

Instituto Superior de Engenharia de Lisboa

CESE - Sistemas e Comunicações

CD – Comunicação de Dados

**“Aplicação da Teoria dos Campos de Galois
na Codificação de Canal“**

(versão provisória)

Semestre de Inverno 1998/99

Artur Ferreira - N° 18557

I. Resumo	3
1. Estruturas Algébricas	4
1.1 Conceito de conjunto e grupóide	4
1.2 Conceito de semigrupo, grupo, sub-grupo e respectiva ordem	4
1.3 Ordem de um elemento e suas propriedades	6
1.4 Anel.....	7
1.5 Campo	7
2. Campos de Galois	8
2.1 Construção	8
2.2 Ordem de um Campo.....	9
3. Espaços vectoriais	9
3.1 Geração de um Espaço Vectorial.....	9
3.2 Base geradora do espaço e respectiva dimensão	10
3.4 Produto interno e Espaço dual	11
3.5 Teorema da Dimensão	12
4. Descrição das propriedades dos Campos de Galois.....	13
4.1 Ordem do Campo.....	13
4.2 Ordem de um elemento.....	13
4.3 Elementos primitivos.....	15
4.4 Característica de um Campo de Galois.....	16
5. Polinómios sobre os Campos de Galois	16
5.1 Propriedades dos Polinómios e suas raízes.....	16
5.2 Características de um Domínio Euclideano	19
5.3 Polinómios mínimos	20
5.4 Elementos conjugados.....	20
5.5 Factorização de $x^n - 1$	21
5.6 Estudo do anel $GF(q)[x]/(x^n - 1)$	24
6. Códigos lineares de bloco.....	25
6.1 Analogia com o conceito de grupo.....	25
6.2 Analogia com a noção de espaço vectorial.....	26
6.3 Códigos sistemáticos.....	28
6.4 Códigos não sistemáticos.....	28
6.5 Códigos lineares modificados.....	29
6.6 Códigos cíclicos	30
6.7 Códigos m-ários.....	34
6.8 Critérios de desenho dos códigos BCH.....	34
6.9 Códigos Reed-Solomon	35
7. Bibliografia e referências.....	37
Apêndice A.....	38
Apêndice B.....	39
Apêndice C.....	40
Apêndice D.....	41
Apêndice E	42
Apêndice F	44

I. Resumo

Com o presente trabalho pretende-se efectuar uma exposição dos conceitos matemáticos que definem a teoria dos códigos utilizados na codificação de canal. Através de uma análise matemática sobre a teoria dos conjuntos e espaços vectoriais, procuram-se as justificações para a construção dos códigos de bloco linear, e códigos cíclicos.

A primeira parte do trabalho consiste numa descrição detalhada das estruturas algébricas que fornecem toda a base matemática necessária para a análise da construção das palavras dos diversos códigos. Descrevem-se as estruturas algébricas necessárias para a compreensão da construção dos Campos de Galois. Recorre-se à utilização dos espaços vectoriais e suas propriedades como ferramenta matemática para a obtenção de Campos de Galois com uma dada ordem em função de outros com ordem inferior.

Efectua-se a analogia entre as palavras de um código e os elementos de um espaço vectorial, tendo em conta a forma como o espaço é gerado. No caso particular dos códigos cíclicos analisam-se as propriedades matemáticas que um dado polinómio deve obedecer para ser gerador de um determinado código. Após uma análise cuidada das propriedades dos polinómios sobre Campos de Galois e Domínios Euclidianos deduz-se uma forma geral de obtenção de polinómios geradores para códigos cíclicos.

No final apresentam-se exemplos de desenho de alguns códigos existentes tal como os códigos BCH e Reed-Solomon, passando pelos códigos de Hamming.

1. Estruturas Algébricas

As estruturas algébricas são um ramo da álgebra moderna que estende o conceito da teoria dos conjuntos, efectuando uma análise sobre os elementos constituintes de uma dada estrutura e respectivas operações entre si.

Neste primeiro capítulo introduzem-se os conceitos relacionados com as estruturas algébricas, de uma forma progressiva, salientando os pontos mais importantes que estão relacionados com a construção dos códigos utilizados na codificação de canal. A análise é efectuada partindo da estrutura mais simples denominada por grupóide até chegar ao campo e posteriormente ao objecto de estudo, o campo de Galois.

1.1 Conceito de conjunto e grupóide

Para além do formalismo matemático associado, um conjunto pode ser definido como um agrupamento de elementos sem operações definidas entre si. O número de elementos que pertencem a um dado conjunto determina a sua dimensão, eventualmente infinita, o que define uma característica muito importante designada por cardinalidade.

Se num dado conjunto E for definida uma operação binária “.” tal que a sua aplicação a dois quaisquer elementos de E , resulte num terceiro elemento pertencente a E (não necessariamente diferente), então esta operação designa-se por lei de composição interna em E , e temos a estrutura algébrica mais simples, o grupóide.

$$(E, .) \text{ é grupóide } \Leftrightarrow \begin{cases} \text{A operação "." é uma lei de composição interna em } E. \\ \text{O conjunto } E \text{ é um espaço fechado.} \end{cases}$$

O grupóide resume-se a um espaço fechado com uma operação entre dois dos seus elementos (designados por operandos) . O resultado da aplicação da operação resulta num terceiro elemento pertencente ao grupóide, e que pode coincidir com um dos operandos.

1.2 Conceito de semigrupo, grupo, sub-grupo e respectiva ordem

Se a operação “.” , para além de ser uma lei de composição interna em E , possuir ainda a propriedade associativa, então a estrutura algébrica adquire uma nova propriedade e passa a designar-se por semigrupo.

$$(E, .) \text{ é semigrupo } \Leftrightarrow \begin{cases} (E, .) \text{ é grupóide.} \\ (a.b).c = a.(b.c), \forall a, \forall b, \forall c \in E \end{cases}$$

Se os elementos do semigrupo E apresentarem as seguintes propriedades :

i) Existência de elemento identidade (neutro) :

$$\exists e \in E : a.e = e.a \forall a \in E$$

ii) Existência de elemento inverso para cada elemento de E :

$$a.a^{-1} = a^{-1}.a = e, \forall a \in E, \forall a^{-1} \in E, a^{-1} \text{ unico}$$

Então podemos concluir que estamos na presença de uma estrutura algébrica mais elaborada, denominada por grupo. No caso da operação “.” ser também comutativa, tem-se um grupo comutativo ou abeliano.

iii) A operação “.” é comutativa quando se verifica a seguinte condição:

$$a.b = b.a, \forall a, \forall b \in E$$

Resumindo, a definição de grupo é a seguinte:

$$(E, .) \text{ é grupo } \Leftrightarrow \begin{cases} (E, .) \text{ é semigrupo.} \\ \text{Existência de elemento identidade em E.} \\ \text{Existência de elemento inverso único para cada elemento de E.} \end{cases}$$

Os grupos podem ter ordem (e.g. cardinalidade) infinita. A ordem de um grupo G denomina-se por $ord(G)$. No entanto para os objetivos do presente estudo apenas se consideram estruturas algébricas com ordem finita. Para simplificar a análise de um determinado grupo este pode ser subdividido em vários sub-grupos com menor cardinalidade que o grupo que lhes deu origem. Um conjunto G é subgrupo de E se respeitar a seguinte relação:

$$(G, .) \text{ é um subgrupo de } (E, .) \begin{cases} (G, .) \text{ é grupo.} \\ G \in E \end{cases}$$

O Teorema de Lagrange enuncia uma propriedade importante que relaciona a ordem do grupo G com a ordem de um dos seus possíveis subgrupos denominado por S.

“ Sendo S um subgrupo de G então $ord(G)$ é múltipla de $ord(S)$ “

1.3 Ordem de um elemento e suas propriedades

No ponto anterior ficou assente que a ordem de um grupo define-se como a cardinalidade do grupo. No entanto associado a cada elemento g do grupo G também existe uma ordem, denominada por $ord(g)$, que se define como o menor número inteiro a que se tem de elevar g para obter o elemento identidade do grupo, designado por e . De uma forma mais formal tem-se :

$$g^{ord(g)} = e, \forall g \in G$$

Tomando como exemplo o grupo de ordem 4, com a operação “.” definida como a multiplicação módulo 5, obtêm-se os seguintes resultados para as várias aplicações da operação:

■	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabela 1 – Grupo de ordem 4 com multiplicação módulo 5.

Como se pode verificar o elemento identidade da operação é o número 1. Cada um dos elementos tem um inverso único. A ordem dos elementos é calculada a partir da definição, e os resultados são os seguintes:

g	ord(g)
1	1
2	4
3	4
4	1

Tabela 2 – Ordem dos elementos do grupo de ordem 4 com multiplicação módulo 5.

Existe uma propriedade importante que relaciona a ordem de um elemento com a ordem do grupo, e que se pode inferir pela tabela acima. Enuncia-se a forma seguinte :

“ A ordem de um elemento é sub-múltipla da ordem do grupo ”

O exemplo anterior serve também para mostrar um Teorema que envolve os grupos e os números primos. O enunciado do Teorema é o seguinte :

- Os elementos $S = \{ 1, 2, 3, \dots, p-1 \}$ formam um grupo comutativo de ordem $p-1$ para a multiplicação módulo p se e só se p for um número primo.

