Quantum LDPC Codes

Adway🧑, Sagnik🧑

CMSC828K, Dec 10, 2020

Motivation for Quantum Codes

Errors in quantum world are more ubiquitous than in the classical world

Many kinds of errors – phase flips, bit flips etc. Most errors are continuous

Measurement destroys quantum information. ECCs are harder to construct

QECCs used to build fault tolerant quantum computers

CSS Codes

Two mutually orthogonal binary codes

$$\mathcal{C}_Z^\perp \subseteq \mathcal{C}_X$$

Dimension

$$k_\mathcal{Q} = \dim\left(\mathcal{C}_X \setminus \mathcal{C}_Z^\perp\right) = \dim\left(\mathcal{C}_Z \setminus \mathcal{C}_X^\perp\right)$$

Distance

$$\begin{aligned}
d_\mathcal{Q} &= \min\ \{d_X, d_Z\} \\
d_X &= \min\left\{|x|, x \in \mathcal{C}_X \setminus \mathcal{C}_Z^\perp\right\} \\
d_Z &= \min\left\{|x|, x \in \mathcal{C}_Z \setminus \mathcal{C}_X^\perp\right\}
\end{aligned}$$

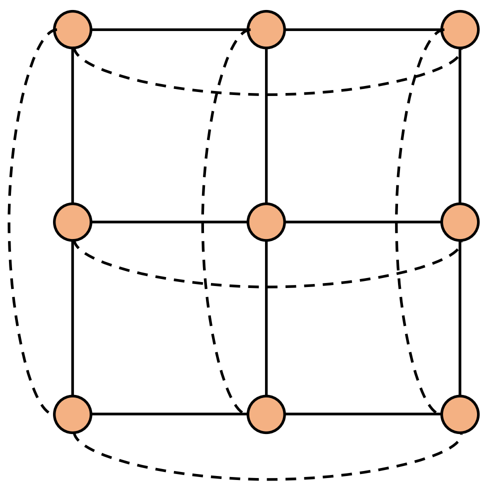
LDPC Codes

- Binary linear code with a sparse parity check matrix
- Efficient decoding algorithms exist. Use Tanner graphs associated with the parity check matrix.

LDPC CSS Code

- When parity check matrices H_X and H_Z are sparse
- Random construction does not work anymore. With probability 1, H_X and H_Z are not orthogonal

The Toric Code (m=2)



The vertex-edge incidence matrix and the face-edge incidence matrix

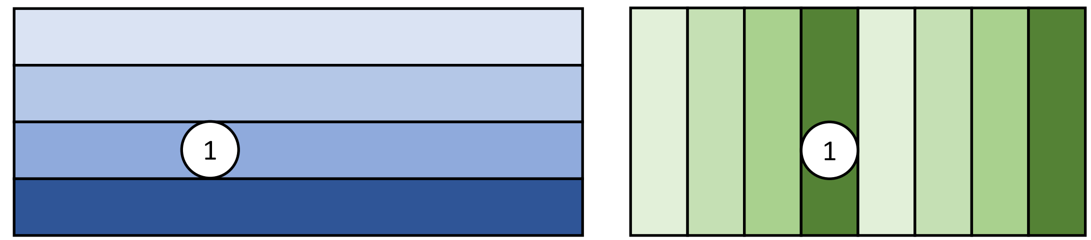
$$H_X = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Can be thought of as a product of two cycles of length m

