Teoría de Información y Codificación

**Ejercicios adicionales** (corresponden a la segunda mitad de la materia)

1. Demostrar que en un código binario lineal la distancia mínima es igual a

   *a*) el mínimo peso (cantidad de elemenos no nulos) de los codewords, exceptuando el codeword nulo

   *b*) mínima cantidad de columnas de $H$ que forman un conjunto linealmente dependiente

   ¿Son válidas esas propiedades también para códigos no binarios?

2. Demostrar que en el standard array cada coset (=fila=tuplas asociadas a un síndrome) contiene $2^k$ elementos distintos. Demostrar además que los cosets no se intersectan.

3. *a*) Dado un código lineal de bloque binario sistemático con matriz $G = [IP]$, explicar por qué la matriz checkeadora $H$ puede construirse como $H = [P^t I]$

   *b*) Analizar si esta construcción es aplicable a códigos no binarios

4. Se usa un código lineal de bloque $(4,2)$ con matriz generadora

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

   para codificar un canal simétrico binario (BSC), con $p < 0.5$ (probabilidad de crossover). Se decodifica por máxima verosimilitud (ML) usando el standard array. Se recibe un cierto simbolo, y el coset leader asociado al síndrome resulta ser 0010

   *a*) Encontrar los otros elementos del coset.

   *b*) Para ese coset, y para el canal dado, ¿es forzoso que el elemento 0010 sea el coset leader, o podría haber sido otro?

   *c*) Puede calcularse, para este símbolo recibido, la probabilidad de decodificación errónea (si sí, explicar como; si no, explicar qué otros datos se necesitarían).

5. Se desea construir un codigo lineal binario $(n, k, d)$ con parámetros $(12, 7, 5)$. Mostrar que es imposible.

6. Mostrar que, en la correccion de errores por síndrome, el coset leader corresponde al pattern de error de menor peso (cantidad de unos) si el canal es BSC con $p < 0.5$ ¿Se mantiene esta propiedad si el canal no es simétrico? ¿Se puede generalizar esto a canales no binarios?

7. Deducir la relación que deben cumplir $n, k$ en un código de Hamming binario.

8. Considerar el código de Hamming extendido $(8,4)$ ($(7,4)$ más un bit de paridad). Cuál es su distancia mínima? Hay alguna mejora, en términos de capacidad de corregir o detectar errores?
   Calcular la probabilidad de error no detectado par un canal binario simétrico si memoria con $p = 0.01$

9. Mostrar que un codigo binario de bloque contiene, o bien todos los codewords con peso par, o la mitad par y la mitad impar.

10. Se desea construir un codigo lineal binario $(n, k, d)$ con parámetros $(12, 7, 5)$. Mostrar que es imposible.

11. Un código lineal de bloque tiene la siguiente matrix generadora:

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

   *a*) Encontrar una matriz checkeadora de paridad $H$

   *b*) Obtener los parámetros básicos del código: $n$, $k$, tasa (rate) y distancia mínima.

12. Armar el código de Hamming ternario $GF(3)$, con $n - k = 2$

13. Dada la siguiente matrix generadora de un código, convertirla a sistemática y encontrar $H$. ¿Es verdad que el $H$ así obtenido (del código sistemático) también sirve como matriz chequeadora de paridad del código original? (Justificar)

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

14. Un código binario sistemático (8,4) computa los bits de paridad según:

$$\begin{aligned} v_0 &= u_1 + u_2 + u_3 \\ v_1 &= u_0 + u_1 + u_2 \\ v_2 &= u_0 + u_1 + u_3 \\ v_3 &= u_0 + u_2 + u_3 \end{aligned}$$

   *a*) Encontrar las matrices G y H y la distancia mínima

   *b*) Calcular la probabilidad de error para un canal BSC con dada $p$

   *c*) Se desea decodificar de manera de corregir errores simples (1 bit) *y* detectar errores dobles (2 bits). ¿Es posible?

