New existence bounds for decoding transition with Q-LDPC codes: percolation on hypergraphs

Leonid Pryadko

UC, Riverside

QEC14: Dec 16, 2014

$$p_e + (1-p_e)[4p_X(1-p_X)]^{1/2} < (w_Z - 1)^{-1}$$

$$2[4q(1-q)]^{1/2} + w_Z\left\{p_e + (1-p_e)[4p_X(1-p_X)]^{1/2}\right\} < 1$$

Ilya Dumer (UCR)
Alexey Kovalev (UNL)
Kathleen Hamilton (UCR)

arXiv:1208.2317
arXiv:1311.7688
arXiv:1405.0050
arXiv:1405.0348 & **new work**

New existence bounds for decoding transition with Q-LDPC codes: percolation on hypergraphs

Leonid Pryadko

UC, Riverside

QEC14: Dec 16, 2014

- Introduction: SAW-based bound for the surface codes
- Old bound for Q-LDPC codes with log distance
- New bounds: count irreducible undetectable operators
- Conclusions and open problems

Ilya Dumer (UCR)
Alexey Kovalev (UNL)
Kathleen Hamilton (UCR)
arXiv:1208.2317
arXiv:1311.7688
arXiv:1405.0050

arXiv:1405.0348 & **new work**

Decoding threshold

Decoding threshold p_c: Consider an infinite family of error correcting codes. With probability p for independent errors per (qu)bit, at $p < p_c$, a large enough code can correct all errors with success probability $P \to 1$, but not at $p > p_c$

Example: code family with **finite relative distance** $\delta = d/n$. A code can detect any error involving $w < d$ (qu)bits, and distinguish between any two errors involving $w < d/2$ qubits each. For such a family, $p_c \geq \delta/2$.

In practice, this does not quite work since such codes have stablizer generators of weight $\sim n$: **measuring syndrome is hard**

All known code families with finite-weight stabilizer generators have distance scaling logarithmically or as a sublinear power of n.

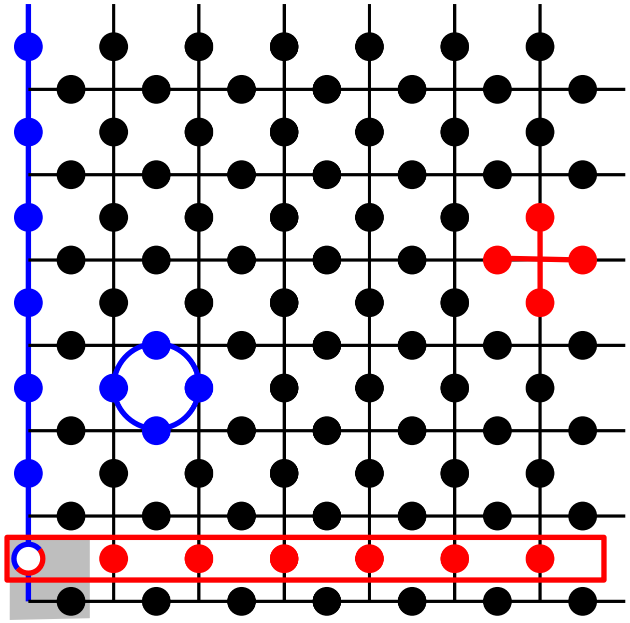
Zero-rate codes: toric (Kitaev)
color (Bombin et al.)
...

Finite-rate: Tillich & Zémor 2009
Andriyanova et al. 2012
...

Surface codes

Family of codes invented by Alexey Kitaev (orig: *toric* codes)

Stabilizer generators: plaquette $A_{\Box} = ZZZZ$ and vertex $B_{+} = XXXX$ operators (this is a CSS code).



