Ans: Recall $g(x) \circ h(x) = x^n - 1$ and $\deg(h(x)) = k$

$$H = \left.\begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & & 0 \\ & \ddots & & & \ddots & & \\ 0 & & & h_k & \cdots & & h_0 \end{bmatrix}\right\} n-k$$

Basically ① Reverse the order of coefficients

② Put them in a matrix form in the same way as G

proof: $\vec{g}_i$ = the i-th row of G, $i = 0, \cdots, (k-1)$

$\vec{h}_j$ = the j-th row of H. $j = 0, \cdots, (n-k-1)$

$\vec{g}_i \circ \vec{h}_j$ = the $(k-i+j)$-th coordinate of $g(x) \circ h(x)$

☆ $\because (k-i+j) \in [1, n-1]$

$\Rightarrow \vec{g}_i \circ \vec{h}_j = 0$

Corollary: If a code C is cyclic, then its dual code $C^{\perp}$ is also cyclic.

Discussion #2: Revisit Steps 2 & 3.

* For a given p^m, only for some n values we can non-trivially factorize $x^n - 1$, so the choices of n in Step 2 is limited by the $GF(p^m)$ being considered.

* One popular choice is setting $n = (p^m)^a - 1$ for some integer a.
which guarantees $x^n - 1$ is factorizable.

* We sometimes fix n, and then retroactively search for the p^m values that allows for the non-trivial factorization of $x^n - 1$.

* Once we fix a pair of feasible

$(GF(p^m), n)$ pair, we

factorize $(x^n - 1) = f_0(x) \cdot f_1(x) \cdot f_2(x) \cdots f_L(x)$

as a product of irreducible polynomials.

finally, we let

$g(x)$ = the product of a subset of the irreducible factors.

$h(x)$ = the product of the complementary subset of irreducible factors.

E.g. $GF(p^m) = GF(2)$

choose $n = 7$. It turns out we can factorize $x^7 - 1 = x^7 + 1$

$$= (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

There are $2^3 = 8$ possible ways to

choose a subset of the

There are $2=8$ possible ways to choose a subset, and two of them are "trivial" (all or nothing)

$\Rightarrow$ There are 6 possible non-trivial cyclic codes in $GF(2)$ with length $n=7$.

E.g. $g(x) = 1 + x + 0 + x^3.$

$$h(x) = (x+1)(x^3+x^2+1)$$

$$= x^4 + 0x^3 + x^2 + x + 1$$

$$\Rightarrow \quad G = \begin{bmatrix} 1 & 1 & & 1 & & & \\ & 1 & 1 & & 1 & & \\ & & 1 & 1 & & 1 & \\ & & & 1 & 1 & & 1 \end{bmatrix}$$

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

It is a Hamming code parity-check matrix

E.g. $g(x) = (1+x)(1+x^{1}+x^{3}) = 1+x^2+x^3+x^4$

$h(x) = (x^3+x^2+1)$

then we have

$$G = \begin{pmatrix} 1 & & 1 & 1 & 1 & & \\ & 1 & & 1 & 1 & 1 & \\ & & 1 & & 1 & 1 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 1 & & 1 & & & \\ & 1 & 1 & & 1 & & \\ & & 1 & 1 & & 1 & \\ & & & 1 & 1 & & 1 \end{pmatrix}$$

---

* Golay (23, 12) code. A perfect code
* NASA used it in Voyager
* $x^{23}+1 = (x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$
$\cdot (x^{11}+x^9+x^7+x^6+x^5+x+1)$

We can choose either

$$g_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

or $g_2(x) = 1 + x^1 + x^5 + x^6 \; x^7 + x^9 \; x^{11}$

Either of them gives us the Golay code. Note that $g_1(x)$ is the reciprocal of $g_2(x)$.