ПОЛИНОМИАЛЬНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ. ВЫЧИСЛЕНИЯ В ПОЛИНОМИАЛЬНЫХ ГРУППАХ, КОЛЬЦАХ И ПОЛЯХ

1 Кольцо многочленов

Напомним, что *кольцо многочленов над полем* F образуется всеми многочленами над F. Оно обозначается $F[X]$. Операции сложения и умножения кольца $F[X]$ определяются теми же правилами, по которым складываются или перемножаются многочлены над действительным полем.

Операция *сложения* сопоставляет двум многочленам $p_1(X) = \sum_{i=0}^{n-1} a_i X^i$ и $p_2(X) = \sum_{i=0}^{n-1} b_i X^i$, их сумму

$$p_1(X) + p_2(X) = \sum_{i=0}^{n-1} (a_i + b_i) X^i. \tag{1}$$

(Здесь и ниже в слагаемых формул, подобных формуле в правой части, имеются в виду операции сложения и умножения в поле F).

Результатом операции *умножения* многочленов $p_1(X) = \sum_{i=0}^{n-1} a_i X^i$ и $p_2(X) = \sum_{i=0}^{n-1} b_i X^i$ является многочлен

$$p(X) = p_1(X) \times p_2(X) = \sum_{i=0}^{2n-2} c_i X^i, \tag{2}$$

где $c_i = \sum_{t+l=i} a_t b_l$.

Нулем кольца многочленов является многочлен 0, все коэффициенты которого нулевые, то есть равны аддитивной единице поля. Единицей кольца многочленов является многочлен 1 нулевой степени. Кольцо многочленов не является полем, так как не всякий многочлен имеет обратный к нему элемент кольца.

Упражнение 1.1 Убедитесь, что приведенное описание кольца многочленов соответствует аксиомам кольца.

2 Конечное расширение поля

Определение 2.1 Пусть F – подполе поля H. Минимальное поле, содержащее F и элемент $\theta \in H$, $\theta \notin F$, называется *простым расширением поля* F и

обозначается $F(\theta)$.

Пример 2.1 Множество $H = \{0,1\}^3$ с операциями $+$ и $\times$, представленными в следующих таблицах

$+$	**000**	**100**	010	110	001	101	011	111
000	**000**	**100**	010	110	001	101	011	111
100	**100**	**000**	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

$\times$	**000**	**100**	010	110	001	101	011	111
000	**000**	**000**	000	000	000	000	000	000
100	**000**	**100**	010	110	001	101	011	111
010	000	010	001	011	110	100	111	101
110	000	110	011	101	111	001	100	010
001	000	001	110	111	011	010	101	100
101	000	101	100	001	010	111	110	011
011	000	011	111	100	101	110	010	001
111	000	111	101	010	100	011	001	110

является полем H.

Множество $\{000, 001\}$ с операциями, представленными в тех же таблицах жирным шрифтом, также является полем. Обозначим это поле F. Поле H получается из поля F добавлением любого нового элемента θ из $\{0,1\}^3$, например, 010, а затем последовательно и всех остальных элементов этого множества, поскольку каждый из них может быть получен из предыдущих с помощью операций поля H. Множество $\{0,1\}^3$ замкнуто относительно операций поля H, таким образом, это поле является минимальным полем, содержащим элементы поля F и элемент θ. Вместо элемента (0,1,0) можно было выбрать любой другой отличный от (0,0,0) и (0,0,1) элемент из $\{0,1\}^3$. Таким образом, $H = F(010) = F(011) = F(100) = F(101) = F(110) = F(111)$ и H есть простое расширение поля F в поле H. В данном случае H есть поле $GF(2^3)$, а F – поле $GF(2)$. Поле H содержит $\varphi(2^3 - 1) = 6$ примитивных элементов 010, 110, 001, 101, 011 и 111.

$$010,\ (010)^3 = 011,\ (010)^5 = 111,\ (010)^7 = 010,$$

а поле $GF(2)$ имеет $\varphi(2) = 1$ примитивный элемент 001.

Определение 2.2 Многочлен над полем F называется неприводимым над данным полем F, если его нельзя представить в виде произведения многочленов меньшей степени над этим полем.

Неприводимый многочлен над полем F, очевидно, не имеет корней в этом поле. Если $x = \theta$ есть корень в поле H, некоторого неприводимым многочлена f степени n над полем F, то простое расширение $F(x)$ называется *простым алгебраическим расширением*, полученным путем присоединения к полю F корня x многочлена f. Если при этом многочлен f является неприводимым многочленом степени n, то расширение $F(x)$ называется *простым алгебраическим расширением поля F степени n*.

Пример 2.2 Поле $GF(2^2)$ можно получить присоединением к полю $GF(2)$ корня x неприводимого многочлена $1 + X + X^2$ и определив операцию умножения, такую, что $x^2 = x + 1$ следующим образом

$$x \cdot 1 = x,\ x \cdot x = x + 1,\ x \cdot (1 + x) = 1,\ (1 + x)(1 + x) = x.$$

Заметим, что элемент $x = 010$ поля H из предыдущего примера есть корень неприводимого многочлена $f(X) = 1+X+X^3$ над полем F (можно проверить, что $f(x) = 1+x+x^3 = 000$). Поле H можно получить присоединением к полю F этого корня: $H = F(010)$. Значит, H есть простое алгебраическое расширение поля F степени 3.

