Improved Decoding of Expander Codes

Xue Chen[1]
University of Science and Technology of China, Anhui, China

Kuan Cheng
Peking University, China

Xin Li
Johns Hopkins University, Baltimore, MD, USA

Minghui Ouyang
Peking University, China

Abstract

We study the classical expander codes, introduced by Sipser and Spielman [10]. Given any constants $0 < \alpha, \varepsilon < 1/2$, and an arbitrary bipartite graph with N vertices on the left, $M < N$ vertices on the right, and left degree D such that any left subset S of size at most αN has at least $(1-\varepsilon)|S|D$ neighbors, we show that the corresponding linear code given by parity checks on the right has distance at least roughly $\frac{\alpha N}{2\varepsilon}$. This is strictly better than the best known previous result of $2(1-\varepsilon)\alpha N$ [11, 12] whenever $\varepsilon < 1/2$, and improves the previous result significantly when ε is small. Furthermore, we show that this distance is tight in general, thus providing a complete characterization of the distance of general expander codes.

Next, we provide several efficient decoding algorithms, which vastly improve previous results in terms of the fraction of errors corrected, whenever $\varepsilon < \frac{1}{4}$. Finally, we also give a bound on the list-decoding radius of general expander codes, which beats the classical Johnson bound in certain situations (e.g., when the graph is almost regular and the code has a high rate).

Our techniques exploit novel combinatorial properties of bipartite expander graphs. In particular, we establish a new size-expansion tradeoff, which may be of independent interests.

2012 ACM Subject Classification Mathematics of computing → Coding theory

Keywords and phrases Expander Code, Decoding

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.43

Related Version *Full Version*: `http://arxiv.org/abs/2111.07629`

Funding *Xin Li*: Supported by NSF CAREER Award CCF-1845349 and NSF Award CCF-2127575.

1 Introduction and Our Results

Expander codes [10] are error-correcting codes derived from bipartite expander graphs that are notable for their ultra-efficient decoding algorithms. In particular, all known asymptotically good error-correcting codes which admit (almost) linear-time decoding algorithms for a constant fraction of adversarial errors are based on expander codes. At the same time, expander codes are closely related to low-density parity-check (LDPC) codes [6] – a random LDPC code is an expander code with high probability. Over the last twenty years, LDPC codes have received increased attention ([5, 4, 1, 3, 8] to name a few) because of their practical performance. Along this line of research, the study of decoding algorithms for expander codes, such as belief-propagation [6, 10, 7], message-passing [9], and linear programming [5, 4, 13], has laid theoretical foundations and sparked new lines of inquiry for LDPC codes.

[1] Part of this work is done while the author was at George Mason University.

In this work, we consider expander codes for adversarial errors. Briefly, given a bipartite graph G with N vertices of degree D on the left, we say it is an $(\alpha N, (1-\varepsilon)D)$ expander if and only if any left subset S with size at most αN has at least $(1-\varepsilon)D \cdot |S|$ distinct neighbors. The code $\mathcal{C}$ of an expander G assigns a bit to each vertex on the left and views each vertex on the right as a parity check over its neighbors. A codeword $C \in \mathcal{C}$ is a vector in $\{0,1\}^N$ that satisfies all parity checks on the right. Moreover, the distance of $\mathcal{C}$ is defined as the minimum Hamming distance between all pairs of codewords. For typical applications, the parameters α, ε and D are assumed to be constants, and there exist explicit constructions (e.g., [2]) of such expander graphs with $M < N$.

For expander codes defined by $(\alpha N, (1-\varepsilon)D)$-expanders, the seminal work of Sipser and Spielman [10] gave the first efficient algorithm to correct a constant fraction (i.e., $(1-2\varepsilon)\cdot\alpha N$) of errors, when $\varepsilon < 1/4$. In fact, their algorithms are super efficient – they provide a linear time algorithm called belief-propagation and a logarithmic time parallel algorithm with a linear number of processors. Subsequently, Feldman et al. [4] and Viderman [13, 12] provided improved algorithms to correct roughly $\frac{1-3\varepsilon}{1-2\varepsilon} \cdot \alpha N$ errors, when $\varepsilon < 1/3$. This fraction of error is strictly larger than that of [10] whenever $\varepsilon < 1/4$. Viderman [12] also showed how to correct $N^{\Omega_{D,\varepsilon,\alpha}(1)}$ errors when $\varepsilon \in [1/3, 1/2)$, and that $\varepsilon < 1/2$ is necessary for correcting even 1 error. However, the following basic question about expander codes remains unclear.

Question: What is the best distance bound one can get from an expander code defined by arbitrary $(\alpha N, (1-\varepsilon)D)$-expanders?

