Meeting 2: P, NP, and All That

Philosophy of Computation at Berkeley
pocab.org

April 21, 2017

1 Computability and Complexity

Last week, we talked about computation and what it means for a problem to be computable or uncomputable. This week, we will zoom in a little more and interrogate the fine-grained subsections that all fall under the branch 'computable'.

> One might think that, once we know something is *computable*, whether it takes 10 seconds or 20 seconds to compute is obviously the concern of engineers rather than philosophers. But that conclusion would *not* be so obvious, if the question were of 10 seconds versus $10^{10^{10}}$ seconds! And indeed, in complexity theory, the quantitative gaps we care about are usually so vast that one has to consider them qualitative gaps as well. Think, for example, of the difference between reading a 400-page book and reading *every possible* such book, or between writing down a thousand-digit number and counting to that number.
> – *Why Philosophers Should Care About Computational Complexity, 2.0*, Scott Aaronson

- What is the difference between quantity[1] and quality[2]?
- An interesting note: exponentiation by infinity leads to uncomputability ($2^{\aleph_0} = \aleph_1$). Exponentiation by a finite number leads to intractability (2^n). Is exponentiation such a big quantitative jump that it somehow becomes a qualitative jump? Why would exponentiation have such a power?
- A similar problem arises in the Riemann Hypothesis, an unresolved problem as notorious as P vs. NP.

> The key to unlocking the Riemann Hypothesis lies in a qualitative rather than solely quantitative appreciation of mathematical relationships...
>
> Throughout its history the Riemann Hypothesis has been the subject of intense investigation by the finest mathematicians. However it has shown itself incredibly resistant to proof with so often, an apparent solution managing to elude final capture in the most tantalising manner. Indeed due to its seemingly impenetrable nature, hints of a more fundamental difficulty can be gleaned through the comments of some of the greatest authorities on the matter.
>
> For example Brian Conrey [1] :
>
> "The Riemann Hypothesis is the most basic connection between addition and multiplication that there is, so I think of it in the simplest terms as something really basic that we don't understand about the link between addition and multiplication." And Alain Connes [2] in somewhat similar fashion:
>
> "The Riemann Hypothesis is probably the most basic problem in mathematics, in the sense that it is the intertwining of addition and multiplication. It's a gaping hole in our understanding..."
>
> – *A Deeper Significance: Resolving the Riemann Hypothesis*, Peter Collins

[1] Merriam-Webster defines quantity as "an indefinite amount or number; a dtereminate or estimated amount; total amount or number".

[2] Merriam-Webster defines quality as "a peculiar and essential character; an inherent feature; capacity, role".

What do you think is the relation between addition and multiplication?[3] Why is the usual explanation, that multiplication is repeated addition, sometimes fail?

2 Chinese Room and Complexity

Here is a breif exposition of the Chinese Room argument: suppose there is a man in a room who does not understand Chinese. There is a man outside the room who in fact knows Chinese. The man inside the room communicates by exchanging strips of paper with Chinese written on it with the man outside the room. Searle purports that the man inside the room, though without understanding Chinese, could use some sort of "lookup table" to find an appropriate response to whatever the man outside the room wrote him. In this way, the man inside the room, though without understanding any Chinese, can convince the man outside that he understands Chinese. This argument is not only subtly racist with its implicit othering and simplification of the Chinese, it is incoherent under the lens of computational complexity, as Aaronson describes.

> Briefly, Searle proposed a thought experiment – the deatils don't concern us here – purporting to show that a computer program could pass the Turing Test, even though the program manifestly lacked anything that a resonable person would call "intelligence" or "understanding". In response, many critics said that Searle's argument was deeply misleading, because it implicitly encouraged us to imagine a computer program that was *simplistic* in its internal operations... And while it was true, the critics went on, that a giant lookup table wouldn't "truly understand" its responses, that point is also *irrelevant*. For the giant lookup table is a philosophical fiction anyway: something that can't even fit in the observable universe! If we instead imagine a *compact, efficient* computer program passing the Turing Test, then the situation changes drastically...
>
> Personally, I find this response to Searle extremely interesting – since if correct, it suggests that the distinction between polynomial and exponential complexity has *metaphysical* significance. According to this response, an exponential-sized lookup table that passed the Turing Test would not be sentient (or conscious, intelligent, self-aware, etc.), but a polynomially-bounded program with exactly the same input/output behavior *would* be sentient. Furthermore, the latter program would be sentient *because* it was polynomially-bounded.
>
> – *Why Philosophers Should Care About Computational Complexity, 4.2*, Scott Aaronson

3 P, NP, Art, and Morality

> If P=NP, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in "creative leaps", no fundamental gap between solving a problem and recognizing the solution once it's found. Everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss; everyone who could recognize a good investment strategy would be Warren Buffett. – Scott Aaronson

P is the set of problems for which an efficient (polynomial-time) algorithm exists. In other words, one can easily find a solution to a P problem. On the other hand, NP is the set of problems for which an efficient *verification algorithm for a given solution* exists. For example, if God comes along and gives you a purported solution to some NP problem, you can easily check whether God is lying to you or not. In other words, while a solution to a NP problem may not be necessarily easy to find, given a solution, it is easy to *verify* that the solution is indeed correct.