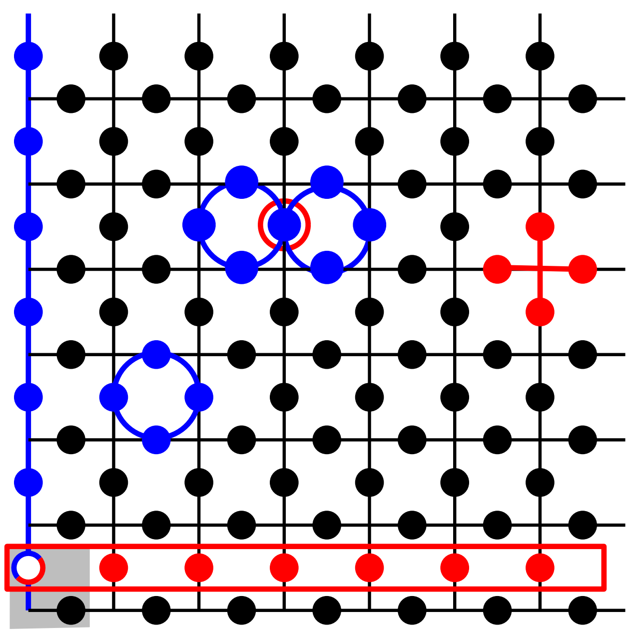
$_3$toric code $[[98, 2, 7]]$

Surface codes

Family of codes invented by Alexey Kitaev (orig: *toric* codes)

Stabilizer generators: plaquette $A_\square = ZZZZ$ and vertex $B_+ = XXXX$ operators (this is a CSS code).

Detectable errors: have open X chains along dual lattice or open Z chains on the original lattice



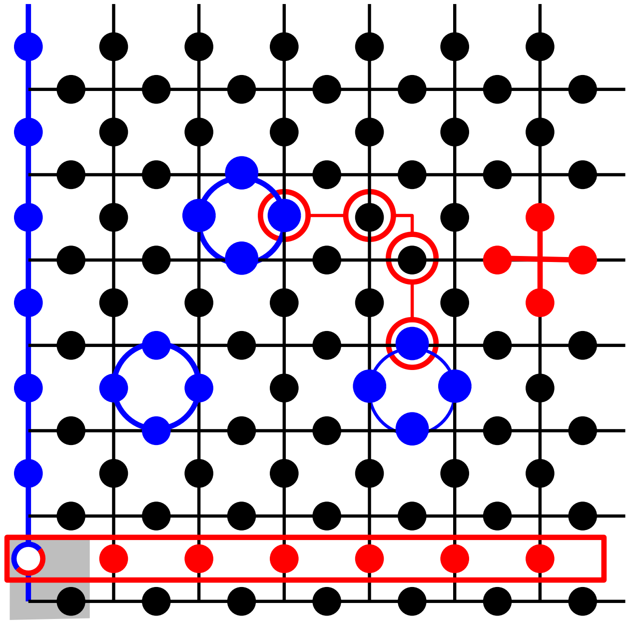
$_3$toric code $[[98, 2, 7]]$

Surface codes

Family of codes invented by Alexey Kitaev (orig: *toric* codes)

Stabilizer generators: plaquette $A_\square = ZZZZ$ and vertex $B_+ = XXXX$ operators (this is a CSS code).

Detectable errors: have open X chains along dual lattice or open Z chains on the original lattice



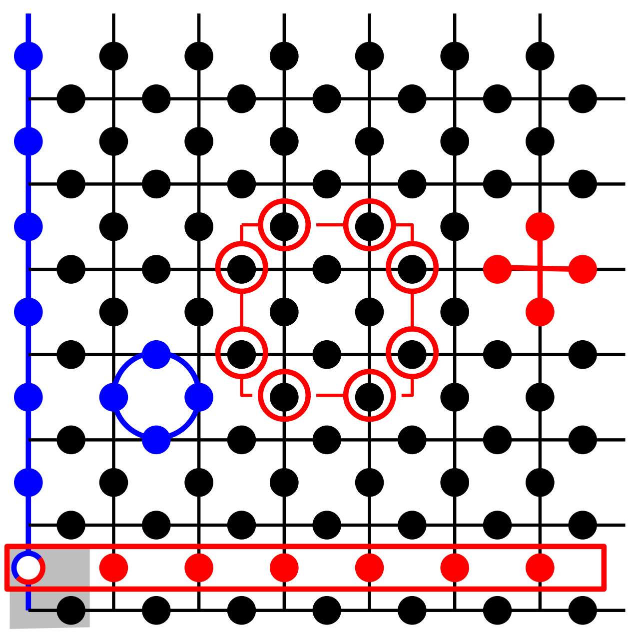
$_3$toric code $[[98, 2, 7]]$

Surface codes

Family of codes invented by Alexey Kitaev (orig: *toric* codes)

Stabilizer generators: plaquette $A_\square = ZZZZ$ and vertex $B_+ = XXXX$ operators (this is a CSS code).

