Goppa Code - Example 1:

$m=4 \quad t=2 \quad n=2^m=2^4=16 \qquad GF(2^4)=GF(16)$

* $k(X)=X^4+X^3+1 \rightarrow$ irreducible, $\mathrm{degree}[k(x)]=4$.

Extension field $GF(2^4) \approx GF(2)[X]/k(X)$

~~Let "a" be a root of k(X). We wish to search~~

We wish to search for a primitive element "a".

Let "a" be a rot of $k(X) \Rightarrow k(a)=0 \Rightarrow a^4+a^3+1=0$

$\Rightarrow a^4=-a^3-1 \equiv a^3+1 \mod (X^4+X^3+1) \Rightarrow \boxed{a^4 \equiv a^3+1}$.

- $\mathrm{order}(a) \mid n-1 = 16-1=15=\mathrm{order}(\mathrm{group}) \Rightarrow \mathrm{order}(a) \mid 15$

$\{\text{divisors of } 15\} = \{1, 3, 5, 15\}$ Check:

- $a^1 \equiv a \mod k(X) \Rightarrow a^1 \not\equiv 1 \mod k(X)$ ✓
- $a^3 \equiv a^3 \mod k(X) \Rightarrow a^3 \not\equiv 1 \mod k(X)$
- $a^5 = a^4 \cdot a = (a^3+1)\cdot a = a^4+a = (a^3+1)+a = a^3+a+1$

$\Rightarrow a^5=a^3+a+1 \Rightarrow a^5 \not\equiv 1 \mod k(X)$

Of course, we always have $a^{n-1}=1 \Rightarrow \boxed{a^{15}=1}$ $\Rightarrow$

$\Rightarrow \mathrm{order}(a)=15=n-1=\mathrm{order}(\mathrm{group})$

$\Rightarrow$ "a" is a primitive element

Therefore, $GF(2^m)^* = \langle a \rangle = \{1, a, a^2, a^3, \dots, \overset{a^{n-2}}{\overset{\parallel}{a^{14}}}\}$

and $GF(2^m) = \{0, 1, a, a^2, a^3, \dots, a^{14}\}$

- Now, using $a^4 \equiv a^3+1$, we represent each element of $GF(2^m)^*$ as a sum of powers of a, up to $a^{m-1}=a^3$:

$a^0=1 \qquad = 1+0a+0a^2+0a^3 = (1,0,0,0)^T = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$

$a^1=a \qquad = 0+1a+0a^2+0a^3 = (0,1,0,0)^T$

$a^2=a^2 \qquad = (0,0,1,0)^T$

$a^3=a^3 \qquad = (0,0,0,1)^T$

$a^4=a^3+1 \quad = 1+0a+0a^2+1a^3 = (1,0,0,1)^T$

$$a^5 = a^4 \cdot a = (a^3+1)\cdot a = a^4+a = a^3+1+a = 1+1a+0a^2+1a^3 = (1,1,0,1)^T$$
$$a^6 = a^5 \cdot a = (a^3+1+a)\cdot a = a^4+a+a^2 = a^3+1+a+a^2 = 1+a+a^2+a^3 = (1,1,1,1)^T$$
$$a^7 = a^6 \cdot a = (1+a+a^2+a^3)\cdot a = a+a^2+a^3+a^4 = a+a^2+a^3+a^3+1 =$$
$$= 1+a+a^2+2a^3 = 1+a+a^2+0a^3 = 1+a+a^2 = (1,1,1,0)^T$$
$$a^8 = a^7 \cdot a = (1+a+a^2)\cdot a = a+a^2+a^3 \equiv (0\ 1\ 1\ 1)^T$$
$$a^9 = a^8 \cdot a = (a+a^2+a^3)\cdot a = a^2+a^3+a^4 = a^2+a^3+a^3+1 = 1+a^2 = (1,0,1,0)^T$$
$$a^{10} = a^9 \cdot a = (1+a^2)\cdot a = a+a^3 = (0\ 1\ 0\ 1)^T$$
$$a^{11} = a^{10} \cdot a = (a+a^3)\cdot a = a^2+a^4 = a^2+a^3+1 = 1+a^2+a^3 = (1\ 0\ 1\ 1)^T$$
$$a^{12} = a^{11} \cdot a = (1+a^2+a^3)\cdot a = a+a^3+a^4 = a+a^3+a^3+1 \equiv 1+a = (1\ 1\ 0\ 0)^T$$
$$a^{13} = a^{12} \cdot a = (1+a)\cdot a = a+a^2 = (0\ 1\ 1\ 0)^T$$
$$a^{14} = a^{13} \cdot a = (a+a^2)\cdot a = a^2+a^3 = (0\ 0\ 1\ 1)^T$$

