EL4005 Principios de Comunicaciones

Clase No.30: Códigos Lineales de Bloque

Patricio Parada

Departamento de Ingeniería Eléctrica
Universidad de Chile

26 de Noviembre de 2010

Contenidos de la Clase (1)

Ejemplos de Códigos de Bloque (1)

- **Códigos de chequeo de paridad**
  - Son códigos donde $n = k + 1$ por lo que $R = \dfrac{k}{k+1} \approx 1$ para k grande.
  - Desempeño pobre y sólo pueden detectar 1 error:

$$d_{\text{min}} = 2 \geq 2t + 1 \Rightarrow t \leq \frac{1}{2}. \tag{1}$$

  - Las palabras de código son de la siguiente forma:

$$\mathbf{c} = (c_0, c_1, \ldots, c_{k-1}, \sum_{l=0}^{k-1} c_l). \tag{2}$$

- **Códigos de repetición**

Ejemplos de Códigos de Bloque (2)

- Pueden corregir hasta $\frac{n-1}{2}$ errores.
- La tasa del código es pequeña: $R = \frac{1}{n}$.

$$0 \leftrightarrow 00\ldots0$$

$$1 \leftrightarrow 11\ldots1$$

- La distancia mínima del código es $d_{\text{min}} = n$. Luego

$$n > 2t + 1 \Rightarrow t < \frac{n-1}{2} \tag{3}$$

- El código corrige hasta

$$t = \left\lfloor \frac{n-1}{2} \right\rfloor \tag{4}$$

errores.

Ejemplos de Códigos de Bloque (3)

- **Códigos de Hamming**
  - Pueden corregir un error.
  - Dado $m \in \mathbb{N}$, tenemos que en un código de Hamming

$$k = 2^m - 1 - m$$

$$n = 2^m - 1$$

por lo que la tasa del código es

$$R = \frac{2^m - 1 - m}{2^m - 1} = 1 - \frac{m}{2^m - 1} \tag{5}$$

  - A medida que $m \to \infty$, la tasa del código se acerca a 1.

Códigos Lineales de Bloque

- Los códigos lineales de bloque, o simplemente códigos lineales, tienen una estructura interna que simplifica las labores de codificación y decodificación.
- Recordemos que hasta ahora hemos dicho que $\mathcal{C}$ es una aplicación entre $\mathbb{F}_p^k$ y $\mathbb{F}_q^n$.
- Los códigos lineales se caracterizan porque esta transformación entre espacios es lineal.

Álgebra de Galois (1)

- El álgebra de campos finitos o de Galois, se define sobre un conjunto $\mathcal{A} = \{0, 1, \ldots, q-1\}$ con las siguientes operaciones:

$$a \oplus b \doteq (a + b) \mod q$$

$$a \otimes b \doteq (a \cdot b) \mod q$$

Álgebra de Galois (2)

- Ejemplo: $q = 5 : \ \mathcal{A} = \{0, 1, 2, 3, 4\}$:

$a \oplus b$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a \otimes b$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Código Lineal

- **Definición:** Un código lineal $\mathcal{C}$ es un subespacio de $\mathbb{F}_q^n$, es decir,
  - (i) Dados $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, entonces $\mathbf{x} + \mathbf{y} \in \mathcal{C}$.
  - (ii) Dado $\lambda \in \mathbb{F}_q$ y $\mathbf{x} \in \mathcal{C}$, entonces $\lambda \mathbf{x} \in \mathcal{C}$.
- Esto implica que siempre está en un código lineal $\mathcal{C}$.
- Ejemplo:

$$\mathcal{C} = \{[0\ 0\ 0], [1\ 0\ 0], [0\ 1\ 0], [1\ 1\ 0]\}$$

Distancia Mínima de un Código Lineal (1)

- Los códigos lineales son invariantes a traslaciones, es decir,

$$\mathbf{c} + \mathcal{C} \doteq \{\mathbf{c} + \mathbf{c}' : \ \mathbf{c}' \in \mathcal{C}\} = \mathcal{C}. \tag{6}$$

- En el ejemplo dado

$$[0\ 1\ 0] + \mathcal{C} = \big\{[0\ 1\ 0], [1\ 1\ 0], [0\ 0\ 0], [1\ 0\ 0]\big\} = \mathcal{C}.$$

- Además, si $\mathbf{c} \in \mathcal{C}$, entonces $-\mathbf{c} \in \mathcal{C}$ y $\mathbf{c} - \mathbf{c} = \mathbf{0} \in \mathcal{C}$.