Detectable errors: have open X chains along dual lattice or open Z chains on the original lattice



3toric code [[98, 2, 7]]

Undetectable error: only closed chains

Trivial undetectable error: topologically trivial loops

Bad undetectable error: topologically non-trivial loop $\Rightarrow$ Code distance $d = L \propto \sqrt{n}$.

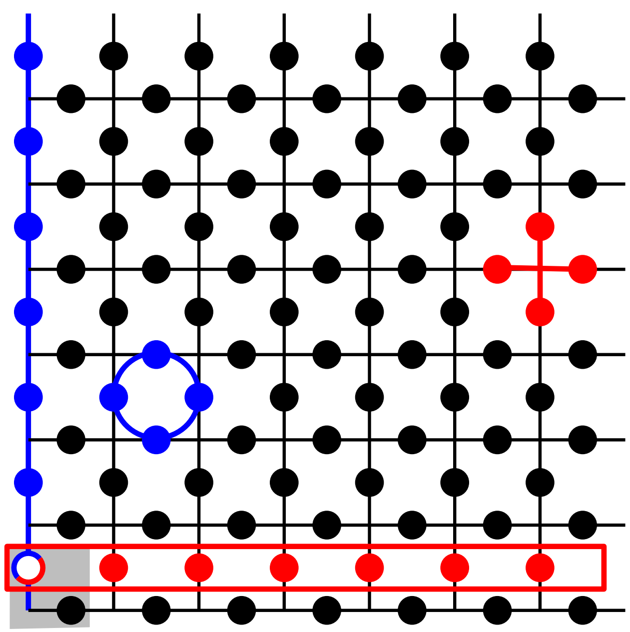
$[[n = 2L^2, k = 2, d = L]]$

Surface codes: finite decoding threshold

Distance scales as $d \propto n^{1/2}$, meaning zero relative distance $\delta \propto n^{-1/2}$, $n \to \infty$. Is there a finite decoding threshold?

Yes! [Dennis, Kitaev, Landahl & Preskill, 2002]

- Counting topologically non-trivial chains
- Mapping to the Ising model with bond disorder



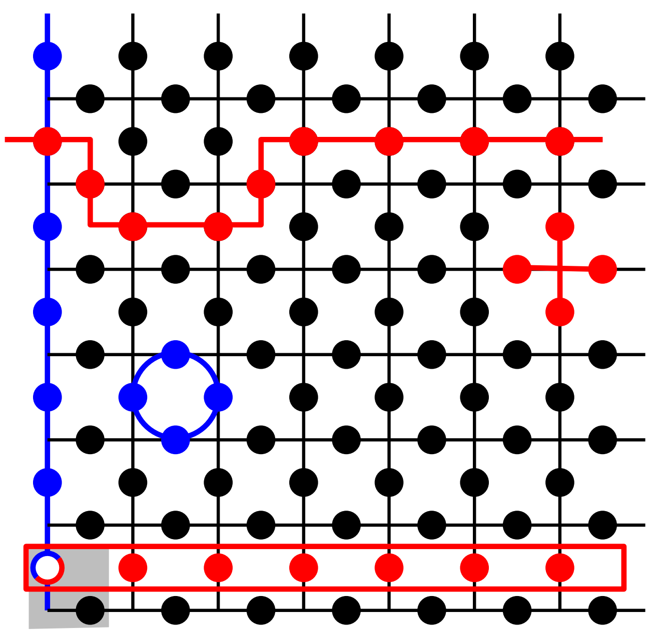
4 toric code $[[98, 2, 7]]$

Surface codes: finite decoding threshold

Distance scales as $d \propto n^{1/2}$, meaning zero relative distance $\delta \propto n^{-1/2}$, $n \to \infty$. Is there a finite decoding threshold?

