Axiomatic Logic

Charlie Tian

February 2017

1 Introduction

The purpose of this article is to help in logic/proof relationship beyond what was given in the guerilla section. Because I did not help out with writing logic problems for the guerilla the problems were a repeat of last semester's, and although it was useful to get working on writing logic tables, not enough indication of logic's power and ability to help think about how rigorous proofs are constructed, and whether a proof is logically sound or not.

I hope that this note at least gives some examples of how logic can be used to solve problems, as well as inspire new topics (that CS70 will face in coming weeks!)

2 Logical Transformation of Proofs

Let's see how we can use the same logical deduction rules covered briefly in the first part of this course to transform proofs into a logically equivalent statement that is easier to prove. In many cases, this transformation is the key insight that allows us to get a proof and then apply lemmas, if such lemmas exist, which are essentially subproofs that may be easier to abstract that the more complex ones.

Let's take a look at some examples that have been covered so far:

1. Consider many stable marriage problems, in which we transform the proof of optimal pairings, or equivalent pairings, into that of the well-ordering principle, when we can logically deduce that some ordered list of actions will occur (e.g. if someone first deviates from the original pairing, or some first non-stable pairing occurs).

2. Graph induction is essentially a transformation of the set of vertices (or whatever variable n that is being inducted upon) into the given set of natural numbers, onto which we can apply the induction paradigm on. The only difference here is that to avoid edge cases in several types of inductive steps, we have to add, delete, and re-add the node to avoid build-up error. We are able to achieve this logical deduction by noticing

that vertices are a discrete (countable) set, and that we can assign an enumeration $\forall v \in V$ for a vertex v in the set of vertices V. There will be more discussion on countability in the future.

3. **Map colorings**: A specific application of graph theory is towards that of maps. With the proper mathematical definition of a map, we can say that each item on the map can represent a node. In any n-color map theory, we are concerned only with the colors of the neighbors of each map item. Therefore, we are logically able to reduce the map to an abstraction such as a planar graph. If we check the logical requirements of the n-color map problem, we are able to see logical step by logical step, that indeed a planar graph is a valid abstraction, and we are able to apply any developed planar graph theorems to the new problem. Essentially we create a n-color planar graph theory. (Of course such proofs as the 4-color map theorem do not get trivial even after this connection, but it is a useful connection nonetheless as we can now harness the power of graph theory).

4. **Goldbach's Conjecture**: Note that logically speaking, a conjecture is a statement that seems to be true based on all experimental tests and thus can't be proven false either, but has never been proven true. It is basically a guess that the statement is true based on experimental evidence.

   Let P be the set of all primes. Then,

   $$\forall n \in N \quad n > 1 \quad \implies \quad \exists p, q \in P \quad 2n = p + q$$

   Essentially, every even positive number greater than 2 is the sum of two prime natural numbers. Not that this is a solution to the problem, as this problem has been one of the notorious unsolved problems in math, but we can see that this becomes a sort of reflection of a sum. That is,

   $$\forall n \in N \quad n > 1 \quad \exists p < 2n \in P \quad 2n - p \in P$$

   Basically, we are saying that pairs of primes exist that sum to an even number, for all the even numbers greater than two. This allows us to think in pairs existing, a sort of symmetry, rather than just enumerating random sums and trying to come up with primes. Note that although this transformation is useless for now, the power of thinking of a statement flexibly in terms of logically equivalent statements is fascinating and a powerful skill maybe useful for other proofs.

Hopefully, as will be demonstrated in lecture soon, we can also see that Fermat's Little Theorem, which states

$$a^{p-1} \equiv 1 (mod \quad p)$$

where $1 \leq a \leq p - 1$ and $p \in P$, can be proven if we make a self-bijection of $GF(p)$ and we equate their complete products. The bijection and full proof will be made clear in the coming lessons. This is yet another example of proof transformation.

Of course, math is filled with intricate connections and amazing "coincidences" that turn out not be coincidences at all. The high amount of varying perspectives we can think about problems give what many believe to be the beauty of math and also the amazing amount of recollection that allow one mathematician to grasp another subfield of math. This is because at the bottom of it all, math is logic worked on different systems, and possibly worked on systems to transform into other systems as just presented.