Пример 2.3 Поле комплексных чисел есть простое алгебраическое расширение поля действительных чисел, получаемое присоединением корня i неприводимого многочлена $X^2 + 1$ над полем действительных чисел.

Определение 2.3 Пусть F – подполе поля H. Поле H называется *конечным расширением поля F,* если поле H содержит элементы $h_1,\ h_2,\ \ldots,\ h_k$, такие, что любой элемент h из H линейно над полем F выражается через эти элементы, то есть уравнение

$$h = h_1 \cdot x_1 + h_2 \cdot x_2 + \ldots + h_k \cdot x_k$$

разрешимо в элементах $x_1, \ldots,\ x_k$, принадлежащих полю F.

Определение 2.4 Если при этом решение единственно, то указанный набор элементов называется *базисом поля H относительно поля F*, а число k элементов базиса называется *степенью конечного расширения поля H относительно поля F* и обозначается $k = [H : F]$.

Определение 2.5 Элементы $x_1, \ldots, x_k$ называются координатами элемента h относительно рассматриваемого базиса. Из следующей далее теоремы вытекает, что число элементов в базисе не зависти от выбора базиса, поэтому понятие степени расширения корректно определено.

Теорема 2.1 *Порядок конечного поля является степенью порядка любого его подполя.*

Доказательство. Сопоставим каждому элементу поля H вектор его координат относительно произвольного базиса над подполем F. Согласно определению это сопоставление взаимно однозначно. Число различных векторов координат равно числу элементов поля F в степени k.

Следствие 2.1 *Пусть H – конечное поле, содержащее подполе K, состоящее из q элементов. Тогда H состоит из q^m элементов, где $m = [H : K]$.*

Пример 2.4 Поле K комплексных чисел является конечным расширением степени 2 поля R действительных чисел, $[K : R] = 2$. Базисом поля комплексных чисел являются его элементы $h_1 = (1, 0) = 1 + 0i$ и $h_2 = (0, 1) = 0 + 1i$.

Пример 2.5 Поле $GF(2^2)$ является конечным расширением поля $GF(2)$ степени 2, значит $[GF(2^2) : GF(2)] = 2$. В качестве базиса $GF(2^2)$ можно выбрать элементы $h_1 = 1$ и $h_2 = x$, где x – корень в поле $GF(2^2)$ неприводимого многочлена $f(X) = 1 + X + X^2$ над полем $GF(2)$. Базис составляют также элементы x и $x^2 = 1 + x$.

Упражнение 2.1 Доказать, что если H – конечное расширение поля W, а поле W – конечное расширение поля F, то H – конечное расширение поля F, при этом $[H : F] = [H : W] \cdot [W : F]$.

Пример 2.6 Поле $GF(2)$ есть подполе поля $GF(2^2)$. Поле $GF(2^4)$ можно рассматривать как конечное расширение степени 2 поля $GF(2^2)$, которое, в свою очередь, является конечным расширением степени 2 поля $GF(2)$. При этом $[GF(2^4) : GF(2)] = GF(2^4) : GF[2^2] \cdot [GF(2^2) : GF(2)]$.

Теорема 2.2 *Пусть F_q – конечное поле и $F_q(\theta)$ – его простое конечное расширение. Тогда $F_q(\theta)$ является простым алгебраическим расширением поля F_q.*

Теорема 2.3 *Любой элемент α простого алгебраического расширения $F(\theta)$ степени n поля F однозначно представим в виде*

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}, \tag{3}$$

где θ корень в $F(\theta)$ некоторого неприводимого многочлена степени n над полем F.

Следствие 2.2 *Если $F = F_q$, H есть кольцо $F_q[X]/(f(X))$ многочленов по модулю многочлена $(f(X))$, $\theta \equiv x(\mathrm{mod} f(X))$,$\theta \in H$, где многочлен $f(X)$ неприводим над полем F_q, а x – его корень в поле H, то расширение $F(\theta)$ является простым алгебраическим расширением и совпадает с полем H.*

Следствие 2.3 *Всякое простое алгебраическое расширение поля F степени n является конечным расширением поля F степени n.*

Следствие 2.4 *Множество* (**??**) *составляет базис поля $F(\theta)$.*

В качестве еще одного следствия получается

Теорема 2.4 *Пусть F_q – конечное поле и $f(X)$ – неприводимый многочлен степени n над этим полем. Тогда кольцо $F_q[X]/(f(X))$ многочленов по модулю многочлена $f(X)$ является конечным полем порядка q^n, в котором класс x вычетов (класс конгруэнтности), содержащий многочлен X, является корнем многочлена $f(X)$. Это поле содержит в себе поле, изоморфное F_q, в качестве подполя.*

Из этой теоремы и доказанного в следующем разделе существования неприводимых многочленов над полем F_q любой заданной степени вытекает существование полей порядка любой степени простого числа.

3 След элемента конечного поля

Определение 3.1 Пусть $P = F_q$, $K = F_{q^m}$ и $\alpha \in K$. *След* $\mathrm{Tr}_{K/P}(\alpha)$ элемента α из поля K в поле P определяется равенством

$$\mathrm{Tr}_{K/P}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Если P – простое подполе поля K, то $\mathrm{Tr}_{K/P}$ называется *абсолютным следом* элемента α и обозначается $\mathrm{Tr}_K(\alpha)$.

