Viderman's Algorithm for Quantum LDPC Codes

Inbal Livni Navon

Stanford University

Anirudh Krishna

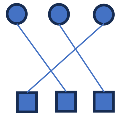
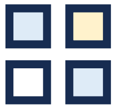
Stanford University
(>>IBM)

Mary Wootters

Stanford University

Simons workshop 2024

In This Talk

- Motivation and background
- Decoding classical LDPC codes 
- Hypergraph product code 
- Viderman's algorithm for hypergraph product codes
- Proof high-level
- Summary and future directions

Motivation

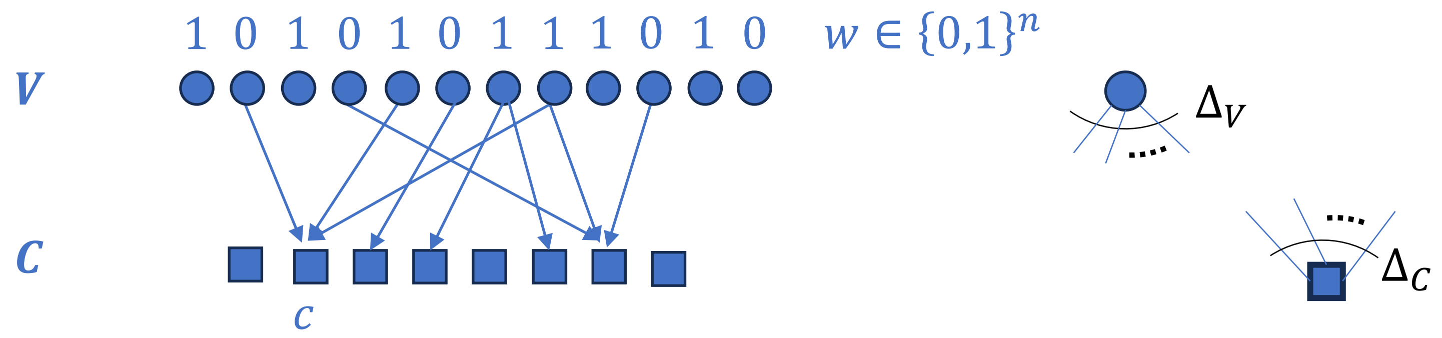
- Need quantum error correction – Qubits+gates imperfect[1,2,3,4].
- Error correction is resource intensive.
- Quantum LDPC codes may be one path to efficient quantum computers[5,6].
- Today: new decoding algorithm for Hypergraph Product codes.

[1]Aharonov, Ben-Or 1997
[2]Kitaev 1997
[3]Knill, Laflamme, Zurek 1998
[4]Aliferis, Gottesman, Preskill 2005
[5]Kovalev, Pryadko 2013
[6]Gottesman 2014

Classical LDPC Codes

- Classical $[\![n,k,d]\!]$ code $\mathcal{C} \subset \{0,1\}^n$ encodes k bits with distance d.
- LDPC code – parity checks bits graph is sparse.

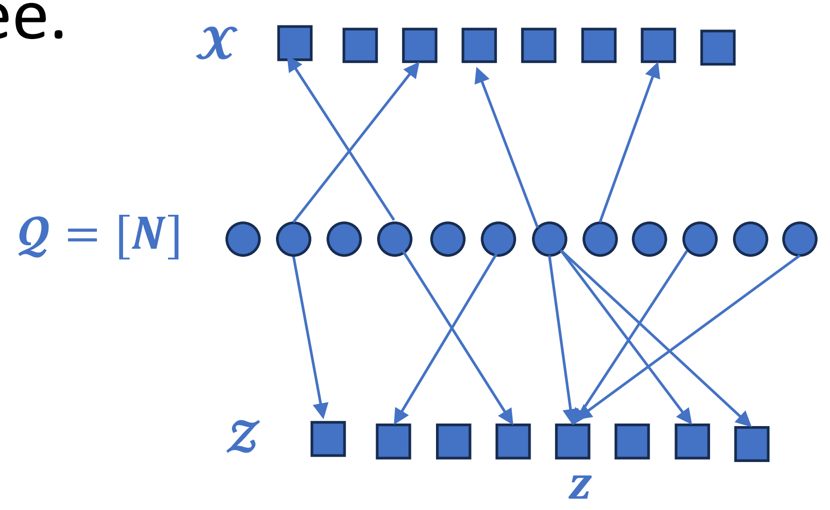
$$w \in \mathcal{C}$$
$$\Updownarrow$$
$$\forall c \in C,\ \bigoplus_{i \leftrightarrow c} w_i = 0$$



