Dr inż. Robert Wójcik, p. 313, C-3, tel. 320-27-40

Katedra Informatyki Technicznej (K30W04ND03)
Wydział Informatyki i Telekomunikacji (W04N)
Politechnika Wrocławska

E-mail: **robert.wojcik@pwr.edu.pl**
Strona internetowa: google: Wójcik Robert

Ochrona danych

Wykład 6.

6. Ciała skończone rozszerzone – konstrukcja i realizacja działań

6.1. Elementy ciała rozszerzonego

6.2. Operacje mnożenia i dodawania elementów

6.3. Wielomiany minimalne elementów ciała rozszerzonego

6.4. Logarytmy Zecha

6.5. Programowa realizacja operacji w ciele

Źródło:

Mochnacki W., Kody korekcyjne i kryptografia, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2000.

Ciała proste są wykorzystywane do konstrukcji ciał rozszerzonych, które z kolei znajdują zastosowanie do konstrukcji kodów cyklicznych binarnych (np. kody BCH) i niebinarnych (np. kody RS).

Do konstrukcji wielomianów generujących kody cykliczne binarne wykorzystywane są wielomiany pierwotne oraz wielomiany minimalne elementów ciała rozszerzonego. W przypadku kodów cyklicznych niebinarnych, które są podklasą niebinarnych kodów BCH, stosowane są wielomiany generujące kod o współczynnikach należących do ciała rozszerzonego.

6.1. Elementy ciała rozszerzonego

W algebrze ciał skończonych ciała rozszerzone $GF(q)$ można konstruować nad ciałami prostymi $GF(p)$ lub ciałami rozszerzonymi niższego stopnia. Liczba elementów q ciała rozszerzonego $GF(q)$ nad ciałem prostym $GF(p)$ wynosi $q=p^m$, gdzie m jest *stopniem rozszerzenia*. Analogicznie, gdy konstruujemy ciało rozszerzone $GF(q)$ stopnia k nad innym ciałem rozszerzonym $GF(s)$, to liczba elementów ciała rozszerzonego wynosi $q = s^k$.

Ciała rozszerzone nie są ciałami liczbowymi, a ich elementy oznaczamy zwykle za pomocą symboli nieliczbowych.

W przypadku ciał skończonych do konstrukcji ciał rozszerzonych stosuje się wielomiany pierwotne. Wtedy pierwiastek wielomianu pierwotnego α jest elementem pierwotnym ciała, a niezerowe elementy ciała rozszerzonego w postaci multyplikatywnej możemy zapisać jako potęgi elementu pierwotnego. Na przykład elementami ciała rozszerzonego $GF(q)$ będą: $0, 1, \alpha^1, \alpha^2, \dots, \alpha^{q-2}$.

Konstrukcja ciała rozszerzonego ma na celu wyznaczenie tabliczek dodawania i mnożenia ciała rozszerzonego.

6.2. Operacje mnożenia i dodawania elementów

Wykorzystując postać multyplikatywną elementów ciała skończonego można wyznaczyć iloczyn dwóch dowolnych elementów ciała. Iloczyn dwóch elementów ciała skończonego α^i i α^j wynosi

$$\alpha^i \cdot \alpha^j = \alpha^{(i+j)\, mod(q-1)}$$

Obliczając iloczyny dla kolejnych elementów ciała, można wyznaczyć całą tabliczkę mnożenia. Tabliczkę mnożenia ciała *GF*(8), utworzonego z wykorzystaniem wielomianu $p(x) = x^3 + x + 1$, pokazano na kolejnej stronie.

W szczególności, dla elementu odwrotnego zachodzi:
$\alpha^{-i} = \alpha^{(-i)mod(q-1)} = \alpha^{q-1-i}$ oraz $\alpha^{q-1} = 1.$

Aby wyznaczyć tabliczkę dodawania, należy zapisać elementy ciała skończonego w postaci addytywnej. Może to być postać macierzowa, wektorowa lub wielomianowa.

