

“Proof Systems in Computer Science”

Jeremy Avigad

Abstract

I will describe various types of proof systems that arise in computer science, including interactive proof systems, cryptographic proof protocols, and proof calculi and exchange formats for automated reasoning. I will also explore some of the goals and constraints that the designers of such systems have to answer to.