Quantum LDPC Codes

- Quantum $[\![N, K, D]\!]$ LDPC code $\mathcal{H}$ encodes K qubits in N qubits with "distance" D.
- Created by two classical ECC $\mathcal{C}_X, \mathcal{C}_Z$ such that $\mathcal{C}_X^{\perp} \subseteq \mathcal{C}_Z$.
- LDPC code – each vertex has a constant degree.
- Reduced Z-type error $\mathcal{E} - w \in \mathcal{C}_Z^{\perp}$:

$$|\mathcal{E}| \leq |\mathcal{E} \oplus w|$$

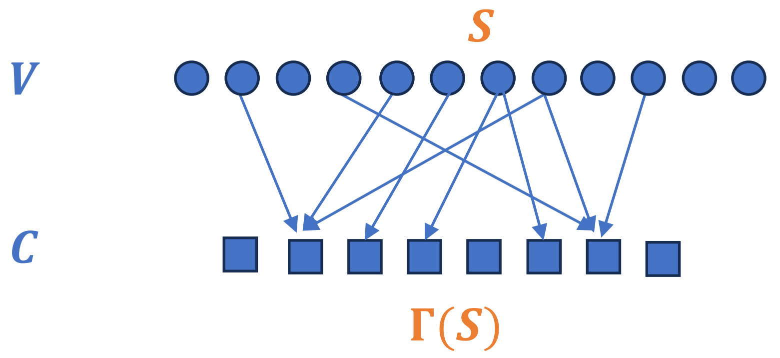


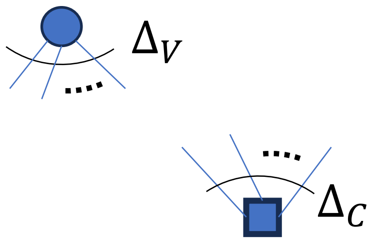
Expansion

- A graph $G = (V \cup C, E)$ is an (α, ϵ)-expander if $\forall\, S \subseteq V$,

$$|S| \leq \alpha\, n$$
$$\Downarrow$$
$$|\Gamma(S)| \geq (1-\epsilon)\Delta_V |S|$$

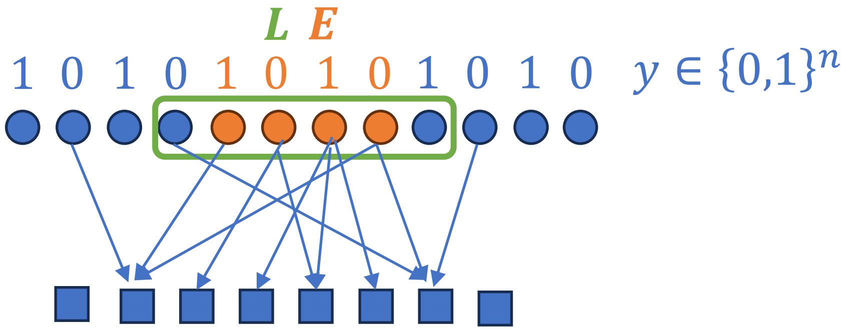
- Bidirectional if it holds also for $S \subseteq C$.





Decoding Classical LDPC codes

- Flip algorithm[1]: decoding based on bit flips.
- Flip bits to reduce unsatisfied parity checks.
- Viderman's algorithm[2]: converts errors to erasure.
- Given $y \in \{0,1\}^V$ when $y = w + 1^E$, $w \in \mathcal{C}$, $|E|$ is small.
- Returns $L \supset E$.



[1]Sipser, Spielman 1996
[2]Viderman 2013

Viderman's Algorithm

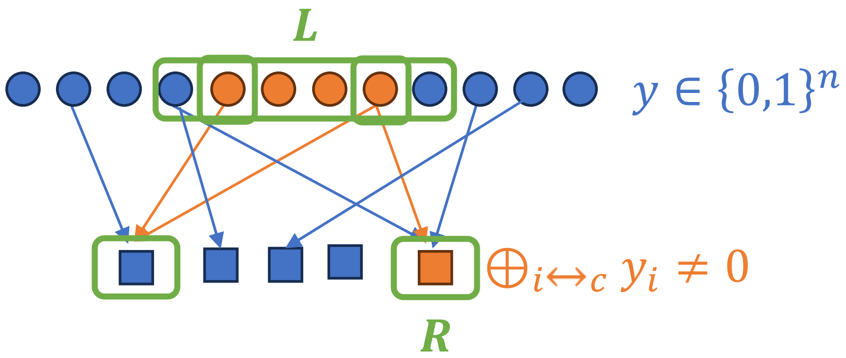
Init:

- $L \leftarrow \emptyset$, $R \leftarrow \text{UNSAT}$.

Iteration:

- While exists v with $|\Gamma(v) \cap R| \geq h$:
  - $L \leftarrow L \cup \{v\}$.
  - $R \leftarrow R \cup \Gamma(v)$.

Output L.