(and, of course, we can verify that:
$$a^{15} = a^{14} \cdot a = (a^2+a^3)\cdot a = a^3+a^4 = a^3+a^3+1 = 1+2a^3 \equiv 1+0a^3 = (1\ 0\ 0\ 0)^T$$
$$\Longrightarrow a^{15} = 1$$
)

- Also, $0 = (0\ 0\ 0\ 0)^T$

Choose $L = GF(2^m) = \{0,\ 1,\ a,\ a^2,\ a^3,\ \ldots,\ \underset{\overset{\shortparallel}{}}{\overset{a^{n-2}}{a^{14}}}\} =$
$= \{a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ \ldots,\ \underset{a_n}{\underset{\shortparallel}{a_{16}}}\}$

i.e. the code locators are: $a_1 = 0$, $a_2 = 1$, $a_3 = a$, $a_4 = a^2, \ldots, a_{16} = a^{14}$.

Now, choose a monic, binary, separable, irreducible polynomial $g(z)$ of $\text{degree}(g(z)) = t = 2$

↳ For instance, let $\boxed{g(z) = z^2 + z + a}$

$g(a_1) = g(0) = a \neq 0$, $g(a_2) = g(1) = 2+a = a \neq 0$, $g(a_3) = g(a) = a^2+2a = a^2 \neq 0$

$g(a_4) = g(a^2) = a^4+a^2+a = a^3+1+a^2+a \neq 0$

$g(a_5) = g(a^3) = a^6+a^3+a = (1\,1\,1\,1)^T+(0\,0\,0\,1)^T+(0\,1\,0\,0)^T = (1\,0\,1\,0)^T \neq 0 = (0\,0\,0\,0)$

$g(a_6) = g(a^4) = a^8+a^4+a = (0\,1\,1\,1)^T+(1\,0\,0\,1)^T+(0\,1\,0\,0)^T = (1\,0\,1\,0)^T \neq 0$

Note: $\boxed{a^{15}=1} \Rightarrow a^{16}=a^1, \quad a^{17}=a^2, \quad a^{15+v}=a^v \quad (v\geq 1, v\in\mathbb{N})$

$[a^v = a^{v-15}, \ \forall \ v\geq 16, \ v\in\mathbb{N}]$

$g(a_7)= g(a^5) = a^{10}+a^5+a = (0101)^T+(1101)^T+(0100)^T=(1100)^T\neq 0$

$g(a_8)= g(a^6) = a^{12}+a^6+a = (1100)^T+(1111)^T+(0100)^T=(0111)^T\neq 0$

$g(a_9)= g(a^7) = a^{14}+a^7+a = (0011)^T+(1110)^T+(0100)^T=(1001)^T\neq 0$

$g(a_{10})= g(a^8) = \underline{a^{16}}+a^8+a = \underline{a^1}+a^8+a = a^8+2a = a^8 = (0\ 1\ 1\ 1)^T \neq 0$

$g(a_{11})= g(a^9) = \underline{a^{18}}+a^9+a = \underline{a^3}+a^9+a = (0001)^T+(1010)^T+(0100)^T=(1111)^T\neq 0$

$g(a_{12})= g(a^{10}) = a^{20}+a^{10}+a = a^5+a^{10}+a = (1101)^T+(0101)^T+(0100)^T=(1100)^T\neq 0$

$g(a_{13})= g(a^{11}) = a^{22}+a^{11}+a = a^7+a^{11}+a = (1110)^T+(1011)^T+(0100)^T=(0001)^T\neq 0$

