Comunicaciones Digitales

Práctico 9

Codificación de canal: códigos de bloques

Cada ejercicio comienza con un símbolo el cuál indica su dificultad de acuerdo a la siguiente escala: ✦ básica, ★ media, ✷ avanzada, y ✹ difícil.

✦ Ejercicio 1

Considere el siguiente espacio vectorial sobre GF(2) con todas las n-tuplas binarias con $n = 3$.

$$V = \{[000], [001], [010], [011], [100], [101], [110], [111]\}$$

Determine cuáles de los siguientes subconjuntos de V forman un subespacio vectorial y justifique su respuesta:

- $V_1 = \{[000],[001],[100],[101]\}$
- $V_2 = \{[000],[100],[110],[111]\}$
- $V_3 = \{[001],[100],[101]\}$

★ Ejercicio 2 (3.6)

Considere un código lineal C (n, k) cuya matriz generadora G tenga todas sus columna no nulas. Arregle todas las palabras de código de C válidas como filas para lograr una nueva matriz $2^k \times n$.

(a) Muestre que la nueva matriz tendrá todas sus columnas no nulas

(b) Muestre que cada columna de la nuestra matriz consiste de 2^{k-1} ceros y 2^{k-1} unos.

(c) Muestre que todo el conjunto de palabras de código válidas, con cero en alguna posición particular, forman un subespacio vectorial de C. ¿Cuál es la dimensión de ese subespacio?

★ Ejercicio 3 (3.1)

Considere un código sistemático $(8, 4)$ cuyas ecuaciones de chequeo de paridad sean las siguientes:

$$\begin{aligned}
s_0 &= x_1 + x_2 + x_3 + p_0,\\
s_1 &= x_0 + x_1 + x_2 + p_1,\\
s_2 &= x_0 + x_1 + x_3 + p_2,\\
s_3 &= x_0 + x_2 + x_3 + p_3
\end{aligned}$$

donde x_0, x_1, x_2 y x_3 son los dígitos del mensaje, $p_0, p_1, p_2,$ y p_3 son los bits de paridad, y s_0, s_1, s_2 y s_3 son los elementos del síndrome.

(a) Determine cuántas palabras de código válidas se tendrán.

(b) Obtenga las matrices de chequeo de paridad y generadora del código.

(c) Obtenga las palabras de código correspondientes a los mensajes (1010) y (0011).

(d) Sin hacer cuentas es posible afirmar que una sola de las siguientes palabras de código (11010010), (11010001) y (11011010) es válida, ¿por qué?

(e) Ahora sí haciendo cuentas determine cuál.

(f) Si usted sabe que el peso mínimo del código es cuatro, ¿cuántos bits errados podrá detectar y cuántos podrá corregir?

✶Ejercicio 4

Sea un código C (n, k) y sea r una n-tupla que queremos mapear hacia una palabra de código válida. Probar que:

$$\tilde{c} = \underset{c \in C}{\arg\min}\ H(c, r),$$

con $H(u, v)$ la distancia de Hamming entre dos vectores de $GF(2)^n$ cualesquiera.

Solución

Ejercicio 1

Es posible verificar que V_1 es un subespacio vectorial: El mismo contiene el vector nulo y la suma de dos tuplas en V_1 pertenece a V_1. Por otro lado V_2 no es cerrado frente a la suma, si tomamos dos tuplas: $110 + 111 = 001 \notin V_2$, por lo que se concluye que no es un subespacio vectorial. V_3 no es un subespacio vectorial ya que no es cerrado frente a la suma ($001 + 001 = 000 \notin V_3$) y no contiene el vector nulo.

Ejercicio 2

(a) De la condición en G, para cualquier posición de dígito, hay una fila en G con una componente de distinto de cero en esa posición. Esta fila será una palabra de código en C. Por lo tanto, en la matriz de código, cada columna contiene al menos una entrada distinta de cero. Por lo tanto, ninguna columna de la matriz de código contiene solo ceros.