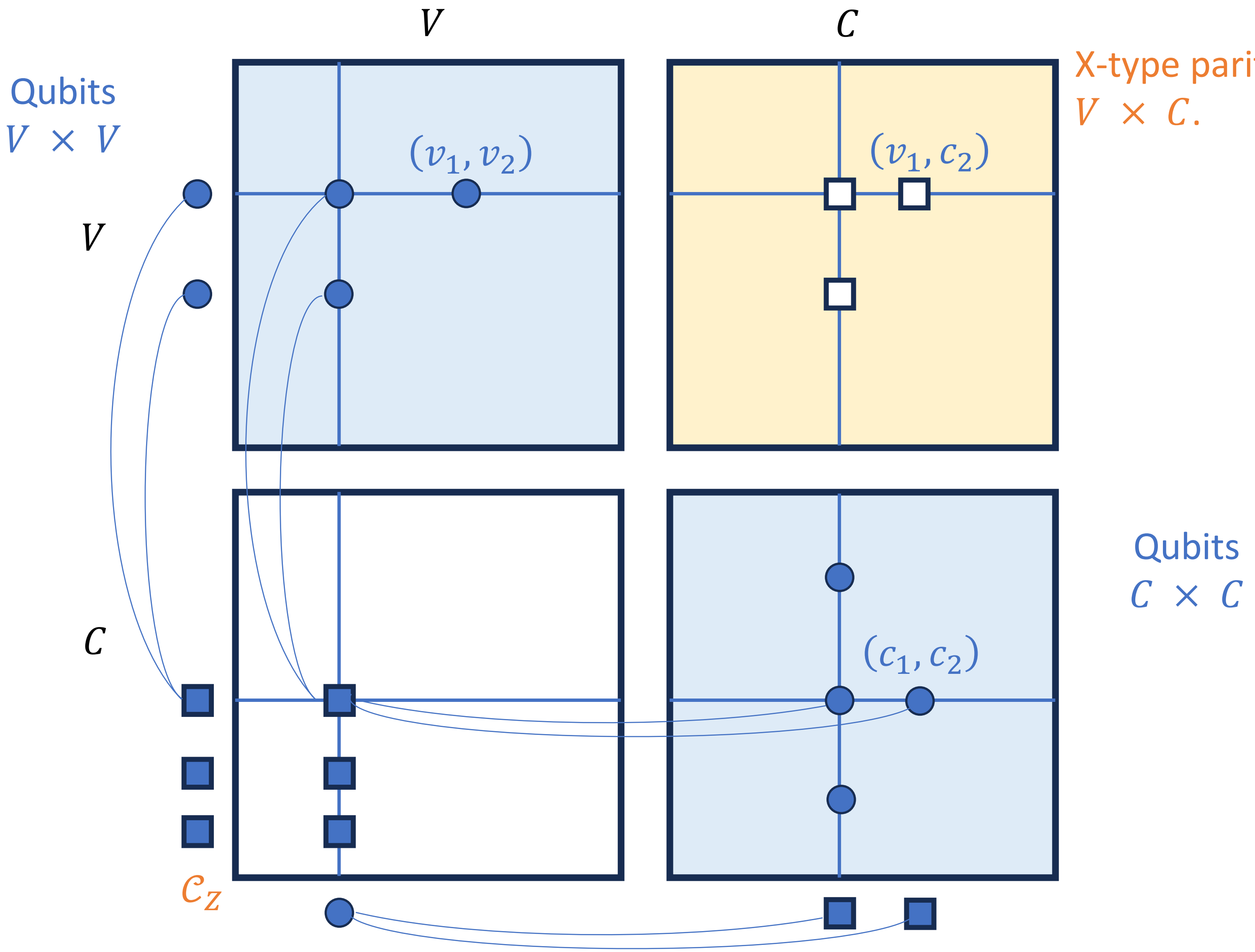
Promise: if E is not too large, $E \subseteq L$, $|L| \leq \gamma|E|$.

Hypergraph Product Codes

- HGP[1] is an $[\![N, \mathrm{K} = \Theta(N), D = \Theta(\sqrt{N})]\!]$ quantum LDPC codes.
- Constructed from bidirectional expander graph.
- Quantum parity check graph is a product of two classical expander graphs.

