Já vimos maneiras de codificar mensagens de modo a que, no caso de ocorrerem alguns erros na sua transmissão, o receptor possa ser capaz de corrigir esses erros. Esses códigos, chamados códigos lineares (ou códigos de Hamming), baseavam-se em definir as palavras codificadas como vectores de soluções em $\mathbb{F}_q$ de sistemas de equações lineares.

Nesta última aula vamos ver exemplos de outra classe de códigos, os chamados códigos BCH, descobertos em 1960 por Bose, Chaudhuri e Hocquenghem. As palavras destes códigos serão vectores definidos pelos coeficientes de polinómios em $\mathbb{F}_q[x]$. Estes polinómios terão como raízes certas potências de um *elemento primitivo* de alguma extensão apropriada do corpo $\mathbb{F}_q$.

Comecemos com um exemplo que usa o corpo $\mathbb{F}_8$ com 8 elementos. Este corpo pode obter-se como extensão de $\mathbb{F}_2[x]$, de modo análogo aos exemplos na Aula 17. Com efeito, seja $m(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. É fácil ver que se trata de um polinómio irredutível sobre $\mathbb{F}_2$, pelo que o quociente $\mathbb{F}_2[x]/(m(x))$ é uma extensão de $\mathbb{F}_2$ com 8 elementos (recorde os exemplos análogos construídos na Aula 17):

$$\begin{aligned}\frac{\mathbb{Z}_2[x]}{(m(x))} &= \{a_0 + a_1x + a_2x + (p(x)) \mid a_0, a_1, a_2 \in \mathbb{Z}_2\} \\ &= \Big\{0 + (m(x)), 1 + (m(x)), x + (m(x)), x + 1 + (m(x)), x^2 + (m(x)), \\ &\qquad x^2 + 1 + (m(x)), x^2 + x + (m(x)), x^2 + x + 1 + (m(x))\Big\}\end{aligned}$$

Denotando estes elementos por, respectivamente, $0, 1, \alpha, \beta, \gamma, \delta, \varepsilon, \varphi$, as tabelas das operações deste corpo são as seguintes:

$+$	0	1	α	β	γ	δ	ε	φ
0	0	1	α	β	γ	δ	ε	φ
1	1	0	β	α	δ	γ	φ	ε
α	α	β	0	1	ε	φ	γ	δ
β	β	α	1	0	φ	ε	δ	γ
γ	γ	δ	ε	φ	0	1	α	β
δ	δ	γ	φ	ε	1	0	β	α
ε	ε	φ	γ	δ	α	β	0	1
φ	φ	ε	δ	γ	β	α	1	0

$\cdot$	0	1	α	β	γ	δ	ε	φ
0	0	0	0	0	0	0	0	0
1	0	1	α	β	γ	δ	ε	φ
α	0	α	γ	ε	β	1	φ	δ
β	0	β	ε	δ	φ	γ	1	α
γ	0	γ	β	φ	ε	α	δ	1
δ	0	δ	1	γ	α	φ	β	ε
ε	0	ε	φ	1	δ	β	α	γ
φ	0	φ	δ	α	1	ε	γ	β

Neste corpo já o polinómio $m(x)$ tem uma raiz (que é o elemento α). Observe que todos os seus elementos podem ser vistos como polinómios em α, onde $\alpha^3+\alpha+1 = 0$, e que α é um *elemento primitivo* de $\mathbb{F}_8$, isto é, α é um gerador do grupo multiplicativo $(\mathbb{F}_8 \setminus \{0\}, \cdot)$:

0	0	0
1	1	1
α	α	α
β	$\alpha+1$	α^3
γ	α^2	α^2
δ	α^2+1	α^6
ε	$\alpha^2+\alpha$	α^4
φ	$\alpha^2+\alpha+1$	α^5

[Pode provar-se que, em qualquer corpo finito $\mathbb{F}_q$, o grupo multiplicativo $(\mathbb{F}_q \setminus \{0\}, \cdot)$ é cíclico. Consulte a bibliografia]

As duas colunas mais à direita desta tabela retêm toda a informação sobre as operações do corpo. Esta é a maneira mais eficiente de trabalhar neste corpo: os seus elementos são potências de α, donde a multiplicação passa a ser imediata (basta reter que $\alpha^7 = 1$)

$\cdot$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

enquanto a adição é simplesmente igual a

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

Vamos agora construir um código usando este corpo, do seguinte modo:

Seja $(a, b, c, d) \in \mathbb{F}_2^4$ uma palavra que queremos transmitir. Formemos o respectivo polinómio

$$p_{\mathcal{C}}(x) = ax^6 + bx^5 + cx^4 + dx^3.$$

Dividindo $p_{\mathcal{C}}(x)$ por $m(x)$ (em $\mathbb{F}_2[x]$) obtemos $p_{\mathcal{C}}(x) = q(x)m(x) + r_{\mathcal{C}}(x)$, onde o resto $r_{\mathcal{C}}(x)$ tem grau inferior a 3, isto é, $r_{\mathcal{C}}(x) = rx^2+sx+t$ para alguns $r, s, t \in \mathbb{F}_2$. Então

$$\begin{aligned} q(x)m(x) &= p_{\mathcal{C}}(x) - r_{\mathcal{C}}(x) \\ &= p_{\mathcal{C}}(x) + r_{\mathcal{C}}(x) \\ &= ax^6 + bx^5 + cx^4 + dx^3 + rx^2 + sx + t. \end{aligned}$$

Este polinómio, que denotaremos por $p(x)$, quando calculado em α, uma raiz de $m(x)$, dá $p(\alpha) = m(\alpha)q(\alpha) = 0$. Codificaremos a palavra inicial (a, b, c, d) pelo vector $(a, b, c, d, r, s, t) \in \mathbb{F}_2^7$ definido pelos coeficientes de $p(x)$. Este vector tem 4 dígitos de informação e 3 dígitos de controle e é caracterizado pela seguinte propriedade:

> *Corresponde ao único polinómio de grau inferior a 7 com coeficientes de maior grau a, b, c, d e tendo α por raiz.*

Na descodificação, quando o receptor recebe a palavra (A, B, C, D, R, S, T), forma o polinómio

$$r(x) = Ax^6 + Bx^5 + Cx^4 + Dx^3 + Rx^2 + Sx + T.$$

Suponhamos que aconteceu no máximo um erro singular. Então o erro

$$e(x) = p(x) - r(x)$$

é o polinómio nulo ou consiste num único termo x^e (onde $e \in \{6, 5, 4, 3, 2, 1, 0\}$ corresponde ao coeficiente onde aconteceu o erro):

$$e(x) = \begin{cases} 0 & \text{se não ocorreram erros} \\ \\ x^e & \text{se ocorreu um erro na posição } e. \end{cases}$$

Por exemplo, se o erro aconteceu no coeficiente c, ou seja, $C \neq c$, então $e(x) = (c - C)x^4 = x^4$. Para detectar e corrigir o erro basta ao receptor calcular $r(\alpha)$:

- *Caso 1*: Se $r(\alpha) = 0$, então, como $p(\alpha) = 0$, $e(\alpha) = 0$. Como $\mathcal{O}(\alpha) = 7$, $e(x)$ só pode ser o polinómio nulo e não ocorreram erros.

- *Caso 2*: Se $r(\alpha) \neq 0$, então, como $p(\alpha) = 0$, $e(\alpha) \neq 0$. Portanto, $e(x) = Ex^e$, donde $E\alpha^e = e(\alpha) = r(\alpha)$. O receptor pode assim descobrir o valor de e onde aconteceu o erro e corrigir automaticamente o erro.

Portanto, calculando $r(x)$ em α, podemos determinar se ocorreu algum erro e, em caso afirmativo, corrigi-lo.

`[Pode provar-se que este código tem distância mínima igual a 3, pelo que corrige erros singulares]`

Exemplo: Para codificar a palavra $(1, 1, 0, 1)$ tomemos o polinómio $p_{\mathcal{C}}(x) = x^6 + x^5 + x^3$ e dividamo-lo por $m(x) = x^3 + x + 1$:

$$x^6 + x^5 + x^3 = (x^3 + x^2 + x + 1)(x^3 + x + 1) + 1.$$

Como o resto $r_{\mathcal{C}}(x)$ é igual a 1, temos $p(x) = x^6 + x^5 + x^3 + 1$. (Note que $p(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + 1 = (\alpha^2 + 1) + (\alpha^2 + \alpha + 1) + (\alpha + 1) + 1 = 0$.) A palavra do código deverá ser então igual a $(1, 1, 0, 1, 0, 0, 1)$. Se o receptor receber a palavra $(1, 1, 0, 1, \underline{1}, 0, 1)$, considera o polinómio $r(x) = x^6 + x^5 + x^3 + x^2 + 1$ e, usando o quadro da página 2, calcula $r(\alpha)$:

$$\begin{array}{rcccccccc}
1 & = & & & & & & & 1 \\
+\alpha^2 & = & \alpha^2 & & & & & & \\
+\alpha^3 & = & & & & \alpha & + & 1 \\
+\alpha^5 & = & \alpha^2 & + & \alpha & + & 1 \\
+\alpha^6 & = & \alpha^2 & & & & + & 1 \\
\hline
r(\alpha) & = & \alpha^2. & & & & &
\end{array}$$

Assim, detecta que ocorreu um erro no coeficiente de x^2 e conclui que a palavra correcta é igual a $(1, 1, 0, 1, \underline{0}, 0, 1)$.