Distancia Mínima de un Código Lineal (2)

- Si $\mathbf{c}_1$, $\mathbf{c}_2$, $\ldots$, $\mathbf{c}_\gamma$ están a distancia d de una palabra dada $\mathbf{c}$, entonces,

$$\mathbf{c}_1 - \mathbf{c}, \mathbf{c}_2 - \mathbf{c}, \ldots, \mathbf{c}_\gamma - \mathbf{c}$$

  están a distancia d de $\mathbf{0}$.

- Luego, determinar la distancia mínima de un código lineal corresponde a estudiar la distancia entre las palabras del código y $\mathbf{0}$.

Distancia Mínima de un Código Lineal (3)

- **Definición**:

  El peso de Hamming $w(\mathbf{c})$ de un vector $\mathbf{c}$ corresponde al número de posiciones donde el valor es distinto de cero, es decir

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}). \tag{7}$$

- **Teorema**:

  La distancia mínima de un código lineal $\mathcal{C}$ es igual a

$$d_{\text{min}} = \min_{\mathbf{c} \neq \mathbf{0}} w(\mathbf{c}) \equiv w_{\text{min}}. \tag{8}$$

Distancia Mínima de un Código Lineal (4)

- Luego, un código lineal con capacidad para corregir t errores satisface que

$$w_{\text{min}} \geq 2t + 1. \tag{9}$$

- Ejemplo: Supongamos que la capacidad correctora de un código es igual a $t = 2$. Luego, el peso mínimo del código $w_{\text{min}} \geq 5$.

Representación Matricial de Códigos Lineales (1)

- El código lineal $\mathcal{C}$, por ser lineal, admite representación matricial.
- La dimensión de $\mathcal{C}$ corresponde a k, la dimensión del espacio de partida (datos).
- Luego, existe una base de k palabras de códigos (vectores) en $\mathcal{C}$ que generan el código completo.
- Estos vectores se ordenan en una matriz de k filas por n columnas.
- La matrix se denota por la letra G por **generadora** del código.
- Esta matriz tiene rango$(G) = k$.

Representación Matricial de Códigos Lineales (2)

- Dado $\mathbf{a} \in \mathbb{F}_q^k$, entonces

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^n | \ \mathbf{c} = \mathbf{a}G, \text{ para todo } \mathbf{a} \in \mathbb{F}_q^k \right\} \tag{10}$$

- Ejemplo: Sea $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ entonces el código es el siguiente:

$\mathbf{a}$	$\mathbf{c}$
000	00000
001	00111
010	01001
011	01110

$\mathbf{a}$	$\mathbf{c}$
100	10010
101	10101
110	11011
111	11100

Representación Matricial de Códigos Lineales (3)

- Notar que la palabra de código de menor peso es 01001, por lo que el código debería corregir a lo más un error.
- La representación matricial de un código es una forma mucho más compacta que permite reducir el espacio necesario para almacenar el código.
- Si $n = 100$ y $k = 50$, se necesitan $100 \times 50 = 5000$ bits para escribir G.
- Para los mismos parámetros necesitaríamos $2^{50} \approx 1{,}13 \times 10^{15}$ bits, es decir, 128 terabytes de espacio. UUFF!!!