$$H_Z = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

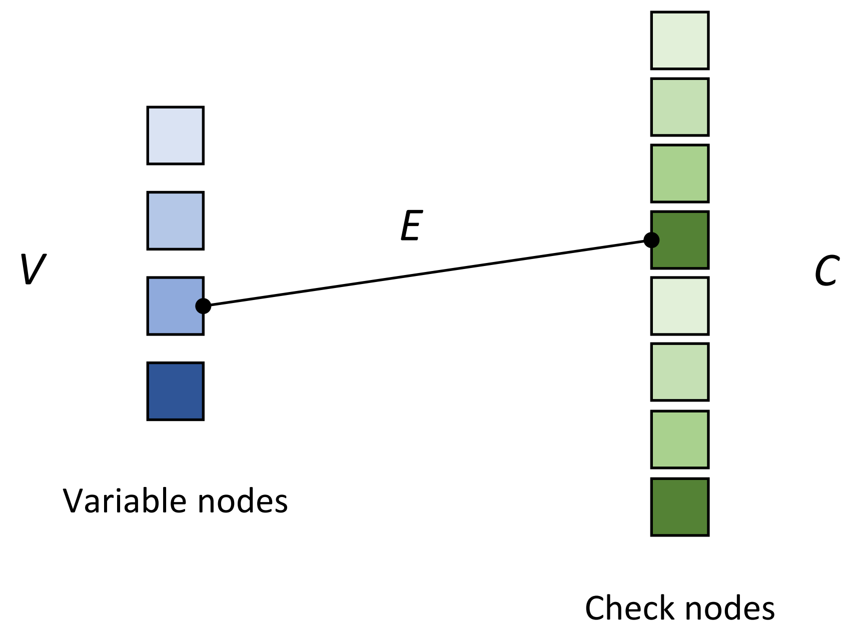
Tanner Graph

Parity check matrix **H**

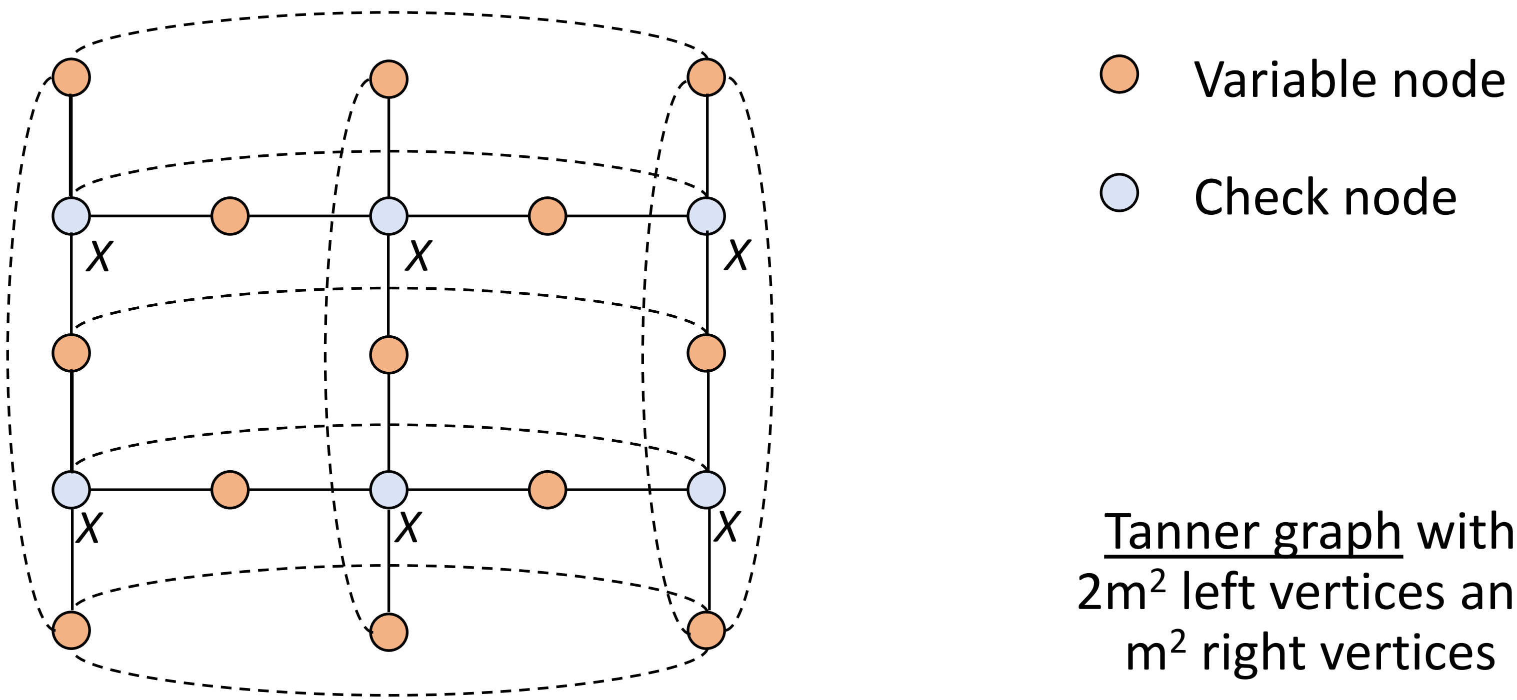


Tanner graph *(V, C, E)*

(bipartite)



Tanner graph of Toric Code *(m = 2)*

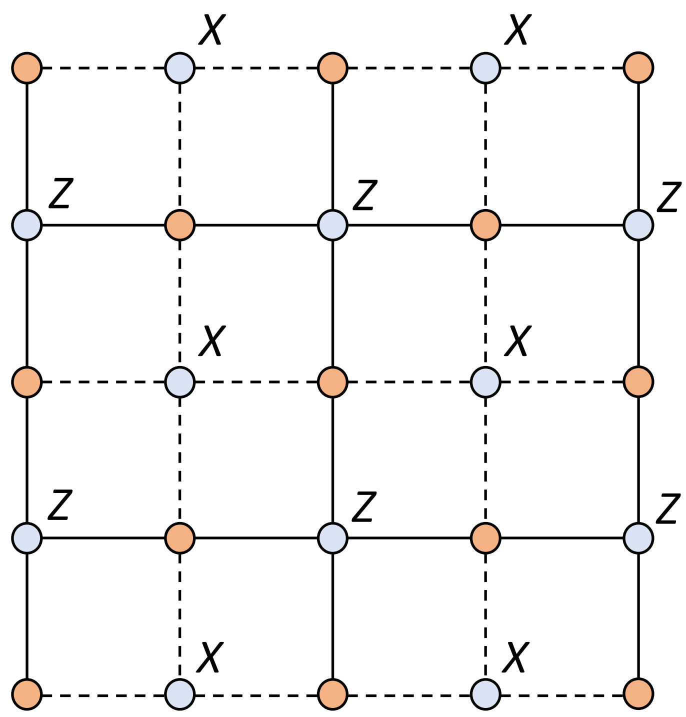


Tanner graph with $2m^2$ left vertices and m^2 right vertices

Can do the same thing with the face-edge incidence matrix ie H_Z

Tanner graph of Toric Code *(m = 2)*

Combining the two Tanner graphs we get…



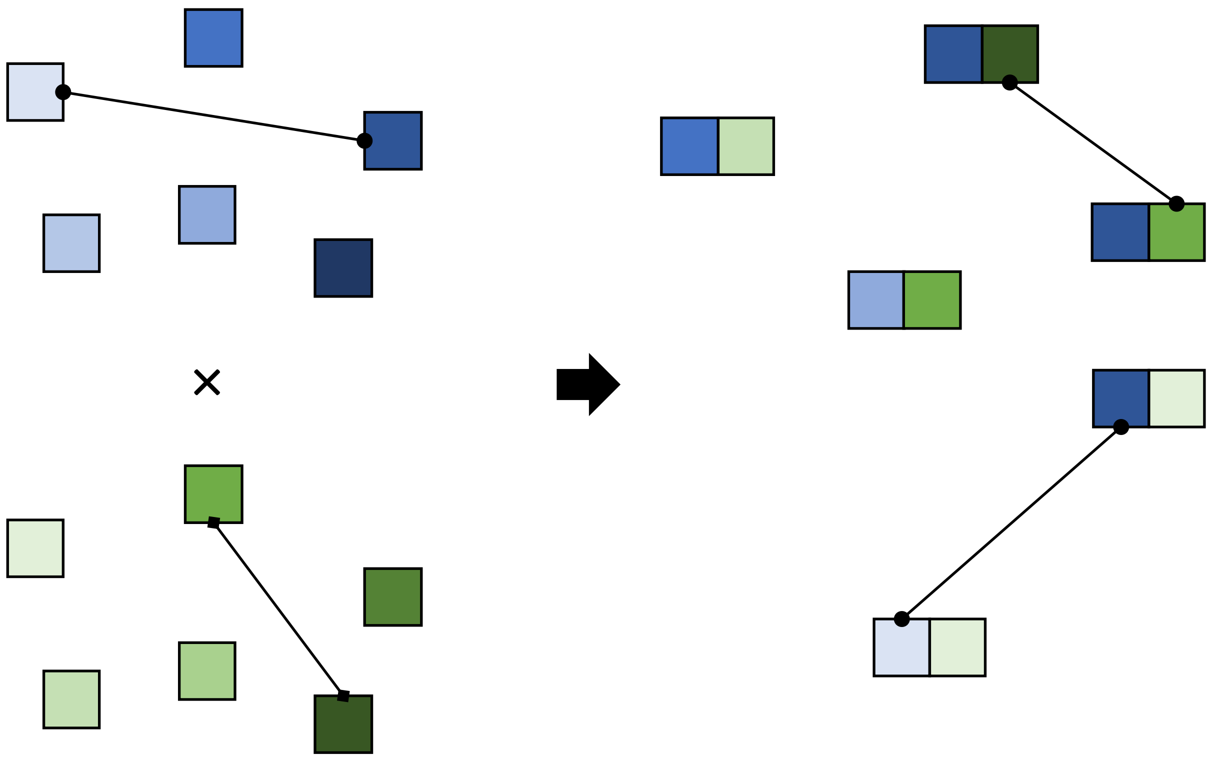
Can be thought of as a product of two cycles of length 2m

