Lecture II : Hypergraph Product Codes Part 1

Def: Graph product

The product $G_1 \times G_2$ of two graphs $G_1 = (V_1, E_1)$ & $G_2 = (V_2, E_2)$ has vertex set $\boxed{V = \{(x,y) : x \in V_1, y \in V_2\}}$.

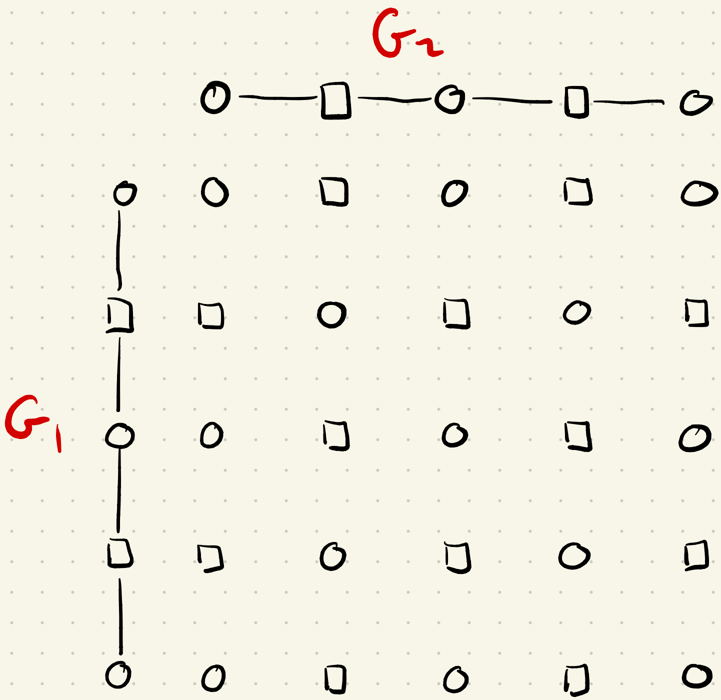
There is an edge between $(x,y) \in V$ & $(x', y') \in V$ if

- $x = x'$ and $\{y, y'\} \in E_2$ or
- $y = y'$ and $\{x, x'\} \in E_1$.

1

Example

$G_1 =$  $= G_2$

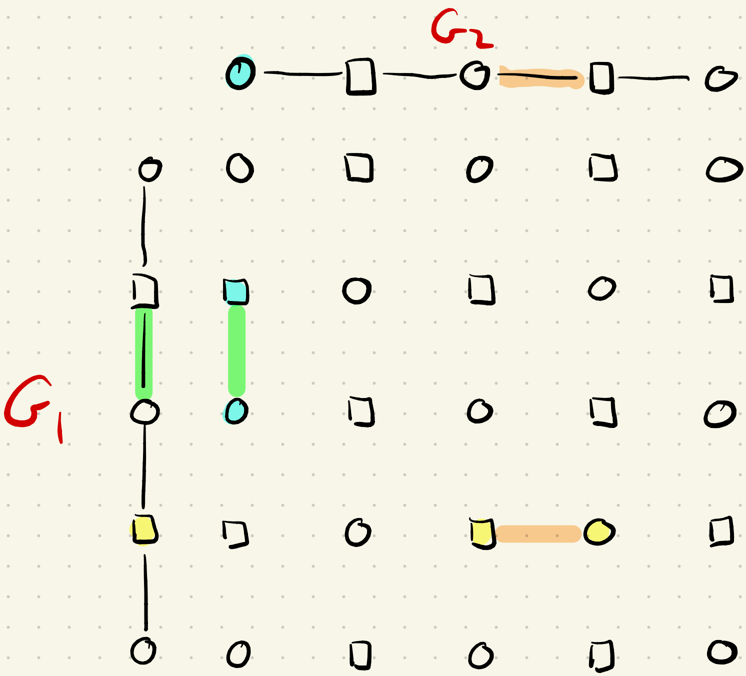


$$V = \{ (x, y) : x \in V_1, \ y \in V_2 \}$$

"row" "column"