3 Axiomatic systems and Formal Proofs

If one can think of transforming a proof into a easier, more fundamental, proof as a sort of "backwards" proof, then preceding from axioms of a system to a proof with inference rules is a sort of "forward" perspective. It may be more intuitive to proceed backwards from a proof and arrive to a tautology (always true logical expression) or axiom, but sometimes it is very confusing if not all inferences are bi-directional implications, and we wind up proving a converse or something like that instead. (Disclaimer: everything I'm about to say is going to be talking about a first-order logical system only)

The purpose of writing this section is to hopefully make clear the expectation of this course and graders instead of making it seem "pointlessly" rigorous. The best way to make sure your proof is correct is to start from known assertions - philosophically there must be some base assertion, and we call these axioms. Not all proofs have to be axiomatic, and rarely are because that would just be extremely tedious. However, it is important to start with the base given assertions; if we haven't derived anything else, we can ONLY use these assumptions. Then, write out in the same mathematical notation the goal, and try to use forward reasoning from the base assertions to the final goal. This allows you to at least thinking forwardly towards the proof, and make the path to the proof clearer. For example, many people get confused with what exactly is a bijection, and our minds can fools us sometimes when we think something is bijective (especially for infinite sets as we'll see in countability!). It might help to just write everything out in formal notation:

$$f : X \mapsto Y . Injective(f) : \forall m, n \in X \quad f(m) = f(n) \Longrightarrow m = n$$

$$Surjective(f) : \forall y \in Y \quad \exists x \in X \quad f(x) = y$$

Then, seeing if both injectivity and surjectivity satisfy for any given function rigorously should make a more exacting approach. Some students that have asked me about this found this approach helpful.

That being said, everything starts from axioms and essentially these are the fundamental assumptions of any system. Note that different systems can have contradictory axioms - many do. For example, in $GF(2)$ we have defined everything to be modular, such that $1+1=0$. This obviously contradicts with what we can observe in $\mathbf{Z}$, for instance.

Any system, thus, creates its own theory and its own logically derived axioms. This is actually a little bit into what deterministic Turing machines try to do with any axiomatic systems. Any system of axioms has three properties that may or may not be true:

1. Independent, or minimal. This is essentially a set of axioms that can't prove each other - any less assertions and there is no way that the same things would be true, and any more and we get redundant assertions. Technically it does not matter if a system is not independent, but since people like to see what is the least number of vague assumptions (since less assumption usually suggests a more provable system) this is desired.

2. Consistent. The axioms don't contradict each other and it's not possible to derive both a statement and its contradiction from the system.

3. Complete. For all statements related to this certain theory or system, it is possible to derive it or prove it to be false. There are no uncertain theorems.

One might wonder if it is possible for something to be both consistent and complete, since this is what we usually think of when we think of math systems - that they do not contradict nor is anything fuzzy. However, think of the statement

This statement is not provable in this math field F.

Clearly, we can see that since this statement can't both be proven/negated without violating either consistency or completeness, respectively. This is called **Godel's First Incompleteness Theorem** and although the actual proof is way more fleshed out and rigorous than my intuitive guide, it uses this as a sort of guidance.

3.1 Example of Formal Proof

Now it's time to show how formal proofs can get; that is even though something we are proving seems so obvious just by our longtime exposure to math, let's assume that we only have a few axioms and are trying to prove said obvious statement.

Consider the axiomatic system of an equivalence relation and equivalence structures. An equivalence structure (A, R^A) is a set A coupled with a binary relation R^A that satisfies the axioms of equivalence.

1. $\forall x \in A \quad xR^Ax$ (reflexive property)

2. $\forall x, y \in A \quad xR^Ay \iff yR^Ax$ (symmetric property)

3. $\forall x, y, z, \in A \quad (xR^Ay \wedge yR^Az) \implies xR^Az$ (transitive property)

Let's try to show now, that for an equivalence relation R (because the superscript was annoying to type in LaTex)

$$(xRu \wedge yRu) \implies \forall z \in A \quad (xRz \iff yRz)$$

This seems obvious when we think about equality, but starting from only those 3 base assumptions, it seems more annoying than originally thought. However, a rigorous proof makes no assumptions, so we have to continue.

1. uRy (symmetric property)
2. xRy (transitive property using xRu and uRy)
3. yRx (symmetric property on 2)
4. Now, prove the forward direction. Assume xRz
5. zRx (symmetric property)
6. Using zRx and xRy, we have zRy (transitive)
7. yRz (symmetric)
8. Now, prove backwards direction. Assume yRz. Everything from this point should be a symmetric proof
9. xRz using xRy and yRz, and we have already finished here (actually the forward proof should've been done this way, so manually edit that)

These types of proofs used to annoy me too, as they proved obvious things. However, using this technique allows you to prove nonobvious things from axioms, so it is a good skill to have to piece together axioms and inferences. Try working out other "obvious" equalities using these 3 axioms - it's a great rigorous exercise and will help your proof skills!

4 Additional topics

So, I don't claim to know all about this and this pretty much is all I have except for some details. For more in-depth knowledge this is all along the fields of mathematical logic (Math 125), abstract algebra (Math 113), and if you're into the Turing and Godel stuff, computation (CS 172).