- A great symphony can be considered a "solution" to the "SYMPHONY" problem. A person who is capable of *appreciating* a great symphony is capable of *verifying* that the "solution", the great symphony, of the "SYMPHONY" problem, is a correct solution. But if P=NP, then verifying a given solution would be the same as finding the solution from scratch. It is in this sense that Aaronson says "If P=NP... everyone who could appreciate a symphony would be Mozart". Of course, this is a

[3] My hunch is that this elusive relation has something in common with the elusive relation between n and c^n, maybe captured somewhat in the logarithmic identity $\log(n * n) = \log(n) + \log(n)$...

controversial statement. Do you agree with it? Can a "great symphony" even be objectively defined? How or why not?

- Is morality an NP problem? That is, is it true that there is some universal criterion that permits one to say that some action is a moral action?
- coNP (complement of NP) is the set of problems where it is not necessarily easy to verify that a solution is correct, but it is easy to check that a purported solution is in fact incorrect. Maybe it is easier, then, to say that morality is a coNP problem: it is easy to verify what kinds of acts are *not* moral. For example, virtually everyone, across all cultures, agree that it is *not moral* to kill a person. What do you think?

4 P vs. PSPACE = IP

P is really a shorthand for P*TIME*[4], so P vs. PSPACE[5] is really PTIME vs. PSPACE, which, factoring out the P, is really TIME vs. SPACE. So what do they mean?

This is what a PSPSACE problem looks like:

$$\exists x_1 \forall x_2 \exists x_3 \forall x_4 ... \exists x_n \phi$$

where ϕ is some boolean proposition. But what does that mean? As an example, the canonical PSPACE problem is chess[6]. This means that a computer that can solve PSPACE problems efficiently can *solve* chess, i.e. always win at it. In the above proposition, $x_1, x_3, ...$ are the moves made by player 1, and $x_2, x_4, ...$ are the moves made by player 2, so it says, there exists a move that player 1 can make (x_1), for all moves player 2 can make (x_2), there exists a move that player 1 can make (x_3), for all moves player 2 can make (x_4) ... such that player 1 wins (ϕ).

> $P \neq NP$ implies $P \neq PSPACE$. So while $P \neq PSPACE$ is not yet proved, it is an extremely secure conjecture by the standards of complexity theory. In slogan form, complexity theorists believe that *space is more powerful than time*.
>
> Now, some people have asked how such a claim could possibly be consistent with modern physics. For didn't Einstein teach us that space and time are merely two aspects of the same structure? One immediate answer is that, even *within* relativity theory, space and time are not interchangeable: space has a positive signature whereas time has a negative signature. In complexity theory, the difference between space and time manifests itself in the straightforward fact that you can *reuse* the same memory cells over and over, but you can't reuse the same moments of time. (scottaaronson.com/blog/?p=368)
>
> Yet, as trivial as that observation sounds, it leads to an interesting thought. Suppose that the laws of physics let us travel *backwards* in time. In such a case, it's nautral to imagine that time would become a "reusable resource" just like space is – and that, as a result, arbitrary PSPACE computations would fall within our grasp. But is that just an idle speculation, or can we rigorously justify it?
>
> – *Why Philosophers Should Care About Computational Complexity*, 10.0, Scott Aaronson

- In your everyday experience, how is time different from space?

Another interesting fact about PSPACE is that IP, or Interactive Proofs, is equal to PSPACE. In other words, suppose God (a PSPACE oracle) exists and tells you you can move this pawn over here to beat Karl in chess. But you, a mere mortal, doubts if God is telling you the truth. In this case, by repeatedly interrogating God with the right questions, you can have God convince you that He is telling you the truth, even though you are just a mere mortal.

[4] the set of problems that can be solved in polynomial time
[5] the set of problems that can be solved in polynomial space
[6] strictly, it is a *generalization* of chess, with a $n \times n$ board, not 8×8 as it usually is.