[1]Tillich, Zémor 2009

Hypergraph Product Codes

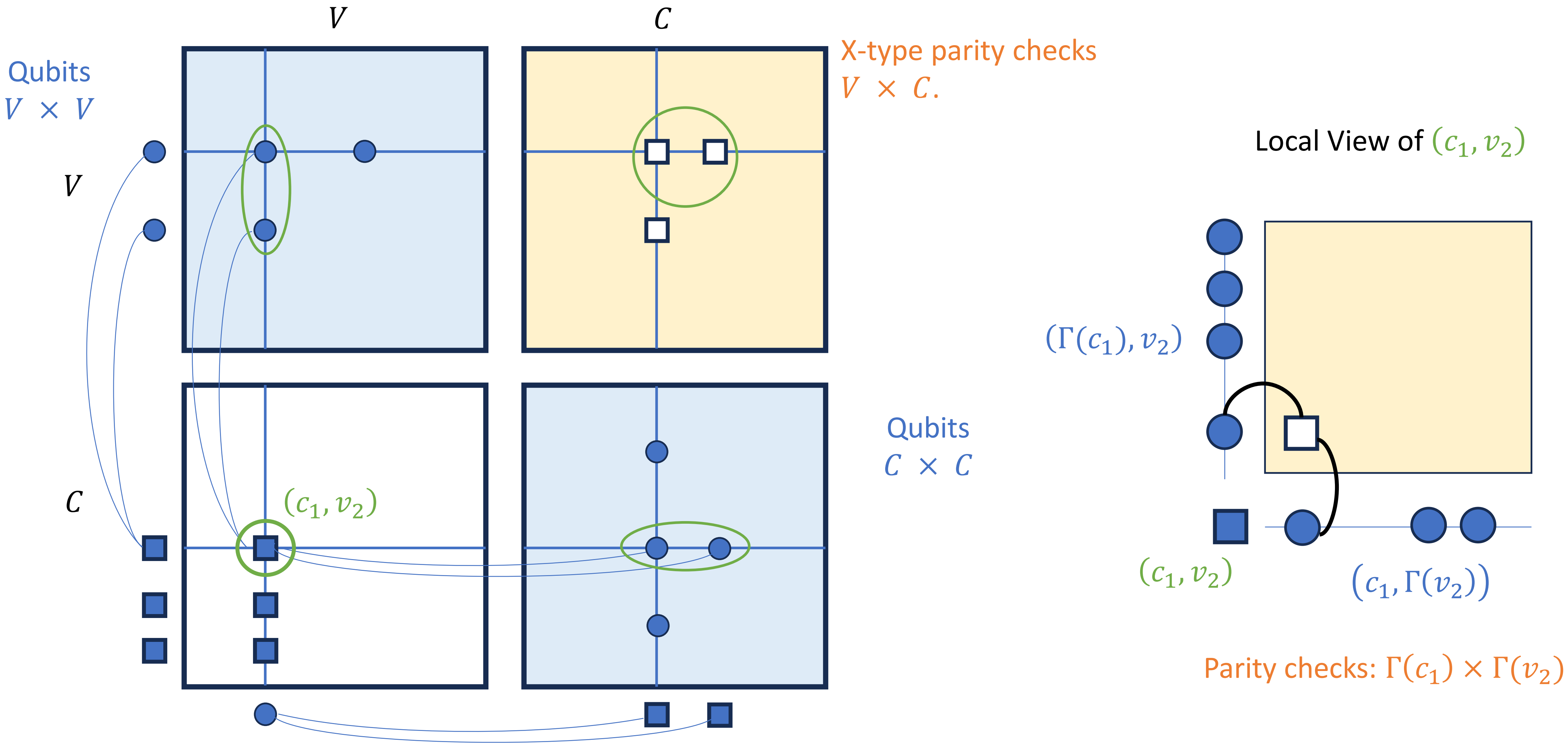


X-type parity checks, defined $\mathcal{C}_X$
$V \times C$.

X-types parity checks of (v_1, v_2):
$(v_1, \Gamma(v_2))$

Qubits in the parity check (v_1, c_2):
$\big(v_1, \Gamma(c_2)\big) \cup (\Gamma(v_1), c_2)$

Local Views


V
C
X-type parity checks
$V \times C$.
Qubits
$V \times V$
V
C
(c_1, v_2)
Qubits
$C \times C$
Local View of (c_1, v_2)
$(\Gamma(c_1), v_2)$
(c_1, v_2)
$(c_1, \Gamma(v_2))$
Parity checks: $\Gamma(c_1) \times \Gamma(v_2)$

Decoding the Hypergraph Product Codes

- Goal: correct $\Theta(D)$ errors.

- Small-Set-Flip[1]: a quantum decoding algorithm for HGP codes.
- Quantum version of the Flip algorithm[2] – uses bit flips.

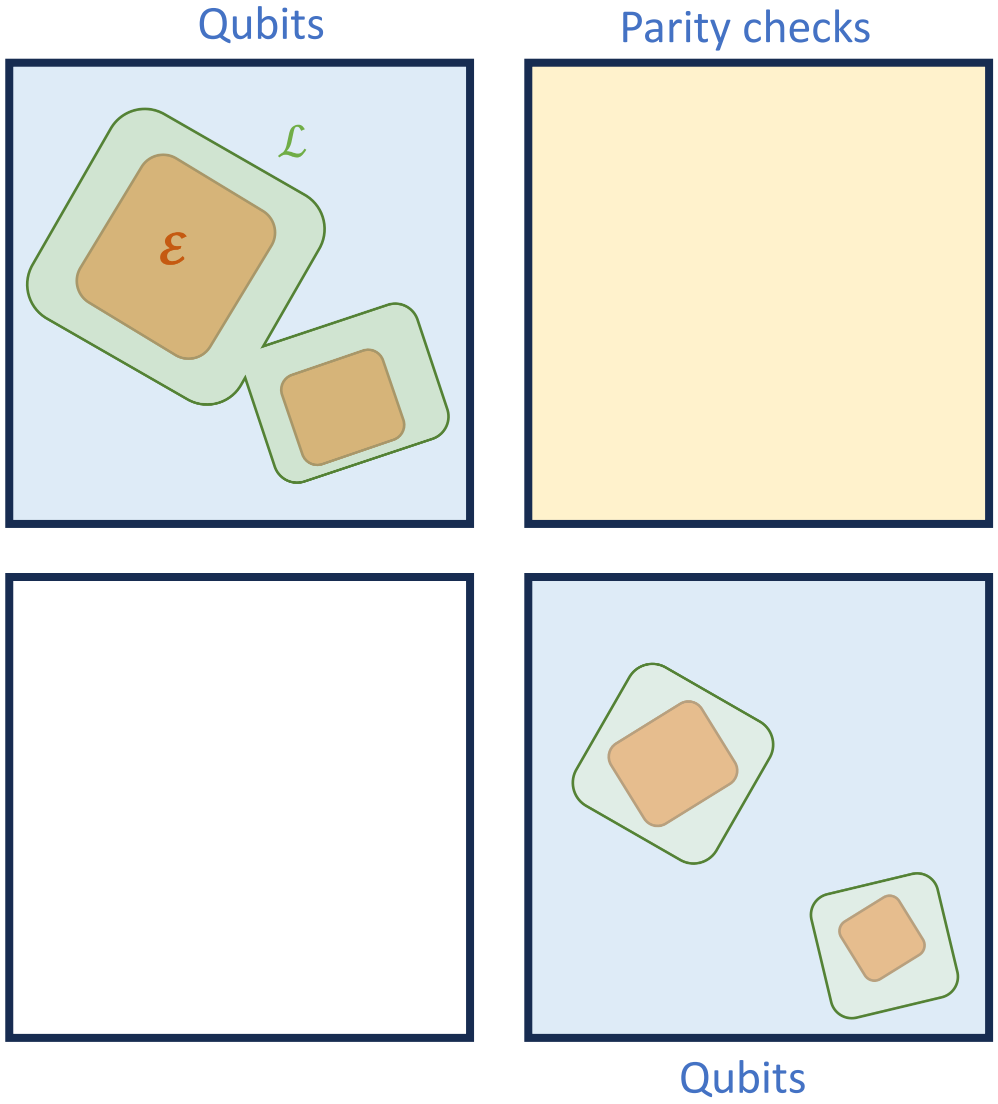
- Can we correct $\Theta(D)$ errors with erasure conversion algorithm?

