UNIVERSIDAD DE MÁLAGA

E.T.S. INGENIERÍA INFORMÁTICA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Tema 7. Teoría Codificación Algebraica

José A. Montenegro

Dpto. Lenguajes y Ciencias de la Computación
ETSI Informática. Universidad de Málaga
monte@lcc.uma.es twitter

26 de septiembre de 2013

1. Códigos Hamming

2. Códigos Cíclicos
   - Propiedades de los códigos cíclicos
   - Corrección Errores en los códigos cíclicos

Códigos Hamming

- En el capitulo anterior mostramos que los métodos algebraicos pueden ser utilizados para construir códigos útiles. Nos centramos en una importante familia de códigos, descubiertos en 1950 por R.W. Hamming.
- Acorde con el teorema 1 del tema 6 un código binario lineal con $\delta \geq 3$ puede ser definido por una matriz de verificación en la cual todas las columnas son distintas y no son igual a cero.
- Si el número m de filas es proporcionado, entonces hay 2^m vectores columnas de longitud m, por lo que el máximo número de columnas distintas no ceros es $2^m - 1$.

- El orden en cual las columnas son listadas no es relevante, aunque en la practica establecer un orden puede resultar útil.
- Reordenar las filas solamente implica una reordenación de los bits de cada palabra codificada, y no afectan a los parámetros del código.
- Dos códigos que difieren en el orden de las filas son equivalentes.

Definición 1 (Código de Hamming)

Un código definido por una matriz de verificación binaria con m filas y $2^m - 1$ *columnas distintas y ninguna cero es un código binario de Hamming.*

Ejemplo 1

Establezca la matriz de verificación y los parámetros del código Hamming con m = 3.

Solución:
Tenemos $2^3 - 1 = 7$ columnas.

Una forma de listarlas todas sería establecer un orden de diccionario.

Pero, como observaremos posteriormente, hay razones para utilizar el orden numérico, el cual es el orden correspondiente a la representación binarias de los números 1, 2, 3, 4, 5, 6, 7:

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Solución:
De forma alternativa podemos ordenar las columnas de forma que aquellas con peso 1 se sitúan al final, obteniendo una matriz de verificación en la *forma estándar*:

$$H_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Los códigos definidos por las matrices H_1 y H_2 son equivalentes.

Los parámetros (n, k, δ) se pueden establecer fácilmente.

La longitud de palabra es n=7 y la dimensión es k = n - m = 4.

La distancia mínima δ es al menos 3, ya que todas las columnas de H_1 son distintas y no ceros, es fácil verificar que c_1=1110000 ($c_1 H_2 = 0$) es una palabra codificada con peso 3, por lo que $\delta = 3$.

- Generalmente, para cada $m \geq 3$, hay un código de Hamming binario con parámetros

$$n = 2^m - 1,\ k = 2^m - 1 - m,\ \delta = 3.$$

- Estos códigos tiene una propiedad muy especial.

Teorema 1

En un código binario de Hamming, todas la palabras en $\mathbb{F}_2^n$ son una palabra codificada o están a una distancia 1 de una palabra codificada.

- Generalmente, un código corrector r tiene la propiedad que $\delta \geq 2r + 1$, por lo que los vecindarios $N_r(c)$ $(c \in C)$ son mutuamente disjuntos.
- Sin embargo hay "huecos" que no cubren esos vecindarios, por lo que algunas palabras no están en ninguno de esos vecindarios $N_r(c)$.

Definición 2 (Código Perfecto)

Un código corrector r C es un código perfecto si todas las palabras están en uno de los vecindarios $N_r(c)$ para algún $c \in C$.

- El teorema 1 establece que un código binario Hamming es un código perfecto con r=1.
- En el caso de m=3 hay $2^4 = 16$ palabras codificadas c, y cada vecindario $N_1(c)$ contiene 1+7=8 palabras.
- Estos 16 vecindarios son disjuntos y ya que 16 x 8= 128 es el número total de palabras, el código es perfecto (véase siguiente Figura).

