Lecture 11: Deductions

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, which is NP-complete, where the witness is a simple truth assignment, validity is co-NP-complete, where a truth assignment is a counter example. This mean that to show validity we have to examine all truth assignment. We are interested in a more principled approach to demonstrate validity, and the focus of this lecture is on proofs of validity.

2 Proof Systems

NOTATION: The notations $*$ and $+$ are briefly described here. X^* denotes an empty or sequence whereas X^+ denotes a non-empty sequence.

Recall that a decision problem P is just a subset of Σ^* for some finite alphabet Σ. The problem is then to decide if a given word $w \in \Sigma^*$ is in P.

Definition 1. *A* proof system *for a decision problem P is a computable function $f : \Delta^* \times \Sigma^* \to \{0, 1\}$, for some finite alphabet Δ, such that*

- *For each $t \in \Sigma^*$ and $u \in \Delta^*$, if $f(u, t) = 1$ then $t \in P$.*
- *for each $t \in P$ there is some $u \in \Delta^*$ such that $f(u, t) = 1$.*

The intuition is that is that $f(u, t) = 1$ means that u is a proof of t, (where Δ is the alphabet of proofs). Condition (1) in the definition says that if t has a proof u, then $t \in P$. Condition (2) says that if $t \in P$, then t has some proof u.

An immediate consequence of this definition is that if P has a proof system that P is computationally enumerable. To check if $t \in P$ for a given $t \in \Sigma^*$, we can enumerate all words $u \in \Delta^*$ and check for each one if $f(u, t) = 1$. If $t \in P$, then we will eventually find a proof. (But if $t \notin P$, then this algorithm will not terminate.)

This definition gives us an *algorithmic lense* on mathematics, because we need to understand computability in order to understand proofs, which are the essential features of mathematics.

3 Deductions

The above algorithmic definition of proof systems does not have the step-by-step feature of traditional mathematicsl proofs. We now introduce the notion of *deductions*, which captures this intuition.

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

Definition 3 (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.): $\frac{p, p \to q}{q}$.

Definition 4 (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 5 (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 6 (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?

[1] Also known as the GIGO principle.

Definition 7 (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 8 (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.

Gödel's Incompleteness Theorem: For every deductive system Γ for arithmetics, there is an arithmetical statement φ_Γ such that $\not\vdash_\Gamma \varphi_\Gamma$ and $\not\vdash_\Gamma (\neg\varphi_\Gamma)$.

Fortunately, for propositional logic we can attain both soundness and completeness.

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

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

Definition 10 (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 9 and 10 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 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 9, 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 11 (Tractability)**.** *Let Deductions*(Γ) *be the set of all* Γ*-Deductions.* Γ *is* tractable *if Deductions*$(\Gamma) \in PTIME$*.*

In fact, tractability should also be a feature of more general proof systems:

Definition 12. *A tractable proof system for a decision problem P is an onto PTIME function $f : \Delta^* \to P$, for some finite alphabet Δ.*

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