15. Se usa el código lineal con $G = (1111)$ sobre un canal BSC con $p < 0.5$

   *a*) Armar el standard array para decodificar con sindrome; señalar el coset leader.

   *b*) Calcular la probabilidad de decodificacion errónea.

   *c*) Decidir si es cíclico. En caso afirmativo, obtener el polinomio generador.

16. Se usa un código de repetición $(3, 1)$ . Escribir la matriz generadora $G$). Encontrar el standard array (tabla de cosets, con coset líderes). El canal no es BSC sino que los pattern de error $e$ tienen probabilidad $p(e) = 1/2$ si $w(e) = 0$ y $p(e) = 1/8$ si $w(e) = 2$, $p(e) = 1/24$ si $w(e) = 2$

17. Un código binario $(n, k)$ se decodifica por síndrome usando el standard array y coset leader dados. $c$ es el código enviado, $r = c + e$ es el recibido, $s = rH$ es el síndrome. Decidir si estas afirmaciones son verdaderas o no, justificando en cada caso

a) Cada coset corresponde a una fila del standard array , y contiene $2^k$ elementos

b) El coset leader se elije siempre como el elemento con menor peso (cantidad de unos) dentro de su fila (coset).

c) Si dos mensajes recibidos $r_1$ $r_2$ dan el mismo síndrome, entonces los pattern de error fueron idénticos $s_2 ? s_2 \implies e_1 = e_2$

d) Dos elementos del array difieren en un codeword $\iff$ pertenecen a la misma fila (coset)

e) La probabilidad de decodificación errónea puede calcularse como

$$1 - \sum_{x_i \in L} P(e = x_i)$$

donde $L$ es el conjunto de coset leaders

18. Propiedades generales de códigos cíclicos (Morreira-Farrel c. 3 ; Lin-Costello c. 4)

    a) Mostrar que la rotación cíclica a la derecha $r$ lugares de una $n-$tupla binaria equivale, en la formulación polinómica, a multiplicar por $X^r$ en módulo $X^n + 1$

    b) Demostrar que $g(x)$ es polinomio generador $\iff$ $g(x)$ es de grado $n - k$ y $g(x)$ es factor de $x^n + 1$

    c) Explicar cómo se codifica un mensaje, si se expresa como un polinomio $m(x)$ o como una tupla $\mathbf{m}$, y cómo pueden armarse las matrices $G$ y $H$.

    d) Explicar por qué el síndrome $s(x)$ se calcula como el resto de dividir $r(x)$ por $g(x)$ - y si no hay error de trasmisión, $s(x) = 0$

    e) Explicar cómo puede transformarse en sistemático trasmitiendo $b(x)g(x) = a(x) + m(x)x^{n-k}$ donde $a(x)$ es el resto de dividir $m(x)$ por $g(x)x^{n-k}$

    f) Explicar qué capacidad (adicional a lo ya visto de códigos lineales) tiene un código cíclico para detectar errores de ráfaga (¿de hasta qué largo?).

19. Se tiene un código lineal ciclico con $n = 5$ y polinomio generador $g(x) = x + 1$

    a) Hallar $k$

    b) Escribir la matrix generadora

    c) Escribir la matrix generadora en forma sistemática

    d) ¿Qué distancia tiene este código, cuantos errores puede detectar y cuántos corregir?

20. a) Dar las condiciones (necesarias y suficientes) que debe cumplir un polinomio $g(x)$ para ser un generador válido de un código binario cíclico $(n, k)$

    b) Para el código del punto anterior, marcar V o F, con breve justificación si corresponde.

       - De todos los codewords no nulos, $g(x)$ es el de menor grado (y no hay ningún otro del mismo grado)
       - De todos los codewords no nulos, $g(x)$ es el de menor peso (y no hay ningún otro del mismo peso )

- Si se usa codificación no sistemática, $g(x)$ es factor de todos los codewords no nulos.
- Si se usa codificación sistemática, $g(x)$ es factor de todos los codewords no nulos.
- El código garantiza detección de hasta $d-1$ bits erróneos (donde $d$ es la distancia mínima)
- El código garantiza detección de errores de ráfaga de largo $\leq n-k+1$
- El código garantiza correción de errores de ráfaga de largo $\leq n-k+1$
- El síndrome será nulo si y solo si el vector recibido $r(x)$ es múltiplo de $g(x)$.

