6.080 / 6.089 Great Ideas in Theoretical Computer Science
Spring 2008

6.080/6.089 GITCS Feb 07, 2008

Lecture 2

Lecturer: Scott Aaronson *Scribe: Mergen Nachin*

Administrative announcements:

- Two scribe notes per student needed.
- If you've already taken 6.840, there's really no reason for you to take this class, unless you enjoy my jokes. But if you take this class, there's reason to take 6.840.

1 Review of last lecture

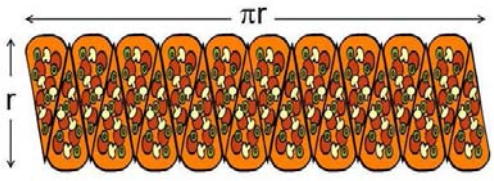
Last week, we talked about online gambling and computation in the ancient world. What I find interesting, incidentally, is that so many basic mathematical ideas were discovered independently by multiple cultures (the Greeks, Mayans, Indians, Chinese, etc). To me, this is a striking empirical refutation of the idea that math is just a "cultural construct." To give one example, Pascal's triangle was discovered in China around 1000 AD – and is instantly recognizable as soon as you see it (a print of the ancient Chinese Pascal's triangle is passed around in class).

We also talked about Euclidean geometry as a model of computation. Euclid laid down a set of simple, clear rules that one can repeatedly apply to construct complicated objects. We also talked about Euclid's GCD algorithm, which was one of the first non-trivial algorithms known to humankind.

Here is some digression. Area of a circle is $A = \pi r^2$. It's obvious that the area of a circle should go like the r^2; the question is why the constant of proportionality (π) should be the same one that relates circumference to diameter - $2\pi r$.

- *Student: can be observed using differential equation.*
- *Scott: yes, that can be one way. But was calculus invented in that time? If you don't have calculus, you can do this by "Sicilian pizza argument".*

Proof by pizza: Cut a circle of radius r into thin pizza slices, and then "Sicilianize" (i.e. stack the slices into a rectangle of height r and length πr).



(Figure taken from http://www.scottaaronson.com/democritus/lec2.html)

2 Today: Logic and Proof

These might seem like dry topics, but they're prerequisites to almost everything else in the course. What does it mean to think logically? Can we formalize what we mean by logical thought, and subject it to logical scrutiny itself?

The credit for being the first logician is usually given to Aristotle, who formalized the concept of the syllogism.

All men are mortal, Socrates is man, therefore Socrates is a mortal.

This is a syllogism. In more modern language, we call it transitivity of implications. In general, a syllogism is

If A $\Rightarrow$ B is valid and B $\Rightarrow$ C is valid, then A $\Rightarrow$ C is valid.

Remark: What do we mean by "$\Rightarrow$"? "A $\Rightarrow$ B" is valid if A is false or B is true or both. If A is true, B has to be true. If A is false, B could be either true or false.

You all know a false statement implies anything? "I am one, the Pope is one, therefore I and the Pope are one." ("proof" of 1+1=1?)

How many of you have seen the puzzle with four cards?

B 5 2 J

Each card has a number on one side and a letter on the other. Which cards would you have to turn over, to test the rule that if there's a J on one side there's a 5 on the other side? You would have to turn J and the 2, not the 5. 80-90 percent of college students get this wrong.

On the other hand, suppose you ask people the following: you say, you're a bouncer in a bar, and you want to make sure the rule "If you are under 21 the you are not drinking". Who do you have to check to test this rule: someone who is drinking, someone who isn't drinking, someone who's over 21, someone who's under 21?

And then, of course, almost everyone gets it right. Even though this problem is logically equivalent in every way to the other problem.

And this brings up a fundamental point about our brains. We're designed for spearing small animals. Not for proving theorems. This class is all about doing things that your brains are *not* designed for. The trick is to co-opt parts of your brain that evolved for something else. "You over there: you're supposed to track leopards leaping across the savanna? Well, now those leopards are going to be arbitrary vectors $v \in \Re^3$. Deal with it."

Remark: Implication is actually going on at two different levels. There are these "implication" arrows inside the statements that the sentence is talking about, then there's also the sentence that's talking about them. These three sentences you can think of as meaningless pieces of code, the sentence is addressed to us; it's telling us one of the rules of the code.

