Códigos Cíclicos

Daniel Penazzi

May 28, 2022

Tabla de Contenidos

1. Definiciones y nociones básicas
   - Definición de Códigos Cíclicos
   - Polinomios
   - Utilidad de mirar las palabras como polinomios
2. Polinomio Generador
   - Definición
   - Teorema fundamental de Códigos Cíclicos

Códigos Cíclicos

- Una clase importante de códigos lineales son los códigos cíclicos.

Códigos Cíclicos

- Una clase importante de códigos lineales son los códigos cíclicos.
- Son una clase de códigos lineales con algunas propiedades extras que hacen que el codificado y decodificado de las palabras sea mas eficiente.

Códigos Cíclicos

- Una clase importante de códigos lineales son los códigos cíclicos.
- Son una clase de códigos lineales con algunas propiedades extras que hacen que el codificado y decodificado de las palabras sea mas eficiente.
- Ademas, en el caso de corrección de mas de un error, tienen un algoritmo mas eficiente que el que podria obtenerse para un código lineal general.

Códigos Cíclicos

- Una clase importante de códigos lineales son los códigos cíclicos.
- Son una clase de códigos lineales con algunas propiedades extras que hacen que el codificado y decodificado de las palabras sea mas eficiente.
- Ademas, en el caso de corrección de mas de un error, tienen un algoritmo mas eficiente que el que podria obtenerse para un código lineal general.
- Y otra propiedad que tienen es que son muy eficientes para corregir “errores en ráfaga"

Códigos Cíclicos

- Una clase importante de códigos lineales son los códigos cíclicos.
- Son una clase de códigos lineales con algunas propiedades extras que hacen que el codificado y decodificado de las palabras sea mas eficiente.
- Ademas, en el caso de corrección de mas de un error, tienen un algoritmo mas eficiente que el que podria obtenerse para un código lineal general.
- Y otra propiedad que tienen es que son muy eficientes para corregir “errores en ráfaga"
- Es decir, cuando las condiciones son tales que es mas probable tener errores en un cierto segmento que aleatoriamente a lo largo de la transmisión.

Códigos Cíclicos

Definición

Un código es cíclico si es lineal y la rotación de cualquiera de sus palabras es otra palabra del código.

Códigos Cíclicos

Definición

Un código es cíclico si es lineal y la rotación de cualquiera de sus palabras es otra palabra del código.

- Por ejemplo $\{000, 011, 101, 110\}$ es cíclico pues cumple ambas propiedades.

Códigos Cíclicos

Definición

Un código es **cíclico** si es lineal y la rotación de cualquiera de sus palabras es otra palabra del código.

- Por ejemplo $\{000, 011, 101, 110\}$ es cíclico pues cumple ambas propiedades.
- Pero $\{000, 001, 110, 111\}$ no lo es pues es lineal pero la rotación de la palabra 001 en un bit a izquierda o derecha (es decir, 010 o 100) no está en el código.

Códigos Cíclicos

Definición

Un código es cíclico si es lineal y la rotación de cualquiera de sus palabras es otra palabra del código.

- Por ejemplo $\{000, 011, 101, 110\}$ es cíclico pues cumple ambas propiedades.
- Pero $\{000, 001, 110, 111\}$ no lo es pues es lineal pero la rotación de la palabra 001 en un bit a izquierda o derecha (es decir, 010 o 100) no está en el código.
- $\{000, 001, 010, 100\}$ cumple que la rotación de cualquier palabra es una palabra del código, pero no es lineal, asi que no es un código cíclico.

Códigos Cíclicos

Definición

Un código es cíclico si es lineal y la rotación de cualquiera de sus palabras es otra palabra del código.

- Por ejemplo $\{000, 011, 101, 110\}$ es cíclico pues cumple ambas propiedades.
- Pero $\{000, 001, 110, 111\}$ no lo es pues es lineal pero la rotación de la palabra 001 en un bit a izquierda o derecha (es decir, 010 o 100) no está en el código.
- $\{000, 001, 010, 100\}$ cumple que la rotación de cualquier palabra es una palabra del código, pero no es lineal, asi que no es un código cíclico.
- A los códigos cíclicos también se los llama CRC (Cyclic redundancy code)

Cambio de notación

Notación

Por motivos que resultaran claros en breve, en vez de denotar las palabras como $w_1...w_n$, las denotaremos como $w_0...w_{n-1}$

Cambio de notación

Notación

Por motivos que resultaran claros en breve, en vez de denotar las palabras como $w_1...w_n$, las denotaremos como $w_0...w_{n-1}$

Definición

Dada una palabra $w = w_0 w_1 \dots\dots w_{n-2} w_{n-1}$, definimos la rotación (o cyclic shift) de w como la palabra $rot(w) = w_{n-1} w_0 w_1 \dots\dots w_{n-2}$

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.
- Como *rot* es lineal, tambien tenemos que un código es cíclico sii es lineal y existe una base de C tal que $rot(w) \in C$ para toda palabra w de la base.

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.
- Como *rot* es lineal, tambien tenemos que un código es cíclico sii es lineal y existe una base de C tal que $rot(w) \in C$ para toda palabra w de la base.
- Por lo tanto es fácil construir códigos cíclicos:

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.
- Como *rot* es lineal, tambien tenemos que un código es cíclico sii es lineal y existe una base de C tal que $rot(w) \in C$ para toda palabra w de la base.
- Por lo tanto es fácil construir códigos cíclicos:
  - Basta tomar una palabra w cualquiera, y tomar el espacio vectorial generado por el conjunto $\{w, rot(w), rot^2(w), ..., rot^{n-1}(w)\}$.

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.
- Como *rot* es lineal, tambien tenemos que un código es cíclico sii es lineal y existe una base de C tal que $rot(w) \in C$ para toda palabra w de la base.
- Por lo tanto es fácil construir códigos cíclicos:
  - Basta tomar una palabra w cualquiera, y tomar el espacio vectorial generado por el conjunto $\{w, rot(w), rot^2(w), ..., rot^{n-1}(w)\}$.
- Como $rot^n(w) = w$, ese conjunto es cerrado por la operacion *rot*

Códigos Cíclicos

- Dado que $rot^2(w) = w_{n-2}w_{n-1}w_0...w_{n-3}$, etc, esta claro que C es cíclico si C es lineal y se cumple que $w \in C \Rightarrow rot(w) \in C$.
- Como *rot* es lineal, tambien tenemos que un código es cíclico sii es lineal y existe una base de C tal que $rot(w) \in C$ para toda palabra w de la base.
- Por lo tanto es fácil construir códigos cíclicos:
  - Basta tomar una palabra w cualquiera, y tomar el espacio vectorial generado por el conjunto $\{w, rot(w), rot^2(w), ..., rot^{n-1}(w)\}$.
- Como $rot^n(w) = w$, ese conjunto es cerrado por la operacion *rot*
- Como genera C, podemos extraer una base del mismo que cumple la propiedad anterior.

