Title: Good quantum LDPC codes and how to decode them

Speakers: Shouzhen (Bailey) Gu

Series: Perimeter Institute Quantum Discussions

Date: December 13, 2023 - 11:00 AM

URL: https://pirsa.org/23120045

Abstract: The last few years have seen rapid progress in the development of quantum low-density parity-check (LDPC) codes. LDPC codes, defined by their constant weight check operators, can have much better parameters than their topological counterparts like the surface code. In particular, a series of pivotal works culminated in the discovery of asymptotically good LDPC codes--those with essentially optimal rate and distance scalings. These codes allow for the possibility fault-tolerant quantum computation with very low overhead. However, for a code to be used in practice, it is necessary to efficiently identify errors from measurement outcomes to get back into the codespace. In this talk, I will present a linear-time decoder for a family of asymptotically good codes called quantum Tanner codes. Furthermore, I will show that quantum Tanner codes support single-shot decoding, which means that one measurement round suffices to perform reliable quantum error correction, even in the presence of measurement errors. These results can be seen as a step toward making quantum LDPC codes more practical.

Zoom link https://pitp.zoom.us/j/94286584094?pwd=Q21IekhHZXI4Qlk4Y1B3MnNobmR6UT09

Good quantum LDPC codes and how to decode them

Shouzhen (Bailey) Gu
Caltech

Perimeter Institute Quantum Discussions Seminar
December 13, 2023

arXiv:2206.06557, **SG**, C.A. Pattison, E. Tang
arXiv:2306.12470, **SG**, E. Tang, L. Caha, S.H. Choe, Z. He, A. Kubica

Quantum error correction

- Quantum error correction is needed to reduce the error rates of physical devices
- Space overhead
  - Choice of code: code parameters
  - Number of ancilla qubits needed
- Time overhead
  - Implementing logical gates
  - Decoding algorithm
- How can we achieve fault-tolerant quantum computation with the lowest overhead?

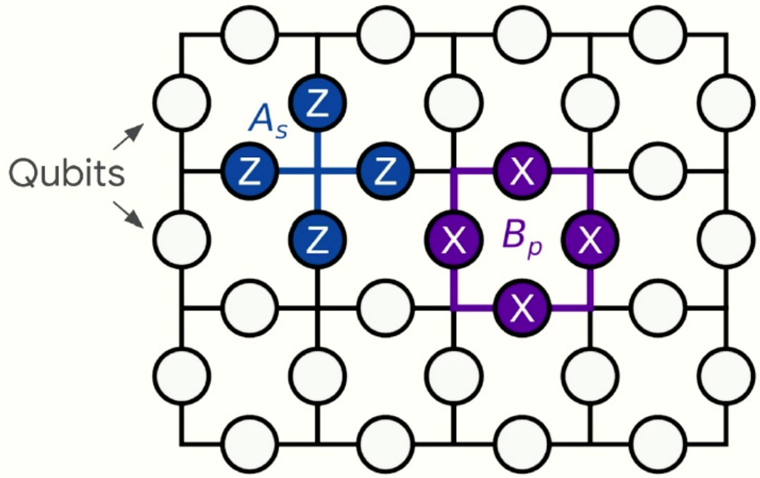
Outline

1. Space overhead of error correction: quantum LDPC codes
2. Time overhead of error correction: decoders for LDPC codes
   - Decoding good quantum LDPC codes (arXiv:2206.06557)
   - Single-shot decoding (arXiv:2306.12470)
3. Conclusions and open problems

Outline

1. Space overhead of error correction: quantum LDPC codes
2. Time overhead of error correction: decoders for LDPC codes
   - Decoding good quantum LDPC codes (arXiv:2206.06557)
   - Single-shot decoding (arXiv:2306.12470)
3. Conclusions and open problems

The surface code



- Codespace is the simultaneous +1 eigenspace of all vertex and plaquette stabilizers
- Currently the leading candidate for practical implementation

https://quantumai.google/cirq/experiments/toric_code/toric_code_ground_state

The surface code: pros and cons

Pros

- Geometrically local stabilizers
- Know how to implement, decode, perform logic, etc.

Cons

- Poor code parameters
  - Code length n: number of physical qubits
  - Dimension k: number of logical qubits
  - Distance d: weight of the smallest nontrivial logical operator
  - Surface code: $[[n, k = 1, d = \Theta(\sqrt{n})]] = [[L^2, 1, L]]$
- High overhead for fault-tolerance

LDPC codes

- Bravyi-Poulin-Terhal bound [BPT10]: $kd^2 = O(n)$ in 2D
- Relax condition on geometric locality
- Low-density parity-check: stabilizers are constant weight
  - Low weight checks are easier to measure
  - Important for fault-tolerance
- Best possible parameters for LDPC codes?