[1]Leverrier, Tillich, Zémor 2015
[2]Sipser, Spielman 1996

Viderman's Algorithm for HGP Codes

- Can we generalize VIDERMAN to the quantum setting?

- We want an envelope $\mathcal{L}$
- Containing the error: $\mathcal{E} \subset \mathcal{L}$
- Not too large: $|\mathcal{L}| \leq \gamma|\mathcal{E}|$



Our Results: Small-Set-Find

Theorem (informal): Let $\mathcal{H}$ be an $[\![N, K, D]\!]$ hypergraph product code. Given an error $\mathcal{E}$, $|\mathcal{E}| \leq \frac{1}{\gamma} D(1 - \mathrm{o}(1))$, Small-Set-Find returns an envelope $\mathcal{L}$ such that $\mathcal{E} \subset \mathcal{L}$ and $|\mathcal{L}| \leq \gamma |\mathcal{E}|$.

- Highlights:
  - New decoding algorithm!
  - Small-Set-Find is a $\Theta(N)$-time algorithm.
  - Can handle $\Theta(D)$-sized errors.
- Note: quantum erasure decoding is not $\Theta(N)$-time.

Small-Set-Find Algorithm – High Level

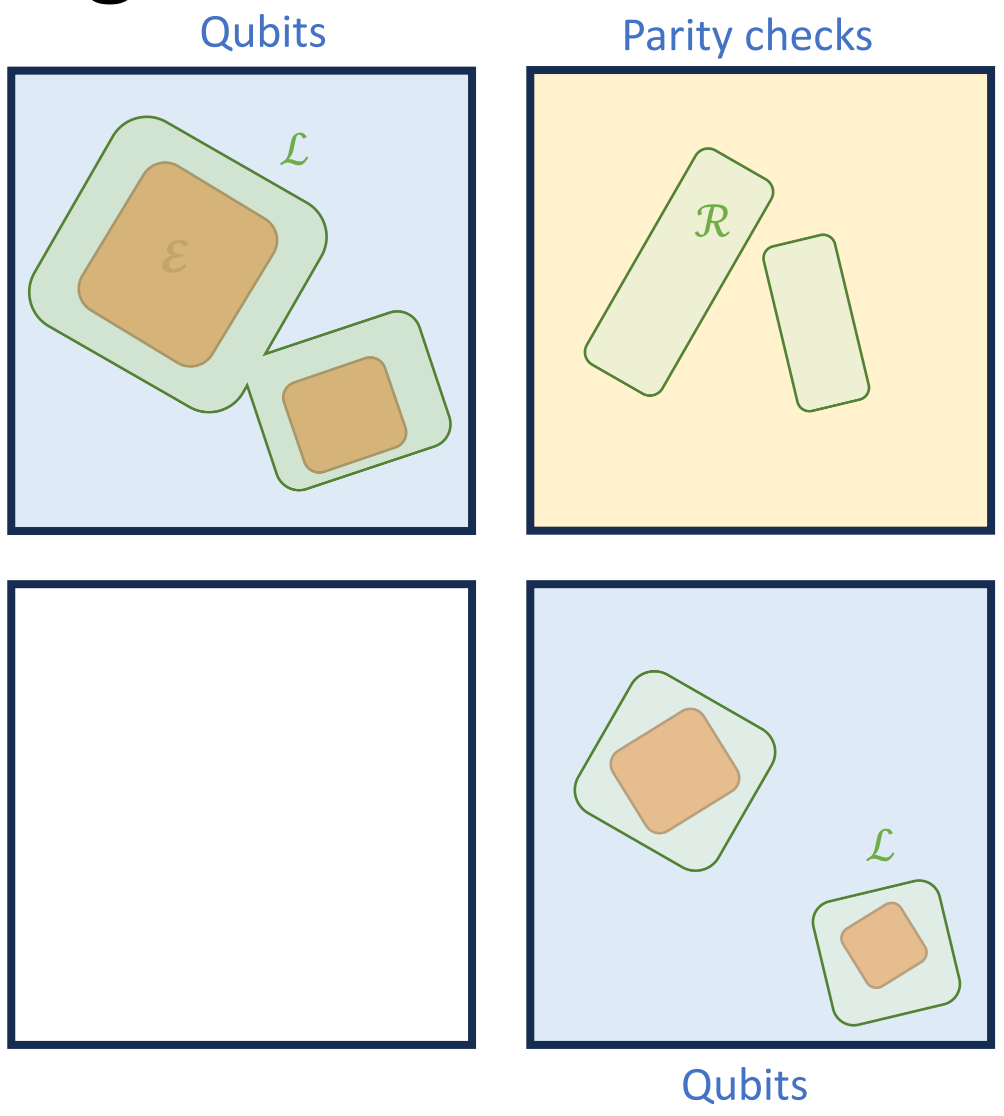
Init:

