Algebra y Algoritmos Entrega 1

Ejercicio 1. Dado $m \in \mathbb{N}$ se define sobre $\mathbb{F}_2$

$$T_m = \sum_{i=0}^{m-1} x^{2^i}$$

$q = 2^k$, $k \in \mathbb{N}_{\geq 1}$ $f \in \mathbb{F}_q[X]$ libre de cuadrados, $\deg(f) = n$

$f = f_1 \cdot f_2 \cdot \ldots \cdot f_r \in \mathbb{F}_q[X]$ $r \geq 2$ irreducibles.

$R = \mathbb{F}_q[x]/\langle f \rangle$ y $R_i = \mathbb{F}_q[x]/\langle f_i \rangle$ $i \in \{1, 2, \ldots, r\}$

χ_i: homomorfismo canónico.

(I) Demuestra:

1. $X^{2^m} + X = T_m(X) \cdot (T_m(X) + 1)$

2. $T_m(\alpha) \in \mathbb{F}_2 \quad \forall \alpha \in \mathbb{F}_{2^m}$

3. $Pr(T_m(\alpha) = 1 \quad T_m(\alpha) = 0) = 1/2$

1. Desarrollemos ambas partes del igual para llegar a la misma expresión.

$$\boxed{Izq} \quad X^{2^m} + X \overset{char=2}{=} X^{2^m} - X \overset{T^{ma}\ A.3.1.}{=} \prod_{\alpha \in \mathbb{F}_{2^m}} (X - \alpha) = 0 \quad \forall \alpha \in \mathbb{F}_{2^m}$$

$$\boxed{Dch} \quad T_m(X) \cdot (T_m(X) + 1) \overset{\text{distributiva}}{=} T_m(X)^2 + T_m(X)$$

Obs: Sea $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_2[x]$

$$P^2(x) = \sum_{i=0}^{n} \sum_{j=0}^{n} (a_i x^i)(a_j x^j) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i \cdot a_j \, x^{i+j}$$

Diferenciamos dos casos

$\boxed{i=j}$ $\sum_{i=0}^{n} a_i^2 \cdot x^{2i}$

$\boxed{i \neq j}$ $\sum_{i \neq j} a_i a_j x^{i+j} = \sum_{0 \leq i < j \leq n} (a_i a_j x^{i+j}) + (a_j a_i x^{j+i}) =$

$= 2 \cdot \sum_{0 \leq i < j \leq n} a_{ij} x^{i+j}$

char $= 2$ $\quad$ 0 $\quad$ $\forall e \in \mathbb{F}_2 \; e^2 = e$

$$\Rightarrow P(x)^2 = \sum_{i=0}^{n} (a_i x^i)^2 + \cancel{2 \cdot \sum_{0 \leq i < j \leq n} a_{ij} x^{i+j}} = \sum_{i=0}^{n} a_i x^i = P(x)$$

char 2

Así

$$T_m(x)^2 + T_m(x) = T_m(x) + T_m(x) = 0$$

Por lo que:

$$x^{2^m} + x = T_m(x) \cdot (T_m(x) + 1)$$

$\square$

2. Sea $\alpha \in \mathbb{F}_{2^m}$ $\quad T_m(\alpha) = \alpha^{2^{m-1}} + \alpha^{2^{m-2}} + \_\_\_ + \alpha^2 + \alpha$

Como char $= 2$ y se trata de una suma finita de elementos

$T_m(\alpha) \in \mathbb{F}_2$

3. Veamos inicialmente la linealidad de $T_m(X)$

$$T_m(X+Y) = \sum_{i=0}^{m-1} (X+Y)^{2^i} = \sum_{i=0}^{m-1} \sum_{k=0}^{2^i} \binom{2^i}{k} X^{2^i-k} \cdot Y^k \overset{\text{char}(\mathbb{Z}2)}{=} \sum_{i=0}^{m-1} X^{2^i} + Y^{2^i}$$

