List Decodable QLDPC Codes

**Thiago Bergamaschi (UC Berkeley), Fernando Granha Jeronimo (UIUC),
Tushant Mittal (Stanford), Shashank Srivastava (Rutgers, IAS), Madhur Tulsiani (TTIC)**

arXiv:2411.04306

List Decodable Quantum Error-Correcting Codes

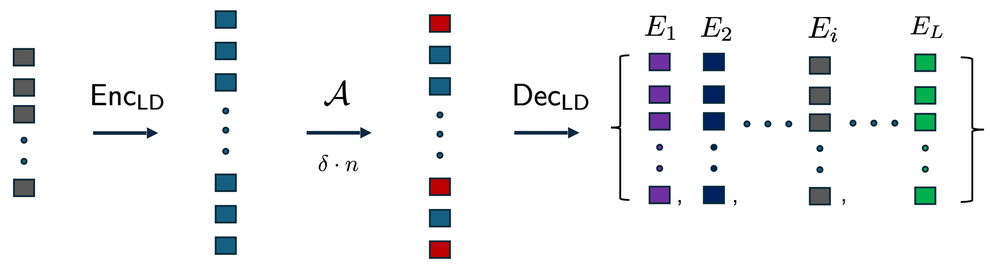

Figure 1: A list decodable code can tolerate more errors by outputting a small list of candidate codewords.

Definition. In a (δ, L) list decodable quantum error-correcting code, there are at most L logically distinct Pauli errors consistent with any given syndrome corresponding to an error of weight at most δn.

Why should we list decode quantum codes?

Improved Decoding. Most unique decoders do not work upto the theoretical limit of $\frac{d}{2}$ and list decoding is a useful way to increase the decoding radius.

Connections to Quantum Secret Sharing. Can construct near-optimal forms of QSS approaching the quantum Singleton bound, using a list-to-unique decoding reduction [4, 3].

Connections to (Interactive) Entanglement Distillation Protocols. One can minimize classical communication in an EDP by measuring stabilizers of list-decodable codes [7, 2].

Alon-Edmonds-Luby (AEL) Distance Amplification

The AEL construction [1] "amplifies" the distance of an outer code by using an inner code, and a bipartite expander (pseudorandom graph).

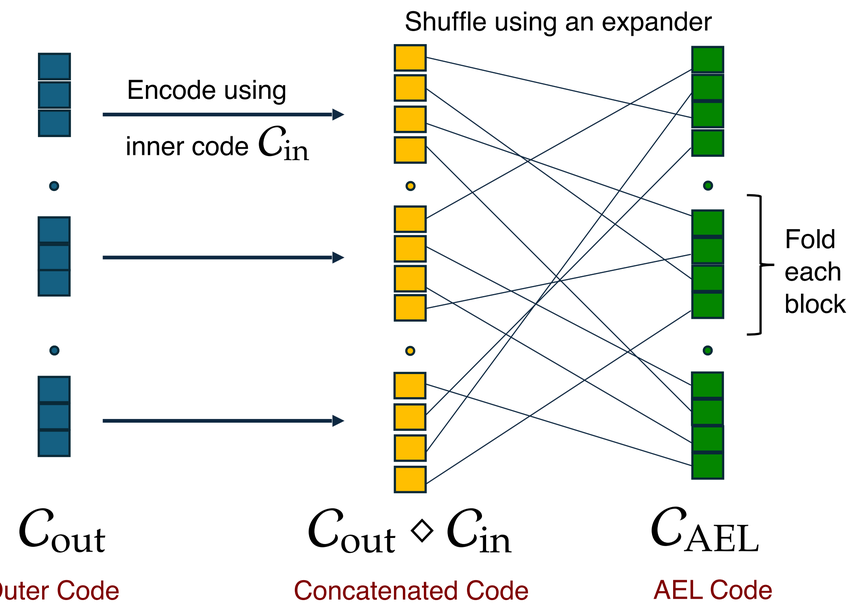

Figure 2: By permuting the concatenated code symbols using an expander graph, the errors spread and distribute "evenly" among outer code symbols.

Quantum AEL The AEL construction generalizes to CSS codes by amplifying each X and Z-type codespaces separately. The extra ingredient is a *duality preserving map* that ensures that the AEL code satisfies the CSS condition.

Distance amplification and quantum Singleton bound. The distance amplification property of AEL codes is the following:

$$\delta(\mathcal{C}_{\text{AEL}}) \;\geq\; \delta(\mathcal{C}_{\text{in}}) - \frac{\lambda}{\delta(\mathcal{C}_{\text{out}})} \;\to\; \frac{1}{2}(1-\rho) \quad \text{if} \quad \delta(\mathcal{C}_{\text{in}}) = \frac{1-\rho}{2}.$$

Here, ρ is the rate of the code and this optimal bound of $\frac{1-\rho}{2}$ is the quantum Singleton bound.

List Decodability of qAEL. The "amplified" (AEL) code inherits many desirable properties from the outer and inner codes, apart from distance. Our work shows the third:

Work	Outer Code	Inner Code	AEL Code
Direct	LDPC	Any	LDPC
[4]	Linear distance	qSingleton Bound	Near qSingleton Bound
This Work	Unique-Decodable upto a constant radius	-	List-Decodable upto Johnson Bound

Our Construction. We use a "good" qLDPC code [8] for the outer code, a quantum Reed-Solomon code for the inner code, and a bipartite spectral expander to perform the AEL procedure. This gives us all three desirable properties stated above.