Пример 3.1 Пусть $P = F = GF(2)$, $K = GF(2^2)$. Тогда

$$Tr_K(0) = 0,\ Tr_K(1) = 1 + 1 = 0,\ Tr_K(\theta) = \theta + \theta^2 = 1,$$
$$Tr_K(1 + \theta) = (1 + \theta) + (1 + \theta)^2 = 1.$$

Определение 3.2 *Характеристическим многочленом* элемента α над полем P называется многочлен $g(X) = f(X)^{m/d}$, где $f(X)$ – минимальный многочлен элемента α над полем P, $d -$ степень многочлена $f(X)$.

Теорема 3.1 *След* $\mathrm{Tr}_{K/P}$ *осуществляет линейное отображение из поля* K *в подполе* P.

Доказательство. Корнями многочлена $f(X)$ являются элементы

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}.$$

Корнями многочлена $g(X)$ в поле K являются те же элементы, взятые с кратностью m/d. Отсюда

$$\begin{aligned} g(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X_1 + a_0 = \\ = (X-\alpha)(X-\alpha^q)\ldots(X-\alpha^{q^{m-1}}). \end{aligned} \tag{4}$$

Сравнение коэффициентов дает $\mathrm{Tr}_{K/P}(\alpha) = -a_{m-1}$. Получаем, что след $\mathrm{Tr}_{F/P}(\alpha)$ всегда является элементом поля P. Имеют место равенства

$$\begin{aligned} &\mathrm{Tr}_{K/P}(x+y) = \mathrm{Tr}_{K/P}(x) + \mathrm{Tr}_{K/P}(y), \\ &\mathrm{Tr}_{K/P}(\alpha x) = \alpha \mathrm{Tr}_{K/P}(x), x, y \in K, \alpha \in P \end{aligned}.$$

4 Алгоритмическое представление конечного поля

Алгоритмически поле Галуа $GF(q^n)$ удобно описывать, имея в виду его представление в виде фактор-кольца $F_q[X]/f(X)$ кольца $F_q[X]$ многочленов над полем F_q по модулю некоторого неприводимого многочлена $f(X)$ степени n над полем F_q. Это представление равносильно представлению поля F_{q^n} как алгебраического расширения $F_q(\theta)$ поля F_q степени n, где θ – корень многочлена $f(X)$ в $GF(q^n)$,

Элементы поля представляются упорядоченными наборами $\alpha = (a_0, a_1, a_2, \ldots, a_{n-1})$ коэффициентов многочленов $\alpha(X)$, представляющих классы $[\alpha(X)]_{\mathrm{mod}\ f(X)}$, они же – коэффициенты полиномиальных выражений $\alpha(\theta)$, определяющих элементы расширения $F_q(\theta)$ поля F_q.

Операция сложения в поле F_{q^n} определяется как покомпонентное сложение указанных векторов с использованием аддитивной операции поля F_q :

$$< a_0, a_1, \ldots, a_{n-1} > + < b_0, b_1, b_2, \ldots, b_{n-1} >=$$
$$=< a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1} >,$$

то есть как набор коэффициентов суммы многочленов

$$\alpha(X) = \sum_{i=0}^{n-1} a_i X^i, \beta(X) = \sum_{i=0}^{n-1} b_i X^i, \alpha(X) + \beta(X) = \sum_{i=0}^{n-1} (a_i + b_i) X^i.$$

Определить произведение

$$< a_0, a_1, a_2, \ldots, a_{n-1} > \cdot < b_0, b_1, b_2, \ldots, b_{n-1} >$$

элементов $\alpha =< a_0, a_1, \ldots, a_{n-1} >$ и $\beta =< b_0, b_1, \ldots, b_{n-1} >$ в поле F_{q^n} можно двумя эквивалентными способами:

1) по теореме о делении с остатком

$$\alpha(X)\beta(X) = f(X)q(X) + \rho(X), \ \deg \rho(X) < n,$$

где $\rho(X) =\mathrm{rem}(\alpha(X) \times \beta(X), f(X))$ откуда

$$\alpha\beta = fq + \rho = \rho = (c_0, c_1, \ldots, c_{n-1}), \tag{5}$$

где f, q и ρ – наборы коэффициентов многочленов $f(X),\ q(X)$ и $\rho(X)$ (вектор ρ определяет класс эквивалентности, которому принадлежит произведение многочленов над полем $GF(q)$)

2) подставкой вместо формальной переменной X корня x неприводимого многочлена $f(X)$ в равенство 5. При этом $\alpha(x) \times \beta(x) = f(x)q(x) + \rho(x) = \rho(x)$, так как $f(x) = 0$.

Таким образом, произведение

$$< a_0, a_1, a_2, \ldots, a_{n-1} > \cdot < b_0, b_1, b_2, \ldots, b_{n-1} >$$

элементов α и β в поле F_{q^n} представляется вектором

$$\sigma =< c_0, c_1, c_2, \ldots, c_{n-1} >,$$

который можно вычислить как набор коэффициентов коэффициентов многочлена $\rho(X) = \mathrm{rem}(\alpha(X)\beta(X), f(X))$, получающегося как остаток при делении произведения многочленов

$$\alpha(X)\beta(X) = \sum_{k=0}^{2n-2} \sum_{i+j=k} a_i b_j X^k,$$

на многочлен $f(X)$. Операцию нахождения этого остатка называют иногда приведением по модулю $f(X)$.