Código Dual (1)

- El hecho que $\mathcal{C}$ sea un subespacio vectorial de $\mathbb{F}_q^n$ tiene ciertas implicancias que son relevantes de mencionar.
- Existe un código dual $\mathcal{C}^\perp$, ortogonal al código original, de dimensión $n-k$ que se define como sigue:

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_q^n | \ \mathbf{c} \cdot \mathbf{v} = 0, \ \forall \ \mathbf{c} \in \mathcal{C}\} \tag{11}$$

- La única palabra en común entre estos dos códigos es $\mathbf{0}$.
- Como $\mathcal{C}^\perp$ es un subespacio de $\mathbb{F}_q^n$, entonces tiene una base de $n-k$ vectores que generan el código completo.

Código Dual (2)

- Esta base se puede escribir en una matriz de $(n-k) \times n$ que denotaremos por H.
- Esta matriz H satisface que

$$\mathbf{c}H^T = \mathbf{0} \tag{12}$$

para todo $\mathbf{c} \in \mathcal{C}$.

- La matriz H recibe el nombre de matriz de chequeo de paridad y cumple que

$$GH^T = [0] \tag{13}$$

donde $[0]$ es una matriz de ceros de $k \times (n-k)$.

Alcances de la Representación Matricial (1)

- La representación matricial de códigos facilita la implementación de códigos lineales, y diseñar su distancia mínima.
- En particular, diseñar un código lineal (n, k) que corrija t errores es equivalente a encontrar una matriz de paridad H de $n - k \times n$ con $2t$ columnas linealmente independientes.
- Las operaciones de permutaciones de filas y/o columnas cambian el código en forma trivial.
- Estos códigos se dicen equivalentes.

Alcances de la Representación Matricial (2)

- La descripción sistemática de un código se realiza tomando la matriz generadora original G y llevándola mediante operaciones fila/columna a la forma:

$$G = [I_k \ P] \tag{14}$$

La matriz de paridad toma la forma

$$H = [-P^T \ I_{n-k}] \tag{15}$$

donde P es una matriz de $k \times n-k$ y las matrices I_k y I_{n-k} representan la matriz identidad de dimensión k y $n-k$, respectivamente.

Decodificación de Códigos Lineales (1)

- La decodificación de un código lineal está íntimamente ligada a las esferas de decodificación (Hamming).
- En el caso de un código lineal, las palabras de código pueden ser listadas en una matriz, conocida como **arreglo estándar**.
- Recordemos que

$$\text{Esf}(t; \mathbf{c}) = \{\mathbf{v}|\ d(\mathbf{v}, \mathbf{c}) \leq t\} \tag{16}$$

- Si $\text{Esf}(t; \mathbf{c}_i) \cap \text{Esf}(t; \mathbf{c}_j) = \emptyset$ para todo $i \neq j$, el código puede corregir hasta t errores.

Decodificación de Códigos Lineales (2)

- Si el código es lineal, $\mathbf{0} \in \mathcal{C}$ por lo que

$$\text{Esf}(t; \mathbf{0}) = \{\mathbf{v} |\ d(\mathbf{v}, \mathbf{0}) \leq t\} \tag{17}$$

y en general

$$\text{Esf}(t; \mathbf{c}) = \{\mathbf{v} |\ d(\mathbf{v} - \mathbf{c}, \mathbf{0}) \leq t\}$$
$$\Rightarrow \text{Esf}(t; \mathbf{c}) = \text{Esf}(t; \mathbf{0}) + \mathbf{c}.$$

- Por lo tanto, describir la totalidad de las esferas de decodificación basta con describir las esfera en torno a $\mathbf{0}$ y obtener el resto por traslación.

Decodificación de Códigos Lineales (3)

- El arreglo estándar es una tabulación de todas las esferas de decodificación.