Este Teorema tem uma grande importância na obtenção de Campos de Galois, pelo que é apresentado nesta fase, para consolidar o conceito da estrutura algébrica grupo. Mais adiante na apresentação da estrutura Campo de Galois e respectiva construção, veremos a sua aplicação.

1.4 Anel

Até este ponto analisámos todas as estruturas algébricas até atingirmos o conceito de grupo. Na base da formação da estrutura grupo está a aplicação de uma operação binária sobre um dado conjunto de elementos que obedecem a um dado conjunto de regras.

É possível juntar a um grupo mais uma operação binária denominada por “+” de forma que se estabeleça um conjunto de relações que obedecem a certas regras de forma a obtermos a estrutura algébrica Anel.

$$(E, +, \cdot) \text{ é anel} \Leftrightarrow \begin{cases} (E, +) \text{ é grupo comutativo} \\ (E, \cdot) \text{ é semigrupo} \\ \text{"\cdot" distribui sobre "+" : } a \cdot (b + c) = ab + a \cdot c, \forall a, \forall b, \forall c \in E \end{cases}$$

Esta é a definição base de anel. No entanto esta estrutura ainda pode ter variantes. No caso da operação “ \cdot ” ser comutativa tem-se um anel comutativo. Se a operação “ \cdot ” tiver um elemento identidade então tem-se um anel com identidade. Na situação em que se verificam ambos os casos anteriores tem-se um anel comutativo com identidade.

1.5 Campo

Partindo da definição anterior sobre a constituição de um Anel, se forem verificadas determinadas condições, obtemos uma nova estrutura algébrica denominada por Campo.

$$(E, +, \cdot) \text{ é campo} \Leftrightarrow \begin{cases} (E, +) \text{ é grupo comutativo} \\ (E - \{0\}, \cdot) \text{ é grupo comutativo} \\ \text{"\cdot" distribui sobre "+" : } a \cdot (b + c) = ab + a \cdot c, \forall a, \forall b, \forall c \in E \end{cases}$$

A definição de Campo é por isso semelhante à definição de Anel, apresentada anteriormente.

A definição de campo pode ser escrita da seguinte forma:

“ Um campo é um anel comutativo com identidade, no qual cada elemento tem um inverso multiplicativo. ”

Ou ainda de outra forma mais simples:

“ Um campo é constituído por dois grupos. Todos os elementos formam um grupo comutativo aditivo. Os elementos diferentes de {0} formam um grupo comutativo multiplicativo. ”

Torna-se necessário colocar ênfase nesta definição porque é sobre a estrutura algébrica Campo que o nosso estudo vai incidir a partir desta altura.

2. Campos de Galois

Um Campo de Galois define-se como sendo um campo de ordem finita. Significa que tem uma cardinalidade perfeitamente conhecida, que o caracteriza completamente. Genericamente um Campo de Galois de ordem p representa-se por $GF(p)$.

2.1 Construção

Para obter um Campo de Galois de ordem p inteiro primo, consideram-se todos os inteiros positivos $S = \{0, 1, 2, \dots, p-1\}$. Desta forma respeitam-se as duas condições de construção de um grupo devido às seguintes propriedades [1]:

O conjunto de inteiros $\{0, 1, 2, \dots, p-1\}$, formam um grupo aditivo comutativo para a soma módulo p .

O conjunto de inteiros $\{0, 1, 2, \dots, p-1\}$, com p um número primo positivo formam um grupo multiplicativo comutativo para a multiplicação módulo p .

A forma mais simples que se pode ter, consiste no Campo de Galois de ordem 2 representado por $GF(2)$. É possível obter Campos de ordem superior q gerados a partir da ordem p tal que se verifiquem as seguintes condições :

- p é um número primo;
- $m > 1$;
- $q = p^m$;

2.2 Ordem de um Campo

A partir dos dados do ponto anterior podemos concluir que os Campos de Galois de ordem prima p com valores baixos são fáceis de construir. O seguinte Teorema enuncia a construção de um Campo de Galois de ordem p :

“ Os inteiros positivos $S = \{ 0, 1, 2, \dots, p-1 \}$, sendo p um número primo, constituem o $GF(p)$ para adição e multiplicação módulo p . “

Daqui podemos retirar a importante conclusão que a condição necessária e suficiente para classificar um campo de ordem p , como sendo um $GF(p)$ se p for um número inteiro positivo primo.

Um Campo de Galois de ordem p^m pode ser obtido como um espaço vectorial sobre um outro Campo de ordem p . Portanto os campos de ordem p servem de base geradora para a construção de outros Campos de ordem superior. Para efectuar a construção de Campos de Galois de ordem superior, a partir de Campos com uma dada ordem, é necessário recorrer ao estudo dos Espaços Vectoriais e das suas propriedades mais importantes.

3. Espaços vectoriais

Com esta secção sobre os espaços vectoriais pretende-se expôr um conjunto de conceitos que são necessários e úteis para a obtenção de Campos de Galois de uma determinada ordem, partindo de um Campo com uma ordem prima (base).

3.1 Geração de um Espaço Vectorial

Dado um conjunto V constituído por vectores v_i , e um conjunto F que contém escalares, podemos definir duas operações da seguinte forma :

1 - a operação “+” define-se como a soma de dois vectores pertencentes a V tal que o resultado da soma é um outro elemento pertencente a V ;

$$v_i + v_j = v_k, \forall v_i, \forall v_j, \forall v_k \in V$$

2 - a operação “.” define-se como a multiplicação escalar que efectua um mapeamento de um escalar pertencente a F e um vector pertencente a V num outro vector pertencente a V .

$$w = a.v_i, \forall v_i, \forall w \in V$$

Existe um conjunto de propriedades que caso se verifiquem o conjunto V constitui um espaço vectorial sobre F . Estas propriedades estão descritas no Apêndice A. Nestas condições, F é denominado por campo escalar do espaço vectorial V .

Seguindo a enumeração das propriedades apresentadas no Apêndice A, concluímos que temos duas operações definidas, que podem ser exemplificadas para $u, v \in V$ e $\alpha \in F$ da seguinte forma:

- Soma de dois vectores: $u + v = (u_0+v_0, u_1+v_1, \dots, u_n+v_n)$;

- Multiplicação por um escalar: $\alpha \cdot u = (\alpha u_0, \alpha \cdot u_1, \dots, \alpha \cdot u_n)$;

Sendo $(V,+)$ um grupo comutativo é possível concluir que $v_i = a_1 \cdot v_1 + a_2 \cdot v_2 + \dots + a_n \cdot v_n$ é um vector que pertence a V , porque resulta de uma combinação linear dos vectores da do espaço vectorial V .

3.2 Base geradora do espaço e respectiva dimensão

A base de um espaço vectorial define-se como o conjunto mínimo de vectores linearmente independentes que são necessários para descrever esse espaço sem redundância. A cardinalidade da base é definida como o número de vectores que a constituem. A este valor corresponde a dimensão do espaço vectorial.

Podem existir várias bases para um dado espaço vectorial V , mas apenas existe uma base canónica, que é a base mais simples que pode representar um dado espaço vectorial.

Para cada vector $vi \in V$ existe uma e uma só representação tal que $vi = a1 \cdot v1 + a2 \cdot v2 + \dots + an \cdot vn$. Podemos afirmar que qualquer vector pode ser representado por uma combinação linear dos vários vectores que constituem a base. A representação de um dado vector sobre a base é única, e referida como $(a_0, a_1, \dots, a_{k-1})$.

Um base possível para o espaço vectorial V^3 será :

$$\text{Base} = \{ (0,1,1) , (1,0,1) , (1,1,1) \}$$

A base canónica do espaço vectorial V^3 é :

$$\text{Base} = \{ (1,0,0) , (0,1,0) , (0,0,1) \}$$

3.2.1 Cardinalidade de um espaço vectorial

Seja V um espaço vectorial e F um campo de escalares aplicado sobre V . Seja K a cardinalidade do campo F . Todos os vectores de V podem ser escritos como uma combinação linear, utilizando os escalares que pertencem ao campo F . Dado que a representação de cada vector $vi \in V$ é única, então existem K^n elementos no espaço vectorial V .

3.3 Subespaço vectorial

A definição de subespaço vectorial é importante na análise dos Espaços Vectoriais, à semelhança do conceito de subgrupo como decomposição de grupo, em que efectua a análise de uma estrutura com uma dada cardinalidade utilizando uma ou mais estruturas com cardinalidade inferior.

Seja V um espaço vectorial, e S um seu subconjunto. Sejam os elementos v_1, v_2, \dots, v_n elementos de V e de S . Quando se verificar que qualquer combinação linear de v_1, v_2, \dots, v_n também pertence a S , então S é um subespaço vectorial de V . Por outras palavras S é um subespaço vectorial de V quando ele próprio é espaço vectorial para as mesmas operações de adição e multiplicação.

De uma forma formal, temos a seguinte condição:

$$a.v_1 + b.v_2 \in V \wedge a.v_1 + b.v_2 \in S, \forall a, \forall b \in F, \forall v_1, \forall v_2 \in V$$

Sempre que esta condição se verificar podemos afirmar que S é um subespaço vectorial de G . A análise de um subespaço vectorial como parte integrante de um espaço vectorial tem uma grande importância na análise de códigos de bloco linear.

