

Cálculos en cuerpos finitos

$$[F:k] = m$$

Ya sea que utilizemos una base polinómica, normal o cualquier otra para un F sobre k , todo elemento $\alpha \in F$ puede ser representado como un vector de la forma $\alpha = (a_1, a_2, \dots, a_m)$ con $a_i \in k$ si $\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_m \alpha_m$ y $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ es una base de F sobre k .

Luego la suma (o la resta) de dos elementos $\alpha, \beta \in F$ se realiza simplemente sumando (restando) coordenada a coordenada en k . En el caso particular en que $k = \mathbb{F}_p$ p primo, la operación en k es la reducción módulo p .

Multiplicación

$$[F:k] = m$$

Fijada una base $B = \{\alpha_0, \dots, \alpha_{m-1}\}$ de F sobre k y dos elementos $a, b \in F$

$$a = a_0 \alpha_0 + a_1 \alpha_1 + \dots + a_{m-1} \alpha_{m-1}$$

$$= (a_0, a_1, \dots, a_{m-1})$$

$$b = b_0 \alpha_0 + b_1 \alpha_1 + \dots + b_{m-1} \alpha_{m-1}$$

$$(b_0, b_1, \dots, b_{m-1})$$

$$a_0, \dots, a_{m-1}, b_0, \dots, b_{m-1} \in k.$$

Para realizar el producto $a.b$

$$\begin{aligned}
 c &= a.b = \left(\sum_{i=0}^{m-1} a_i \alpha_i \right) \cdot \left(\sum_{j=0}^{m-1} b_j \alpha_j \right) = \\
 &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j \underbrace{\alpha_i \alpha_j}_{\sum_{k=0}^{m-1} \underbrace{t_{ij}^{(k)}}_{\text{green circle}} \alpha_k} \quad \text{green arrow } \epsilon^k \\
 &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j \left(\sum_{k=0}^{m-1} t_{ij}^{(k)} \alpha_k \right) \\
 &= \sum_{k=0}^{m-1} \underbrace{\left(\sum_{i,j} a_i b_j t_{ij}^{(k)} \right)}_{c_k} \alpha_k \quad \checkmark
 \end{aligned}$$

$$\boxed{c_k = \vec{a} \cdot T_k \cdot \vec{b}^t} = (a_0, \dots, a_{m-1}) T_k \begin{pmatrix} b_0 \\ \vdots \\ b_{m-1} \end{pmatrix}$$

Si denotamos por $T_k = (t_{ij}^k)_{\substack{i=0, \dots, m-1 \\ j=0, \dots, m-1}}$

la matriz formada

por todas las entradas t_{ij}^k para cada $k=0, \dots, m-1$
 donde t_{ij}^k es el coeficiente de α_k en el producto $\alpha_i \cdot \alpha_j$.

$$\underbrace{\alpha_i \cdot \alpha_j}_{\text{red box}} = \sum_{k=0}^{m-1} t_{ij}^k \cdot \underbrace{\alpha_k}_{\text{red box}}$$

Las m matrices de $m \times m$ T_k se denominan tablas de multiplicación

Las tablas de multiplicación determinan completamente el producto y pueden implementarse bien en un software almacenando las m tablas.

Base polinómica

Si consideramos la base $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ donde α es una raíz de un polinomio $p(x) \in k[x]$ mónico e irreducible de grado m , digamos

$$p(x) = x^m + d_{m-1} x^{m-1} + \dots + d_1 x + d_0$$

entonces las matrices T_k se forman con los coeficientes t_{ij}^k en el producto $\alpha_i \cdot \alpha_j$ y en este caso

$$\alpha_i \cdot \alpha_j = \alpha^i \cdot \alpha^j = \alpha^{i+j}$$

- Si $i+j < m \Rightarrow \alpha_i \alpha_j = \alpha^{i+j} \rightarrow t_{ij}^{i+j} = 1$
- Si $i+j \geq m \Rightarrow$ hay que reducir α^{i+j}

usando que $p(\alpha) = 0$, es decir que

$$\alpha^m = -d_{m-1} \alpha^{m-1} - \dots - d_1 \alpha - d_0$$

y en este caso

$$\alpha_i \cdot \alpha_j = \alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^m \cdot \alpha^{i+j-m} \dots$$