21. Decidir si los siguientes polinomios pueden ser generadores de un código $(n,k)$ con $n=7$. En caso afirmativo, obtener $k$.

    *a*) $p_1(x) = x + x^2$

    *b*) $p_2(x) = 1 + x$

    *c*) $p_3(x) = 1 + x^2 + x^3$

22. Sean $C_1$ y $C_2$ dos códigos cíclicos de largo de bloque $n$, generados por $g_1(x)$ y $g_2(x)$

    *a*) Se desea construir un código cíclico (del menor tamaño posible) que incluya todos los codewords de $C_1$ y $C_2$. Encontrar el generador.

    *b*) Encontrar el polinomio generador de la intersección de $C_1$ y $C_2$

23. Considerar el codigo:

    0000
    1010
    0101
    1111

    Cuál es su rate? Es lineal? Y ciclico? (Si lo es, indicar su polinomio generador) Cuál es su distancia mínima? Puede detectar errores de ráfaga (de qué largo)?

24. Demostrar que la distribución gaussiana maximiza la entropía diferencial $h(X)$, si nos dan media y varianza, y deducir la expresion de $h(X)$.

25. Deducir la capacidad del canal AWGN (tiempo discreto).

26. Un canal aditivo tiene una entrada discreta $\mathcal{X} = \{0, \pm 1, \pm 2\}$, y la salida es continua, $Y = X + Z$, donde $Z$ es uniforme en $[-1, 1]$. Calcular la capacidad.

27. Mostrar que un canal AWGN con entrada restringida a tomar dos valores ($X = \pm 1$) y con decisión "hard" equivale a una canal BSC - calcular $p$.

28. Mostrar que en un canal gaussiano (tiempo discreto) para decodificar minimizando la prob de error conviene elegir el codeword que minimize la distancia euclídea con respecto a la tupla recibida. Qué pasaría si tuviéramos un ruido aditivo laplaciano $f_Z(z) \propto \exp(-\lambda|z|)$?

29. Ejercicios Morreira-Farrel, 2.4 a 2.9 , 3.1 a 3.8

30. Propiedades generales de códigos convolucionales (Morreira-Farrel cap 6 ; Lin-Costello cap 10-11)

    a) Dado el diagrama de código convolucional, obtener la tasa $R = k/n$, la memoria $K$, y su descripción en términos funciones de transferencia (transformada $D$). Determinar si es no sistemático, y si es FIR o IIR.

    b) Viceversa, dado el código según la transformada $D$, hacer el gráfico de bloques.

    c) Armar el diagrama de estados y el trellis.

    d) Explicar cómo se usa el trellis para decodificar, con Viterbi, tanto con hard como con soft decision.

2.4 A binary block code has code vectors in systematic form as given in Table P.2.1.

**Table P.2.1** A block code table

| | | | | | |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 |

(a) What is the rate of the code?
(b) Write down the generator and parity check matrices of this code in systematic form.
(c) What is the minimum Hamming distance of the code?
(d) How many errors can it correct, and how many can it detect?
(e) Compute the syndrome vector for the received vector $r = (101011)$ and hence find the location of any error.

2.5 (a) Construct a linear block code $C_b(5, 2)$, maximizing its minimum Hamming distance.
(b) Determine the generator and parity check matrices of this code.

2.6 A binary linear block code has the following generator matrix in systematic form:

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

(a) Find the parity check matrix $H$ and hence write down the parity check equations.
(b) Find the minimum Hamming distance of the code.

