Randomness Conductors and Constant-Degree Expansion Beyond the Degree / 2 Barrier

PRELIMINARY VERSION

Michael Capalbo[*] Omer Reingold[†] Salil Vadhan[‡] Avi Wigderson[§]

November 15, 2001

Abstract

The main concrete result of this paper is the first explicit construction of constant degree *lossless* expanders. In these graphs, the expansion factor is almost as large as possible: $(1-\epsilon)D$, where D is the degree and ϵ is an arbitrarily small constant. Such graphs are essential components in networks that can implement fast distributed, routing algorithms e.g. [PU89, ALM96, BFU99]. They are useful in expander-based linear codes e.g. [SS96, Spi96, LMSS01]. Their highly unbalanced relatives are used in various storage schemes [UW87, BMRS00] and are the basis of hard tautologies for various proof systems [BW99, ABRW00, AR01]. The best previous explicit constructions gave expansion factor $D/2$, which is too weak for the above applications. The $D/2$ bound was obtained via the eigenvalue method, and as shown in [Kah95], this method cannot give better bounds.

The main abstract contribution of this paper is the introduction and initial study of *randomness conductors*, a notion which generalizes extractors, expanders, condensers and other similar objects. In all these functions, certain guarantee on the input "entropy" is converted to a guarantee on the output "entropy". For historical reasons, specific objects used specific guarantees of different flavors (eg in expanders entropy means "support size", and their property is satisfied whenever input entropy is small. In contrast, in extractors, entropy means "min-entropy" and their property is satisfied whenever input entropy is large). We show that the flexibility afforded by the conductor definition leads to interesting combinations of these objects, and to better constructions such as those above.

The main technical tool in these constructions is a natural generalization to conductors, of the zig-zag products defined by [RVW00] for expanders and extractors. This product maintains certain conductivity properties of the conductors it combines, leading to new iterative constructions.

Keywords: expander graphs, extractors, condensers, graph products.

[*]Institute for Advanced Study, School of Mathematics, Einstein Drive, Princeton, NJ 08540. E-mail: `mrc@ias.edu`.

[†]AT&T Labs - Research. Room A243, 180 Park Avenue, Bldg. 103, Florham Park, NJ, 07932, USA. E-mail: `omer@research.att.com`. Part of this research was performed while visiting the Institute for Advanced Study, Princeton, NJ.

[‡]Harvard University, Division of Engineering and Applied Sciences, Maxwell Dworkin 337, 33 Oxford Street Cambridge, MA 02138, USA. E-mail: `salil@eecs.harvard.edu`. URL: `http://www.eecs.harvard.edu/~salil`. Work begun while at MIT and the Institute for Advanced Study, supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

[§]Institute for Advanced Study, Princeton and the Hebrew University, Jerusalem. Address: Institute for Advanced Study, School of Mathematics, Einstein Drive, Princeton, NJ 08540. E-mail: `avi@ias.edu`.