Democritus's writings survive. Some survived into the Middle Ages, but they're lost now. What we know about him is mostly due to other philosophers, like Aristotle, bringing him up in order to criticize him.

So, what did they criticize? Democritus thought the whole universe is composed of atoms in a void, constantly moving around according to determinate, understandable laws. These atoms can hit each other and bounce off, or they can stick together to make bigger things. They can have different sizes, weights, and shapes – maybe some are spheres, some are cylinders, whatever. On the other hand, Democritus says that properties like color and taste are *not* intrinsic to atoms, but instead emerge out of the interactions of many atoms.

For if the atoms that made up the ocean were "intrinsically blue," then how could they form the white froth on waves?

Remember, this is 400 BC. So far we're batting pretty well.

Why does Democritus think that things are made of atoms? He gives a few arguments, one of which can be paraphrased as follows: suppose we have an apple, and suppose the apple is made not of atoms but of continuous, hard stuff. And suppose we take a knife and slice the apple into two pieces. It's clear that the points on one side go into the first piece and the points on the other side go into the second piece, but what about the points exactly on the boundary? Do they disappear? Do they get duplicated? Is the symmetry broken? None of these possibilities seem particularly elegant.

Incidentally, there's a debate raging even today between atomists and anti-atomists. At issue in this debate is whether space and time *themselves* are made up of indivisible atoms, at the Planck scale of 10^{-33} cm or 10^{-43} s. Once again, the physicists have very little experimental evidence to go on, and are basically in the same situation that Democritus was in, 2400 years ago. If you want an ignorant, uninformed layperson's opinion, my money is on the atomist side. And the arguments I'd use are not *entirely* different from the ones Democritus used: they hinge mostly on inherent mathematical difficulties with the continuum.

One passage of Democritus that does survive is a dialogue between the intellect and the senses. The intellect starts out, saying "By convention there is sweetness, by convention bitterness, by convention color, in reality only atoms and the void." For me, this single line already puts Democritus shoulder to shoulder with Plato, Aristotle, or any other ancient philosopher you care to name: it would be hard to give a more accurate one-sentence summary of the entire scientific worldview that would develop 2000 years later! But the dialogue doesn't stop there. The senses respond, saying "Foolish intellect! Do you seek to overthrow us, while it is from us that you take your evidence?"

I first came across this dialogue in a book by Schrödinger.[1] Ah, Schrödinger! – you see we're inching toward the "quantum computing" in the book title. We're gonna get there, don't worry about that.

But why would Schrödinger be interested in this dialogue? Well, Schrödinger was interested in a lot of things. He was not an intellectual monogamist (or really any kind of monogamist). But one reason he *might've* been interested is that he was one of the originators of quantum mechanics – in my opinion the most surprising discovery of the twentieth century (relativity is a close second), and a theory that adds a whole new angle to the millennia-old debate between the intellect and the senses, even as it fails to resolve it.

Here's the thing: for any isolated region of the universe that you want to consider, quantum mechanics describes the evolution in time of the state of that region, which we represent as a linear combination – a *superposition* – of all the possible configurations of elementary particles in that region. So, this is a bizarre picture of reality, where a given particle is not *here*, not *there*, but in a sort of weighted sum over all the places it could be. But it works. As we all know, it does pretty well at describing the "atoms and the void" that Democritus talked about.

The part where it maybe doesn't do so well is the "from us you take your evidence" part. What's the problem? Well, if you take quantum mechanics seriously, *you yourself* ought to be in a superposition of different places at once. After all, you're made of elementary particles too, right? In particular, suppose you measure a particle that's in a superposition of two locations, A and B. Then the most naive, straightforward reading of quantum mechanics would predict that the universe itself should split into two "branches": one where the particle is at A and you see it at A, one where the particle is at B and you see it at B! So what do you think: *do* you split into several copies of yourself every time you look at something? I don't *feel* like I do!

[1] E. Schrödinger, *What is Life? With Mind and Matter and Autobiographical Sketches*, Cambridge University Press (reprinted edition), 2012.

You might wonder how such a crazy theory could be *useful* to physicists, even at the crassest level. How could it even make *predictions*, if it essentially says that everything that could happen does? Well, the thing I didn't tell you is that there's a separate rule for what happens when you make a measurement: a rule that's "tacked on" (so to speak), external to the equations themselves. That rule says, essentially, that the act of looking at a particle *forces it to make up its mind* about where it wants to be, and that the particle makes its choice *probabilistically*. And the rule tells you exactly how to calculate the probabilities. And of course it's been spectacularly well confirmed.