2.7 The generator matrix of a binary linear block code is given below:

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

(a) Write down the parity check equations of the code.
(b) Determine the code rate and minimum Hamming distance.
(c) If the error rate at the input of the decoder is $10^{-3}$, estimate the error rate at the output of the decoder.



2.8 The Hamming block code $C_b(15, 11)$ has the following parity check submatrix:

$$P = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

(a) Construct the parity check matrix of the code.
(b) Construct the error pattern syndrome table.
(c) Apply syndrome decoding to the received vector $r = (011111001011011)$.

2.9 A binary Hamming single-error-correcting code has length $n = 10$. What is
(a) the number of information digits $k$;
(b) the number of parity check digits $n - k$;
(c) the rate of the code;
(d) the parity check equation;
(e) the code vector if all the information digits are '1's and
(f) the syndrome if an error occurs at the seventh digit of a code vector?

2.10 Random errors with probability $p = 10^{-3}$ on a BSC are to be corrected by a random-error-control block code with $n = 15$, $k = 11$ and $d_{min} = 3$. What is the overall throughput rate and block error probability after decoding, when the code is used
(a) in FEC mode and
(b) in retransmission error correction (ARQ) mode?

2.11 An FEC scheme operates on an AWGN channel and it should perform with a bit error rate $P_{be} < 10^{-4}$, using the minimum transmitted power. Options for this scheme are the block codes as given in Table P.2.2.

**Table P.2.2** Options for Problem 2.11

| $n$ | $k$ | $d_{min}$ |
|---|---|---|
| 31 | 26 | 3 |
| 31 | 21 | 5 |
| 31 | 16 | 7 |

(a) Determine the best option if minimum transmitted power is required.
(b) Calculate the coding gain at the desired $P_{be}$ with respect to uncoded transmission.

## Problems

3.1 Determine if the polynomial $1 + X + X^3 + X^4$ is a generator polynomial of a binary linear cyclic block code with code length $n \leq 7$.

3.2 Verify that the generator polynomial $g(X) = 1 + X + X^2 + X^3$ generates a binary cyclic code $C_{cyc}(8, 5)$ and determine the code polynomial for the message vector $\mathbf{m} = (10101)$ in systematic form.

3.3 A binary linear cyclic code $C_{cyc}(n, k)$ has code length $n = 7$ and generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.
(a) Find the code rate, the generator and parity check matrices of the code in systematic form, and its Hamming distance.
(b) If all the information symbols are '1's, what is the corresponding code vector?
(c) Find the syndrome corresponding to an error in the first information symbol, and show that the code is capable of correcting this error.

3.4 Define what is meant by a cyclic error-control code.

3.5 A binary linear cyclic block code $C_{cyc}(n, k)$ has code length $n = 14$ and generator polynomial $g(X) = 1 + X^3 + X^4 + X^5$.
(a) If all the information symbols are '1's, what is the corresponding code vector?
(b) Find the syndrome corresponding to an error in the last information symbol. Is this code capable of correcting this error?
(c) Can cyclic codes be non-linear?

3.6 (a) Determine the table of code vectors of the binary linear cyclic block code $C_{cyc}(6, 2)$ generated by the polynomial $g(X) = 1 + X + X^3 + X^4$.
(b) Calculate the minimum Hamming distance of the code, and its error-correction capability.

3.7 A binary linear cyclic block code with a code length of $n = 14$ has the generator polynomial $g(X) = 1 + X^2 + X^6$.
(a) Determine the number of information and parity check bits in each code vector.
(b) Determine the number of code vectors in the code.
(c) Determine the generator and parity check matrices of the code.
(d) Determine the minimum Hamming distance of the code.
(e) Determine the burst error-correction capability of the code.
(f) Describe briefly how to encode and decode this code.

3.8 For a given binary linear cyclic block code $C_{cyc}(15, 11)$ generated by the polynomial $g(X) = 1 + X + X^4$,
(a) determine the code vector in systematic form of the message vector $m = (11001101011)$ and
(b) decode the received vector $\mathbf{r} = (000010001101011)$.