Preface

Roughly speaking, a *deterministic extractor* is a function that 'extracts' almost perfect random bits from a 'weak random source' - a distribution that contains some entropy but is far from being truly random. In this book we explicitly construct deterministic extractors and related objects for various types of sources. A basic theme in this book is a methodology of recycling randomness that enables increasing the output length of deterministic extractors to near-optimal length. Our results are as follows.

Deterministic Extractors for Bit-Fixing Sources An (n, k)-*bit-fixing source* is a distribution X over $\{0,1\}^n$ such that there is a subset of k variables in $X_1, \ldots, X_n$ that are uniformly distributed and independent of each other, and the remaining $n - k$ variables are fixed in advance to some (unknown) constants. We give constructions of deterministic bit-fixing source extractors that extract $(1-o(1))k$ bits whenever $k > (\log n)^c$ for some universal constant $c > 0$. Thus, our constructions extract almost all the randomness from bit-fixing sources and work even when k is small. Our technique gives a general method to transform deterministic bit-fixing source extractors that extract few bits into extractors which extract almost all the bits.

Deterministic Extractors for Affine Sources over Large Fields An (n, k)-*affine source* over a finite field $\mathbb{F}$ is a random variable $X = (X_1, ..., X_n) \in \mathbb{F}^n$, that is uniformly distributed over an (unknown) k-dimensional affine subspace of $\mathbb{F}^n$. There has been much interest lately in extractors for affine sources over $\mathbb{F}_2$. It can be shown that a random function $D : \{0,1\}^n \mapsto \{0,1\}$ is with high probability an extractor for (n, k)-affine sources over $\mathbb{F}_2$ whenever $k \geq 3 \cdot \log n$. The best explicit construction due to Bourgain [10] works when $k = \delta \cdot n$ for constant δ.

We focus on the case of a *large* field, specifically, a field of size n^c for constant $c > 0$, i.e., a field size that is polynomially large in the dimension of the space. When working with a field of size larger than n^{20} we show how to deterministically extract practically all the randomness from an (n, k)-affine source for any $k \geq 2$.

Extractors and Rank Extractors for Polynomial Sources We construct explicit deterministic extractors from *polynomial sources*, namely from distributions sampled by low degree multivariate polynomials over finite fields. This naturally generalizes previous work on extraction from affine sources (which are degree 1 polynomials).

The first step in our construction is a construction of *rank extractors*, which are polynomial mappings that "extract" the algebraic rank from any system of low-degree polynomials. More precisely, for any n polynomials, k of which are algebraically independent, a rank extractor outputs k algebraically independent polynomials of slightly higher degree.

We then use theorems of Wooley and Bombieri from algebraic geometry, which enable us to extract a constant fraction of the randomness from 'full rank' polynomial sources when the field is exponentially large in the degrees of the defining polynomials.

Increasing the Output Length of Zero-Error Dispersers A zero-error disperser for a family of weak random sources is a function that guarantees the output distribution will have full support for any source in the family. We develop a general method of increasing the output length of zero-error dispersers. We use this method to significantly improve previous constructions. More specifically, we obtain zero-error dispersers for 2-independent sources, bit-fixing sources and affine sources over large fields with output length $\Omega(k)$ where k is the min-entropy of the source.

April 2010 Ariel Gabizon

Acknowledgements

This monograph is based on my doctoral dissertation, written under the supervision of Ran Raz and Ronen Shaltiel, and submitted to the Weizmann Institute in Israel in June 2008. Above all, I'd like to thank my advisors Ran and Ronen for showing a lot of faith in me and my abilities when I started out.

Ran showed a very positive attitude from the start and gave the feeling that 'anything is possible' and 'everything is going great'. This created a very comfortable and carefree environment for doing research for me, where I felt what I had already done was great and I was free to try out anything in the future. This feeling was preserved due to Ran's ability to remain open-minded and patient throughout the years. For me, Ran is an incredible model for clarity of thought, effective thought and patience with people (and these qualities indeed manifested in a few crucial points of the research).

