BCH codes
(t bit error correction possibility)

Information Theory and Coding – Video Lecture Series (For B.Tech, MCA, M.Tech)

BCH-CODES

BCH Codes are the Subset of Cyclic Codes whose generator polynomials have roots Carefully specified so as to give good error correcting Capability.

[IMP:- Each BCH code is a 't' error correcting code in that it can detect and correct upto 't' random errors per code word.]

Parameters of BCH CODES:- $(m \geq 3)$

(i) BLOCK Length $n = 2^m - 1$

(ii) No. of message bits : $k \geq n - mt$

(iii) Minimum distance : $d_{min} \geq 2t + 1$

Degree, r of $(n, k) = n - k$

$k = 2^m - 1 - r$

$\boxed{k = n - r}$

Generator Polynomial :-

$$g(x) = LCM\left[m_1(x), m_2(x), \ldots\ldots m_{2t}(x)\right]$$

Double Error Correcting Code.

$t = 2$

$$g(x) = LCM\left[m_1(x), m_2(x), m_3(x), m_4(x)\right]$$

Information Theory and Coding – Video Lecture Series (For B.Tech, MCA, M.Tech)

BCH CODES

Example:- Construct a triple Error-Correcting ... $m_{2t}(x)$ BCH code with blocklength $n=31$ over $GF(2^5)$.

$t=3$

$$g(x) = LCM\left[m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)\right]$$

$$g(x) = LCM\left[m_1(x), m_3(x), m_5(x)\right]$$

In $GF(2^5)$,

$m_1(x) = x^5 + x^2 + 1$

$m_2(x) = m_1(x)$

$m_3(x) = x^5 + x^4 + x^3 + x^2 + 1$

$m_4(x) = m_2(x)$

$m_5(x) = x^5 + x^4 + x^2 + x + 1$

$m_6(x) = m_3(x)$.

Information Theory and Coding – Video Lecture Series (For B.Tech, MCA, M.Tech)

BCH CODES

Example:- Construct a triple Error-Correcting ... $m_{2t}(x)$ BCH code with blocklength $n=31$ over $GF(2^5)$.

$t=3$

$g(x) = LCM[m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)]$

$g(x) = LCM[m_1(x), m_3(x), m_5(x)]$

In $GF(2^5)$, $m_1(x) = x^5 + x^2 + 1$

$m_2(x) = m_1(x)$

$m_3(x) = x^5 + x^4 + x^3 + x^2 + 1$

$m_4(x) = m_2(x)$

$m_5(x) = x^5 + x^4 + x^2 + x + 1$

$m_6(x) = m_3(x)$.

$g(x) = [m_1(x) . m_3(x) . m_5(x)]$

$g(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1.$

Info. Length $(k) = n - mt$

$n = 2^m - 1$

$31 = 2^m - 1$

or $2^m = 32$, $m = 5$

$= 31 - 5 \times 3$

$= 31 - 15$, $k = 16$

Information Theory and Coding – Video Lecture Series (For B.Tech, MCA, M.Tech)

BCH CODES

Example:- Construct a triple Error-Correcting ... $m_{2t}(x)$ } (n, k)

BCH code with blocklength $n=31$ over $GF(2^5)$. } $(31, 16)$ triple-error Correcting

$t = 3$

$g(x) = LCM[m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)]$

In $GF(2^5)$, $m_1(x) = x^5 + x^2 + 1$

$m_2(x) = m_1(x)$

$m_3(x) = x^5 + x^4 + x^3 + x^2 + 1$

$m_4(x) = m_2(x)$

$m_5(x) = x^5 + x^4 + x^2 + x + 1$

$m_6(x) = m_3(x)$.

$g(x) = LCM[m_1(x), m_3(x), m_5(x)]$

$g(x) = [m_1(x) \cdot m_3(x) \cdot m_5(x)]$

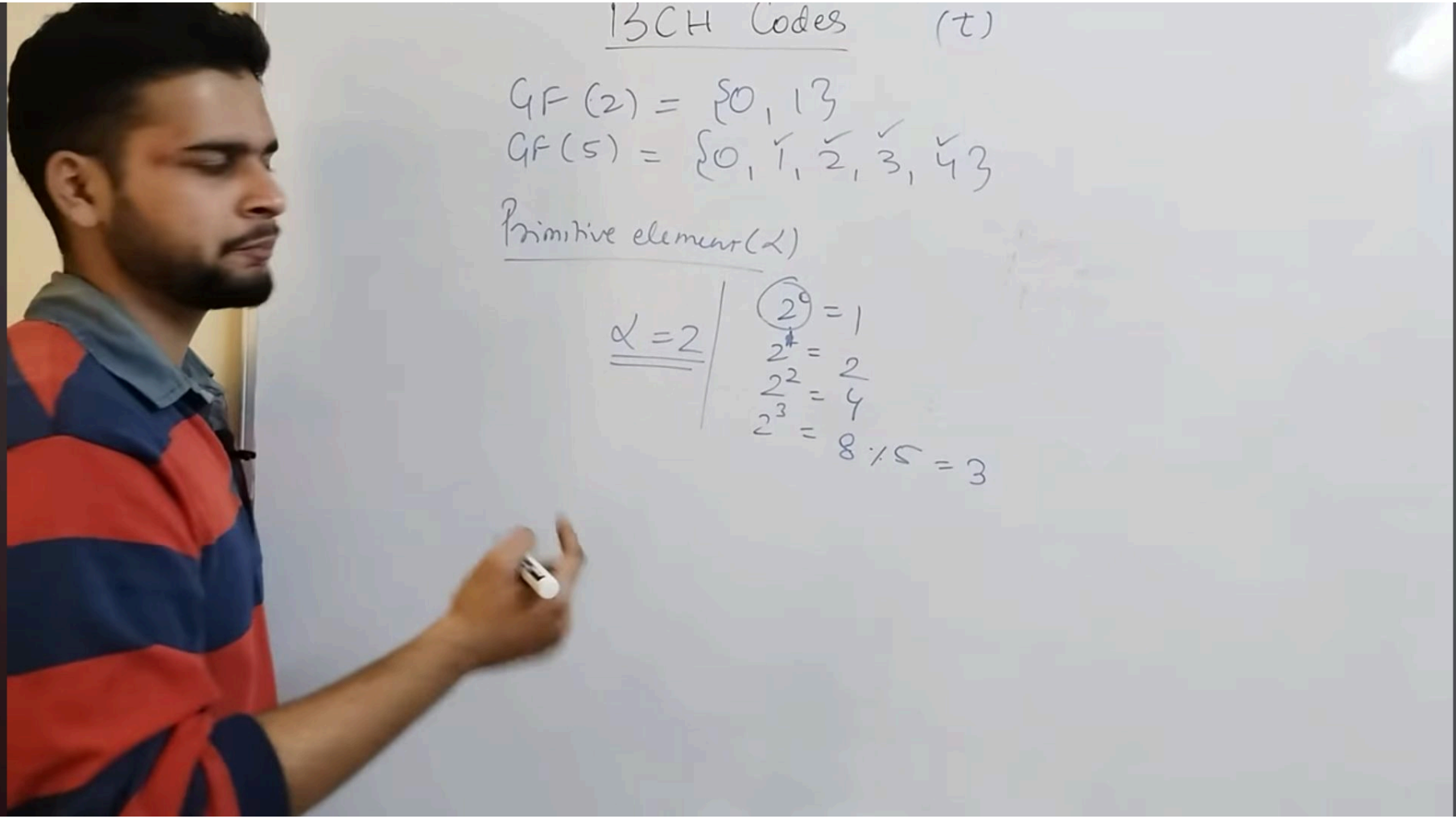
$g(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 +$

