Códigos ~~lineales~~ cíclicos

<u>Def</u>: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1}$

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

<u>Ejemplo</u>

$F = \mathbb{F}_2$, $C \subseteq F^7$

$C = \{ (0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1),$
$(1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1) \}$

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \subseteq F^7$

$$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1),$$
$$(1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \;\; \longleftrightarrow \;\; w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \leq F^7$

$$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1), (1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \leq F[x]$ y $R = F[x]/I$.

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \leq F^7$

$$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1),$$
$$(1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \leq F[x]$ y $R = F[x]/I$.

Cada $f(x) \in F[x]$ tiene un representante en R con grado menor o igual a $n-1$:

$$f(x) = (x^n - 1) q(x) + r(x)$$

$$r(x) \longleftrightarrow w \in F^n.$$

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \subseteq F^7$

$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1),$
$(1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \subseteq F[x]$ y $R = F[x]/I$.

Cada $f(x) \in F[x]$ tiene un representante en R con grado menor o igual a $n-1$:

$$f(x) = (x^n - 1)q(x) + r(x)$$
$$\updownarrow$$
$$w \in F^n.$$

Prop: Un código C de longitud n es cíclico sii los elementos correspondientes forman un ideal en R.

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \subseteq F^7$

$$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1), (1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \subseteq F[x]$ y $R = F[x]/I$.

Cada $f(x) \in F[x]$ tiene un representante en R con grado menor o igual a $n-1$:

$$f(x) = (x^n - 1) q(x) + \underbrace{r(x)}_{\displaystyle w \in F^n.}$$

Prop: Un código C de longitud n es cíclico sii los elementos correspondientes forman un ideal en R.

Dem: El desplazamiento cíclico correspondiente a multiplicar por x:

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un código cíclico si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \subseteq F^7$

$$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1), (1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \subseteq F[x]$ y $R = F[x]/I$.

Cada $f(x) \in F[x]$ tiene un representante en R con grado menor o igual a $n-1$:

$$f(x) = (x^n - 1) q(x) + r(x)$$
$$r(x) \longleftrightarrow w \in F^n.$$

Prop: Un código C de longitud n es cíclico sii los elementos correspondientes forman un ideal en R.

Dem: El desplazamiento cíclico correspondiente a multiplicar por x:

$$w = a_0 \cdots a_{n-1} \longrightarrow a_{n-1} a_0 \cdots a_{n-2}$$

$$w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

$$a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}$$

$=$

Códigos ~~lineales~~ cíclicos

Def: Sea C un código lineal es un <u>código cíclico</u> si, para cada palabra código $c = c_1 \cdots c_n \in C$, también la palabra $c_n c_1 \cdots c_{n-1} \in$

Ejemplo

$F = \mathbb{F}_2$, $C \subseteq F^7$

$C = \{(0,0,0,0,0,0,0), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1),$
$(1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,0,0,1,0,1,1)\}$

Para describir C es mejor enumerar las coordenadas de 0 a $n-1$.

$$w = a_0 \cdots a_{n-1} \in F \longleftrightarrow w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x].$$

Sea $I = (x^n - 1) \subseteq F[x]$ y $R = F[x]/I$.

Cada $f(x) \in F[x]$ tiene un representante en R con grado menor o igual a $n-1$:

$$f(x) = (x^n - 1) q(x) + r(x)$$
$$r(x) \longleftrightarrow w \in F^n.$$

Prop: Un código C de longitud n es cíclico sii los elementos correspondientes forman un ideal en R.

Dem: El desplazamiento cíclico correspondiente a multiplicar por x:

$$w = a_0 \cdots a_{n-1} \longrightarrow a_{n-1} a_0 \cdots a_{n-2}$$
$$w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \qquad a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}$$

$$x\, w(x) = a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} + a_{n-1} x^n = a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}$$

en R $x^n - 1 = 0 \iff x^n = 1$!

Ahora, si C es un ideal, es cerrado por suma y multiplicación por un escalar (i.e.: C es un código lineal), y por x (y C es cí=clico).

Ahora, si C es un ideal, es cerrado por suma y multiplicación por un escalar (i.e.: C es un código lineal), y por x (y C es cí= clico).

De ~~la~~ otro lado, si C es cíclico es cerrado bajo la suma y multiplicación por escalar o x. Combinando estas operaciones obtenemos todos los polinomios y entonces C es un ideal. $\square$