For $r \le m \le 2^r-1$

$e_{r-1} = 1$

(does this imply $e_0 = 1$ also?)

(yes; proposition is $\bar{e}_1 = \mathrm{rev}(\bar{e}_2)$ and error pattern must have leading 1

$$S_1^{(1)}(m) = \begin{bmatrix} g_{r-1} & 1 & 0 & \cdots & 0 \\ g_{r-2} & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_1 & 0 & \cdots & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}^{m-r} \begin{bmatrix} e_{r-1} \\ e_{r-2} \\ \vdots \\ e_1 \\ e_0 \end{bmatrix}$$

$$S_2^{(1)}(m) = \begin{bmatrix} g_{r-1} & 1 & 0 & \cdots & 0 \\ g_{r-2} & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_1 & 0 & \cdots & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}^{m-r} \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{r-1} \end{bmatrix}$$

$$S_1^{(2)}(m) = \begin{bmatrix} g_1 & 1 & 0 & \cdots & 0 \\ g_2 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_{r-1} & 0 & \cdots & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}^{m-r} \begin{bmatrix} e_{r-1} \\ e_{r-2} \\ \vdots \\ e_1 \\ e_0 \end{bmatrix}$$

$$S_2^{(2)}(m) = \begin{bmatrix} g_1 & 1 & 0 & \cdots & 0 \\ g_2 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_{r-1} & 0 & \cdots & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}^{m-r} \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{r-2} \\ e_{r-1} \end{bmatrix}$$

Proposition: $\exists$ $m < 2^r-1$ such that

$$S_1^{(1)}(m) = S_2^{(1)}(2^r-1) \quad \text{and} \quad S_1^{(2)}(m) = S_2^{(2)}(2^r-1)$$

Hmm... This might be the wrong proposition. But it may be equivalent. If $\exists$ m s.t. $G^m e^{(1)} = e^{(2)}$, the subsequent syndrome patterns will match since $\Rightarrow G^{m+1} e^{(1)} = G e^{(2)}$, $G^{m+2} e^{(1)} = G^2 e^{(2)}$, ...

Then

$$G_1^{m-r}\begin{bmatrix}1\\e_{r-2}\\e_{r-3}\\\vdots\\e_1\\1\end{bmatrix} = G_1^{2^r-1-r}\begin{bmatrix}1\\e_1\\\vdots\\e_{r-2}\\1\end{bmatrix}$$

$\Rightarrow$

$$G_1^{m-r}\underbrace{\begin{bmatrix}1\\e_{r-2}\\e_{r-3}\\\vdots\\e_1\\1\end{bmatrix}}_{e^{(1)}} = G_1^{2^r-1-r}\underbrace{\begin{bmatrix}1\\e_1\\e_2\\\vdots\\e_{r-2}\\1\end{bmatrix}}_{e^{(2)}}$$

$$\Rightarrow \quad G_1^{m}\, e^{(1)} = G_1^{2^r-1}\, e^{(2)}$$

Is there any special property about $G_1^{2^r-1}$?

There should be because code is cyclic

Look at example

$$g(x) = x^3 + x + 1 \quad \Rightarrow \quad g_1 = 1 \quad g_2 = 0 \qquad r = 3$$

$$\begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}^2 = \begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix} = \begin{bmatrix}1&0&1\\1&1&0\\0&1&0\end{bmatrix}$$

$$G^3 = \begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}1&0&1\\1&1&0\\0&1&0\end{bmatrix} = \begin{bmatrix}1&1&0\\1&1&1\\1&0&1\end{bmatrix}$$

$$G^4 = \begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}1&1&0\\1&1&1\\1&0&1\end{bmatrix} = \begin{bmatrix}1&1&1\\0&1&1\\1&1&0\end{bmatrix}$$

$$G^5 = \begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}1&1&1\\0&1&1\\1&1&0\end{bmatrix} = \begin{bmatrix}0&1&1\\0&0&1\\1&1&1\end{bmatrix}$$

$$G^6 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$G^7 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

$$\therefore \; G^{2^r-1} = I$$

$$\therefore \; \boxed{G_1^{\,n} e^{(1)} = e^{(2)}}$$ ← image condition

Now let $g(x) = x^3+x^2+1$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$G^3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\begin{matrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{matrix}$$

$$G^4 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$G^5 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$G^6 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$G^7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \checkmark$$

since G is $r \times r$, it's easy enough to use the computer to verify all the bit-reversed cases (though it may take awhile!). It's tougher to show that the condition is not met for $e^{(1)} \neq \text{rev}(e^{(0)})$. Or is it? The argument is a symmetry argument which ~~a~~ involves both G_1 and G_2.

since
$$e^{(1)} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ e_{r-2} \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ e_{r-3} \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

$$e^{(2)} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ e_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ e_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

does it do any good to expand the "key" equation?

