Teoria de Códigos

exercícios 2005:2006

1. $^{\mu}$ Calcule o digito de controlo, segundo o ISBN[1]-10, de:
   (a) 0-19-853803-
   (b) 3-540-66336-
   (c) 84-9789-613-
   (d) 84-7658-486-
2. $^{\mu}$ Verifique a validade, segundo o ISBN-10, de:
   (a) 972-25-1375-3
   (b) 972-8839-21-9
   (c) 972-8839-06-5
   (d) 972-41-3663-9
3. $^{\mu}$ Verifique a validade, segundo o EAN[2]-13, de:
   (a) 5601405001101
   (b) 5601522469075
   (c) 5601038100202
   (d) 5601537332739
   (e) 5601370031127
   (f) 8003410344315
   (g) 5000265090209
4. $^{\mu}$ Crie os ISBN[3]-13 dos ISBN-10 da questão 2, com o prefixo 978-.
5. $^{\mu}$ Construa um procedimento que teste o código ISBN-10 recebido.
6. $^{\mu}$ Construa um procedimento que gere o digito de controlo (*checksum*) para o ISBN-10.
7. $^{\mu}$ Construa um procedimento que teste o código EAN-13 recebido.
8. $^{\mu}$ Construa um procedimento que gere o digito de controlo (*checksum*) para o EAN-13.
9. $^{\mu}$ Construa um procedimento que teste o código usado nos cheques bancários[4].

[1] $x_1x_2\ldots x_{10}$ é tal que $(x_1, x_2, \ldots, x_{10})\cdot(10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \equiv 0 \mod 11$, onde $x_i = 0..9$, se $i = 1..9$, e $x_{10} = 0..10$. 10 é representado por X.

[2] $x_1x_2\ldots x_{13}$ é tal que $(x_1, x_2, \ldots, x_{13}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) \equiv 0 \mod 10$, onde $x_i = 0..9$, se $i = 1..13$. Pode obter mais informações em http://www.barcodeisland.com/ean13.phtml.

[3] A conversão para -13 dos ISBN-10 é feita, ao não se considerar o digito de controlo deste último, concatenando o prefixo 978 ou o 979, e ao resultante aplicar o EAN-13. Veja mais em http://en.wikipedia.org/wiki/ISBN-13.

[4] Além do número do cheque e o número de conta, em alguns bancos é usado ainda um outro número com 9 dígitos $a_1a_2\ldots a_9$ que identifica o banco emissor, e é tal que $(a_1, a_2, \ldots, a_9) \cdot (7, 3, 9, 7, 3, 9, 7, 3, -1) \equiv 0 \mod 10$.

10. $^{\mu}$ Encontre uma base para o espaço nulo das matrizes seguintes:

    (a) $\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$, matriz sobre $\mathbb{Z}_2$.

    (b) $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$, matriz sobre $\mathbb{Z}_2$.

    (c) $\begin{pmatrix} 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 2 & 2 & 0 \end{pmatrix}$, matriz sobre $\mathbb{Z}_3$.

    (d) $\begin{pmatrix} 9 & 12 & 12 & 33 & 9 \\ 24 & 29 & 18 & 9 & 5 \\ 5 & 15 & 17 & 16 & 19 \end{pmatrix}$, matriz sobre $\mathbb{Z}_{37}$.

    (e) $\begin{pmatrix} 110416 & 31572 & 554310 & 604695 \\ 462290 & 192626 & 378018 & 389981 \end{pmatrix}$, matriz sobre $\mathbb{Z}_{877651}$.

11. $^{\mu}$ Use o *mupad* para gerar uma matriz aleatória[5] sobre um $\mathbb{Z}_p$ à sua escolha, calcula a nulidade e uma base para o seu espaço nulo.

12. $^{\mu}$ De forma aleatória,

    (a) crie corpos de Galois $\mathbb{F}_q$ de ordem

        i. $q = 8$
        ii. $q = 9$
        iii. $q = 343$
        iv. $q = 14641$
        v. $q = 531441$
        vi. $q = 1220703125$

    (b) matrizes, e determine a nulidade e uma base para o espaço nulo, sobre os corpos da alínea anterior.