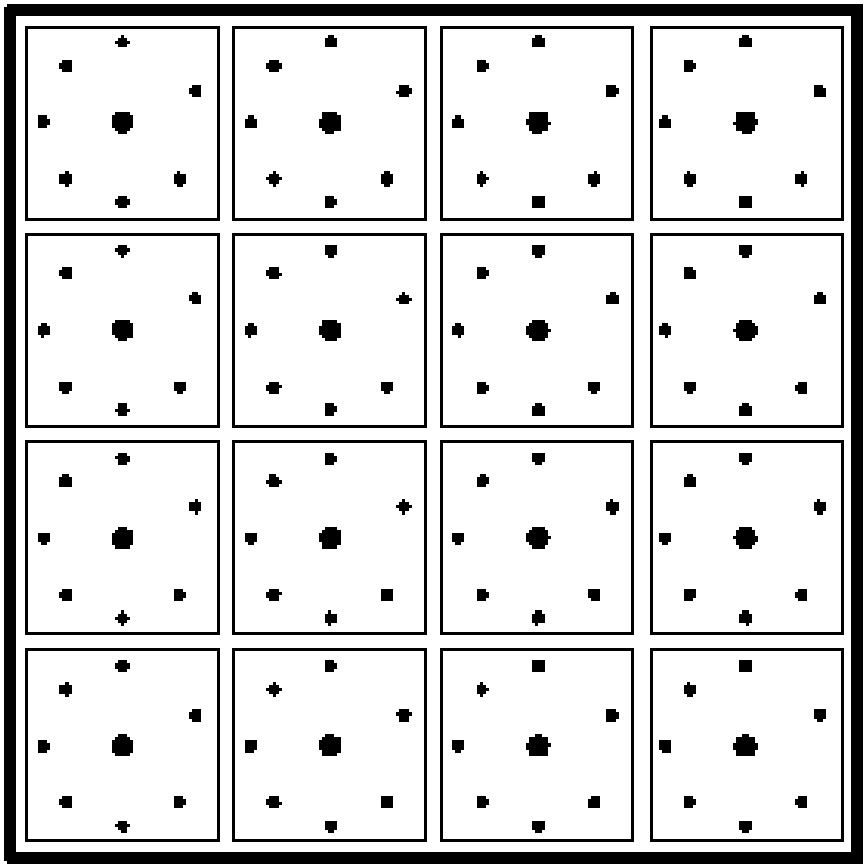

Figura 1 : El código Hamming con parámetros (7, 4, 3) es perfecto

La mayor razón para utilizar métodos algebraicos es que las estructuras algebraicas pueden proporcionar buenos algoritmos para codificar y decodificar.

Para los códigos binarios de Hamming, podemos utilizar las siguientes técnicas.

Codificación Las columnas de la matriz de verificación H están ordenadas en orden numérico.

Entonces los bits $x_1, x_2, x_4, \ldots, x_{2^{m-1}}$ son bits de verificación, y podemos escribir las ecuaciones que los definen en términos de los bits restantes (mensaje).

Por ejemplo, en el caso de m=3, las ecuaciones derivadas de H_1 son

$$\begin{aligned} x_1 &= x_3 + x_5 + x_7, \\ x_2 &= x_3 + x_6 + x_7, \\ x_4 &= x_5 + x_6 + x_7. \end{aligned}$$

cont Codificación A veces es conveniente utilizar los primeros k bits como los bits de mensaje y el resto n-k bits como bits de verificación.

Esto corresponde a escribir la matriz de verificación en su forma estándar H_2, las columnas son obtenidas de H_1 mediante permutación

$$1 \mapsto 7, 2 \mapsto 6, 3 \mapsto 1, 4 \mapsto 5, 5 \mapsto 2, 6 \mapsto 3, 7 \mapsto 4.$$

Aplicando estas permutaciones y reordenando las ecuaciones, los bits de verificación son dados por:

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4, \\ x_6 &= x_1 + x_3 + x_4, \\ x_7 &= x_1 + x_2 + x_4. \end{aligned}$$

Decodificación Cuando la matriz de verificación son ordenadas en un orden numérico, la regla de decodificación del síndrome toma una forma muy simple.