$g(a_{14})= g(a^{12}) = a^{24}+a^{12}+a = a^9+a^{12}+a = (1010)^T+(1100)^T+(0100)^T=(0010)^T\neq 0$

$g(a_{15})= g(a^{13}) = a^{26}+a^{13}+a = a^{11}+a^{13}+a = (1011)^T+(0110)^T+(0100)^T=(1001)^T\neq 0$

$g(a_{16})= g(a^{14}) = a^{28}+a^{14}+a = a^{13}+a^{14}+a = (0110)^T+(0011)^T+(0100)^T=(0001)^T\neq 0$

Therefore, $g(z)\neq 0 \quad \forall \quad z\in L=\{a_1, a_2, \dots, a_{16}\}$ ✓

Also, $g(z) = z^2+z+a = 1z^2+1z+a$ $(t=2)$

$= g_2z^2+g_1z+g_0 \Rightarrow \boxed{g_2=1} \ (=g_t)$

$\boxed{g_1=1} \ (=g_{t-1})$

$(g_0=a)$

Now compute the inverses: $g(a_i)^{-1}=\frac{1}{g(a_i)}$ (for $i=1,2,\dots,16$)

$g(a_1)^{-1} = \frac{1}{g(a_1)} = \frac{1}{g(0)} = \frac{1}{a} = a^{-1} = a^{14}$

$g(a_2)^{-1} = \frac{1}{g(a_2)} = \frac{1}{g(1)} = \frac{1}{a} = a^{-1} = a^{14}$

$g(a_3)^{-1} = \frac{1}{g(a_3)} = \frac{1}{g(a)} = \frac{1}{a^2} = a^{-2} = a^{13}$

$\frac{1}{g(a_4)} = \frac{1}{g(a^2)} = \frac{1}{a^3+a^2+a+1} = \frac{1}{(1111)^T} = \frac{1}{a^6} = a^{-6} = a^{-6+15} = a^9$

$\frac{1}{g(a_5)} = \frac{1}{g(a^3)} = \frac{1}{(1010)^T} = \frac{1}{a^9} = a^{-9} = a^6$

$$\frac{1}{g(a_6)} = \frac{1}{g(a^4)} = \frac{1}{(1010)^T} = \frac{1}{a^9} = a^{-9} = a^6$$

$$\frac{1}{g(a_7)} = \frac{1}{g(a^5)} = \frac{1}{(1100)^T} = \frac{1}{a^{12}} = a^{-12} = a^3$$

$$\frac{1}{g(a_8)} = \frac{1}{g(a^6)} = \frac{1}{(0111)^T} = \frac{1}{a^8} = a^{-8} = a^7$$

$$\frac{1}{g(a_9)} = \frac{1}{g(a^7)} = \frac{1}{(1001)^T} = \frac{1}{a^4} = a^{-4} = a^{11}$$

$$\frac{1}{g(a_{10})} = \frac{1}{g(a^8)} = \frac{1}{(0111)^T} = \frac{1}{a^8} = a^{-8} = a^7$$

$$\frac{1}{g(a_{11})} = \frac{1}{g(a^9)} = \frac{1}{(1111)^T} = \frac{1}{a^6} = a^{-6} = a^9$$

$$\frac{1}{g(a_{12})} = \frac{1}{g(a^{10})} = \frac{1}{(1100)^T} = \frac{1}{a^{12}} = a^{-12} = a^3$$

$$\frac{1}{g(a_{13})} = \frac{1}{g(a^{11})} = \frac{1}{(0001)^T} = \frac{1}{a^3} = a^{-3} = a^{12}$$

$$\frac{1}{g(a_{14})} = \frac{1}{g(a^{12})} = \frac{1}{(0010)^T} = \frac{1}{a^2} = a^{-2} = a^{13}$$

$$\frac{1}{g(a_{15})} = \frac{1}{g(a^{13})} = \frac{1}{(1001)^T} = \frac{1}{a^4} = a^{-4} = a^{11}$$

$$\frac{1}{g(a_{16})} = \frac{1}{g(a^{14})} = \frac{1}{(0001)^T} = \frac{1}{a^3} = a^{-3} = a^{12}$$