13. Sejam $D = \mathbb{Z}_3[x], f(x) = x^2 + x + 2, g(x) = x^2 + 1$. Calcule:

    (a) $(x + 2) + (2x + 2)$ em $D/(f(x))$ e em $D/(g(x))$;

    (b) $(x + 2)(2x + 2)$ em $D/(f(x))$ e em $D/(g(x))$;

14. Seja $f(x) = x^2 + x + 2$.

    (a) Mostre que $f(x)$ é primitivo em $\mathbb{Z}_3[x]$.

    (b) Mostre que $f(x)$ é primitivo em $\mathbb{Z}_5[x]$.

    (c) Mostre que $f(x)$ não é primitivo em $\mathbb{Z}_{11}[x]$.

15. Mostre que $f(x) = x^3 + x + 1$ é primitivo em $\mathbb{Z}_2[x]$.

16. Mostre que $f(x) = x^3 + x^2 + 1$ é primitivo em $\mathbb{Z}_2[x]$.

17. Mostre que $f(x) = x^4 + x + 1$ é primitivo em $\mathbb{Z}_2[x]$.

[5] Use o comando `linalg::randomMatrix`.

18. Para $f(x) = x^4 + x^3 + x^2 + x + 1$, $g(x) = x^4 + x^3 + x^2 + 1$,$h(x) = x^4 + x^3 + 1$, mostre, em $\mathbb{Z}_2[x]$, qual deles é primitivo, irredutível e não primitivo, e não irredutível. Para o que é irredutível e não primitivo, calcule a ordem do polinómio x.

19. Construa o elementos não nulos de um corpo de Galois com 128 elementos.

20. Construa o elementos não nulos de um corpo de Galois com 127 elementos.

21. Dado um código $(15, 16, 8)$ binário, calcule o número de erros que são corrigíveis e o número de vectores corrigíveis. Sendo o canal simétrico binário, com $p = 0.1$ a probabilidade de um símbolo ser recebido erradamente, calcule a probabilidade de uma palavra ser corrigível.

22. Dado um código $(8, 16, 4)$ binário, calcule o número de erros que são corrigíveis e o número de vectores corrigíveis. Sendo o canal simétrico binário, com $p = 0.1$ a probabilidade de um símbolo ser recebido erradamente, calcule a probabilidade de uma palavra ser corrigível.

23. Construa um procedimento `bin2dec:=proc(v)` que escreva na representação decimal a entrada $(v_1 v_2 \cdots v_k)_2$, onde $v = (v_1, \ldots, v_k)$.

24. Construa um procedimento `hamming:=proc(numero:Type::PosInt)` onde n é um argumento de entrada, número inteiro positivo, e cujo resultado final é uma matriz $n \times (2^n - 1)$, cuja coluna j é a representação do número natural j na sua escrita binária. A matriz resultante chama-se *matriz de Hamming*. Por exemplo,
    ```
    >> hamming(3);
    ```
$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

25. Verifique se a mensagem recebida é uma palavra-código, onde os códigos usados são de Hamming:

    (a) r=(1,1,1,1,1,1,1)^T no código $[7, 4]$;

    (b) r=(1,0,1,0,1,1,1)^T no código $[7, 4]$;

    (c) r=(1,0,1,0,1,1,1,0,0,1,1,1,0,0,0)^T, no código $[15, 11]$;

    (d) r=(0,0,1,1,0,0,0,0,1,0,0,0,0,1,0)^T, no código $[15, 11]$;

    (e) r=(1,0,1,0,0,0,1,0,1,1,1,1,0,0,0)^T, no código $[15, 11]$;

    (f) r=(1,1,0,0,1,0,1,1,1,0,0,0,0,0,0)^T, no código $[15, 11]$;

    (g) r=(1,1,0,0,1,1,1,1,1,0,0,1,1,1,1,0,1,1,1,0,1,1,1,0,1,0,0,0,1,1,1)^T no código $[31, 26]$;

    (h) r=(1,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,1,1,1,0,1,0,0,0,0,1,0)^T no código $[31, 26]$;

26. Calcule as matrizes geradoras dos códigos de Hamming $[7, 4]$ e $[15, 11]$.

27. Seja C o código de Hamming $[31, 26]$.

    (a) Construa a matriz de paridade e uma matriz geradora do código C.