But here's the problem: as the universe is chugging along, doing its thing, how are we supposed to know when to apply this measurement rule, and when not to? What counts as a "measurement," anyway? The laws of physics aren't supposed to say things like "such-and-such happens *until someone looks*, and then a completely different thing happens!" Physical laws are supposed to be *universal*. They're supposed to describe human beings the same way they describe supernovas and quasars: all just examples of vast, complicated clumps of particles interacting according to simple rules.

So from a physics perspective, things would be so much cleaner if we could dispense with this "measurement" business entirely! Then we could say, in a more sophisticated update of Democritus: there's nothing but atoms and the void, evolving in quantum superposition.

But wait: if we're not here making nosy measurements, wrecking the pristine beauty of quantum mechanics, then how did "we" (whatever that means) ever get the evidence in the first place that quantum mechanics is true? How did we ever come to believe in this theory that seems so uncomfortable with the fact of our own existence?

So, that's the modern version of the Democritus dilemma, and physicists and philosophers have been arguing about it for almost a hundred years, and in this book we're not going to solve it.

The other thing I'm not going to do in this book is try to sell you on some favorite "interpretation" of quantum mechanics. You're free to believe whatever interpretation your conscience dictates. (What's my own view? Well, I agree with *every* interpretation to the extent it says there's a problem, and disagree with every interpretation to the extent it claims to have solved the problem!)

See, just like we can classify religions as monotheistic and polytheistic, we can classify interpretations of quantum mechanics by where they come down on the "putting-yourself-in-coherent-superposition" issue. On the one side, we've got the interpretations that enthusiastically sweep the issue under the rug: Copenhagen and its Bayesian and epistemic grandchildren. In these interpretations, you've got your quantum system, you've got your measuring device, and there's a line between them. Sure, the line can shift from one experiment to the next, but for any given experiment, it's gotta be somewhere. In principle, you can even imagine putting other people on the quantum side, but you *yourself* are always on the classical side. Why? Because a quantum state is just a representation of your knowledge – and you, by definition, are a classical being.

But what if you want to apply quantum mechanics to the whole universe, *including* yourself? The answer, in the epistemic-type interpretations, is simply that you don't ask that sort of question! Incidentally, that was Bohr's all-time favorite philosophical move, his WWF piledriver: "You're not allowed to ask such a question!"

On the other side, we've got the interpretations that *do* try in different ways to make sense of putting yourself in superposition: many-worlds, Bohmian mechanics, etc.

Now, to hardheaded problem-solvers like ourselves, this might seem like a big dispute over words – why bother? I actually agree with that: if it were just a dispute over words, then we *shouldn't* bother! But as David Deutsch pointed out in the late 1970s, we *can* conceive of experiments that would differentiate the first type of interpretation from the second type. The simplest experiment would just be to put yourself in coherent superposition and see what happens! Or if that's too dangerous, put someone *else* in coherent superposition. The point being that, if human beings were regularly put into superposition, then the whole business of drawing a line between "classical observers" and the rest of the universe would become untenable.

But alright – human brains are wet, goopy, sloppy things, and maybe we won't be able to maintain them in coherent superposition for 500 million years. So what's the next best thing? Well, we could try to put a *computer* in superposition. The more sophisticated the computer was – the more it resembled something like a brain, like ourselves – the further up we would have pushed the "line" between quantum and classical. You can see how it's only a minuscule step from here to the idea of quantum computing.

I'd like to draw a more general lesson here. What's the point of talking about philosophical questions? Because we're going to be doing a fair bit of it here – I mean, of philosophical bullshitting. Well, there's a standard answer, and it's that philosophy is an intellectual clean-up job – the janitors who come in after the scientists have made a mess, to try and pick up the pieces. So in this view, philosophers sit in their armchairs waiting for something surprising to happen in science – like quantum mechanics, like the Bell inequality, like Gödel's Theorem – and then (to switch metaphors) swoop in like vultures and say, ah, this is what it *really* meant.

Well, on its face, that seems sort of boring. But as you get more accustomed to this sort of work, I think what you'll find is . . . it's *still* boring!

Personally, I'm interested in results – in finding solutions to nontrivial, well-defined open problems. So, what's the role of philosophy in that? I want to suggest a more exalted role than intellectual janitor: philosophy can be a *scout*. It can be an explorer – mapping out intellectual terrain for science to *later* move in on, and build condominiums on or whatever. Not every branch of science was scouted out ahead of time by philosophy, but some were. And in recent history, I think quantum computing is really the poster child here. It's fine to tell people to "Shut up and calculate," but the question is, *what* should they calculate? At least in quantum computing, which is my field, the sorts of things that we like to calculate – capacities of quantum channels, error probabilities of quantum algorithms – are things people would never have *thought* to calculate if not for philosophy.

