UNIVERSIDAD DE GRANADA

ALGORITMO DE SUGIYAMA PARA CÓDIGOS REED-SOLOMON TORCIDOS

VÍCTOR ESTEBAN BOTA

Trabajo Fin de Grado

Doble Grado en Ingeniería Informática y Matemáticas

Tutores

Gabriel Navarro Garulo

FACULTAD DE CIENCIAS

E.T.S. INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

Granada, a 27 de febrero de 2023

ÍNDICE GENERAL

1

INTRODUCCIÓN A LOS CÓDIGOS LINEALES

Todo el desarrollo de este capítulo está basado en Huffman & Pless (2010) .

1.1 CÓDIGOS LINEALES

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, denotamos $\mathbb{F}_q^n$ al espacio vectorial de las n-tuplas sobre el cuerpo finito $\mathbb{F}_q$. A los vectores $(a_1, a_2, \cdots, a_n)$ de $\mathbb{F}_q$ generalmente los escribiremos como $a_1 a_2 \cdots a_n$.

Definición 1. Un (n, M) *código* $\mathcal{C}$ sobre $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ de tamaño M. Llamaremos *palabras código* a los elementos de $\mathcal{C}$.

Ejemplo 1.

- En el cuerpo $\mathbb{F}_2$, a los códigos se les conoce como *códigos binarios* y un ejemplo sería $\mathcal{C} = \{00, 01, 10, 11\}$.
- En el cuerpo $\mathbb{F}_3$, a los códigos se les conoce como *códigos ternarios* y un ejemplo sería $\mathcal{C} = \{01, 12, 02, 10, 20, 21, 22\}$.

Si $\mathcal{C}$ es un espacio k-dimensional de $\mathbb{F}_q^n$, entonces decimos que $\mathcal{C}$ es un $[n, k]$ *código linear* sobre $\mathbb{F}_q$ y tiene q^k palabras código. Las dos formas más comunes de representar un código lineal son con la *matriz generadora* o la *matriz de paridad*.

Definición 2. Una *matriz generadora* de un $[n, k]$ *código linear* $\mathcal{C}$ es cualquier matriz $k \times n$ cuyas columnas forman una base de $\mathcal{C}$.

Para cada conjunto de k columnas independientes de una matriz generadora G, se dice que el conjunto de coordenadas forman un *conjunto de información* de $\mathcal{C}$. Las $r = n - k$ coordenadas restantes forman el *conjunto de redundancia* y el número r es la *redundancia* de $\mathcal{C}$.

En general no hay una única matriz generadora pero si las primeras k coordenadas forman un conjunto de información, entonces el código tiene una única matriz generado de la forma $[I_k|A]$, donde I_k es la matriz identidad $k \times k$. Esta matriz se dice que está en *forma estándar*.

Como un código linear es un subespacio de un espacio vectorial, es el núcleo de alguna transformación lineal.

Definición 3. Una *matriz de paridad* H de dimensión $(n-k)\times k$ de un $[n,k]$ *código linear* $\mathcal{C}$ es una matriz que verifica :

$$C = \{x \in \mathbb{F}_q^n | Hx^T = 0\}$$

Como ocurría con la matriz generadora, la matriz de paridad no es única. Con el siguiente resultado podremos obtener una de ellas cuando $\mathcal{C}$ tiene una matriz generadora en forma estándar.

Teorema 1 (Matriz de paridad a partir de la generadora)**.** *Si* $G = [I_k|A]$ *es una matriz generadora del* $[n,k]$ *código* $\mathcal{C}$ *en su forma estándar, entonces* $H = \left[-A^T|I_{n-k}\right]$ *es la matriz de paridad de* $\mathcal{C}$*.*

Demostración. Sabemos que $HG^T = -A^T + A^T = 0$, luego $\mathcal{C}$ está contenido en el núcleo de la transformación lineal $x \mapsto Hx^T$. Como H tiene rango $n-k$, el núcleo de esta transformación es de dimensión k que coincide con la dimensión de $\mathcal{C}$. $\square$

Ejemplo 2. Sea la matriz $G = [I_4|A]$, donde

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

es la matriz generadora en forma estándar del $[7,4]$ código binario que denotaremos por $\mathcal{H}_3$. Por el teorema, la matriz de paridad de $\mathcal{H}_3$ es

$$H = \left[A^T|I_3\right] = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Este código se le conoce como el $[7,4]$ *código de Hamming*.

