
Лекция №8 (05.11.20)

---

3. Нормальные базисы.

3.2. Арифметика в представлении нормальных базисов.

Обозначим $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$. Если $\xi \in E$, то $\xi = x_0\alpha + x_1\alpha^q + \ldots + x_{n-1}\alpha^{q^{n-1}}$, где α – образующая нормального базиса в расширении E/F. Очевидно, что сложение элементов при таком представлении – тривиально. Вычисляя образ элемента ξ относительно действия автоморфизма Фробениуса σ, то есть $\sigma(\xi)$ – q-ю степень ξ, осуществляется циклический сдвиг координат вправо

$$\xi^q = x_{n-1}\alpha + x_0\alpha^q + x_1\alpha^{q^2} + \ldots + x_{n-2}\alpha^{q^{n-1}}.$$

Аналогично, образ ξ относительно σ^{-1} есть циклический сдвиг координат влево

$$\xi^{q^{n-1}} = x_1\alpha + x_2\alpha^q + \ldots + x_{n-2}\alpha^{q^{n-2}} + x_0\alpha^{q^{n-1}}.$$

Покажем, как можно использовать нормальный базис для существенного уменьшения числа умножений, необходимых для вычисления степени и обратного элемента. Следующий алгоритм дает стандартный метод вычисления экспонент.

Алгоритм 1 (Возведение в квадрат и умножение)**. Ввод:** *Элемент b, экспонента e.*
Вывод: $x = b^e$.
(1) $x := 1$, $y := b$, $c := e$.
(2) While $c > 0$ do
(3) If c – *нечетно*
(4) Then $x := xy$, $c := c - 1$
(5) Else $y := y^2$, $c := \frac{c}{2}$.
(6) Fi
(6) Od

Как много умножений необходимо выполнить с помощью этого алгоритма? Если представить величину c в бинарном виде, то есть

$$c = (c_{k-1}, \ldots, c_0), \quad \text{где} \quad c = 2^{k-1}c_{k-1} + \ldots + 2c_1 + c_0,$$

то выбор шага (4) или (5) зависит от того $c_0 = 1$ или $c_0 = 0$. В первом случае необходимо одно умножение, и тогда c можно заменить на $c' := c - 1$. Отметим, что бинарное представление c' получено посредством замены последнего бита c_0 на 0. Во втором случае необходимо одно возведение в квадрат, и тогда можно заменить $c' := \frac{c}{2}$. При этом бинарное представление c' получено посредством отбрасывания последнего бита c_0. Эти замечания показывают, что нам потребуются в точности $s = [\log_2 e - 1]$ возведений в квадрат на шаге (5), а число умножений на шаге (4) равно числу единиц в бинарном представлении e. Приблизительно требуется $s/2$ умножений и s возведений в квадрат.

Теперь перейдем к изучению умножения в представлении нормальным базисом. Рассмотрим второй элемент

$$\eta = y_0\alpha + y_1\alpha^q + \ldots + y_{n-1}\alpha^{q^{n-1}}.$$

Получаем

$$\pi = \xi \cdot \eta = \sum_{i,j=0}^{n-1} \alpha^{q^i}\alpha^{q^j}x_iy_j = \sum_{i,j=0}^{n-1} \alpha^{q^i+q^j}x_iy_j = \sum_{i,j=0}^{n-1} (\alpha^{q^{i-j}+1})^{q^j}x_iy_j.$$

Тогда

$$\alpha \cdot \alpha^{q^m} = \alpha^{q^m+1} := \sum_{k=0}^{n-1} \alpha^{q^k}t_{mk}.$$

Осуществляя подстановку, получаем следующее уравнение

$$\pi = \xi \cdot \eta = \sum_{i,j,k=0}^{n-1} \alpha^{q^{k+j}}t_{i-j,k}x_iy_j = \sum_{i,j,m=0}^{n-1} \alpha^{q^m}t_{i-j,m-j}x_iy_j.$$

Обозначим матрицу $T = (t_{ij})_{i,j\in[0,\ldots,n-1]}$. Коэффициенты в последнем разложении по базису имеют вид

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

Тогда коэффициент при $\alpha^{q^{m+1}}$ равен

$$p_{m+1} = \sum_{i,j=0}^{n-1} t_{i-j,m+1-j}x_iy_j = \sum_{i,j=0}^{n-1} t_{i-j,m-j}x_{i+1}y_{j+1}.$$

Отметим, что p_{m+1} также равен коэффициенту при $\alpha^{q^{m-1}}$ в представлении $\pi = \xi \cdot \eta$ при циклическом сдвиге координат на одну позицию слева.

Пример 1. *Пусть α – корень примитивного многочлена*

$$f(X) = X^5 + X^4 + X^2 + X + !$$

над $\mathbb{F}_2$. Вычислим представления для произведения сопряженных элементов с α:

$$\alpha^3 = \alpha + \alpha^8,\ \alpha^5 = \alpha^8 + \alpha^{16},\ \alpha^9 = \alpha^2 + \alpha^4,\ \alpha^{17} = \alpha^4 + \alpha^{16}.$$

Тогда результирующая матрица T имеет вид:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

3.3. Сложность нормальных базисов.

Определим сложность C_B нормального базиса B поля $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$, порожденного элементом α, как число ненулевых коэффициентов соответствующей матрицы T, определенной в предыдущем параграфе. Следующий результат дает нижнюю границу для этого числа.

Теорема 1. *Пусть B – нормальный базис $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$. Тогда*

$$C_B \geq 2n - 1.$$

Кроме того, C_B – четно, если $q = 2$.

Нормальный базис B, для которого выполняется равенство $C_B = 2n - 1$, называется *оптимальным*.

Теорема 2. *Пусть q – степень простого числа, $n + 1$ – простое и предположим, что q – примитивный корень по модулю $n+1$. Тогда круговой многочлен Φ_{n+1} неприводим над $\mathbb{F}_q$, и его корни образуют оптимальный нормальный базис $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$.*

Отметим, что с помощью предыдущей теоремы нельзя построить оптимальный нормальный базис для произвольного простого $n \neq 2$. Однако, все известные криптографические приложения рассматривают расширение $\mathbb{F}_2$ простой степени n. Положим

$$f_0 = 1, \quad f_1 = X + 1, \quad f_k = X f_{k-1} + f^{k-2} \text{ для } k > 1.$$

Теорема 3. *Пусть* $2n+1$ *– простое число. Предположим, что* 2 *– примитивный корень по модулю* $2n+1$ *или* $2n+1 \equiv 3 \pmod 4$ *и* 2 *– квадратичный вычет по модулю* $2n+1$*. Тогда многочлен* $f_n \in \mathbb{F}_2[X]$*, определенный выше, является неприводимым и его корни образуют оптимальный нормальный базис для* $\mathbb{F}_{2^n}/\mathbb{F}_2$*.*

Для случая $q = 2$ известны следующие результаты, касающиеся сложности нормального базиса:

1. $kn - (k^2 - 3k + 3) \leq C_B \leq kn - k + 1$, если k – четное;
2. $(k+1)n - (k^2 + k + 1) \leq C_B \leq (k+1)n - 2k + 1$, если k – нечетное;
3. $C_B = 4n - 7$ для $k = 3$ и $k = 4$;
4. $C_B = 6n - 21$ для $k = 5$ и $n > 2$ и для $k = 6$ и $n > 3$;
5. $C_B = 8n - 43$ для $k = 7$ и $n > 4$.