$GF(2^2)$ x^2+x+1 $x^2 = -x-1 = x+1$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

*	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

$GF(2^k) \sim \underbrace{01\,01\ldots}_{k}$

Пример

$GF(2^8)$

$x^8+x^4+x^3+x+1$ $x^8 = x^4+x^3+x+1$

$(x^5+x^2+x) \times (x^7+x^4+x^3+x^2+x)$

1) $x^{12}+x^9+x^8+x^7+x^6+x^3+x^6+x^5+x^4+x^3+x^8+x^5+x^4+x^3+x^2 = x^{12}+x^7+x^2 =$

$= (x^4+x^3+x+1)\,x^4+x^7+x^2 = x^5+x^3+x^2+x+1$

x^5+x^2+x

2) $P = 10011110 = x^7+x^4+x^3+x^2+x$

$x \cdot P$	сдвиг на 1 ← ; $\overset{x^8}{=}$: $00111100 + 00011011 = 00100111$	+	$00101111 =$
$x^2 \cdot P$	01001110 ←	+	$x^5+x^3+x^2+x+1$
$x^3 \cdot P$	10011100 ←		
$x^4 \cdot P$	$00111000 + 00011011 = 00100011$; $\overset{x^8}{=}$		
$x^5 \cdot P$	01110000 ←	+	

Пример

$GF(2^4)$ $\quad P = x^4 + x + 1 \Rightarrow x^4 = x + 1$

0000, $g^0 = 0001$, $g^1 = 0010$, $g^2 = 0100$, $g^3 = 1000$

$g^4 = 0011$, $g^5 = 0110$, $g^6 = 1100$, $g^7 = 1011$

$g^8 = 0101$, $g^9 = 1010$, $g^{10} = 0111$, $g^{11} = 1110$

$g^{12} = 1111$, $g^{13} = 1101$, $g^{14} = 1001$, $g^{15} = 0001$

Коды Хэмминга

ожидаем $\rightarrow$ пришло

M $\quad N > M$

$1 - \frac{M}{N}$ – избыточность

$\frac{M}{N}$ – вероятность ошибки

Расстояние Хэмминга

$d(X, Y) = d(1101, 1110) = 2$

пришло			
	N	$N+1$ бит	для детектирования
	N	$2N+1$ бит	для исправления

Алгоритм

$(m, k) \Rightarrow$ $m-k$ бит добавить и проверить

Пример

$i_1, i_2, i_3, i_4 \rightarrow i_1, i_2, i_3, i_4, r_1, r_2, r_3 \qquad r_1 = r_2 = r_3 = 0$

$=$

$r_1 = i_1 + i_2 + i_3$

$r_2 = i_2 + i_3 + i_4$

$r_3 = i_1 + i_2 + i_4$

$$(i_1, i_2, i_3, i_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$