Seminar on Randomness Extractors

Gil Cohen

October 24, 2022

Overview

Randomness extractors

Randomness extractors are algorithms that "extract" high-quality randomness from weak random sources.

They were introduced when studying randomness but also in cryptography and in space-bounded derandomization

- von Neumann 1951
- Santha-Vazirani 1984
- Chor-Goldreich 1984
- Chor-Goldreich-Hastad-Freidmann-Rudich-Smolensky 1985
- Nisan-Zuckerman 1993

Extractors are extremely useful in TOC, coding theory, cryptography, and are related to questions in combinatorics. Randomness extractors theory is a vibrant research field.

About me

I am a theoretical computer scientist

Technion → Weizmann
→ Caltech
→ Princeton
→ Tel Aviv University

My interests are

1. Complexity theory, especially randomness related questions
2. Pseudo-randomness and explicit constructions
3. Coding theory (tree codes, LCC, AG codes)
4. Spectral graph theory

Course mechanics

1. We meet physically on Mondays 9:10-11 at Shenkar-Physics Building, room 204.
2. `https://www.gilcohen.org/2022-extractors-seminar`.
3. Strong preference to board talks.
4. I will ask questions both to measure understanding and for clarification.
5. You are welcome to consult with me prior to your talk. Schedule by email. Do not wait for the day before the talk.
6. Most papers cannot be covered in two hours, even when restricted to the part I would ask you to read. It is your responsibility to decide what to present in-depth and what to cover at a high-level.

Grade and participation

The grade will be determined by

1. The quality of the lecture, including its preparation, presentation, and level of understanding.
2. Participation during the talks.

Grade and participation

All students are required to physically attend the seminar. However,

1. A student may choose not to attend one lecture (email me before the lecture you are about to miss). Missing two or more lectures will affect the grade.
2. We will not connect remotely (say, via Zoom).

Overview

Tips

1. Understand everything you are asked to read to the deepest level you possibly can.
2. Read a bit more to get the context.
3. Digest with friends.
4. Practice your talk prior to the meeting at least twice.
5. Welcome questions during your talk.

Overview

Part 0 - Introduction

Lecture 1. An introduction to randomness extractors (given by the lecturer).

Lecture 2. Kakeya sets, new mergers and old extractors by Dvir and Wigderson (given by the lecturer).

Part 1 - Seeded extractors

Lecture 3. Basic constructions of extractors from Vadhan's survey

Lecture 4. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes by Guruswami, Umans, and Vadhan

Part 2 - 3-Source extractors and 2-source dispersers

Lecture 5. An exposition of Bourgain's 2-source extractor by Rao

Lecture 6. Extracting randomness using few independent sources by Barak, Impagliazzo and Wigderson

Lecture 7. Extractors for a constant number of independent sources with polylogarithmic min-entropy by Li

Lecture 8. Three-source extractors for polylogarithmic min-entropy by Li

Lecture 9. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs by Cohen

Part 3 - Non-malleable extractors and 2-source extractors

Lecture 10. Non-malleable extractors with short seeds and applications to privacy amplification by Cohen, Raz and Segev

Lecture 11. Local correlation breakers and applications to three-source extractors and mergers by Cohen

Lecture 12. Non-malleable extractors and codes, with their many tampered extensions by Chattopadhyay, Goyal, and Li

Lecture 13. Explicit two-source extractors and resilient functions by Chattopadhyay and Zuckerman

Overview

What's next?

1. I will give some background today and next week.
2. Each student will email me (coheng@gmail.com) its first, second and third choice by the end of October 27, and I will try to accommodate your requests. There are no guarantees.