Lecture III: Hypergraph product codes

Part II

In this lecture we will derive the number of encoded qubits, k, and the code distance, d, of a hypergraph product code.

Def: transpose code

Consider a linear code C with parity-check matrix H.

The transpose code C^T is the linear code with parity check matrix H^T.

Lemma 1

The number of encoded qubits,
or dimension, of $\mathcal{C}^T$ is

$$k^T = k - n + m$$

where n is the number of physical
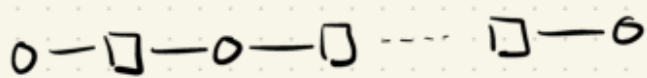qubits in $\mathcal{C}$ and m is the number
of rows in H.

Proof

$$k^T = m - \text{rank}(H^T)$$
$$= m - \text{rank}(H) = m - (n - k)$$
$$= m - n + k$$

$\square$

Note : if H is full rank, i.e.,

$$n - m = k \quad \text{then} \quad k^T = 0.$$

Example : repetition code

Tanner graph
$$H = \begin{bmatrix} 1 & 1 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ 0 & \cdots & 1 & 1 \end{bmatrix}$$

$\circ\!-\!\square\!-\!\circ\!-\!\square \cdots \square\!-\!\circ$

Transpose code just exchanges variable and check nodes in the Tanner graph.

$\square\!-\!\circ\!-\!\square\!-\!\circ \cdots \circ\!-\!\square$

$$H = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & & \vdots \\ \vdots & \vdots & & 1 \\ 0 & 0 & & 1 \end{bmatrix}$$

Def : subgraph product

Let $G_1 = (\{V_1, C_1\}, E_1)$ and $G_2 = (\{V_2, C_2\}, E_2)$ be two Tanner graphs.

Define $G_1 \otimes G_2$ to be the induced subgraph of $G_1 \times G_2$ with variable node set $V_1 \times V_2$ and check node set $C_1 \times V_2 \cup V_1 \times C_2$.

___

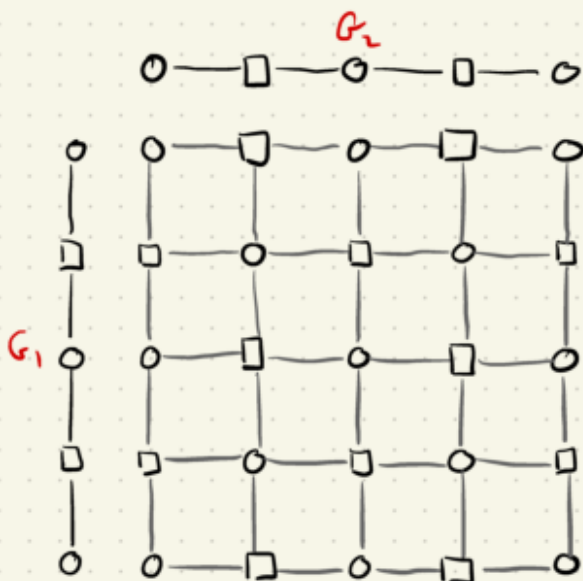We emphasize $G_1 \otimes G_2 \neq G_1 \times G_2$!

