Ma31a Elementos de Álgebra	**26 de Noviembre, 2007**

Pauta Examen

Prof. Cátedra: M. Kiwi | *Prof. Auxiliar: R. Cortez*

(i).- Observar que $CH^T = 0$ si y sólo si para todo $j \in \{0, \ldots, \delta - 2\}$

$$\sum_{i=0}^{n-1} c_i \beta^{i(\ell+j)} = 0\,.$$

Pero, esto último equivale a decir que $C(\beta^{\ell+j}) = 0$.

(ii).- Sea $C \in \mathcal{C}$. Sigue que C es un múltiplo de G. Pero G es divisible por el polinomio minimal de $\beta^{\ell+j}$, luego $\beta^{\ell+j}$ es raíz de G y también de C.

Para probar el converso, denotaremos por $M^{(i)}(x)$ al polinomio minimal de β^i. Supongamos entonces que $C(\beta^{\ell+j}) = 0$ para todo $j \in \{0, \ldots, \delta - 2\}$. Sigue que C comparte una raíz con $M^{(\ell+j)}(x)$. Por irreducibilidad del polinomio minimal y propiedad vista, sigue que $C(x)$ es divisible por $M^{(\ell+j)}(x)$. Luego, $C(x)$ es divisible por el mínimo común múltiplo de los $M^{(\ell+j)}(x)$, i.e. $C(x)$ es divisible por $G(x)$ y por lo tanto pertenece a $\mathcal{C}$.

(iii).- La submatriz que se forma con las columnas $i_1, \ldots, i_{\delta-1}$ de H es

$$H_{i_1,\ldots,i_{\delta-1}} = \begin{pmatrix} \beta^{i_1\ell} & \beta^{i_2\ell} & \beta^{i_3\ell} & \ldots & \beta^{i_{\delta-1}\ell} \\ \beta^{i_1(\ell+1)} & \beta^{i_2(\ell+1)} & \beta^{i_3(\ell+1)} & \ldots & \beta^{i_{\delta-1}(\ell+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta^{i_1(\ell+\delta-2)} & \beta^{i_2(\ell+\delta-2)} & \beta^{i_3(\ell+\delta-2)} & \ldots & \beta^{i_{\delta-1}(\ell+\delta-2)} \end{pmatrix}.$$

Por propiedades del determinante, sigue que

$$\mathrm{Det}\, H_{i_1,\ldots,i_{\delta-1}} = \beta^{(i_1+i_2+\ldots+i_{\delta-2})\ell} \cdot \mathrm{Det} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \beta^{i_1} & \beta^{i_2} & \ldots & \beta^{i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{i_1(\delta-2)} & \beta^{i_2(\delta-2)} & \ldots & \beta^{i_{\delta-1}(\delta-2)} \end{pmatrix}.$$

La matriz en esta última identidad es una matriz de Vandermonde y su determinante es por lo tanto igual a $\prod_{r<s}(\beta^{i_r} - \beta^{i_s})$. Como β es elemento primitivo, se tiene que

$\beta^i \neq \beta^j$ cualquiera que sean $i, j \in \{0, \ldots, n-1\}$, $i \neq j$. Luego el determinante de $H_{i_1,\ldots,i_{\delta-1}}$ es no-nulo.

(iv).- Supongamos que existe un $C \in \mathcal{C}$, $C \neq \vec{0}$, tal que $d = |\{i : c_i \neq 0\}| < \delta$. Sean $i_1 < i_2 < \ldots < i_d$ tales que $c_{i_j} \neq 0$. De la parte (i) tenemos que $CH^T = 0$ porque $C \in \mathcal{C}$. Pero esto implica que las columns $i_1, \ldots, i_d$ de H no son linealmente independientes, lo que contradice el resultado establecido en la parte (ii).

(v).- Tenemos que verificar que β tiene orden 7 en $\mathbb{F}_{2^3}^*$. Pero esto es obvio puesto que como $\beta \notin \mathbb{F}_2$ se tiene que $\beta \neq 1$ y por lo tanto su orden es estrictamente mayor que 1. Por Lagrange, el orden de β debe dividir 7. Sigue que el orden de β es igual a 7.

(vi).- Para obtener H debemos representar cada uno de los elementos $1, \beta, \beta^2, \ldots, \beta^7 \in \mathbb{F}_{2^3}$ como vectores en $\mathbb{F}_2^3$ sobre la base $\{1, \beta, \beta^2\}$. En particular observar que

i	0	1	2	3	4	5	6
β^i	1	β	β^2	$\beta+1$	$\beta^2+\beta$	$\beta^2+\beta+1$	β^2+1

Luego,

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} .$$

Si la palabra recibida fue $R = (1, 1, 0, 1, 0, 1, 0)$, y dado que $RH^T = (1, 1, 1) \neq 0$, necesarimante tuvieron que ocurrir errores de transmisión. Si sólo hubo un error en la transmisión este debió ser en la posición correspondiente a la columna de H igual a RH^T, i.e. en el 6-to caracter transmitido. Por lo tanto, la palabra enviada fue $(1, 1, 0, 1, 0, 0, 0)$.