Graph Products

Product of two graphs $\mathcal{G}_1$ and $\mathcal{G}_2$, has vertex set $V_1 \times V_2$. The vertices (x,y) and (x',y') are connected if x = x' and y, y' are connected in $\mathcal{G}_2$ or y = y' and x, x' are connected in $\mathcal{G}_1$.

Graph 1
(V_1, E_1)

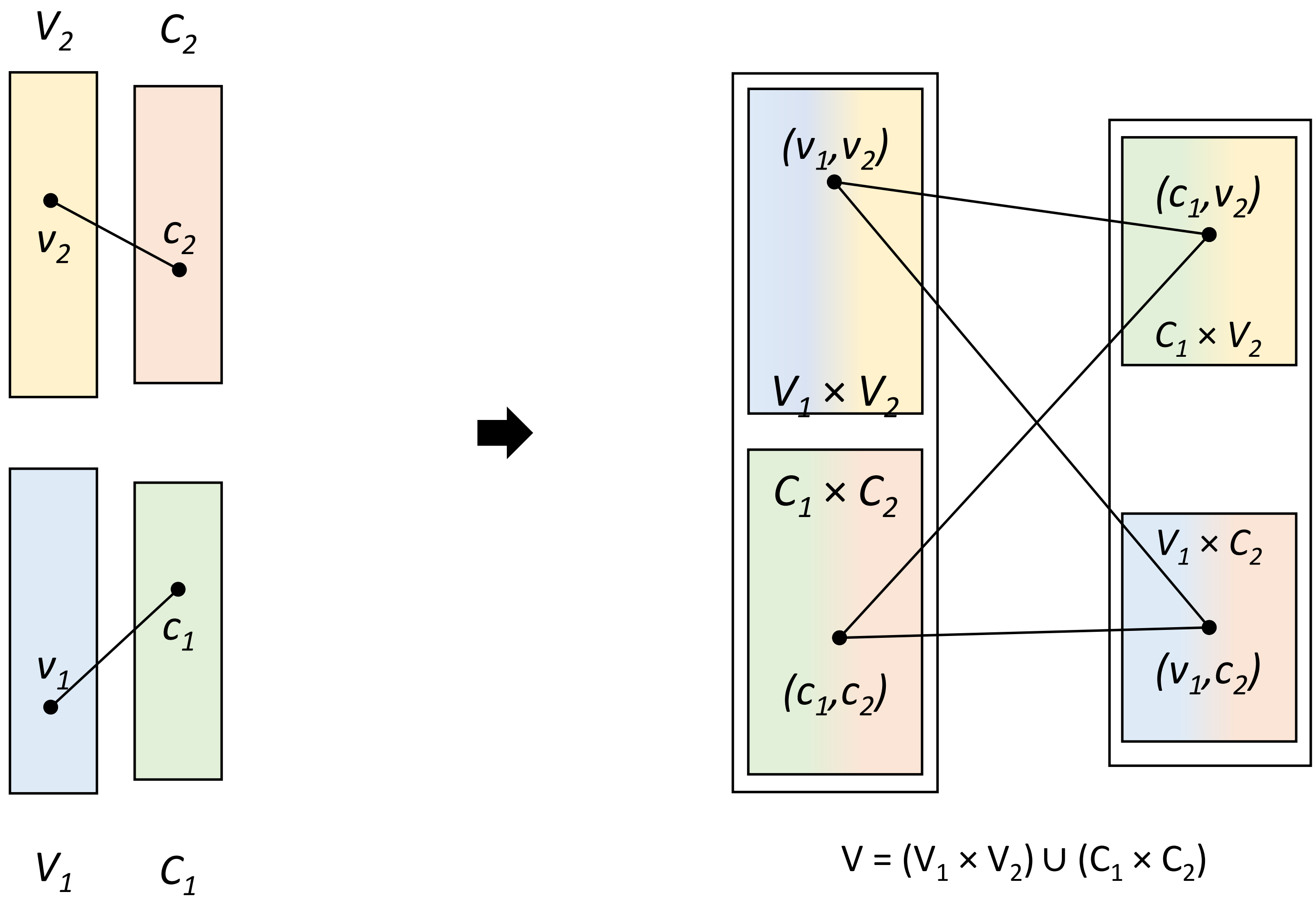
Graph 2
(V_2, E_2)



Question

What if we take products of arbitrary graphs?

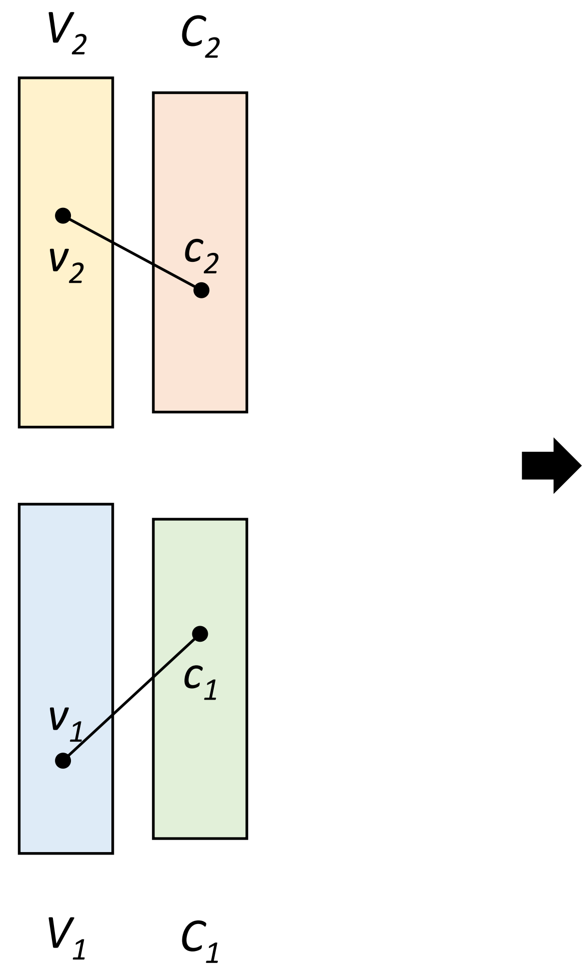
Product of Tanner Graphs

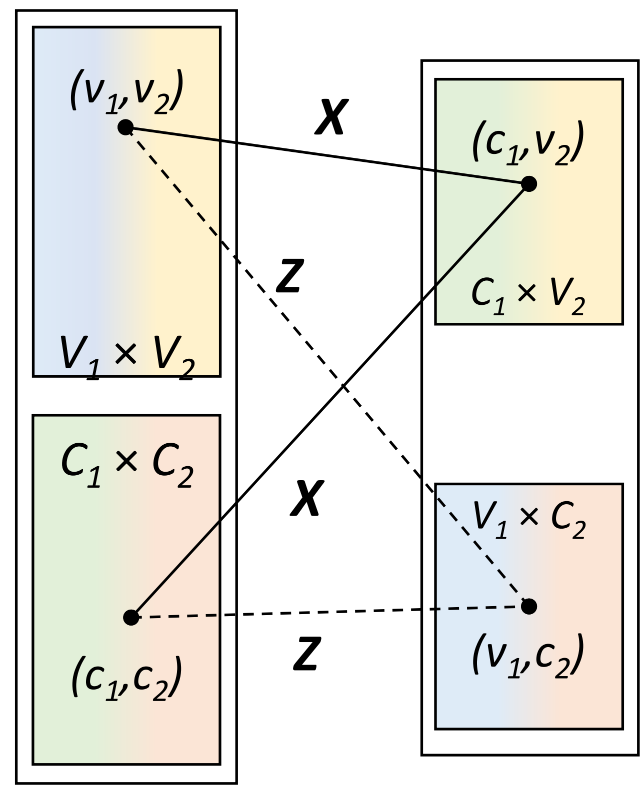


$V = (V_1 \times V_2) \cup (C_1 \times C_2)$

$C = (C_1 \times V_2) \cup (V_1 \times C_2)$

Product of Tanner Graphs





$V = (V_1 \times V_2) \cup (C_1 \times C_2)$

$C = (C_1 \times V_2) \cup (V_1 \times C_2)$

This graph product gives a CSS code

Proposition – Let $\mathcal{G}_1 = (V_1, C_1, E_1)$ and $\mathcal{G}_2 = (V_2, C_2, E_2)$ be two Tanner graphs. Then we have

$$\mathcal{C}_X(\mathcal{G}_1 \times \mathcal{G}_2)^\perp \subseteq \mathcal{C}_Z(\mathcal{G}_1 \times \mathcal{G}_2)$$

- Let $v_i \in V_i$ and $c_i \in C_i$ for $i = 1, 2$
- $h_X(c_1, v_2)$ is the row of H_X corresponding to check node (c_1, v_2)
- $h_Z(v_1, c_2)$ is the row of H_Z corresponding to check node (v_1, c_2)
- $\langle h_X(c_1, v_2), h_Z(v_1, c_2)\rangle$ = # nodes adjacent to both in V
- If v_i is not adjacent to c_i in $\mathcal{G}_i$ for any i, then this number is 0
- Otherwise this number is 2.

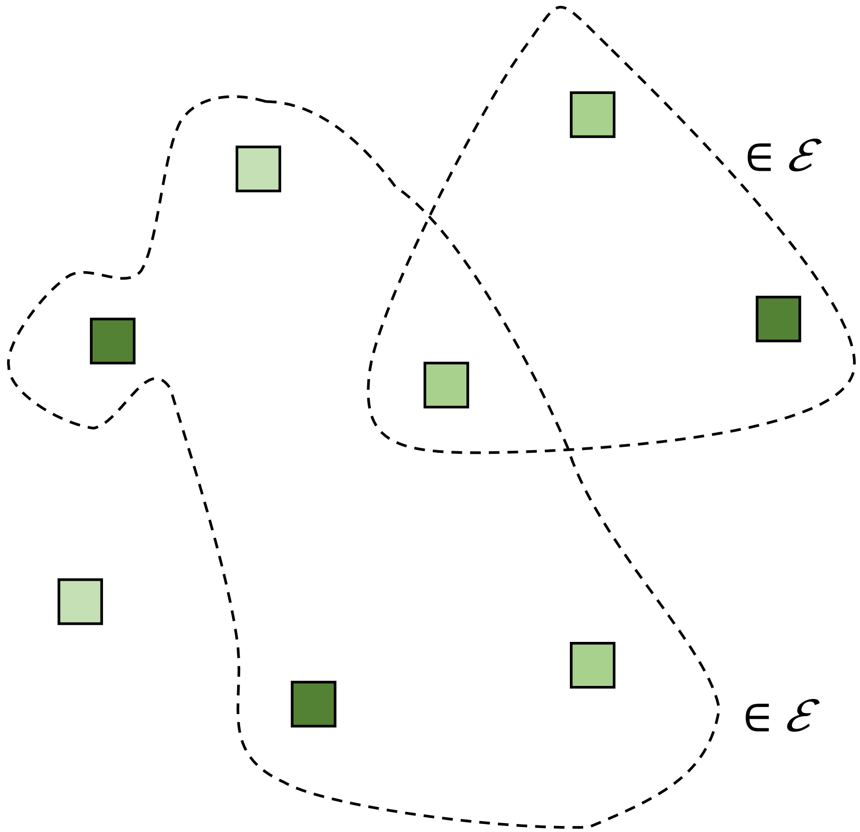
Question

We have a CSS code 🥳

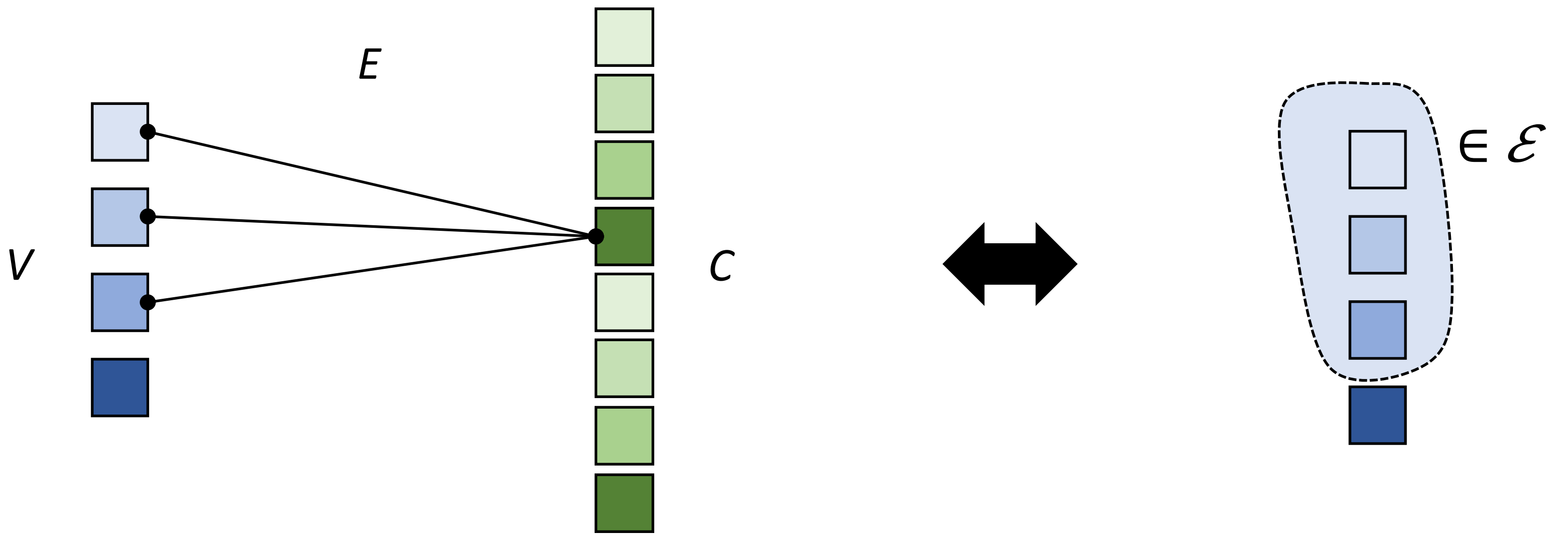
What about dimension and distance? 🤔

Hypergraph *(V, $\mathcal{E}$)*

A 'graph' in which each (hyper)edge connects more than one vertex



Bipartite (Tanner) Graphs and Hypergraphs



Tanner graph *(V, C, E)*

(bipartite)

Hypergraph *(V, ℰ)*

The neighbourhood of a check node becomes a hyperedge.

Hypergraph Products

Generalization of graph products

Product of two hypergraphs $\mathcal{H}_1$ and $\mathcal{H}_2$, has vertex set $V=V_1 \times V_2$.
Hyperedges of the product are of the form

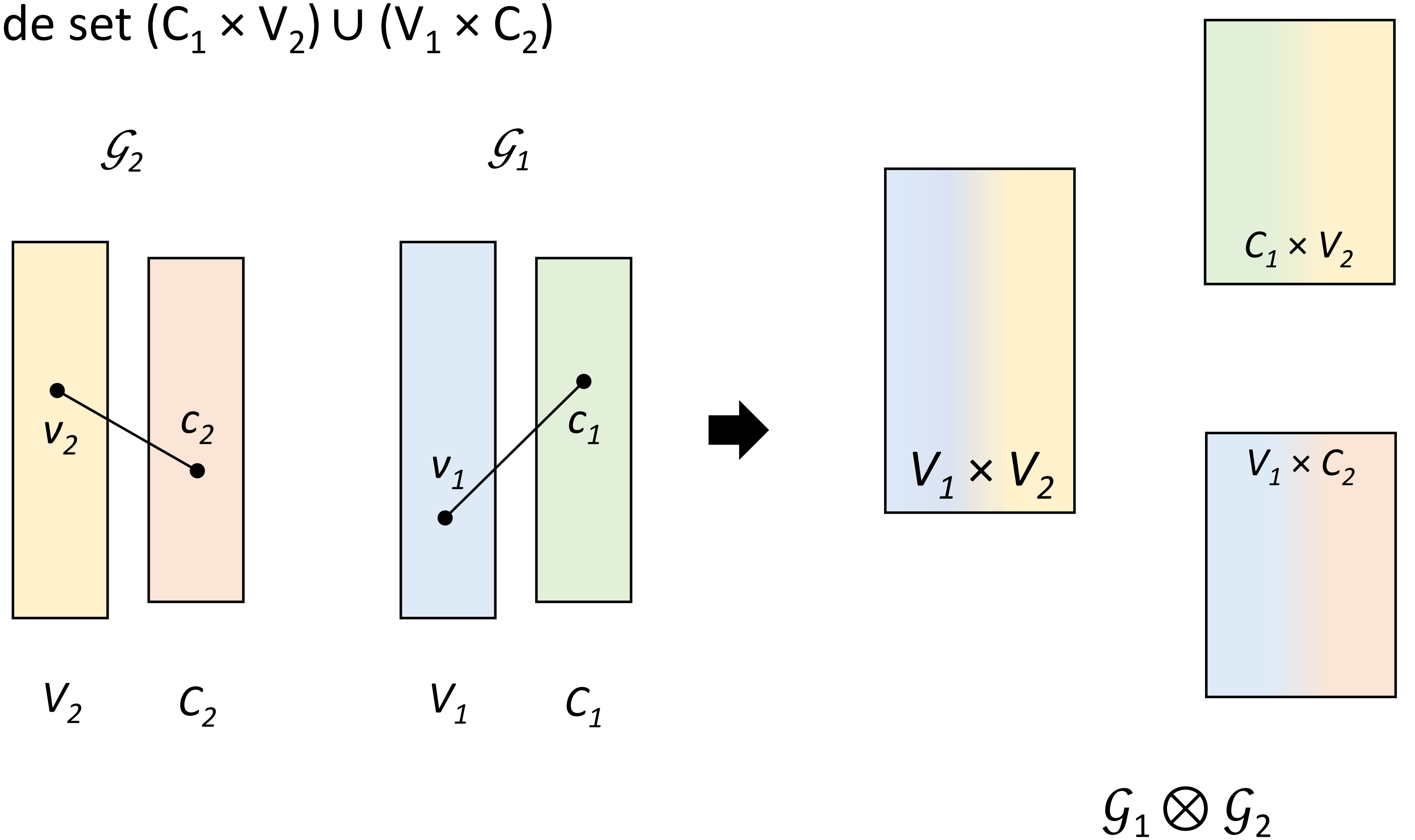
- $\{v_1\} \times e_2$ or
- $e_1 \times \{v_2\}$

where e_1 and e_2 are in $\mathcal{E}_1$ and $\mathcal{E}_2$ respectively.

We can define a new product $\otimes$ of Tanner graphs by using this definition and the equivalence between Tanner graphs and hypergraphs

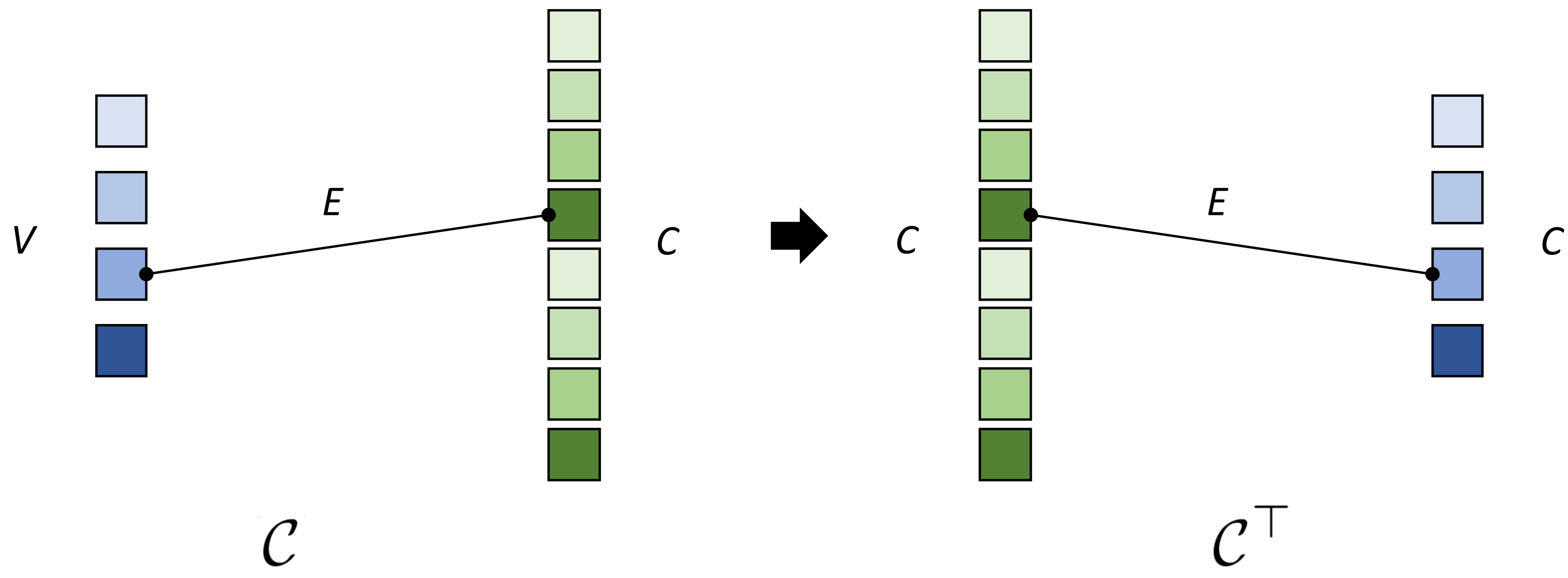
Hypergraph Products in terms of Tanner graphs

Induced subgraph of $\mathcal{G}_1 \times \mathcal{G}_2$ with variable node set $V_1 \times V_2$ and check node set $(C_1 \times V_2) \cup (V_1 \times C_2)$



Transpose of a Tanner Graph

Tanner graph *(V, C, E)* → Tanner graph *(C, V, E)*



$$\dim(\mathcal{C}) = |V| - |C| + \dim(\mathcal{C}^\top)$$

Connection to Product Codes

For two binary linear codes of $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n_1 and n_2 the product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is made up of codewords in the form of $n_1 \times n_2$ binary matrices with columns in $\mathcal{C}_1$ and rows in $\mathcal{C}_2$

$$\dim(\mathcal{C}_1 \otimes \mathcal{C}_2) = \dim \mathcal{C}_1 \dim \mathcal{C}_2$$

Proposition: The Tanner graph for $\mathcal{C}_1 \otimes \mathcal{C}_2$ is given by $\mathcal{G}_1 \otimes \mathcal{G}_2$

CSS Codes from Product Codes

With these definitions, we redefine the previously defined CSS code using Tanner graphs $\mathcal{G}_1$ and $\mathcal{G}_2$.

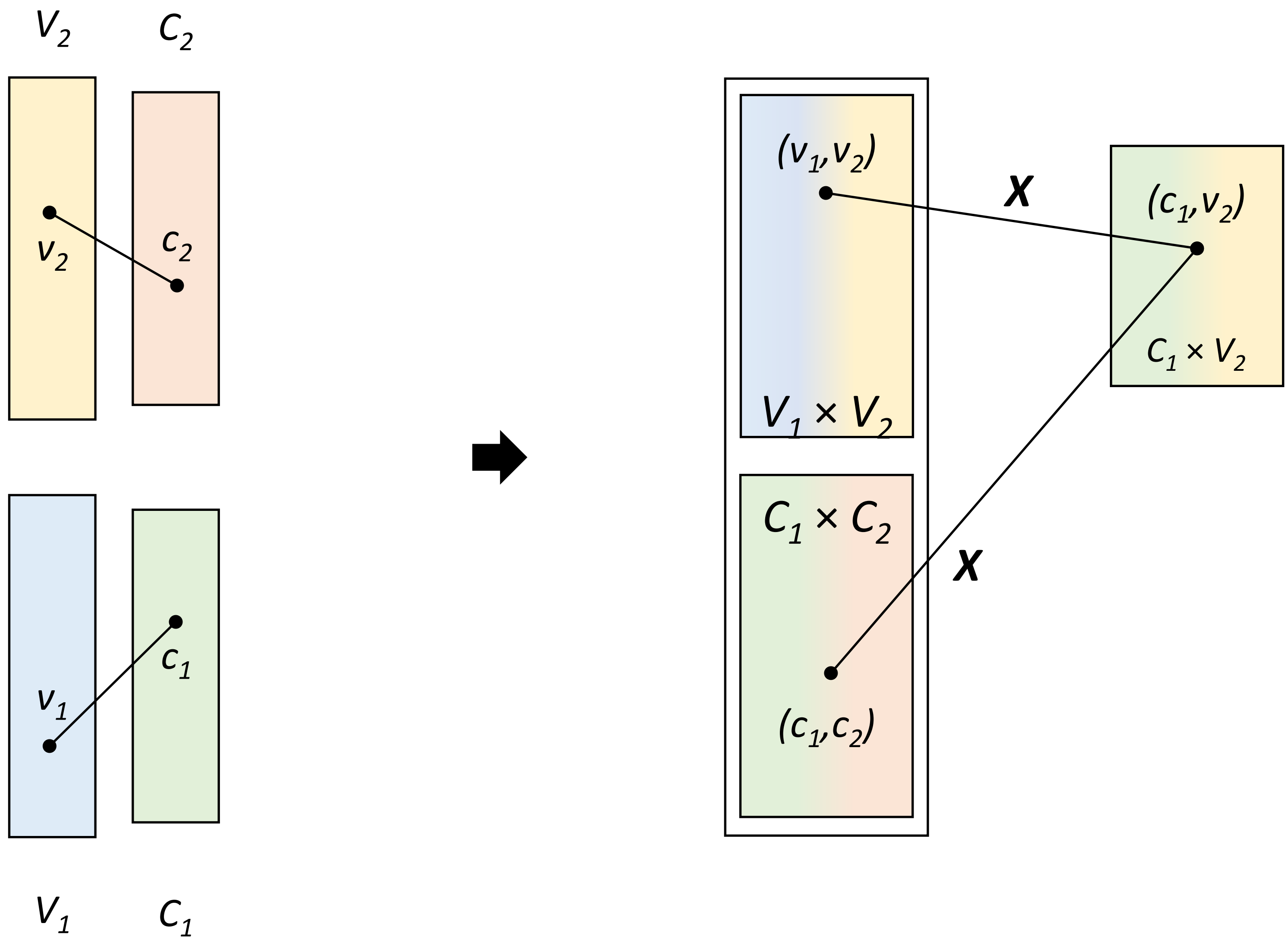
$$\mathcal{G}_1 \times_X \mathcal{G}_2 = (\mathcal{G}_1^\top \otimes \mathcal{G}_2)^\top$$

$$\mathcal{G}_1 \times_Z \mathcal{G}_2 = (\mathcal{G}_1 \otimes \mathcal{G}_2^\top)^\top$$

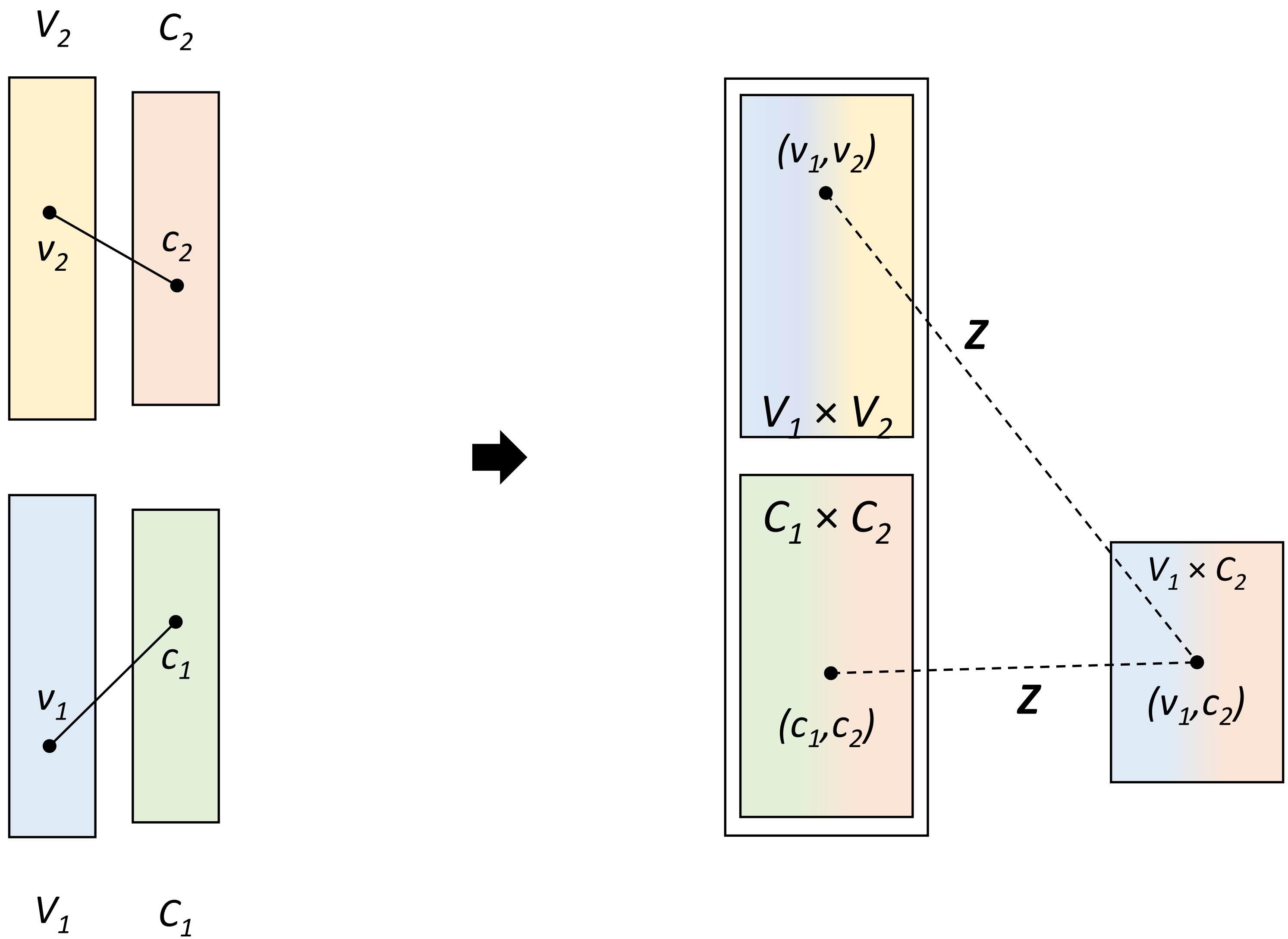
$$\mathcal{C}_X(\mathcal{G}_1 \times \mathcal{G}_2)^\top = \mathcal{C}_1^\top \otimes \mathcal{C}_2$$

$$\mathcal{C}_Z(\mathcal{G}_1 \times \mathcal{G}_2)^\top = \mathcal{C}_1 \otimes \mathcal{C}_2^\top$$

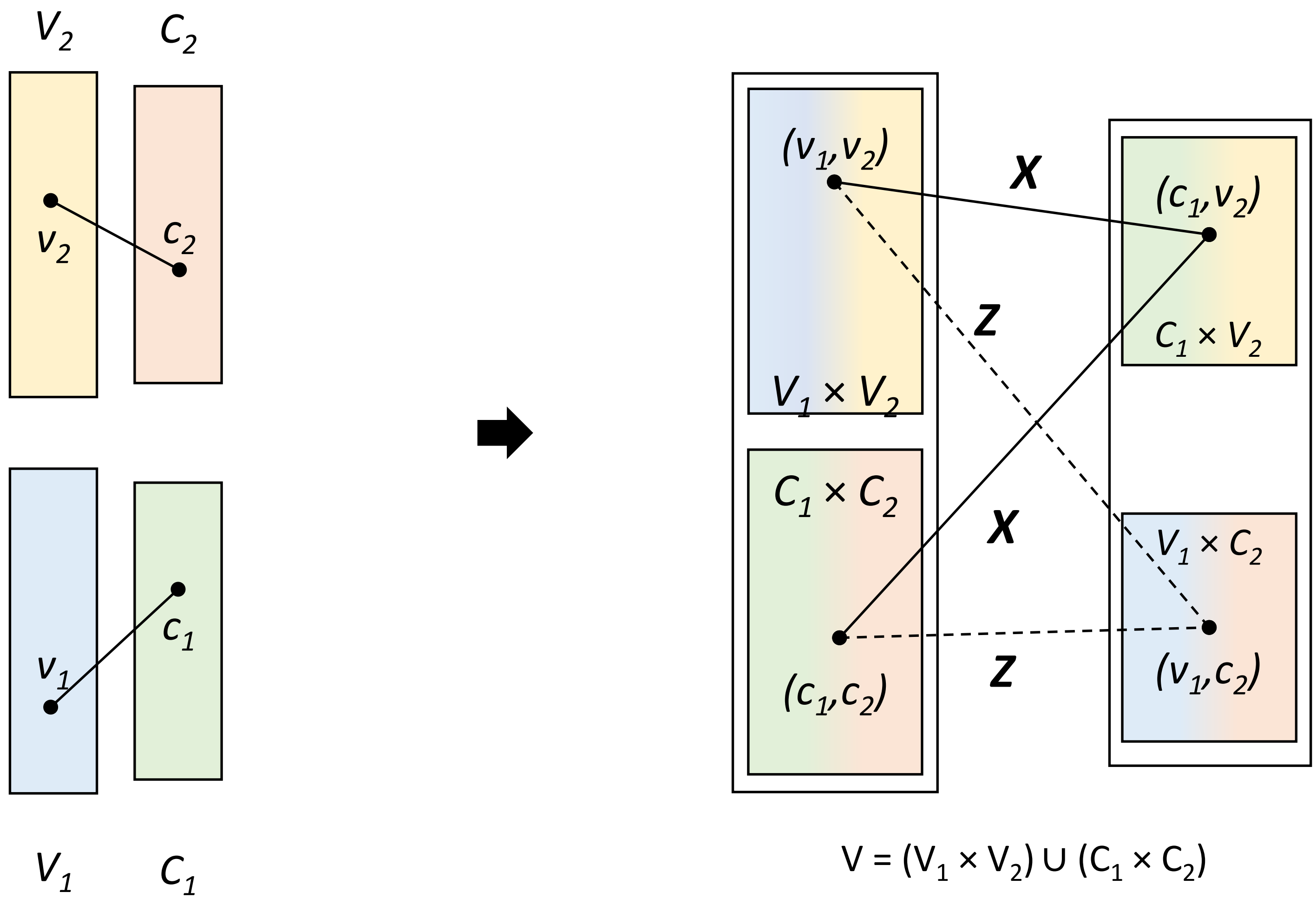
X code from $\mathcal{C}_1 \otimes \mathcal{C}_2$



Z code from $\mathcal{C}_1 \otimes \mathcal{C}_2$



CSS Codes Assemble!



$V = (V_1 \times V_2) \cup (C_1 \times C_2)$

$C = (C_1 \times V_2) \cup (V_1 \times C_2)$

Finally, the dimension…

$$
\begin{aligned}
\dim(\mathcal{C}_X(\mathcal{G}_1 \times \mathcal{G}_2)) &= n_1 n_2 + r_1 r_2 - r_1 n_2 + \dim(\mathcal{C}_X(\mathcal{G}_1 \times \mathcal{G}_2)^\top) \\
&= n_1 n_2 + r_1 r_2 - r_1 n_2 + k_1^\top k_2
\end{aligned}
$$

Similarly…

$$
\dim(\mathcal{C}_Z(\mathcal{G}_1 \times \mathcal{G}_2)) = n_1 n_2 + r_1 r_2 - r_2 n_1 + k_2^\top k_1
$$

And…

$$
\begin{aligned}
k_\mathcal{Q} &= \dim(\mathcal{C}_X(\mathcal{G}_1 \times \mathcal{G}_2)) - (n_1 n_2 + r_1 r_2 - \dim(\mathcal{C}_Z(\mathcal{G}_1 \times \mathcal{G}_2))) \\
&= k_1 k_2 + k_1^\top k_2^\top
\end{aligned}
$$

Minimum Distance

Let d_i be the minimum distance of $\mathcal{G}_i$ and $d_i^\top$ be the minimum distance of $\mathcal{G}_i^\top$, then

$$d_{\mathcal{Q}} \geq \min(d_1, d_2, d_1^\top, d_2^\top)$$

Equality is achieved when none of the four codes is <u>trivial</u>.

Subsequent Work 💻 (N qubits)

Construction	Minimum Distance	Dimension
Toric Code	$\sqrt{N}$	2
This paper (hypergraph products, tilings)	$\sqrt{N}$	*cN*
Couvreur-Delfosse-Zemor (Cayley Graphs, no topology)	$\sqrt{N}$	$\sqrt{N}$
Evra-Kaufman-Zemor (high dimensional expanders)	$\sqrt{N}\log(N)$	'about' $\sqrt{N}$
Hastings-Haah-O'Donnell (fibre bundle codes)	$N^{3/5}/\text{poly}\log(N)$	$N^{3/5}$
Panteleev-Kalachev (lifted product)(3 days back)	$N/\log N$	$\log N$

Thank you! 🙋🙋