Example $G_1 = G_2 = $ ○—▢—○—▢—○

$G_1 \times G_2$

Node set

$V_1 \times V_2 \cup C_1 \times C_2$

$G_1 \otimes G_2$

Node set

$V_1 \times V_2$

⑤
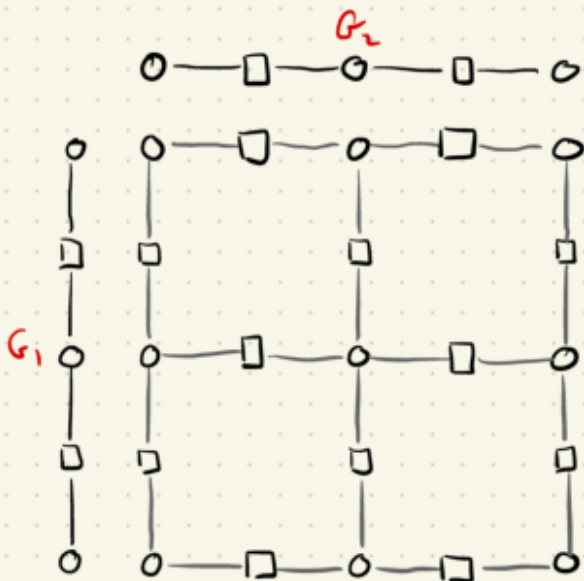
<u>Def</u> : product code

Let ℓ_1 and ℓ_2 be two linear codes w/ parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, respectively.

The <u>product code</u> $\ell_1 \otimes \ell_2$ is the linear code with $n = n_1 n_2$ whose codewords may be viewed as binary matrices of size $n_1 \times n_2$ such that a matrix belongs to $\ell_1 \otimes \ell_2$ iff all its columns belong to ℓ_1 and all its rows belong to ℓ_2.

Example

$e_1 = e_2 = 3$ bit repetition code

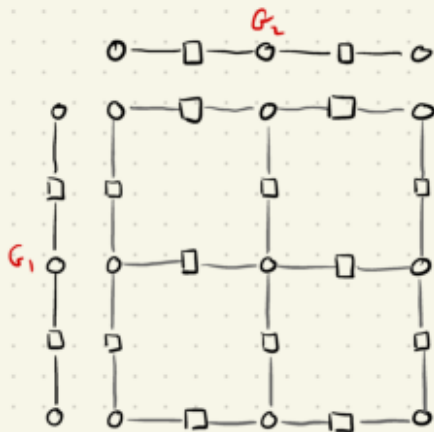$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Code words $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

The corresponding Tanner graph is exactly $G_1 \otimes G_2$, where G_1 is the Tanner graph of e_1 & G_2 is the Tanner graph of e_2.

Lemma 2: The dimension of the product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is $k_1 k_2$ where k_i is the dimension of $\mathcal{C}_i$.

Proof

The codewords of the product code are tensor products

$$u^T \otimes v \quad \text{where} \quad u \in \mathcal{C}_1 \quad \text{and} \quad v \in \mathcal{C}_2.$$

We can reshape this matrix into a vector $u \otimes v$.

Recall that a generator matrix of $\mathcal{C}_i$ is a $k_i \times n_i$ matrix whose rows form a basis for $\mathcal{C}_i$.

From the form of the codewords
above we observe that

$J_1 \otimes J_2$ is a generator matrix

for $\mathcal{C}_1 \otimes \mathcal{C}_2$, where J_i is the

generator matrix of $\mathcal{C}_i$.

$J_1 \otimes J_2$ is a $k_1 k_2 \times n_1 n_2$

matrix, hence the dimension of

the product code is $k_1 k_2$. $\qquad \square$

Lemma 3: Consider the code

$HGP(H_1, H_2)$, where $G_1 = (\{V_1, C_1\}, E_1)$

is the Tanner graph corresponding to

H_1 and $G_2 = (\{V_2, C_2\}, E_2)$ is the Tanner

graph corresponding to H_2.

Then the Tanner graph corresponding

to H_X is $(G_1^T \otimes G_2)^T$ and

the Tanner graph corresponding

to H_Z is $(G_1 \otimes G_2^T)^T$.