Was Aristotle the first person in history to apply such an inference? Obviously he wasn't. As we all see in our everyday life, everyone draws inferences all the time. However, what he was (as far as I know) was the first person in the historical record to (as it were) draw a box around the inference rule, to say that this is a general law of thought.This is crucial because it allows us to reason about the rule itself.

2.1 Leibniz and the Calculus Ratiocinator: "Gentlemen, let us calculate!"

Today, Leibniz's dream that we could use an automatic reasoning machine to settle legal disputes strikes us as naïve, especially when we think about the sorts of arguments that actually get used in courtrooms: "If it does not fit, you must acquit," etc.

More to the point, in real court cases, often the difficulty is not that people don't draw the right inferences from the facts, it's that they don't agree about the facts! Or the facts are probabilistic and uncertain, and people don't agree how much weight different facts entered into evidence should be assigned. On top of that, the laws themselves are necessarily vague, and people disagree in their preferred interpretation of the law.

Nevertheless, this idea of Leibniz that we could automate even part of human thought was extremely bold for its time.

Moreover, Leibniz had what today we would see as the right picture of what such a machine would be. To him, it's not that you would take some lifeless clump of clay, and utter some mystical incantation that would magically imbue it the power of speech – like in the legend of Pinocchio, or the legend of the Golem, or even in a lot of science fiction. Leibniz's idea, rather, was that you'd "merely" be building a complicated machine. Any individual gear in the machine would not be thinking – it's just a gear. But if you step back and consider *all* the gears, then it might look like it was thinking.

On this view, the role of logic is to tell us what are the "atoms of thought" that we would need to build a reasoning machine.

If you know A⇒B and B⇒C, and you conclude A⇒C, you really haven't done much in the way of thinking. We do this sort of thinking every morning: "My socks go on my feet, these are my socks, therefore these go on my feet."

Yet suppose you strung together hundreds or thousands of these baby steps. Then maybe you'd end up with the most profound thought in the history of the world! Conversely, if you consider the most profound thoughts anyone ever had, how do we know they *can't* be analyzed into thousands of baby steps? Maybe they can! Many things seem magical until you know the mechanism. So why not logical reasoning itself?

To me, that's really the motivation for studying logic: to discover "The Laws of Thought." But to go further, we need to roll up our sleeves, and talk about some real examples of logical rule systems.

Maybe the simplest interesting system is the one where every statement has the form

- $A \Rightarrow B$
- $\neg A \Rightarrow B$
- $A \Rightarrow \neg B$ or
- $\neg A \Rightarrow \neg B$

and the only rules are:

- Given $A \Rightarrow B$ and $B \Rightarrow C$, you can deduce $A \Rightarrow C$.
- Given $\neg A \Rightarrow A$ and $A \Rightarrow \neg A$, you can deduce a contradiction.

Can we have both $\neg A \Rightarrow A$ and $A \Rightarrow \neg A$ valid at the same time? If we assign A=false then $A \Rightarrow \neg A$ is valid. But $\neg A \Rightarrow A$ is not valid. Similarly if we assign A=true then $A \Rightarrow \neg A$ is not valid. Now consider the following example.

- $A \Rightarrow B$

- $\neg C \Rightarrow A$
- $\neg A \Rightarrow \neg C$
- $B \Rightarrow \neg A$

Can these sentences simultaneously be satisfied? I.e. is there some way of setting A,B,C,D to "true" or "false" that satisfies all four sentences?

No. By applying the rules, we can reach a contradiction! You agree that if we reach a logical contradiction by applying the rules, then the sentences can't all be valid?

Suppose a set of sentences is inconsistent (i.e., there's no way of setting the variables so that all of them are satisfied). Can we always discover the contradiction always by applying the above rules?

Yes, we can always discover the contradiction. You can just imagine a big graph. The nodes are the variables and their negations. A,¬ A,B,¬ B,C, ¬ C.... Place directed edge from node A to node B whenever $A \Rightarrow B$. Whenever we apply a rule, we can think as if we were walking through the graph. So $A \Rightarrow B$, $B \Rightarrow C$ then $A \Rightarrow C$ actually means C is reachable from A. Start with A=true and if we reach ¬ A then it means $A \Rightarrow \neg A$. If we also end up connecting $\neg A$ and A, in other words if we have cycle, then we have discovered a contradiction.

What we're talking about are two properties of logical systems called "soundness" and "completeness."

Soundness: Any statement you get by cranking the rules is true. (That's a pretty basic requirement.)

Completeness: Any statement that's true, you can get by cranking the rules.

In the next lecture: a bit of first-order logic!