(vii).- Dado que $\mathbb{F}_q$ es de característica p, tenemos que cualquiera que sea el polinomio $Q \in \mathbb{F}_p[x]$ y el elemento $\alpha \in \mathbb{F}_{q^m}$ se tiene que

$$(Q(\alpha))^p = \left(\sum_{n \in \mathbb{N}} q_n \alpha^n \right)^p = \sum_{n \in \mathbb{N}} q_n^p \alpha^{pn} = \sum_{n \in \mathbb{N}} q_n \alpha^{pn} = Q(\alpha^{pn}) ,$$

donde la penúltima igualdad es consecuencia del pequeño Teorema de Fermat.

Sigue que,

$$0 = (M^{(s)}(\beta^s))^p = M^{(s)}(\beta^{ps}) .$$

Luego, $M^{(s)}(x)$ y $M^{(ps)}(x)$ son ambos irreducibles en $\mathbb{F}_p[x]$ y comparten un raíz en una extensión de $\mathbb{F}_p$ por lo que deben ser divisores uno del otro, i.e. $M^{(s)}(x) = M^{(ps)}(x)$.

En otros palabras, si $i \in C_s$, entonces β^j es raíz de $M^{(s)}(x)$ cualquiera que sea $j \in C_s$. Luego, $M^{(i)}(x)$ es divisible por

$$\prod_{j \in C_s} \left(x - \beta^j\right) .$$

(viii).- Supongamos que $\alpha \in \mathbb{F}_{p^s}$. Si $\alpha = 0$, entonces $\alpha^{p^s} = \alpha$. Si $\alpha \neq 0$, entonces $\alpha^{p^s} = \alpha \cdot \alpha^{|\mathbb{F}^*_{p^s}|} = \alpha$.

Supongamos ahora que $\alpha^{p^s} = \alpha$. Sigue que α es raíz del polinomio $x^{p^s} - x \in \mathbb{F}_p[x]$. Como $\mathbb{F}_{p^s}$ es el cuerpo de descomposición de $x^{p^s} - x \in \mathbb{F}_p[x]$. Se tiene que $\alpha \in \mathbb{F}_{p^s}$.

Sea $P(x) = \prod_{j \in C_s}(x - \beta^j) \in \mathbb{F}_q[x]$. Veamos que los coeficientes de $P(x)$ están en $\mathbb{F}_p$. Por el párrafo anterior, bastará probar que $p_i^p = p_i$, donde p_i es el i-ésimo coeficiente de $P(x)$. En efecto, como $\mathbb{F}_q$ es de característica p, entonces

$$(P(x))^p = \prod_{j \in C_s} (x - \beta^j)^p = \prod_{j \in C_s} (x^p - \beta^{pj}) = \prod_{j \in C_s} (x^p - \beta^j) = P(x^p)\,,$$

donde la penúltima igualdad se tiene porque $\beta^{pj} = \beta^{pj \bmod n}$ y $C_s = \{pj \bmod n : j \in C_s\}$. Por igualdad de polinomios, se tiene que $p_i^p = p_i$ y por lo tanto $p_i \in \mathbb{F}_p$. Sigue inmediatamente que $P(x) \in \mathbb{F}_p[x]$.

Como $P(x) \in \mathbb{F}_p[x]$ divide a $M^{(i)}(x)$ y tiene a β^i como raíz, por minimalidad de $M^{(i)}(x)$ sigue que $M^{(i)}(x) = P(x)$.

(ix).- Primero observemos que $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ y $C_3 = \{3, 6, 5\}$. Luego, de la parte (viii), usando la tabla construida en (vi), y como $\beta^7 = 1$, sigue que

$$\begin{aligned} M^{(1)}(x) &= (x - \beta)\left(x - \beta^2\right)\left(x - \beta^4\right) \\ &= x^3 + (\beta + \beta^2 + \beta^4)x^2 + (\beta^3 + \beta^5 + \beta^6)x + \beta^7 \\ &= x^3 + x + 1\,. \end{aligned}$$

Análogamente se tiene que

$$\begin{aligned} M^{(3)}(x) &= \left(x - \beta^3\right)\left(x - \beta^6\right)\left(x - \beta^5\right) \\ &= x^3 + (\beta^3 + \beta^6 + \beta^5)x^2 + (\beta^8 + \beta^9 + \beta^{11}) + \beta^{14} \\ &= x^3 + x^2 + 1\,. \end{aligned}$$

Además $M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x)$ y $M^{(3)}(x) = M^{(5)}(x) = M^{(6)}(x)$. Luego, el mínimo común mútliplo de $\left\{M^{(s)} : 1 \leq s \leq \delta - 1\right\}$ es igual a $G_1(x) = M^{(1)}(x)$ si $\delta \in \{2, 3\}$ y $G_2(x) = M^{(1)}(x)M^{(3)}(x)$ si $\delta \in \{4, 5, 6\}$. Luego,

$$\begin{aligned} G_1(x) &= x^3 + x + 1\,, \\ G_2(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\,. \end{aligned}$$