Códigos Cíclicos

- El problema con hacer esto es que no tenemos la menor idea de cual sera la dimensión de C, por ejemplo.

Códigos Cíclicos

- El problema con hacer esto es que no tenemos la menor idea de cual sera la dimensión de C, por ejemplo.
- Veremos que podemos elejir la palabra w mas cuidadosamente, de forma tal de obtener una base que consistirá en las primeras k rotaciónes de w.

Códigos Cíclicos

- El problema con hacer esto es que no tenemos la menor idea de cual sera la dimensión de C, por ejemplo.
- Veremos que podemos elejir la palabra w mas cuidadosamente, de forma tal de obtener una base que consistirá en las primeras k rotaciónes de w.
- Ademas, esta palabra w especial tendra otras propiedades que la harán muy efectiva.

Códigos Cíclicos

- El problema con hacer esto es que no tenemos la menor idea de cual sera la dimensión de C, por ejemplo.
- Veremos que podemos elejir la palabra w mas cuidadosamente, de forma tal de obtener una base que consistirá en las primeras k rotaciónes de w.
- Ademas, esta palabra w especial tendra otras propiedades que la harán muy efectiva.
- En particular, en vez de tener que guardar toda una matriz $k \times n$ generadora, o $r \times (r + k)$ de chequeo, bastará guardar una sola palabra de longitud n.

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.
- Cuando yo era estudiante, nos enseñaban bien esta diferencia en primer año de famaf, pero creo que la calidad ha decaido y no estoy seguro si siguen haciendolo.

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.
- Cuando yo era estudiante, nos enseñaban bien esta diferencia en primer año de famaf, pero creo que la calidad ha decaido y no estoy seguro si siguen haciendolo.
- Asi que repasaremos un poco acerca de polinomios.

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.
- Cuando yo era estudiante, nos enseñaban bien esta diferencia en primer año de famaf, pero creo que la calidad ha decaido y no estoy seguro si siguen haciendolo.
- Asi que repasaremos un poco acerca de polinomios.
- Todos “sabemos" que los polinomios son “cosas" como $1 + x, 2 + x^2, x + x^4 + 5x^7 + x^{10}$, etc

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.
- Cuando yo era estudiante, nos enseñaban bien esta diferencia en primer año de famaf, pero creo que la calidad ha decaido y no estoy seguro si siguen haciendolo.
- Asi que repasaremos un poco acerca de polinomios.
- Todos “sabemos" que los polinomios son “cosas" como $1+x, 2+x^2, x+x^4+5x^7+x^{10}$, etc
- En general, algo de la forma $\sum_{i=0}^{d} a_i x^i$.

Álgebra

- Hay una cosa que debería quedar claro en el secundario, pero nunca o casi nunca la enseñan bien.
- Cuando yo era estudiante, nos enseñaban bien esta diferencia en primer año de famaf, pero creo que la calidad ha decaido y no estoy seguro si siguen haciendolo.
- Asi que repasaremos un poco acerca de polinomios.
- Todos “sabemos" que los polinomios son “cosas" como $1+x, 2+x^2, x+x^4+5x^7+x^{10}$, etc
- En general, algo de la forma $\sum_{i=0}^{d} a_i x^i$.
- Pero ¿qué son, exactamente, esas “cosas"?

Polinomios

- Uno esta tentado a decir que son funciones, pero eso esta mal.

Polinomios

- Uno esta tentado a decir que son funciones, pero eso esta mal.
- Una función polinómica es una función de la forma $f(x) = \sum_{i=0}^{d} a_i x^i$, definida en algún lugar donde tenga sentido la suma y el producto con algunas propiedades minimas, es decir, en un anillo.

Polinomios

- Uno esta tentado a decir que son funciones, pero eso esta mal.
- Una función polinómica es una función de la forma $f(x) = \sum_{i=0}^{d} a_i x^i$, definida en algún lugar donde tenga sentido la suma y el producto con algunas propiedades minimas, es decir, en un anillo.
- Pero eso no es un polinomio.

Polinomios

- Uno esta tentado a decir que son funciones, pero eso esta mal.
- Una función polinómica es una función de la forma $f(x) = \sum_{i=0}^{d} a_i x^i$, definida en algún lugar donde tenga sentido la suma y el producto con algunas propiedades minimas, es decir, en un anillo.
- Pero eso no es un polinomio.
- La confusión viene porque en $\mathbb{R}$ las dos cosas se pueden identificar: toda función polinómica “es" un polinomio y viceversa.

Polinomios

- Uno esta tentado a decir que son funciones, pero eso esta mal.
- Una función polinómica es una función de la forma $f(x) = \sum_{i=0}^{d} a_i x^i$, definida en algún lugar donde tenga sentido la suma y el producto con algunas propiedades minimas, es decir, en un anillo.
- Pero eso no es un polinomio.
- La confusión viene porque en $\mathbb{R}$ las dos cosas se pueden identificar: toda función polinómica “es" un polinomio y viceversa.
- Pero en otros anillos eso no pasa.

Polinomios

- La propiedad fundamental que tienen los polinomios es que si $\sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{r} b_i x^i$ con a_d, b_r no nulos, entonces $d = r$ y $a_i = b_i$ para todo i.

Polinomios

- La propiedad fundamental que tienen los polinomios es que si $\sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{r} b_i x^i$ con a_d, b_r no nulos, entonces $d = r$ y $a_i = b_i$ para todo i.
- Entonces por ejemplo en $\{0,1\}$, los polinomios $1 + x$ y $1 + x^2$ son distintos, pero las funciones polinomicas $x \mapsto 1 + x$ y $1 + x^2$ son iguales, pues dos funciones f, g son iguales sii $f(x) = g(x)$ para todo x, y $1 + x = 1 + x^2$ para todo $x \in \{0,1\}$.

Polinomios

- La propiedad fundamental que tienen los polinomios es que si $\sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{r} b_i x^i$ con a_d, b_r no nulos, entonces $d = r$ y $a_i = b_i$ para todo i.
- Entonces por ejemplo en $\{0, 1\}$, los polinomios $1 + x$ y $1 + x^2$ son distintos, pero las funciones polinomicas $x \mapsto 1 + x$ y $1 + x^2$ son iguales, pues dos funciones f, g son iguales sii $f(x) = g(x)$ para todo x, y $1 + x = 1 + x^2$ para todo $x \in \{0, 1\}$.
- Asi que en general se define un polinomio simplemente como la “suma formal" $\sum_{i=0}^{d} a_i x^i$.