Example

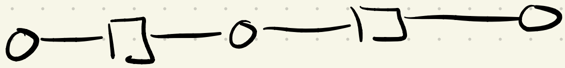
$G_1 =$  $= G_2$

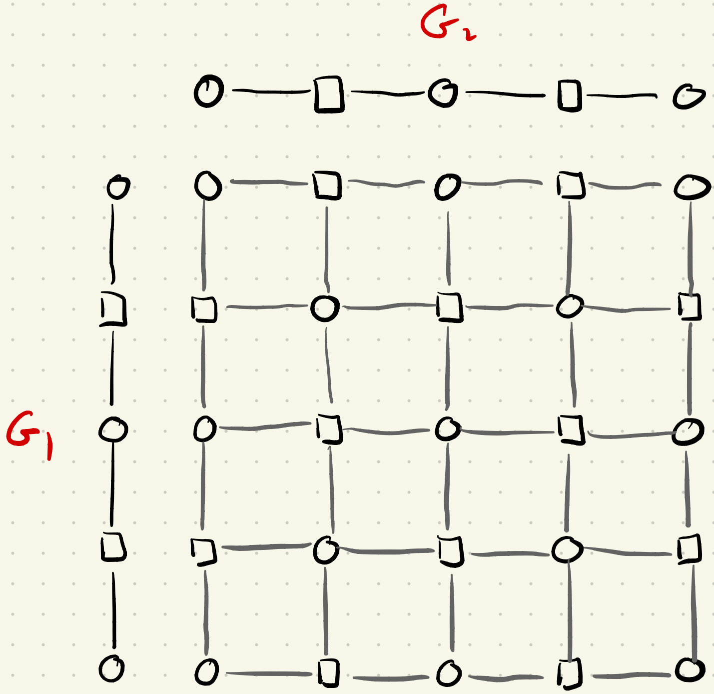


There is an edge between

$(x, y) \in V$ & $(x', y') \in V$ if

- $x = x'$ and $\{y, y'\} \in E_2$ or
- $y = y'$ and $\{x, x'\} \in E_1$.

G_1 =  = G_2



<u>Note</u> that any two edges $\{a,b\} \in G_1$

$\{x,y\} \in G_2$ define a 4-cycle in

$G_1 \times G_2$

$$\begin{tikzcd}
(a,y) \arrow[r, dash] \arrow[d, dash] & (b,y) \arrow[d, dash] \\
(a,x) \arrow[r, dash] & (b,x)
\end{tikzcd}$$

Def: Hypergraph product code

(Tillich e Zémor)

Let $G_1 = (V_1, C_1, E_1)$ &

$G_2 = (V_2, C_2, E_2)$ be two

Tanner graphs.

The hypergraph product code

$HGP(G_1, G_2)$ is the CSS code

with Tanner graph

$G = (V, C_X, C_Z, E)$

where

- $\boxed{V = V_1 \times V_2 \cup C_1 \times C_2}$

- $\boxed{C_X = C_1 \times V_2}$
- $\boxed{C_Z = V_1 \times C_2}$

with edges given by those of the graph product $G_1 \times G_2$.

Specifically consider X check

$(x, y) \in C_X \quad x \in C_1, \; y \in V_2$

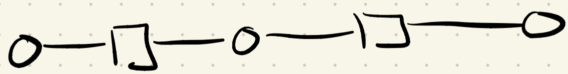
This is connected to variables (qubits)

$(x', y') \in V$ where either

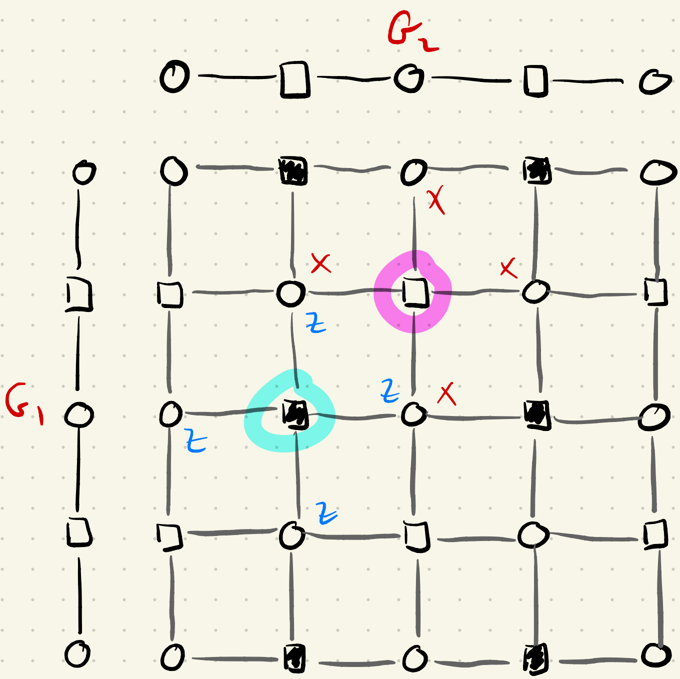
- $x = x'$ and $\{y, y'\} \in E_2$ (and $y' \in C_1$)
- $y = y'$ and $\{x, x\} \in E_1$ (and $x' \in V_2$)

always the case

Example

G_1 =  = G_2

Tanner graph of the (3-bit) repetition code



$C_X = C_1 \times V_2$

$C_Z = V_1 \times C_2$

This, as you may know, is Kitaev's famous toric code.