Se o receptor receber a palavra $(1, 1, \underline{1}, 1, 0, 0, 1)$, considera o polinómio $r(x) = x^6 + x^5 + x^4 + x^3 + 1$ e calcula $r(\alpha)$:

$$\begin{array}{rcccccc}
1 & = & & & & & 1 \\
+\alpha^3 & = & & & \alpha & + & 1 \\
+\alpha^4 & = & \alpha^2 & + & \alpha & & \\
+\alpha^5 & = & \alpha^2 & + & \alpha & + & 1 \\
+\alpha^6 & = & \alpha^2 & & & + & 1 \\
\hline
r(\alpha) & = & \alpha^2 & + & \alpha & & \\
 & = & \alpha^4. & & & &
\end{array}$$

Assim, detecta que ocorreu um erro no coeficiente de x^4 e conclui que a palavra correcta é igual a $(1, 1, \underline{0}, 1, 0, 0, 1)$.

Vamos apresentar agora um código deste tipo que detecte erros duplos. Para isso precisamos de um corpo maior (o corpo $\mathbb{F}_{16}$ descrito no final da Aula 17). Neste corpo, o elemento g é um elemento primitivo ($g^2 = i$, $g^3 = e$, $g^4 = h$, $g^5 = \alpha$, $g^6 = k$, $g^7 = n$, $g^8 = j$, $g^9 = m$, $g^{10} = \beta$, $g^{11} = c$, $g^{12} = d$, $g^{13} = l$, $g^{14} = f$ e $g^{15} = 1$) que é raiz do polinómio $m(x) = x^4 + x + 1$, irredutível sobre $\mathbb{F}_2$. Portanto $\mathbb{F}_{16}$ pode obter-se como extensão de $\mathbb{F}_2$, através do quociente $\mathbb{F}_2[x]/(m(x))$, e podemos olhar todos os seus elementos não nulos como potências de g (onde $g^{15} = 1$). Uma vez que $m(g) = g^4 + g + 1 = 0$, todo o elemento deste corpo pode exprimir-se como polinómio em g de grau inferior a 4:

0	0	0
1	1	1
g	g	g
i	g^2	g^2
e	g^3	g^3
h	g^4	$g+1$
α	g^5	g^2+g
k	g^6	g^3+g^2
n	g^7	g^3+g+1
j	g^8	g^2+1
m	g^9	g^3+g
β	g^{10}	g^2+g+1
c	g^{11}	g^3+g^2+g
d	g^{12}	g^3+g^2+g+1
l	g^{13}	g^3+g^2+1
f	g^{14}	g^3+1
1	g^{15}	

A ideia para este código é utilizar palavras de comprimento 15 construídas com os coeficientes dos polinómios de grau 14 em $\mathbb{F}_2[x]$ que têm g e g^3 como raízes. Já sabemos que $m(x) = x^4 + x + 1$ é o polinómio mínimo de g sobre $\mathbb{F}_2$. Por outro lado, é fácil provar que $m_3(x) = x^4 + x^3 + x^2 + x + 1$ é o polinómio mínimo de g^3. Então o polinómio $m_{13}(x)$ de menor grau que tem simultaneamente g e g^3 como raízes é o menor múltiplo comum de $m(x)$ e $m_3(x)$; como são ambos irredutíveis,

$$m_{13}(x) = m(x)m_3(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

Como se trata de um polinómio de grau 8, as palavras do código terão comprimento 15, com 7 dígitos de informação e 8 dígitos de controle. Sendo $(a_{14}, a_{13}, \ldots, a_8)$ a palavra com a informação a transmitir, calculamos a respectiva palavra do código do seguinte modo:

Seja $p_{\mathcal{C}}(x) = a_{14}x^{14} + a_{13}x^{13} + \cdots + a_8x^8$. Dividimos $p_{\mathcal{C}}(x)$ por $m_{13}(x)$ (em $\mathbb{F}_2[x]$):

$$p_{\mathcal{C}}(x) = q(x)m_{13}(x) + r_{\mathcal{C}}(x),$$

onde o resto $r_{\mathcal{C}}(x)$ tem grau inferior a 8, isto é, $r_{\mathcal{C}}(x) = a_7x^7 + a_6x^6 + \cdots + a_1x + a_0$. Então

$$\begin{aligned} q(x)m_{13}(x) &= p_{\mathcal{C}}(x) - r_{\mathcal{C}}(x) \\ &= p_{\mathcal{C}}(x) + r_{\mathcal{C}}(x) \\ &= a_{14}x^{14} + a_{13}x^{13} + \cdots + a_1x + a_0. \end{aligned}$$

Este polinómio, que denotaremos por $p(x)$, quando calculado em g e g^3, raízes de $m_{13}(x)$, dá $p(g) = m_{13}(g)q(g) = 0$. Codificaremos a palavra inicial $(a_{14}, a_{13}, \ldots, a_8)$ pelo vector $(a_{14}, a_{13}, \ldots, a_0) \in \mathbb{F}_2^{15}$ definido pelos coeficientes de $p(x)$. Este vector tem 7 dígitos de informação e 8 dígitos de controle e é caracterizado pela seguinte propriedade:

> *Corresponde ao único polinómio de grau inferior a 15 com coeficientes de maior grau $a_{14}, \ldots, a_8$ e tendo g e g^3 como raízes.*

Na descodificação, quando o receptor recebe a palavra $(A_{14}, A_{13}, \ldots, A_0)$, forma o polinómio

$$r(x) = A_{14}x^{14} + A_{13}x^{13} + \cdots + A_1x + A_0.$$

Suponhamos que no canal de comunicação ocorrem, quando muito, erros duplos. Então o vector erro $e(x) = p(x) - r(x)$ é o polinómio nulo, ou consiste num único termo x^e (onde $e \in \{14, 13, \ldots, 1, 0\}$ corresponde ao coeficiente onde ocorreu o

erro), ou consiste na soma de dois termos $x^{e_1} + x^{e_2}$ (onde $e_1, e_2 \in \{14, 13, \ldots, 1, 0\}$ correspondem aos coeficientes onde ocorreram os dois erros):

$$e(x) = \begin{cases} 0 & \text{se não ocorreram erros} \\ x^e & \text{se ocorreu um erro na posição } e \\ x^{e_1} + x^{e_2} & \text{se ocorreram erros nas posições } e_1 \text{ e } e_2. \end{cases}$$

Como $m_{13}(x)$ divide $p(x)$, temos:

- $r(g) = e(g)$, porque $m_{13}(g) = 0$;
- $r(g^2) = e(g^2)$, porque $m_{13}(g) = 0$ (logo $m_{13}(g^2) = (m_{13}(g))^2 = 0$);

  [Exercício: Prove, usando o Teorema Binomial e indução sobre o grau, que qualquer polinómio $p(x)$ em $\mathbb{F}_2[x]$ satisfaz a propriedade $(p(x))^2 = p(x^2)$]

- $r(g^3) = e(g^3)$, porque $m_{13}(g^3) = 0$.

Consideremos o polinómio

$$P(x) = r(g)x^2 + r(g^2)x + (r(g^3) + r(g)r(g^2))).$$

- *Caso 1*: Se $e(x) = 0$, então $e(g) = e(g^2) = e(g^3) = 0$; consequentemente, $r(g) = r(g^2) = r(g^3) = 0$ e $P(x) = 0$.
- *Caso 2*: Se $e(x) = x^e$, então

$$P(x) = g^e x^2 + g^{2e} x + (g^{3e} + g^{2e} g) = g^e x(x + g^e).$$

- *Caso 3*: Se $e(x) = x^{e_1} + x^{e_2}$, então

$$\begin{aligned} P(x) &= (g^{e_1} + g^{e_2})x^2 + (g^{2e_1} + g^{2e_2})x + (g^{3e_1} + g^{3e_2}) + (g^{2e_1} + g^{2e_2})(g^{e_1} + g^{e_2}) \\ &= (g^{e_1} + g^{e_2})[x^2 + (g^{e_1} + g^{e_2})x + g^{e_1} g^{e_2}] \\ &= (g^{e_1} + g^{e_2})[(x + g^{e_1})(x + g^{e_2})]. \end{aligned}$$

Isto mostra que, se há raízes de $P(x)$, estas são necessariamente potências de g, cujo expoente indica a posição onde ocorreram os erros. O receptor pode assim descobrir o(s) valor(es) de e (e_1 e e_2) e corrigir automaticamente o(s) erro(s). Só tem que calcular $P(x)$ e determinar as suas raízes.