Proof:

$G_1^T \otimes G_2$ has node set

$V = C_1 \times V_2$ and check set

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

and there is an edge between

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

if $x = x'$ and $\{y, y'\} \in E_2$

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

$(G_1^T \otimes G_2)^T$ has vertex set

$C = C_1 \times V_2$

$V = V_1 \times V_2 \cup C_1 \times C_2$ and the
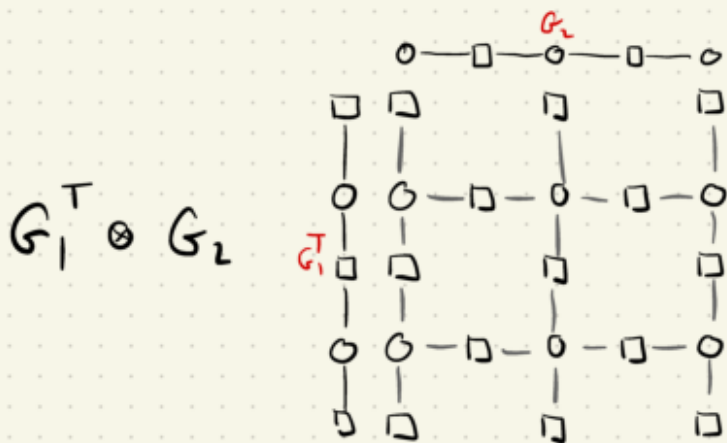 same edge set.

This is exactly the subgraph of

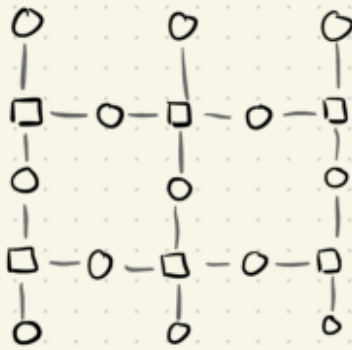$G_1 \times G_2$ induced by $C_1 \times V_2$ ie the

⑪

the Tanner graph of Hx.
The argument for H_z is
analogous.   □

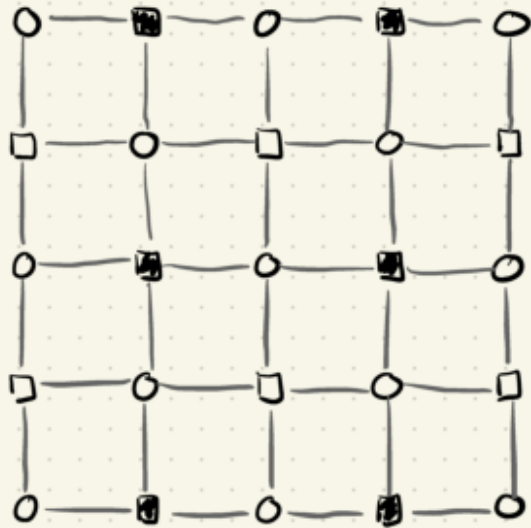**Example** $H_1 = H_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$G_1 = G_2 = $ o—▢—o—▢—o

$G_1^T \otimes G_2$

$$\left(G_1^{\top} \otimes G_2\right)^{\top}$$

$$HGP(H_1, H_2)$$

$$\left(G_1 \otimes G_2^{\top}\right)^{\top}$$
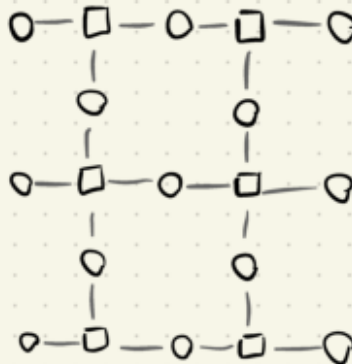
Lemma 4: The number of encoded qubits of the code $HGP(H_1, H_2)$ is $\boxed{k = k_1 k_2 + k_1^T k_2^T}$, where $H_1 \in M_{m_1 \times n_1}(\mathbb{F}_2)$ is the pcm of linear code $\mathcal{C}_1$ w/ parameters $[n_1, k_1, d_1]$ and $H_2 \in M_{m_2 \times n_2}(\mathbb{F}_2)$ is the pcm of linear code $\mathcal{C}_2$ w/ parameters $[n_2, k_2, d_2]$.