Polinomios

- La propiedad fundamental que tienen los polinomios es que si $\sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{r} b_i x^i$ con a_d, b_r no nulos, entonces $d = r$ y $a_i = b_i$ para todo i.
- Entonces por ejemplo en $\{0,1\}$, los polinomios $1+x$ y $1+x^2$ son distintos, pero las funciones polinomicas $x \mapsto 1+x$ y $1+x^2$ son iguales, pues dos funciones f, g son iguales sii $f(x) = g(x)$ para todo x, y $1+x = 1+x^2$ para todo $x \in \{0,1\}$.
- Asi que en general se define un polinomio simplemente como la "suma formal" $\sum_{i=0}^{d} a_i x^i$.
- Esto parece un acto de magia, pero se puede definir formalmente.

Polinomios

- La propiedad fundamental que tienen los polinomios es que si $\sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{r} b_i x^i$ con a_d, b_r no nulos, entonces $d = r$ y $a_i = b_i$ para todo i.
- Entonces por ejemplo en $\{0, 1\}$, los polinomios $1 + x$ y $1 + x^2$ son distintos, pero las funciones polinomicas $x \mapsto 1 + x$ y $1 + x^2$ son iguales, pues dos funciones f, g son iguales sii $f(x) = g(x)$ para todo x, y $1 + x = 1 + x^2$ para todo $x \in \{0, 1\}$.
- Asi que en general se define un polinomio simplemente como la "suma formal" $\sum_{i=0}^{d} a_i x^i$.
- Esto parece un acto de magia, pero se puede definir formalmente.
- Hay varias formas, ahora explico una que es la que nos será útil.

Polinomios

- Se define "x" como la palabra infinita 010.....

Polinomios

- Se define “x" como la palabra infinita 010.....
- x^2 como 001000...

Polinomios

- Se define "x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.

Polinomios

- Se define “x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.
- Y la suma y multiplicación de constantes de la forma obvia.

Polinomios

- Se define "x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.
- Y la suma y multiplicación de constantes de la forma obvia.
- Asi, $1 + x^4 + 5x^7 + 8x^{10} = 10001005008001...$

Polinomios

- Se define "x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.
- Y la suma y multiplicación de constantes de la forma obvia.
- Asi, $1 + x^4 + 5x^7 + 8x^{10} = 1000100500800....$
- Un polinomio entonces será simplemente una palabra infinita pero tal que tenga una cantidad finita de entradas no nulas.

Polinomios

- Se define “x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.
- Y la suma y multiplicación de constantes de la forma obvia.
- Asi, $1+x^4+5x^7+8x^{10}=100010050080 0\ldots$
- Un polinomio entonces será simplemente una palabra infinita pero tal que tenga una cantidad finita de entradas no nulas.
- Asi que las entradas infinitas nulas a derecha pueden no escribirse y se puede escribir $1+x^4+5x^7+8x^{10}=10001005008$ entendiendo que luego siguen todos ceros.

Polinomios

- Se define "x" como la palabra infinita 010.....
- x^2 como 001000...
- y en general x^i como la palabra infinita a derecha que tiene un 1 en la posición im contando desde 0, y cero en las otras.
- Y la suma y multiplicación de constantes de la forma obvia.
- Asi, $1 + x^4 + 5x^7 + 8x^{10} = 1000100500800....$
- Un polinomio entonces será simplemente una palabra infinita pero tal que tenga una cantidad finita de entradas no nulas.
- Asi que las entradas infinitas nulas a derecha pueden no escribirse y se puede escribir $1 + x^4 + 5x^7 + 8x^{10} = 10001005008$ entendiendo que luego siguen todos ceros.
- Luego se define la multiplicación entre polinomios de forma tal que obedezca las reglas que ya conocemos.

Lo importante

- Si no leyeron nada de lo anterior, o leyeron pero no entendieron, lo importante que les debe quedar, y que es lo que vamos a usar es lo siguiente:

Lo importante

- Si no leyeron nada de lo anterior, o leyeron pero no entendieron, lo importante que les debe quedar, y que es lo que vamos a usar es lo siguiente:

Clave

La palabra $w_0 w_1 .... w_{n-1}$ se puede pensar como el polinomio $w_0 + w_1 x + w_2 x^2 + \cdots + w_{n-1} x^{n-1}$.

Lo importante

- Si no leyeron nada de lo anterior, o leyeron pero no entendieron, lo importante que les debe quedar, y que es lo que vamos a usar es lo siguiente:

Clave

La palabra $w_0 w_1 \ldots. w_{n-1}$ se puede pensar como el polinomio $w_0 + w_1 x + w_2 x^2 + \cdots + w_{n-1} x^{n-1}$.

- Por ejemplo, $1010 = 1 + x^2$

Lo importante

- Si no leyeron nada de lo anterior, o leyeron pero no entendieron, lo importante que les debe quedar, y que es lo que vamos a usar es lo siguiente:

Clave

La palabra $w_0 w_1 .... w_{n-1}$ se puede pensar como el polinomio $w_0 + w_1 x + w_2 x^2 + \cdots + w_{n-1} x^{n-1}$.

- Por ejemplo, $1010 = 1 + x^2$
- Advertencia: en algunos textos la identificación es asumiendo que el termino de mas a la izquierda es el termino de MAYOR grado. En ese caso, 1010 representa al polinomio $x^3 + x$ y no al $1 + x^2$, asi que hay que prestar atención a cual identificación se hace.

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?
- Que los polinomios se pueden multiplicar.

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?
- Que los polinomios se pueden multiplicar.
- Y entonces se pueden mirar los códigos con una estructura algebraica mas “rica" que permite deducir propiedades.

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?
- Que los polinomios se pueden multiplicar.
- Y entonces se pueden mirar los códigos con una estructura algebraica mas “rica" que permite deducir propiedades.
- Pero hay un small problem.

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?
- Que los polinomios se pueden multiplicar.
- Y entonces se pueden mirar los códigos con una estructura algebraica mas “rica" que permite deducir propiedades.
- Pero hay un small problem.
- Dado que estamos trabajando con códigos de longitud n, entonces estamos trabajando con polinomios de grado menor que n. (es decir, el termino no nulo de grado mas alto es $n-1$ o menor)

Palabras y polinomios

- ¿Que ganamos pensando en una palabra como un polinomio?
- Que los polinomios se pueden multiplicar.
- Y entonces se pueden mirar los códigos con una estructura algebraica mas “rica" que permite deducir propiedades.
- Pero hay un small problem.
- Dado que estamos trabajando con códigos de longitud n, entonces estamos trabajando con polinomios de grado menor que n. (es decir, el termino no nulo de grado mas alto es $n-1$ o menor)
- Y si multiplicamos polinomios el grado crece.

Palabras y polinomios

- Por ejemplo, si multiplicaramos:

Palabras y polinomios

- Por ejemplo, si multiplicaramos:
- $1010.0110 = (1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = 01111$

Palabras y polinomios

- Por ejemplo, si multiplicaramos:
- $1010.0110 = (1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = 01111$
- Pasariamos de palabras de longitud 4 a palabras de longitud 5.