- $$T = \begin{bmatrix} g_t & 0 & \cdots & 0 \\ g_{t-1} & g_t & & 0 \\ \vdots & & & \vdots \\ g_1 & g_2 & \cdots & g_t \end{bmatrix} \Rightarrow T = \begin{bmatrix} g_2 & 0 \\ g_1 & g_2 \end{bmatrix} \Rightarrow \underbrace{T}_{2\times 2} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

This applies only if we use the 2nd method: $H_a = T \cdot V \cdot D$

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & & & \\ a_1^{t-1} & a_2^{t-1} & \cdots & a_n^{t-1} \end{bmatrix} \xrightarrow[t-1=1]{t=2} V = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_{16} \end{bmatrix}$$

$$\Rightarrow \underbrace{V}_{2\times 16} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & a & a^2 & a^3 & a^4 & \cdots & a^{13} & a^{14} \end{bmatrix}$$

$$X = \begin{pmatrix} \frac{1}{g(a_1)} & \frac{1}{g(a_2)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \frac{a_2}{g(a_2)} & \cdots & \frac{a_n}{g(a_n)} \\ \frac{a_1^2}{g(a_1)} & \frac{a_2^2}{g(a_2)} & \cdots & \frac{a_n^2}{g(a_n)} \\ \vdots & \vdots & & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \frac{a_2^{t-1}}{g(a_2)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}$$

$t \times n$

$\Rightarrow 2 \times 16$

$$\Rightarrow X = \begin{bmatrix} \frac{1}{g(a_1)} & \frac{1}{g(a_2)} & \frac{1}{g(a_3)} & \cdots & \frac{1}{g(a_{16})} \\ a_1 \cdot \frac{1}{g(a_1)} & a_2 \cdot \frac{1}{g(a_2)} & a_3 \cdot \frac{1}{g(a_3)} & \cdots & a_{16} \cdot \frac{1}{g(a_{16})} \end{bmatrix}$$

$$\Rightarrow X = \left[\begin{array}{cccc|c|c|c|c|c|c|c|c|c|c|c|c} a^{14} & a^{14} & a^{13} & a^{9} & a^{6} & a^{6} & a^{3} & a^{7} & a^{11} & a^{7} & a^{9} & a^{3} & a^{12} & a^{13} & a^{11} & a^{12} \\ 0 \cdot a^{14} & 1 \cdot a^{14} & a \cdot a^{13} & a^2 \cdot a^9 & a^3 \cdot a^6 & a^4 \cdot a^6 & a^5 \cdot a^3 & a^6 \cdot a^7 & \underbrace{a^7 \cdot a^{11}}_{a^{18} = a^3} & \underbrace{a^8 \cdot a^7}_{a^{15} = 1} & \underbrace{a^9 \cdot a^9}_{a^{18} = a^3} & a^{10} \cdot a^3 & \underbrace{a^{11} \cdot a^{12}}_{a^{23} = a^8} & \underbrace{a^{12} \cdot a^{13}}_{a^{10}} & * & ** \end{array}\right]$$

$* = a^{13} \cdot a^{11} = a^9$

$** = a^{14} \cdot a^{12} = a^{11}$

$$\Rightarrow X = \begin{bmatrix} a^{14} & a^{14} & a^{13} & a^{9} & a^{6} & a^{6} & a^{3} & a^{7} & a^{11} & a^{7} & a^{9} & a^{3} & a^{12} & a^{13} & a^{11} & a^{12} \\ 0 & a^{14} & a^{14} & a^{11} & a^{9} & a^{10} & a^{8} & a^{13} & a^{3} & 1 & a^{3} & a^{13} & a^{8} & a^{10} & a^{9} & a^{11} \end{bmatrix}$$

$$H_a = T\cdot X = \overset{2\times 2}{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}} \cdot \overset{2\times 16}{\begin{bmatrix} a^{14} & a^{14} & a^{13} & a^{9} & a^{6} & a^{6} & a^{3} & a^{7} & a^{11} & a^{7} & a^{9} & a^{3} & a^{12} & a^{13} & a^{11} & a^{12} \\ 0 & a^{14} & a^{14} & a^{11} & a^{9} & a^{10} & a^{8} & a^{13} & a^{3} & 1 & a^{3} & a^{13} & a^{8} & a^{10} & a^{9} & a^{11} \end{bmatrix}}$$