Proof:

$$k = n - \text{rank}(H_X) - \text{rank}(H_Z)$$

$$= n - \left(n - \dim(\mathcal{C}_X)\right) - \left(n - \dim(\mathcal{C}_Z)\right)$$

linear
code defined by H_X

(14)

$$k = \dim(\ell_x) + \dim(\ell_z) - n$$

$$\dim(\ell_x) = n_1 n_2 + m_1 m_2 - m_1 n_2 \qquad \text{Lem. 1}$$
$$+ \dim(\ell_x^T)$$
$$= n_1 n_2 + m_1 m_2 - m_1 n_2 \qquad \text{Lem. 3}$$
$$+ \dim(\ell_1^T \otimes \ell_2) \qquad \text{Lem. 2}$$
$$= n_1 n_2 + m_1 m_2 - m_1 n_2 + k_1^T k_2$$

$$\dim(\ell_z) = n_1 n_2 + m_1 m_2 - n_1 m_2 \qquad \text{Lem. 1}$$
$$+ \dim(\ell_z^T)$$
$$= n_1 n_2 + m_1 m_2 - n_1 m_2 + k_1 k_2^T$$

$$k = n_1 n_2 + m_1 m_2 - m_1 n_2 + k_1^T k_2$$
$$+ \cancel{n_1 n_2} + m_1 m_2 - n_1 m_2 + k_1 k_2^T$$
$$- \cancel{n_1 n_2}$$

$$\boxed{15}$$

$$k = n_1 n_2 + m_1 m_2 - m_1 n_2 + k_1^T k_2$$
$$+ m_1 m_2 - n_1 m_2 + k_1 k_2^T$$

$$= n_1 (n_2 - m_2) - m_1 (n_2 - m_2)$$
$$+ m_1 m_2 + k_1^T k_2 + k_1 k_2^T$$

$$= (n_1 - m_1)(n_2 - m_2)$$
$$+ k_1^T k_2 + k_1 k_2^T$$

$$= (k_1 - k_1^T)(k_2 - k_2^T) \quad \text{Lemma 1}$$
$$+ k_1^T k_2 + k_1 k_2^T$$

$$= k_1 k_2 - k_1 k_2^T - k_1^T k_2 + k_1^T k_2^T$$
$$+ k_1^T k_2 + k_1 k_2^T$$

$$= k_1 k_2 + k_1^T k_2^T$$

□ (16)

Lemma 5 : The code distance

of the code $HGP(H_1, H_2)$

$$\boxed{d \geqslant \min(d_1, d_2, d_1^T, d_2^T)}, \quad \text{where}$$

$H_1 \in M_{m_1 \times n_1}(\mathbb{F}_2)$ is the pcm of linear code

$\mathcal{C}_1$ w/ parameters $[n_1, k_1, d_1]$ and

$H_2 \in M_{m_2 \times n_2}(\mathbb{F}_2)$ is the pcm of linear code

$\mathcal{C}_2$ w/ parameters $[n_2, k_2, d_2]$.

Proof

Consider a Pauli Z-type operator

that commutes with the X-type

stabilizes of $HGP(H_1, H_2)$ and

has weight $\leq \min(d_1, d_2^T)$. (17)

Such an operator can be represented by a codeword $z \in \mathcal{C}_X$, where $\mathcal{C}_X$ is the linear code defined by H_X.