$\uparrow$
 $(-d_{m-1} \alpha^{m-1} - \dots - d_1 \alpha - d_0)$

$$\dots = \sum_{k=0}^{m-1} f_k \cdot \alpha_k \rightarrow t_{ij}^k = f_k.$$

Por ejemplo: cuando miramos el producto $\alpha_i \cdot \alpha_j$ en donde $\alpha_i = 1$ (la unidad del producto)

$$\alpha_0 \cdot \alpha_j = \alpha_j \rightarrow t_{0j}^j = 1 \quad t_{0j}^i = 0 \text{ si } i \neq j$$

$$T_0 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & & & & \\ 0 & & & & \\ \vdots & & & & \end{pmatrix}$$

...

$$T_{m-1} = \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ \vdots & & & & \\ \vdots & & & & \\ 0 & & & & \\ 1 & & & & \end{pmatrix}$$

Ejemplo: $\mathbb{F}_4 = \mathbb{F}_2(\alpha) \quad \alpha^2 + \alpha + 1 = 0 \quad - \quad P(X) = X^2 + X + 1.$
 $= \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$

Consideremos la base polinómica $\{1, \alpha\}$.

$$a \in \mathbb{F}_4 \Rightarrow a = a_0 \cdot 1 + a_1 \cdot \alpha = a_0 + a_1 \alpha = (a_0, a_1)$$

$$b \in \mathbb{F}_4 \Rightarrow b = b_0 \cdot 1 + b_1 \cdot \alpha = b_0 + b_1 \alpha = (b_0, b_1)$$

$$a \cdot b = (a_0 + a_1 \alpha)(b_0 + b_1 \alpha) =$$

$$= a_0 b_0 + a_0 b_1 \alpha + a_1 b_0 \alpha + a_1 b_1 \alpha^2$$

$$= \underbrace{(a_0 b_0 + a_1 b_1)}_{(a_0, a_1) T_0 (b_0, b_1)} \cdot 1 + \underbrace{(a_0 b_1 + a_1 b_0 + a_1 b_1)}_{(a_0, a_1) T_1 (b_0, b_1)} \alpha$$

$$\begin{matrix} T_0 & T_1 \\ \uparrow & \uparrow \\ \{1, \alpha\} & \{1, \alpha\} \end{matrix}$$

T_0 : $\leftarrow$ multiplicación por 1
 T_k

$$\begin{matrix} t_{00}^0 = 1 \\ t_{00}^1 = 0 \end{matrix}$$

$$1 \cdot 1 = 1 = 1 \cdot 1 + 0 \cdot \alpha = (1, 0)$$

$$1 \cdot \alpha = \alpha = 0 \cdot 1 + 1 \cdot \alpha = (0, 1)$$

$$T_0 = \begin{pmatrix} \boxed{1} & \boxed{0} \\ \boxed{0} & \boxed{1} \end{pmatrix}$$

$$T_1 = \begin{pmatrix} \boxed{0} & \boxed{1} \\ \boxed{1} & \boxed{1} \end{pmatrix}$$

$$\begin{matrix} t_{01}^0 = 0 = t_{10}^0 \\ t_{01}^1 = 1 = t_{10}^1 \end{matrix}$$

$$T_2: \quad \alpha \cdot 1 = (0, 1)$$

$$\alpha \cdot \alpha = \alpha^2 = 1 + \alpha = (1, 1)$$

$$\begin{matrix} t_{11}^0 = 1 \\ t_{11}^1 = 1 \end{matrix}$$

Ejemplo: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ donde α es raíz del polinomio

$$p(x) = x^3 + x + 1 = 0$$

y la base polinómica $\left\{ \underset{\alpha_0}{1}, \underset{\alpha_1}{\alpha}, \underset{\alpha_2}{\alpha^2} \right\}$