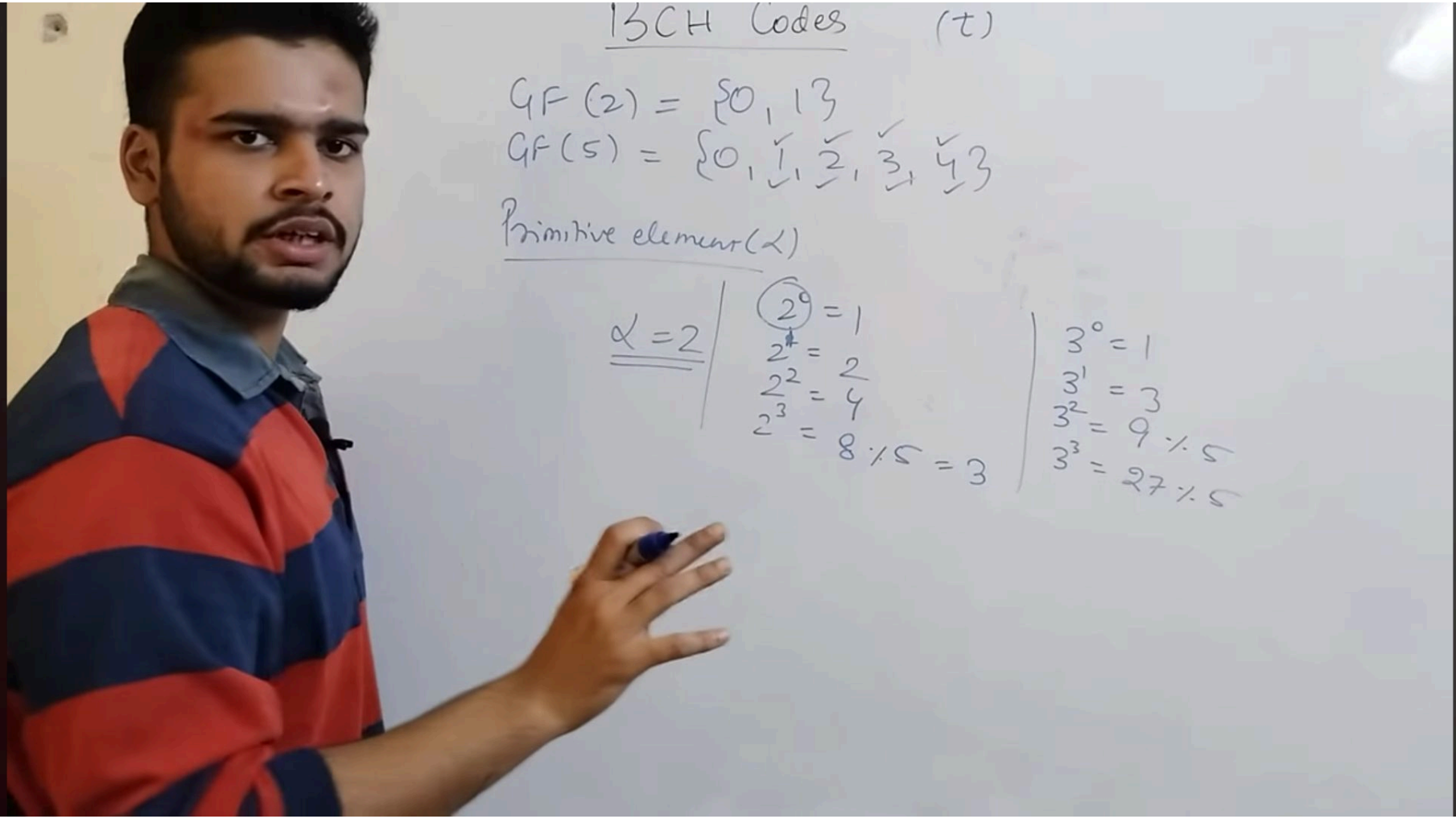
Info. Length $(k) = n - mt$

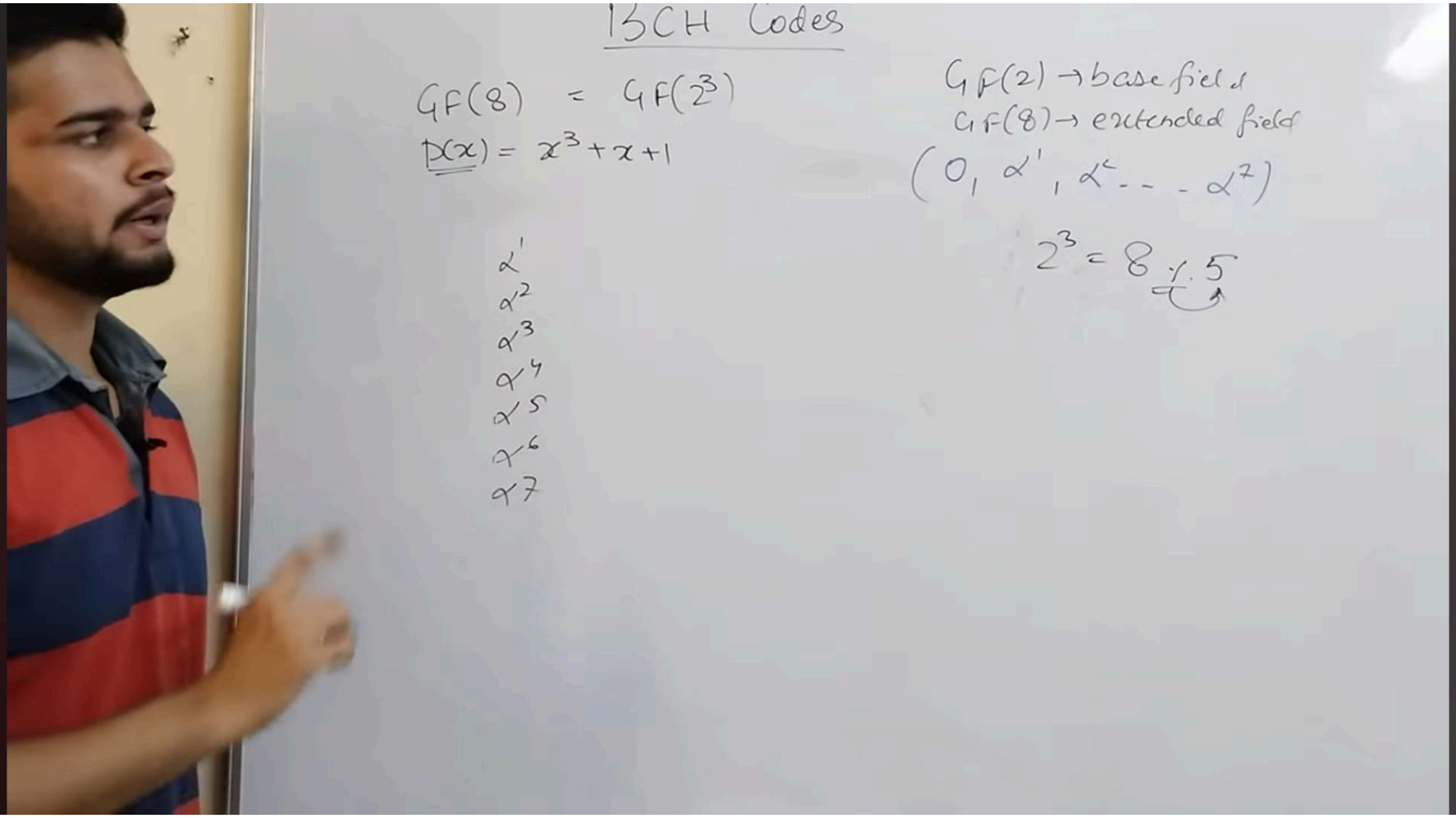
$n = 2^m - 1$ $= 31 - 5 \times 3$

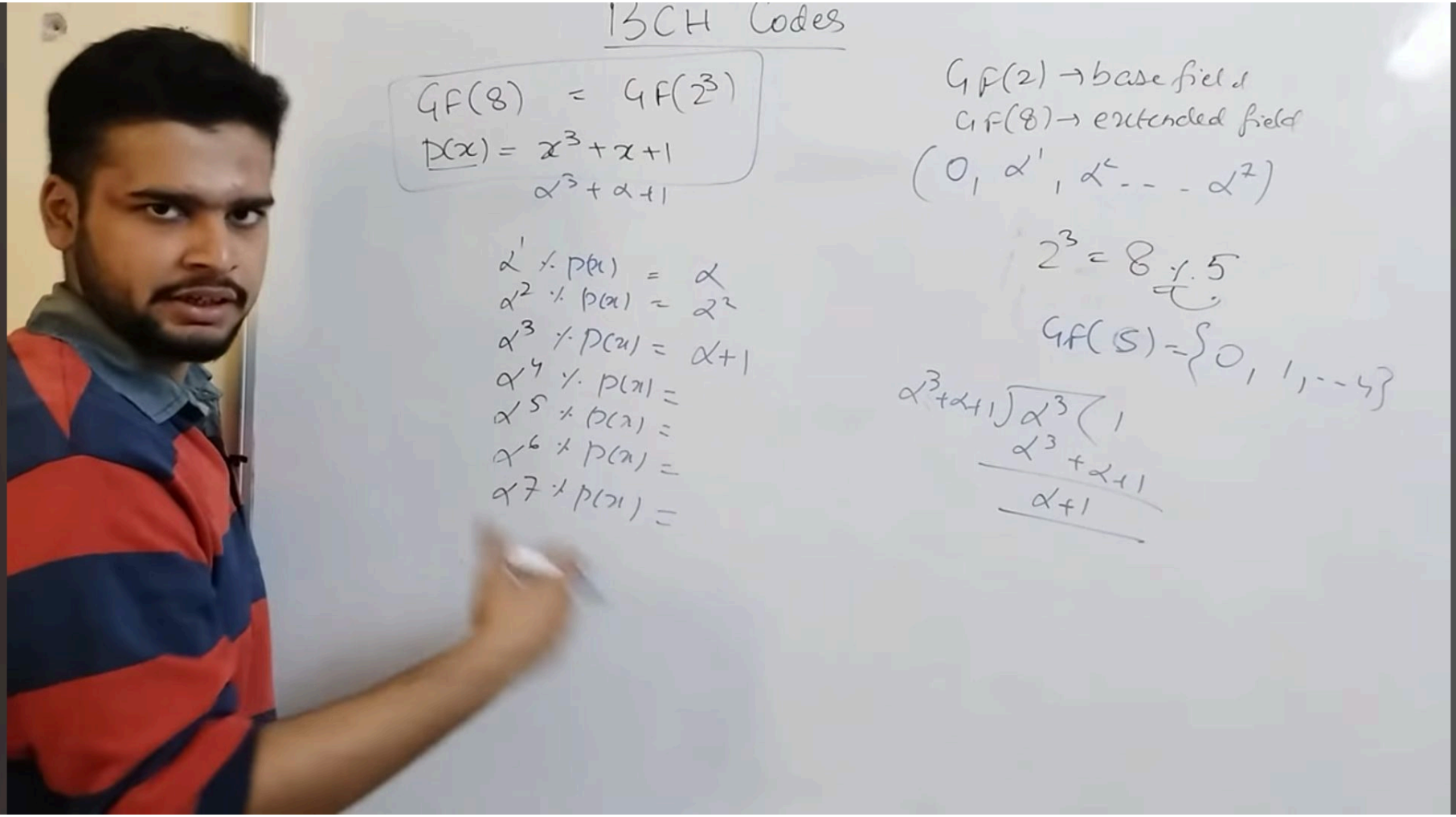
$31 = 2^m - 1$ $= 31 - 15$, $k = 16$