    (b) Codifique, em C, o vector

$$w = (10110101110110111110111000).$$

    (c) Corrija os erros e descodifique[6] os vectores recebidos:

[6] O sistema $Ax = b$ é resolvido, no MuPAD, por `linalg::matlinsolve(A,b);`.

i. $r = (11010111001101101101011110111)$

ii. $r = (00010111001111101101011110111)$

iii. $r = (00000000011100100101010101010)$

28. Corrija e descodifique os vectores recebidos referentes à questão 25.

29. Considerando o código de Hamming $[63, 57]$, e depois de gerar aleatoriamente um vector r que se assume recebido, corrija o erro em r.

30. Averigue se é possível construir um código linear binário

    (a) $[6, 2]$ que seja c.c. 2-erros.

    (b) $[8, 3]$ que seja c.c. 2-erros.

    (c) $[6, 2]$ que seja c.c. 2-erros.

    (d) $[10, 3]$ que seja c.c. 3-erros.

    (e) $[12, 4]$ que seja c.c. 3-erros.

31. Considere as matrizes, sobre $\mathbb{Z}_2$,

$$G_1 = \left[\begin{array}{cc|c} 1 & 1 & \\ 1 & 1 & I_3 \\ 0 & 1 & \end{array}\right], G_2 = \left[\begin{array}{c|cc} & 0 & 1 \\ I_3 & 1 & 1 \\ & 1 & 1 \end{array}\right], G_3 = \left[\begin{array}{c|ccc} & 1 & 1 & 0 \\ & 1 & 1 & 1 \\ I_4 & 1 & 1 & 0 \\ & 1 & 0 & 1 \end{array}\right]$$

    Para cada uma delas,

    (a) determine o número de elementos do código de que a matriz é geradora;

    (b) indique uma base para o espaço nulo.

    (c) encontre uma matriz de paridade para cada um dos códigos gerados pelas matrizes;

    (d) verifique se os códigos corrigem erros singulares.

32. Calcule as matrizes de paridade das seguintes matrizes geradoras:

(a) $\left[\begin{array}{c|ccc} & 1 & 1 & 0 \\ I_3 & 0 & 1 & 1 \\ & 1 & 1 & 1 \end{array}\right]$ (b) $\left[\begin{array}{c|ccc} & 1 & 1 & 1 \\ I_3 & 0 & 1 & 1 \\ & 1 & 1 & 0 \end{array}\right]$ (c) $\left[\begin{array}{c|ccc} & 0 & 1 & 1 \\ I_3 & 1 & 1 & 1 \\ & 1 & 1 & 0 \end{array}\right]$

(d) $\left[\begin{array}{c|ccc} & 1 & 1 & 0 \\ & 0 & 1 & 1 \\ I_4 & 1 & 0 & 1 \\ & 1 & 1 & 1 \end{array}\right]$ (e) $\left[\begin{array}{c|ccc} & 1 & 1 & 1 \\ & 0 & 1 & 1 \\ I_4 & 1 & 0 & 1 \\ & 1 & 1 & 1 \end{array}\right]$

33. Seja C um código linear $[n, k]$.

    (a) Considere a relação binária $\sim$ definida am $\mathbb{Z}_2^n$ por

$$a \sim b \text{ se } a - b \in C.$$

    i. Verifique se $\sim$ é uma relação de equivalência.

    ii. Mostre que $u \sim v$ se e só se $Hu^T = Hv^T$, onde H é a matriz de paridade do código C.

(b) Verifique se a distância de Hamming é uma métrica.

34. Construa um código binário linear auto-dual em $\mathbb{Z}_2^6$.

35. Construa um código binário linear auto-dual em $\mathbb{Z}_2^8$.

36. Seja $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ a matriz de paridade de um código linear. Calcule o número de posições corrigíveis nesse código.