List Decoding qLDPC codes up to the Johnson bound

Main Result. For any constant rate $0 < \rho < 1$ and small enough $\varepsilon > 0$, there is an infinite family of explicit quantum LDPC codes, with the following properties:

Approaches the quantum Singleton bound. The code has parameters $[n, \tilde{\rho}n, \delta n]$ where

$$\tilde{\rho} \;\geq\; \rho, \quad \delta \;\geq\; \frac{1}{2}(1-\rho) - \epsilon.$$

Constant-sized alphabet. The code is defined over qudits of dimension $2^{\mathcal{O}(\varepsilon^{-6}\log(1/\varepsilon))}$.

List-Decodable up to the Johnson bound. Each code can be decoded in time $n^{\mathcal{O}_\varepsilon(1)}$, into lists of size $\mathsf{poly}(1/\varepsilon)$, from errors of (fractional) weight:

$$\mathcal{J}\big(\delta\big) - \Theta(\varepsilon) \;\geq\; 1 - \sqrt{1-\delta} - \Theta(\varepsilon) \;>\; \delta/2.$$

List Decoding Algorithms via Sum-of-Squares (SoS)

The Proofs-to-Algorithms Paradigm. Proofs that only use low-degree polynomial reasoning can be algorithmically discovered via semidefinite programming [5, 6]. In the context of error-correction:

Low-Degree SoS Proofs of Distance $\Rightarrow$ List decoding algorithms.

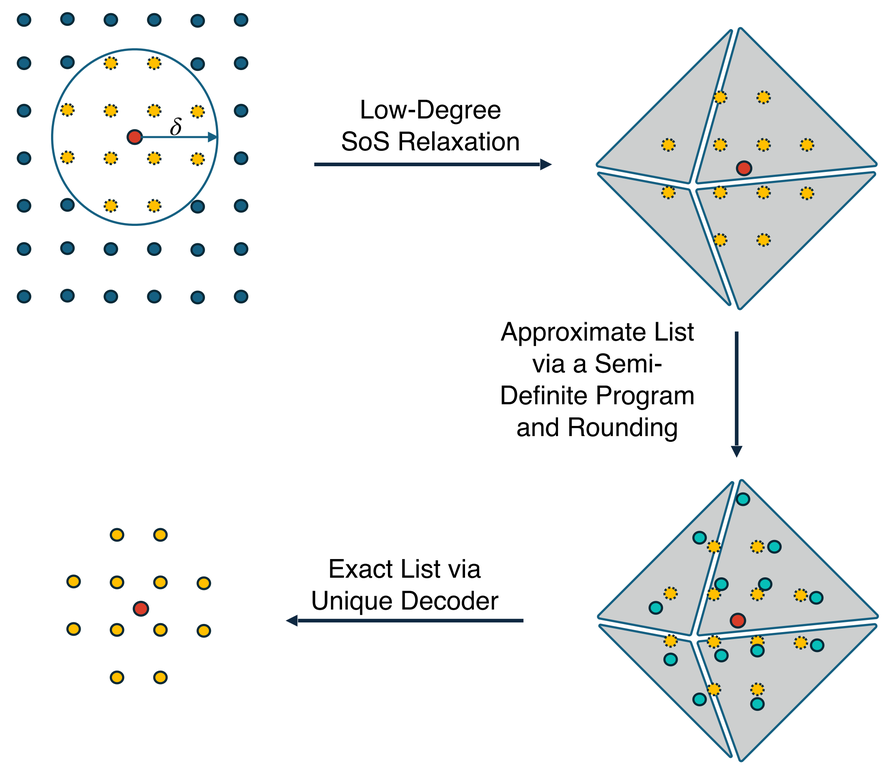

Figure 3: A high-level overview of decoding via the SoS framework

Key Contribution. A low-degree SoS proof for distance amplification of AEL codes.

Open Questions and Future Directions

List-Decoding Algorithms for other Quantum Codes.

Practical Entanglement Distillation from List-Decoding Algorithms.

Applications of List Decodable Quantum Codes to Quantum Pseudorandomness.

References

[1] N. Alon, J. Edmonds, and M. Luby, *Linear time erasure codes with nearly optimal recovery*, in Proceedings of IEEE 36th Annual Foundations of Computer Science, 1995, pp. 512–519.

[2] A. Ambainis and D. Gottesman, *The minimum distance problem for two-way entanglement purification*, IEEE Transactions on Information Theory, 52 (2006), pp. 748–753.

[3] T. Bergamaschi, *Pauli manipulation detection codes and applications to quantum communication over adversarial channels*, in Advances in Cryptology – EUROCRYPT, 2024.

[4] T. Bergamaschi, L. Golowich, and S. Gunn, *Approaching the quantum singleton bound with approximate error correction*, in Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC), 2024.

[5] N. Fleming, P. Kothari, and T. Pitassi, *Semialgebraic proofs and efficient algorithm design*, Foundations and Trends in Theoretical Computer Science, 14 (2019).

[6] F. G. Jeronimo, S. Srivastava, and M. Tulsiani, *List decoding of Tanner and expander amplified codes from distance certificates*, 2023.

[7] D. Leung and G. Smith, *Communicating over adversarial quantum channels using quantum list codes*, IEEE Transactions on Information Theory, 54 (2008), pp. 883–887.

[8] A. Leverrier and G. Zémor, *Quantum Tanner codes*, in Proceedings of the 63rd IEEE Symposium on Foundations of Computer Science (FOCS), 2022.

Acknowledgements

Part of this work was completed while the authors were participating in the "Analysis and TCS" program at the Simons Institute in Berkeley. We thank the program organizers and Simons administration and staff for their kind hospitality during this visit.