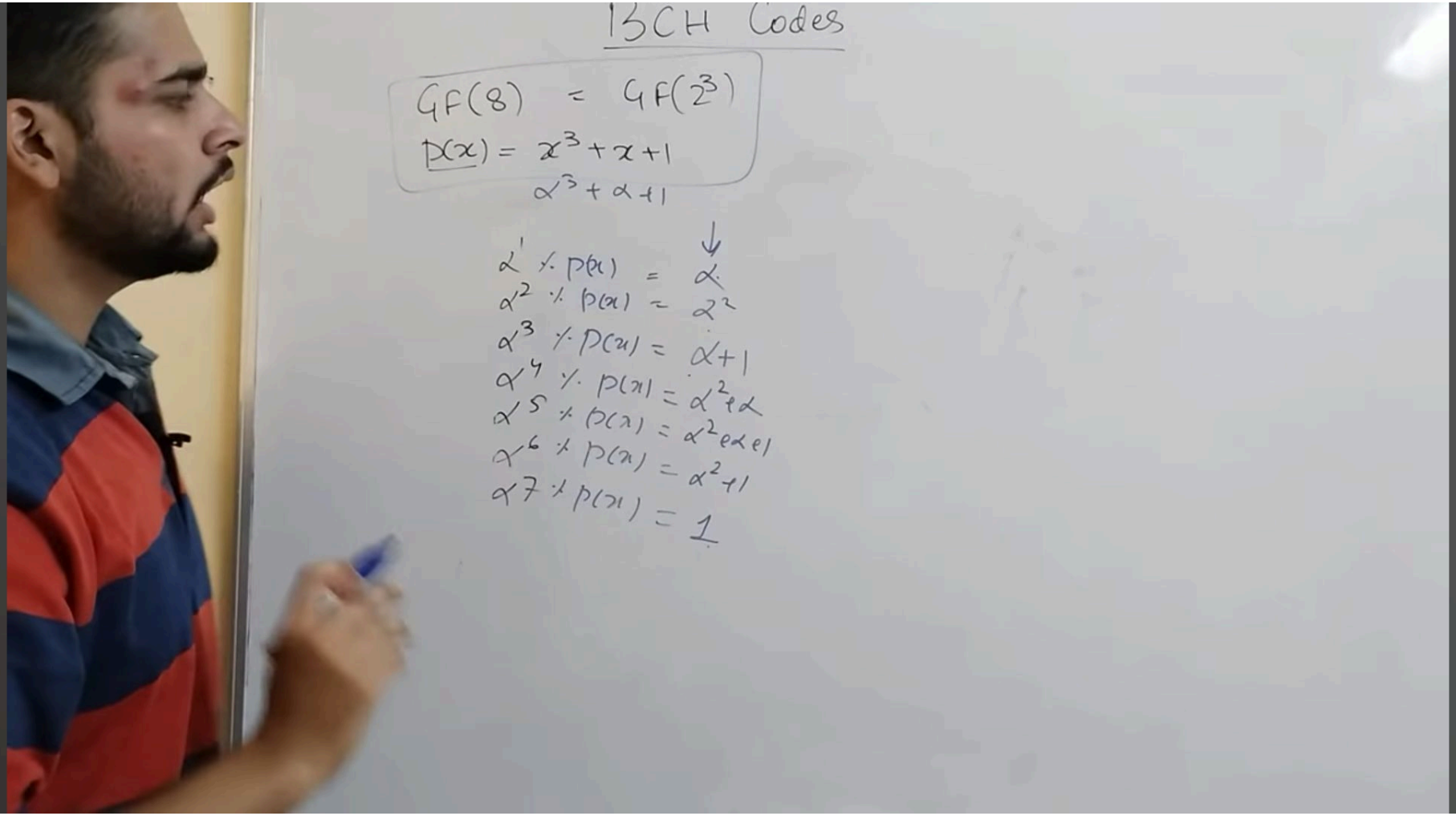
or $2^m = 32$, $m = 5$

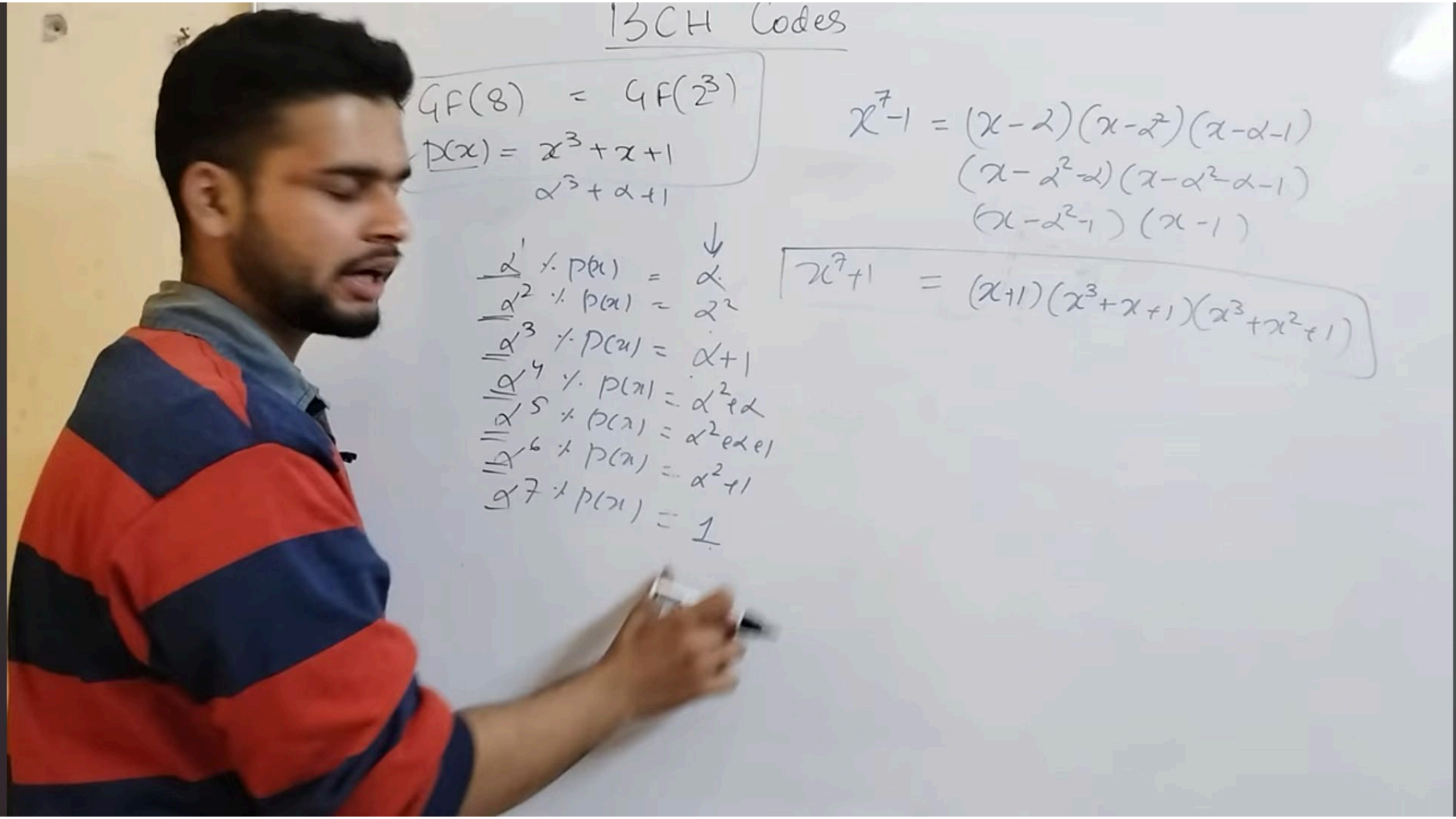

BCH Codes (t)
GF(2) = {0, 1}
GF(5) = {0, 1, 2, 3, 4}
Primitive element(α)
α = 2
$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8 \% 5 = 3$