- $\mathcal{L} \leftarrow \emptyset, \mathcal{R} \leftarrow \text{UNSAT}.$
- $\mathcal{S} \leftarrow$ collection of small sets of qubits.

Step:

- While exists $\mathcal{F} \in \mathcal{S}$ with $\text{score}(\mathcal{F}) \leq h$:
  - $\mathcal{L} \leftarrow \mathcal{L} \cup \mathcal{F}$.
  - $\mathcal{R} \leftarrow \mathcal{R} \cup \Gamma(\mathcal{F})$.

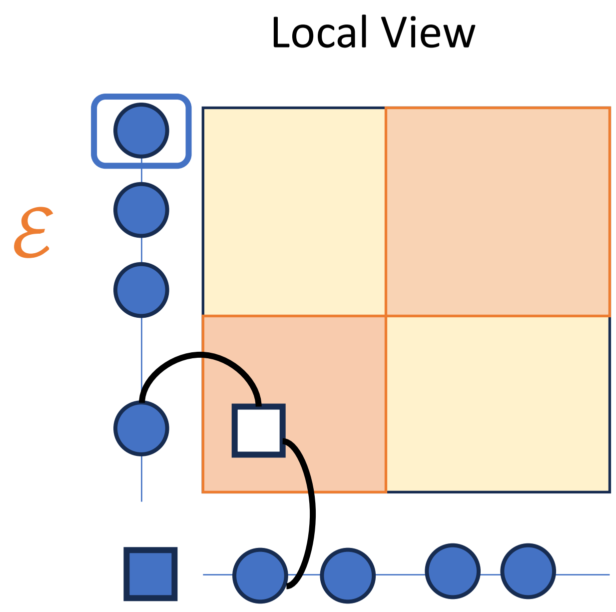
Output $\mathcal{L}$.



Why Small Sets?

- The classical Viderman's algorithm iterates over single bits:
$$|\Gamma(v) \cap R| \geq h \Longrightarrow L \leftarrow L \cup \{v\}.$$

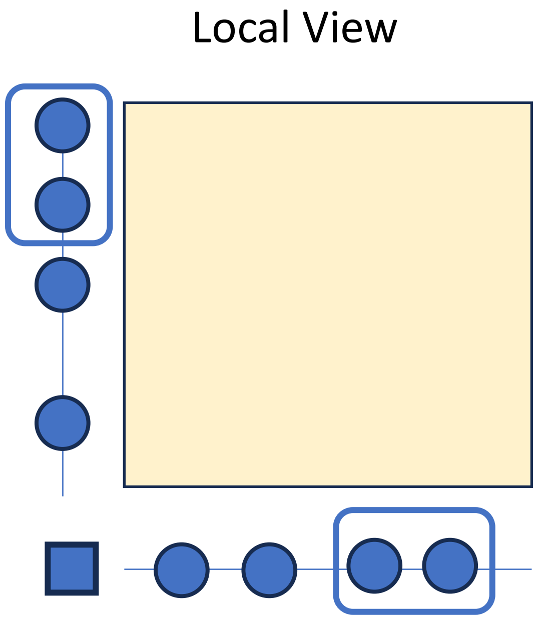
- Problem: underlying graph is not expanding.
- For $\mathcal{E}$= half the local view, need to set $h = \frac{1}{2}\Delta$.
- This threshold is too low to bound $|\mathcal{L}|$.



The Small Sets

- Solution: consider small sets $\mathcal{F}$.
- Define $\mathcal{S}$: all reduced sets $\mathcal{F}$ in all local views.
- $\mathcal{F}$ is reduced: $||\mathcal{F}|| \leq \frac{1}{2}||\text{local view qubits}||$.