Palabras y polinomios

- Por ejemplo, si multiplicaramos:
- $1010.0110 = (1+x^2)(x+x^2) = x+x^2+x^3+x^4 = 01111$
- Pasariamos de palabras de longitud 4 a palabras de longitud 5.
- Pero queremos quedarnos “dentro" de las palabras de longitud 4, pues queremos trabajar con códigos de bloque.

Palabras y polinomios

- Por ejemplo, si multiplicaramos:
- $1010.0110 = (1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = 01111$
- Pasariamos de palabras de longitud 4 a palabras de longitud 5.
- Pero queremos quedarnos “dentro" de las palabras de longitud 4, pues queremos trabajar con códigos de bloque.
- Para resolver ese problema, tomamos módulo, porque otra cosa que se puede hacer con polinomios es dividir.

Códigos Cíclicos

Definición

Si $p(x)$ y $m(x)$ son polinomios, entonces "$p(x) \bmod m(x)$" denotará el resto de la division de $p(x)$ por $m(x)$.
Es decir, $p(x) \bmod m(x)$ es el único polinomio $r(x)$ de grado menor que el grado de $m(x)$ tal que existe un polimonio $q(x)$ con $p(x) = q(x)m(x) + r(x)$

Códigos Cíclicos

Definición

Si $p(x)$ y $m(x)$ son polinomios, entonces "$p(x) \bmod m(x)$" denotará el resto de la division de $p(x)$ por $m(x)$.
Es decir, $p(x) \bmod m(x)$ es el único polinomio $r(x)$ de grado menor que el grado de $m(x)$ tal que existe un polimonio $q(x)$ con
$p(x) = q(x)m(x) + r(x)$

- Tambien diremos que $p(x) \equiv q(x)_{(\bmod h(x))}$ sii:

Códigos Cíclicos

Definición

Si $p(x)$ y $m(x)$ son polinomios, entonces “$p(x) \bmod m(x)$" denotará el resto de la division de $p(x)$ por $m(x)$.
Es decir, $p(x) \bmod m(x)$ es el único polinomio $r(x)$ de grado menor que el grado de $m(x)$ tal que existe un polimonio $q(x)$ con $p(x) = q(x)m(x) + r(x)$

- Tambien diremos que $p(x) \equiv q(x)_{(\bmod h(x))}$ sii:
  - $p(x) \bmod h(x) = q(x) \bmod h(x)$.

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n
  - es decir, multiplicar dos polinomios de grado menor que n y obtener otro polinomio de grado menor que n

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n
    - es decir, multiplicar dos polinomios de grado menor que n y obtener otro polinomio de grado menor que n
- bastará con multiplicar los polinomios correspondientes y luego tomar modulo algun polinomio de grado n.

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n
  - es decir, multiplicar dos polinomios de grado menor que n y obtener otro polinomio de grado menor que n
- bastará con multiplicar los polinomios correspondientes y luego tomar modulo algun polinomio de grado n.
- Por ejemplo, podriamos tomar el producto módulo x^n.

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n
  - es decir, multiplicar dos polinomios de grado menor que n y obtener otro polinomio de grado menor que n
- bastará con multiplicar los polinomios correspondientes y luego tomar modulo algun polinomio de grado n.
- Por ejemplo, podriamos tomar el producto módulo x^n.
- Pero será mejor tomar el producto módulo $1 + x^n$

- Por lo tanto, si queremos “multiplicar" dos palabras de longitud n y obtener otra vez una palabra de longitud n
  - es decir, multiplicar dos polinomios de grado menor que n y obtener otro polinomio de grado menor que n
- bastará con multiplicar los polinomios correspondientes y luego tomar modulo algun polinomio de grado n.
- Por ejemplo, podriamos tomar el producto módulo x^n.
- Pero será mejor tomar el producto módulo $1 + x^n$
- Para no confundirnos con la multiplicación usual de polinomios, la denotaremos con un simbolo especial

Códigos Cíclicos

Notación

Dadas dos palabras v y w de longitud n, identificadas con los polinomios $v(x)$, $w(x)$, definimos:

$$v \odot w = v(x)w(x) \mod (1 + x^n)$$

Códigos Cíclicos

Notación

Dadas dos palabras v y w de longitud n, identificadas con los polinomios $v(x)$, $w(x)$, definimos:

$$v \odot w = v(x)w(x) \mod (1 + x^n)$$

- Nota: en ocasiones extenderemos la definición a casos donde una de las palabras tenga mas de n bits, definiendola de la misma forma.

Códigos Cíclicos

Notación

Dadas dos palabras v y w de longitud n, identificadas con los polinomios $v(x)$, $w(x)$, definimos:

$$v \odot w = v(x)w(x) \mod (1 + x^n)$$

- Nota: en ocasiones extenderemos la definición a casos donde una de las palabras tenga mas de n bits, definiendola de la misma forma.
- Ejemplo: Si $n = 4$ tenemos:

$$1010 \odot 0110 \quad = \quad (1 + x^2)(x + x^2) \bmod 1 + x^4$$

Códigos Cíclicos

Notación

Dadas dos palabras v y w de longitud n, identificadas con los polinomios $v(x)$, $w(x)$, definimos:

$$v \odot w = v(x)w(x) \mod (1 + x^n)$$

- Nota: en ocasiones extenderemos la definición a casos donde una de las palabras tenga mas de n bits, definiendola de la misma forma.
- Ejemplo: Si $n = 4$ tenemos:

$$\begin{aligned} 1010 \odot 0110 &= (1 + x^2)(x + x^2) \text{ mod } 1 + x^4 \\ &= (x + x^2 + x^3 + x^4) \text{ mod } 1 + x^4 \end{aligned}$$

Códigos Cíclicos

Notación

Dadas dos palabras v y w de longitud n, identificadas con los polinomios $v(x)$, $w(x)$, definimos:

$$v \odot w = v(x)w(x) \mod (1 + x^n)$$

- Nota: en ocasiones extenderemos la definición a casos donde una de las palabras tenga mas de n bits, definiendola de la misma forma.
- Ejemplo: Si $n = 4$ tenemos:

$$\begin{aligned} 1010 \odot 0110 &= (1 + x^2)(x + x^2) \mod 1 + x^4 \\ &= (x + x^2 + x^3 + x^4) \mod 1 + x^4 \\ &= 1 + x + x^2 + x^3 = 1111 \end{aligned}$$

Códigos Cíclicos

- Para tomar módulo $1 + x^n$ no hace falta dividir el polinomio por $1 + x^n$ y calcular el resto.

Códigos Cíclicos

- Para tomar módulo $1 + x^n$ no hace falta dividir el polinomio por $1 + x^n$ y calcular el resto.
- Basta recordar que $\mod$ es lineal

Códigos Cíclicos

- Para tomar módulo $1+x^n$ no hace falta dividir el polinomio por $1+x^n$ y calcular el resto.
- Basta recordar que $\bmod$ es lineal
- Por lo tanto,como $(1+x^n) \bmod (1+x^n) = 0$, entonces obviamente $x^n \bmod (1+x^n) = 1$.