(b) Consideremos la l-esima columna de la matríz de código. De la parte (a) podemos observar que estas columnas contienen al menos un 1. Sea S_0 las palabras de código con un 0 en la l-esima posición y S_1 las palabras de código con 1 en la l-esima posición. Sea x una palabra de código de S_1. Sumando x a cada vector de S_0, obtenemos un conjunto S_1' de palabras de código con un 1 en la l-esima posición.

$$|S_1'| = |S_0|$$

y

$$S_1' \subseteq S_1$$

Adicionando x a cada vector en S_1, obtenemos un conjunto S_0' de palabras de código con un 0 en la l-esima posición. Observamos que

$$|S_0'| = |S_1|$$

$$S_0' \subseteq S_0$$

De las anteriores relaciones se obtiene

$$|S_0| \leq |S_1|$$

$$|s_1| \leq |S_0|$$

Finalmente $|S_0| = |S_1|$; lo cuál implica que la l-esima columna de la matríz de código consisten en 2^{k-1} ceros y 2^{k-1} unos.

(c) Sea S_0 el conjunto de palabras de código con un 0 en la l-esima posición. De la parte (b), podemos observar que S_0 consiste de 2^{k-1} palabras de código. Sea x e y dos palabras de código en S_0. La suma $x + y$ también tendra su l-esima componente en cero y por lo tanto la palabra de código pertencerá a S_0. Entonces S_0 es un subespeacio del espacio vectorial de todas las n-tuplas sobre GF. Como S_0 es un subconjunto de C será un subespacio de C. La dimensión de S_0 es $k - 1$.

Ejercicio 3

(a) Como $k = 4$, entonces partimos de mensajes que tienen k bits de información. Por lo tanto tendremos $2^k = 16$ palabras decódigo válidas.

(b) Sabemos que la matriz de chequeo de paridad tendrá la forma

$$H^t = \begin{pmatrix} P \\ I_{n-k} \end{pmatrix},$$

y la forma de calcular el síndrome del mensaje es

$$s = cH^t.$$

Además, como el código es sistemático sabemos que se cumple la siguiente relación:

$$s = (x_0, x_1, x_2, x_3, p_0, p_1, p_2, p_3) \begin{pmatrix} P \\ I_{n-k} \end{pmatrix}.$$

Basado en lo anterior, de las ecuaciones de la letra es posible calcular la columnas de P:

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

y por lo tanto también las matrices H y G:

$$H = \begin{pmatrix} P^t & I_{n-k} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

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

(c) Para obtener las palabras de código correspondientes a cierto mensaje en particular, debemos multiplicarlo por la matriz generadora G:

$$c_1 = (1010)G = (10101010)$$
$$c_2 = (0011)G = (00110110)$$

(d) Porque se trata de un código lineal sistemático, y a juzgar por los primeros cuatro bits de las tres palabras de código, todas corresponden al mensaje (1101). Sin embargo, en un código de bloques (útil) debe haber una correspondiencia uno a uno entre mensaje y palabra de código.

(e) Para solucionar este problema tenemos dos caminos posibles:

(i) Como se trata de un código sistemático podemos ver qué palabra de código le corresponde al mensjae (1101), operando como en la parte (c). En ese caso tenemos que $c = (11010010)$.

(ii) Otro camino posible es ver si alguna de las palabras anteriores tiene síndrome cero:

$$
\begin{aligned}
s &= cH^t \\
\checkmark(0000) &= (11010010)H^t \\
(0011) &= (11010001)H^t \\
(1000) &= (11011010)H^t
\end{aligned}
$$

(f) Sea D la distancia del código, tendrá una capacidad de corrección de

- hasta $D - 1$ bits errados (3 bits en este caso), y
- hasta $\lfloor \frac{D-1}{2} \rfloor$ bits errados (1 bit en este caso).