3.4 Produto interno e Espaço dual

Nesta secção apresenta-se o conceito de espaço dual, que é bastante importante na construção de códigos, a partir de um outro código conhecido. De facto, existem situações em que é mais vantajoso analisar as características de um dado subespaço vectorial a partir do estudo das propriedades do respectivo subespaço dual.

Para a definição de espaço dual ser perfeitamente consolidada, é necessário apresentar o conceito de produto interno entre dois vectores que têm coeficientes sobre a mesma base.

Sejam u e v dois vectores pertencentes ao espaço vectorial V . Estes vectores podem ser descritos pelos seus coeficientes escalares sobre os vectores da base na seguinte forma :

$$\begin{aligned} u &= (u_0, u_1, \dots, u_n) \\ v &= (v_0, v_1, \dots, v_n) \end{aligned}$$

O produto interno entre estes dois vectores é obtido pela multiplicação dos seus coeficientes escalares, sendo definida da seguinte forma:

$$u.v = \sum_{i=0}^{n-1} u_i.v_i = u_0.v_0 + u_1.v_1 + \dots + u_n.v_n$$

As seguintes propriedades podem ser retiradas desta definição:

- i) Comutatividade: $u.v = v.u$;
- ii) Associatividade com multiplicação escalar : $a.(u.v) = (a.u).v$;
- iii) Distributividade para com a adição vectorial : $u.(v + w) = u.v + u.w$;

Com este conhecimento é possível definir o espaço dual de um dado espaço vectorial.

“ Seja S um espaço com dimensão K , e subespaço vectorial de V . Seja S^\perp o conjunto de todos os vectores v que pertencem a V de tal forma que todos os elementos v que pertencem a S^\perp são ortogonais a todos os elementos de S . Nesta situação o espaço vectorial S^\perp define-se como o espaço dual de S . “

Outra propriedade importante que resulta desta definição é que o espaço dual também é um subespaço vectorial de V . Repare-se que os espaços vectoriais S e S^\perp não são complementares porque ambos têm o vector nulo como elemento.

3.5 Teorema da Dimensão

A Teorema da Dimensão enuncia uma propriedade importante que relaciona a dimensão de um espaço S com o seu espaço dual S^\perp . A soma das dimensões destes dois subespaços corresponde à dimensão do espaço vectorial V .

$$\dim(S) + \dim(S^\perp) = \dim(V)$$

Este Teorema, aliado ao conceito de base geradora de um espaço tem uma importância fundamental na construção dos códigos lineares de bloco.

3.5.1 Relação entre um espaço e o seu dual

Sejam V e S dois espaços vectoriais com cardinalidade N , e K respectivamente. O conjunto de vectores $\{g_1, g_2, \dots, g_k\}$ formam uma base do espaço S . Podemos definir uma matriz G com dimensões $[k \times n]$, cujas linhas são os vectores da base de S .

$$G = \begin{bmatrix} g_1 \\ g_2 \\ \dots \\ g_k \end{bmatrix}$$

Como as linhas desta matriz são independentes por definição de base, temos uma matriz geradora de um espaço vectorial de dimensão K . A cardinalidade desse espaço vectorial é K^n . Pela definição de base e de espaço dual, um elemento pertence ao espaço dual S^\perp se o seu produto pela matriz G é nulo. Sendo S^\perp um espaço vectorial, de dimensão t , também pode ser descrito por uma base H .

$$H = (h_1, h_2, \dots, h_t)$$

Esta base pode ser estendida de forma a gerar o espaço vectorial V . Neste caso a base toma a forma:

$$Base = (h_1, h_2, \dots, h_t, d_1, d_2, \dots, d_{n-t})$$

A expansão da base formada pelas colunas da matriz G , formam o espaço vectorial V , de forma que os vectores obtidos por combinação linear das colunas de G , constituem

um espaço vectorial. Um dado elemento v pertencente a esse espaço vectorial pode ser escrito na forma $v = G.X^T$, com $X \in V$.

Obtemos então um espaço vectorial V_1 que pode ser obtido pelos vectores coluna de G , acrescentando um conjunto de expansão. Este espaço V_1 pode ser descrito na forma,

$$\{G.h_1^T, G.h_2^T, \dots, G.h_t^T, G.d_1^T, G.d_2^T, \dots, G.d_{n-t}^T\}$$

Como os produtos dos primeiros t elementos do conjunto anterior são nulos, porque os vectores h_1, \dots, h_t pertencem ao espaço dual S^\perp , os últimos $n-t$ elementos, como são linearmente independentes, devem gerar um espaço de dimensão $n-t = k$. Desta forma confirma-se que a dimensão do espaço dual S^\perp é dada por $t = n - k$. Note-se que um espaço e o respectivo espaço dual não são obrigatoriamente disjuntos. Pelo menos têm como elemento comum o vector nulo. Existem situações particulares em que um espaço vectorial coincide com o seu próprio dual.

4. Descrição das propriedades dos Campos de Galois

Dentro desta secção efectua-se uma análise detalhada de todas as características de um Campo de Galois e dos respectivos elementos que os constituem. Para o conseguir é necessário conjugar propriedades das estruturas algébricas (descritas na primeira secção), com propriedades dos espaços vectoriais descritos na secção anterior.

Começa-se por analisar as propriedades dos Campos de uma forma geral, e em seguida passa-se para a análise dos elementos que o constituem, descrevendo um conjunto de propriedades úteis, que servem de fundamento à aplicação de polinómios sobre o Campo e à factorização do polinómio $x^n + I$, que é a chave para a criação de um código cíclico.

4.1 Ordem do Campo

Sendo um Campo com ordem finita e com todas as suas propriedades bem conhecidas, podemos afirmar que um Campo é completamente caracterizado pela sua ordem. A notação $\mathbf{GF}(p)$ representa um Campo de Galois de ordem p . No caso de termos a notação $\mathbf{GF}(p)[x]$, significa que temos uma aplicação de polinómios sobre os campos de Galois, e que os coeficientes dos polinómios tomam valores entre 0 e $p-1$. O grau dos polinómios designa-se por n e é independente dos coeficientes dos mesmos.

Exemplo :

Campo de Galois com ordem 2 : $\mathbf{GF}(2) = \{ 0, 1 \}$;

Campo de Galois com ordem 3 : $\mathbf{GF}(3) = \{ 0, 1, 2 \}$;

Como será tratado nas secções seguintes, a aplicação de polinómios sobre os Campos de Galois é determinante para a construção de códigos cíclicos.

4.2 Ordem de um elemento

À semelhança da ordem de um elemento de um Grupo, também existe o conceito de ordem de um elemento quando se trata de um Campo, recordando que um Campo é constituído por duas estruturas algébricas do tipo Grupo. A ordem de um

elemento define-se como o menor número inteiro positivo tal que esse elemento precisa de ser operado, usando a operação de carácter multiplicativo do Campo, para obter o seu elemento identidade designado por “1”. De uma forma mais formal temos:

“ Seja $\mathbf{b} \in \text{GF}(p)$. A ordem de \mathbf{b} que se designa por $\text{ord}(\mathbf{b})$ é o menor inteiro positivo m tal que $\mathbf{b}^m = 1$ “

4.2.1 Propriedades

Devido à construção do Campo, verifica-se que a ordem de qualquer elemento $\beta \in \text{GF}(p)$ é um submúltiplo de $p-1$. Este é um resultado que pode ser obtido facilmente a partir do Teorema de Lagrange, que indica que a ordem de um subgrupo S divide com resto zero a ordem de um Grupo G . Este Teorema pode ser enunciado da seguinte forma:

Seja G um Grupo, e S um subgrupo de G . Verifica-se a relação:

$$\text{rem}\left(\frac{\text{ord}(G)}{\text{ord}(S)}\right) = 0$$

Esta propriedade é importante na medida em que indica quais as ordens possíveis dos elementos que constituem um dado Campo. Por exemplo, para um $\text{GF}(16)$, os elementos que o constituem apenas podem ter como ordem os seguintes valores:

$$\{1, 3, 5, 15\}$$

Este é o conjunto dos submúltiplos de 15. Como se pode verificar temos um conjunto de elementos relativamente primos (não partilham nenhum divisor comum para além de 1), excluindo o valor 15.