Lemma 1

HGP(G_1, G_2) defines a valid CSS code.

$G = (V, E)$
$v \in V$
Neighbourhood
$N(v) = \{ u \in V : \{u, v\} \in E \}$

Proof

Recall $C_X = C_1 \times V_2$
$C_Z = V_1 \times C_2$

Consider some $(c_1, v_2) \in C_X$
$(v_1, c_2) \in C_Z$

What is the overlap of their neighbourhoods? Iff even then they commute.

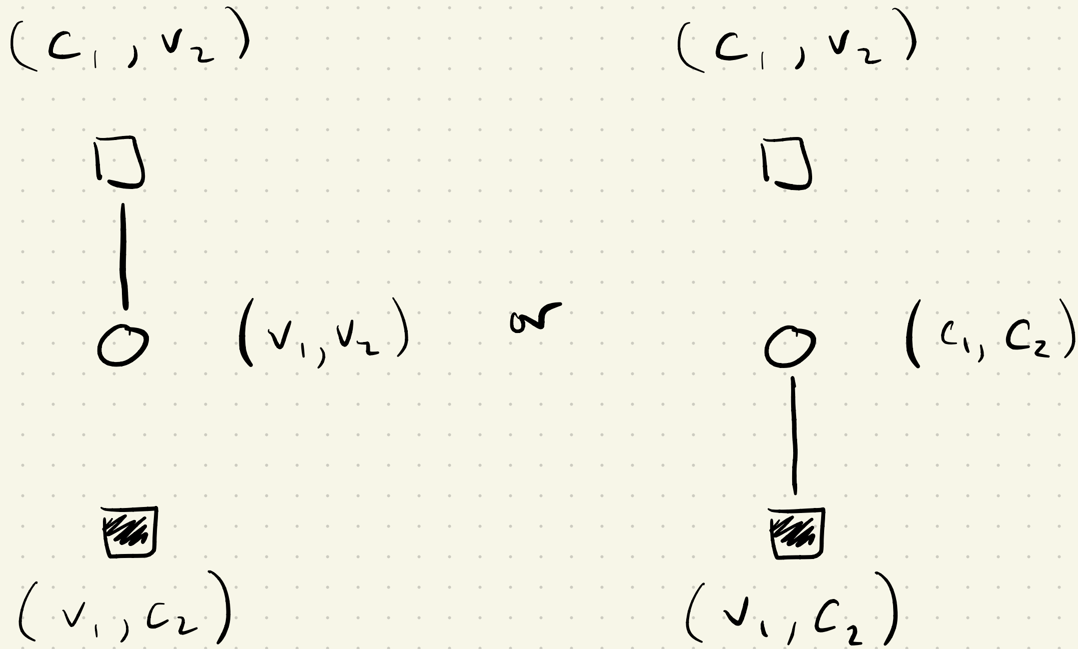
If $\{c_1, v_1\} \notin E_1$ or $\{c_2, v_2\} \notin E_2$

then the overlap is empty.

(Note $v_1 \neq c_1$ and $v_2 \neq c_2$ always.)