Códigos Cíclicos

- Para tomar módulo $1+x^n$ no hace falta dividir el polinomio por $1+x^n$ y calcular el resto.
- Basta recordar que $\bmod$ es lineal
- Por lo tanto,como $(1+x^n) \bmod (1+x^n)=0$, entonces obviamente $x^n \bmod (1+x^n)=1$.
- (esto ultimo pues estamos trabajando en $\{0,1\}$)

Códigos Cíclicos

- Para tomar módulo $1+x^n$ no hace falta dividir el polinomio por $1+x^n$ y calcular el resto.
- Basta recordar que $\mod$ es lineal
- Por lo tanto,como $(1+x^n) \mod (1+x^n) = 0$, entonces obviamente $x^n \mod (1+x^n) = 1$.
- (esto ultimo pues estamos trabajando en $\{0,1\}$)
- Se puede ver esto directamente: $x^n = (1+x^n).1+1$.

Códigos Cíclicos

- Para tomar módulo $1 + x^n$ no hace falta dividir el polinomio por $1 + x^n$ y calcular el resto.
- Basta recordar que mod es lineal
- Por lo tanto,como $(1 + x^n) \bmod (1 + x^n) = 0$, entonces obviamente $x^n \bmod (1 + x^n) = 1$.
- (esto ultimo pues estamos trabajando en $\{0, 1\}$)
- Se puede ver esto directamente: $x^n = (1 + x^n).1 + 1$.
- En general si se trabaja en entornos donde $1 \neq -1$, en vez de tomar el polinomio $1 + x^n$ como módulo, se toma el polinomio $-1 + x^n$.

Códigos Cíclicos

- Para tomar módulo $1 + x^n$ no hace falta dividir el polinomio por $1 + x^n$ y calcular el resto.
- Basta recordar que $\mod$ es lineal
- Por lo tanto,como $(1 + x^n) \mod (1 + x^n) = 0$, entonces obviamente $x^n \mod (1 + x^n) = 1$.
- (esto ultimo pues estamos trabajando en $\{0, 1\}$)
- Se puede ver esto directamente: $x^n = (1 + x^n).1 + 1$.
- En general si se trabaja en entornos donde $1 \neq -1$, en vez de tomar el polinomio $1 + x^n$ como módulo, se toma el polinomio $-1 + x^n$.
- Pues $x^n \mod (-1 + x^n) = 1$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

$$x \odot w(x) \quad = \quad x(w_0 + w_1 x + \ldots + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod (1 + x^n)$$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

$$\begin{aligned} x \odot w(x) &= x(w_0 + w_1 x + \ldots + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod (1 + x^n) \\ &= (w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1}x^n) \bmod (1 + x^n) \end{aligned}$$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

$$\begin{aligned} x \odot w(x) &= x(w_0 + w_1 x + \ldots + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod (1 + x^n) \\ &= (w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1}x^n) \bmod (1 + x^n) \\ &= w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1} \end{aligned}$$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

$$\begin{aligned}
x \odot w(x) &= x(w_0 + w_1 x + \ldots + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod (1 + x^n) \\
&= (w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1}x^n) \bmod (1 + x^n) \\
&= w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1} \\
&= w_{n-1} + w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1}
\end{aligned}$$

Clave para la utilidad de los códigos cíclicos

Propiedad

$$rot(w) = x \odot w(x)$$

Prueba:

$$\begin{aligned}
x \odot w(x) &= x(w_0 + w_1 x + \ldots + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod (1 + x^n) \\
&= (w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1}x^n) \bmod (1 + x^n) \\
&= w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} + w_{n-1} \\
&= w_{n-1} + w_0 x + w_1 x^2 + \ldots + w_{n-2}x^{n-1} \\
&= rot(w)
\end{aligned}$$

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)
- Por lo tanto $x^i \odot w \in C$ para todo i.

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)
- Por lo tanto $x^i \odot w \in C$ para todo i.
- Como C, al ser cíclico, es lineal, entonces cualquier combinación lineal de $x^i \odot w$ estará en C.

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)
- Por lo tanto $x^i \odot w \in C$ para todo i.
- Como C, al ser cíclico, es lineal, entonces cualquier combinación lineal de $x^i \odot w$ estará en C.
- Es decir, $\sum a_i(x^i \odot w) \in C$ para cualesquiera a_i.

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)
- Por lo tanto $x^i \odot w \in C$ para todo i.
- Como C, al ser cíclico, es lineal, entonces cualquier combinación lineal de $x^i \odot w$ estará en C.
- Es decir, $\sum a_i(x^i \odot w) \in C$ para cualesquiera a_i.
- Pero $\sum a_i(x^i \odot w) = (\sum a_i x^i) \odot w$.

Clave para la utilidad de los códigos cíclicos

Propiedad

Sea C un código cíclico, $w \in C$ y v una palabra cualquiera. Entonces $v \odot w \in C$.

- Prueba: por la propiedad anterior, $x \odot w = rot(w) \in C$ (pues C es cíclico)
- Por lo tanto $x^i \odot w \in C$ para todo i.
- Como C, al ser cíclico, es lineal, entonces cualquier combinación lineal de $x^i \odot w$ estará en C.
- Es decir, $\sum a_i(x^i \odot w) \in C$ para cualesquiera a_i.
- Pero $\sum a_i(x^i \odot w) = (\sum a_i x^i) \odot w$.
- Concluimos que $v \odot w \in C$ para cualesquiera $v = \sum a_i x^i$.

Ideales

- En matemática a un objeto que tiene esa propiedad “absorbente" se le llama un ideal.

Ideales

- En matemática a un objeto que tiene esa propiedad “absorbente" se le llama un ideal.
- Asi que un código cíclico es un ideal.

Ideales

- En matemática a un objeto que tiene esa propiedad “absorbente" se le llama un ideal.
- Asi que un código cíclico es un ideal.
- Para seguir con las propiedades de códigos cíclicos, enunciaremos una propiedad que vale para cualquier código lineal.

Ideales

- En matemática a un objeto que tiene esa propiedad “absorbente" se le llama un ideal.
- Asi que un código cíclico es un ideal.
- Para seguir con las propiedades de códigos cíclicos, enunciaremos una propiedad que vale para cualquier código lineal.
- Sólo que es una propiedad útil exclusivamente en el caso de los códigos cíclicos, por eso no la dimos antes.

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

- Nota: esta propiedad vale sólo en $\{0, 1\}$. Si no estamos en $\{0, 1\}$ hay que agregar la condición de que sea mónico para la unicidad.

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

- Nota: esta propiedad vale sólo en $\{0, 1\}$. Si no estamos en $\{0, 1\}$ hay que agregar la condición de que sea mónico para la unicidad.
- Prueba: Supongamos que hubiera dos distintos: $g_1 \neq g_2$.