Yes! [Dennis, Kitaev, Landahl & Preskill, 2002]

- Counting topologically non-trivial chains
- Mapping to the Ising model with bond disorder



toric code [[98, 2, 7]]

Erasures: unrecoverable chain len. $\ell \geq d$:

$$Q_\ell \leq n\, p^\ell \#(\mathrm{SAW}_\ell) \leq n\,(3p)^\ell$$

Uncorrectable error: such a chain more than half-filled with errors. Probability:

$$P_\ell \leq n\,\#(\mathrm{SAW}_\ell) \sum_{m \geq \lfloor \ell/2 \rfloor} \binom{\ell}{m} p^m (1-p)^{\ell-m}$$

$$P_\ell \leq n\, 3^\ell \times 2^\ell [p(1-p)]^{\ell/2}$$

Neither happens at sufficiently small p!

General (h, w)-limited Q-LDPC codes

Example: hypergraph product code constructed from $[7, 3, 4]$ cyclic code. Column weights $\leq h = 3$, row weights $\leq w = 6$.

$$G_X = \left(\begin{array}{cccccccccc|ccccc}
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & 0 & \ldots \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ldots \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & \ldots \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & \ldots & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots
\end{array}\right)$$

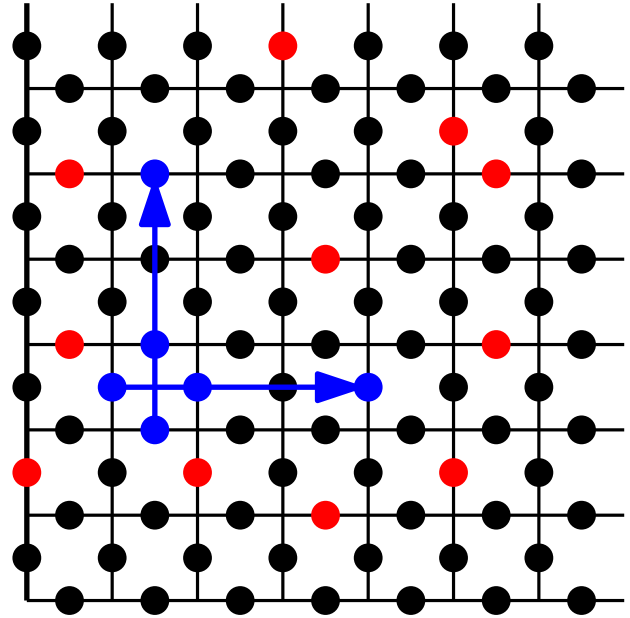
Observation: for small p, errors can be separated into clusters which affect different subsets of generators.

Here, each qubit has up to $z \equiv h(w-1)$ neighbors.

Formation of large clusters can be viewed as percolation on a graph with vertex degrees bounded by z.

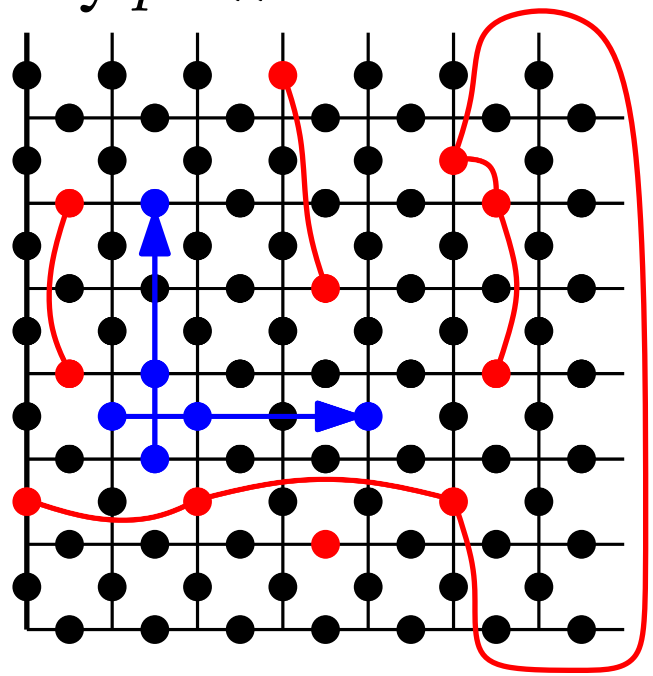
Threshold theorem and sparse-graph codes (cont'd)