1.2 CÓDIGOS DUALES

La matriz generadora G de un $[n,k]$ código $\mathcal{C}$ es simplemente una matriz cuyas filas son independientes y que expanden el código. Las filas de la matriz de paridad H también son independientes, luego H es la matriz generadora del mismo código al que llamaremos *código dual u ortogonal* y lo denotaremos como $\mathcal{C}^\perp$. Notamos que $\mathcal{C}^\perp$ es un $[n, n-k]$ código. Otra forma de verlo es de la siguiente manera:

Definición 4. $\mathcal{C}$ es un subespacio de un espacio vectorial luego a su ortogonal es a lo que llamamos *espacio dual u ortogonal* de $\mathcal{C}$ y viene dado por

$$\mathcal{C}^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} \cdot \mathbf{c} = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\}$$

Vamos a obtener ahora la matriz generadora y de paridad de $\mathcal{C}^{\perp}$ a partir de las de $\mathcal{C}$

Proposición 1. *Si G y H son las matrices generadora y de paridad de $\mathcal{C}$ respectivamente, entonces H y G son las matrices generadora y de paridad de $\mathcal{C}^{\perp}$.*

Demostración. Sea $G = [I_k|A]$ la matriz generadora y $H = \left[-A^T|I_{n-k}\right]$ la matriz de paridad del $[n,k]$ código $\mathcal{C}$.

Sabemos que $HG^T = GH^T = 0$ luego

$$\mathcal{C}^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} \cdot \mathbf{c} = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} \cdot G^T = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\} =$$
$$= \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ G \cdot \mathbf{x}^T = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\}$$

Luego $\mathcal{C}^{\perp}$ está contenido en el núcleo de la transformación lineal $x \mapsto Gx^T$. Como G tiene rango k, el núcleo de esta transformación es de dimensión $n-k$ que coincide con la dimensión de $\mathcal{C}^{\perp}$. Por tanto, G es la matriz de paridad de $\mathcal{C}^{\perp}$.

Por último, como $HG^T = 0$ entonces H es la matriz generadora de $\mathcal{C}^{\perp}$. □

Tras este resultado se ve claramente que $\mathcal{C}^{\perp}$ es un $[n, n-k]$ código.

Definición 5. Diremos que un código $\mathcal{C}$ es auto-ortogonal si $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ y diremos que es autodual si $\mathcal{C} = \mathcal{C}^{\perp}$

Ejemplo 3. Tenemos una matriz generadora del código de Hamming $[7,4]$ dada en el ejemplo 2. Ahora definimos $\mathcal{H}_3'$ como el $[8,4]$ código en donde hemos añadido una columna a la paridad de G. Sea

$$G' = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

donde G' es la matriz generadora de $\mathcal{H}_3'$. Veamos que es autodual:

Sabemos que $G' = [I_4|A']$ y en este caso A' es la siguiente matriz:

$$A' = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

y $(A')^T$ es la misma matriz. Luego como $A'(A')^T = I_4$ entonces $\mathcal{H}_3'$ es autodual.

1.3 PESOS Y DISTANCIAS

Definición 6. La *distancia de Hamming* $d(x, y)$ entre dos vectores $x, y \in \mathbb{F}_q^n$ es el número de coordenadas en las que x e y difieren.

Ejemplo 4. Sea $\mathbf{x} = 20110$ y $\mathbf{y} = 10121$ entonces $d(x, y) = 3$.

