РАСЧЁТНАЯ РАБОТА № 3

- Смирнова Полина Олеговна, гр. N3352
- Вариант 129
- Порождающий многочлен:
  $g(x) = x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{24} + x^{23} + x^{22} + x^{19} + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x + 1$
- Размерность $k = 32$
- Кодовый многочлен
  $c(x) = x^{41} + x^{40} + x^{38} + x^{33} + x^{31} + x^{29} + x^{28} + x^{23} + x^{22} + x^{21} + x^{19} + x^{18} + x^{16} + x^{15} + x^{12} + x^9 + x^8 + x^5 + x^2 + x$

Подробное решение:

Дано:

- $\pi(x) = x^6 + x^5 + x^5 + x^2 + 1$
- $d = 11$
- $b = 55$
- $n = 63$
- Информационный многочлен $a(x) = x^{10} + x^9 + x^7 + x^2 + 1$

Максимальная степень многочлена $\pi = 6$. Построим циклотомические классы на поле $GF(2^6)$ над полем $GF(2)$:

$C_0 = \{ 1 \}$
$C_1 = \{ \alpha^{32} \quad \alpha^{16} \quad \alpha^8 \quad \alpha^4 \quad \alpha^2 \quad \alpha \}$
$C_3 = \{ \alpha^{48} \quad \alpha^{33} \quad \alpha^{24} \quad \alpha^{12} \quad \alpha^6 \quad \alpha^3 \}$
$C_5 = \{ \alpha^{40} \quad \alpha^{34} \quad \alpha^{20} \quad \alpha^{17} \quad \alpha^{10} \quad \alpha^5 \}$
$C_7 = \{ \alpha^{56} \quad \alpha^{49} \quad \alpha^{35} \quad \alpha^{28} \quad \alpha^{14} \quad \alpha^7 \}$
$C_9 = \{ \alpha^{36} \quad \alpha^{18} \quad \alpha^9 \}$
$C_{11} = \{ \alpha^{50} \quad \alpha^{44} \quad \alpha^{37} \quad \alpha^{25} \quad \alpha^{22} \quad \alpha^{11} \}$
$C_{13} = \{ \alpha^{52} \quad \alpha^{41} \quad \alpha^{38} \quad \alpha^{26} \quad \alpha^{19} \quad \alpha^{13} \}$
$C_{15} = \{ \alpha^{60} \quad \alpha^{57} \quad \alpha^{51} \quad \alpha^{39} \quad \alpha^{30} \quad \alpha^{15} \}$
$C_{21} = \{ \alpha^{42} \quad \alpha^{21} \}$
$C_{23} = \{ \alpha^{58} \quad \alpha^{53} \quad \alpha^{46} \quad \alpha^{43} \quad \alpha^{29} \quad \alpha^{23} \}$
$C_{27} = \{ \alpha^{54} \quad \alpha^{45} \quad \alpha^{27} \}$
$C_{31} = \{ \alpha^{62} \quad \alpha^{61} \quad \alpha^{59} \quad \alpha^{55} \quad \alpha^{47} \quad \alpha^{31} \}$

Так как $b = 55$ по условию, для нахождения $g(x)$ нам необходимо найти неприводимые полиномы, корнями которого являются элементы от $\alpha^b = \alpha^{55}$ до $\alpha^{b+d-2} = \alpha^{64} = \alpha^1$ (отмечены синим цветом) циклотомических классов.

Вычисляем полиномы из корней:
$C_0 \to x + 1$
$C_1 \to x^6 + x^5 + x^3 + x^2 + 1$
$C_7 \to x^6 + x^3 + 1$
$C_{15} \to x^6 + x^5 + x^4 + x^2 + 1$
$C_{23} \to x^6 + x + 1$
$C_{31} \to x^6 + x^4 + x^3 + x + 1$

Затем перемножая все образованные многочлены получаем порождающий многочлен $g(x) = x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{24} + x^{23} + x^{22} + x^{19} + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x + 1$

Можем проверить правильность нахождения порождающего многолена, поставив в $g(x)$ α, которые выбирали изначально и являются его корнями. При успрощении выражений, действительно, получаем нули.

Находим k как $k = n - deg(g(x)) = 63 - 31 = 32$. То есть, можем закодировать полином с максимальной степенью равной 32.

Кодируя с помощью $g(x)$ информационный многочлен $a(x)$ находим
$c(x) = x^{41}+x^{40}+x^{38}+x^{33}+x^{31}+x^{29}+x^{28}+x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{16}+x^{15}+x^{12}+x^9+x^8+x^5+x^2+x$