Primeros, observamos que hay n + 1 clases de equivalencia

$$0 + C,\ e_1 + C,\ e_2 + C,\ \ldots\ ,\ e_n + C,$$

donde e_i denota la palabra $0 \ldots 010 \ldots 0$ en el cual el i^{th} bit es 1.

El síndrome de las clase de equivalencia $e_i + C$ es He_i' el cual es igual a la i^{th} columna de H.

Por lo que la regla para corregir un simple error es: si el síndrome de la palabra recibida z es la representación binaria de i, entonces el i^{th} bit es erróneo.

Ejercicio 1

Establece la matriz de verificación para el código Hamming de longitud 15, utilizando el orden numérico de las columnas.

¿Cuantas palabras codificadas tenemos?

¿Cuales de las siguientes palabras son palabras codificadas? 011010110110000, 100000100000011, 110010110111111.

Corrige aquellas que no son palabras codificadas, asumiendo que solamente puede ocurrir un error.

Solución:
Los parámetros serían n=15, $n = 2^m - 1$; m =4. k =n-m= 11.
Con lo cual tendremos $2^{11} = 2048$. Palabras codificadas.
La matriz es:

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

$z_0(011010110110000)$; H $z_0 = 1010 = 10 = 011010110010000$
$z_1(100000100000011)$; H $z_1 = 0111 = 7 = 100000000000011$
$z_2(110010110111111)$; H $z_2 = 1000 = 8 = 110010100111111$

Códigos Cíclicos

- Los códigos Hamming proporciona una familia de ejemplos en los cuales la dimensión k del código, y por tanto tiene tamaño $|C| = 2^k$, puede ser tan largos como necesitemos, mientras que la distancia mínima es constante.

  ¿Es posible construir explícitamente familias de códigos lineas en los cuales la dimensión y la distancia mínima puede ser tan grande como sea necesario?

- Para contestar a esta pregunta daremos:

  (i) un método general para construir códigos lineales, basadas en ideas algebraicas simples, y

  (ii) una construcción específica utilizando el método general.

- En el resto de este capítulo utilizaremos esta notación $a = a_0 a_1 \dots a_{n-1}$ para representar una palabra en $\mathbb{F}_2^n$.
- El *desplazamiento cíclico* de a es una palabra

$$\hat{a} = a_{n-1}\ a_0\ a_1\ \dots\ a_{n-2}.$$

Definición 3 (Código Cíclico)

Un Conjunto $C \subseteq \mathbb{F}_2^n$ es un código cíclico si

- *(i) es un código lineal,*
- *(ii) $\hat{c}$ está en C si* **c** *está en C, esto es,*

$$c_0\, c_1\, c_2 \ldots c_{n-1} \in C \Rightarrow c_{n-1}\, c_0\, c_1 \ldots c_{n-2} \in C.$$

La definición implica que si C es cíclica y $c \in C$ entonces la palabra

$$c_i\, c_{i+1} \ldots c_{n-1}\, c_0 \ldots c_{i-1}$$

es obtenida de **c** *mediante un número de desplazamientos también están en C.*

Ejemplo 2

¿Cual de los siguientes códigos son cíclicos?

$$C_1 = \{000, 100, 010, 001\}, C_2 = \{0000, 1010, 0101, 1111\}$$

Ejemplo 2

¿Cual de los siguientes códigos son cíclicos?

$$C_1 = \{000, 100, 010, 001\}, C_2 = \{0000, 1010, 0101, 1111\}$$

Solución:

Un código cíclico debe ser lineal, y debe ser cerrado bajo la operación de desplazamiento cíclica. Por tanto, C_1 no es un código cíclico, debido a que no es un código lineal ($100 + 010 = 110$, el cual no está C_1, por ejemplo).

Por otro lado, C_2 es un código cíclico, debido a que se cumple ambas condiciones: por ejemplo, el desplazamiento cíclico de la palabra codificada 1010 es la palabra codificada 0101.