Suppose

$\{c_1, v_1\} \in E_1$ $\{c_2, v_2\} \notin E_2$

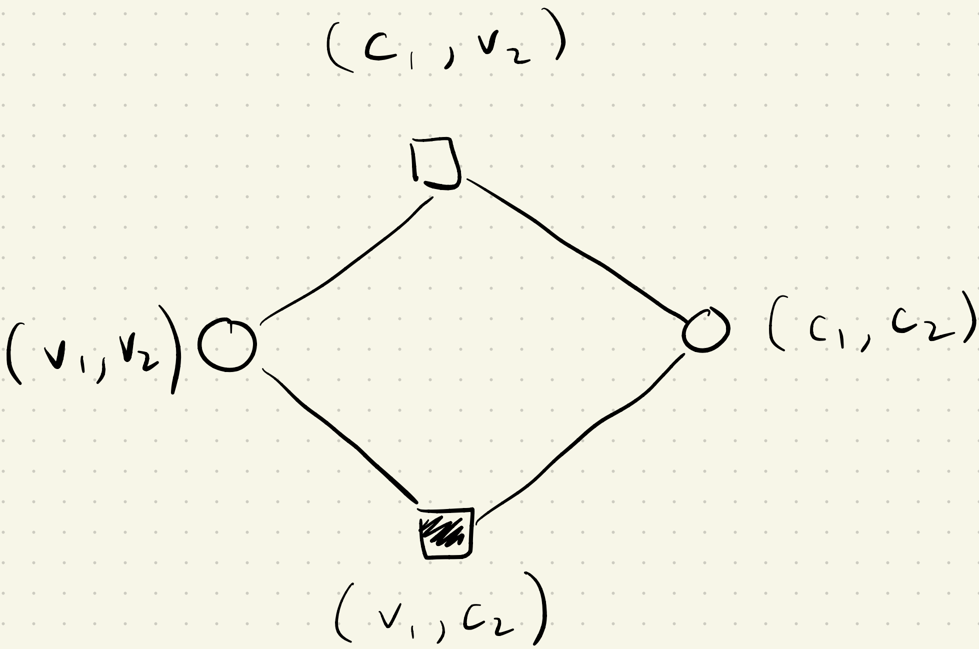


Either way the overlap of their neighbourhoods is empty.

$\{c_1, v_1\} \in E_1$ $\{c_2, v_2\} \notin E_2$ case is the same by symmetry.

Now suppose

$\{c_1, v_1\} \in E_1$ and $\{c_2, v_2\} \in E_2$



These are the only options so their neighbourhoods have even overlap. $\square$

Why "hypergraph" if we are talking about graphs?

The original construction is more general and applies to hypergraphs.

We can also define the HGP in terms of parity-check matrices

Let $H_1 \in M_{m_1 \times n_1}(\mathbb{F}_2)$ and $H_2 \in M_{m_2 \times n_2}(\mathbb{F}_2)$ be two binary parity-check matrices.

Then $HGP(H_1, H_2)$ is the CSS code with

$$\boxed{\begin{aligned} H_X &= \left[\, H_1 \otimes I_{n_2} \;\middle|\; I_{m_1} \otimes H_2^T \,\right] \\ H_Z &= \left[\, I_{n_1} \otimes H_2 \;\middle|\; H_1^T \otimes I_{m_2} \,\right] \end{aligned}}$$

Example

$$H_1 = H_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

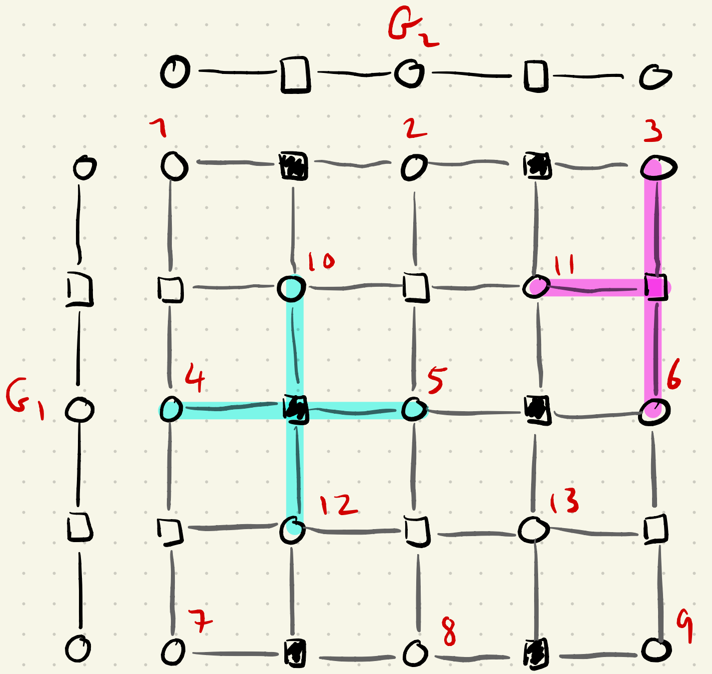
(3-bit rep. code again)