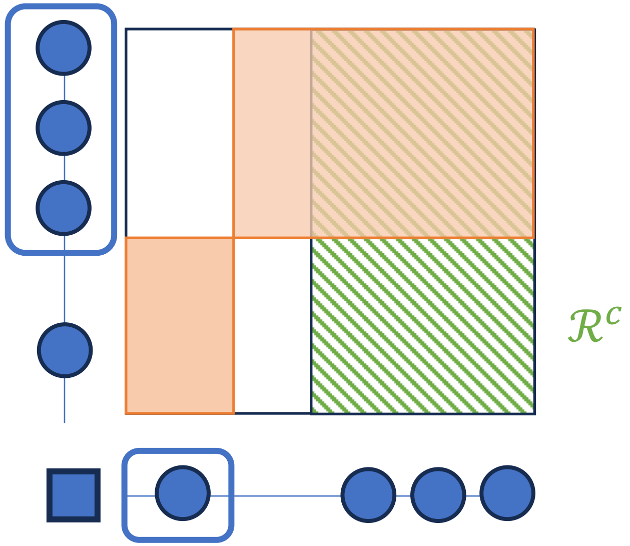
- We have:
  - $|\mathcal{S}| = \Theta(N)$.
  - Decompose non-expanding sets are covered by $\mathcal{S}$.



The Score Function

- When is $\mathcal{F} \in \mathcal{S}$ suspicious?

$$\text{score}(\mathcal{F}) = \frac{\left|\Gamma^{(u)}(\mathcal{F}) \cap \mathcal{R}^c\right|}{\|\mathcal{F}\|} \leq h$$



The score function is:

- Uses unique neighborhood.
- Intersection with $\mathcal{R}^c$.
- Normalized by size of $\mathcal{F}$.

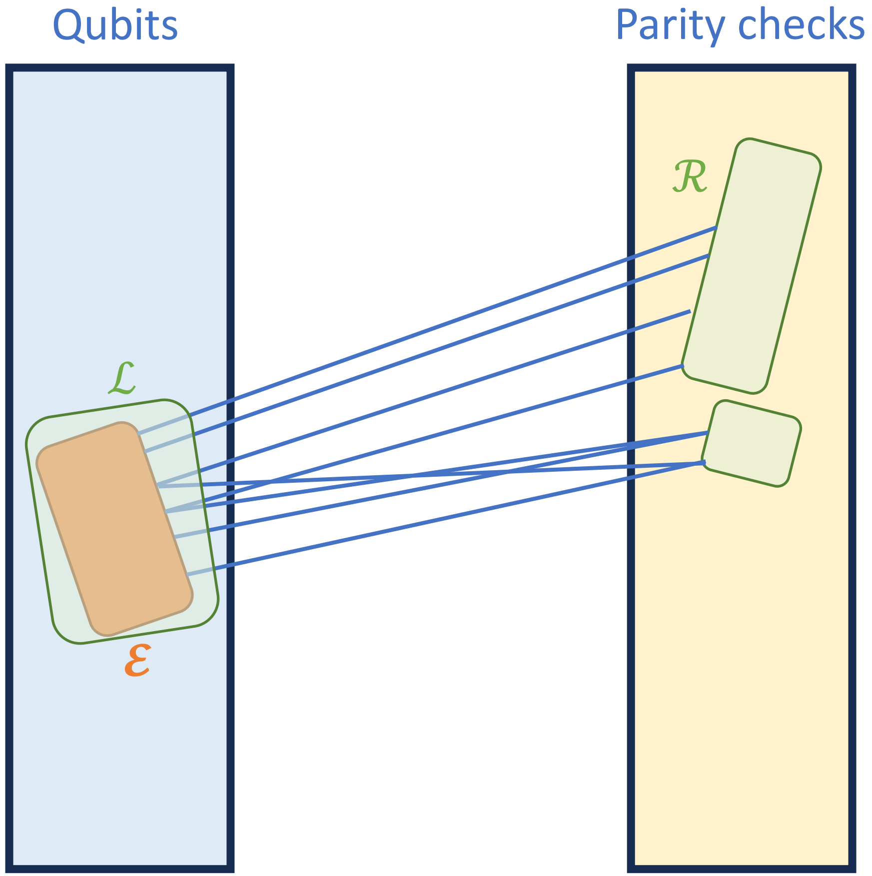
Comparing to Union Find

- UNION FIND
  - Erasure conversion algorithm for surface codes[1].
  - Does not directly generalize to HGP codes.
  - For Hypergraph Product Codes [2] – achieve decoding radius $O(D^{\beta})$ where $\beta < 1$.
- Key difference: Viderman's algorithm does not try to find explanation for the syndrome.

[1]Delfosse, Nickerson 2021
[2]Delfosse, Beverland, Londe 2022

Algorithm Intuition

- Parity check in $\Gamma(\mathcal{E})$ is either UNSAT or adjacent to multiple errors.
- Graph is expanding – many errors are adjacent to UNSAT parity checks.



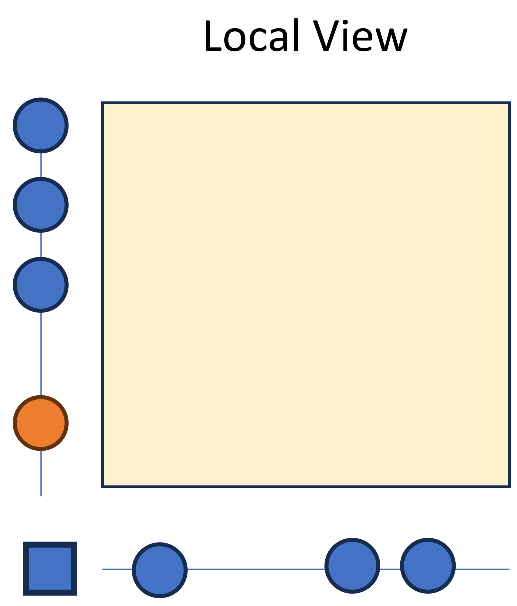
Proof Overview

The proof has two parts:

Claim 1: the envelope $\mathcal{L}$ covers the error: $\mathcal{E} \subset \mathcal{L}$.