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

- Nota: esta propiedad vale sólo en $\{0, 1\}$. Si no estamos en $\{0, 1\}$ hay que agregar la condición de que sea mónico para la unicidad.
- Prueba: Supongamos que hubiera dos distintos: $g_1 \neq g_2$.
- Como son distintos, y estamos en $\{0, 1\}$, $g_1 + g_2 \neq 0$.

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

- Nota: esta propiedad vale sólo en $\{0, 1\}$. Si no estamos en $\{0, 1\}$ hay que agregar la condición de que sea mónico para la unicidad.
- Prueba: Supongamos que hubiera dos distintos: $g_1 \neq g_2$.
- Como son distintos, y estamos en $\{0, 1\}$, $g_1 + g_2 \neq 0$.
- Como C es lineal, $g_1 + g_2$ está en C.

Códigos Cíclicos

Propiedad

Si C es lineal, entonces existe **un único** polinomio no nulo en C de grado mínimo

- Nota: esta propiedad vale sólo en $\{0,1\}$. Si no estamos en $\{0,1\}$ hay que agregar la condición de que sea mónico para la unicidad.
- Prueba: Supongamos que hubiera dos distintos: $g_1 \neq g_2$.
- Como son distintos, y estamos en $\{0,1\}$, $g_1 + g_2 \neq 0$.
- Como C es lineal, $g_1 + g_2$ está en C.
- Pero ¿cual es el grado de $g_1 + g_2$?

Continuación prueba

- Sea t el grado común a g_1, g_2.

Continuación prueba

- Sea t el grado común a g_1, g_2.
- Ambos son de la forma x^t+cosas de grado mas chico.

Continuación prueba

- Sea t el grado común a g_1, g_2.
- Ambos son de la forma x^t+cosas de grado mas chico.
- Por lo tanto, al sumarlos, queda $x^t + x^t+$cosas de grado mas chico.

Continuación prueba

- Sea t el grado común a g_1, g_2.
- Ambos son de la forma x^t+cosas de grado mas chico.
- Por lo tanto, al sumarlos, queda $x^t + x^t+$cosas de grado mas chico.
- Como estamos en $\{0, 1\}$, $x^t + x^t = 0$

Continuación prueba

- Sea t el grado común a g_1, g_2.
- Ambos son de la forma x^t+cosas de grado mas chico.
- Por lo tanto, al sumarlos, queda $x^t + x^t$+cosas de grado mas chico.
- Como estamos en $\{0, 1\}$, $x^t + x^t = 0$
- Asi que el grado de $g_1 + g_2$ es estrictamente menor que t

Continuación prueba

- Sea t el grado común a g_1, g_2.
- Ambos son de la forma x^t+cosas de grado mas chico.
- Por lo tanto, al sumarlos, queda $x^t + x^t+$cosas de grado mas chico.
- Como estamos en $\{0,1\}$, $x^t + x^t = 0$
- Asi que el grado de $g_1 + g_2$ es estrictamente menor que t
- Absurdo, pues como $g_1 + g_2 \neq 0$, tendriamos un polinomio no nulo de grado mas chico que el menor grado de un polinomio no nulo.

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

- ¿Por qué se le llama el polinomio generador?

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

- ¿Por qué se le llama el polinomio generador?
- Porque vamos a ver que el polinomio genera algebráicamente todo el código.

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

- ¿Por qué se le llama el polinomio generador?
- Porque vamos a ver que el polinomio genera algebráicamente todo el código.
- Por lo tanto, en vez de tener que guardar una matriz generadora, basta con guardar al polinomio generador.

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

- ¿Por qué se le llama el polinomio generador?
- Porque vamos a ver que el polinomio genera algebráicamente todo el código.
- Por lo tanto, en vez de tener que guardar una matriz generadora, basta con guardar al polinomio generador.
- De hecho, hay listas de códigos cíclicos muy utiles en la literatura, y lo único que se dan son los polinomios generadores.

Polinomio Generador

Definición

Si C es cíclico, el único polinomio no nulo de menor grado se llama el polinomio generador y se lo suele denotar por $g(x)$.

- ¿Por qué se le llama el polinomio generador?
- Porque vamos a ver que el polinomio genera algebráicamente todo el código.
- Por lo tanto, en vez de tener que guardar una matriz generadora, basta con guardar al polinomio generador.
- De hecho, hay listas de códigos cíclicos muy utiles en la literatura, y lo único que se dan son los polinomios generadores.
- De hecho, hay tablas de estos códigos, lo que se suele dar en cada entrada son los indices de los coeficientes que son 1.

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

1. C esta formado por los multiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \& g(x) | p(x)\}$

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

1. C esta formado por los multiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \& g(x) | p(x)\}$
2. $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

1. C esta formado por los multiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \& g(x)|p(x)\}$
2. $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$
3. $gr(g(x)) = n - k$.

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

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

Teorema fundamental de códigos cíclicos

Teorema

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n. Entonces:

1. C esta formado por los multiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \& g(x) | p(x)\}$
2. $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$
3. $gr(g(x)) = n - k$.
4. $g(x)$ divide a $1 + x^n$
5. $g_0 = 1$

Prueba

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

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x) | p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.
- Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.
- Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = p(x) + q(x)g(x)$.

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.
- Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = p(x) + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, entonces $r(x) = r(x) \bmod (1 + x^n)$

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.
- Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = p(x) + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, entonces $r(x) = r(x) \bmod (1 + x^n)$
- Como $p(x) \in C$, entonces $gr(p) < n$, y $p(x) = p(x) \bmod (1 + x^n)$

Prueba

- Prueba: Sea $C_1 = \{p(x) : gr(p) < n \& g(x) | p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v$ es un polinomio cualquiera$\}$.
- Por la propiedad que probamos antes, $C_2 \subseteq C$, pues $g(x) \in C$.
- Sea $p(x) \in C$.
- Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = p(x) + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, entonces $r(x) = r(x) \bmod (1 + x^n)$
- Como $p(x) \in C$, entonces $gr(p) < n$, y $p(x) = p(x) \bmod (1 + x^n)$
- Entonces:

Continuación Prueba

$$r(x) \quad = \quad r(x) \bmod (1 + x^n)$$

Continuación Prueba

$$\begin{aligned} r(x) &= r(x) \bmod (1 + x^n) \\ &= (p(x) + q(x)g(x)) \bmod (1 + x^n) \end{aligned}$$

Continuación Prueba

$$
\begin{aligned}
r(x) &= r(x) \bmod (1+x^n)\\
&= (p(x)+q(x)g(x)) \bmod (1+x^n)\\
&= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n)
\end{aligned}
$$

Continuación Prueba

$$
\begin{aligned}
r(x) &= r(x) \bmod (1+x^n) \\
&= (p(x)+q(x)g(x)) \bmod (1+x^n) \\
&= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n) \\
&= p(x) + q \odot g
\end{aligned}
$$

Continuación Prueba

$$
\begin{aligned}
r(x) &= r(x) \bmod (1+x^n) \\
&= (p(x)+q(x)g(x)) \bmod (1+x^n) \\
&= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n) \\
&= p(x) + q \odot g
\end{aligned}
$$

- Como $p(x) \in C$ y $q \odot g \in C$ y C es lineal, concluimos que $r \in C$.