History of quantum LDPC codes

Code	k (Dim)	d (Dist)
Surface code [Kit03] • Geometrically local checks	1	$\Theta(\sqrt{n})$
Hypergraph product codes [TZ14, BH14] • Uses good classical codes	$\Theta(n)$	$\Theta(\sqrt{n})$
Fibre bundle codes [HHO21] • First to break the $\sqrt{n}$ distance barrier	$\tilde{\Theta}(n^{3/5})$	$\tilde{\Omega}(n^{3/5})$
Lifted product codes [PK22b]	$\tilde{\Theta}(n^{\alpha})$	$\tilde{\Omega}(n^{1-\alpha/2})$
Balanced product codes [BE21]	$\Theta(n^{4/5})$	$\Omega(n^{3/5})$
Expander lifted product codes [PK22a] • First good quantum LDPC code	$\Theta(n)$	$\Theta(n)$
Quantum Tanner codes [LZ22]	$\Theta(n)$	$\Theta(n)$
DHLV codes [DHLV22]	$\Theta(n)$	$\Theta(n)$

History of quantum LDPC codes

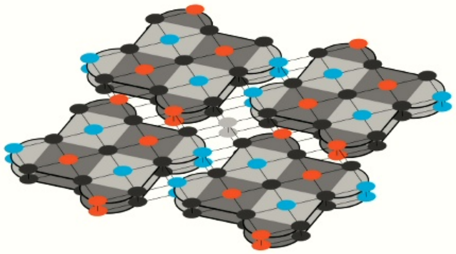
Code	k (Dim)	d (Dist)
Surface code [Kit03] • Geometrically local checks	1	$\Theta(\sqrt{n})$
Hypergraph product codes [TZ14, BH14] • Uses good classical codes	$\Theta(n)$	$\Theta(\sqrt{n})$
Fibre bundle codes [HHO21] • First to break the $\sqrt{n}$ distance barrier	$\tilde{\Theta}(n^{3/5})$	$\tilde{\Omega}(n^{3/5})$
Lifted product codes [PK22b]	$\tilde{\Theta}(n^{\alpha})$	$\tilde{\Omega}(n^{1-\alpha/2})$
Balanced product codes [BE21]	$\Theta(n^{4/5})$	$\Omega(n^{3/5})$
Expander lifted product codes [PK22a] • First good quantum LDPC code	$\Theta(n)$	$\Theta(n)$
Quantum Tanner codes [LZ22]	$\Theta(n)$	$\Theta(n)$
DHLV codes [DHLV22]	$\Theta(n)$	$\Theta(n)$

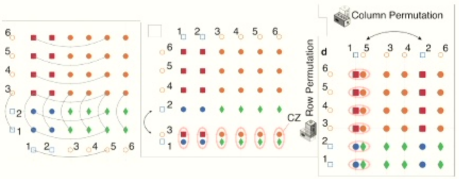
Constant space overhead

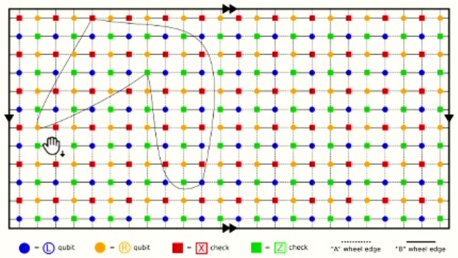
- Gottesman [Got14]: LDPC code with parameters $[[n, k = \Theta(n), d = \Omega(n^{\alpha})]] \implies$ constant space overhead
- Assumptions
  - Long-range interactions
  - Efficient decoder

Implementing LDPC codes

- Only geometrically local interactions
  - Concatenate with surface codes [PKP23]
- All-to-all connectivity
  - Proposal based on neutral atom arrays [XAP+23, VYL+23]
- Limited number of long-range connections
  - Proposal using 2 long-range interactions per qubit [BCG+23]







https://arxiv.org/abs/2303.04798

https://arxiv.org/abs/2308.08648

https://arxiv.org/abs/2308.07915

Outline

1. Space overhead of error correction: quantum LDPC codes

2. Time overhead of error correction: decoders for LDPC codes
   - Decoding good quantum LDPC codes (arXiv:2206.06557)
   - Single-shot decoding (arXiv:2306.12470)

