Proofs and algorithms

Boaz Barak

**Disclaimer:** The MS-Word version of this text has significant formatting issues compared to the PDF and HTML versions.

# Proofs and algorithms

*“Let’s not try to define knowledge, but try to define zero-knowledge.”*, Shafi Goldwasser.

*Proofs* have captured human imagination for thousands of years, ever since the publication of Euclid’s *Elements*, a book second only to the bible in the number of editions printed.

Plan:

* Proofs and algorithms
* Interactive proofs
* Zero knowledge proofs
* Propositions as types, Coq and other proof assistants.

## Exercises

## Bibliographical notes