- Existe una forma alternativa de representar un desplazamiento cíclico en términos algebraicos.
- La expresión

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$$

- en el cual $a_0, a_1, a_2, \ldots, a_d$ están en $\mathbb{F}_2$, es denominado un *polinomio* con coeficientes en $\mathbb{F}_2$. Si $a_d \neq 0$ entonces el grado de a(x) es d.
- Los polinomios pueden ser sumados y multiplicados acorde con las reglas que conocemos de la algebra elemental y con estas reglas forman un *anillo*, denotado como $\mathbb{F}_2[x]$.
- Claramente, hay una correspondencia entre el polinomio $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$ en $\mathbb{F}_2[n]$, y la palabra $a_0 a_1 \ldots a_{n-1}$ en $\mathbb{F}_2^n$.

- En esta correspondencia, el desplazamiento cíclico $\hat{a}$ de **a** es representado por el polinomio $\hat{a}(x)$, donde

$$\begin{aligned}\hat{a}(x) &= a_{n-1} + a_0 x + \ldots + a_{n-2}x^{n-1} \\ &= x(a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1) \\ &= xa(x) - a_{n-1}(x^n - 1).\end{aligned}$$

- Hemos mantenidos el signo negativo para mantener la claridad, pero debido a que los coeficientes pertenecen a $\mathbb{F}_2$ podemos reescribir el signo menos como un signo más.
- El resultad de los cálculos es que $\hat{a}(x)$ es igual $xa(x)$, excepto para un múltiplo de $x^n - 1$; en otro caso

$$\hat{a}(x) \text{ es igual a } xa(x) \text{ modulo } x^n - 1.$$

- Definimos una nueva regla para multiplicar los polinomios, dado a(x) y b(x), los multiplicamos de la forma usual, y los reducimos modulo $x^n - 1$.
- Esto significa que tomaremos $x^n - 1$ equivalente al 0, y para la reducción es equivalente remplazar x^n por 1, x^{n+1} por x, x^{n+2} por x^2, y continuamos así.
- Vamos a denotar por $V^n[x]$ el anillo de polinomios con coeficientes en $\mathbb{F}_2$, utilizando la multiplicación modulo $x^n - 1$.
- Hemos construido el anillo $V^n[x]$ por lo que tenemos una correspondencia biyectiva con $\mathbb{F}_2^n$, específicamente $a(x) \leftrightarrow a$.
- Además, si a(x) y b(x) corresponde a **a** y **b**, entonces $a(x) + b(x)$ corresponde a **a + b** y $xa(x)$ corresponde a $\hat{a}$, el primer desplazamiento cíclico de a.

Ejemplo 3

Escribe los polinomios en $V^6[x]$ que corresponden a las palabras 110101 y 010110, y encontrar sus productos como elementos de $V^6[x]$.

Ejemplo 3

Escribe los polinomios en $V^6[x]$ que corresponden a las palabras 110101 y 010110, y encontrar sus productos como elementos de $V^6[x]$.

Solución:

110101 es representado mediante $1 + x + x^3 + x^5$ y 010110 esta representado por $x + x^3 + x^4$. Multiplicando y estableciendo $x_6 = 1, x_7 = x$, y demás, obtenemos

$$
\begin{aligned}
&(1 + x + x^3 + x^5)(x + x^3 + x^4) \\
&= (x + x^3 + x^4) + (x^2 + x^4 + x^5) + (x^4 + x^6 + x^7) + (x^6 + x^8 + x^9) \\
&= x + x^2 + x^3 + x^4 + x^5 + x^7 + x^8 + x^9 \\
&= x + x^2 + x^3 + x^4 + x^5 + x + x^2 + x^3 \\
&= x^4 + x^5.
\end{aligned}
$$

- Mostraremos que un código cíclico en $\mathbb{F}_2^n$ corresponde a una especie particular de subconjunto de $V^n[x]$.
- Sea R un anillo con la propiedad commutativa en la multiplicación.
- Un subconjunto S de R es denominado como *ideal* si
  - (i) $a, b \in S \Rightarrow a + b \in S$
  - (ii)$r \in R$ y $a \in S \Rightarrow ra \in S$.
- En otras palabras, un *ideal* S es cerrado bajo la suma y bajo la multiplicación por un elemento de R.

