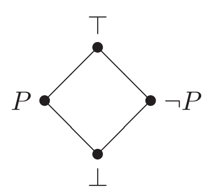
Lecturer: Dexter Kozen

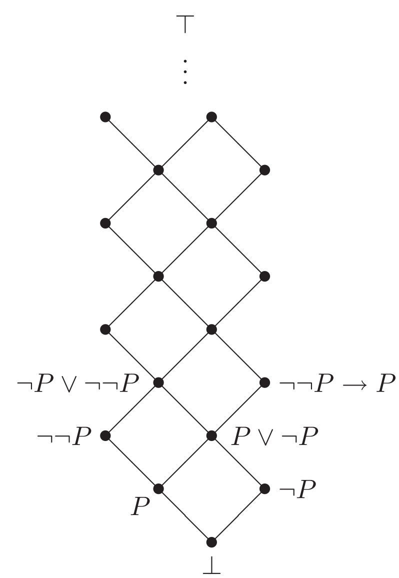
1 A Digression on Heyting Algebra

As discussed last time, there are fewer formulas that are considered intuitionistically valid than classically valid. The law of double negation ($\neg\neg\varphi \to \varphi$), the law of excluded middle ($\varphi \vee \neg\varphi$), and proof by contradiction or reductio ad absurdum are no longer accepted.

Boolean algebra is to classical logic as *Heyting algebra* is to intuitionistic logic. A Heyting algebra is an algebraic structure of the same signature as Boolean algebra, but satisfying only those equations that are provable intuitionistically. Whereas the free Boolean algebra on n generators has 2^{2^n} elements, the free Heyting algebra on one generator has infinitely many elements.



Free Boolean algebra on one generator



Free Heyting algebra on one generator

The picture on the right is sometimes called the *Rieger–Nishimura ladder*.

2 Extracting Computational Content

Many automated deduction systems, such as NuPrl and Coq, are based on constructive logic. Automatic programming was a significant research direction that motivated the development of these systems. The idea was that a constructive proof of the existence of a function would automatically yield a program to compute it: the statement asserting the existence of the function is a type, and a constructive proof yields a λ-term inhabiting that type. For example, to obtain a program computing square roots, one merely has to give a constructive proof of the statement $\forall x \geq 0\ \exists y\ y^2 = x$.

3 Other Directions

Many fruitful correspondences have been found between constructive logic and types. Other logics have been used to give intuition about typing systems and vice versa.

For example, *linear logic* is a logic that keeps track of resources. One may only use an assumption in the application of a rule once; the assumption is consumed and may not be reused. This corresponds to functions that consume their arguments, and hence is a possible model for systems with bounded resources.

4 KAT Demo

The remainder of the lecture was a demo of the KAT interactive proof assistant. This system is based on constructive equational logic of universal Horn formulas (formulas of the form $\forall\bar{x}\ s_1 = t_1 \to \cdots \to s_n = t_n \to s = t$). In the demo, we illustrated how proofs are represented as λ-terms that are extracted automatically as rules are applied.

The system is available for downloading from http://www.cs.cornell.edu/Projects/KAT/.