37. Seja $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ e suponha que

$$r_1 = (100011),\ r_2 = (101010),\ r_3 = (111100).$$

(a) Construa o código linear gerado por G.

(b) Calcule o número de posições corrigíveis.

(c) Liste os líderes e respectivos síndromes.

(d) Corrija, se possível, os vectores recebidos r_1, r_2 e r_3.

38. Se $G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ é a matriz geradora de um código linear C, encontre:

(a) os parâmetros $[n, k]$;

(b) a matriz de paridade;

(c) a distância mínima do código e o número de posições corrigíveis;

(d) a correcção dos vectores recebidos $r_1 = (100010)$ e $r_2 = (001100)$.

39. Seja $W = RS(G)$ com $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$.

(a) Encontre a matriz de paridade H de W e os parâmetros $[n, k, d]$.

(b) Verifique se W é auto-dual.

(c) Corrija os vectores recebidos $r_1 = (111111)$ e $r_2 = (101111)$

40. Seja C um código linear com matriz de paridade

$$\left[\begin{array}{c|ccc} & 1 & 0 & 1 \\ & 1 & 0 & 1 \\ I_4 & 0 & 1 & 1 \\ & 0 & 1 & 1 \end{array}\right].$$

Corrija e descodifique, se possível, cada um dos seguintes vectores recebidos:

(a) (1101011);

(b) (0110111);

(c) (0111000).

41. Encontre os completamentos de $H = \begin{bmatrix} ? & 1 & 0 \\ ? & 0 & 1 \end{bmatrix}$ de forma a que seja a matriz de paridade de uma código linear com correcção de 1 *bit*.

42. Para $\pi(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$,

    (a) mostre, via MuPad, que $\pi(x)$ é irredutível

    (b) mostre que $\pi(x)$ é primitivo

        i. usando matrizes;

        ii. via MuPad.

    (c) Para cada um dos polinómios em $\mathbb{Z}_2[x]$ apresentados, construa, se possível, o código BCH e os respectivos parâmetros $[n, k, d]$ e número de p.c.:

        i. $\pi(x) = x^3 + x^2 + 1$ c.c. 1-erro,

        ii. $\pi(x) = x^3 + x^2 + 1$ c.c. 2-erros,

        iii. $\pi(x) = x^3 + x^2 + 1$ c.c. 3-erros,

        iv. $\pi(x) = x^4 + x + 1$ de forma a que seja $[15, 7]$,

        v. $\pi(x) = x^4 + x^3 + 1$ c.c. 2-erros,

        vi. $\pi(x) = x^4 + x^3 + 1$ c.c. 3-erros,

        vii. $\pi(x) = x^6 + x^5 + 1$ c.c. 3-erros.

    (d) Seja C o código BCH obtido do polinómio primitivo $\pi(x) = x^4+x+1 \in \mathbb{Z}_2[x]$, considerando as primeiras 6 potências de α. Corrija, em C, os seguintes vectores recebidos por um canal com ruído:

        i. $r_1 = (100011011001010)$;

        ii. $r_2 = (011111010011010)$;

        iii. $r_3 = (101000011101100)$;

        iv. $r_4 = (111011001010100)$.

43. Seja C o código BCH obtido do polinómio primitivo $\pi(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$, considerando as primeiras 4 potências de α.

    (a) Mostre que $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ é polinómio gerador de C.

    (b) Corrija, em C, o seguinte vector recebido por um canal com ruído:

$$r = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

44. Considere o polinómio irredutível $\pi(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

    (a) Verifique que $\pi(x)$ é primitivo.

    (b) Encontre os polinómios minimais aniquiladores das 6 primeiras potências de α.

    (c) Seja C o código BCH obtido do polinómio primitivo $\pi(x)$ corrector de 2 erros. Corrija, em C, o seguinte vector recebido por um canal com ruído:

$$r = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

45. Seja C o código BCH obtido do polinómio primitivo $\pi(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ corrector de 2 erros.

(a) Codifique, em C, o vector

$$r = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

apresentando o resultado final como um vector linha sobre $\mathbb{Z}_2$.

(b) Corrija, em C, o seguinte vector recebido por um canal com ruído:

$$r = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$