Teorema 2

Un código binario con palabras codificadas de longitud n es cíclico sii corresponde a un ideal en $V^n[x]$.

- Obtenemos del teorema que la construcción de códigos cíclicos de longitud n es equivalente a la construcción de ideales en $V^n[x]$.
- Sea f(x) un polinomio en $V^n[x]$. El conjunto de todos los múltiplos de f(x) en $V^n[x]$ es un *ideal*, si a(x) y b(x) son múltiplos de f(x), por lo que a(x) + b(x) y p(x) a(x) para cualquier p(x).
- Denotaremos este ideal como $\langle f(x) \rangle$ y nos referimos a el como el ideal generado mediante $f(x)$.

Ejemplo 4

Construya el ideal generado mediante $f(x) = 1 + x^2$ *en* $V^3[x]$, *y escriba el código correspondiente* $C \subseteq \mathbb{F}_2^3$.

Solución:
Multiplicaremos f(x) por cada elemento p(x) de $V^3[x]$ y reduciendo modulo $x^3 - 1$, obtendremos la siguiente relación:

$\mathbb{F}_2^3$	$p(x)$	$p(x)f(x) mod(x^3 - 1)$
000	0	$\mathbf{0}$
100	1	$\mathbf{1 + x^2}$
010	x	$x + x^3 = \mathbf{1 + x}$
110	$x + 1$	$x + x^3 + 1 + x^2 = \mathbf{x + x^2}$
001	x^2	$x^2 + x^4 = \mathbf{x^2 + x}$
101	$x^2 + 1$	$1 + x^2 + x^4 + x^2 = \mathbf{1 + x}$
011	$x^2 + x$	$x^2 + x + x^4 + x^3 = \mathbf{x^2 + 1}$
111	$x^2 + x + 1$	$x^2 + x + 1 + x^4 + x^3 + x^2 = \mathbf{0}$

Por tanto el ideal es $\langle 1 + x^2 \rangle$ que tiene solamente cuatro elementos:

$$0, (x + 1), (x^2 + 1), (x^2 + x)$$

El código correspondiente en $\mathbb{F}_2^3$ es $C = \{000, 011, 101, 110\}$.

Ejercicio 2

¿Cual de los siguientes códigos son cíclicos?
$C_1 = \{0000, 1100, 0110, 0011, 1001\}$,
$C_2 = \{0000, 1100, 0110, 0011, 1001, 1010, 0101, 1111\}$.

Ejercicio 2

¿Cual de los siguientes códigos son cíclicos?
$C_1 = \{0000, 1100, 0110, 0011, 1001\}$,
$C_2 = \{0000, 1100, 0110, 0011, 1001, 1010, 0101, 1111\}$.

Solución:
c_1:1100+0110 = 1010 No es lineal.
0110+0011= 0101, 0110+1001=1111, 0110+1010=1100, 0110+0101=0011.

Ejercicio 3

Escribe las palabras codificadas del código cíclico correspondiente al ideal $\langle 1 + x + x^2 \rangle$, *en* $V^3[x]$ *y encuentra la matriz de verificación para este código.*

Solución:

Multiplicaremos f(x) por cada elemento p(x) de $V^3[x]$ y reduciendo modulo $x^3 - 1$, obtendremos la siguiente relación:

$\mathbb{F}_2^3$	$p(x)$	$p(x)f(x)mod(x^3-1)$
000	0	$\mathbf{0}$
100	1	$\mathbf{1 + x + x^2}$
010	x	$x + x^2 + x^3 = \mathbf{1 + x + x^2}$
110	$x + 1$	$x + x^2 + x^3 + 1 + x + x^2 = \mathbf{0}$
001	x^2	$x^2 + x^3 + x^4 = \mathbf{1 + x + x^2}$
101	$x^2 + 1$	$x^2 + x^3 + x^4 + 1 + x + x^2 = \mathbf{0}$
011	$x^2 + x$	$x^2 + x^3 + x^4 + x + x^2 + x^3 = \mathbf{0}$
111	$x^2 + x + 1$	$x^2 + x^3 + x^4 + x + x^2 + x^3 + 1 + x + x^2 = \mathbf{1 + x + x^2}$

Por tanto el ideal es $\langle 1 + x + x^2 \rangle$ que tiene solamente 2 elementos:

$$0, (1 + x + x^2)$$

El código correspondiente en $\mathbb{F}_2^3$ es $C = \{000, 111\}$.