5 Поле Галуа как векторное пространство

Векторное пространство над полем Галуа. Определим $n-$мерное векторное пространство над полем Галуа $GF(q)$ как множество векторов

$$\mathbf{a} = (a_1, \ldots, a_i, \ldots, a_n)$$

длины n, состоящих из элементов поля. Операция сложения векторов определяется как покомпонентное сложение по правилам сложения в поле $GF(q)$. Операция умножения вектора $\mathbf{a}$ на на произвольный элемент α (скаляр) поля $GF(q)$ определяется равенством:

$$\alpha \cdot \mathbf{a} = (\alpha a_1, \ldots, \alpha a_i, \ldots, \alpha a_n).$$

Используя свойства операций в поле $GF(q)$, легко проверить, что данное определение корректно, то есть удовлетворяет всем аксиомам общего определения векторного пространства: операция сложения коммутативна и ассоциативна, имеет нулевой элемент, для любого вектора $\mathbf{a}$ существует противоположный вектор $\mathbf{b}$ такой, что $\mathbf{a} + \mathbf{b} = \mathbf{0}$, умножение на единицу поля $GF(q)$ не приводит к изменению вектора, умножение на скаляр ассоциативно $(\alpha(\beta\mathbf{a})) = ((\alpha \cdot \beta)\mathbf{a})$, дистрибутивно относительно векторного множителя и дистрибутивно относительно скалярного множителя

$$(\alpha + \beta) \cdot \mathbf{a} = \alpha \cdot \mathbf{a} + \beta \cdot \mathbf{a}, \alpha(\mathbf{a} + \mathbf{b}) = \alpha \cdot \mathbf{a} + \alpha \cdot \mathbf{b}.$$

Как и в общем случае, выражение

$$\alpha_1 \mathbf{e_1} + \cdots + \alpha_i \mathbf{e_i} + \cdots + \alpha_n \mathbf{e_n}$$

называется *линейной комбинацией* векторов $\mathbf{e_1}, \ldots, \mathbf{e_i}, \ldots, \mathbf{e_n}$ с коэффициентами

$$\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n.$$

Если хотя бы один из коэффициентов отличен от нуля, то линейная комбинация называется *нетривиальной* . Векторы $\mathbf{e_1}, \ldots, \mathbf{e_i}, \ldots, \mathbf{e_n}$ называются *линейно зависимыми* , если существует хотя бы одна их нетривиальная комбинация, равная нулю, иначе векторы называются *линейно независимыми*. Векторное пространство называется n-мерным, если существует n линейно независимых векторов, а любые $n+1$ векторов линейно зависимы. Любые n линейно независимых векторов n-мерного векторного пространства образуют его *базис* . Если $\mathbf{e_1}, \ldots, \mathbf{e_i}, \ldots, \mathbf{e_n}$ есть базис векторного пространства, то любой вектор представим линейной комбинацией базисных векторов.

Очевидно, что поле $GF(q^n)$ можно рассматривать как n-мерное векторное пространство над полем $GF(q)$. Базисы такого векторного пространства иногда называют *базисами поля* $GF(q^n)$.

Полиномиальные и нормальные базисы. Пусть задан неприводимый многочлен $p(X)$ над простым полем $GF(p)$ степени n. Характеристика этого поля есть p. Тогда конечное расширение $GF(p)(x) = GF(p^n)$ степени n поля $GF(p)$, где x – корень многочлена $p(X)$, можно рассматривать как векторное пространство размерности n. По следствию 2.4, множество элементов

$$1,\ x,\ x^2,\ \ldots,\ x^{n-1}$$

составляет базис n-мерного векторного пространства и одновременно базис поля $GF(p^n)$. Действительно, это множество линейно независимо и позволяет представить любой элемент

$$q(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{n-1}x^{n-1}. \tag{6}$$

из $GF(2^n)$.

Этот базис называется *полиномиальным* или *стандартным* базисом и обозначается далее S. Он определяется неоднозначно, так как зависит от выбора неприводимого многочлена (определяющего базис). Формально базис зависит также от выбора корня этого многочлена, но легко видеть что правило умножения в этом базисе не зависит от выбора корня.

Базисом поля $GF(p^n)$ может оказаться также множество сопряженных с элементом поля x элементов

$$\{x,\ x^p,\ x^{p^2}, \ldots, x^{p^{n-1}}\}.$$

Это множество называется *нормальной* системой (множеством).

Все элементы этой системы различны, поскольку они являются корнями неприводимого многочлена $p(x)$, и если они окажутся линейно независимыми, то любой элемент поля $GF(p^n)$ можно будет представить линейной комбинацией

$$a = a_0 x + \ a_1 x^p + \ a_2 x^{p^2} + \cdots + \ a_{n-1} x^{p^{n-1}} = \sum_{i=0}^{n-1} a_i x^{p^i}.$$

Тогда это множество называется *нормальным* базисом поля $GF(2^n)$ и обозначается N.

Теорема 5.1 *В любом поле $GF(p^n)$ существует*

$$\frac{(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})}{n!}$$

различных базисов, из них

$$I_p(n) = \sum_{d|n} \mu(d) p^{n/d}$$

полиномиальных базисов. Количество нормальных базисов равно

$$\frac{1}{n} p^n \prod_{d|m} \left(1 - p^{-o_d(p)}\right)^{\varphi(d)/o_d(p)},$$

где $n = p^a m$, m не кратно p, $o_d(p)$ минимальное натуральное число o, такое, что $p^o - 1$ кратно d.

Пример 5.1 Число нормальных базисов в поле $GF(2^6)$ равно

$$\frac{1}{6} 2^6 \left(1 - 2^{(-1)}\right)\left(1 - 2^{-2)}\right) = 4$$

так как $\varphi(3) = 2 = o_3(2)$.