Exemplo: Suponhamos que pretendemos enviar os dígitos de informação 1101101. Para isso consideramos o polinómio $p_{\mathcal{C}}(x) = x^{14}+x^{13}+x^{11}+x^{10}+x^8$ e dividimo-lo por $m_{13}(x) = x^8 + x^7 + x^6 + x^4 + 1$:

$$p_{\mathcal{C}}(x) = (x^6 + x^4 + x^2 + x)m_{13}(x) + (x^7 + x^5 + x^4 + x^2 + x).$$

Portanto, os dígitos de controle da palavra a enviar são 10110110, ou seja, a palavra codificada a enviar é a palavra

$$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0).$$

Suponhamos que o receptor recebe

$$(1, 1, 0, 1, 1, \underline{1}, 1, \underline{0}, 0, 1, 1, 0, 1, 1, 0).$$

Então $r(x) = x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^2 + x$, donde:

$$\begin{aligned}
r(g) &= g^{14} + g^{13} + g^{11} + g^{10} + g^9 + g^8 + g^5 + g^4 + g^2 + g; \\
r(g^2) &= (r(g))^2 \quad \text{(porque o corpo tem característica 2);} \\
r(g^3) &= g^{42} + g^{39} + g^{33} + g^{30} + g^{27} + g^{24} + g^{15} + g^{12} + g^6 + g^3 \\
&= g^{12} + g^9 + g^3 + 1 + g^{12} + g^9 + 1 + g^{12} + g^6 + g^3 \quad \text{(pois } g^{15} = 1\text{)} \\
&= g^{12} + g^6.
\end{aligned}$$

Usando a tabela da página 5, substituímos todos estes termos por polinómios em g de grau inferior a 4. Por exemplo, em $r(g)$:

Coeficientes de	g^3	g^2	g	1
g^{14}	1			1
g^{13}	1	1		1
g^{11}	1	1	1	
g^{10}		1	1	1
g^9	1		1	
g^8		1		1
g^5		1	1	
g^4			1	1
g^2		1		
g			1	
$r(g)$	0	0	0	1

Assim, $r(g) = 1$. Então $r(g^2) = r(g)^2 = 1$. Por outro lado,

$$r(g^3) = g^{12} + g^6 = (g^3 + g^2 + g + 1) + (g^3 + g^2) = g + 1.$$

Portanto,

$$P(x) = x^2 + x + \left(\frac{g+1}{1} + 1\right) = x^2 + x + g.$$

Para determinar as raízes de $P(x)$ podemos testar todas as hipóteses, usando a tabela da página 5 para exprimir tudo em termos de 1, g, g^2, g^3:

x	x^2	x (pela Tabela p. 5)	x^2	$x^2 + x + g$
0	0	0	0	g
1	1	1	1	g
g	g^2	g	g^2	g^2
g^2	g^4	g	$g+1$	$g+1$
g^3	g^6	g^3	g^3+g^2	g^2+g
g^4	g^8	$g+1$	g^2+1	g^2
g^5	g^{10}	g^2+g	g^2+g+1	$g+1$
g^6	g^{12}	g^3+g^2	g^3+g^2+g+1	1
g^7	g^{14}	g^3+g+1	g^3+1	0

Paramos em g^7 porque se trata de uma raiz. Então $P(x) = (x + g^7)(x + g^{e_1})$ para algum e_1, pelo que $g^7 g^{e_1} = g = g^{16}$, isto é, $e_1 = 9$. Em conclusão,

$$P(x) = (x + g^9)(x + g^7).$$

Isto significa que os erros ocorreram nas posições de x^9 e x^7.

[São códigos deste tipo que são utilizados na gravação da informação nos discos áudio CD. Mais concretamente, utilizam-se dois códigos sobre o corpo $\mathbb{F}_{256} = \mathbb{F}_{2^8}$, com palavras de comprimento $n = 255$. Habitualmente escolhe-se o elemento primitivo α que tem o polinómio mínimo $m(x) = x^8 + x^4 + x^3 + x^2 + 1$. Estes códigos têm distância mínima igual a 5. Para mais informação, consulte *Error correction and compact discs*, D. Dorninger e H. Kaiser, UMAP Journal 21 (2) (2000) 139-156]

[É possível formalizar estes códigos de modo geral sobre um corpo qualquer $\mathbb{F}_q$ e determinar a sua eficiência na correcção de erros; não o faremos por manifesta falta de tempo]