Расширенное поле Галуа

Определение 8: Множество ММ степени не выше n-1 с коэф-ми из простого поля Галуа GF(p) образуют $GF(p^n)$ относительно бинарных операций сложения и умножения по модулю p(mod p) и по модулю M(x)(mod M(x)).

- Примечание: В большинстве практических задач кода образования в качестве ММ M(x) степени n над простым полем Галуа при p=2 используется многочлен $M(x) = x^n + 1$

Пример: Расширенного поля Галуа:

P=2, GF(p)={0,1}, n=3, $GF(p^n) = GF(2^3)$

Коды $GF(2^3)$

$$\left\{\begin{array}{lllll} 0x^2 & + & 0x^1 & + & 0x^0 \\ 0x^2 & + & 0x^1 & + & 1x^0 \\ 0x^2 & + & 1x^1 & + & 0x^0 \\ 0x^2 & + & 1x^1 & + & 1x^0 \end{array}\right\} \begin{array}{l} \sim 000 \\ \sim 001 \\ \sim 010 \\ \sim 011 \end{array}$$

$$\left\{\begin{array}{lllll} 1x^2 & + & 0x^1 & + & 0x^0 \\ 1x^2 & + & 0x^1 & + & 1x^0 \\ 1x^2 & + & 1x^1 & + & 0x^0 \\ 1x^2 & + & 1x^1 & + & 1x^0 \end{array}\right\} \begin{array}{l} \sim 100 \\ \sim 101 \\ \sim 110 \\ \sim 111 \end{array}$$

- Пример обеспечения помехоустойчивости передачи на основе полей Галуа

Базовые концепции:

1. *Передача информации в кодовой форме;*
2. *Код и ММ – это синонимы;*
3. *Исходная информация является помехонезащищенной, помехозащита осуществляется с помощью кодирующего устройства. Кодирующее устройство (к)-разрядную кодовую комбинацию превращает в (n,к)-помехозащитную КК, имеющую n-разрядов,*

   из них к-информационных;

4. *Формирование n-разрядных разрешенных КК из исходных к-разрядных осуществляется так, что их ММ делятся без остатка на ММ в степени m=n-к, принятый за образующий многочлен-кода.*

5. *Процесс искажения КК в канале связи при передаче представляется суммированием ММ передаваемых КК и ММ помехи*

6. *Декодирование – состоит в проверке делимости модулярного многочлена y(x), принятой КК на образующий м-н g(x), при этом если остаток от деления равен 0, то КК при передаче не была искажена*

$$rest\frac{y(x)}{g(x)} = E(x) = 0 \Rightarrow \xi(x) = 0$$

Синдром ошибки

$$rest\frac{y(x)}{g(x)} = E(x) \neq 0 \Rightarrow \xi(x) \neq 0$$

тогда корректирующие способности могут быть использованы в 2-х режимах:

1. Режим обнаружения:

$E(x) \neq 0$ то принятая КК разрушается и на передающую сторону делается запрос на повторение передач.

2.Режим исправления:

Число различных синдромов не меньше числа возможных ошибок

$$[E(x) = rest\frac{y(x)}{g(x)}] \quad \rangle \quad N_{ош}$$

Способы формирования помехозащищенного кода с $f(x): rest \frac{y(x)}{g(x)} = 0$

1. Путем перемножения ММ f(x)=a(x)g(x).

Свойства:

- *Простота*
- *Не сохраняется (к)-код как фрагмент кода*

2. С помощью деления.

$$f(x) = a(x)x^m + r(x):$$

$$где \quad r(x) = rest \frac{a(x)x^m}{g(x)} \quad , m = \deg\{g(x)\}.$$

Пример:

I. Дано: 1.Массив команд Q=16, 2.Наиболее вероятная ошибка в КС -однократная ошибка в одном разряде, 3. Корректирующую способность кода реализовать в режиме исправления.

