Randomness Conductors and Constant-Degree Lossless Expanders*

(_abstract)

Michael Capalbo
Institute for Advanced Study
Princeton, NJ
mrc@ias.edu

Omer Reingold†
AT&T Labs — Research
Florham Park, NJ
omer@research.att.com

Salil Vadhan‡
Harvard University
Cambridge, MA
salil@eecs.harvard.edu

Avi Wigderson
Hebrew University, Jerusalem, and
Institute for Advanced Study, Princeton
avi@ias.edu

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 \(\epsilon\) is an arbitrarily small constant. Such graphs are known to have many applications, e.g. in constructing networks that can implement fast distributed, routing algorithms, expander-based linear codes, various storage schemes, and hard tautologies for various proof systems. The best previous explicit constructions gave expansion factor \(D/2\), which is too weak for many applications. The \(D/2\) bound was obtained via the eigenvalue method, and is known that that 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 (e.g., 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 graph product, previously defined for expanders and extractors.

Consider a bipartite graph \(G\) with \(N\) inputs \(I\), \(M\) outputs \(O\), and every input connected to \(D\) outputs. \(G\) is called an \((K,A)\)-expander if every set \(X\) of at most \(K\) inputs is connected to at least \(A \cdot |X|\) outputs. The \(D/2\) bound was obtained via the eigenvalue method, and is known that that 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 (e.g., 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 graph product, previously defined for expanders and extractors.

Consider a bipartite graph \(G\) with \(N\) inputs \(I\), \(M\) outputs \(O\), and every input connected to \(D\) outputs. \(G\) is called an \((K,A)\)-expander if every set \(X\) of at most \(K\) inputs is connected to at least \(A \cdot |X|\) outputs.

Clearly, the best one can hope for with these parameters is \(A\) as close as possible to \(D\); when \(A = (1 - \epsilon) \cdot D\) for a small \(\epsilon\) we call the expander lossless. We can hope for such expansion factor only up to \(K \approx M/D\). A nonconstructive probabilistic argument shows that such graphs exist with \(D \approx O(\log(N/M))\), and this value of \(D\) is best possible. (Here and below, we fix \(\epsilon\) to be an arbitrarily small constant for simplicity.)

Our main result is an explicit construction of such “lossless” expanders for any setting of the parameters \(N,M\). When they are within a constant factor of each other, the degree of our graphs is constant, and linear-sized subsets of \(N\) expand losslessly. More specifically, the degree of our graphs is \(D = \text{o}(\log(N/M))\) when \(N/M\) is relatively small (so that an optimal graph of size \(\text{o}(N/M)\) can be found by, say, exhaustive search) and \(D = \exp(\text{polylog}(N/M))\) in general. (Here, for simplicity, we fix \(\epsilon\) to be an arbitrarily small constant). The size of sets that expand losslessly in all cases is \(\Omega(M/D)\), which is the best possible up to a constant factor.

---

* A full version of this paper will be posted on the Electronic Colloquium on Computational Complexity, http://www.eccc.uni-trier.de/eccc/.
† Part of this research was performed while visiting the Institute for Advanced Study, Princeton, NJ.
‡ Work begun while at MIT and the Institute for Advanced Study, supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.