Sposób obliczania elementów ciała rozszerzonego i tabliczek działań pokażemy na przykładzie ciała *GF*(2^3) generowanego przez wielomian pierwotny $p(x)$ trzeciego stopnia nad *GF*(2), który ma postać:

$$p(x) = x^3 + x + 1.$$

Wielomian ten umożliwia konstrukcję ciała rozszerzonego *GF*(2^3) zawierającego osiem elementów. Niżej pokazano metodę wyznaczania elementów ciała rozszerzonego *GF*(2^3) = *GF*(8) w postaci addytywnej za pomocą wektorów.

Wektorowa postać elementów ciała rozszerzonego jest wygodna, gdy konstruujemy ciało metodami programowymi. W celu wyznaczenia wektorowej postaci elementów ciała skończonego *GF*(8) wykorzystujemy sekwencję pseudolosową generowaną przez wielomian pierwotny służący do konstrukcji ciała rozszerzonego. Aby wygenerować sekwencję okresową, piszemy zależność rekurencyjną stowarzyszoną z wielomianem:

$$s_{j+3} = s_{j+1} + s_j, \quad j = 0,1,2, \ldots$$

Zakładając ciąg początkowy 100, otrzymamy następującą sekwencję pseudolosową

1 0 0 1 0 1 1 1 0 0 ...

Zastosowany wielomian daje rozszerzenie trzeciego stopnia (*m*=3), dlatego też wektory odpowiadające elementom ciała rozszerzonego będą zawierały po trzy współrzędne. Biorąc kolejne grupy trzyelementowe, z powyższej sekwencji pseudolosowej otrzymamy elementy ciała rozszerzonego w postaci wektorowej:

$0 = [0\ 0\ 0], \quad 1 = [1\ 0\ 0], \quad \alpha = [0\ 0\ 1], \quad \alpha^2 = [0\ 1\ 0],$

$\alpha^3 = [1\ 0\ 1], \quad \alpha^4 = [0\ 1\ 1], \quad \alpha^5 = [1\ 1\ 1], \quad \alpha^6 = [1\ 1\ 0].$

Zbiór wektorów jest uzupełniany wektorem zerowym 0 = [0 0 0].
Posługując się elementami ciała w postaci wektorowej, można wyznaczyć sumę dowolnych elementów ciała oraz całą tabliczkę dodawania. Na przykład suma dwóch elementów ciała α^2 i α^3 wynosi:

$\alpha^2 + \alpha^3 = [0\ 1\ 0] + [1\ 0\ 1] = [1\ 1\ 1] = \alpha^5.$

Współrzędne sumujemy modulo 2. Tabliczki mnożenia i dodawania elementów w ciele rozszerzonym *GF*(2^3) = *GF*(8) pokazano poniżej.

Tabliczki mnożenia i dodawania ciała $GF(8)$

·	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

+	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

W ciałach charakterystyki 2 (postaci *GF*(2^m)) mamy $-\alpha^i = \alpha^i$, czyli element przeciwny do danego elementu jest równy temu elementowi.

Dla ciał charakterystyki p > 2 element przeciwny do α^i wynosi:

$-\alpha^i = \alpha^{i+(q-1)/2}$.

6.3. Wielomiany minimalne elementów ciała rozszerzonego

Dla każdego elementu ciała można wyznaczyć wielomian minimalny. Wielomianem minimalnym $m_i(x)$ elementu ciała α^i jest wielomian najniższego stopnia taki, że α^i jest pierwiastkiem tego wielomianu, tj.

$m_i(\alpha^i) = 0.$

Generalnie wielomian minimalny $m_i(x)$ stopnia *k* nad *GF*(*q*), gdzie $q = p^m$, ma następujące pierwiastki:

$$\alpha^i, \alpha^{ip}, \alpha^{ip^2}, \ldots, \alpha^{ip^{i-1\,(mod(q-1))}}$$

Elementy tego ciągu są nazywane elementami sprzężonymi i mają taki sam rząd multyplikatywny. Posługując się powyższym ciągiem, można rozbić na warstwy cyklotomiczne niezerowe elementy każdego ciała rozszerzonego. Aby utworzyć te warstwy, bierzemy kolejne elementy ciała, które nie występują w warstwach poprzednich. Pierwszą warstwę tworzy element 1.