4.2.2 Número de elementos com uma dada ordem

Desta forma constata-se que existe a possibilidade, de determinar exactamente o número de elementos com uma ordem t num dado Campo. Este resultado pode ser obtido através da função de Euler $\phi(t)$, que dado um conjunto de números inteiros no intervalo $\{1, \dots, t-1\}$, indica quais são os elementos desse conjunto que são relativamente primos. A função de Euler $\phi(t)$, está definida como:

$$f(t) = |\{1 \leq i < t \mid \text{GCD}(i, t) = 1\}| = t \prod_{p|t} \left(1 - \frac{1}{p}\right)$$

A expressão é validada para todos os inteiros positivos primos no intervalo $p < t$, que são divisíveis por t . Indica quais são os elementos desse conjunto que são relativamente primos. Apesar do aspecto da definição da função de Euler parecer algo complexo, é possível simplificar e enunciar de outra forma:

“ Dado um conjunto de inteiros positivos no intervalo $\{1, \dots, t-1\}$, com t um número primo, a função de Euler $f(t)$, obtém o número de elementos que não são relativamente primos a t , ou seja, o número de elementos nesse intervalo que não é submúltiplo de t . “

Enunciamos de seguida duas propriedades importantes desta função, que terão uso mais adiante no tratamento da factorização da expressão x^n-1 .:

- 1 - Se p é um número primo, então $\phi(p) = p-1$, porque todos os elementos diferentes de zero são relativamente primos a um número primo;
- 2 - $\phi(p^m) = p^{m-1} \cdot (p-1)$, para um número primo p ;
- 3 - $\phi(n) \geq 1$, com n positivo;

Exemplo :

$$\phi(6) = \phi(2 \cdot 3) = 6 \cdot (1 - 1/2) \cdot (1 - 1/3) = 2;$$

$$\phi(7) = 7 \cdot (1 - 1/7) = 7 \cdot (6/7) = 6 ;$$

$$\phi(8) = 8 \cdot (1 - 1/2) = 4 ;$$

$$\phi(30) = \phi(2 \cdot 3 \cdot 5) = 30(1 - 1/2) (1 - 1/3) (1 - 1/5) = 30 \cdot (1/2) \cdot (2/3) \cdot (4/5) = 8;$$

4.2.2.1 Generalização para a ordem t

É possível efectuar uma generalização da análise multiplicativa da ordem dos elementos do Campo de Galois. Dado um $GF(q)$ e dada uma ordem t , é possível determinar se existem elementos com essa ordem, e no caso de existirem quantos são.

Considere-se o $GF(q)$ e um dado valor inteiro positivo t .

1. Se t não divide $q-1$, então não existem elementos de ordem t em $GF(q)$;
2. Se t divide $q-1$, então existem $\phi(t)$ elementos de ordem t em $GF(q)$;

4.3 Elementos primitivos

Um elemento que pertence um $GF(q)$, define-se como um elemento primitivo se tiver ordem $q-1$. Partindo deste resultado podemos concluir que cada Campo de Galois de ordem q , denominado por $GF(q)$ contém exactamente $\phi(q-1)$ elementos primitivos.

Por exemplo, dado um $GF(7)$, (ordem prima) temos $\phi(6)=2$ elementos primitivos no Campo. A caracterização deste conjunto de propriedades dos elementos de um Campo de Galois é bastante importante porque serve para caracterizar o Campo e a forma como os seus elementos podem ser representados. A conclusão seguinte é o corolário de todas as propriedades enunciadas até ao momento. De facto, consegue-se provar que,

“ Cada elemento não nulo de um Campo de Galois pode ser representado através de um conjunto com potências de um elemento primitivo, com o expoente a variar de 1 até $q-1$. “

Geralmente um elemento primitivo de $GF(p)$, denomina-se por α .

4.4 Característica de um Campo de Galois

Até este ponto tem sido feita uma análise sobre a operação de carácter multiplicativo (“.”), que pertence ao Campo. Nesta secção descrevem-se as propriedades relacionadas com a operação de carácter aditivo, fornecendo a base para o estudo da aplicação de polinómios.

Seja a função $m(1)$, a representação formal para a soma de m elementos “1”. A característica de um $\text{GF}(p)$ é o menor número inteiro positivo m tal que a soma de m 1's é zero, ou seja, $m(1)=0$. Recorde-se que 0 é o elemento neutro da estrutura aditiva do GF. É possível provar que a característica de um $\text{GF}(p)$ é sempre um número primo inteiro[1]. No caso do $\text{GF}(7)$ tem-se $m(1) = 7$ e no caso de $\text{GF}(4)$ tem-se $m(1)=4$. Efectivamente um $\text{GF}(q)$ de característica p , tem um subcampo de ordem prima que pode ser descrito da seguinte forma:

$$Z_p = \{0, 1, 2(1), 3(1), \dots, (p-1)1\}$$

Analisando a definição anterior da característica de um Campo, conjuntamente com estes os resultados apresentados para $\text{GF}(4)$ e $\text{GF}(7)$, é possível concluir que dado um GF de ordem q , e característica p , podemos concluir que $p(\alpha) = 0, \forall \alpha \in \text{GF}(q)$.

Verifica-se que qualquer Campo $\text{GF}(q)$ contém um subcampo $\text{GF}(p)$ de ordem prima. Visto que $\text{GF}(q)$ forma um grupo aditivo, então podemos concluir que pode ser visto com um espaço vectorial sobre o subcampo $\text{GF}(p)$. Esta é uma propriedade importante, porque indica que um dado campo pode ser gerado a partir de um subcampo de ordem prima.

5. Polinómios sobre os Campos de Galois

Nesta secção juntamos os polinómios, como ferramenta matemática, ao conhecimento já adquirido sobre os Campos de Galois. São enunciadas algumas propriedades que caracterizam os polinómios de grau n , e são recordadas as características mais relevantes dos Campos.

A notação $\text{GF}[q](x)$ é utilizada para indicar um Campo de Galois que tem ordem q , sobre o qual são aplicados polinómios de grau n e com coeficientes com valores compreendidos entre 0 e $q-1$. Um exemplo de um polinómio $p(x)$ pode ser o seguinte:

$$p(x) = a_5 \cdot x^5 + a_4 \cdot x^4 + a \cdot x + 1$$

Os coeficientes de um polinómio a_i pertencem obrigatoriamente ao $\text{GF}(p)$, ao passo que o grau do polinómio n , pode ter um valor qualquer.

5.1 Propriedades dos Polinómios e suas raízes

5.1.1 Irreducibilidade

Um polinómio designa-se por irreduzível quando não é possível efectuar a sua factorização em pelo menos dois polinómios de grau inferior, usando coeficientes até uma determinada ordem.

Exemplo :

Dado o $\text{GF}[2](x)$, e $p(x) = x^2 + x + 1$ um polinómio cujos coeficientes estão compreendidos entre 0 e 1, inclusivé. Este polinómio é irredutível em $\text{GF}(2)$. Mas no caso de considerar $\text{GF}(4)$ (coeficientes a_i tomam valores entre 0 e 3), deixa de ser irredutível.

5.1.2 Primitivo

Um polinómio $p(x)$ de grau m é primitivo em $\text{GF}(p)[x]$ se fôr irredutível e verificar as seguintes condições :

$$\text{rem} \left[\frac{x^n - 1}{p(x)} \right] = 0 ,$$

$$n = p^m - 1$$

Para ser um polinómio primitivo, $p(x)$ deve ser irredutível. No entanto nem todos os polinómios irredutíveis são primitivos. O caso contrário verifica-se sempre. Todos os polinómios primitivos são irredutíveis.

Recordando a função de Euler $\phi(t)$, verifica-se que é possível provar que existem $\phi(2^n - 1)/n$ polinómios primitivos de grau n .

5.1.3 Raízes de um polinómio primitivo

As raízes de um polinómio primitivo possuem propriedades bastante interessantes no estudo dos Campos de Galois, e que servem posteriormente para a geração de Campos de q a partir de subcampos de ordem p . Recorde-se que cada Campo de Galois de ordem q , possui um subcampo de ordem prima p .

A propriedade importante a reter é a seguinte:

“ As raízes (i de um polinómio primitivo, de grau m , $p(x)$ ($\text{GF}(p)[x]$ têm ordem $pm-1$.”

Então se considerarmos que $\text{GF}(p)$ é um subcampo de ordem prima de um campo $\text{GF}(q)$, podemos retirar a seguinte conclusão :

“ **As raízes do polinómio primitivo, de grau m , $p(x) \in \text{GF}(p)[x]$, são elementos primitivos em $\text{GF}(q)$, com $q = p^m$.**“

Isto significa que um $\text{GF}(q)$, pode ser construído à custa de um subcampo de ordem prima $\text{GF}(p)$, e de um seu polinómio primitivo, ou seja, $\text{GF}(q)$ é um espaço vectorial sobre $\text{GF}(p)$. Quando o $\text{GF}(p)$ tem ordem prima, o $\text{GF}(q)$ pode designar-se como a sua extensão.

Tal como os grupos contêm subgrupos, os Campos de Galois também contêm subcampos, para além do subcampo base de ordem prima.

5.1.4 Exemplo da construção de GF(8)

GF(8) pode ser visto como espaço vectorial sobre GF(2). O polinómio $p(x) = x^3 + x + 1$ é primitivo em GF(2). As suas raízes são elementos primitivos de GF(q) com $q = p^m = 2^3 = 8$. Tal como indicado nas propriedades dos elementos primitivos, prova-se que todos os elementos de um GF(q) podem ser obtidos à custa de (q-1) produtos dos elementos primitivos, (Seccção 4.3).

Seja α uma raiz do polinómio primitivo $p(x)$. Podemos obter uma representação vectorial de GF(8) , tal como apresentado na tabela seguinte, através do conjunto base $\{1, \alpha, \alpha^2\}$.

0	(0,0,0)
α	(0,1,0)
α^2	(0,0,1)
$\alpha^3 = \alpha + 1$	(1,1,0)
$\alpha^4 = \alpha^2 + \alpha$	(0,1,1)
$\alpha^5 = \alpha^2 + \alpha + 1$	(1,1,1)
$\alpha^6 = \alpha^2 + 1$	(1,0,1)
$\alpha^7 = 1$	(1,0,0)

Tabela 3 - Representação de GF(8) em forma vectorial.