- Start with a small per-qubit error probability $p \ll 1$.
- Connect errors affecting common generators. For small p and a sparse code these form small disconnected clusters



Threshold theorem and sparse-graph codes (cont'd)

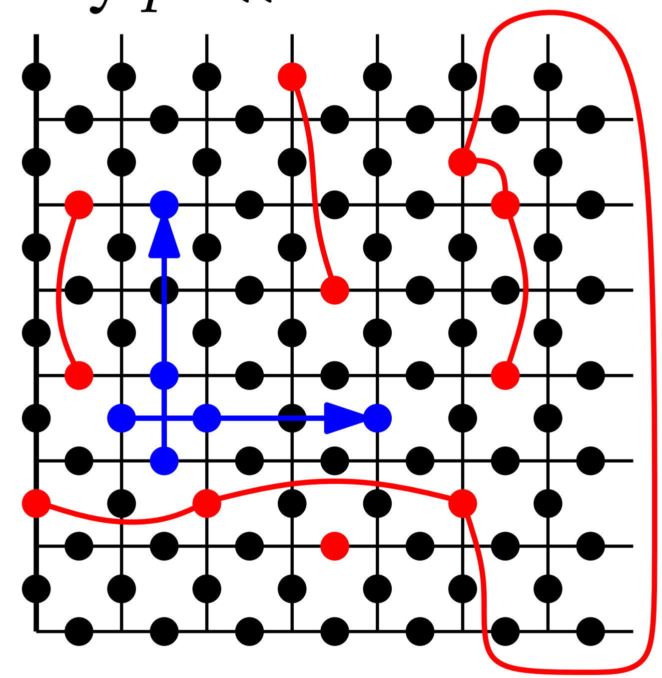
- Start with a small per-qubit error probability $p \ll 1$.
- Connect errors affecting common generators. For small p and a sparse code these form small disconnected clusters
- Key observation: disconnected clusters can be detected independently; they do not affect each other's syndromes.



This implies that errors formed by clusters of weight $w < d$ are all detectable

Threshold theorem and sparse-graph codes (cont'd)

- Start with a small per-qubit error probability $p \ll 1$.
- Connect errors affecting common generators. For small p and a sparse code these form small disconnected clusters
- Key observation: disconnected clusters can be detected independently; they do not affect each other's syndromes.



This implies that errors formed by clusters of weight $w < d$ are all detectable

- Below percolation limit p_c, probability to have a cluster of large weight w is exponentially small with w.
- Maximum cluster size grows logarithmically with n (for small enough p this is also true for confusing half-filled clusters)

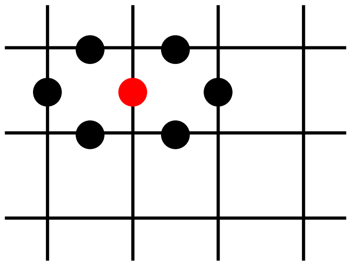
Conclusion: as long as $d \propto n^{\alpha}$, $\alpha > 0$ (or even logarithmic), a sparse-graph code can correct errors at finite p. [Kovalev & LPP, '13]

Percolation-based threshold for quantum LDPC codes

Actual value of the threshold for erasures: $p_e \geq (z-1)^{-1}$ for (h,w)-limited code. For depolarizing channel: $p_d \geq [2e(z-1)]^{-2}$ (assuming power-law distance).

Here $z \equiv h(w-1)$.

Trouble: This threshold is much weaker than what we have for the toric codes ($h=2$, $w=4$), even though both thresholds are related to percolation.