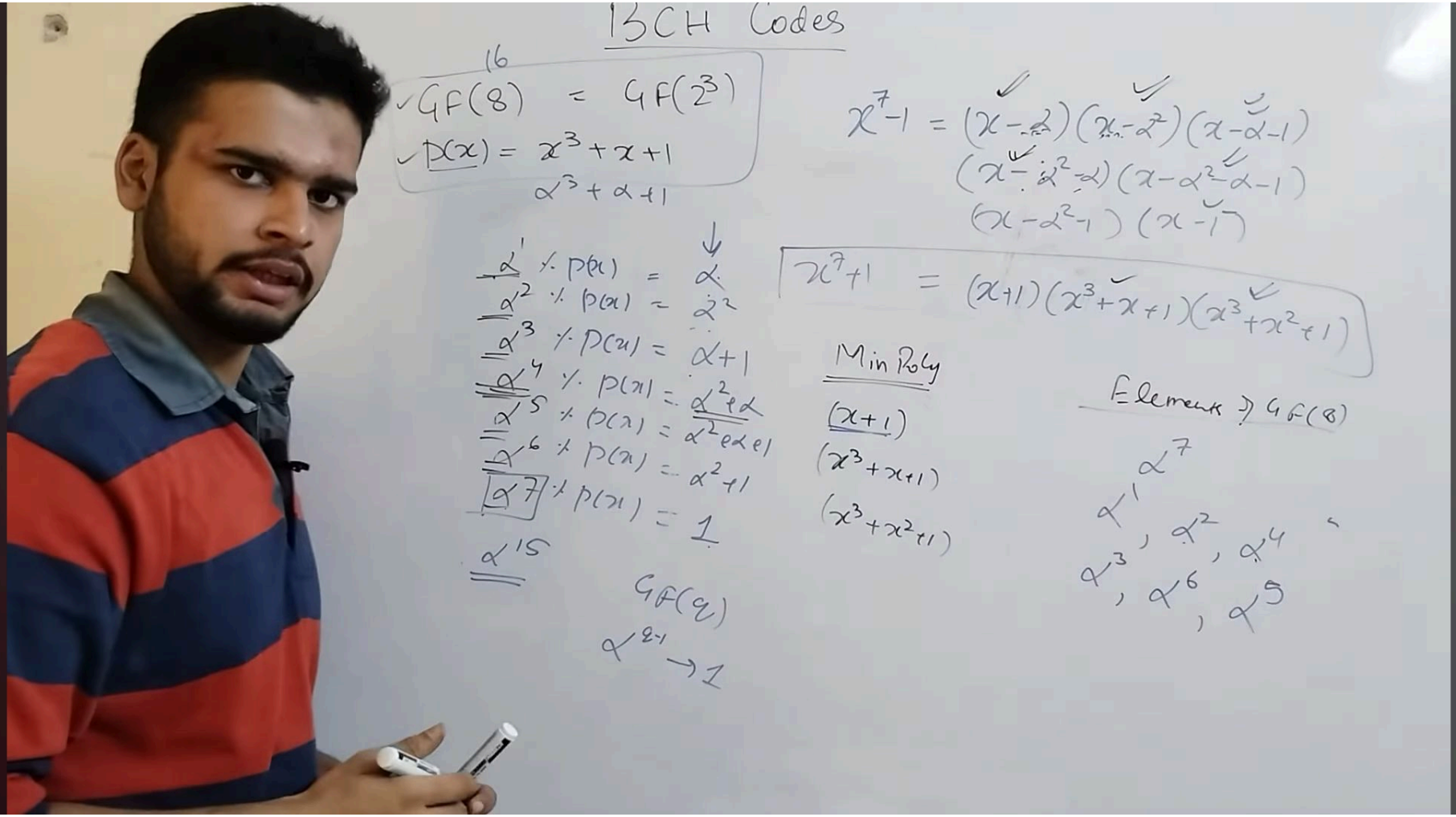

BCH Codes (t)
GF(2) = {0, 1}
GF(5) = {0, 1, 2, 3, 4}
Primitive element(α)
α = 2
2^0 = 1
2^1 = 2
2^2 = 4
2^3 = 8 % 5 = 3
3^0 = 1
3^1 = 3
3^2 = 9 % 5
3^3 = 27 % 5

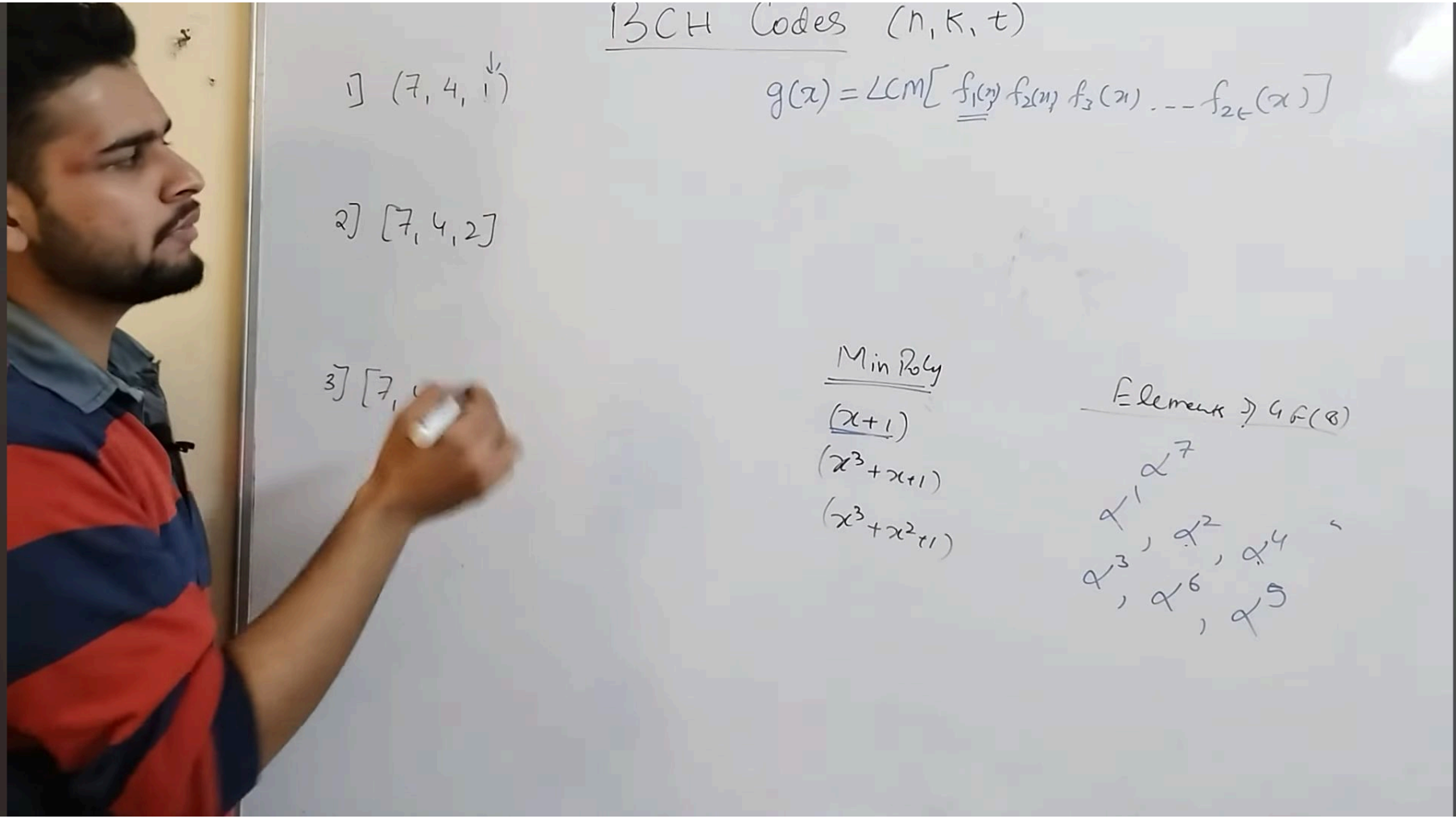

BCH Codes
GF(8) = GF(2^3)
p(x) = x^3 + x + 1
α^1
α^2
α^3
α^4
α^5
α^6
α^7
GF(2) → base field
GF(8) → extended field
(0, α^1, α^2 - - - α^7)
2^3 = 8 i.e. 5


BCH Codes
GF(8) = GF(2^3)
p(x) = x^3 + x + 1
α^3 + α + 1
α^1 % p(x) = α
α^2 % p(x) = α^2
α^3 % p(x) = α + 1
α^4 % p(x) =
α^5 % p(x) =
α^6 % p(x) =
α^7 % p(x) =
GF(2) → base field
GF(8) → extended field
(0, α^1, α^2 - - - α^7)
2^3 = 8 ∴ 5
GF(5) = {0, 1, - - 4}
α^3 + α + 1) α^3 (1
α^3 + α + 1
α + 1


BCH Codes
GF(8) = GF(2^3)
p(x) = x^3 + x + 1
α^3 + α + 1
α^1 % p(x) = α
α^2 % p(x) = α^2
α^3 % p(x) = α + 1
α^4 % p(x) = α^2 + α
α^5 % p(x) = α^2 + α + 1
α^6 % p(x) = α^2 + 1
α^7 % p(x) = 1


BCH Codes
GF(8) = GF(2^3)
p(x) = x^3 + x + 1
α^3 + α + 1
α^1 % p(x) = α
α^2 % p(x) = α^2
α^3 % p(x) = α + 1
α^4 % p(x) = α^2 + α
α^5 % p(x) = α^2 + α + 1
α^6 % p(x) = α^2 + 1
α^7 % p(x) = 1
x^7 - 1 = (x - α)(x - α^2)(x - α - 1)
(x - α^2 - α)(x - α^2 - α - 1)
(x - α^2 - 1)(x - 1)
x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)


BCH Codes
GF(8) = GF(2^3)
p(x) = x^3 + x + 1
α^3 + α + 1
α^1 % p(x) = α
α^2 % p(x) = α^2
α^3 % p(x) = α + 1
α^4 % p(x) = α^2 + α
α^5 % p(x) = α^2 + α + 1
α^6 % p(x) = α^2 + 1
α^7 % p(x) = 1
α^15
GF(q)
α^(q-1) → 1
x^7 - 1 = (x - α)(x - α^2)(x - α^4)(x - α^3)(x - α^5)(x - α^6)(x - α^7)
(x - α^7)(x - α^14)(x - α^28)(x - α^56)(x - 1)
x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)
Min Poly
(x + 1)
(x^3 + x + 1)
(x^3 + x^2 + 1)
Element → GF(8)
α^7
α^1, α^2, α^4
α^3, α^6, α^5


BCH Codes (n, K, t)
1] (7, 4, 1)
g(x) = LCM[f1(x) f2(x) f3(x) ... f2t(x)]
2] [7, 4, 2]
3] [7,
Min Poly
(x+1)
(x^3+x+1)
(x^3+x^2+1)
Element => GF(8)
α^7
α^1
α^2
α^4
α^3
α^6
α^5

BCH Codes (n, K, t)

1] $(7, 4, 1)$

$g(x) = LCM[f_1(x)\, f_2(x)\, f_3(x) \ldots f_{2t}(x)]$

$g(x) = LCM[f_1(x), f_2(x)] = x^3 + x + 1$

2] $[7, 4, 2]$

3] $[7, 4, 3]$

Min Poly

$(x+1)$

$(x^3 + x + 1)$

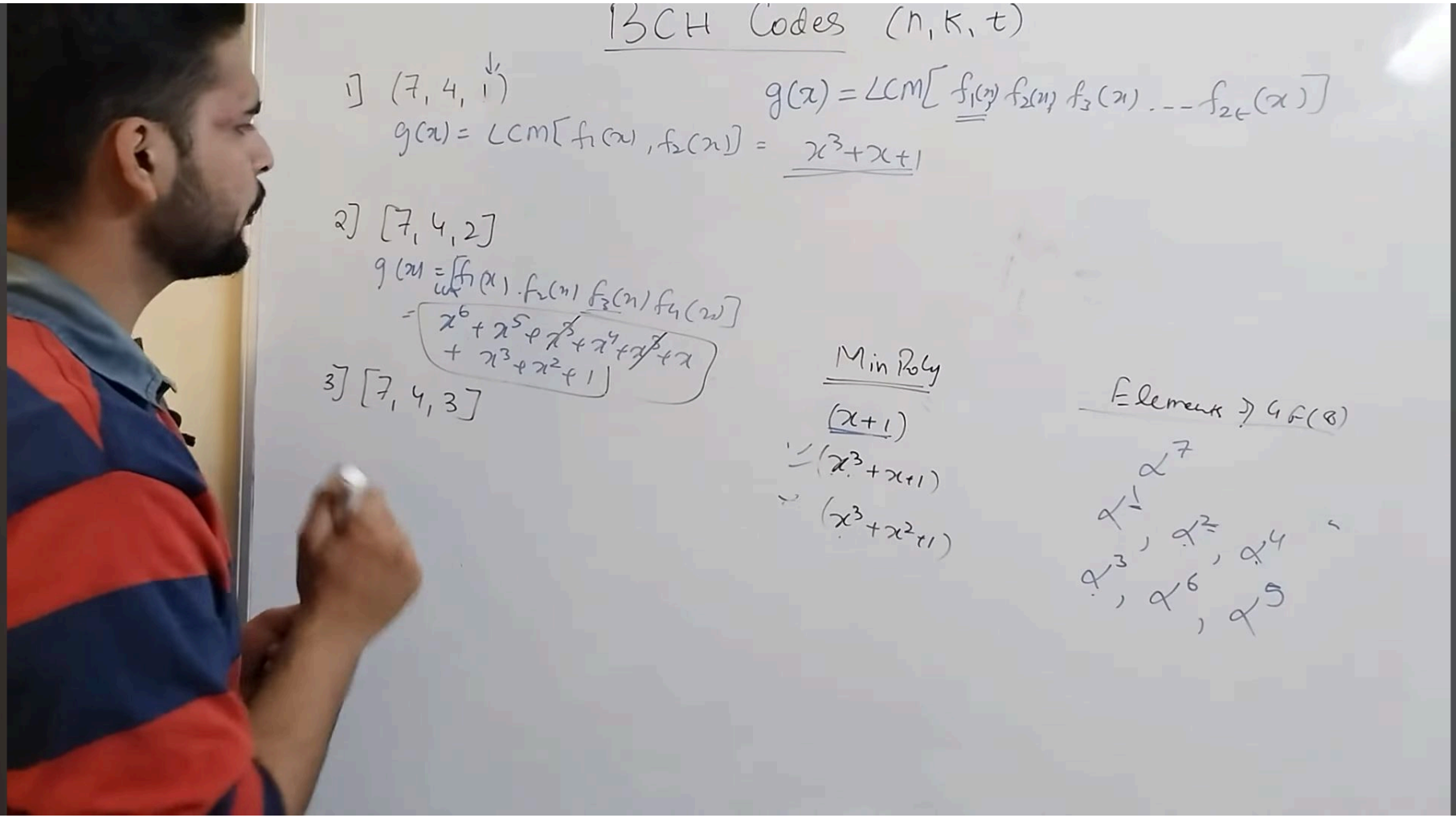
$(x^3 + x^2 + 1)$

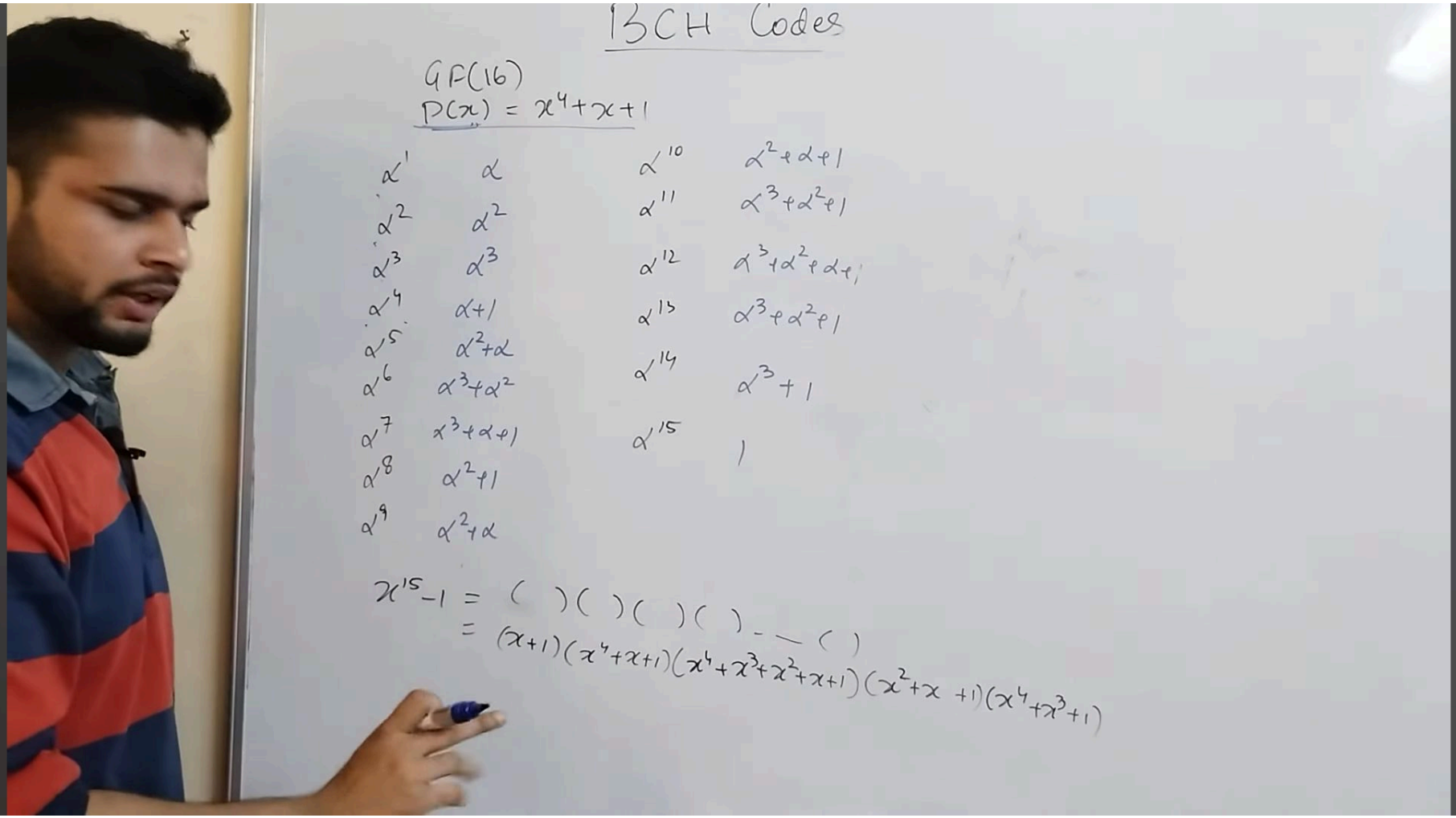
Element $\Rightarrow$ GF(8)