If the algorithm stopped and $\mathcal{E} \not\subseteq \mathcal{L}$:

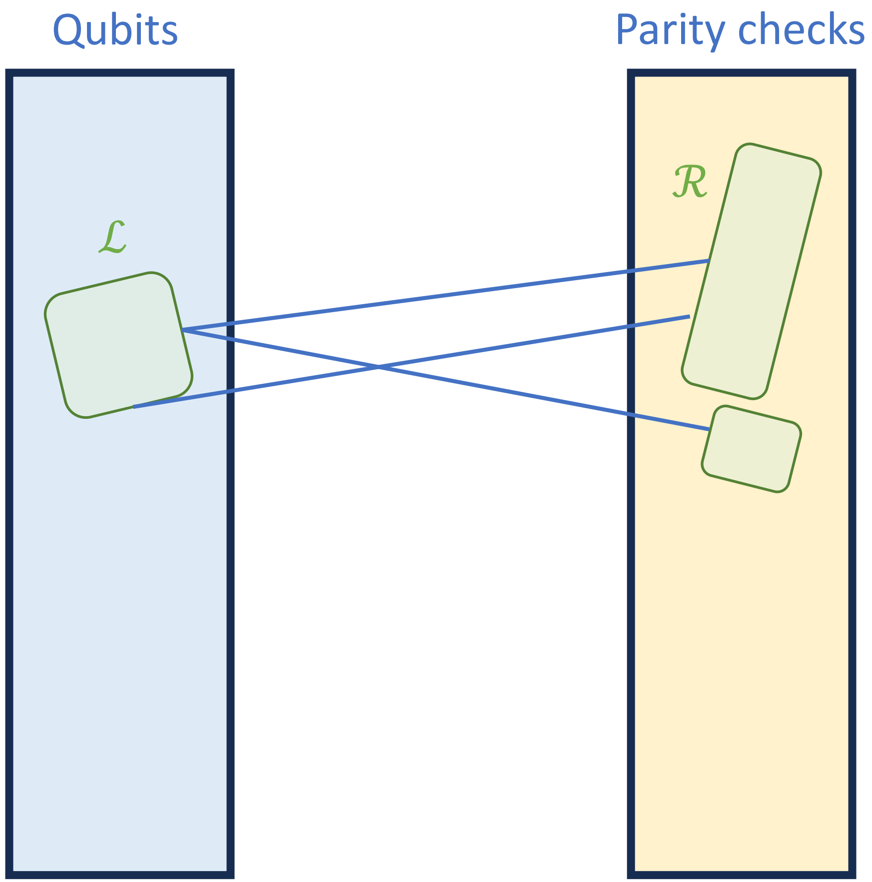
- Exists a local view with $\mathcal{E} \setminus \mathcal{L}$ and few external interactions.
- Exists $\mathcal{F} \in \mathcal{S}$ with $\text{score}(\mathcal{F}) \leq h$.



Proof Overview

Claim 2: the envelope $\mathcal{L}$ is not too large: $|\mathcal{L}| \leq \frac{1}{\gamma}|\mathcal{E}|$.

- Every set $\mathcal{F}$ we add to $\mathcal{L}$ has small $\left|\Gamma^{(u)}(\mathcal{F}) \cap \mathcal{R}^c\right|$.
- The graph is expanding: $\Gamma(\mathcal{L}) \geq \frac{1}{2}(1-\epsilon)\Delta|\mathcal{L}|$.



Comparing FLIP Algorithm

- HPG code on a bipartite graph with:
  - Degrees Δ_V, Δ_C. Ratio $r = \frac{\Delta_V}{\Delta_C} < 1$.
  - (α, ϵ) expander.

Algorithm	Decoding Radius	Minimal Expansion
SSFlip [LTZ15][1]	$\frac{1}{3(1+\Delta_C)} D$	$\epsilon < \frac{1}{6}$
SSFlip [FGL18][2]	$\frac{2r(1-8\epsilon)}{4+2r(1-8\epsilon)} \frac{r}{\sqrt{1+r^2}} \mathrm{D}$	$\epsilon < \frac{1}{8}$
Viderman's Algorithm	$\frac{1-10\epsilon}{4} rD$	$\epsilon < \frac{1}{10}$

[1]Leverrier, Tillich, Zémor 2015
[2]Fawzi, Grospellier, Leverrier 2018

Summary and Outlook

- Summary:
  - Linear-time erasure-conversion algorithm for Hypergraph Product codes.
- Future questions:
  - Can we improve the parameters?
  - Can we generalize to good LDPC codes i.e. codes with $D = \Theta(N)$?
  - Are there linear-time erasure decoding algorithms?

Thank you!