Reason: This approximates code as a qubit-connectivity graph. Any structure associated with the action of generators is ignored

Irreducible cluster counting algorithm

Definition 1 *For a given stabilizer code, an undetectable operator is called irreducible if it cannot be decomposed as a product of two disjoint undetectable Pauli operators.*

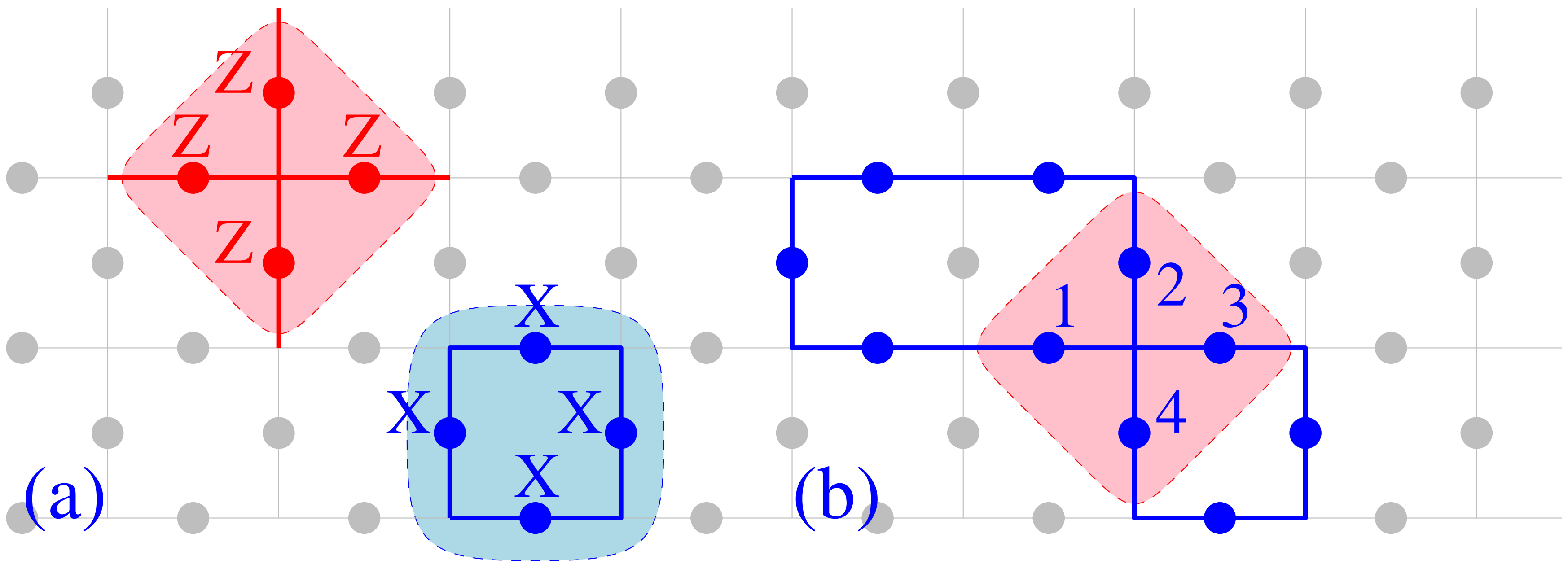
Algorithm for CSS code (X errors)

- Order the stabilizer generators; pick a starting bit (n choices)
- At each recursion step, deal with topmost ”unhappy” stabilizer generator and pick a bit among unselected points in its support (up to $w-1$ choices)
- Recursion stops when syndrome is zero (an undetectable operator is found), or when there are no more positions for a given generator (have to go back).
- After m recursion steps, return all irreducible undetectable operators of weight up to m. Complexity $\overline{N}_m = n\,(w-1)^{m-1}$.

This gives upper bound for the number N_m of irreducible logical operators at $m \geq d$.

Toric code example

Reducible cluster will be returned or not, depending on the order in which the numbered qubits are encountered



Minimum-energy decoding

Let $P(E)$ be some error probability, energy $\varepsilon = -\ln P(E)$.

- For an (unknown) error E, let E' be the minimum-energy error with the same syndrome $\Rightarrow$ $E'E^\dagger$ is undetectable.
- Decompose $E'E^\dagger = \prod_j J_j$ into irreducible operators J_j.
- Error found correctly if $\varepsilon(J_j E) > \varepsilon(E)$ for all J_j that are non-trivial logical operators (J_j not in stabilizer)

Decoding is asymptotically correct at $n \to \infty$ if the probability for a "bad" error for any irreducible $J \in \mathcal{C}(\mathcal{S}) \setminus \mathcal{S}$ vanishes.