Continuación Prueba

$$
\begin{aligned}
r(x) &= r(x) \bmod (1+x^n) \\
&= (p(x)+q(x)g(x)) \bmod (1+x^n) \\
&= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n) \\
&= p(x) + q \odot g
\end{aligned}
$$

- Como $p(x) \in C$ y $q \odot g \in C$ y C es lineal, concluimos que $r \in C$.
- Pero $gr(r) < gr(g)$ que es el polinomio no nulo de menor grado de C.

Continuación Prueba

$$\begin{aligned} r(x) &= r(x) \bmod (1+x^n) \\ &= (p(x)+q(x)g(x)) \bmod (1+x^n) \\ &= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n) \\ &= p(x) + q \odot g \end{aligned}$$

- Como $p(x) \in C$ y $q \odot g \in C$ y C es lineal, concluimos que $r \in C$.
- Pero $gr(r) < gr(g)$ que es el polinomio no nulo de menor grado de C.
- Concluimos que $r = 0$.

Continuación Prueba

$$\begin{aligned} r(x) &= r(x) \bmod (1+x^n) \\ &= (p(x)+q(x)g(x)) \bmod (1+x^n) \\ &= p(x) \bmod (1+x^n) + (q(x)g(x)) \bmod (1+x^n) \\ &= p(x) + q \odot g \end{aligned}$$

- Como $p(x) \in C$ y $q \odot g \in C$ y C es lineal, concluimos que $r \in C$.
- Pero $gr(r) < gr(g)$ que es el polinomio no nulo de menor grado de C.
- Concluimos que $r = 0$.
- Por lo tanto $p(x) = q(x)g(x) + r(x) = q(x)g(x) \in C_1$.

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.
- Pero esa inclusión es obvia, pues si $gr(p) < n$ y $p(x) = q(x)g(x)$, entonces:

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.
- Pero esa inclusión es obvia, pues si $gr(p) < n$ y $p(x) = q(x)g(x)$, entonces:
- $p(x) = p(x) \bmod (1 + x^n)$ (pues $gr(p) < n$)

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.
- Pero esa inclusión es obvia, pues si $gr(p) < n$ y $p(x) = q(x)g(x)$, entonces:
- $p(x) = p(x) \bmod (1 + x^n)$ (pues $gr(p) < n$)
- Y por lo tanto $p(x) = q(x)g(x) \bmod (1 + x^n) = q \odot g \in C_2$.

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.
- Pero esa inclusión es obvia, pues si $gr(p) < n$ y $p(x) = q(x)g(x)$, entonces:
- $p(x) = p(x) \bmod (1 + x^n)$ (pues $gr(p) < n$)
- Y por lo tanto $p(x) = q(x)g(x) \bmod (1 + x^n) = q \odot g \in C_2$.
- Con esto hemos probado las partes 1) y 2) del teorema.

Continuación Prueba

- Entonces concluimos que $C \subseteq C_1$ y habiamos visto $C_2 \subseteq C$, sólo nos resta ver que $C_1 \subseteq C_2$.
- Pero esa inclusión es obvia, pues si $gr(p) < n$ y $p(x) = q(x)g(x)$, entonces:
- $p(x) = p(x) \bmod (1 + x^n)$ (pues $gr(p) < n$)
- Y por lo tanto $p(x) = q(x)g(x) \bmod (1 + x^n) = q \odot g \in C_2$.
- Con esto hemos probado las partes 1) y 2) del teorema.
- Vamos a la 3).

Continuación Prueba

- Sea t el grado de $g(x)$.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.
- Pero como el grado de los elementos de C es menor que n, entonces el grado de $q(x)g(x)$ debe ser menor que n.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.
- Pero como el grado de los elementos de C es menor que n, entonces el grado de $q(x)g(x)$ debe ser menor que n.
- Por lo tanto el grado de $q(x)$ debe ser menor que $n - t$.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.
- Pero como el grado de los elementos de C es menor que n, entonces el grado de $q(x)g(x)$ debe ser menor que n.
- Por lo tanto el grado de $q(x)$ debe ser menor que $n - t$.
- Asi, para cada polinomio de grado menor que $n - t$ corresponde un polinomio de C, y vicecersa.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.
- Pero como el grado de los elementos de C es menor que n, entonces el grado de $q(x)g(x)$ debe ser menor que n.
- Por lo tanto el grado de $q(x)$ debe ser menor que $n - t$.
- Asi, para cada polinomio de grado menor que $n - t$ corresponde un polinomio de C, y vicecersa.
- Por lo tanto la cardinalidad de C es igual a la cardinalidad del conjunto de polinomios de grado menor que $n - t$.

Continuación Prueba

- Sea t el grado de $g(x)$.
- Por 1), $p(x) \in C$ sii es de la forma $q(x)g(x)$ para algun polinomio $q(x)$.
- Pero como el grado de los elementos de C es menor que n, entonces el grado de $q(x)g(x)$ debe ser menor que n.
- Por lo tanto el grado de $q(x)$ debe ser menor que $n-t$.
- Asi, para cada polinomio de grado menor que $n-t$ corresponde un polinomio de C, y vicecersa.
- Por lo tanto la cardinalidad de C es igual a la cardinalidad del conjunto de polinomios de grado menor que $n-t$.
- ¿Cual es esa cardinalidad? Piensenlo un poco antes de ver la siguiente página.

Continuación Prueba

- Los polinomios de grado menor que $n - t$ tienen $n - t$ coeficientes (los de los términos de grado $0, 1, ..., n - t - 1$).

Continuación Prueba

- Los polinomios de grado menor que $n - t$ tienen $n - t$ coeficientes (los de los términos de grado $0, 1, ..., n - t - 1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.

Continuación Prueba

- Los polinomios de grado menor que $n - t$ tienen $n - t$ coeficientes (los de los términos de grado $0, 1, ..., n - t - 1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.
- Como son $n - t$, el total de polinomios posibles es 2^{n-t}.

Continuación Prueba

- Los polinomios de grado menor que $n-t$ tienen $n-t$ coeficientes (los de los términos de grado $0, 1, ..., n-t-1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.
- Como son $n-t$, el total de polinomios posibles es 2^{n-t}.
- Entonces hemos probado que la cardinalidad de C es 2^{n-t}.

Continuación Prueba

- Los polinomios de grado menor que $n-t$ tienen $n-t$ coeficientes (los de los términos de grado $0, 1, ..., n-t-1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.
- Como son $n-t$, el total de polinomios posibles es 2^{n-t}.
- Entonces hemos probado que la cardinalidad de C es 2^{n-t}.
- Pero como C es lineal, sabemos que su cardinalidad es 2^k.

