Laboratorium ochrony danych

Ćwiczenie nr 2

Temat ćwiczenia: Ciała skończone rozszerzone

Cel dydaktyczny: Opanowanie programowej metody konstruowania ciał skończonych rozszerzonych $GF(p^m)$, poznanie ich własności oraz techniki wykonywania działań na elementach tych systemów algebraicznych.

Wprowadzenie teoretyczne

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*. 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: $0, 1, \alpha, a^2, \ldots, \alpha^{q-2}$. Konstrukcja ciała rozszerzonego ma na celu wyznaczenie tabliczek dodawania i mnożenia ciała rozszerzonego.

Postać multyplikatywna elementów ciała skończonego pozwala wyznaczyć iloczyn dwóch dowolnych elementów ciała. Iloczyn dwóch elementów ciała skończonego α^i i α^j wynosi

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

Obliczając iloczyny dla kolejnych elementów ciała, można wyznaczyć całą tabliczkę mnożenia.

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 $GF(2)$

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

Wielomian ten umożliwia konstrukcję ciała rozszerzonego $GF(2^3)$ zawierającego osiem elementów. Niżej pokazano sposoby wyznaczania elementów ciała rozszerzonego $GF(2^3)$ 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

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

Zakładając ciąg początkowy 100, otrzymamy następującą sekwencję pseudolosową

$$1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,\ldots$$

Zastosowany wielomian daje rozszerzenie trzeciego stopnia, 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:

$$0=[000], \quad 1=[100], \quad \alpha=[001], \quad \alpha^2=[010],$$
$$\alpha^3=[101], \quad \alpha^4=[011], \quad \alpha^5=[111], \quad \alpha^6=[110].$$

Zbiór wektorów jest uzupełniany wektorem zerowym.

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

$$\alpha^2 + \alpha^3 = [010] + [101] = [111] = \alpha^5.$$

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

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

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

Generalnie wielomian minimalny stopnia k nad $GF(q)$ ma następujące pierwiastki:

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

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 $GF(2^4)$ otrzymamy następujące warstwy cyklotomiczne:

$$1;$$
$$\alpha, \alpha^2, \alpha^4, \alpha^8;$$
$$\alpha, {}^3\alpha^6, \alpha^{12}, \alpha^9;$$
$$\alpha^5, \alpha^{10};$$
$$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}.$$

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. Jeśli znamy pierwiastki wielomianu $x_1, x_2, \ldots, x_n$, to wielomian 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 elementu α^3 ciała $GF(2^4)$

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

Obliczenie powyższego iloczynu wymaga znajomości elementów ciała w postaci addytywnej lub tabliczki dodawania.

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: $0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$. 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 następująco (y > x)

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

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, np. dla $GF(2^3)$ z $p(x) = x^3 + x + 1$, oraz zależności:

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

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

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

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:

$$\sigma: \quad \left\{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\right\} \to \left\{0,1,2,3,\ldots,q-1\right\}.$$

Odwzorowanie to określa funkcja:

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

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}

$$\sigma^{-1}: \quad \left\{0,1,2,3,\ldots,q-1\right\} \to \left\{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\right\},$$

przy czym

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

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

Sumę $S(x,y)$.

Element przeciwny $OE(x)$.

Iloczyn $P(x,y)$.

Element odwrotny $IE(x)$.

Po uwzględnieniu powyższych odwzorowań można obliczyć te cztery funkcje:

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

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

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

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

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.

Przebieg ćwiczenia

1. Napisać podprogram do wykonywania mnożenia w ciele $GF(p^m)$. Zastosować wzór $\alpha^i \cdot \alpha^j = \alpha^{i+j(\mathrm{mod}(q-1))}$. Wydrukować tabliczki mnożenia dla przypadku ciał $GF(2^3)$ i $GF(2^4)$. Na wydrukach zastąpić symbol α^i tekstem ai.
2. Napisać podprogram do wykonywania dodawania i mnożenia w ciele $GF(p^m)$ oraz sprawdzić jego działanie dla przypadku ciał $GF(2^2)$, $GF(2^3)$ i $GF(2^4)$. Zastosować logarytmy Zecha. Wartości logarytmów (dla q = 4, 8, 16; x = 1,2, …, q-2) zdefiniować jako stałe w programie. Do obliczenia sumy ($x+y$), gdzie elementy x i y są podawane z klawiatury, wykorzystać wzór $S(x,y)$, a do obliczenia ich iloczynu wzór $P(x,y)$.
3. Wydrukować tabliczki mnożenia i dodawania w ciałach $GF(2^2)$, $GF(2^3)$ i $GF(2^4)$ w oparciu o podprogramy zrealizowane w zadaniu drugim.
4. Obliczyć wielomian czwartego stopnia elementów ciała $GF(2^4)$

$$m_i(x) = (x + x_1)(x + x_2)(x + x_3)(x + x_4) =$$
$$x^4 + [(x_1 + x_2) + (x_3 + x_4)]x^3 + [(x_1 + x_2)(x_3 + x_4) + x_1x_2 + x_3x_4]x^2 +$$
$$[(x_3 + x_4)x_1x_2 + (x_1 + x_2)x_3x_4]x + x_1x_2x_3x_4.$$

   Na przykład, dla $x_1 = \alpha$, $x_2 = \alpha^2$, $x_3 = \alpha^4$ i $x_4 = \alpha^8$ otrzymamy wielomian minimalny $m_1(x) = x^4 + x + 1$. Wykorzystać wzory na sumę oraz iloczyn dwóch elementów ciała. Wartości elementów: $x_1 = \alpha = 2$, $x_2 = \alpha^2 = 3$, $x_3 = \alpha^4 = 5$ i $x_4 = \alpha^8 = 9$ są podawane przez użytkownika.

Zadania rozwiązać w dowolnym języku programowania.