Если один нормальный базис $\{x_1, \ldots, x_n\}$ в поле $GF(p^n)$ известен, то все остальные можно выразить через него в явном виде путем умножения на *невырожденную циркулянтную матрицу* $(c_{i,j})$, $c_{i,j} = c_{i+1 \bmod n, j+1 \bmod n}$, т.е. такую,

у которой каждая следующая строка получается из предыдущей циклическим сдвигом вправо. Подсчитывая число таких матриц, отсюда можно получить формулу для числа нормальных базисов теоремы 5.1. Несмотря на наличие такой формулы и на довольно большую вероятность случайно выбранного элемента x порождать нормальный базис, явной конструкции нормальных базисов для любой размерности, видимо, не известно.

Замечательно, что в нормальном базисе возведение в степень характеристики поля p равносильно циклическому сдвигу векторного представления элемента поля (учитывая, что $x^{p^n} = x$):

$$a^p = (a_0 x + \ a_1 x^p + \ a_2 x^{p^2} + \ldots + \ a_{n-1} x^{p^{n-1}})^p =$$

$$= a_0 x^p + \ a_1 x^{p^2} + \ a_2 x^{p^3} + \ldots + \ a_{n-2} x^{p^{n-1}} + \ a_{n-1} x^{p^n} =$$

$$= a_{n-1} x + a_0 x^p + \ a_1 x^{p^2} + \ a_2 x^{p^3} + \ldots + \ a_{n-2} x^{p^{n-1}}.$$

Таким образом,

$$a^p = (a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1})^p = (a_{n-1}, a_0, a_1, a_2 \ldots, a_{n-2}).$$

В нормальном базисе также очень просто вычислять след элемента a, $a \in GF(p^n)$: значение $\mathrm{Tr}(a) = a + a^p + a^{p^2} + \ldots + a^{p^{n-1}}$ равно сумме элементов вектора a, умноженного на сумму базисных векторов Действительно, рассмотрим матрицу, строками которой являются элементы a, a^p, $a^{p^2}, \ldots,$ $a^{p^{n-1}}$. Её столбцами являются те же векторы, так как $j-$й столбец представляет собой циклический сдвиг на j позиций первого столбца. Следовательно, сумма строк матрицы есть вектор с компонентами, равными сумме компонент вектора a.

Пример 5.2 Вычислим след $Tr(10110)$ элемента (10110) поля $GF(2^5)$.

$$\begin{aligned} a &= 10110 \\ a^2 &= 01011 \\ a^{2^2} &= 10101 \\ a^{2^3} &= 11010 \\ a^{2^4} &= 01101 \end{aligned}$$

Сумма строк равна $(1, 1, 1, 1, 1)$, то есть $Tr(10110) = 1$.

Вычисление следа в полиномиальном базисе несколько сложнее, но может быть ускорено за счёт предварительного вычисления так называемого вектора следа. Рассмотрим только случай бинарного поля. Составим матрицу, строками которой являются представленные в полиномиальном базисе элементы x^0, x^1, x^2, x^{n-1}, x^n, $\ldots$, x^{2n-2}.

Пример 5.3 В поле $GF(2^5)$, порождаемом неприводимым многочленом $x^5 + x^2 + 1$, такая матрица имеет вид

$$\begin{aligned} x^0 &= 10000 \\ x^1 &= 01000 \\ x^2 &= 00100 \\ x^3 &= 00010 \\ x^4 &= 00001 \\ x^5 &= 10100 \\ x^6 &= 01010 \\ x^7 &= 00101 \\ x^8 &= 10110 \end{aligned}$$

Элементы $t_i,\ i = 0, \ldots, n-1$ вектора следа $(t_0, \ldots,\ t_{n-1})$ образуются суммированием по модулю два элементов матрицы, расположенных по диагонали (слева направо и сверху вниз) в соседних векторах $a_i,\ a_{i+1}, \ldots, a_{i+n-1}$. Например, $t_0 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1$. Вектор следа следующий: $(t_0, t_1, t_2, t_3, t_4) = (1, 0, 0, 1, 0)$. Значение функции следа для элемента a поля $GF(2^n)$ равно сумме (дизъюнкции) элементов вектора, получаемого как поразрядное произведение (конъюнкция) элементов вектора a и вектора следа.

Пример 5.4 Вычислим значение функции следа элемента $a = (0 \cdot x^0, 1 \cdot x^1, 1 \cdot x^2, 0 \cdot x^3, 1 \cdot x^4)$. Найдем покомпонентное произведение вектора следа и векторного представления элемента $a = (01101)$:

$$(t_0, t_1, t_2, t_3, t_4)\&(01101) = (10010)\&(01101) = (00000).$$

Сумма элементов полученного вектора равна 0. След элемента (11100) является суммой элементов вектора $(10010)\&(11100) = (10000)$, т.е. $Tr(11100) = 1$.

Умножение в полиномиальном базисе выполняется, как описано в предыдущем разделе, а именно, путем умножения многочленов над полем Галуа и последующего приведения полученного результата по модулю неприводимого многочлена, порождающего этот базис.

