1014-68-1107 **Madhu Sudan***, The Stata Center, 32 Vassar Street, Cambridge, MA 02139. *Probabilistically Checkable Proofs.*

Probabilistically checkable proof (PCP) systems provide a methodology for writing and verifying proofs so that verification of proofs becomes extremely easy, though occasionally the verification procedure (verifier) makes errors. Specifically in such a system the verifier probabilistically probes a purported proof of an assertion in only a constant number of bits (independent of the length of the proof/assertion) and always accepts valid proofs using the right methodology (format) while rejecting any claimed proof of an invalid assertion with constant probability. The PCP theorem, first proven in the early 90s, shows (somewhat surprisingly) that PCP systems do exist where the length of the proofs in the new format is only slightly (polynomially) longer than their length is any other proof system. Recently a new (and significantly simpler) construction of PCP systems was given by Irit Dinur. In the talk, we will attempt to describe the notion of a PCP, its relevance to computational complexity, and, time permitting, give a bird's eye view of Dinur's construction. (Received September 27, 2005)