Construcción del Arreglo Estándar

Paso 1. Escribir todas las palabras de código en la primera fila:

$$\mathbf{0} \quad \mathbf{c}_1 \quad \mathbf{c}_2 \quad \mathbf{c}_3 \quad \dots \quad \mathbf{c}_M$$

Paso 2. Sea $\mathbf{v}_1$ el primer elemento no trivial en $\text{Esf}(t; \mathbf{0})$. Luego, la segunda fila es

$$\mathbf{0}+\mathbf{v}_1 \quad \mathbf{c}_1+\mathbf{v}_1 \quad \mathbf{c}_2+\mathbf{v}_1 \quad \mathbf{c}_3+\mathbf{v}_1 \quad \dots \quad \mathbf{c}_M+\mathbf{v}_1$$

Paso 3. Repetir con el resto de los elementos de la esfera $\text{Esf}(t; \mathbf{0})$.

Arreglo Estándar (1)

$$
\begin{array}{cccccc}
\mathbf{0} & \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \dots & \mathbf{c}_M \\
\mathbf{0}+\mathbf{v}_1 & \mathbf{c}_1+\mathbf{v}_1 & \mathbf{c}_2+\mathbf{v}_1 & \mathbf{c}_3+\mathbf{v}_1 & \dots & \mathbf{c}_M+\mathbf{v}_1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\mathbf{0}+\mathbf{v}_j & \mathbf{c}_1+\mathbf{v}_j & \mathbf{c}_2+\mathbf{v}_j & \mathbf{c}_3+\mathbf{v}_j & \dots & \mathbf{c}_M+\mathbf{v}_j
\end{array}
$$

- El arreglo estándar no produce elementos repetidos.

Arreglo Estándar (2)

- Por ejemplo, si existiesen dos elementos repetidos en la misma fila, entonces tendríamos que existen dos palabras de código distintas $\mathbf{c}_i$ y $\mathbf{c}_j$ tal que

$$\mathbf{c}_i + \mathbf{v}_l = \mathbf{c}_j + \mathbf{v}_l. \tag{18}$$

  para algún $\mathbf{v}_l \in \text{Esf}(t; \mathbf{0})$.

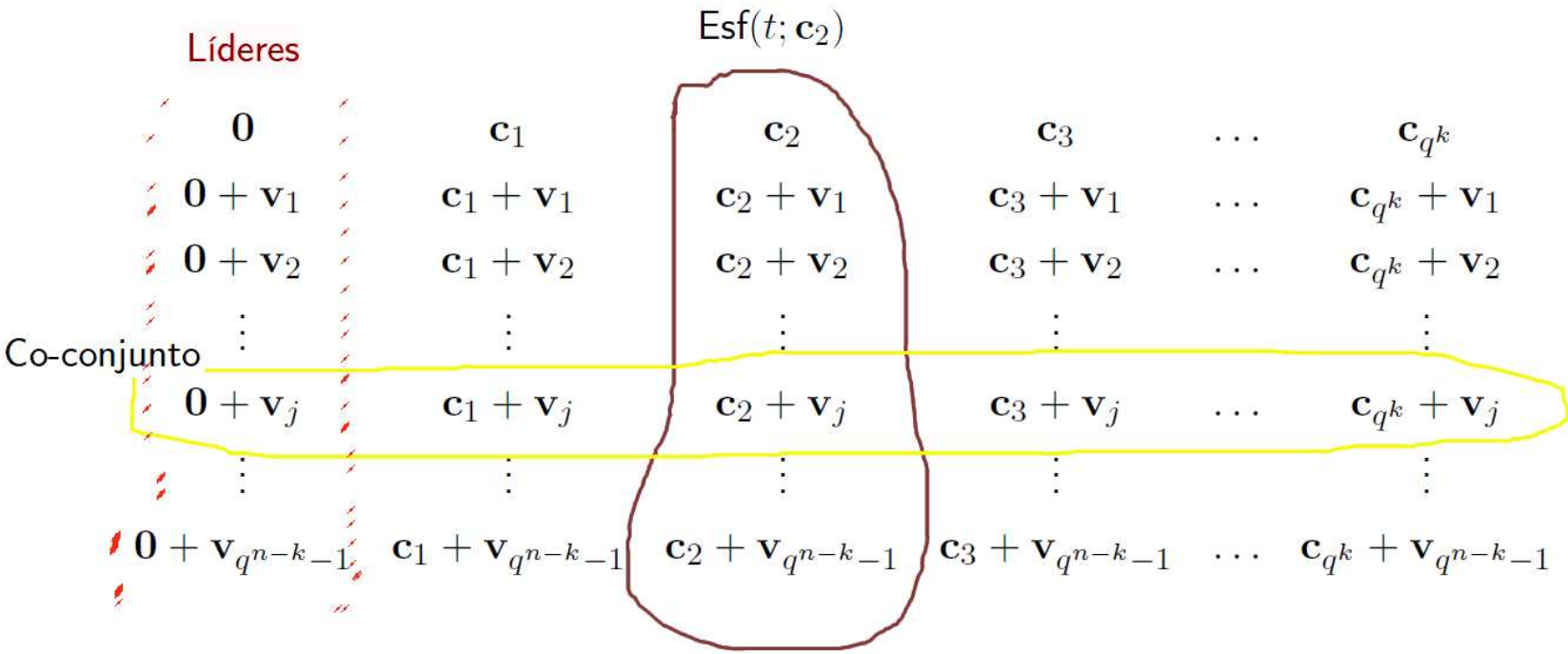
- Pero como $\mathbf{v}_l \in \mathbb{F}_q^n$, tiene un inverso $\mathbf{v'}_l$ tal que $\mathbf{v}_l + \mathbf{v'}_l = \mathbf{0}$.
- Luego concluimos que $\mathbf{c}_i = \mathbf{c}_j$, lo que contradice nuestra hipótesis original.