$$n_1 = n_2 = 3, \quad m_1 = m_2 = 2$$

$$H_X = \begin{array}{c} \left[\begin{array}{ccccccccc|cccc} 1&0&0&1&0&0&0&0&0&1&0&0&0 \\ 0&1&0&0&1&0&0&0&0&1&1&0&0 \\ 0&0&1&0&0&1&0&0&0&0&1&0&0 \\ 0&0&0&1&0&0&1&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&1&0&0&0&1&1 \\ 0&0&0&0&0&1&0&0&1&0&0&0&1 \end{array}\right] \\ \begin{array}{ccccccccccccc} 1&2&3&4&5&6&7&8&9&10&11&12&13 \end{array} \end{array}$$

$$H_Z = \left[\begin{array}{ccc ccc ccc|cccc}
1&1&0 & 0&0&0 & 0&0&0 & 1&0&0&0 \\
0&1&1 & 0&0&0 & 0&0&0 & 0&1&0&0 \\
0&0&0 & 1&1&0 & 0&0&0 & 1&0&1&0 \\
0&0&0 & 0&1&1 & 0&0&0 & 0&1&0&1 \\
0&0&0 & 0&0&0 & 1&1&0 & 0&0&1&0 \\
0&0&0 & 0&0&0 & 0&1&1 & 0&0&0&1
\end{array}\right]$$

$$H_X = \left[\begin{array}{ccc ccc ccc|cccc}
1&0&0 & 1&0&0 & 0&0&0 & 1&0&0&0 \\
0&1&0 & 0&1&0 & 0&0&0 & 1&1&0&0 \\
0&0&1 & 0&0&1 & 0&0&0 & 0&1&0&0 \\
0&0&0 & 1&0&0 & 1&0&0 & 0&0&1&0 \\
0&0&0 & 0&1&0 & 0&1&0 & 0&0&1&1 \\
0&0&0 & 0&0&1 & 0&0&1 & 0&0&0&1
\end{array}\right]$$



Stabilizer commutation is easier to show in this picture. We want to show that $H_X H_Z^T = 0$

$$H_X = [\, H_1 \otimes I_{n_2} \mid I_{m_1} \otimes H_2^T \,]$$

$$H_Z = [\, I_{n_1} \otimes H_2 \mid H_1^T \otimes I_{m_2} \,]$$

We have

$$H_X H_Z^T = H_1 \otimes H_2^T + (H_1^T)^T \otimes H_2^T$$

$$= 2 H_1 \otimes H_2^T = 0 \pmod 2$$

where I used the property of the Kronecker product

$$(A \otimes B)(C \otimes D) = (AB) \otimes (CD)$$

Lemma

Let H_1 & H_2 be two parity-check matrices with max row and column weights (r_1, c_1) & (r_2, c_2), respectively.

Then the hypergraph product code has

$$w_X \leq r_1 + c_2$$

$$q_X \leq \max(c_1, r_2)$$

$$w_Z \leq c_1 + r_2$$

$$q_Z \leq \max(r_1, c_2)$$

Proof

$$H_X = [\, H_1 \otimes I_{n_2} \mid I_{m_1} \otimes H_2^T \,]$$

Any row of $H_1 \otimes I_{n_2}$ has weight at most r_1.

Any row of $I_{m_1} \otimes H_2^T$ has row weight at most c_2.

$\Rightarrow w_X \leq r_1 + c_2$

Any column of $H \otimes I_{n_2}$ has weight at most c_1, any column of $I_{m_1} \otimes H_2^T$ has weight at most r_2 $\Rightarrow q_X \leq \max(c_1, r_2)$

$$H_Z = \left[I_{n_1} \otimes H_2 \mid H_1^T \otimes I_{m_2} \right]$$

The same argument applies and so we can conclude

$$w_Z \leq r_2 + c_1$$

$$q_Z \leq \max(c_2, r_1) \qquad \square$$

Example in case it's not obvious

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

$$h \otimes I = \begin{bmatrix} I & 0 & I & I & 0 \end{bmatrix}$$

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

$$I \otimes h = \begin{bmatrix} h & 0 \\ 0 & h \end{bmatrix}$$

This has an important corollary, if $\{H_L\}$ is an LDPC family of parity-check matrices, then $\{HGP(H_L, H_L)\}$ will be a qLDPC family.

Next time we will derive the parameters of HGP codes, namely k (the number of encoded qubits) & d (the code distance).

We will then use these results to prove that qLDPC code families exist w/ parameters $[[n, \Theta(n), \Theta(\sqrt{n})]]$.

References

- "Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$", Tillich & Zémor

arXiv: 0903.0566

Accessible paper!