Ao conseguir efectuar a construção de GF(8) desta forma, ficando como representação vectorial, as operações efectuadas sobre este Campo ficam bastante facilitadas na medida em quando se pretende efectuar adição em GF(8), basta efectuar adição de vectores sobre GF(2). Este é um aspecto importante a ter em conta quando se pretende efectuar a implementação de um GF(q) , com $q=p^m$, tanto em *hardware* como em *software*, porque basta ter os vectores da base e efectuar combinações entre eles para obter um determinado elemento. Por exemplo, para obter o elemento α^5 tem-se :

$$\alpha^5 = \alpha^2 + \alpha + 1$$

A soma de vectores correspondente é dada por:

$$(0,0,1) + (0,1,0) + (1,0,0) = (1,1,1).$$

Desta forma fica ilustrada a importância das propriedades dos polinómios primitivos e das suas raízes na construção de Campos de Galois.

5.1.5 Tamanho de um polinómio

Uma métrica possível que se pode aplicar sobre qualquer polinómio $p(x)$ consiste no seu tamanho. O tamanho de um polinómio define-se como o seu grau, e

geralmente representa-se por $g(p)$. A sua aplicação a um $GF(p)[x]$, que é um anel comutativo com identidade, transforma o anel num Domínio Euclideano [Apêndice B].

5.2 Características de um Domínio Euclideano

Os Domínios Euclidianos tal como estão definidos fornecem uma forma intuitiva para a noção de divisão, sendo por isso utilizados para efectuar divisões de polinómios. Se considerarmos dois elementos a e b pertencentes a um Domínio Euclideano D , podemos afirmar que a é o divisor de b , se existir um elemento $c \in D$ tal que $a.c = b$.

5.2.1 Máximo divisor comum

Define-se como divisor comum de um conjunto de elementos $\{ b_0, b_1, \dots, b_n \}$, um elemento d (que pode pertencer ao conjunto), tal que exista divisão inteira de todos os elementos do conjunto por d . Podem existir vários divisores comuns para um dado conjunto. O máximo divisor comum define-se como o maior dos divisores comuns de uma dado conjunto.

O máximo divisor comum entre dois números inteiros exprime-se na forma $GCD(a,b)$. O algoritmo de Euclides[Apêndice B] fornece uma forma rápida de encontrar o GCD entre dois elementos que pertencem a um Domínio Euclideano. Por exemplo, o conjunto dos inteiros positivos forma um Domínio Euclideano.

5.2.2 Aplicação a polinómios

Verifica-se que a aplicação de polinómios sobre um Campo com dimensão finita, formam um Domínio Euclideano. É possível concluir que então que o algoritmo de Euclides pode ser aplicado para encontrar o máximo divisor comum entre dois polinómios sobre um dado $GF(p)$.

Consideremos os seguintes polinómios definidos em $GF(2)$:

$$\begin{aligned} p_1(x) &= x^5 + x^3 + x + 1 \\ p_2(x) &= x^4 + x^2 + x + 1 \end{aligned}$$

Aplicando o algoritmo de Euclides, podemos encontrar o máximo divisor comum entre estes dois polinómios, dado por :

$$GCD(p_1(x), p_2(x)) = (x + 1)$$

Outro aspecto importante, é que o GCD entre dois quaisquer elementos de um Domínio Euclideano pode ser obtido à custa da combinação linear desses mesmos elementos.

Recordando o caso dos dois polinómios anteriores, podemos efectuar os seguintes cálculos:

$$\begin{aligned} &GCD(x^5 + x^3 + x + 1, x^4 + x^2 + x + 1) \\ &= (x + 1) \\ &= (x^4 + x^2 + x + 1) + (x^2 + 1). x^2 \\ &= (x^4 + x^2 + x + 1) + (x^5 + x^3 + x + 1 + (x^4 + x^2 + x + 1).x). x^2 \\ &= (x^4 + x^2 + x + 1). (1 + x^3) + (x^5 + x^3 + x + 1). x^2 \end{aligned}$$

De uma forma genérica podemos afirmar que $\text{GCD}(a,b) = r.a + s.b$. Este resultado pode ser generalizado para um Domínio Euclideano da seguinte forma :

“ Seja $B = \{ b_1, b_2, \dots, b_n \}$ um subconjunto finito de elementos de um domínio euclideano D . O subconjunto B terá um GCD designado por d , que pode ser expresso na forma $\sum \lambda_i b_i$, em que os coeficientes λ_i estão contidos em D . “

Este conjunto de coeficientes pode ser obtido de uma forma sistemática através do algoritmo estendido de Euclides [Apêndice C]. De facto, este algoritmo para além de encontrar o máximo divisor comum, também obtém os coeficientes que formam a combinação linear.

5.3 Polinómios mínimos

A definição de polinómio mínimo é importante na medida em que estabelece uma relação entre os polinómios e elementos primitivos de $\text{GF}(q)$.

Seja $\alpha \in \text{GF}(q^m)$. O polinómio mínimo de α em ordem a $\text{GF}(q)$ é o polinómio $p(x)$ não nulo de menor grau possível em $\text{GF}(q)[x]$, tal que $p(\alpha)=0$. Para cada elemento α , existe um polinómio mínimo tal que $p(\alpha)=0$.

5.3.1 Propriedades

Um polinómio mínimo $p(x)$ sobre os elementos $\alpha \in \text{GF}(q^m)$, apresenta as seguintes propriedades :

- $p(\alpha) = 0$;
- grau de $p(x)$ é menor ou igual que m ;
- $f(\alpha) = 0$ implica que $f(x)$ é múltiplo de $p(x)$;
- $p(x)$ é irredutível em $\text{GF}[q](x)$;

Conjugando este conjunto de propriedades, podemos afirmar que “ um polinómio primitivo é um polinómio mínimo sobre um elemento primitivo “.

A factorização de polinómios mínimos em campos de ordem superior é a chave para a implementação de códigos cíclicos. Repare-se que um polinómio mínimo é irredutível em $\text{GF}[q](x)$, mas não o será em $\text{GF}(q^m)[x]$.

5.4 Elementos conjugados

Continuando a análise da factorização de polinómios mínimos, vamos analisar o conceito de elemento conjugado e classe de elementos conjugados.

Cada elemento $\beta \in \text{GF}(q^m)$ possui um conjunto de elementos conjugados, em ordem ao subcampo $\text{GF}(q)$, dados por :

$$\{ \mathbf{b}, \mathbf{b}^q, \mathbf{b}^{q^2}, \mathbf{b}^{q^3}, \dots \}$$

O conjunto destes elementos designa-se por **classe dos elementos conjugados de \mathbf{b} , em relação $\text{GF}(q)$** . O número de elementos d que constituem esta classe é dado pela expressão:

$$\mathbf{a}^{q^d} = \mathbf{a}, \text{ sendo } d \text{ um submúltiplo de } m.$$

Exemplo de uma classe de elementos conjugados:

Seja α um elemento de ordem 3 pertencente a $GF(16)$. A classe de elementos conjugados de α em relação a $GF(2)$ é dada pela análise do conjunto:

$$\{ \mathbf{a}, \\ \mathbf{a}^{2^1}, \\ \mathbf{a}^{2^2} = \mathbf{a} \\ \}$$

Como o terceiro elemento começa a repetir a sequência, a classe de elementos conjugados é:

$$\{ \mathbf{a}, \mathbf{a}^2 \}$$

A definição de classe de elementos conjugados pode ser aplicada sobre as raízes de um polinómio mínimo $p(x)$, e obtemos o seguinte Teorema sobre a localização das suas raízes.

“ Seja $\mathbf{a} \in GF(q^m)$. Seja $p(x)$ um polinómio mínimo de \mathbf{a} em relação a $GF(q)$. As raízes de $p(x)$ são os conjugados de \mathbf{a} em relação a $GF(q)$. “

Esta propriedade das raízes do polinómio mínimo é suficiente para garantir que os coeficientes do mesmo estão no subcampo $GF(q)$. Logo é possível termos um polinómio primitivo num campo de ordem q^m , cujos coeficientes são elementos de $GF(q)$.

5.5 Factorização de $x^n - 1$

Concluída a apresentação das propriedades dos polinómios sobre os Campos de Galois, passamos a analisar a questão da factorização da expressão $x^n - 1$ que é a questão central para a implementação de códigos cíclicos.

A factorização da expressão $x^n - 1$ em $GF(q^m)$ é feita à custa da utilização de polinómios mínimos para os elementos diferentes de zero pertencentes a $GF(q^m)$. Torna-se necessário enunciar mais um Teorema que é consequência da junção da análise que tem sido feita sobre as propriedades dos polinómios, e a criação de $GF(q^m)$ a partir de $GF(q)$.

“ O conjunto dos elementos diferentes de zero que pertencem a $GF(q^m)$ constituem o conjunto total das raízes da expressão $x^{(q^m-1)} - 1 = 0$. ”

Deste Teorema podemos concluir que a utilização de polinómios mínimos sobre os elementos diferentes de zero que pertencem a $GF(q^m)$, efectuam a factorização completa da expressão indicada acima.