3. Conclusions and open problems

How to correct errors: the decoding problem

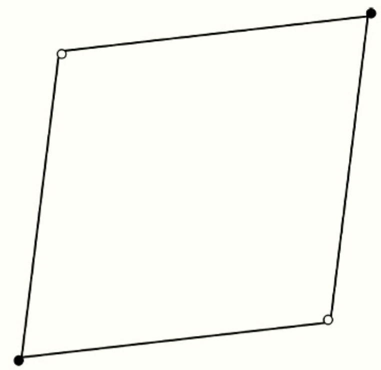
- Unknown error e applied to a code state
- Extract syndrome by measuring stabilizers
- Input: syndrome σ of an error e
- Output: a correction $\hat{f}$
- Succeed if $e + \hat{f}$ is a stabilizer

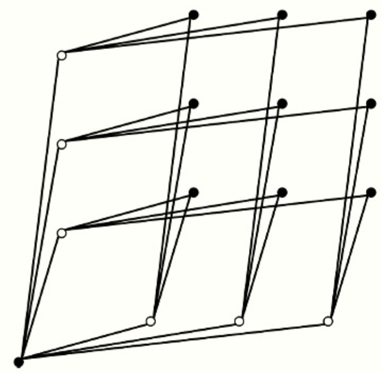
Finding efficient decoders

- Should decode faster than errors accumulate
  - Need to know Pauli frame for certain logical operations
- Intractable problem in general (NP/#P complete)
- Efficient decoders for many codes exist
- Two settings for decoding
  - Adversarial noise: decode any error of weight up to a constant fraction of the distance
  - Stochastic noise: decoder random noise with high probability

Lightning overview of quantum Tanner codes [LZ22]

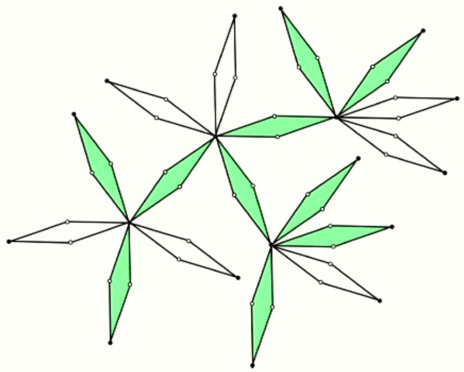
- Left-right Cayley complex (two-dimensional expanding object)
  - Vertices $V = V_X \sqcup V_Z$
  - Edges E
  - Squares Q
- Qubits placed on squares Q
- S_X generated by checks on faces incident to vertices in V_X
- S_Z generated by checks on faces incident to vertices in V_Z





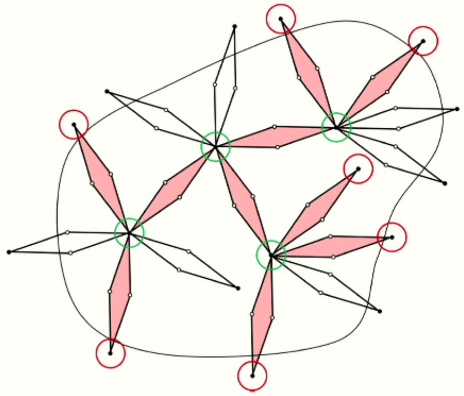
Distance of quantum Tanner codes

- Consider a nontrivial logical operator L
- Local check at vertex $v \implies$ high weight around v
- Also must be high weight around neighbouring vertices v'
- Expansion $\implies L = \Omega(n)$
- Gives a code with parameters $[[n, k = \Theta(n), d = \Theta(n)]]$



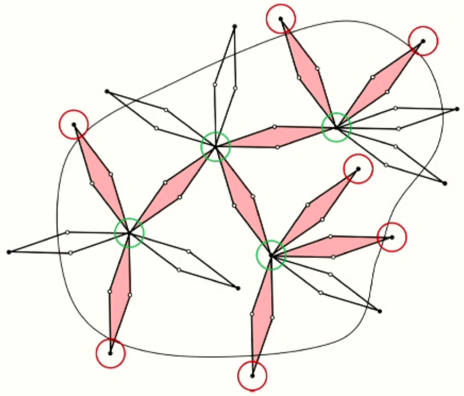
Decoding quantum Tanner codes

- Consider X error e of low weight
- e may satisfy all checks in its “bulk”
- Many violations near its “boundary”