since $e^{(2)} = rev(e^{(1)})$ $\qquad$ rev = row reversal operation

$$rev\left[G_1^m e^{(1)} \right] = e^{(1)}$$

Let $h_{ij} = i,j^{th}$ entry of G_1^m

Then
$$G_1^m e^{(1)} = \begin{bmatrix} h_{00} & h_{01} & \cdots & h_{0,r-1} \\ h_{10} & h_{11} & \cdots & h_{1,r-1} \\ \vdots & & & \\ h_{r-1,0} & h_{r-1,1} & \cdots & h_{r-1,r-1} \end{bmatrix} \begin{bmatrix} 1 \\ e_{r-2} \\ \vdots \\ e_1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} \sum_{i=0}^{r-1} h_{0,i}\, e_i^{(1)} \\ \sum_{i=0}^{r-1} h_{1,i}\, e_i^{(1)} \\ \vdots \\ \sum_{i=0}^{r-1} h_{r-1,i}\, e_i^{(1)} \end{bmatrix}$$

$$\therefore\ rev\left[G_1^m e^{(1)} \right] = \begin{bmatrix} \sum_{i=0}^{r-1} h_{r-1,i}\, e_i^{(1)} \\ \vdots \\ \sum_{i=0}^{r-1} h_{0,i}\, e_i^{(1)} \end{bmatrix} = rev(G^m)\, e^{(1)}$$

$$\Rightarrow\ rev\left(G_1^m \right) e^{(1)} = e^{(1)}$$

$\Rightarrow\ rev(G_1^m) = I \ \Rightarrow m = 2^r - 1$ for general case

- However, this must <u>not</u> be the only solution. This is the trivial case.

General condition requires

$$\sum_{i=0}^{r-1} h_{j,i} \, e_i^{(1)} = e_j^{(1)}$$

This is equivalent to

$$\sum_{\substack{i=0 \\ h_{j,i} \neq 0}}^{r-1} h_{j,i} \, e_i^{(1)} = e_j^{(1)}$$

but this isn't getting me much closer!

Key equation

$$G_1^m e^{(1)} = e^{(2)} \quad \text{and} \quad G_2^m e^{(1)} = e^{(2)}$$

$$\Rightarrow \quad G_1^m e^{(1)} = G_2^{(m)} e^{(1)}$$

$$\Rightarrow \quad \left(G_1^m - G_2^m \right) e^{(1)} = 0$$

$$\Rightarrow \quad G_1^m - G_2^m = 0$$ as one case. (Not <u>necessarily</u> the <u>only</u> case)

$$\Rightarrow \quad G_1^m = G_2^m$$

(This one's independent of $e^{(1)}$ and $e^{(2)}$ so it's not even "the" vital case <u>unless</u> no solution exists for it)

$$\Rightarrow \begin{bmatrix} g_{r-1} & 1 & 0 & \cdots & 0 \\ g_{r-2} & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_1 & 0 & \cdots & \cdots & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}^m = \begin{bmatrix} g_1 & 1 & 0 & \cdots & 0 \\ g_2 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_{r-1} & 0 & \cdots & \cdots & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}^m$$

$$\cancel{G_1^2 = \begin{bmatrix} g_{r-1}^2 + g_{r-2}, & g_{r-1} & g_{r-2} & \cdots & g_1 \\ g_{r-1} g_{r-2} + g_{r-3}, & g_{r-2} & & & \end{bmatrix}}$$

$$G_1^2 = \begin{bmatrix} g_{r-1} & 1 & 0 & \cdots & 0 \\ g_{r-2} & 0 & 1 & 0 \cdots & 0 \\ \vdots & \vdots & 0 & & \\ & & \vdots & & \\ g_1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} g_{r-1} & 1 & 0 & \cdots & 0 \\ g_{r-2} & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ g_1 & 0 & \cdots & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}$$

$$= \begin{bmatrix} g_{r-1}+g_{r-2} & g_{r-1} & 1 & 0 & \cdots & & 0 \\ g_{r-1}g_{r-2}+g_{r-3} & g_{r-2} & 0 & 1 & 0 & \cdots & 0 \\ g_{r-1}g_{r-3}+g_{r-4} & g_{r-3} & 0 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & & & \\ g_{r-1} & 1 & 0 & \cdots & & & 0 \end{bmatrix}$$

well, this get's me nowhere fast!

$$G_1 = \left[\begin{array}{c|c} g_{r-1} & \\ g_{r-2} & I \\ \vdots & \\ \hline g_0 & 0 \end{array}\right] \qquad G_2 = \left[\begin{array}{c|c} g_0 & \\ g_1 & I \\ \vdots & \\ \hline g_{r-1} & 0 \end{array}\right]$$

$$G_1^T = \left[\begin{array}{cc} g_{r-1} \; g_{r-2} & \cdots \; g_0 \\ \hline I & 0 \end{array}\right]$$

hmm ... is there any way to diagonalize G_1 and G_2 ?

$$G_1^m e^{(1)} = e^{(2)} = G_2^m e^{(1)}$$

$$e^{(2)} e^{(2)T} = \begin{bmatrix} 1 \\ e_1 \\ e_2 \\ \vdots \\ e_{r-2} \\ 1 \end{bmatrix} \begin{bmatrix} 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \end{bmatrix} = \begin{bmatrix} 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \\ e_1 & e_1^2 & e_1e_2 & \cdots & e_1e_{r-2} & e_1 \\ e_2 & e_2e_1 & e_2^2 & \cdots & e_2e_{r-2} & e_2 \\ & & \vdots & & & \\ e_{r-2} & e_{r-2}e_1 & \cdots & & e_{r-2}^2 & e_{r-2} \\ 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \end{bmatrix}$$

rank $\leq r-1$

$$e^{(1)} e^{(2)T} = \begin{bmatrix} 1 \\ e_{r-2} \\ \vdots \\ e_2 \\ e_1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \end{bmatrix} = \begin{bmatrix} 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \\ e_{r-2} & e_{r-2}e_1 & \cdots & & e_{r-2}^2 & e_{r-2} \\ \vdots & & & & & \\ e_1 & e_1^2 & e_1e_2 & \cdots & e_1e_{r-2} & e_1 \\ 1 & e_1 & e_2 & \cdots & e_{r-2} & 1 \end{bmatrix} = \mathrm{rev}\left(e^{(2)} e^{(2)T}\right)$$