Exemplo:

Factorização de x^7-1 em $\text{GF}(2)[x]$:

$$x^7-1 = (x+1) \cdot (x^3+x+1) \cdot (x^3+x^2+1)$$

5.5.1 Utilização das classes de elementos conjugados

A utilização das classes de elementos conjugados pode ser estendida para efectuar a factorização da expressão x^n-1 . Do Teorema anterior podemos inferir que todas as raízes de x^n-1 são raízes de ordem n da unidade (elementos de $\text{GF}(q^m)$ cuja ordem é n). Depois de identificadas as raízes, é necessário determinar o Campo ao qual todas pertencem, efectuar um agrupamento em classes de elementos conjugados, e determinar os respectivos polinómios mínimos.

A obtenção de um polinómio mínimo (gerador) pode ser feita da seguinte forma:

- Sobre um $\text{GF}(q^m)$, assume-se a existência de um elemento β , tal que a sua ordem seja n ;
- Consideram-se todas as suas potências $\beta^2, \beta^3, \dots, \beta^n$. Estes valores são únicos;
- Todas as potências satisfazem a condição $x^n-1=0$.
- As n potências de β constituem as n raízes da expressão x^n-1 ;

Devido ao referido no ponto 4, os elementos de ordem n num dado $\text{GF}(q^m)$ são normalmente designados n raízes primitivas da unidade. Para o método de cálculo anterior ser válido é necessário encontrar o elemento β de ordem n . Segue-se a demonstração da existência do elemento β .

Prova da existência de um elemento de ordem n em $\text{GF}(p^m)$:

Na secção 4.2.2, constatou-se que existem $\phi(n)$ elementos com ordem n , dado que n é divisor de p^m-1 . Sempre que $n \geq 1$, existe a garantia da existência de pelo menos um elemento nessas condições, o que garante imediatamente a existência de uma raiz primitiva da unidade no campo $\text{GF}(p^m)$. Torna-se então necessário obter um valor inteiro positivo m tal que n divida a expressão p^m-1 com resto zero.

5.5.1.1 Menor ordem de extensão possível

Até esta altura foi referida uma extensão de ordem m , de um $\text{GF}(p)$, obtendo-se $\text{GF}(p^m)$. Existem várias extensões que se podem efectuar sobre um Campo de Galois. No desenho de determinados códigos existe interesse em determinar qual a menor extensão possível que se pode efectuar sobre um determinado $\text{GF}(p)$. A resposta a esta questão está na definição de ordem q modulo n , que é a seguinte :

“ A ordem q modulo n , é o menor inteiro positivo m tal que n é dividido por q^m-1 com resto zero. “

Se m for a ordem de q modulo n , então $\text{GF}(q^m)$ é a menor extensão de $\text{GF}(q)$ na qual é possível encontrar raízes de ordem n primitivas da unidade.

5.5.1.2 Regra geral de factorização

Exemplo:

Factorização de x^5-1 em $GF(4)[x]$:

Verifica-se que $5 \mid (2^4-1)$, sendo $m=4$, o menor inteiro positivo que efectua a divisão indicada com resto zero. Podemos concluir que $GF(16)$ é o Campo que efectua a menor extensão binária de $GF(2)$, onde é possível encontrar raízes de ordem quinta primitivas da unidade.

Podemos encontrar os polinómios mínimos para os elementos de $GF(16)$ através da classe de elementos conjugados. Foi constatado acima que existem em $GF(16)$ raízes de ordem quinta primitivas da unidade. Considerando um elemento primitivo α (com ordem 15). Seguindo esta ordem de raciocínio α^3 deve ter ordem 5, logo é uma raiz primitiva da unidade. Se fizermos $\beta=\alpha^3$ e determinarmos as classes de elementos conjugados (contendo as raízes pretendidas), podemos obter os polinómios mínimos.

Classe de elementos conjugados	Polinómio mínimo
$\{\alpha^0 = 1\}$	$M_0(x) = (x - 1) = x + 1$
$\{\beta, \beta^4\} = \{\alpha^3, \alpha^{12}\}$	$M_3(x) = x^2 + \alpha^{10}x + 1$
$\{\beta^2, \beta^3\} = \{\alpha^6, \alpha^9\}$	$M_6(x) = x^2 + \alpha^5x + 1$

Tabela 4 - Classes de elementos conjugados e respectivos polinómios mínimos em $GF(16)$.

Concluimos então que utilizando um elemento primitivo de $GF(16)$ podemos factorizar o polinómio x^5-1 da seguinte forma:

$$x^5 - 1 = (x + 1). (x^2 + \alpha^{10}x + 1) .(x^2 + \alpha^5x + 1)$$

Analisando a tabela anterior de uma forma mais atenta verificamos que a cada classe corresponde um factor. Existe ainda mais informação que se pode retirar da tabela, tal como é apresentada de seguida.

No caso de apenas ser pretendido determinar o número e o grau dos factores de x^n-1 , é possível proceder da seguinte forma :

- 1 - O número de classes de elementos conjugados é o número de factores no qual se pode decompôr o polinómio x^n-1 .
- 2- A cardinalidade de cada classe de elementos conjugados indica o grau do polinómio associado.

Este é um processo para a obtenção de polinómios geradores de códigos cíclicos. Note-se que um polinómio que seja gerador não constrói necessariamente um bom código cíclico. É portanto necessário analisar as palavras produzidas, nomeadamente em relação ao seu peso de Hamming, para determinar se o código produzido tem uma boa capacidade de controlo de erros, para o *code rate* que possui.

Na secção seguinte veremos como é possível chegar a estes resultados de uma forma mais rápida tirando partido das propriedades enunciadas para os Domínios Euclidianos.

5.6 Estudo do anel $\text{GF}(q)[x]/(x^n-1)$

Efectuando uma análise ainda mais profunda sobre a Teoria dos Domínios Euclidianos, é possível obter polinómios geradores de uma forma ainda mais rápida. Recordando os conceitos de Anel e Campo, introduzidos na secções 1.4 e 1.5 respectivamente, verificamos que se o conjunto dos inteiros fosse limitado em módulo m , sendo m um número inteiro, temos um Anel comutativo com identidade. No caso de ser um valor primo temos um Campo.

O mesmo comportamento acontece para o caso dos Domínios Euclidianos com polinómios. Se um dado domínio for reduzido em módulo $f(x)$, sendo $f(x)$ um polinómio, obtêm-se resultados análogos. Nesta situação utiliza-se a notação $\text{GF}(q)[x] / f(x)$ para a representação do Domínio Euclidiano. Podemos enunciar o seguinte Teorema :

“ Se $p(x)$ for um polinómio irredutível em $\text{GF}(q)[x]$, então $\text{GF}(q)[x]/p(x)$ é um Campo. ”

Fazendo $p(x) = x^n - 1$, obtemos um conjunto de propriedades que são determinantes na construção de códigos cíclicos. De facto trata-se de uma estrutura algébrica com uma disposição interna bem definida em relação aos seus ideais. Torna-se necessário a definição e enumeração das propriedades desta nova estrutura algébrica.

5.6.1 Definição de Ideal e Ideal principal

Seja R um Anel, e I um subconjunto de R . O conjunto I é um ideal se respeitar as seguintes condições:

- $(I,+)$ é um grupo, sendo “+” a operação de carácter aditivo em R ;
- $a.r = b \in I, \forall a \in I \text{ e } \forall r \in R$;

Partindo da definição de ideal, e impondo mais uma condição podemos extrair a definição de ideal principal, que pode ser enunciada da seguinte forma :

“ Seja I um ideal de R . Se existir um elemento $g \in I$, tal que cada elemento $c \in I$ possa ser expresso pelo produto $m.g$, com $m \in R$, diz-se que I é o ideal principal de R . “

Nesta situação o elemento g designa-se por elemento gerador, visto que pode ser utilizado para representar todos os restantes elementos do Ideal principal. A representação do Ideal principal é designada por $\langle g \rangle$.

5.6.2 Ideal sobre $\text{GF}(q)[x]/(x^n-1)$

Juntando a análise efectuada sobre polinómios irredutíveis aplicados a Campos de Galois de ordem q ($\text{GF}(q)[x]/p(x)$), com a definição de Ideal principal de um Anel, obtemos um conjunto de propriedades [1], que são as seguintes :

Seja I um Ideal em $GF(q)[x] / (x^n-1)$.

1. Existe um único polinómio $g(x) \in I$, com grau mínimo;
2. I é principal com gerador $g(x)$;
3. $g(x)$ é factor de x^n-1 em $GF(q)[x]$;

Através da factorização do polinómio x^n-1 é possível caracterizar todos os ideais no Anel $GF(q)[x] / x^n-1$.

Exemplo:

Para $GF(2)[x] / (x^7-1)$, temos os seguintes ideais :

- i) $x+1$;
- ii) x^3+x+1 ;
- iii) x^3+x^2+1 ;
- iv) $\langle (x+1)(x^3+x^2+1) \rangle$;
- v) $\langle (x^3+x+1)(x^3+x^2+1) \rangle$;
- vi) $\langle (x+1)(x^3+x+1) \rangle$;

Recorde-se das secções anteriores que os polinómios x^3+x+1 e x^3+x^2+1 são polinómios mínimos em $GF(2)[x]$.