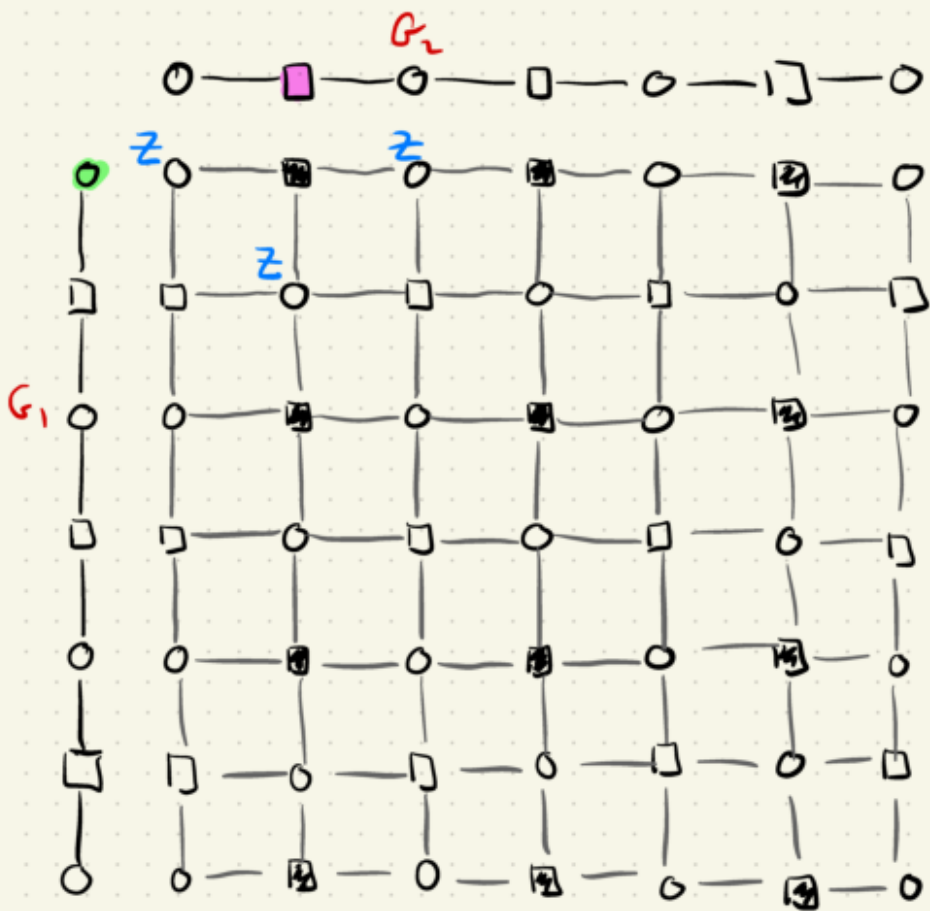Let $\text{supp}(z) \subseteq V_1 \times V_2 \cup C_1 \times C_2$ denote the support of z.

Define

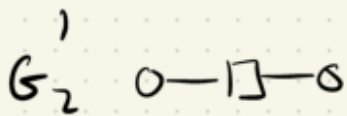$V_1' := \{ v' \in V_1 : \exists v \in V_2, (v', v) \in \text{supp}(z) \}$

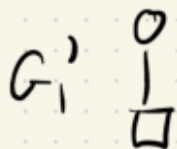$C_2' := \{ c' \in C_2 : \exists c \in C_1, (c', c) \in \text{supp}(z) \}$

Let G_1' be the subgraph of G_1 $\leftarrow$ Tanner graph of H_1 induced by $V_1' \cup C_2$ and let G_2' be the subgraph of G_2 induced by $V_1 \cup C_2'$.

(18)

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

G_1'
G_2'

z

V_1'

C_2'

Let ℓ_i and ℓ_i' be the linear
code defined by the Tanner graphs
G_i a G_i', respectively.

Any code word of ℓ_i' can be
extended to a codeword of ℓ_1
by padding it with zeros.

$(x_0, x_1, \ldots, x_{|v_i'|}) \in \ell_i'$

$(x_0, x_1, \ldots, x_{|v_i'|}, 0, 0, \ldots, 0) \in \ell_1$

We also have $|V_1'| < d_1$ and
so $x_0 = x_1 = \ldots = x_{|v_i'|} = 0$, i.e.

$\dim (\ell_1') = 0$.

Similarly any codeword of $\ell_2'^{T}$
can be extended to a codeword

of ℓ_2^{T} by padding w/ zeros but

the codeword has wt $\leq d_2^{T}$ so $\dim(\ell_2'^{T})=0$.