Arreglo Estándar (3)

- Por un argumento similar uno puede demostrar que la misma columna no puede producir el mismo símbolo en dos posiciones diferentes.
- ¿Cuántos elementos hay en este arreglo?
- Si estamos operando sobre $\mathbb{F}_q^k$, existen q^k palabras de código.
- Por lo tanto el arreglo estándar tiene q^k columnas.
- Por otro lado, el número total de secuencias en $\mathbb{F}_q^n$ es q^n.
- Pero $\mathcal{C}$ es un subgrupo aditivo de $\mathbb{F}_q^n$.
- Luego la cardinalidad de $\mathcal{C}$ divide a q^n.

Arreglo Estándar (4)

- Luego existen q^{n-k} filas diferentes en el arreglo.



Arreglo Estándar (5)

- Si la esfera tiene j elementos, eso implica que las primeras $j+1$ filas del arreglo contienen la totalidad de secuencias que pueden ser decodificadas de manera exitosa.
- El resto de las filas contiene las secuencias que viven entre las distintas esferas de decodificación.

Síndrome (1)

- No es necesario almacenar el arreglo completo para poder utilizarlo.
- Basta con conocer la primera columna y el resto calcularlo por traslaciones.
- Los elementos de $\text{Esf}(t; \mathbf{0})$ son los **patrones de error** que el código puede corregir.
- **Definición**

  Sea $\mathbf{r} \in \mathbb{F}_q^n$ una palabra recibida. El **síndrome** de $\mathbf{r}$, que denotaremos por $\mathbf{s}$, tal que:

$$\mathbf{s} = \mathbf{r}H^T. \tag{19}$$

Síndrome (2)

- **Teorema**

  Todos los vectores en el mismo co-conjunto tienen el mismo síndrome.

- Por lo tanto, basta con codificar los líderes de co-conjuntos y sus respectivos síndromes para determinar la palabra original.

Resumen

Hemos revisado:

- Códigos lineales
- Matrices generadora y de chequeo de paridad.
- Decodificación, arreglo estándar y síndrome.

Lecturas

- Proakis & Salehi, *Communication System Engineering*, capítulo 9, secciones 9.4 y 9.5.
- R. Blahut, *Algebraic Codes for Data Transmission*, capítulos 3.
- W. Peterson & E. Weldon Jr, *Error-Correcting Codes*, capítulo 1.