Teorema 2. *La función distancia $d(x, y)$ satisface las siguientes cuatro propiedades:*

1. *No negatividad:* $d(x, y) \geq 0 \quad \forall x, y \in \mathbb{F}_q^n$.
2. $d(x, y) = 0 \Leftrightarrow x = y$.
3. *Simetría:* $d(x, y) = d(y, x) \quad \forall x, y \in \mathbb{F}_q^n$.
4. *Desigualdad triangular:* $d(x, z) \leq d(x, y) + d(y, z) \quad \forall x, y, z \in \mathbb{F}_q^n$

Demostración. Las tres primeras propiedades son evidentes por la definición de la distancia, comprobemos la última propiedad.

Distinguimos dos casos, si $x = z$ tenemos que $d(x, z) = 0$ y por tanto se verifica la desigualdad. Si $x \neq z$ entonces, no puede ocurrir que $x = y = z$, por tanto $d(x, y) \neq 0$ o $d(y, z) \neq 0$ y por la no negatividad se tendría la desigualdad, en el caso de que $x = y$ o $y = z$ tendríamos la igualdad. □

Llamaremos *distancia mínima* de un código $\mathcal{C}$ a la menor distancia no-nula entre dos palabras cualquiera del código. Además, esta distancia es un invariante y es importante a la hora de determinar la capacidad de corrección de errores del código $\mathcal{C}$.

Ejemplo 5. Sea $\mathcal{C} = \{201310, 311210, 202210, 312100\}$ un código. Sus distancias son:

$$d(201310, 311210) = 3, \quad d(201310, 202210) = 2, \quad d(201310, 312100) = 5,$$

$$d(311210, 202210) = 3, \quad d(311210, 312100) = 3, \quad d(202210, 312100) = 4$$

Luego, la distancia mínima es $d(\mathcal{C}) = 2$.

Definición 7. El *peso de Hamming* o $\mathrm{wt}(x)$ de un vector $x \in \mathbb{F}_q^n$ es el número de coordenadas no-nulas en x. Llamaremos *peso de* $\mathcal{C}$ a $\mathrm{wt}(\mathcal{C}) = \min(\mathrm{wt}(x))$ con $x \neq 0$.

Ejemplo 6. Sea $\mathbf{x} = 202210$ un vector en $\mathbb{F}_3^6$ entonces $\mathrm{wt}(x) = 4$.

Teorema 3. *Si $x, y \in \mathbb{F}_q^n$, entonces $d(x, y) = \mathrm{wt}(x - y)$. Si $\mathcal{C}$ es un código linear, la mínima distancia d es igual al mínimo peso de $\mathcal{C}$.*

Demostración. Como $\mathcal{C}$ es lineal, tenemos que $0 \in \mathcal{C}$ y además $\mathrm{wt}(x) = d(x, 0) \quad \forall x \in \mathcal{C}$, luego $d(\mathcal{C}) \leq \mathrm{wt}(\mathcal{C})$.

Por otro lado, sea $x, y \in \mathcal{C}$ entonces $x - y \in \mathcal{C} \quad \forall x, y \in \mathcal{C}$ y sabemos que $d(x,y) = \mathrm{wt}(x-y) \geq \mathrm{wt}(\mathcal{C})$ para cualesquiera $x, y \in \mathcal{C}$. Se tiene que $d(\mathcal{C}) \geq \mathrm{wt}(\mathcal{C})$.

Hemos conseguido así la igualdad, $d(\mathcal{C}) = \mathrm{wt}(\mathcal{C})$. □

Como resultado de este teorema, para códigos lineales, la *mínima distancia* también se denomina el *peso mínimo* de un código. Si se conoce el peso mínimo de un código, entonces nos referiremos a él como el $[n, k, d]$ código.

BIBLIOGRAFÍA

Huffman, W. C., & Pless, V. (2010). *Fundamentals of Error-Correcting Codes*. Cambridge University Press. ISBN: 978-0-521-13170-4. Accedido el 2022-04-25. URL http://www.cambridge.org/9780521782807