
Лекция №9 (19.11.20)

---

4. Дуальные базисы.

4.1. Фундаментальные результаты.

Пусть $B = \{\beta_0, \ldots, \beta_{n-1}\}$ и $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ – базисы поля $\mathbb{F}_{q^n}/\mathbb{F}_q$. Базис C называется *дуальным к* B, если

$$\mathrm{Tr}(\beta_i\gamma_j) \text{ для } i, j = 0, \ldots, n-1.$$

Теорема 1. *Для базиса B поля $E = \mathbb{F}_{q^n}$ над $F = \mathbb{F}_q$ существует единственный дуальный базис.*

Причина рассмотрения дуальных базисов заключается в том, что они позволяют определить координатное представление произвольных элементов. Пусть $B = \{\beta_0, \ldots, \beta_{n-1}\}$ и $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ – дуальные базисы поля E/F. Рассмотрим элемент

$$\xi = x_0\beta_0 + \ldots + x_{n-1}\beta_{n-1}$$

поля K. Запишем

$$r_B(\xi) := (x_0, \ldots, x_{n-1})$$

для координатного представления ξ относительно базиса B. Элементы x_i называются *основными координатами* ξ. Также используем координаты ξ относительно базиса C, а именно, дуальные координаты ξ. Положим

$$r_C(\xi) := ((\xi)_0, \ldots, (\xi)_{n-1})$$

тогда $\xi = (\xi)_0\gamma_0 + \ldots + (\xi)_{n-1}\gamma_{n-1}$.

Лемма 1. *Пусть $B = \{\beta_0, \ldots, \beta_{n-1}\}$ и $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ – дуальные базисы поля E/F. Пусть ξ – произвольный элемент поля $\mathbb{F}_{q^n}$. Тогда координата x_i у β_i в $r_B(\xi)$ равна $\mathrm{Tr}(\xi\gamma_i)$, а координата $(\xi)_i$ у γ_i в $r_C(\xi)$ равна $\mathrm{Tr}(\xi\beta_i)$.*

Лемма 2. *Дуальный базис к нормальному базису также является нормальным.*

Теорема 2. *Пусть $F = \mathbb{F}_q$ и $E = \mathbb{F}_{q^n}$, β – образующая нормального базиса E/F. Для $i = 0, \ldots, n-1$ положим $\beta_i := \beta^{q^i}$ и $t_i = \mathrm{Tr}_{E/F}(\beta_0 \beta_i)$. Рассмотрим многочлен*

$$h(X) = t_{n-1}X^{n-1} + \ldots + t_1 X + t_0.$$

Пусть $g(X) = d_{n-1}X^{n-1} + \ldots + d_1 X + d_0$ – единственный унитарный многочлен степени $< n$, удовлетворяющий условию

$$g(X)h(X) \equiv 1 \pmod{X^n - 1}.$$

(Отметим, что h обратим по модулю $X^n - 1$). Тогда дуальный базис к нормальному базису B, порожденному β, является нормальным базисом, порожденным элементом

$$\gamma = d_0\beta_0 + \ldots + d_{n-1}\beta_{n-1}.$$

Теорема 3. *Пусть $B = \{\beta_0, \ldots, \beta_{n-1}\}$ – полиномиальный базис поля $E = \mathbb{F}_{q^n}$ над $F = \mathbb{F}_q$*

$$\beta_0 = 1,\ \beta_1 = \beta, \ldots,\ \beta_{n-1} = \beta^{n-1}$$

и предположим, что минимальный многочлен $f = m_\beta$ элемента β расщепляется над E

$$f(X) = (X - \beta)(\alpha_0 + \alpha_1 + \ldots + \alpha_{n-1}X^{n-1}).$$

Тогда дуальный базис $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ к B может быть вычислен следующим образом:

$$\gamma_i = \alpha_i / f'(\beta) \ \text{ для } \ i = 0, \ldots, n-1,$$

где f' – формальная производная f.

4.2. Битовые последовательные мультипликаторы дуальных базисов.

Пусть $B = \{1, \beta, \ldots, \beta^{n-1}\}$ – полиномиальный базис $E = \mathbb{F}_{2^n}$ над $F = \mathbb{F}_2$ и пусть $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ – дуальный базис к B. Используем обозначение координатного представления относительно B и C

$$r_C(\xi) = ((\xi)_0, \ldots, (\xi)_{n-1}) = (\mathrm{Tr}(\xi), \mathrm{Tr}(\xi\beta), \ldots, \mathrm{Tr}(\xi\beta^{n-1})) \quad (4.2.1)$$

для дуальных координат элемента $\xi \in E$.

Используя (4.2.1) легко вычислить $\beta\xi$ в дуальных координатах. Мы получаем

$$(\beta\gamma)_i = \mathrm{Tr}(\beta\xi\beta^i) = \mathrm{Tr}(\xi\beta^{i+1}) = (\xi)_{i+1} \ \text{ для } \ i = 0, \ldots, n-2$$

и

$$(\beta\gamma)_{n-1} = \mathrm{Tr}(\xi\beta^n) = \mathrm{Tr}(a_0\xi + \ldots + a_{n-1}\xi\beta^{n-1}) = \beta_0(\xi)_0 + \ldots + \beta_{n-1}(\xi)_{n-1},$$

где $m_\beta = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ – минимальный многочлен элемента β.

Для дуальных координат справедливо следующее симметричное свойство:

$$(\beta^j\xi)_i = \mathrm{Tr}(\xi\beta^{i+j}) = (\beta^i\xi)_j \text{ для } i,j = 0,\ldots,n-1.$$

Используя это свойство симметрии, мы получаем

$$(\pi)_j = \left(\sum_{i=0}^{n-1} y_i\beta^i\xi\right) = \sum_{i=0}^{n-1} y_i(\beta^i\xi)_j = \sum_{i=0}^{n-1} y_i(\beta^j\xi)_i.$$