Los parámetros son n=3; $n = 2^m - 1$; m=2. $k = n - m = 3 - 2 = 1$

La matriz es:

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

Propiedades de los códigos cíclicos

El próximo teorema muestra que todos los códigos cíclicos corresponden a un ideal generado por un polinomio.

Teorema 3

Sea $C \neq \{0\}$ un código cíclico (ideal) en $V^n[x]$. Entonces existe un polinomio g(x) en C tal que $C = \langle g(x) \rangle$.

- En el ejemplo 4 hemos listado el ideal en $V^3[x]$ generados por $1 + x^2$.
- Revisando la lista sabemos que el único polinomio que no es igual a cero de menor grado es 1+x, y el teorema 3 nos dice que este polinomio es también un generador para el ideal.
- En general, un código cíclico C tendrá numerosos generadores, pero solamente uno de ellos tendrá el menor grado en C.
- Nos referiremos al único polinomio con esta propiedad como el *generador canónico* de C.

Teorema 4

El generador canónico g(x) de un código cíclico en $V^n[x]$ es un divisor de $x^n - 1$ en $\mathbb{F}_2[x]$.

- Ahora mostraremos como el generador canónico g(x) determina la dimensión de un código cíclico, y la matriz de verificación asociada. Ya que g(x) es un divisor $x^n - 1$, tendremos que $g(x)h(x) = x^n - 1$ en $\mathbb{F}_2[x]$. Sea

$$g(x) = g_0 + g_1x + \ldots + g_{n-k}x^{n-k},\ h(x) = h_0 + h_1x + \ldots + h_kx^k,$$

- donde los coeficiente s g_0, h_0, g_{n-k}, h_k deben ser todos 1, ya que el producto de los polinomios es $x^n - 1$. Sea **g** la palabra

$$g = g_0g_1 \ldots g_{n-k}00 \ldots 0,$$

- en $\mathbb{F}_2^n$, y sea h^* la palabra aquella cuales los primeros $k + 1$ bits son los coeficientes de h(x) a la inversa, seguidos de n - k - 1 ceros:

$$h^* = h_kh_{k-1} \ldots h_000 \ldots 0,$$

Sea H la matriz (n-k) x n cuyas filas son h^* y las primeras n-k-1 desplazamientos cíclicos de h^*:

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & 0 \\ 0 & 0 & \dots & h_2 & h_1 & h_0 & 0 \\ . & . & \dots & . & . & . & . \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

Lema 1

Sea g(i) la fila vector $00\dots0g_0g_1\dots g_{n-k}00\dots0$ *donde hay* i *ceros al comienzo y k-1-i ceros al final, o sea, el desplazamiento cíclico de* g *correspondiente a* $x^i g(x)$ *en* $V^n[x]$.

Entonces $Hg'_{(i)} = 0'$ $(0 \leq i \leq n-1)$.

Teorema 5

La matriz H es una matriz de verificación para el código cíclico $C = \langle g(x) \rangle$, y la dimensión de C es k.

Los resultados mostrados implican que, para encontrar todos los códigos cíclicos con longitud de palabra n, es suficiente encontrar los factores irreducibles de $x^n - 1$ en $\mathbb{F}_2[x]$.

Ejemplo 5

Dado que hay tres factores irreducible de $x^7 - 1$ *en* $\mathbb{F}_2[x]$*:*

$$x^7 - 1 = (1 + x)\ (1 + x + x^3)\ (1 + x^2 + x^3),$$

¿Cuales son las posibilidades para un código cíclico con longitud de palabra de 7?

Solución:

Combinando los tres factores irreducibles en todas las posibilidades podemos obtener $2^3 = 8$ divisores de $x^7 - 1$ en $\mathbb{F}_2[x]$.