Умножение в нормальном базисе выполняется по правилам умножения многочленов

$$p(x) \cdot s(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{p^i} x^{p^j},$$

где $p(x) = a_0 x + a_1 x^p + \cdots + a_{n-1} x^{p^{n-1}}$, $s(x) = b_0 x + b_1 x^p + \cdots + b_{n-1} x^{p^{n-1}}$, при этом приведения результата по модулю неприводимого многочлена не требуется. В

то же время слагаемые

$$c_{i,j} = a_i b_j x^{p^i} x^{p^j}$$

в указанной двойной сумме в общем случае не являются элементами нормального базиса, и должны представляться как линейные комбинации элементов базиса. Это усложняет операцию умножения в нормальном базисе по сравнению с операцией умножения в полиномиальном базисе.

Методы умножения, возведения в степень и инвертирования в нормальных базисах рассматриваются частично в разделе 7 и более подробно в четвертой главе.

6 Проверка, является ли нормальная система базисом. Переход от нормального базиса к стандартному.

Пусть $\{x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}\}$ — нормальная система элементов поля $GF(p^n)$, где x – корень неприводимого многочлена $f(X)$. Для проверки того, образует ли она базис в этом поле, достаточно выяснить, является ли она линейно независимой над полем $GF(p)$. Для этого можно вычислить коэффициенты $a_{i,j}$ разложения элементов x^{p^i} по тому базису поля $GF(p^n)$, который используется в рассматриваемом представлении этого поля, и проверить $n \times n$ матрицу $(a_{i,j})$ на вырожденность.

Для вычисления матрицы $(a_{i,j})$ можно использовать алгоритм вычисления последовательности $X, X^p, \ldots, X^{p^{n-1}}$ по модулю неприводимого многочлена $p(X)$, соответствующего полиномиальному базису рассматриваемого представления поля. Строки $(a_{i,j})$ образуются как последовательности коэффициентов многочлена $X^{p^i} rm\ mod\ f(X)$. При использовании в качестве $p(X)$ многочлена с малым числом одночленов (то есть многочлена малого веса) сложность этого вычисления будет $O(n^2 \log_2^2 p)$. Если же удается пользоваться представлением поля $GF(p^n)$ с помощью нормального базиса, то указанная сложность равна нулю.

Матрица будет $(a_{i,j})$ вырожденной тогда и только тогда, когда соответствующая ей система линейных уравнений с нулевой правой частью имеет ненулевое

решение. Базис будет нормальным, если и только если эта матрица невырождена. Конечно, матрица будет вырожденной, если элементы последовательности $\{x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}\}$ циклически повторяются. В противном случае для решения системы можно применить метод Гаусса, имеющий оценку сложности $O(n^3)$. В случае $p = 2$ работу этого алгоритма можно ускорить в 32 раза, если при выполнении элементарных преобразований столбцов матрицы представлять их в виде векторов из $n/32$ длинных целых чисел и для сложения столбцов по модулю два применять операцию XOR с длинными целыми числами. Объем используемой памяти при этом тоже уменьшается в 32 раза.

Опишем указанный алгоритм в применении к бинарному случаю более подробно. В стандартном базисе $S = \{1, x, x^2, \ldots, x^{n-1}\}$ любой элемент поля $GF(2^n)$ выражается некоторой линейной комбинацией элементов базиса S – бинарным вектором длиной n.

Элементы базиса соответствующего нормального базиса N как наборы из n таких векторов составляют бинарную матрицу M размером $n \times n$, которую можно компактно представить таблицей $R(T)$ размером $n \times k$, если элементы базиса N задавать наборами $t_1, t_2, \ldots t_k,\ k = \lceil \frac{n}{s} \rceil$ целых неотрицательных чисел, представляющих машинными словами длины s в совокупности все коэффициенты бинарного вектора.

Покажем, как определить такие наборы и построить таблицу $R(T)$ для элементов множества N.

Для элемента x (многочлена X) соответствующий набор имеет вид $0, 1, 0, \ldots, 0$. Пусть $t_1, t_2, \ldots t_k$ - набор чисел, задающих элемент x^{2^i} (многочлен X^{2^i}). Рассмотрим элементарные многочлены $t_j(x), \quad j = 1, 2, \ldots, k$, задаваемые числами $t_j, \quad j = 1, 2, \ldots, k$. Тогда для многочлена $g(X) = \sum_{j=1}^{n} t_j X^{s(j-1)}$ имеем $X^{2^i} \equiv g(X) \pmod{p(X)}$. Умножив многочлен $g(X)$ на себя и взяв остаток от деления результата на многочлен $p(X)$, получим набор чисел $t'_1, t'_2, \ldots t'_n$ задающих многочлен $X^{2^{i+1}}$. Последовательность его коэффициентов задает элемент $x^{2^{i+1}}$ в стандартном базисе.

Рассмотрим таблицу $R(T)$ с n строками и k столбцами, $(i+1)$-я строка которой, читаемая слева направо, совпадает с набором чисел $t_1, t_2, \ldots t_k$, задающих многочлен x^{2^i} в стандартном базисе $i = 0, 1, \ldots, n-1$.

Легко видеть, что множество N является базисом в точности тогда, когда

матрица из нулей и единиц, соответствующая таблице $R(T)$, невырождена.

По таблице $R(T)$ можно построить таблицу $C(T)$, представляющую матрицу M аналогичным образом, но в виде, когда слова длины s составляются из элементов столбцов матрицы M.

Упражнение 6.1 Покажите, как построить таблицу $C(R)$ по таблице $R(T)$, не прибегая к преобразованию последней в бинарную форму матрицы M.