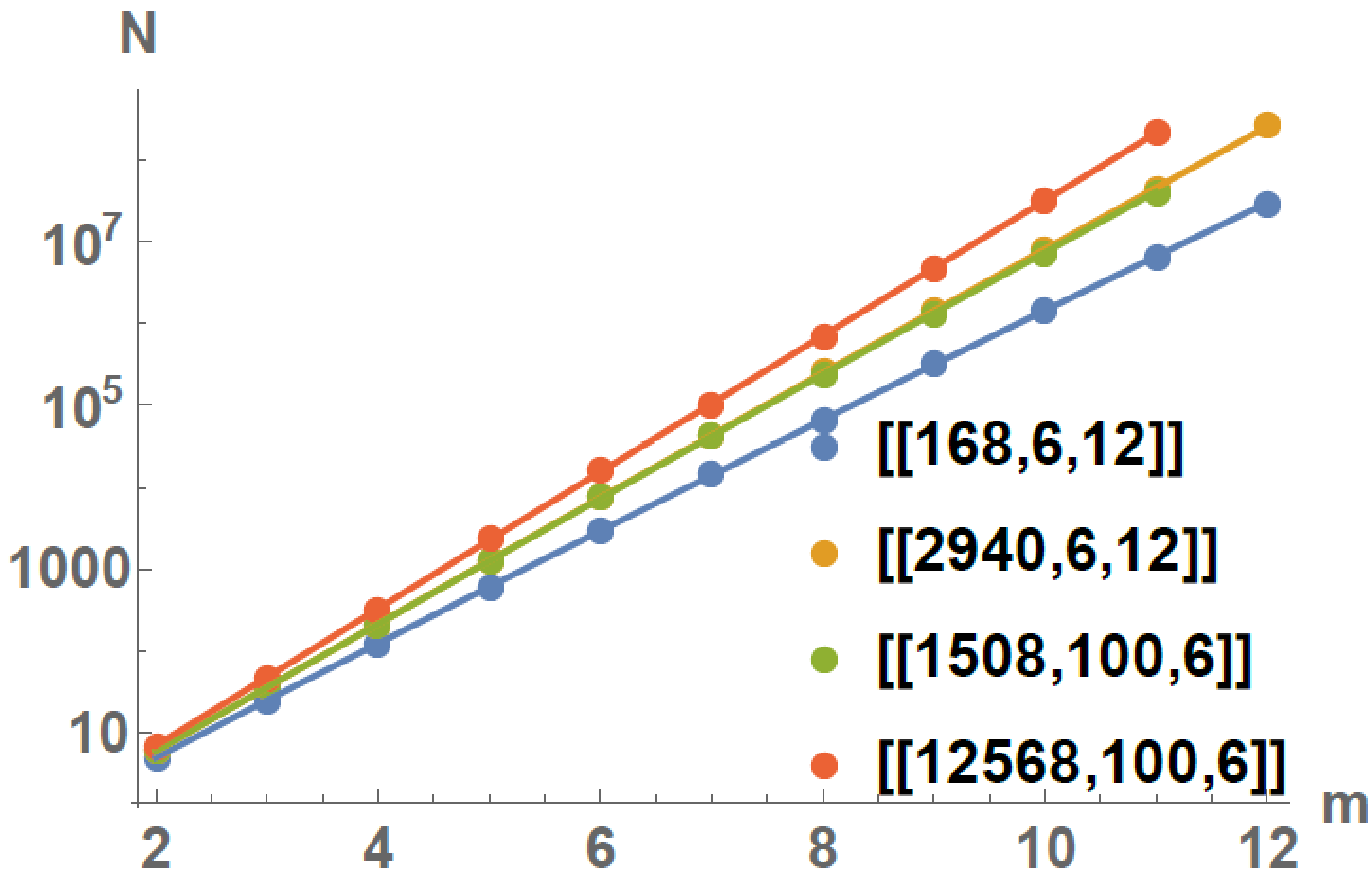
Let $\varepsilon(E)$ correspond to uniform uncorrelated errors. Then for a given J, probability P_m of bad error only depends on $m \equiv \mathrm{wgt}\, J$.