Esto se da porque $\binom{2^i}{k}$ es par cuando $k \neq 0 \neq 2^i$

$$= \sum_{i=0}^{m-1} X^{2^i} + \sum_{i=0}^{m-1} Y^{2^i} = T_m(X) + T_m(Y)$$

$$T_m(\lambda X) = \sum_{i=0}^{m-1} (\lambda X)^{2^i} = \sum_{i=0}^{m-1} \lambda^{2^i} X^{2^i} \overset{\text{char } 2}{=} \sum_{i=0}^{m-1} \lambda X^{2^i} = \lambda \sum_{i=0}^{m-1} X^{2^i}$$

$$= \lambda T_m(X)$$

Bien, hemos visto que es lineal, analicemos el Kernel

$Ker(T_m) = \{\alpha \in \mathbb{F}_{2^m} : T_m(\alpha) = 0\}$, como la aplicación es lineal $\dim(Ker(T_m)) = \dim(\mathbb{F}_{2^m}) - \dim(\mathbb{F}_2) =$ $= m-1$, así # elementos en $Ker(T_m) = 2^{m-1}$

Que es la mitad del espacio. Por lo que 2^{m-1} elentos toman valor 0 y 2^{m-1} elentos toman valor 1. Asumiendo por hipótesis una distribución uniforme concluimos que

$$P_r(T_m(\alpha) = 0) = P_r(T_m(\alpha) = 1) = \frac{2^{m-1}}{2^m} = 1/2$$

D

(II) Usando el resultado anterior y con el siguiente desarrollo

$$\chi_i(T_k(\alpha)) = T_k(\alpha \bmod f_i) \overset{\alpha_i := \alpha \bmod f_i}{=} T_k(\alpha_i) \in \mathbb{F}_2$$

análogo apartado I. 2.

De manera similar al apartado 2 y usando los resultados.

Para que $T_k(\alpha) \in \mathbb{F}_2$ $\quad T_k(\alpha_1) = T_k(\alpha_2) = \_\_\_ = T_k(\alpha_r)$

Como hemos visto $P_r(T_k(\alpha_i) = 1) = 1/2 = P_r(T_k(\alpha_i) = 0)$

Por lo que, intuitivamente, la primera coordenada puede ser cualquier estado, pero el resto deben de ser iguales a la primera. Así:

$$P_r(T_k(\alpha) \in \mathbb{F}_2) = 2 \cdot \left(\tfrac{1}{2}\right)^r = \left(\tfrac{1}{2}\right)^{r-1}$$

(III) Con el contexto de (II)

No encontrar un factor equivale a que la traza de α sea la misma en todas las coordenadas por lo que

$$P_r(\text{no factorizar}) = \frac{2}{2^r} = \left(\tfrac{1}{2}\right)^{r-1} = 2^{-(r-1)}$$

Además si realizamos N intentos

$$P_r(\text{no factorizar en } N \text{ intentos}) = 2^{-N(r-1)}$$

Ejercicio 3.

(I) Procedemos por inducción sobre n el grado de $F \in \mathbb{R}[x]$

$\boxed{\text{caso base } n=1}$

$$\left.\begin{array}{l} F(x) = ax+b \quad a \neq 0 \\ F'(x) = a \end{array}\right\} \Rightarrow DF = [F, F'] = [ax+b, a]$$

$\sigma = (\sigma_0, \sigma_1) \in \{-1, 0, 1\}^2$

Observamos que signo$(F') = \sigma_1 \in \{-1, 1\}$ cte.

$\to$ si signo$(a) \neq$ signo(F') $\Rightarrow R(\sigma) = \emptyset$

$\to$ si signo$(a) = \sigma_1$

$\to$ si $\sigma_0 = 0$, necesitamos $F(x) = 0 \to x = -b/a$

$\Rightarrow R(\sigma)$ es un punto único

$\to$ si $\sigma_0 = \pm 1$, necesitamos $\pm(ax+b) > 0$

$\Rightarrow R(\sigma)$ es un intervalo ~~ó el cjto vacío~~.

