Demostración de las 4 equivalencias que se dan a partir de $g(x)$ polinomio generador de un código C

Nicolás Cagliero

28 de junio de 2024

Theorem 1. *Sea C un código cíclico de dimensión k y longitud n y sea $g(x)$ su polinomio generador. Probar que:*

1. *C está formado por los múltiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \;\&\; g(x)|p(x)\}$*
2. *$C = \{v(x) \odot g(x) : v$ es un polinomio cualquiera$\}$*
3. *$gr(g(x)) = n - k$*
4. *$g(x)$ divide a $1 + x^n$*

Demostración.
Sea $C_1 = \{p(x) : gr(p) < n \;\&\; g(x)|p(x)\}$
Sea $C_2 = \{v(x) \odot g(x) : v$ es un polinomio cualquiera$\}$

Vamos a ver que $C = C_1$ y $C = C_2$ para demostrar los dos primeros items.

1. $C_1 \subseteq C_2$. Sea $p(x) \in C_1 \Rightarrow gr(p(x)) < n \;\&\; g(x)|p(x)$. Luego $\exists q(x) : p(x) = g(x) \cdot q(x)$ y además $p(x) mod(1 + x^n) = p(x)$. De esta forma obtenemos que $p(x) mod(1 + x^n) = (g(x) \cdot q(x)) mod(1 + x^n) \Rightarrow p(x) = g(x) \odot q(x) \in C_2$

2. $C_2 \subseteq C$. Sea $p(x) = g(x) \odot v(x) = v(x) \odot g(x)$ con algún $v(x)$

$$\begin{aligned}
\Rightarrow p(x) &= (v_0 + v_1 x + ...v_d x^d) \odot g(x) \\
&= v_0 \odot g(x) + ... + (v_d x^d) \odot g(x) \\
&= v_0 \odot g(x) + ... + v_d (x^d \odot g(x)) \\
&= v_0 \cdot g(x) + ... + v_d \cdot Rot^d(g(x))
\end{aligned}$$

Como todas las componentes pertenecen a $C \Rightarrow p(x) \in C$

3. $C \subseteq C_1$. Sea $p(x) \in C \Rightarrow gr(p(x)) < n$. Ahora dividamos $p(x)$ por $g(x)$. Existe $q(x), r(x) : p(x) = q(x) \cdot g(x) + r(x)$ con $gr(r) < gr(g)$

   Tomando módulo:

$$p(x) \; mod \; (1 + x^n) = (q(x) \cdot g(x) + r(x)) \; mod \; (1 + x^n)$$

$$p(x) = g(x) \odot q(x) + r(x)$$

$$\Rightarrow r(x) = p(x) + g(x) \odot q(x) \in C$$

Pero $r(x) \in C$ y además $gr(r) < gr(g) \Rightarrow r = 0 \Rightarrow p(x) = q(x) \cdot g(x) \in C_1$

Ahora demuestro el tercer ítem. Como vimos que $C = C_1$, sabemos que $p(x) \in C \iff gr(p) < n \;\&\; \exists q : p = qg$.

Como $gr(p)$ debe ser menor estricto que $n \to gr(g) + gr(q) < n \Rightarrow gr(q) < n - gr(g)$

Viceversa, si tomo un $q(x)$ cualquiera con $gr(q) < n - gr(g)$ Entonces $gr(gq) < n \therefore gq \in C \therefore$ existe una bitección entre C y el conjunto de polinomios de grado menor que $n - gr(g)$

$\Rightarrow |C| = |\text{conjunto de polinomios de grado } < n - gr(g)|$

$\Rightarrow 2^k = 2^{n-gr(g)}$

$\Rightarrow k = n - gr(g) \Rightarrow gr(g) = n - k$

Por último, veamos el cuarto ítem, dividamos $1 + x^n$ por $g(x)$. Existe $q(x), r(x)$ con $gr(r) < gr(g) : 1 + x^n = g(x) \cdot q(x) + r(x)$. Tomando módulo $0 = g(x) \odot q(x) + r(x) \Rightarrow r(x) = g(x) \odot g(x) \in C$.

Por lo mismo que antes, $r(x) \in C$ y además $gr(r) < gr(g) \Rightarrow r = 0 \Rightarrow g(x)$ divide a $1 + x^n$ $\square$