6. Códigos lineares de bloco

Nesta última secção é feita uma correspondência entre toda a teoria sobre Campos de Galois, apresentada nas últimas secções, e a implementação prática de códigos, nomeadamente códigos lineares de bloco cíclicos e não cíclicos.

A referência aos códigos de bloco linear será feita utilizando a notação típica (n,k) , em que n é o número de bits da palavra de código, e k o número de bits da mensagem. A partir destes dois parâmetros do código, é possível deduzir que este tem um número de bits de paridade (redundância para controlo de erros) dado por $q = n - k$.

Para um determinado código de bloco (n,k) ser caracterizado como linear, é necessário respeitar as seguintes propriedades:

- vector nulo $X = (0 \ 0 \ \dots \ 0)$ é uma palavra válida do código;
- A soma de duas quaisquer palavras do código é uma outra palavra válida;

6.1 Analogia com o conceito de grupo

Efectuando a analogia com a definição da estrutura algébrica grupo (referida na secção 1.2) concluímos que as palavras do código constituem um grupo comutativo sobre a adição, designado por $(X,+)$. Sobre um código linear é possível estabelecer um conjunto de propriedades.

- i) As palavras do código formam um espaço fechado para a adição, que é uma lei de composição interna em X ;
- ii) A operação adição é associativa;
- iii) Cada palavra somada com ela própria resulta no elemento identidade, logo todas as palavras têm inverso para a adição;
- iv) O vector nulo $X=(0 \ 0 \ \dots \ 0)$ é o elemento identidade (neutro) para a adição;

- v) A adição é uma operação comutativa;

6.2 Analogia com a noção de espaço vectorial

Cada código linear tem uma matriz geradora G através da qual se obtêm as várias palavras do código. Para um código (n,k) , a matriz geradora G tem como dimensões $k \times n$. Esta matriz caracteriza-se por ter um conjunto de k linhas linearmente independentes entre si, de forma que é uma base de um espaço vectorial de dimensão k . Recorde-se que a dimensão de um espaço vectorial é o número de elementos (vectores) que constituem a base desse espaço. As palavras mensagem M constituem os coeficientes que pertencem a um grupo de escalares. Tem-se portanto a aplicação de um conjunto de escalares sobre um espaço vectorial.

As palavras do código são obtidas pela multiplicação $X = M \cdot G$, em que M é o vector mensagem com dimensões $1 \times k$, G é a matriz geradora $k \times n$, e X é a palavra de código com dimensões $1 \times n$. De facto a obtenção de uma palavra do código resume-se a efectuar uma combinação linear das linhas da matriz geradora.

Exemplo:

Para o código de Hamming $(7,4)$:

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

Seja o vector mensagem para a palavra nº 6 $M_6 = [1 \ 0 \ 1 \ 0]$. Para obter a palavra de código correspondente X_6 temos a soma da primeira e terceira linhas :

$$X_6 = [1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1] + [0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0] = [1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1]$$

Desta forma podemos afirmar que X_6 corresponde à combinação linear dos vectores da base, utilizando o conjunto de coeficientes $\{ 1 \ 0 \ 1 \ 0 \}$. Outra forma de efectuar este análise é verificar que os elementos do espaço vectorial formam um grupo sob operação adição.

A dimensão de um código linear define-se como a dimensão do espaço vectorial associado. No caso genérico de um código (n,k) temos uma dimensão k , para um número total de palavras dado por 2^k . Para o exemplo do código de Hamming(7,4) temos um código de dimensão 4 com 16 palavras possíveis. A existência da linearidade garante um conjunto de propriedades para esta família de códigos, que podem ser obtidas directamente dos espaços vectoriais.

6.2.1 Código dual

Um dado código C^\perp define-se como dual de um outro código C com dimensões (n,k) se possuir as seguintes características[4]:

- tem como dimensão das palavras de código e de mensagem n e $n-k$ bits respectivamente;

- a matriz geradora G do código (n,k) é a matriz de teste de paridade H do código $(n,n-k)$:
- a matriz de teste de paridade H do código (n,k) é a matriz geradora do código $(n,n-k)$:

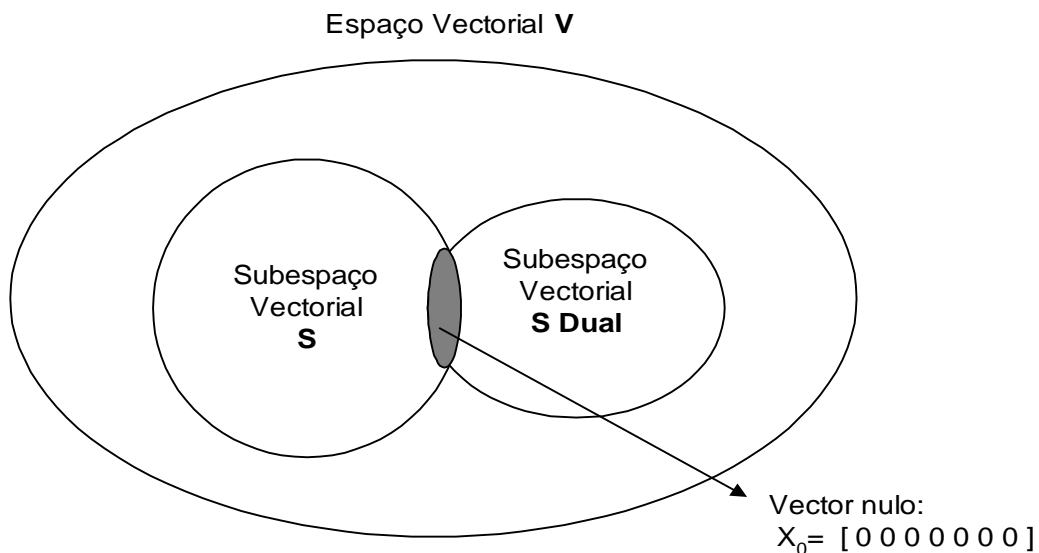
Verifica-se ainda que ambos os códigos são lineares. Deste conjunto de propriedades resulta que as palavras de ambos os códigos são ortogonais entre si. O desenho do código dual pode ser obtido através da análise da definição de subespaço vectorial e respectivo espaço dual, passando pelo Teorema da Dimensão. Dado um espaço vectorial S , o seu espaço dual S^\perp caracteriza-se por todos os seus elementos serem ortogonais entre si e ambos contêm o vector nulo.

Por definição de código linear de bloco tem-se que o produto entre a matriz geradora G e a matriz de controlo de paridade H é nulo.

$$G.H^T = 0$$

Para o produto das duas matrizes ser nulo, é necessário que todas as linhas da matriz G sejam linearmente independentes das colunas da matriz H^T . Como as colunas desta matriz correspondem às linhas da matriz H , então podemos concluir que existe ortogonalidade entre os vectores das matrizes G e H . Pela definição de código dual, verificamos que as matrizes geradores de um código e do seu dual são ortogonais entre si. No apêndice D encontra-se uma análise mais pormenorizada da implementação de um código de Hamming $(7,4)$ e respectivo código dual $(7,3)$.

Em termos de espaços vectoriais podemos verificar que temos um espaço vectorial V de dimensão 7. Este espaço vectorial pode ser analisado através de um subespaço vectorial e respectivo espaço dual, passando pelo Teorema da Dimensão referido na secção 3.5. Em termos gráficos podemos representar as palavras de ambos os códigos como dois subespaços, que são duais mas não são disjuntos porque ambos contêm o vector nulo.



Figural - Representação das palavras de um código e do respectivo dual, em termos de decomposição de um espaço vectorial em dois subespaços duais entre si.

Em termos de matrizes geradoras e de teste de paridade, verificam-se as seguintes igualdades :

- a matriz geradora G do código (n,k) corresponde à base do espaço vectorial S , que por sua vez coincide com a matriz de teste de paridade do código associado ao espaço S dual.

- a matriz geradora G_d do código dual $(n,n-k)$ constitui a base do espaço vectorial S^\perp . Esta corresponde à matriz de teste de paridade do código (n,k) .

6.3 Códigos sistemáticos

Os códigos sistemáticos caracterizam-se por dispôr as palavras de uma forma tal que os *bits* da mensagem estão separados dos *bits* de redundância. A implementação feita desta forma destina-se a facilitar a recepção das palavras e respectiva construção do decodificador. As palavras do código são obtidas pela multiplicação de vectores mensagem por uma matriz geradora que constitui a base do espaço. Sendo o código sistemático, então a matriz I_k deve integrar G , para manter os *bits* de mensagem inalterados quando se obtém a palavra de código. Desta forma existem duas hipóteses para definir esta matriz :

$$G = [P \mid I_k] \text{ ou } G = [I_k \mid P],$$

com P a submatriz geradora de paridade com dimensões $k \times q$.

No ponto anterior o código de Hamming(7,4) é um exemplo de um código de bloco linear sistemático. As palavras estão organizadas na forma $[M \mid C]$.

6.4 Códigos não sistemáticos

O caso dos códigos não sistemáticos é mais complicado. Nesta situação a matriz geradora G já não contém a matriz identidade I_k . Os bits de mensagem estão intercalados com os *bits* de paridade.