II. Решение задачи:1.Определение размерности к информационного кода:

$$p = 2; \quad p^k \geq Q(массив) \quad \Rightarrow 2^k \geq Q = 16 \Rightarrow \boxed{k = 4}$$

2.Число разрядов помехозащищенного кода n=k + m

где m=deg {g(x)}

$$m \quad : \quad N_{ош} \leq N_{синдромов} = [E(x)] = 2^m - 1; \quad 2^m - 1 \geq n = m + k$$

$$m = 1 \quad : \quad n = m + k = 1 + 4 = 5; \quad 2^1 - 1 = 1 \leq 5$$

$$m = 2: \quad n = m + k = 2 + 4 = 6; \quad 2^2 - 1 = 3 \leq 6$$

$$m = 3: \quad n = m + k = 3 + 4 = 7; \quad 2^3 - 1 = 7 \geq 7; \quad \boxed{n = 7}$$

II. *Выбор образующего ММ g(x) кода:*

1.deg{g(x)}=m=3,

2.g(x)-неприводимый ММ : $g(x) = x^3 + x^2 + 1$

V. *Процесс формирования помехозащищенного кода в силу алгоритма:*

$$f(x) = a(x)x^m + r(x); r(x) = rest\,\frac{a(x)x^m}{g(x)}$$

$$(к) - код: \qquad 1011 \sim \mathrm{a(x)} = \mathrm{x}^3 + \mathrm{x} + 1$$

$$a(x)x^m = (\mathrm{x}^3 + \mathrm{x} + 1)\mathrm{x}^3 = \mathrm{x}^6 + \mathrm{x}^4 + \mathrm{x}^3$$

$$r(x) = rest\,\frac{a(x)x^m}{g(x)} = \frac{\mathrm{x}^6 + \mathrm{x}^4 + \mathrm{x}^3}{\mathrm{x}^3 + \mathrm{x}^2 + 1} = x^2$$

$$x^6 + x^4 + x^3 \quad | \; x^3 + x^2 + 1$$

$$x^6 + x^5 + x^3$$

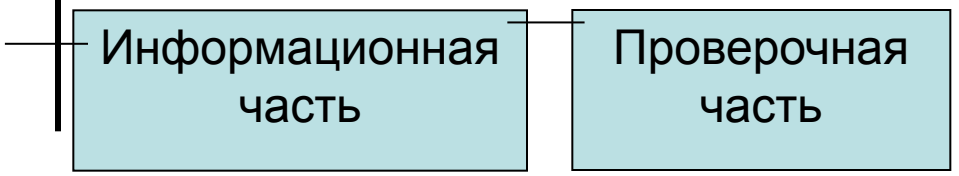
$$x^5 + x^4$$

$$x^5 + x^4 + x^2$$

$$r(x) = x^2$$

k{f(x)}=(n,k)

код: 1011100



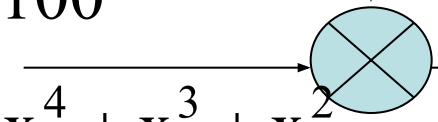
V. *Искажение передаваемого КК в КС*

$$k\{\xi(x)\} = 001000$$

$$001000 \sim \xi(x) = x^4$$

1011100

1001100



$$f(x) = x^6 + x^4 + x^3 + x^2$$

$$y(x) = x^6 + [illegible] + x^4 + x^3 + x^2 = x^6 + x^3 + x^2$$

0

VI. Декодирование

$$
\begin{array}{l|l}
x^6 + x^3 + x^2 & x^3 + x^2 + 1 \\
\hline
x^6 + x^5 + x^3 & x^3 + x^2 + x + 1 \\
\hline
x^5 + x^2 & \\
\hline
x^5 + x^4 + x^2 & \\
\hline
x^4 & \\
\hline
x^4 + x^3 + x & \\
\hline
x^3 + x & \\
\hline
x^3 + x^2 + 1 & \\
\hline
x^2 + x + 1 &
\end{array}
$$

$k\{E(x) = x^2 + x + 1\} = 111$ –

синдром ошибки в каждом разряде.