Los divisores son además de 1 y $x^7 - 1$,

$$(1+x),\ (1+x+x^3),\ (1+x^2+x^3),\ (1+x)(1+x+x^3),$$
$$(1+x)\ (1+x^2+x^3),\ (1+x+x^3)\ (1+x^2+x^3).$$

Cada uno de los divisores generan un código cíclico, y (por teorema 3 y 4) son los únicos códigos cíclicos de longitud 7.

$\langle 1 \rangle$ es el código en el cual cada palabra es una palabra codificada, y $\langle x^7 - 1 \rangle = \langle 0 \rangle$ es el código en el cual la única palabra codificada es 0.

Los otros códigos son más interesantes.

Por ejemplo, sea C el código con un generador canónico $g(x) = 1 + x + x^3$, por lo que

$$h(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$$

y $h^* = 1011100$. Del teorema 5 obtenemos que la dimensión de C es 4, y la matriz de verificación para C es:

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

Las sietes columnas de esta matriz son distintas y no son iguales a cero, por lo que el código C es equivalente al código Hamming en $\mathbb{F}_2^7$.

Ejercicio 4

Escribe los factores $x^3 - 1$ en $\mathbb{F}_2[x]$ y determina todos los códigos cíclicos de longitud 3.

Ejercicio 4

Escribe los factores $x^3 - 1$ en $\mathbb{F}_2[x]$ y determina todos los códigos cíclicos de longitud 3.

Solución:
Sabemos que los códigos cíclicos corresponden a los ideales en $V^3[x]$ y sabemos que $X^3 - 1 = (X + 1)(X^2 + X + 1)$ en $\mathbb{F}_2[x]$. Por tanto tenemos 4 códigos cíclicos:

- $g = 1$: que obtenemos $C = \mathbb{F}_2^3$
- $g = X + 1$: donde $C = \{000, 011, 101, 110\}$ que es el código de verificación de paridad (el conjunto de todas las palabras de peso par)
- $g = X^2 + X + 1$: que es $C = \{000, 111\}$ el código de repetición triple.
- $g = X^3 - 1$: donde $C = \{000\}$

Ejercicio 5

Completa la clasificación de los códigos cíclicos de longitud 7, mediante las lineas del Ejemplo 5.

Ejercicio 5

Completa la clasificación de los códigos cíclicos de longitud 7, mediante las lineas del Ejemplo 5.

Solución:

- En el caso de g(x)= $1 + x$ tenemos h(x)= $(1 + x^2 + x^3)\ (1 + x + x^3)$= $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$

  y $h^* = 1111111$. Sabemos que la dimensión de C (k) =1, por tanto la matriz de verificación.

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

$C = \{$ 1100000, 0110000, 0011000, 0001100, 0000110, 0000011, 1000001, 0000000$\}$

- En el caso de g(x)= $1 + x^2 + x^3$ tenemos h(x)= $(1 + x)\ (1 + x + x^3)$= $1 + x^2 + x^3 + x^4$ y $h^* = 1110100$. Sabemos que la dimensión de C (k) =4, por tanto la matriz de verificación.

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

El código resultante es un código Hamming.

$C = \{$ 1011000, 0101100, 0010110, 0001011, 1000101, 1100010, 0110001,0000000$\}$

- En el caso de g(x)= $(1+x)\ (1+x^2+x^3)$=$1+x+x^2+x^4$ tenemos h(x)= $(1+x+x^3)$ y $h^* = 1011000$. Sabemos que la dimensión de C (k) =3, por tanto la matriz de verificación.

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

$C = \{$ 1110100, 0111010, 0011101, 1011100, 0101110, 0010111, 1010011, 1101001, 0000000$\}$

- En el caso de g(x)= $(1+x)(1+x+x^3)$=$1+x^2+x^3+x^4$ tenemos h(x)= $(1+x^2+x^3)$ y $h^* = 1101000$. Sabemos que la dimensión de C (k) =3, por tanto la matriz de verificación.

