FOUNDATIONS AND FRONTIERS OF PROBABILISTIC PROOFS

Summer Graduate School Online

ZISC, ETH Zürich, Switzerland, July 26 to August 6, 2021

Suggested prerequisites

(1) *Fundamentals of computational complexity.*

For example, chapters 1, 2, 4, 6, 7 of

> S. Arora and B. Barak, *Computational complexity: A modern approach*, Cambridge University Press, Cambridge, 2009, ISBN 978-0-521-42426-4. MR 2500087. Zbl 1193.68112. doi: 10.1017/CBO9780511804090

Most importantly:

- Turing machines, complexity classes, and reductions (1.2-1.5, 2.2).
- The Cook-Levin theorem (2.3).
- Familiarity with the classes P, NP, PSPACE, NEXP, and their complete languages (1.6, 2.1, 2.6, 4.1, 4.2).
- The computation model of Boolean circuits, circuit satisfiability, and exponential size circuits (6.1-6.4, 6.8).
- Probabilistic computation and the class BPP (7.1-7.4).

(2) *Basic knowledge of finite fields and their properties.*

For example, as covered in the following references:

- D. Forney, Introduction to finite fields, 2005, chapter 7, lecture notes
- A. Sutherland, Finite fields and integer arithmetic, 2017, chapter 3, lecture notes
- V. Guruswami, Basics of finite fields, 2014, cheat sheet

Further reading

O. Goldreich, *Computational complexity: A conceptual perspective*, Cambridge University Press, Cambridge, 2008, ISBN 978-0-521-88473-0. MR 2400985. Zbl 1154.68056. doi: 10.1017/CBO9780511804106

O. Goldreich, *Introduction to property testing*, Cambridge University Press, Cambridge, 2017, ISBN 978-1-107-19405-2. MR 3837126. Zbl 06797790. doi: 10.1017/9781108135252

Date: April 19, 2021.

Bibliography by Alessandro Chiesa.