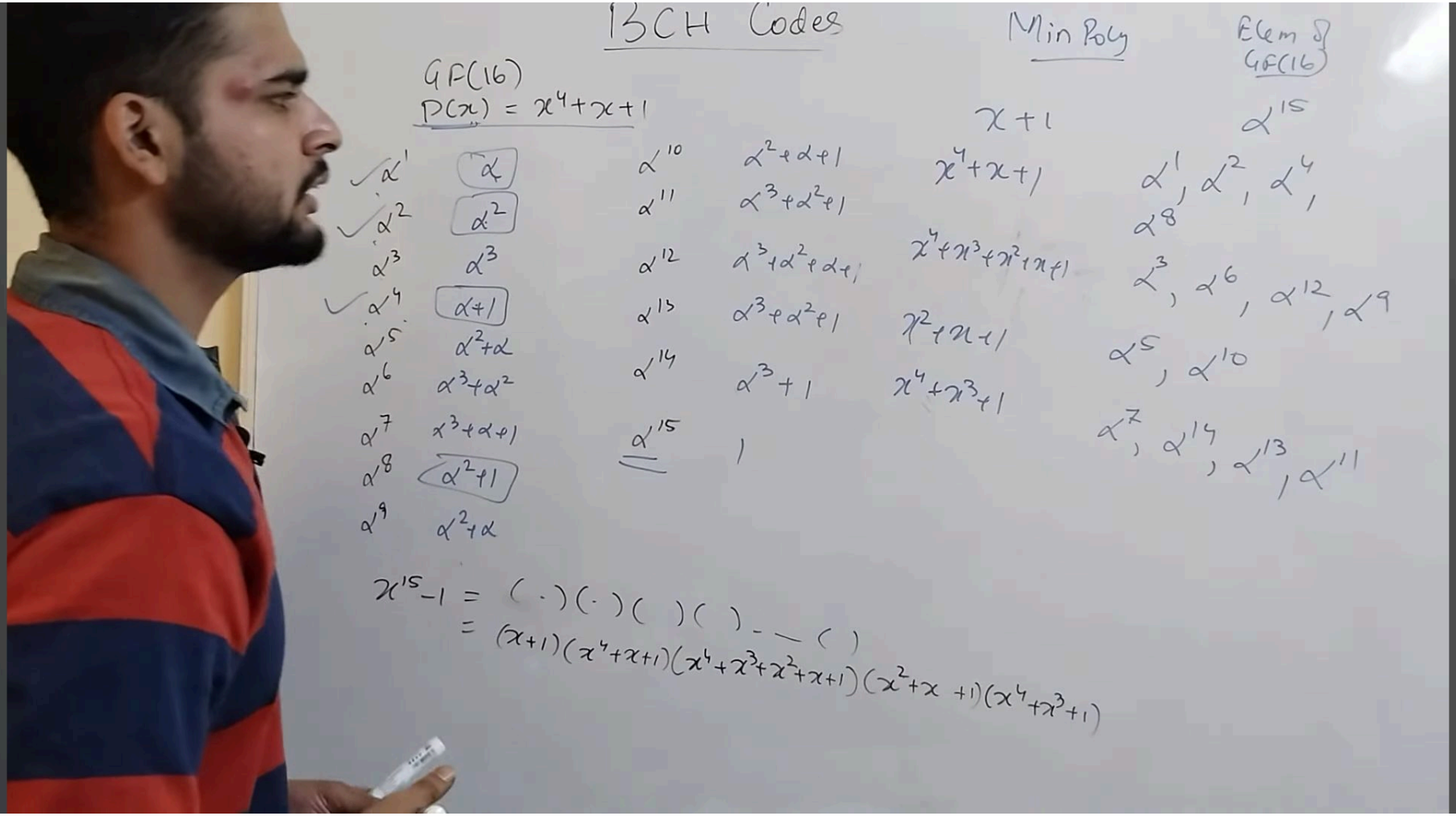
α^7

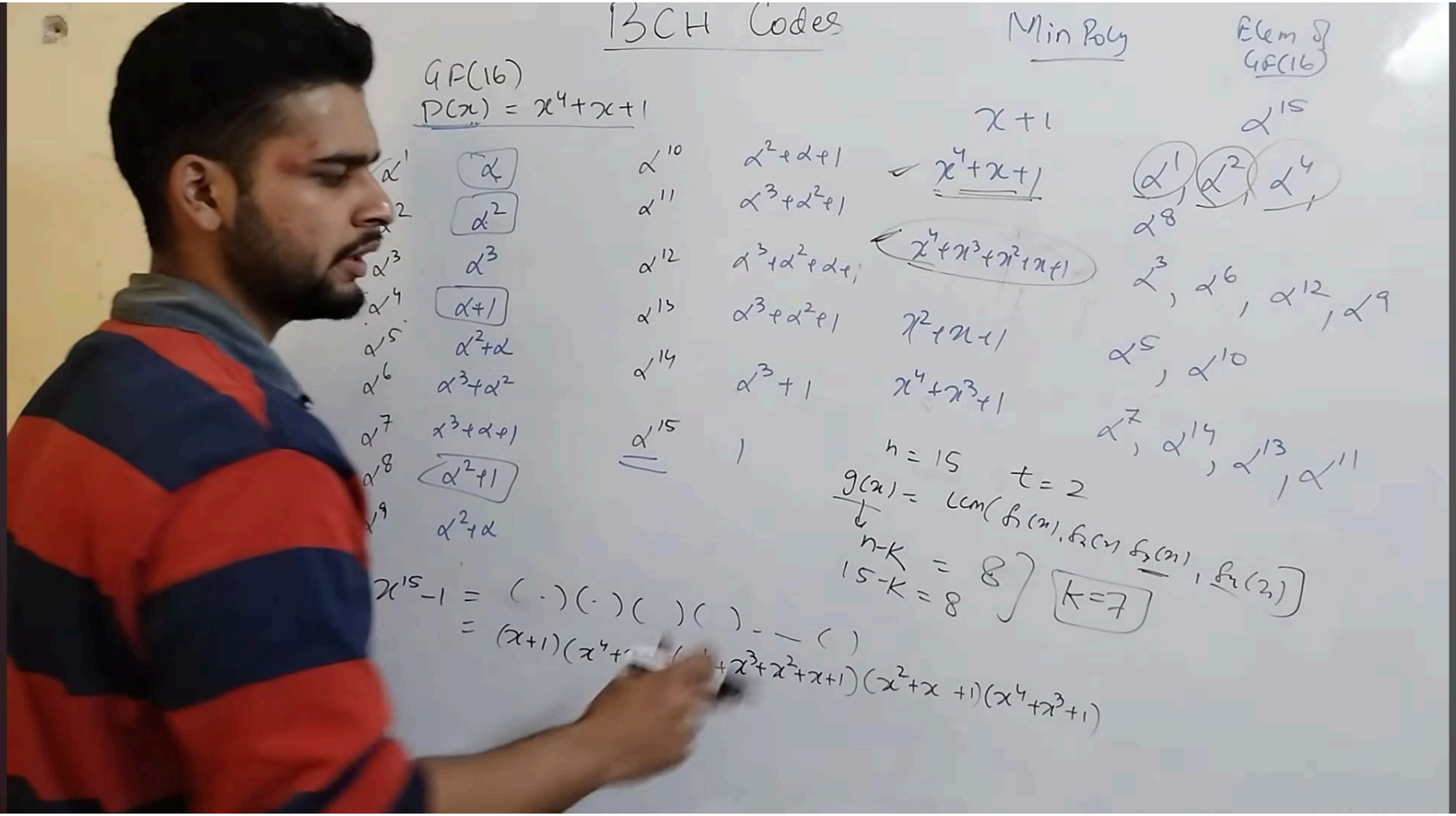
$\alpha^1, \alpha^2, \alpha^4$

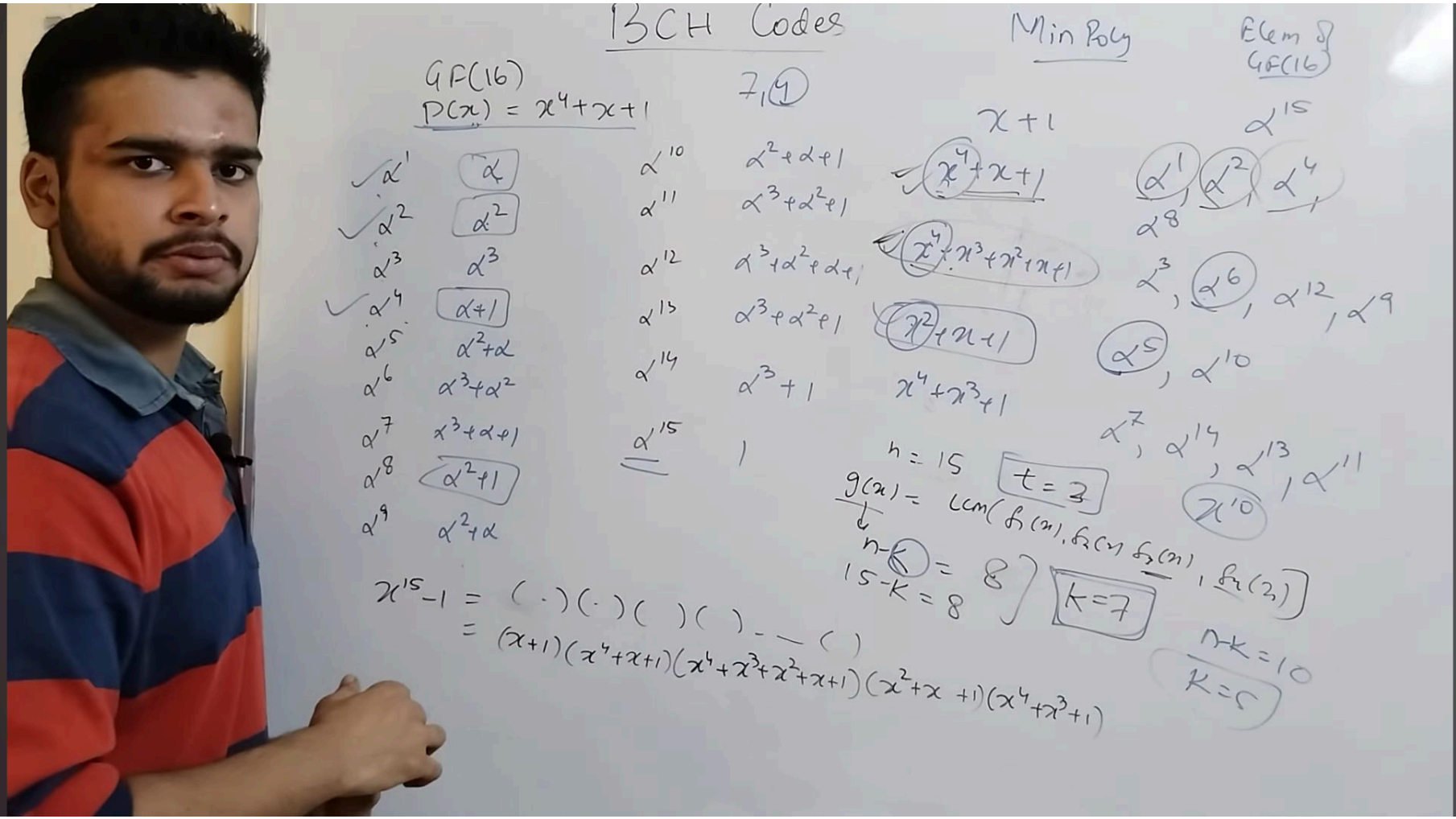
$\alpha^3, \alpha^6, \alpha^5$


BCH Codes (n, K, t)
1] (7, 4, 1)
g(x) = LCM[f1(x) f2(x) f3(x) ... f2t(x)]
g(x) = LCM[f1(x), f2(x)] = x^3+x+1
2] [7, 4, 2]
g(x) = LCM[f1(x) . f2(x) f3(x) f4(x)]
= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
3] [7, 4, 3]
Min Poly
(x+1)
(x^3+x+1)
(x^3+x^2+1)
Element → GF(8)
α^7
α^1, α^2, α^4
α^3, α^6, α^5


BCH Codes
GF(16)
$P(x) = x^4 + x + 1$
α^1 α
α^2 α^2
α^3 α^3
α^4 $\alpha+1$
α^5 $\alpha^2+\alpha$
α^6 $\alpha^3+\alpha^2$
α^7 $\alpha^3+\alpha+1$
α^8 α^2+1
α^9 $\alpha^2+\alpha$
α^{10} $\alpha^2+\alpha+1$
α^{11} $\alpha^3+\alpha^2+1$
α^{12} $\alpha^3+\alpha^2+\alpha+1$
α^{13} $\alpha^3+\alpha^2+1$
α^{14} α^3+1
α^{15} 1
$x^{15}-1 = (\ )(\ )(\ )(\ )\ldots(\ )$
$= (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$


BCH Codes
GF(16)
P(x) = x^4+x+1
Min Poly
Elem of GF(16)
x+1
α^15
x^4+x+1
α^1, α^2, α^4, α^8
x^4+x^3+x^2+x+1
α^3, α^6, α^12, α^9
x^2+x+1
α^5, α^10
x^4+x^3+1
α^7, α^14, α^13, α^11
α^1 α
α^2 α^2
α^3 α^3
α^4 α+1
α^5 α^2+α
α^6 α^3+α^2
α^7 α^3+α+1
α^8 α^2+1
α^9 α^2+α
α^10 α^2+α+1
α^11 α^3+α^2+1
α^12 α^3+α^2+α+1