Cambridge University Press
978-0-521-19956-8 - Quantum Computing since Democritus
Scott Aaronson
Excerpt
More information

2 Sets

Here, we're gonna talk about sets. What will these sets contain? Other sets! Like a bunch of cardboard boxes that you open only to find *more* cardboard boxes, and so on all the way down.

You might ask "how is this relevant to a book on quantum computing?"

Well, hopefully we'll see a few answers later. For now, suffice it to say that math is the foundation of all human thought, and set theory – countable, uncountable, etc. – that's the foundation of math. So regardless of what a book is about, it seems like a fine place to start.

I probably should tell you explicitly that I'm compressing a whole math course into this chapter. On the one hand, that means I don't really expect you to understand everything. On the other hand, to the extent you do understand – hey! You got a whole math course in one chapter! You're welcome.

So let's start with the empty set and see how far we get.

THE EMPTY SET.

Any questions so far?

Actually, before we talk about sets, we need a language for talking about sets. The language that Frege, Russell, and others developed is called *first-order logic*. It includes Boolean connectives (and, or, not), the equals sign, parentheses, variables, predicates, quantifiers ("there exists" and "for all") – and that's about it. I'm told that the physicists have trouble with these. Hey, I'm just ribbin' ya. If you haven't seen this way of thinking before, then you haven't seen it. But maybe, for the benefit of the physicists, let's go over the basic rules of logic.

RULES OF FIRST-ORDER LOGIC

The rules all concern how to construct sentences that are *valid* – which, informally, means "tautologically true" (true for all possible settings of the variables), but which for now we can just think of as a combinatorial property of certain strings of symbols. I'll write logical sentences in a typewriter font in order to distinguish them from the surrounding English.

- **Propositional tautologies:** `A or not A`, `not(A and not A)`, etc., are valid.
- **Modus ponens:** If `A` is valid and `A implies B` is valid, then `B` is valid.
- **Equality rules:** `x=x`, `x=y implies y=x`, `x=y and y=z implies x=z`, and `x=y implies f(x)=f(y)` are all valid.
- **Change of variables:** Changing variable names leaves a statement valid.
- **Quantifier elimination:** If `For all x, A(x)` is valid, then `A(y)` is valid for any y.
- **Quantifier addition:** If `A(y)` is valid where y is an unrestricted variable, then `For all x, A(x)` is valid.
- **Quantifier rules:** If `not(For all x, A(x))` is valid, then `There exists an x such that not(A(x))` is valid. Etc.

So, for example, here are the Peano axioms for the nonnegative integers written in first-order logic. In these, $S(x)$ is the successor function, intuitively $S(x) = x + 1$, and I'm assuming functions have already been defined.

PEANO AXIOMS FOR THE NONNEGATIVE INTEGERS

- **Zero exists:** `There exists a z such that for all x, S(x) is not equal to z`. (This z is taken to be 0.)
- **Every integer has at most one predecessor:** `For all x,y, if S(x)=S(y) then x=y`.

The nonnegative integers themselves are called a *model* for the axioms: in logic, the word "model" just means any collection of objects and functions of those objects that satisfies the axioms. Interestingly, though, just as the axioms of group theory can be satisfied by many different groups, so too the nonnegative integers are not the only model of the Peano axioms. For example, you should check that you can get another valid model by adding extra, made-up integers that aren't reachable from 0 – integers 'beyond infinity,' so to speak. Though once you add one such integer, you need to add infinitely many of them, since every integer needs a successor.

Writing down these axioms seems like pointless hairsplitting – and indeed, there's an obvious chicken-and-egg problem. How can we state axioms that will put the integers on a more secure foundation, when the very symbols and so on that we're using to write down the axioms presuppose that we *already know* what the integers are?

Well, precisely because of this point, I *don't* think that axioms and formal logic can be used to place arithmetic on a more secure foundation. If you don't already agree that $1 + 1 = 2$, then a lifetime of studying mathematical logic won't make it any clearer! But this stuff is still extremely interesting for at least three reasons.

1. The situation will change once we start talking not about integers, but about different sizes of infinity. There, writing down axioms and working out their consequences is pretty much all we have to go on!
2. Once we've formalized everything, we can then program a computer to reason for us:
   - **Premise 1:** `For all x, if A(x) is true, then B(x) is true.`
   - **Premise 2:** `There exists an x such that A(x) is true.`
   - **Conclusion:** `There exists an x such that B(x) is true.`

   Well, you get the idea. The point is that deriving the conclusion from the premises is purely a *syntactic* operation – one that doesn't require any understanding of what the statements mean.
3. Besides having a computer find proofs for us, we can also treat proofs themselves as mathematical objects, which opens the way to *meta-mathematics*.

Anyway, enough pussyfooting around. Let's see some axioms for set theory. I'll state the axioms in English; converting them to first-order logic is left as an exercise for the reader in most cases.