Ejercicio: Calcular las 3 matrices de 3×3 que formen las tablas de multiplicar T_0, T_1, T_2

y verificar que $a = a_0 + a_1\alpha + a_2\alpha^2$ y $b = b_0 + b_1\alpha + b_2\alpha^2$

entonces $a \cdot b = c_0 + c_1\alpha + c_2\alpha^2$

donde $C_i = (a_0, a_1, a_2) T_i \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \quad i=0,1,2.$

$$T_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \textcircled{1} & \\ 0 & & \vdots \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \textcircled{1} & \\ 0 & & \vdots \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & \textcircled{1} & \\ 1 & & \cdot \end{pmatrix}$$

$$\alpha_1 \cdot \alpha_1 = \underbrace{\hspace{1cm}} \alpha_0 + \underbrace{\hspace{1cm}} \alpha_1 + \underbrace{\hspace{1cm}} \alpha_2$$

$$\alpha_1 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1 =$$

$$\alpha_2 \cdot \alpha_2 =$$

Ejemplo: Consideremos $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ donde α es raíz
 $p(x) = x^2 + 1$ $\alpha^2 + 1 = 0 \rightarrow \alpha^2 = -1 = 2$

y la base polinómica $\left\{ \overset{\alpha_0}{1}, \overset{\alpha_1}{\alpha} \right\}$

$$a, b \in \mathbb{F}_9 \rightarrow \underline{a} = (a_0, a_1) \quad \underline{b} = (b_0, b_1)$$

$$a = a_0 + a_1 \alpha \quad b = b_0 + b_1 \alpha$$

$$\begin{aligned} a \cdot b &= (a_0 + a_1 \alpha) \cdot (b_0 + b_1 \alpha) = \\ &= a_0 b_0 + a_0 b_1 \alpha + a_1 b_0 \alpha + a_1 b_1 \alpha^2 \\ &= \underbrace{(a_0 b_0 + 2 a_1 b_1)}_{c_0} \cdot 1 + \underbrace{(a_0 b_1 + a_1 b_0)}_{c_1} \cdot \alpha \\ &\quad \underbrace{a \cdot T_0 \cdot b^t}_{c_0} \quad \underbrace{a \cdot T_1 \cdot b^t}_{c_1} \end{aligned}$$

$$T_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\underline{\alpha_1 \cdot \alpha_1} = \alpha \cdot \alpha = \alpha^2 = 2 = 2 \cdot 1 = 2 \cdot \alpha_0 + 0 \cdot \alpha_1 \rightarrow t_{11}^0 = 2$$

$$\rightarrow t_{11}^1 = 0$$

Ejercicio: Considera $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ $\alpha^3 + 2\alpha + 1 = 0$

- 1) Verificar que $p(x) = x^3 + 2x + 1$ es irreducible/ $\mathbb{F}_3$.
- 2) Calcular las tablas de mult. para la base $\{1, \alpha, \alpha^2\}$

Bases normales

$$\alpha_i = \alpha^{p^i}$$

Si se utiliza una base normal $B = \{ \overset{\alpha_0}{\underset{0}{\alpha}}, \overset{\alpha_1}{\underset{1}{\alpha^p}}, \dots, \overset{\alpha_{m-1}}{\underset{m-1}{\alpha^{p^{m-1}}}} \}$

entonces las tablas de multiplicación T_k satisfacen lo siguiente

Proposición: Para $0 < l \leq m-1$ se tiene que

$$t_{ij}^l = t_{i-l, j-l}^0$$

Es decir, la tabla T_l se obtiene de la tabla T_0 desplazando l posiciones las filas y las columnas.

Demostración

Por un lado

$$(\alpha_{i-l} \cdot \alpha_{j-l})^{p^l} = (\alpha^{p^{i-l}} \cdot \alpha^{p^{j-l}})^{p^l} = \alpha^{p^i} \cdot \alpha^{p^j} =$$

$$\begin{aligned} &= \alpha_i \cdot \alpha_j = \sum_{k=0}^{m-1} t_{ij}^k \alpha_k = \sum_{k=0}^{m-1} (t_{ij}^k)^{p^l} (\alpha^{p^{k-l}})^{p^l} \\ &= \left(\sum_{k=0}^{m-1} t_{ij}^k \alpha^{p^{k-l}} \right)^{p^l} = \left(\sum_{k=0}^{m-1} t_{ij}^k \alpha_{k-l} \right)^{p^l} \end{aligned}$$

$$\Rightarrow \alpha_{i-l} \cdot \alpha_{j-l} = \sum_{k=0}^{m-1} t_{ij}^k \alpha_{k-l}$$

$$\alpha_{i-l} \cdot \alpha_{j-l} = \sum_{k=0}^{m-1} t_{ij}^k \alpha_{k-l} \quad (1)$$

Por otro lado, por la def. de las tablas de mult. tenemos que

$$\alpha_{i-l} \cdot \alpha_{j-l} = \sum_{k=0}^{m-1} t_{i-l, j-l}^k \cdot \alpha_k \quad (2)$$

Iguando los coeficientes de α_0 en (1) y (2)

$$(1) \rightarrow k=l \rightarrow \text{el coef de } \alpha_0 \text{ es } t_{ij}^l$$

$$(2) \rightarrow k=0 \rightarrow \text{el coef de } \alpha_0 \text{ es } t_{i-l, j-l}^0$$

$$\Rightarrow t_{ij}^l = t_{i-l, j-l}^0$$

En consecuencia, en este caso si se tiene un algoritmo para calcular la primera coordenada del producto, el mismo algoritmo calcule la coordenada c_l usando las coordenadas de a y b desplazados.

Exemple: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ donde α es raíz de $\alpha^3 + \alpha^2 + 1 = 0$

entonces $\{\alpha_0, \alpha_1, \alpha_2\}$ es una base normal de $\mathbb{F}_8$ sobre $\mathbb{F}_2$.
 $\alpha_0 \alpha_1 \alpha_2$
 $\alpha^4 + \alpha = \alpha^3$ $\alpha^4 = \alpha \cdot \alpha^3 = \alpha + \alpha^3$

$$\alpha_0 \cdot \alpha_0 = \alpha \cdot \alpha = \alpha^2 = 0 \cdot \alpha_0 + 1 \cdot \alpha_1 + 0 \cdot \alpha_2 \rightarrow t_{00}^0 = 0$$

$$t_{00}^1 = 1$$

$$t_{00}^2 = 0$$

$$\alpha_0 \cdot \alpha_1 = \alpha \cdot \alpha^2 = \alpha^3 = 1 \cdot \alpha_0 + 0 \cdot \alpha_1 + 1 \cdot \alpha_2$$

$$t_{01}^0 = 1 = t_{10}^0$$

$$t_{01}^1 = 0 = t_{10}^1$$

$$t_{01}^2 = 1 = t_{10}^2$$

$$\alpha_0 \cdot \alpha_2 = \alpha \cdot \alpha^4 = \alpha^5 = \alpha^2 \cdot \alpha^3 = \alpha^2 (1 + \alpha^2) = \alpha^2 + \alpha^4 = 0 \cdot \alpha_0 + 1 \cdot \alpha_1 + 1 \cdot \alpha_2$$

$$t_{02}^0 = 0 = t_{20}^0$$

$$t_{02}^1 = 1 = t_{20}^1$$

$$t_{02}^2 = 1$$

$$t_{20}^2 = 1$$

$$T_0 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & & \\ 0 & & \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & & \\ 1 & & \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & & \\ 1 & & \end{pmatrix}$$

Ejercicio: Completen las tablas anteriores.

Resol.

$$T_0 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad T_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$T_0 \xrightarrow{\text{derecha}} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \xrightarrow{\text{abajo}} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = T_1$$

$$T_0 \xrightarrow{2 \text{ derecha}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \xrightarrow{2 \text{ abajo}} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = T_2$$

Tablas de multiplicación para $\mathbb{F}_8/\mathbb{F}_2$ con

$$\mathbb{F}_8 = \mathbb{F}_2(\alpha) \quad \alpha^3 + \alpha + 1 = 0 \quad \text{y base } \{1, \alpha, \alpha^2\}$$

$$T_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Tablas de multiplicación para $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$
con $\alpha^3 + 2\alpha + 1 = 0$ base $\{1, \alpha, \alpha^2\}$

$$T_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \quad T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \quad T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$