This thesis began with an idea of Ronen Shaltiel on the possibility of 'recycling randomness' in a certain situation. This idea became a central theme to which almost all results in this thesis are connected. Thus, I owe this thesis to Ronen in a very concrete sense. I am grateful to Ronen for the great willingness, enthusiasm and modesty with which he shares his knowledge. Indeed, it was at a colloquium lecture of Ronen at the Hebrew University that I first realized how cool pseudorandomness and complexity theory are. Ronen has helped direct and focus me with his 'stock' of great research directions, and his almost magical ability to take any vague idea you bring, develop it, find where it may be useful, all the while making it seem like it is still just *your* idea!

During the last year and a half of the thesis I spent a lot of time learning about function fields and algebraic geometric codes. This became much more effective in the last few months thanks to Irit Dinur who took active interest in the learning process, invested a lot of time, and created an environment where I was forced, to a certain extent, to really know what I was talking about.

I'd like to thank Chris Umans for a great two weeks spent working with him at Caltech. He really taught me what it is like to 'brainstorm' with someone and inspired me with his evident passion for research. Thanks to my coauthors Zeev Dvir and Avi Wigderson who participated in the research presented here (Chapter 4 is joint research with them). I had a fun and fruitful time in China thanks to Andy Yao's inviting me to China Theory Week 2007. Thanks to my PhD committee Oded Goldreich and Omer Reingold. Thanks again to Oded Goldreich for useful comments on all chapters in this monograph.

There was a talented theory group at Weizmann thanks to Zeev Dvir, Dana Moshkovitz, Amir Yehudayoff, Anup Rao (who visited for a summer), Adi Shraibman, Danny Harnik, Tal Moran, Ronen Gradwohl, Gil Segev, Iftach Haitner, Noam Livne, Yuval Emek, Asaf Nussbaum, Shachar Lovett, Erez Kantor, Gillat Kol, Or Meir, Zvika Brakerski, Omer Kadmiel, Ran Halprin, Chandan Dubey and Guy Kindler. I feel grateful that I was able to spend my time in a field full of creativity, depth and beauty. I think that doing this for a living is really a privilege.

The Weizmann Institute will always have a special place in my heart. With every day that passed, through meeting impressive and inspiring people, and enjoying the great freedom we have to develop both personally and professionally, I became more convinced what a great place Weizmann is. I could also say Weizmann is 'in my blood', as I was born to two Weizmann Ph.D. students who met at the Wolfson building right across from the building where I worked all those years.

My period at Weizmann started rather spontaneously. I actually started my graduate studies elsewhere. Towards the end of the first semester, while browsing the Weizmann web site and seeing the courses for the next semester, I had a strong feeling I should move to Weizmann immediately, and study complexity theory.

A possible definition of 'fate' might be 'the things that start working out when you give a small nudge in their direction'. A friend of mine, who was already a Weizmann student said I could move into a spare room in his apartment in Rehovot. I am very grateful to him, as knowing my laziness in these matters and my fear of unknown roommates, and with only a few weeks left till the beginning of the second semester, without his offer there is a good chance I would have forsaken the plan. I also want to thank Uri Feige who was my 'first contact' with the department. Uri was then in charge of teaching, and I phoned him to ask about the possibility of taking courses as an informal student. He was extremely kind and patient with my questions and helped me relax and feel that 'it was going to be OK'.

I distinctly remember the day I moved to Rehovot, arriving that evening with my luggage at my friend's apartment. For me, that moment was a sharp turning point, setting in motion a new course in my life.

To my family and all the good people I met during those 5 years, thank you for your support. May you be happy.

http://www.springer.com/978-3-642-14902-3

Deterministic Extraction from Weak Random Sources
Gabizon, A.
2011, XII, 148 p., Hardcover
ISBN: 978-3-642-14902-3