α^13 α^3+α^2+1
α^14 α^3+1
α^15 1
x^15-1 = ( )( )( )( ) — ( )
= (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)


BCH Codes
Min Poly
Elem of GF(16)
GF(16)
P(x) = x^4+x+1
x+1
α^15
x^4+x+1
α^1, α^2, α^4, α^8
x^4+x^3+x^2+x+1
α^3, α^6, α^12, α^9
x^2+x+1
α^5, α^10
x^4+x^3+1
α^7, α^14, α^13, α^11
n = 15 t = 2
g(x) = lcm(f1(x), f2(x), f3(x), f5(x))
n-k = 8
15-k = 8
k=7
x^15-1 = (x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)


BCH Codes
GF(16)
$P(x) = x^4+x+1$
Min Poly
Elem of GF(16)
α^1 α
α^2 α^2
α^3 α^3
α^4 $\alpha+1$
α^5 $\alpha^2+\alpha$
α^6 $\alpha^3+\alpha^2$
α^7 $\alpha^3+\alpha+1$
α^8 α^2+1
α^9 $\alpha^2+\alpha$
α^{10} $\alpha^2+\alpha+1$
α^{11} $\alpha^3+\alpha^2+1$
α^{12} $\alpha^3+\alpha^2+\alpha+1$
α^{13} $\alpha^3+\alpha^2+1$
α^{14} α^3+1
α^{15} 1
$x+1$
x^4+x+1
$x^4+x^3+x^2+x+1$
x^2+x+1
x^4+x^3+1
α^{15}
$\alpha^1, \alpha^2, \alpha^4, \alpha^8$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$
α^5, α^{10}
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$
x^{10}
$n = 15$
$t = 3$
$g(x) = \text{LCM}(f_1(x), f_2(x), f_3(x), f_6(x))$
$n-k = 8$
$15-k = 8$
$k = 7$
$n-k = 10$
$k = 5$
$x^{15}-1 = (\cdot)(\cdot)(\ )(\ )\ldots(\ )$
$= (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$