Dla ciała $GF(2^4)=GF(16)$, utworzonego z wielomianu $p(x) = x^4 + x + 1$, otrzymamy następujące warstwy cyklotomiczne ($q = 16$; $q - 1 = 15$):

1;
$\alpha^1, \alpha^2, \alpha^4, \alpha^8$; kolejny: $\alpha^{16\ mod\ 15} = \alpha^1$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$;
α^5, α^{10};
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$; wszystkie elementy już na liście

Każda z tych warstw odpowiada jednemu wielomianowi minimalnemu, którego pierwiastkami będą elementy warstwy. W powyższym przykładzie warstwa druga, trzecia i piąta utworzą wielomiany czwartego stopnia, warstwa czwarta wielomian drugiego stopnia, a jedynka, znajdująca się w warstwie pierwszej, utworzy wielomian pierwszego stopnia.

Znajomość rozkładu pierwiastków na warstwy cyklotomiczne pozwala obliczyć wielomiany minimalne elementów ciała. Jeśli znamy pierwiastki wielomianu $x_1, x_2, \ldots, x_n$, to wielomian o tych pierwiastkach można obliczyć ze znanego w algebrze wzoru

$$p(x) = (x - x_1)(x - x_2) \ldots (x - x_n).$$

W ciałach charakterystyki 2 odejmowanie zastępuje się dodawaniem. Dla przykładu wielomian minimalny $m_3(x)$ elementu α^3 ciała $GF(2^4)$ ma postać:

$$m_3(x) = (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9).$$

Obliczenie powyższego iloczynu wymaga znajomości elementów ciała w postaci addytywnej lub tabliczki dodawania. Po wymnożeniu pojawią się sumy elementów ciała, które można obliczyć na podstawie tabelek dodawania, np.

$$m_3(x) = (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9) =$$
$$= (x^2 + (\alpha^3 + \alpha^6)x + \alpha^9)(x + \alpha^{12})(x + \alpha^9).$$

6.4. Logarytmy Zecha

Programową realizację dodawania w ciałach skończonych ułatwiają Logarytmy Zecha. Przyjmujemy, że elementy ciała skończonego $GF(q)$ charakterystyki p wyrażamy za pomocą potęg elementu pierwotnego α, tj. $0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}$. Wykładniki potęg są liczbami całkowitymi liczonymi modulo $(q-1)$. Element zerowy w postaci potęgowej można zapisać za pomocą symbolu $\alpha^{-\infty} = 0$.

Logarytm Zecha oznaczamy przez $Z(x)$ i definiujemy za pomocą równania

$$\alpha^{Z(x)} = \alpha^x + 1 .$$

Dla ciał charakterystyki 2: $Z(0) = -\infty$, a $Z(-\infty) = 0$.

Dla ciał charakterystyki p>2: $Z((q-1)/2) = -\infty$, a $Z(-\infty) = 0$.

Dodawanie z wykorzystaniem logarytmu Zecha wykonuje się korzystając z zależności (dla y >= x):

$$\alpha^x + \alpha^y = \alpha^x(1 + \alpha^{y-x}) = \alpha^{x+Z(y-x)} .$$

Dla (x >= y) zamienia się zmienne x, y. Wynik dodawania nie zmienia się.

Implementacja tej metody dodawania wymaga, aby utworzyć tablice logarytmów Zecha albo na bieżąco obliczać wartości logarytmów Zecha.

Logarytmy Zecha dla danego ciała można obliczać z wielomianu generującego ciało (zobacz tabela logarytmów Zecha), np. dla $GF(2^2) = GF(4)$ z $p(x) = x^2 + x + 1$, dla $GF(2^3) = GF(8)$ z $p(x) = x^3 + x + 1$, dla $GF(2^4) = GF(16)$ z $p(x) = x^4 + x + 1$, oraz zależności:

$$Z\left((q-1-x)p^i \bmod (q-1)\right) = (Z(x)-x))p^i \bmod (q-1)\ ,$$

$$Z\left(xp^i \bmod (q-1)\right) = Z(x)p^i \bmod (q-1).$$

Logarytmy Zecha dla ciał charakterystyki dwa

q	Logarytmy Zecha dla $x = 1, 2, ..., q-2$
4	2 1
8	3 6 1 5 **4** 2
16	4 8 14 1 **10** 13 9 2 7 **5** 12 11 6 3
32	20 9 26 18 **8** 21 29 5 2 **16** 12 11 17 27 **25** 10 13 4 30 **1** 6 24 28 22 **15** 3 14 23 7 **19**
64	6 12 32 24 **62** 1 26 48 45 **61** 25 2 35 52 **23** 33 47 27 56 **59** 42 50 15 4 **11** 7 18 41 60 **46** 34 3 16 31 **13** 54 44 49 43 **55** 28 21 39 37 **9** 30 17 8 38 **22** 53 14 51 36 **40** 19 58 57 20 **29** 10 5

6.5. Programowa realizacja operacji w ciele

Aby było możliwe zastosowanie komputerowych technik obliczeniowych w tej dziedzinie, należy przedstawić elementy ciała w postaci liczbowej i określić działania na tych liczbach.

W tym celu można przyjąć odwzorowanie zbioru elementów ciała $GF(q)$ na q-elementowy zbiór całkowitych liczb dodatnich:

$$\sigma:\ \{0, 1, \alpha^1, \alpha^2, \dots, \alpha^{q-2}\}\ \rightarrow\ \{0, 1, 2, 3, \dots, q-1\}\ .$$

Odwzorowanie to określa funkcja:

$$\sigma(\alpha^x) = \begin{cases} x+1 & dla\quad \alpha^x \neq 0, \\ 0 & dla\quad \alpha^x = 0\ . \end{cases}$$

Tak więc zerowy element ciał odwzorowuje się na zero, a elementy niezerowe α^x odwzorowują się na liczby równe $x+1$. Odwzorowanie to jest wzajemnie jednoznaczne i izomorficzne.

Dla odwzorowania σ istnieje odwzorowanie odwrotne σ^{-1} :

$$\sigma^{-1}\colon\ \{0,1,2,3,\dots,q-1\}\ \rightarrow\ \ \{0,1,\alpha^1,\alpha^2,\dots,\alpha^{q-2}\}\,,$$

przy czym dla x = 0, 1, 2, …, *q*-1 jest:

$$\sigma^{-1}(x)=\begin{cases}\alpha^{x-1} & dla\quad x>0,\\ 0 & dla\quad x=0\,.\end{cases}$$

Dla większości zastosowań wystarczy zdefiniować cztery funkcje (dla x>=y; w przeciwnym wypadku zamienia się zmienne x, y).

Sumę: $S(x,y)$.

Element przeciwny: $OE(x)$.

Iloczyn: $P(x,y)$.

Element odwrotny: $IE(x)$.

Po uwzględnieniu powyższych zależności można obliczyć wartości tych czterech funkcji wykorzystując następujące wzory:

$$S(x,y)=\begin{cases}(y+Z(x-y)-1)\ mod\ (q-1)\ +1\quad dla\quad x,y\neq 0\quad i\quad x>y\,,\\ x+y\quad dla\quad x=0\quad lub\quad y=0\,,\\ 0\quad dla\quad x\neq 0\quad i\quad y=OE(x)\,.\end{cases}$$

$$OE(x)=\begin{cases}(x+(q-1)/2)\ mod\ (q-1)\quad dla\quad x\neq 0\quad i\quad p>2\,,\\ x\quad dla\quad x\neq 0\quad i\quad p=2\,,\\ 0\quad dla\quad x=0\ .\end{cases}$$

$$P(x,y)=\begin{cases}1+(x+y-2)\ mod\ (q-1)\quad dla\quad x>0\ \ i\quad y>0\,,\\ \\ 0\quad dla\quad x=0\quad lub\quad y=0\,.\end{cases}$$

$$IE(x)=\begin{cases}(q+1-x)\ \ dla\quad x>1\,,\\ \\ 1\quad dla\quad x=1\,.\end{cases}$$

W ciałach charakterystyki 2 dla elementu przeciwnego zachodzi:
$y = OE(x) = x$.