Let H_i' be the pcm corresponding

to G_i'.

By Lemma 4, the code

$HGP(H_1', H_2')$ has
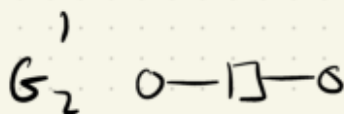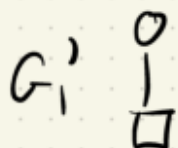
$$k' = k_1' k_2' + k_1'^{T} k_2'^{T} = 0$$

$$\underset{\substack{\uparrow \\ \textcolor{red}{0} \\ \dim(\ell_1')}}{} \qquad \underset{\substack{\uparrow \\ \textcolor{red}{0} \\ \dim(\ell_2'^{T})}}{\phantom{k_1'^{T}k_2'^{T}}}$$

Denote by $\mathfrak{z}'$ the restriction of

$\mathfrak{z}$ to $V_1' \times V_2 \cup C_1 \times C_2'$.

Example

G_1' $\overset{O}{\underset{\square}{|}}$ $\qquad$ G_2' $\ O - \square - O$

$HGP(H_1', H_2')$

G_1' $\qquad$ G_2'

$\mathfrak{z}'$

Denote by $h_z(v_1, c_2)$ the row of H_z corresponding to $v_1 \in V_1$ & $c_2 \in C_2$ and similar for $h'_z(v'_1, c'_2)$ with $v'_1 \in V'_1$ and $c'_2 \in C'_2$.

Note that as $k' = 0$ any operator z' that commutes with the X-type stabilizers of $HGP(H'_1, H'_2)$ must be a Z-type stabilizer of $HGP(H'_1, H'_2)$.

$$z' = \bigoplus_{(v'_1, c'_2) \in J} h'_z(v'_1, c'_2) \quad \text{where}$$

$$J \subseteq V'_1 \times C'_2$$

$$\boxed{23}$$

The set of neighbours of any
$(v_1', c_2') \in V'$ is the same as
in the corresponding $(v_1', c_2') \in V$.

Recall the vertex set of G_1' is $V_1' \cup C_1$
and the vertex set of G_2' is $V_2 \cup C_2'$,
and $v_1' \in V_1'$, $c_2' \in C_2'$.
$\Rightarrow$ The vertex set of $G_1' \times G_2'$
is $V_1' \times V_2 \cup C_1 \times C_2'$.

All the neighbours of (v_1', c_2') in
$G_1 \times G_2$ are contained in
$\{v_1'\} \times V_2 \cup C_1 \times \{c_2'\}$, which
is a subset of the above. (24)

Therefore we also have

$$3 = \bigoplus_{(v_i', c_i') \in J} h_z(v_i', c_i') \quad \text{ie}$$

3 is a Z-type stabilizer.

Therefore any Z-type operator that commutes w/ the X stabilizers w/ weight $\leq \min(d_1, d_2^T)$ must be a Z-type stabilizer. Running the same argument w/ X & Z exchanged allows us to conclude that any X-type operator that commutes w/ the

Z stabilizes and has weight $\leq \min(d_1^T, d_2)$ must be an X-type stabilizer.

Therefore any operator that commutes with all the stabilizers and is not itself a stabilizer has weight $\geq \min(d_1, d_2, d_1^T, d_2^T)$. $\square$

One can also show that
the code distance of

$HGP(H_1, H_2)$

$$d \leq \min(d_1, d_2, d_1^T, d_2^T)$$

and therefore

$$d = \min(d_1, d_2, d_1^T, d_2^T)$$

We can therefore conclude that
the hypergraph product code
HGP (H_1, H_2) has parameters

$$[[\, n_1 n_2 + m_1 m_2 \, , \, k_1 k_2 + k_1^\top k_2^\top \, ,$$
$$\min (\, d_1 \, , \, d_2 \, , \, d_1^\top \, , \, d_2^\top \,) \,]]$$