Матрица M и, соответственно, таблица $C(R)$ задают переход от системы координат, определяемой нормальным базисом к системе координат в стандартном базисе (далее такая матрица и таблица называются матрицей и таблицей перехода от нормального базиса к стандартному). Пусть $(t_1, \ldots, t_k)$ компактное представление элемента поля в нормальном базисе. Тогда бинарное представление этого элемента в стандартном базисе получается вычислением произведения

$$(t_1, \ldots, t_k) \times C(R)$$

и заменой его элементов (слов длины s) нулем при четном числе единиц в слове и единицей при нечетном числе 1 в нем.

Пример 6.1 Пусть $n = 3, \quad s = 2$. Рассмотрим неприводимый многочлен $p(X) = 1+X^2+X^3$. Далее,

$$X \equiv X \pmod{p(X)}, X^2 \equiv X^2 \pmod{p(X)},$$

$$X^4 = 1 + X + X^2 + (1 + X)p(X) \equiv 1 + X + X^2 \pmod{p(X)}.$$

Матрица перехода от нормального базиса к стандартному имеет вид

$$M = \begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1. \end{matrix}$$

Матрица M невырождена. Поэтому элементы x, x^2, x^4, где x – корень многочлена $p(X)$ образуют нормальный базис. Рассмотрим элемент $a = x^2+x^4$, заданный в нормальном базисе. Тогда имеет место равенство $v = (0, 1, 1)$. Умножая вектор v на матрицу M, получим вектор $v' = (1, 1, 0)$. Поэтому в стандартном базисе элемент a представляется в виде $1 + x$.

Этот пример можно проследить дальше, если при $s = 2$ преобразовать матрицу M к таблице $T = R(M)$,

$$T = \begin{matrix} 0 & 2 \\ 0 & 1 \\ 1 & 3, \end{matrix}$$

а вектор v к таблице $R(v) = (03)$. Таблицу $R(M)$ преобразуем в таблицу

$$C(M) = \begin{matrix} 0 & 1 & 0 \\ 1 & 1 & 3 \end{matrix}$$

Результатом умножения таблицы $R(v) = (0, 3)$ на таблицу $C(M)$, является таблица (1 1 3), что соответствует (после замены слов бинарными символами) бинарному вектору v' =(1,1,0), или элементу $1 + x$.

7 Переход от стандартного базиса к нормальному.

Пусть таблица $C(M)$ представляет невырожденную бинарную матрицу M перехода от нормального базиса к стандартному, т.е. нормальная система является базисом. В этом случае построим таблицу $C(M)'$, представляющую бинарную матрицу M^{-1}, обратную к M. Рассмотрим набор $u = (t'_1, t'_2, \ldots t'_k)$ целых неотрицательных чисел, который задает элемент a поля $GF(2^n))$ в стандартном базисе$a = \sum_{i=1}^{n} a_i x^{i-1}, \quad a_i \in \{0, 1\}$. Тогда произведение вектор-строки u на таблицу T' задает этот же элемент, но уже в нормальном базисе.

Пример 7.1 Пусть многочлен $p(x)$ и матрица M такие же, как и в предыдущем примере. Для матрицы M^{-1} обратной к M, имеем

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{matrix} .$$

Найдем, например, представление в нормальном базисе элемента $1+x$, заданного в стандартном базисе. Для этого умножим вектор-строку $v' = (1, 1, 0)$ на матрицу M^{-1}. Получим строку $v = (0, 1, 1)$, соответствующую представлению $x^2 + x^4$ элемента a в нормальном базисе.

Если умножить таблицу (12), соответствующую при $s = 2$ вектор-строке $v' = (1, 1, 0)$, на таблицу $C(M)'$,

$$\begin{matrix} 1 & 1 & 1 \\ 2 & 1 & 0 \end{matrix} ,$$

задающую матрицу M^{-1}, то получается таблица (311). По ней определим бинарный вектор v =(0,1,1) который в нормальном базисе задает элемент $x^2 + x^4$.

Оптимальные и гауссовы нормальные базисы Для оптимизации времени умножения или схемной реализации умножения в нормальных базисах

используют оптимальные или близкие к ним гауссовы нормальные базисы. Оптимальные нормальные базисы были обнаружены Mullin, Onyszchuk, Vanstone, Wilson. Они удачно могут быть использованы в мультиплере (схеме умножения), запатентованном в 1985 г. Massey и Omura.

Сложностью C_B произвольного нормальъного базиса

$$B = \{x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}\}$$

называется число ненулевых элементов в матрице T, i-я строка которой есть вектор коэффициентов элемента xx^{q^i} поля $GF(q^n)$ относительно базиса B, то есть

$$xx^{q^i} = \sum_{j=0}^{n-1} t_{i,j} x^{q^j}.$$

В соответствии с этим определением, сложность нормального базиса можно найти следующим образом. Пусть после проверки матрицы $M = (m_i(x))$ на предмет того, является ли базисом соответствующая нормальная система, построена матрица M^{-1} перехода от стандартного базиса к нормальному. Построим матрицу $T = (t_i(x))$, строки которой вычисляются следующим образом: $t_i(x) = (xm_i(x)M^{-1})$. (Здесь xm_i – произведение в поле $GF(2^n)$). Находим сложность нормального базиса, подсчитав число единиц в полученной матрице.