This question is important since it is well known that for unique decoding, the code can and can only correct up to half the distance number of errors. In [10], Sipser and Spielman showed that the distance of such expander codes is at least αN, while a simple generalization improves this bound to $2(1-\varepsilon)\alpha N$ (see e.g., [11] and [12]). Perhaps somewhat surprisingly, this simple bound is the best known distance bound for an arbitrary expander code. In fact, Viderman [12] asserted that this is the best distance bound one can achieve based only on the expansion property of the graph, and hence when ε converges to 0, the number of errors corrected in [12], $\frac{1-3\varepsilon}{1-2\varepsilon} \cdot \alpha N$ converges to the half distance bound. Yet, no evidence was known to support this claim. Thus it is natural to ask whether any improvement is possible, and if so, can one design efficient algorithms to correct more errors?

In this work, we give affirmative answers to the above questions, as well as improved linear time decoding algorithms. Our results can be summarized as follows.

▶ **Theorem 1.** *Given any $(\alpha N, (1-\varepsilon)D)$-expander, let $\mathcal{C}$ be the expander code defined by it. The distance of $\mathcal{C}$ is at least $\frac{\alpha}{2\varepsilon} \cdot N - O_\varepsilon(1)$.*

Moreover, for any constant $\eta > 0$ there exists an $(\alpha N, (1-\varepsilon)D)$-expander whose expander code has distance at most $(\frac{\alpha}{2\varepsilon} + \eta) \cdot N$.

Table 1 Summary of the distance and decoding radii for ε.

	$\varepsilon \in (0, \frac{3-2\sqrt{2}}{2})$	$\varepsilon \in [\frac{3-2\sqrt{2}}{2}, 1/8)$	$\varepsilon \in [1/8, 1/4)$
Distance from Theorem 1 of this work	$\frac{1}{2\varepsilon} \cdot \alpha N$	$\frac{1}{2\varepsilon} \cdot \alpha N$	$\frac{1}{2\varepsilon} \cdot \alpha N$
Decoding radius from [4, 12]	$\frac{1-3\varepsilon}{1-2\varepsilon} \cdot \alpha N$	$\frac{1-3\varepsilon}{1-2\varepsilon} \cdot \alpha N$	$\frac{1-3\varepsilon}{1-2\varepsilon} \cdot \alpha N$
Decoding radius from this work	$\frac{\sqrt{2}-1}{2\varepsilon} \cdot \alpha N$	$\frac{1-2\varepsilon}{4\varepsilon} \cdot \alpha N$	$\frac{3}{16\varepsilon} \cdot \alpha N$

References

1 Sanjeev Arora, Constantinos Daskalakis, and David Steurer. Message-passing algorithms and improved LP decoding. *IEEE Trans. Inf. Theory*, 58(12):7260–7271, 2012. doi:10.1109/TIT.2012.2208584.

2 Michael Capalbo, Omer Reingold, Salil Vadhan, and Avi Wigderson. Randomness conductors and constant-degree lossless expanders. In *Proceedings of the 34th Annual ACM STOC*, pages 659–668. ACM, 2002.

3 A. G. Dimakis, R. Smarandache, and P. O. Vontobel. Ldpc codes for compressed sensing. *IEEE Transactions on Information Theory*, 58(5):3093–3114, 2012.

4 J. Feldman, T. Malkin, R. A. Servedio, C. Stein, and M. J. Wainwright. Lp decoding corrects a constant fraction of errors. *IEEE Transactions on Information Theory*, 53(1):82–89, 2007. doi:10.1109/TIT.2006.887523.

5 Jon Feldman, Martin J. Wainwright, and David R. Karger. Using linear programming to decode binary linear codes. *IEEE Trans. Inf. Theory*, 51(3):954–972, 2005. doi:10.1109/TIT.2004.842696.

6 Robert G. Gallager. *Low-Density Parity-Check Codes*. The MIT Press, September 1963. doi:10.7551/mitpress/4347.001.0001.

7 M.G. Luby, M. Amin Shokrolloahi, M. Mizenmacher, and D.A. Spielman. Improved low-density parity-check codes using irregular graphs and belief propagation. In *Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)*, page 117, 1998.

8 Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. Ldpc codes achieve list decoding capacity. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 458–469, 2020. doi:10.1109/FOCS46700.2020.00050.

9 T.J. Richardson and R.L. Urbanke. The capacity of low-density parity-check codes under message-passing decoding. *IEEE Transactions on Information Theory*, 47(2):599–618, 2001.

10 M. Sipser and D. A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996. doi:10.1109/18.556667.

11 Madhu Sudan. A crash course on coding theory. availabel at http://people.seas.harvard.edu/~madhusudan/MIT/coding/ibm/, 2000.

12 Michael Viderman. Linear-time decoding of regular expander codes. *ACM Trans. Comput. Theory*, 5(3), August 2013. doi:10.1145/2493252.2493255.

13 Michael Viderman. Lp decoding of codes with expansion parameter above 2/3. *Inf. Process. Lett.*, 113(7):225–228, April 2013. doi:10.1016/j.ipl.2013.01.012.