Decoding quantum Tanner codes

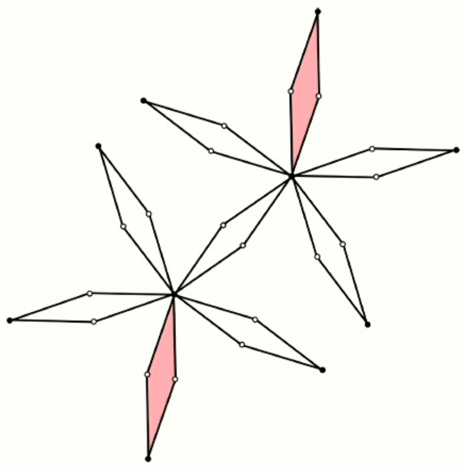
- Consider X error e of low weight
- e may satisfy all checks in its "bulk"
- Many violations near its "boundary"
- Flipping qubits at the boundary of e will result in more satisfied checks



Potential-based decoder [GPT23]

1. For each $v \in V_Z$, determine a candidate correction ε_v on the qubits in its neighbourhood
   - Choose ε_v to have minimal weight while satisfying all local checks at v
2. Compute a potential function $U = \sum_{v \in V_Z} |\varepsilon_v|$
3. At every step, flip qubits in a local region to decrease U

All stabilizer checks are satisfied when $U = 0$.



Main theorem

Theorem (Potential-based decoder [GPT23])

There is a family of quantum Tanner codes with parameters $[[n, \Theta(n), \Theta(n)]]$ *such that the potential-based decoder can correct all errors of weight* $|e| \leq p^* n$*, where* p^* *is a constant. The time complexity is* $O(n)$.

Main theorem

Theorem (Potential-based decoder [GPT23])

There is a family of quantum Tanner codes with parameters $[[n, \Theta(n), \Theta(n)]]$ *such that the potential-based decoder can correct all errors of weight* $|e| \leq p^* n$*, where* p^* *is a constant. The time complexity is* $O(n)$.

- First decoder to correct adversarial errors of weight $O(n)$
- Previous best [EKZ22]: $O(\sqrt{n \log n})$

Proof outline

Correctness

- Prove that for small errors, we can find a local correction to decrease the potential function $U = \sum_{v \in V_Z} |\varepsilon_v|$
- Prove that the error remains small throughout decoding, and the final codeword is equivalent to the original

Runtime

- Initialization: $O(n)$ time to compute potential function U
- Update: $O(n)$ iterations with constant number of updates in each iteration

Main theorem

Theorem (Potential-based decoder [GPT23])

There is a family of quantum Tanner codes with parameters $[[n, \Theta(n), \Theta(n)]]$ such that the potential-based decoder can correct all errors of weight $|e| \leq p^* n$, where p^* is a constant. The time complexity is $O(n)$.

- First decoder to correct adversarial errors of weight $O(n)$
- Previous best [EKZ22]: $O(\sqrt{n \log n})$

Proof outline

Correctness

- Prove that for small errors, we can find a local correction to decrease the potential function $U = \sum_{v \in V_Z} |\varepsilon_v|$
- Prove that the error remains small throughout decoding, and the final codeword is equivalent to the original

Stochastic errors: existence of threshold

Corollary

For i.i.d. errors with probability $p < p^*$, *the decoder succeeds with probability* $1 - O(e^{-an})$ *with* $a > 0$.

Proof.

- By our main theorem, the decoder succeeds if $|e| \leq p^* n$
- Hoeffding's inequality: $\Pr(|e| > p^* n) < e^{-2n(p^* - p)^2}$

□

Soundness

Corollary

If $|e| < p^* n$, then $|\sigma| \geq \rho|e|_R$ for a constant ρ.

Soundness

Corollary

If $|e| < p^* n$, then $|\sigma| \geq \rho |e|_R$ for a constant ρ.

Proof.

- e can be corrected to a codeword in at most U steps
- At most c_1 are flipped in each step $\implies |e|_R \leq c_1 U$
- $|\sigma| \geq c_2 U \geq \frac{c_2}{c_1} |e|_R$

□

Remarks on soundness property

- Weaker version of local testability
- An important property (also called clustering of approximate codewords) used in [ABN22] to show quantum Tanner codes give NLTS Hamiltonians

Outline

1. Space overhead of error correction: quantum LDPC codes

2. Time overhead of error correction: decoders for LDPC codes
    - Decoding good quantum LDPC codes (arXiv:2206.06557)
    - Single-shot decoding (arXiv:2306.12470)

3. Conclusions and open problems

Dealing with measurement noise

- What if syndrome σ is corrupted?