Do obliczenia sumy $S(x, y)$ wykorzystuje się logarytmy Zecha. Za pomocą powyższych wzorów można w dowolnym języku programowania napisać procedury realizujące algorytmy działań w rozszerzonych ciałach skończonych.

Przykład obliczeniowy.

Rozważamy ciało rozszerzone $GF(p^m) = GF(2^2) = GF(4) = GF(q)$, utworzone z wykorzystaniem wielomianu pierwotnego $p(x) = x^2 + x + 1$ nad GF(2) = GF(p), gdzie $q = p^m$, $p = 2$, $m = 2$, $q = 4$.

Równanie rekurencyjne i sekwencja okresowa stowarzyszone z wielomianem $p(x) = x^2 + x + 1$:

$$x^2 + x + 1 = 0 ,$$

$$x^2 = -x - 1 ,$$

$$x^2 = x + 1.$$

Równanie rekurencyjne:

$$S_{j+2} = S_{j+1} + S_j , \quad j = 0, 1, 2, \ldots$$

$$S_0 = 1,\ S_1 = 0 ,$$

S_0	S_1	S_2	S_3	S_4	S_5
1	0	1	1	0	1

Elementy ciała rozszerzonego $GF(4) = \{0, 1, \alpha^1, \alpha^2\}$:

$$0 = [0\ 0], \qquad 1 = [1\ 0], \qquad \alpha = [0\ 1], \qquad \alpha^2 = [1\ 1].$$

Odwzorowanie elementów ciała na wartości liczbowe $x = 0, 1, 2, 3$ używane w programie:

$$\sigma:\ \{0, 1, \alpha^1, \alpha^2\} \ \rightarrow \ \{0, 1, 2, 3\} .$$

Wartości logarytmów Zecha obliczone z wielomianu $p(x) = x^2 + x + 1$ dla *q* = 4 (podane w Tabeli dla *q* = 4).

Dla x = 1; Z(1) = 2

Dla x = 2; Z(2) = 1.

Tabliczka dodawania elementów w ciele *GF*(4) wyznaczona z postaci wektorowej elementów ciała:

$+$	0	1	α^1	α^2
0	0	1	α^1	α^2
1	1	0	α^2	α^1
α^1	α^1	α^2	0	1
α^2	α^2	α^1	1	0

1 + 1 = [1 0] + [1 0] = [0 0] ,

1 + α^1 = [1 0] + [0 1] = [1 1] = α^2,

1 + α^2 = [1 0] + [1 1] = [0 1] = α^1,

Te same obliczenia można wykonać z wykorzystaniem logarytmów Zecha przyjmując:

$x, y \in \{0, 1, 2, 3\}$ oraz wzór na sumę elementów x + y dla x >= y):

$$S(x,y) = \begin{cases} (y + Z(x-y) - 1) \ mod \ (q-1) \ + 1 \quad dla \quad x, y \neq 0 \quad i \quad x > y \,, \\ x + y \quad dla \quad x = 0 \quad lub \quad y = 0 \,, \\ 0 \quad dla \quad x \neq 0 \quad i \quad y = OE(x) \,. \end{cases}$$

Mamy:

dla x = 2; y = 1;

$S(x,y) = S(2,1) = [1 + Z(1) - 1] \ mod \ 3 \ + \ 1 = 2 + 1 = 3$;

dla x = 3; y = 1;

$S(x,y) = S(3,1) = [1 + Z(2) - 1] \ mod \ 3 \ + \ 1 = 1 + 1 = 2$;

dla x = 3; y = 3;

$S(x, y) = S(3,3) = 0$;

dla x = 1; y = 3;

$S(x, y) = S(1,3) = S(3,1) = 2$.

W efekcie otrzymujemy następującą tabelkę dodawania x + y w ciele *GF*(4):

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Tabelka mnożenia w *GF*(4) wyznaczona z zależności:

$\alpha^i \cdot \alpha^j = \alpha^{(i+j)\, mod(q-1)}$ oraz zależności $P(x, y)$.

·	0	1	α^1	α^2
0	0	0	0	0
1	0	1	α^1	α^2
α^1	0	α^1	α^2	1
α^2	0	α^2	1	α^1

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2