Example: Erasures with probability $p_e \Rightarrow P_m = p_e^m$.

Total probability to fail: $P_{\text{fail}} \le \sum_{m \ge d} P_m \overline{N}_m \le \dfrac{n[(w-1)p_e]^d}{1-(w-1)p_e}$

Improved cluster counting

For toric code, $w = 4$, and this bound is the same as simple-minded walk counting ($N_m \sim n\, 3^{m-1}$)



Power-law scaling of N_m for different codes — exponents can be used for improved bounds, just like SAW exponent in the case of the toric code [$\zeta_6 \approx 4.76$, $\zeta_7 \approx 5.74$, $\zeta_8 \approx 5.79$ and $\zeta_9 \approx 6.78$]

Combination of erasures and independent X/Z errors

Combined erasures (probability p_e) and X errors (probability p).

Probability of E: a erasures and b X errors in a cluster of size m:
$P_E = \binom{m}{a} p_e^a (1-p_e)^{m-a} \binom{m-a}{b} p^b (1-p)^{m-a-b}$.

Probability of JE (invert bits outside of the erasure):
$P_{JE} = \binom{m}{a} p_e^a (1-p_e)^{m-a} \binom{m-a}{b} (1-p)^b p^{m-a-b}$.

Bad errors: $P_E \le P_{JE}$, which gives $m - a - 2b > 0$.

Upper bound for bad error probability in a cluster of size m:

$$P_m = \left\{p_e + (1-p_e)[4p(1-p)]^{1/2}\right\}^m.$$

With code distance scaling as a power law $d \ge An^\alpha$, $\alpha > 0$, minimum-energy decoding asymptotically successful if

$$p_e + (1-p_e)[4p(1-p)]^{1/2} \le (w-1)^{-1}.$$

Fault-tolerant case

With syndrome errors, use aux 3D code with CSS-like generators (analog of 3D line matching): $P = \left(I_m \otimes H_{r\times n}, R_{m\times(m-1)} \otimes I_r\right)$

Degeneracy generator: $Q = \begin{pmatrix} [R^T]_{(m-1)\times m} \otimes I_n & I_{m-1} \otimes [H^T]_{n\times r} \\ I_m \otimes G_{r'\times n}, & 0 \end{pmatrix}$

Repetition code check matrix: $[R^T]_{(m-1)\times m} \equiv \begin{pmatrix} 1 & 1 & & & \\ 0 & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \end{pmatrix}$

Bound the number of clusters of size m, with m_q qubit errors: $\overline{N}_{m,m_q} \leq \binom{m}{m_q} w^{m_q} 2^{m-m_q}$

For combination of uncorrelated erasures (p_e), depolarizing (p), and syndrome errors, with distance $d \geq D \ln n$, we get

$$4[q(1-q)]^{1/2} + wY \leq e^{-1/D},$$
$$Y \equiv p_e + (1-p_e)\left\{\frac{2p}{3} + 2\left[\frac{p}{3}(1-p)\right]^{1/2}\right\}$$

Summary

- New analytic lower bound for the thresholds with minimum-energy decoder
  - Same accuracy as counting SAWs for the toric code
  - Simple expressions for uncorrelated errors
  - Phenomenological syndrome errors included on equal footing
  - Way better than the old percolation-based bound

- Erasure threshold, e.g., $p_e \geq (w-1)^{-1}$ for CSS codes, also gives bounds:
  - for code rate, using $1 - R \geq 2p_e \Rightarrow R < 1 - 2/(w-1)$
  - for codes with transverse logical ops in m th level of Clifford chierarcy, $p_e \leq 1/w$ [Yoshida & Pastawski (2014)]

- This corresponds to a bound on percolation of (binary) cycles on hypergraphs

- Yet percolation on a graph (like the old bound) can be also used:
  - With large variations of w, e.g., $p_e \geq 1/\lambda_{\max}(A)$ [Hamilton & LPP, 2014]
  - With correlated errors [in progress]

  Not clear if something similar can be done in the present case.
  Need to come up with MF theory for percolation on hypergraphs

A good postdoc is needed to work on this, LDPC codes & related stat-mech!