Dealing with measurement noise

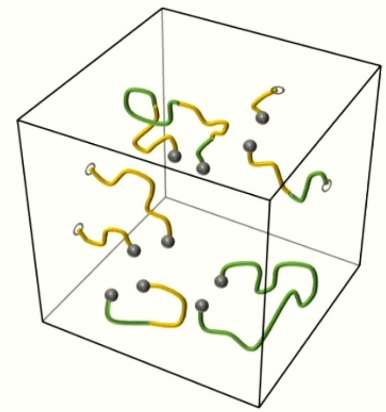
- What if syndrome σ is corrupted?
- Standard procedures
  - Repeat measurement rounds [Sho96]: large time overhead
  - Prepare ancilla offline [Ste97]: large space overhead
- Problems
  - Could weaken the advantage of a quantum algorithm
  - Must decode faster than errors accumulate

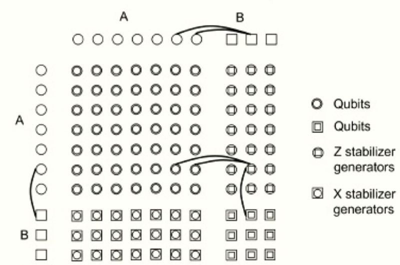
Single-shot error correction

- Alternative approach: single-shot quantum error correction [Bom15]
    - Make progress in decoding with noisy syndrome data
- Can also consider adversarial or stochastic noise

Existing single-shot decoders

- Topological codes
  - 4D toric code [BDMT17], 3D subsystem toric code [KV22], 3D gauge colour code [Bom15]
  - Use redundancy of checks
- Expansion based LDPC code
  - Quantum expander codes [FGL18]
  - Expansion provides single-shot property
- Arbitrary stabilizer codes can be made single-shot [Cam19]
  - May not keep LDPC property





https://www.nature.com/articles/s41467-022-33923-4/figures/7

https://arxiv.org/abs/2208.01002

Definition of single-shot

Setup

- Input: noisy syndrome $\tilde{\sigma}$
  - Data error e
  - Syndrome error D
- Output: a correction $\hat{f}$

Definition

A decoder is (α, β)-single-shot if for sufficiently low-weight errors,

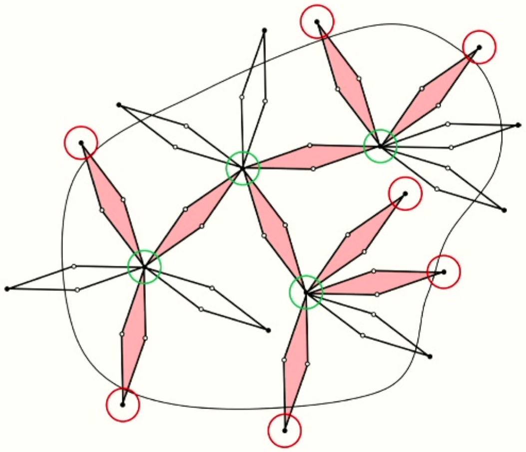
$$|e + \hat{f}|_R \leq \alpha |e|_R + \beta |D| \,.$$

Mismatch decomposition decoder [LZ23]

- Also a local greedy decoder, but uses the mismatch $Z = \left|\sum_{v \in V_Z} \varepsilon_v\right|$ instead of the potential $U = \sum_{v \in V_Z} |\varepsilon_v|$
- At every step, flip qubits in some local region to decrease Z
  - Stop when no more flips possible
- The algorithm can be run sequentially or in parallel
  - Sequential decoder: $O(n)$ runtime
  - Parallel decoder: $O(\log n)$ runtime

Why is this decoder single-shot?