Определение сложности нормального базиса мотивируется следующим алгоритмом умножения в нормальном базисе B (алгоритмом Massey-Omura):
пусть

$$\xi = \sum_{i=0}^{n-1} x_i x^{q^i}, \quad \zeta = \sum_{j=0}^{n-1} y_j x^{q^j},$$

произвольные элементы поля $GF(q^n)$, разложенные по нормальному базису B, тогда их произведение можно вычислить по формуле:

$$\pi = \xi\zeta = \sum_{i,j=0}^{n-1} x_i y_j x^{q^j+q^i} = \sum_{i,j=0}^{n-1} x_i y_j x^{(q^{i-j}+1)q^j},$$

где разность $i - j$ вычисляется по модулю n, а так как

$$x^{(q^{i-j}+1)q^j} = \left(x^{q^{i-j}+1}\right)^{q^j} = \left(\sum_{k=0}^{n-1} t_{i-j,k} x^{q^k}\right)^{q^j} =$$

$$= \sum_{k=0}^{n-1} t_{i-j,k} x^{q^{k+j}} = \sum_{m=0}^{n-1} t_{i-j,m-j} x^{q^m} ,$$

где разность $m-j$ и сумма $k+j$ тоже вычисляются по модулю n, то

$$\pi = \sum_{m=0}^{n-1} p_m x^{q^m} ,$$

где

$$p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j$$

некоторая билинейная форма над полем $GF(q)$.

Так как при возведении элементов ξ, ζ в степень q происходит циклический сдвиг переменных в каждом из векторов $x_i, i = 1, \ldots, n$ и $y_j, = 1, \ldots, n$ на одну позицию вправо, а $\pi^q = \xi^q \zeta^q$, то координаты элемента π^q вычисляются по формулам $P_i = p_i(S(x), S(y))$. Но при возведении элемента π в степень q происходит такой же циклический сдвиг координат , т.е. координата p_i переходит в координату $p_{i+1 \bmod n}$, значит $p_{i-1 \bmod n}(x,y) = p_i(S(x), S(y)), i = 0, \ldots n-1$ откуда следует, что $p_{i-k \bmod n}(x,y) = p_i(S^k(x), S^k(y)), i = 0, \ldots n-1$ т.е. все остальные формы формы получаются из формы p_0 по формуле $p_{m \bmod n}(x,y) = p_0(S^{n-m}(x), S^{n-m}(y)), k = 1, \ldots, n-1$ где S^{n-m} – операция циклического сдвига координат вектора вправо на $n-m$ позиций, или, что равносильно, влево на m позиций. Этот сдвиг можно явно определить формулой

$$S^{n-m}(x_0, \ldots, x_{n-1}) = (x_m, \ldots, x_{n-1}, x_0, \ldots x_{m-1}) = \\ (x_{i+m \bmod n}, i = 0, \ldots, n-1) .$$

Определив матрицу A равенствами $a_{i,j} = t_{i-j,-j}$, где $i-j$ и $-j$ вычисляются по модулю n, замечаем, что предыдущую формулу можно переписать в виде

$$p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j = p_0(S^{n-m}(x), S^{n-m}(y)) ,$$

где

$$p_0(x,y) = A(x,y) = \sum_{i,j=0}^{n-1} a_{i,j} x_i y_j .$$

Матрица A симметрическая, и число ее ненулевых элементов, а также их сумма такие же, как и у матрицы T. Для вычисления билинейной формы $A(x,y)$

достаточно выполнить $2C_B$ умножений и $n-1$ сложений в поле $GF(q)$. Если пренебречь временем выполнения циклических сдвигов, то сложность выполнения умножения над нормальным базисом поля $GF(q^n)$ оценивается сверху как $n(2C_B+n-1)$ операций в поле $GF(q)$, что видно из следующей формулы: $\xi\zeta =$

$$= A(\xi,\zeta)x + A(\xi^{q^{n-1}},\zeta^{q^{n-1}})x^q + A(\xi^{q^{n-2}},\zeta^{q^{n-2}})x^{q^2} + \cdots + \ A(\xi^q,\zeta^q)x^{q^{n-1}}.$$

Таким образом, сложность умножения зависит только от количества ненулевых элементов C_B в матрице A.

Упражнение 7.1 Докажите, что в случае $q = 2$ сложность умножения оценивается как $n(C_B + n - 1)$.

Матрица A («таблица умножения» в базисе B) однозначно определяет операцию умножения в рассматриваемом поле.

О сложности нормальных базисов известно следующая

Теорема 7.1 *Для любого нормального базиса B поля $GF(q^n)$ его сложность C_B не меньше $2n-1$. Более того, если $q = 2$, то сложность – нечетна.*

Нормальные базисы, для которых достигается эта граница, называют *оптимальными* .

Упражнение 7.2 Докажите эту теорему

Известны нормальные базисы B, у которых функция сложности C_B является линейной. Стандартный алгоритм умножения для таких базисов имеет квадратичную оценку сложности. Эти базисы, получившие название *гауссовых нормальных базисов* (ГНБ).

Более подробно о полях и их конечных расширениях см. монографию [1] и учебное пособие [2].

8 Контрольный вопросы

1. Как определяется кольцо многочленов над конечным полем?

1. Какое поле называется простым?

2. Как определяется расширение поля?

3. В каком случае расширение конечного поля называется алгебраическим расширение определенной степени?

4. Каковы особенности конечного поля как векторного пространства?

5. Как определяется след элемента поля. Каковы свойства этой функции

6. Что такое нормальное множество и как тестируется свойство базисности такого множества?

7. Назовите два типа базисов конечного поля.

Литература

1. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М: Комкнига, 2007.

2. Болотов А.А., Гашков С.Б., Фролов А.Б. Криптографические протоколы на эллиптических кривых. – М: Издательский дом МЭИ, 2007.