Extractors and Rank Extractors for Polynomial Sources

Zeev Dvir[*] Ariel Gabizon[†] Avi Wigderson[‡]

Abstract

In this paper we construct explicit deterministic extractors from *polynomial sources*, which are 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). A direct consequence is a deterministic extractor for distributions sampled by polynomial size arithmetic circuits over exponentially large fields. The steps in our extractor construction, and the tools (mainly from algebraic geometry) that we use for them, are of independent interest:

The first step is a construction of *rank extractors*, which are polynomial mappings which "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. The rank extractors we construct are applicable not only over finite fields but also over fields of characteristic zero.

The next step is relating algebraic independence to min-entropy. We use a theorem of Wooley to show that these parameters are tightly connected. This allows replacing the algebraic assumption on the source (above) by the natural information theoretic one. It also shows that a rank extractor is already a high quality *condenser* for polynomial sources over polynomially large fields.

Finally, to turn the condensers into extractors, we employ a theorem of Bombieri, giving a character sum estimate for polynomials defined over curves. It allows extracting all the randomness (up to a multiplicative constant) from polynomial sources over exponentially large prime fields.

[*] Department of Computer Science, Weizmann institute of science, Rehovot, Israel. `zeev.dvir@weizmann.ac.il`.
Research supported by Binational Science Foundation (BSF) grant and by Minerva Foundation grant.

[†] Department of Computer Science, Weizmann institute of science, Rehovot, Israel. `ariel.gabizon@weizmann.ac.il`.
Research supported by Binational Science Foundation (BSF) grant and by Minerva Foundation grant.

[‡] Institute for Advanced Study, Princeton, NJ, `avi@ias.edu`