$$= \begin{bmatrix} a^{14} & a^{14} & a^{13} & a^{9} & a^{6} & a^{6} & a^{3} & a^{7} & a^{11} & a^{7} & a^{9} & a^{3} & a^{12} & a^{13} & a^{11} & a^{12} \\ a^{14} & \underbrace{a^{14}+a^{14}}_{=0}, & \underbrace{a^{13}+a^{14}}_{=a^{10}}, & \underbrace{a^{9}+a^{11}}_{=a^{3}}, & \underbrace{a^{6}+a^{9}}_{=a^{10}}, & \underbrace{a^{6}+a^{10}}_{=a^{9}} & \underbrace{a^{3}+a^{8}}_{=a^{13}}, & \underbrace{a^{7}+a^{13}}_{=1}, & a^{11}+a^{3}, & a^{7}+1, & a^{9}+a^{3}, & a^{3}+a^{13}, & a^{12}+a^{8}, & \underset{*}{a^{13}+a^{10}}, & \underset{**}{a^{11}+a^{9}}, & \underset{***}{a^{12}+a^{11}} \end{bmatrix}$$

<u>where:</u>

$a^{14}+a^{14} = a^2+a^3+a^2+a^3 = 2a^2+2a^3 = 0$

$a^{13}+a^{14}$: $\begin{pmatrix}0\\1\\1\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=a^{10}$

$a^{6}+a^{9}$: $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=a^{10}$

$a^{7}+a^{13}$: $\begin{pmatrix}1\\1\\1\\0\end{pmatrix}+\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=1$

$a^{7}+1$: $\begin{pmatrix}1\\1\\1\\0\end{pmatrix}+\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=a^{13}$

$a^{12}+a^{8}$: $\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}=a^{11}$

$a^3+a^{13}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}+\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=a^8$

$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}+\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=a^{13}$

$a^9+a^3=\begin{pmatrix}1\\0\\1\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}=a^{11}$

$a^9+a^{11}=(1\ 0\ 1\ 0)^T+(1\ 0\ 1\ 1)^T=(0\ 0\ 0\ 1)^T=a^3$

$a^6+a^{10}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=(1\ 0\ 1\ 0)^T=a^9$

$a^{11}+a^3=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=a^9$

$*\ a^{13}+a^{10}=(0\ 1\ 1\ 0)^T+(0\ 1\ 0\ 1)^T=(0\ 0\ 1\ 1)^T=a^{14}$

$**\ a^{11}+a^{9}=(1\ 0\ 1\ 1)^T+(1\ 0\ 1\ 0)^T=(0\ 0\ 0\ 1)^T=a^{3}$

$***\ a^{12}+a^{11}=(1\ 1\ 0\ 0)^T+(1\ 0\ 1\ 1)^T=(0\ 1\ 1\ 1)^T=a^{8}$

$$\Rightarrow H_a = \begin{bmatrix} a^{14} & a^{14} & a^{13} & a^{9} & a^{6} & a^{6} & a^{3} & a^{7} & a^{11} & a^{7} & a^{9} & a^{3} & a^{12} & a^{13} & a^{11} & a^{12} \\ a^{14} & 0 & a^{10} & a^{3} & a^{10} & a^{9} & a^{13} & 1 & a^{9} & a^{13} & a^{11} & a^{8} & a^{11} & a^{4} & a^{3} & a^{8} \end{bmatrix}$$

2×16

Also, by replacing a^{14} with $a^{14} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$, $a^{13} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ etc, we get :

$$H_b = \left[\begin{array}{cccc} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} & \cdots\cdots \\ \hline \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \cdots\cdots & \text{e.t.c.} \end{array} \right]$$

$$\Rightarrow H_b = \left[\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right]$$

8×16

$(m \cdot t) \times n$

$\begin{bmatrix} a^7 \\ a^{13} \end{bmatrix}$