Continuación Prueba

- Los polinomios de grado menor que $n - t$ tienen $n - t$ coeficientes (los de los términos de grado $0, 1, ..., n - t - 1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.
- Como son $n - t$, el total de polinomios posibles es 2^{n-t}.
- Entonces hemos probado que la cardinalidad de C es 2^{n-t}.
- Pero como C es lineal, sabemos que su cardinalidad es 2^k.
- Asi que $2^k = 2^{n-t}$, por lo tanto $k = n - t$, y el grado de $g(x)$ es $t = n - k$.

Continuación Prueba

- Los polinomios de grado menor que $n-t$ tienen $n-t$ coeficientes (los de los términos de grado $0, 1, ..., n-t-1$).
- Cada uno de esos coeficientes puede ser 1 o 0, asi que cada uno tiene dos posibilidades.
- Como son $n-t$, el total de polinomios posibles es 2^{n-t}.
- Entonces hemos probado que la cardinalidad de C es 2^{n-t}.
- Pero como C es lineal, sabemos que su cardinalidad es 2^k.
- Asi que $2^k = 2^{n-t}$, por lo tanto $k = n-t$, y el grado de $g(x)$ es $t = n-k$.
- Fin parte 3

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = 1 + x^n + q(x)g(x)$.

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = 1 + x^n + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, $r(x) = r(x) \bmod (1 + x^n)$.

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = 1 + x^n + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, $r(x) = r(x) \bmod (1 + x^n)$.
- Asi: $r(x) = (1 + x^n + q(x)g(x)) \bmod (1 + x^n) = q \odot g \in C$

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = 1 + x^n + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, $r(x) = r(x) \bmod (1 + x^n)$.
- Asi: $r(x) = (1 + x^n + q(x)g(x)) \bmod (1 + x^n) = q \odot g \in C$
- (en la igualdad anterior usamos $(1 + x^n) \bmod (1 + x^n) = 0$)

Continuación Prueba

- La parte 4) se puede probar de varias formas. Veamos una:
- Dividimos $1 + x^n$ por $g(x)$, obteniendo $q(x), r(x)$ con $gr(r) < gr(g)$ tal que $1 + x^n = q(x)g(x) + r(x)$.
- Por lo tanto $r(x) = 1 + x^n + q(x)g(x)$.
- Como $gr(r) < gr(g) < n$, $r(x) = r(x) \bmod (1 + x^n)$.
- Asi: $r(x) = (1 + x^n + q(x)g(x)) \bmod (1 + x^n) = q \odot g \in C$
- (en la igualdad anterior usamos $(1 + x^n) \bmod (1 + x^n) = 0$)
- Como $r \in C$ y $gr(r) < gr(g)$, entonces $r = 0$ y $g(x)|(1 + x^n)$

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + (1 + x^n)$

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + (1 + x^n)$
- Pero $1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} = rot^k(g)$, asi que:

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + (1 + x^n)$
- Pero $1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} = rot^k(g)$, asi que:
- $x^k g(x) = rot^k(g) + (1 + x^n)$.

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + (1 + x^n)$
- Pero $1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} = rot^k(g)$, asi que:
- $x^k g(x) = rot^k(g) + (1 + x^n)$.
- Como $rot^k(g) \in C$, entonces por la parte 1) del teorema tenemos que $rot^k(g) = q(x)g(x)$ para algún q de grado adecuado.

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + \ldots + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + \ldots + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + \ldots + g_{n-k-1} x^{n-1} + (1 + x^n)$
- Pero $1 + g_0 x^k + g_1 x^{k+1} + \ldots + g_{n-k-1} x^{n-1} = rot^k(g)$, asi que:
- $x^k g(x) = rot^k(g) + (1 + x^n)$.
- Como $rot^k(g) \in C$, entonces por la parte 1) del teorema tenemos que $rot^k(g) = q(x)g(x)$ para algún q de grado adecuado.
- Entonces $1 + x^n = x^k g(x) + rot^k(g) = x^k g(x) + q(x)g(x) = (x^k + q(x))g(x)$

Continuación Prueba

- Otra prueba es observar que por la parte 3), g es de la forma $g_0 + g_1 x + ... + g_{n-k-1} x^{n-k-1} + x^{n-k}$
- Por lo tanto $x^k g(x) = g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + x^n$.
- Como 1+1=0, tenemos:
- $x^k g(x) = 1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} + (1 + x^n)$
- Pero $1 + g_0 x^k + g_1 x^{k+1} + ... + g_{n-k-1} x^{n-1} = rot^k(g)$, asi que:
- $x^k g(x) = rot^k(g) + (1 + x^n)$.
- Como $rot^k(g) \in C$, entonces por la parte 1) del teorema tenemos que $rot^k(g) = q(x)g(x)$ para algún q de grado adecuado.
- Entonces $1 + x^n = x^k g(x) + rot^k(g) = x^k g(x) + q(x)g(x) = (x^k + q(x))g(x)$
- Es decir, g divide a $1 + x^n$.

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.
- Fin prueba

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.
- Fin prueba
- Como g divide a $1 + x^n$, $\frac{1+x^n}{g(x)}$ es un polinomio, que se suele llamar el polinomio chequeador y lo denotaremos por $h(x)$.

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.
- Fin prueba
- Como g divide a $1 + x^n$, $\frac{1+x^n}{g(x)}$ es un polinomio, que se suele llamar el polinomio chequeador y lo denotaremos por $h(x)$.
- Se llama asi pues si $p(x) \in C$, entonces, como $p(x) = q(x)g(x)$ para algún q:

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.
- Fin prueba
- Como g divide a $1 + x^n$, $\frac{1+x^n}{g(x)}$ es un polinomio, que se suele llamar el polinomio chequeador y lo denotaremos por $h(x)$.
- Se llama asi pues si $p(x) \in C$, entonces, como $p(x) = q(x)g(x)$ para algún q:
- $h(x) \odot p(x) = h(x)p(x) \bmod (1 + x^n) = h(x)q(x)g(x) \bmod (1 + x^n) = 0$.

Fin Prueba

- Para la parte 5) basta observar que si $1 + x^n = q(x)g(x)$ entonces $1 = q_0 g_0$ por lo tanto $g_0 = 1$.
- Fin prueba
- Como g divide a $1 + x^n$, $\frac{1+x^n}{g(x)}$ es un polinomio, que se suele llamar el polinomio chequeador y lo denotaremos por $h(x)$.
- Se llama asi pues si $p(x) \in C$, entonces, como $p(x) = q(x)g(x)$ para algún q:
- $h(x) \odot p(x) = h(x)p(x) \bmod (1 + x^n) = h(x)q(x)g(x) \bmod (1 + x^n) = 0$.
- La última igualdad pues $h(x)g(x) = 1 + x^n$ por definición de h.