Hipótesis inductiva: Suponemos cierto para los polinomios de grado $\leq n-1$

$\boxed{\text{caso } n}$

Como $deg(F) = n$ $\quad F^{(n)} = c_n \neq 0 \in \mathbb{R}$ cte

$\to$ si $\sigma_n = 0 \Rightarrow R(\sigma) = \emptyset$ ya que $c_n \neq 0$

$\to$ si $\sigma_n \neq \text{signo}(c_n) \Rightarrow R(\sigma) = \emptyset$

$\to$ si $\sigma_n = \text{signo}(c_n)$, hay que analizar el signo de las derivadas $[F, F', \_\_\_, F^{n-1}]$

Cada F^{i} tiene sus raíces, definimos el conjunto finito de todas ellas

$$S = \bigcup_{i=0}^{n-1} \{x \in \mathbb{R} : F^{(i)}(x) = 0\}$$

Usando el conjunto S analizaremos los punto $s \in S$ y $\mathbb{R} \setminus S$

- Sea $(a,b) \subseteq \mathbb{R} \setminus S$ t.q. $\text{signo}(F^{(i)}(x))$ constante si $x \in (a,b)$ (σ_f)
  - $\to$ si $\sigma_f \neq \sigma_i \Rightarrow R(\sigma) = \emptyset$
  - $\to$ si $\sigma_f = \sigma_i \Rightarrow \forall x \in (a,b) \quad x \in R(\sigma)$

- Sea $x \in S$
  - $\to$ si $\sigma_i = 0$ y $F^{(i)}(x) = 0 \Rightarrow x \in R(\sigma)$
  - $\to$ si $\sigma_i = 1$ o $\sigma_i = -1$ y $F^{(i)}(x) > 0$ o $F^{(i)}(x) < 0$ respect.

(II) Supongamos que $R(\sigma) = \{c\}$ y $\sigma \in \{-1,1\}^n$

Así, $\text{signo}(F^{(i)}(c)) = \sigma_i \in \{-1,1\}$, por lo tanto

$F^{(i)}(c) \neq 0 \quad \forall i$

Sin embargo, $F^{(i)}$ es un polinomio y por lo tanto continua

así, como $F^{(i)}(c) \neq 0$ $\exists\, \varepsilon$ t.q.

$$\forall x \text{ t.q. } |x-c| < \varepsilon \quad \text{signo}(F^{(i)}(x)) = \text{signo}(F^{(i)}(c)) = \sigma_i$$

Por lo que $x \in R(\sigma)$ # ya que $R(\sigma) = \{c\}$

Así concluimos que una condición necesaria para que $R(\sigma)$ sea un punto es que $0 \in \sigma$.

(III) Por contraposición, veamos que si $V_{DF}(c) = V_{DF}(d)$ entonces $c = d \in \mathbb{R}$

$$\text{si } V_{DF}(c) = V_{DF}(d) \rightarrow R(V_{DF}(c)) = R(V_{DF}(d)) \xrightarrow{\text{raíces}}$$

$c = d$.

(V) Como k maximo indice t.q. $F^{(k)}(x) \neq F^{(k)}(y)$

$\rightarrow \forall j > k$ $F^{(j)}(x) = F^{(j)}(y)$ en particular F

- En particular, $F^{(k+1)}(x) = F^{(k+1)}(y) \rightarrow$ signo$(F^{k+1}(x)) =$ signo$(F^{k+1}(y))$

Veamos que signo $(F^{k+1}(x)) \neq 0$, por R.A. supongamos que

signo$(F^{k+1}(x)) = 0 \rightarrow F^{k+1}(x) = 0 \rightarrow x$ anula $F(x)$ y
x anula $F(x)$

Por lo que x es raiz con multiplicidad > 1, esto contradice el hecho de que F sea polinomio mínimo. ⨳.

- signo $(F^{k+1}(x)) =$ signo $(F^{k+1}(y)) = 1$

Como la derivada $k+1$-ésima es positiva en un entorno de x e y Por el lema de Thom $F^{(k)}(z)$ es creciente en ese entorno, así, si

$x > y \rightarrow F^{(k)}(x) > F^{(k)}(y)$ por monotonía.

- signo $(F^{k+1}(x)) =$ signo $(F^{k+1}(y)) = -1$

Análogo al apartado anterior, como la derivada $F^{k+1}(x) < 0$ y por el lema de Thom trabajamos en un intervalo, lo tenemos como entorno de x e y así $F^{(k)}(z)$ es decreciente en ese entorno así, si

$x > y \rightarrow F^{k}(x) < F^{k}(y)$