- Recall: intuition that valid corrections are near the "boundary" of the error region
- Expansion $\implies$ large boundary $\implies$ many candidate corrections
- Syndrome noise can affect a limited number of these corrections



Main results for single-shot decoding

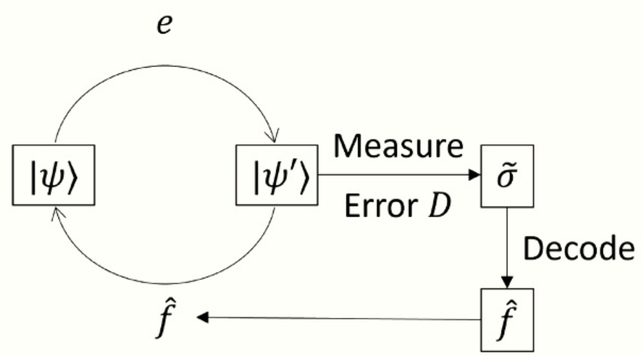
Theorem (Single-shot property [GTC+23])

There exists a constants β such that we have the following:

1. *The sequential decoder is $(\alpha = 0, \beta)$-single-shot.*
2. *The parallel decoder with k-iterations is $(\alpha = 2^{-\Omega(k)}, \beta)$-single-shot.*

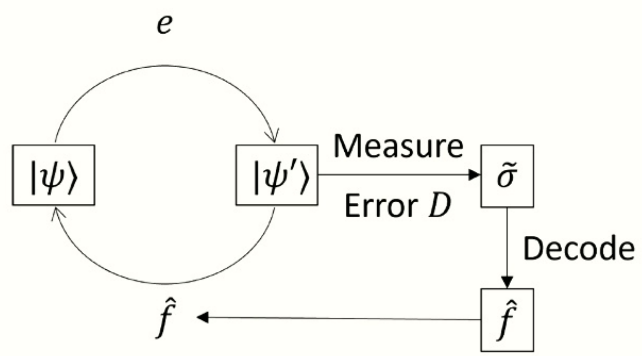
(Recall: (α, β)-single-shot means $|e + \hat{f}|_R \leq \alpha |e|_R + \beta |D|$.)

Multiple rounds of errors (stochastic setting)



- For i.i.d. errors (e_i, D_i) with probability $p < p^*$, quantum information is maintained for $\Omega(e^{an})$ rounds with probability $1 - O(e^{-bn})$ with $a, b > 0$

Multiple rounds of errors (stochastic setting)



- For i.i.d. errors (e_i, D_i) with probability $p < p^*$, quantum information is maintained for $\Omega(e^{an})$ rounds with probability $1 - O(e^{-bn})$ with $a, b > 0$
- Generalizes to space/time correlated errors
  - E.g. circuit noise

Constant-time decoding of quantum Tanner codes

- The k-iteration parallel decoder is $(\alpha = 2^{-\Omega(k)}, \beta)$-single-shot
  - Choose k a sufficiently large constant
- During the computation: residual errors are small (nonzero)
- Last round: measure all qubits in the Z basis
  - Treat measurement errors as X qubit errors
  - Use ideal $O(\log n)$-iteration parallel decoder or sequential decoder to recover information exactly ($|e + \hat{f}|_R \leq \alpha |e|_R + \beta |D|$ with $\alpha = 0$ and $|D| = 0$)
- Constant time overhead using quantum Tanner codes

Constant-time decoding of quantum Tanner codes

- The k-iteration parallel decoder is $(\alpha = 2^{-\Omega(k)}, \beta)$-single-shot
  - Choose k a sufficiently large constant
- During the computation: residual errors are small (nonzero)
- Last round: measure all qubits in the Z basis
  - Treat measurement errors as X qubit errors
  - Use ideal $O(\log n)$-iteration parallel decoder or sequential decoder to recover information exactly ($|e + \hat{f}|_R \leq \alpha|e|_R + \beta|D|$ with $\alpha = 0$ and $|D| = 0$)

Constant-time decoding of quantum Tanner codes

- The k-iteration parallel decoder is $(\alpha = 2^{-\Omega(k)}, \beta)$-single-shot
  - Choose k a sufficiently large constant
- During the computation: residual errors are small (nonzero)
- Last round: measure all qubits in the Z basis
  - Treat measurement errors as X qubit errors
  - Use ideal $O(\log n)$-iteration parallel decoder or sequential decoder to recover information exactly ($|e + \hat{f}|_R \leq \alpha |e|_R + \beta |D|$ with $\alpha = 0$ and $|D| = 0$)
- Constant time overhead using quantum Tanner codes

Conclusions

Summary

- Provably correct and efficient decoders for quantum Tanner codes
- Single-shot property of the sequential and parallel decoders
- Quantum error correction with constant space and time overhead

Open questions

- Logical gates for LDPC codes
- How to choose the right LDPC code to use?
  - Decrease constants involved in the good code constructions
- General framework for analyzing local greedy decoders