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

$C = \{$ 1011100, 0101110, 0010111, 1001011, 1100101, 1100010, 0110001,000000$\}$

- En el caso de g(x)= $(1+x^2+x^3)(1+x+x^3) = 1+x+x^2+x^3+x^4+x^5+x^6$ tenemos h(x)= $(1+x)$ y $h^* = 1100000$. Sabemos que la dimensión de C (k) =1, por tanto la matriz de verificación.

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

$C = \{$ 1111111,000000$\}$

Ejercicio 6

Considere el generador $g(X) = X^3 + X + 1$ *en* $V^7[x]$ *(sabiendo que g divide* $X^7 - 1$*). Codifique el mensaje m=1010 y decodifique el mensaje z= 1001011.*

Ejercicio 6

Considere el generador $g(X) = X^3 + X + 1$ en $V^7[x]$ (sabiendo que g divide $X^7 - 1$). Codifique el mensaje m=1010 y decodifique el mensaje z= 1001011.

Solución:

Codificación Transformamos el mensaje 1010 en un polinomio de la forma m(X)=$X^2 + 1$ y lo multiplicamos por g(X) y obtenemos c(X)=$m(X)g(X) = X^5 + 2X^3 + X^2 + X + 1$ que nos da la palabra codificada 1110010.

Hubiéramos obtenido el mismo mensaje si en vez de utilizar el polinomio utilizáramos la matriz generadora.

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

cont Solución:

Decodificación Sabemos que la matriz de verificación es la siguiente.

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

Si multiplicamos Hz = (1001011) H =(000) por lo que pertenece a la codificación.

Sabemos que $z(X) = c(X)g(X)$, por lo que solamente tenemos que buscar el polinomio resto de la división por el polinomio generador.

$1 + X^3 + X^5 + X^6 = c(X)(X^3 + X + 1)$ por tanto
$c(X) = 1 + X + X^2 + X^3$ y c=(1111).

Corrección Errores en los códigos cíclicos

Sea C un código cíclico corrector de error t. Asumimos que recibimos el mensaje w(X).

1. Calcular el polinomio síndrome $s(X) \equiv w(X) \, mod \, g(X)$
2. Para $i = 0, \ldots, n-1$ calcula los desplazamientos cíclicos $s_i(X) \equiv X^i s(X) \, mod \, g(X)$ hasta encontrar un síndrome s_j tal que $w(s_j) \leq t$.

   La palabra error de menor peso es

$$e(X) = X^{n-j} s_j(X) \, mod \, (X^n - 1)$$

Ejemplo 6

Sea $g(X) = X^3 + X + 1$ *y w=(1011011);*

Ejemplo 6

Sea $g(X) = X^3 + X + 1$ y w=(1011011);

Solución:
Entonces $w(X) = 1 + X^2 + X^3 + X^5 + X^6$, $syn(w) = X^2$ ya que $w(X) = (X^3 + X^2 + X + 1)g(X) + X^2$, asumiendo que solamente ha ocurrido un error la palabra codificada correcta era (1001011).

Ejemplo 7

Sea $g(X) = X^8 + X^7 + X^6 + x^4 + 1$ un generador de tipo [15,7,5], o lo que es lo mismo un código corrector 2. Si recibimos w=(110011101100010); corrige el posible error.

Ejemplo 7

Sea $g(X) = X^8 + X^7 + X^6 + x^4 + 1$ un generador de tipo [15,7,5], o lo que es lo mismo un código corrector 2. Si recibimos w=(110011101100010); corrige el posible error.

Solución:
Entonces $w(X) = (X + X^2 + X^4 + X^5)g(X) + (1 + X^2 + X^5 + X^7)$,
y calculando los síndromes $s_i(X)$:

0	10100101
1	11011001
2	11100111
3	11111000
4	01111100
5	00111110
6	00011111
7	10000100

Por tanto la palabra error es $X^{15-7}(s_7|0) = X^8$ (100001000000000) = (000000001000010), y obtenemos $r - e = (110011100100000)$.

José A. Montenegro Montes
Dpto. Lenguajes y Ciencias de la Computación
ETSI Informática. Universidad de Málaga
monte@lcc.uma.es
twitter

UNIVERSIDAD DE MÁLAGA

E.T.S. INGENIERÍA INFORMÁTICA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA