Lecture 16

October 12, 2005

1 Motivation

In the previous lectures we have discussed algorithms for satisfiability, but so far we haven't been able to develop one for validity. In contrast to checking for satisfiability, where the witness is a simple truth assignment, to show validity we need to develop an entire proof. This lecture will focus on proofs of this type.

2 Deductions

Intuitively, a deduction is a sequence of statements, such that every statement follows from some statements before it. More formally, we say that there is a relation between the statements in the deduction. This relation can only refer to earlier elements, and is of arbitrary arity. The relation is defined as a subset of $Form^+$, and intuitively is a series of *antecedents* and one *consequent*.

We formalize the notion of a deduction in the following definitions.

Definition 1 (Deductive System). *A* Deductive System Γ *is a set* $\Gamma \subseteq Form^+$ *of relations, called* inference rules*.*

Definition 2 (Inference Rule). *An* inference rule *is a sequence of formulas* $<\varphi_1, \ldots, \varphi_k> \in \Gamma$*, also denoted as* $\frac{\varphi_1, \ldots, \varphi_{k-1}}{\varphi_k}$*. We say that* φ_k *follows from* $\varphi_1, \ldots, \varphi_{k-1}$*.*

An example of an inductive rule is Modus Ponens (M.P.): $\frac{p, p \rightarrow q}{q}$.

Definition 3 (Axioms). *An* axiom *is a particular type of an inference rule for which there are no antecedents. An axiom* φ *is denoted as* $<\varphi> \in \Gamma$*, or, equivalently, as* $\frac{}{\varphi}$*.*

Definition 4 (Deduction). *A valid* Γ*-Deduction is a sequence of formulas* $<\varphi_1, \ldots, \varphi_n>$ *such that for every* φ_i *there exist* $i_1, \ldots, i_k$*, where* $i_k < i$*, such that*

$$\frac{\varphi_{i_1}, \ldots, \varphi_{i_k}}{\varphi_i} \in \Gamma.$$

Intuitively, a deduction requires a justification for every statement. Note that this means that φ_1 must be an axiom, because there is nothing that could justify it.

Definition 5 (Γ-Deducibility). *If $< \varphi_1, \ldots, \varphi_n >$ is a Γ-Deduction, then we say that φ_n is Γ-Deducible, denoted by $\vdash_\Gamma \varphi_n$.*

The definitions so far are purely syntactical. A deduction can be seen as some evidence in support of the consequent. Naturally, we would like to know what is the connection between this evidence and Truth? Suppose that $\vdash_\Gamma \varphi$. What does this say about φ? We want to be able to prove only those things that are true, but is this always the case? We have the following

Desideratum: Whenever we have $\vdash_\Gamma \varphi$, we have $\models \varphi$.

Note that this desire relies on the inference rules in Γ. Clearly, if we have garbage in, we will get garbage out[1]. So we need to be able to define a good Γ. How do we do this?

Definition 6 (Soundness). *A deductive system Γ is* sound *if whenever $\vdash_\Gamma \varphi$ we have $\models \varphi$.*

Soundness of a deductive system is clearly a minimal condition on Γ, because we do not want unsound reasoning. But it is fairly easy to come up with a system that has this property. For example, the simplest system with this property is $\Gamma = \emptyset$. This deductive system cannot derive anything, thus it is vacuously true that everything it derives is valid. This motivates our next

Desideratum: Whenever $\models \varphi$ we have $\vdash_\Gamma \varphi$

Definition 7 (Completeness). *A deductive system is complete if whenever $\models \varphi$ we have $\vdash_\Gamma \varphi$.*

Completeness is also fairly easy to attain. The simplest system with this property is $\Gamma = \Sigma^*$. In this system everything is an axiom, therefore in particular every valid statement is an axiom and is deducible in 1 step. This observation motivates our next

Desideratum: $\models \varphi$ iff $\vdash_\Gamma \varphi$.

Propositional logic is sound *and* complete, so we have the best of both worlds. The completeness proof is fairly involved and thus it is outside of the scope of the class. One of Hilbert's dreams was to create a sound and complete system for Mathematics. His dream was shattered to pieces when Gödel proved this to be impossible.

In the remainder of this section we will focus on soundness.

Definition 8 (Sound). *An inference rule $\frac{\varphi_1, \ldots, \varphi_k}{\varphi}$ is* sound *if whenever $\models \varphi_1, \ldots, \models \varphi_k$, then $\models \varphi$.*

[1]Also known as the GIGO principle.

Definition 9 (Strongly Sound). *An inference rule* $\frac{\varphi_1,\ldots,\varphi_k}{\varphi}$ *is* strongly sound *if* $\{\varphi_1, \ldots, \varphi_k\} \models \varphi$.

Note that being strongly sound implies being sound.

Definitions 8 and 9 define soundness only for inference rules. We would like to know when a deductive system as a whole is sound. The following theorem is the answer to this question.

Theorem 1 (Soundness of a Deductive System). *A deductive system* Γ *is sound if and only if all the rules in* Γ *are sound*

Proof. We give a proof by induction on the length of the deduction.

- Base Case: Suppose that $< \varphi >$ is a Γ deduction. Then $< \varphi > \in \Gamma$, so φ must be an axiom, therefore $\models \varphi$.
- Inductive Step: Suppose that $< \varphi_1, \ldots, \varphi_n >$ is a Γ-deduction. By definition of a deduction there are $i_1, \ldots, i_k$, where $i_k < n$, such that $\frac{\varphi_{i_1},\ldots,\varphi_{i_k}}{\varphi_n}$. Since $\varphi_{i_1}, \ldots, \varphi_{i_k}$ occur earlier in the sequence, by the inductive hypothesis they are deducible and valid. Therefore, knowing that all rules are sound, and using Definition 8, it follows that $\models \varphi_n$.

□

It is fairly easy to get a sound and complete system. For example, the system $\Gamma = \{< \varphi > : \models \varphi\}$, which declares all valid formulas to be axioms, is sound and complete. This looks more like a paradox rather than a genuine sound and complete system[2]. There must be some other aspects of sound and complete proofs that we left out. The missing piece is that the steps of the proof should be fairly easy to follow. This our next and final

Desideratum: All deductions in Γ should be efficiently verifiable.

Definition 10 (Tractability). *Let Deductions*(Γ) *be the set of all* Γ*-Deductions.* Γ *is* tractable *if Deductions*$(\Gamma) \in PTIME$.

3 Hilbert's System

Hilbert discovered a very elegant deductive system that is both sound and complete. His system uses only the connectives $\{\neg, \rightarrow\}$, which we know are an adequate basis. It has also been shown that each of the 3 axioms given below are necessary for the system to be sound and complete. Hilbert's System consists of the following:

- Three axioms (all are strongly sound):

[2] This is known as a *model busting result* that shows that we failed to capture something.

– A1: $(p \to (q \to p))$ *Axiom of simplification.*

– A2: $((p \to (q \to r)) \to ((p \to q) \to (p \to r)))$ *Frege's axiom.*

– A3: $((\neg p \to q) \to ((\neg p \to \neg q) \to p))$ *Reductio ad absurdum.*

- Inference Rules:
  - Modus Ponens: $\frac{p, p \to q}{q}$ (Strongly Sound)
  - Substitution: $\frac{\varphi}{\varphi[\theta]}$, where θ is a substitution $(p \to \psi)$. (Sound)

The Substitution Inference Rule is shorthand for all sequences of the form $\langle \varphi, \varphi[\theta] \rangle$. It is sometimes called a schema for generating inference rules. Note that in general, it is not the case that $\varphi \models \varphi[\theta]$, for example p $\not\models$ q. However, in assignment 2, we showed that if $\models \varphi$, then $\models \varphi[\theta]$. This is why this rule is sound but not strongly sound.

Theorem 2. *Hilbert's system is sound, complete, and tractable.*

Proof. We prove each property separately.

- Soundness: Since all axioms are strongly sound, and the two inference rules are sound, the whole system is sound.

- Completeness: The proof of this property is fairly involved and thus it is outside the scope of the class.

- Tractability: Given $\Gamma \in \textsc{Form}^+$ and $\varphi_1, \ldots, \varphi_n$, is $\varphi_1, \ldots, \varphi_n \in \mathit{Deductions}(\Gamma)$?

  Clearly, $< \varphi_1 >$ is in Γ only if it is an axiom. But $< \varphi_2 >$ could be in Γ, $< \varphi_1, \varphi 2 >$ could be in Γ, $< \varphi_1, \varphi_1, \varphi_2 >$ could be in Γ, and so on. In order to check whether φ_2 is deducible, we have to check all possible deductions. This gets very hard to check!

  But if we know that the rules have bounded arity, this problem becomes easier. Clearly the arity of Hilbert's System is 3 since the maximum number of antecedents in an inference rule in the system is two. So the first condition of polynomial tractability holds. To check whether a formula can be deduced we have to check whether it is an axiom or modus ponens or the result of a substitution. All these can be checked in polynomial time by pattern matching if we think of axioms and rules as patterns, and if we can parse the formulas(to find substitutions):

  1. $< \varphi_1 > \in \Gamma$ (an axiom, easy to check).
  2. For φ_i, cycle over all $i_1, \ldots, i_k$, $i_k < i$, and check whether $< \varphi_{i_1}, \ldots, \varphi_{i_k}, \varphi_i > \in \Gamma$.

$\square$

Here, the cost of the loop is n^k for a fixed k, and is thus in PTIME. We still need to decide if the sequence is in Γ, but this can also be done in PTIME. This leads to the following theorem:

Theorem 3. *If Γ is of bounded arity and $\Gamma \in$ PTIME, then Γ is tractable.*

It is easy to check axioms and modus ponens, but the substitution rule is tricky.

$< \varphi, \psi >$ is an instance of the substitution rule, iff there is a substitution θ such that $\psi = \varphi[\theta]$. This yields the *Matching Problem*: Given φ and ψ, is there a substitution θ such that $\psi = \varphi[\theta]$? Matching is in P-time, so Hilbert's system is tractable.