O código de Hamming(7,4) original tinha a característica não sistemática[2], para facilitar a detecção e correcção. As palavras deste código estão organizadas na forma $X = [c_1 \ c_2 \ m_1 \ c_3 \ m_2 \ m_3 \ m_4]$. A matriz geradora é a seguinte :

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

O objectivo da implementação do código desta forma é facilitar a correcção de erros, dado que ao construir a tabela de síndromas, verifica-se que o número representado pelo valor do síndrome indica qual o *bit* errado (apêndice E). Os códigos de Hamming caracterizam-se por ser códigos perfeitos para a correcção de erros de um *bit*.

6.5 Códigos lineares modificados

Por vezes existem restrições na prática que levam a uma modificação do comprimento das palavras de código a enviar por um determinado canal. Um caso flagrante de uma situação deste género está presente na comunicação série. Quando se pretende transmitir dados via canal série utilizando um UART, geralmente os dados devem ser enviados em blocos de 8 *bits* que constituem um *byte*. Se pretendermos enviar palavras de um código Hamming(7,4) é vantajoso aproveitar o “oitavo *bit* extra” para melhorar as características do código, uma vez que as palavras devem ser enviadas em blocos.

6.5.1 Extensão

A extensão de um código linear de bloco (n,k) consiste em acrescentar mais um *bit* de redundância, passando a ter a representação (n+1,k). Para os mesmos *bits* de mensagem existe mais um *bit* de controlo de paridade, o que aumenta a capacidade de controlo de erros, mas diminui a *code rate* do código (eficiência).

Em termos de espaço vectorial o número de vectores que constituem a matriz geradora mantém-se e portanto a dimensão do código não se altera. O comprimento das palavras aumenta de um. Se for efectuada a extensão de um código de Hamming (7,4) obtem-se um código (8,4).

Um exemplo de extensão é acrescentar um *bit* de redundância que efectua a paridade de todos os *bits* anteriores que constituem a palavra. Seguindo este critério a matriz geradora do código de Hamming estendido será a seguinte

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

6.5.2 Redução

A redução de um código (n,k) consiste em retirar um *bit* da mensagem, mantendo o número de *bits* redundantes, o que resulta num código (n-1,k-1). Nesta situação para além do comprimento das palavras também a dimensão do código é alterada. Para o caso do código de Hamming(7,4) obtem-se um código (6,3) cuja matriz geradora pode ser representada da seguinte forma

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

Visto que se diminui o número de *bits* de mensagem mantendo o número de *bits* de redundância, a capacidade de controlo de erros do código reduzido será sempre igual ou superior à do código original. Note-se que tanto a redução como a extensão de um código cíclico não resulta obrigatoriamente noutra código cíclico. Na secção seguinte está descrita a forma como as palavras de um código cíclico são desenhadas e toda a teoria associada.

Existem outras formas de modificação dos códigos lineares que podem ser aplicadas e estão referidas em [1 Pags 94-96].

6.6 Códigos cíclicos

Os códigos cíclicos são uma família importante dos códigos lineares. Todos os códigos cíclicos são lineares, mas a recíproca não é verdadeira. De facto, na prática são bastante usados, especialmente na comunicação entre computadores, devido a várias características entre as quais se podem referir :

- simplicidade e eficiência tanto em termos de codificação como de descodificação;
- *code rate* razoável com uma boa capacidade de detecção de erros;
- capacidade razoável de correcção de erros;
- detecção de *bursts* de erros;

Um código cujas palavras têm comprimento n é cíclico se todas as suas palavras formam um Ideal sobre $\text{GF}(q)[x] / (x^n - 1)$.

6.6.1 Desenho das palavras do código

Na secção 5.3.1 afirmou-se que a factorização de polinómios mínimos em campos de ordem superior, recorrendo à classe dos elementos conjugados, é a chave para a implementação de códigos cíclicos. A questão que se coloca no desenho de um código cíclico é a seguinte:

“ Tendo um polinómio $p(x)$ com coeficientes em $\text{GF}(q)$, pretende-se que esse polinómio tenha uma raiz em $\text{GF}(q^m)$. Que outras raízes o polinómio deve ter ? “

A resposta a esta questão passa pelos elementos conjugados e classe de elementos conjugados, apresentada na secção 5.4, em que se verifica que as raízes de um polinómio mínimo $\text{GF}(q^m)$ têm um conjunto de propriedades tal que se verifica que os coeficientes do polinómio estão no campo $\text{GF}(q)$. Sendo um polinómio primitivo, temos então o polinómio gerador de um código.

Recordando a construção de $\text{GF}(8)$ a partir de $\text{GF}(2)$ (secção 5.1.4), consideramos o polinómio $p(x) = x^3 + x + 1$ primitivo em $\text{GF}(2)$, e uma raiz desse polinómio designada por α . Os elementos constituintes de $\text{GF}(8)$ podem ser gerados a partir desse elemento primitivo.

Representação exponencial	Representação polinomial
α^0	1
α	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$
α^7	1

Tabela 5 - Representação polinomial e exponencial de $\text{GF}(8)$.

Calculando as classes de elementos conjugados e agrupando os elementos pelas respectivas classes, e polinómios mínimos temos a seguinte ordenação:

Classe de elementos conjugados	Polinómio mínimo associado
{ 0 }	$(x - 0) = x$
{ $\alpha^0 = 1$ }	$(x - 1) = x + 1$
{ $\alpha, \alpha^2, \alpha^4$ }	$(x-\alpha)(x-\alpha^2)(x-\alpha^4) = x^3 + x + 1$
{ $\alpha^3, \alpha^6, \alpha^5$ }	$(x-\alpha^3)(x-\alpha^6)(x-\alpha^5) = x^3 + x^2 + 1$

Tabela 6 - Classes de elementos conjugados e polinómios mínimos em GF(8).

Os polinómios mínimos são calculados a partir dos valores das classes de elementos conjugados, tal como apresentado na tabela. Recordando o código de bloco linear sistemático cíclico Hamming(7,4), cujo polinómio gerador é $G(p) = p^3 + p + 1$. Se analisarmos a tabela com atenção verificamos que este polinómio está representado na lista dos polinómios mínimos obtidos.

Da tabela 6 podemos ainda extrair outro polinómio $G(p) = p^3 + p^2 + 1$. Este segundo polinómio também gera um código cíclico, tal como apresentado no apêndice E.

6.6.2 Polinómio gerador

No ponto anterior verificamos que temos dois polinómios mínimos sobre GF(8) que geram códigos cíclicos. De facto, para obter um código cíclico é necessário um **polinómio gerador que seja factor de um polinómio mínimo**.

As propriedades dum polinómio gerador de um código cíclico são as seguintes:

Consideremos C um código linear cíclico (n, k) :

1- No conjunto de todos os polinómios que correspondem a palavras de código em C, existe um único polinómio $g(x)$ com um grau q , que é denominado de polinómio gerador.

2 - Todos os polinómios $c(x)$ que constituem as palavras de código podem ser expressos de uma forma inequívoca designada por $c(x) = m(x) \cdot g(x)$, em que $g(x)$ é o polinómio gerador de C e $m(x)$ é um polinómio com grau inferior ou igual a $k-1$.

3 - O polinómio gerador $g(x)$ de C é um factor de x^n-1 em $GF(q)[x]$;

Confrontando estas características dos códigos cíclicos com as propriedades dos Ideais e seu elemento gerador (secção 5.6.2), podemos concluir que existe uma correspondência directa. De facto, a utilização da estrutura Ideal sobre $GF(q)[x] / x^n-1$, permite encontrar de uma forma imediata um polinómio gerador para um determinado código cíclico.

6.6.3 Código dual e respectivo polinómio gerador

Seja C um código linear cíclico (n, k) , com polinómio gerador $g(x)$ e polinómio de teste de paridade $h(x)$. C^\perp é um código cíclico $(n, n-k)$ cujo polinómio gerador é $h^*(x)$, o polinómio recíproco de $h(x)$. O polinómio recíproco é obtido da seguinte forma:

Seja $f(x)$ um polinómio de grau n , $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$. O recíproco $f^*(x)$ é dado por $x^n \cdot f(x^{-1}) = f_n + f_{n-1}x + f_{n-2}x^2 + \dots + f_0x^n$.

Exemplo:

1. Geração do código Hamming(7,4)

O polinómio gerador do código de Hamming $(7,4)$ é $G_1(p) = p^3 + p + 1$. O polinómio de teste de paridade $H_1(p)$ deste código é dado pelo quociente da divisão

$$H_1(p) = \frac{p^7 + 1}{p^3 + p + 1} = p^4 + p^2 + p + 1$$

visto que $G_1(p)$ é factor de $p^7 + 1$, o resto desta divisão é zero.

O polinómio recíproco $H_1^*(p)$ torna-se gerador do código dual $(7,3)$, e é dado por $G_{1d}(p) = p^4 + p^3 + p^2 + 1$. Este polinómio gera o código dual correspondente ao código $(7,4)$ indicado acima.

Existe outro polinómio gerador para o código de Hamming $(7,4)$, dado por $G_2(p) = p^3 + p^2 + 1$, tal como indicado na Tabela 6. De facto, existem 24 possibilidades diferentes para estabelecer um código de Hamming $(7,4)$, tal como referido no apêndice D. Procedendo da mesma forma tal como no caso anterior obtemos

$$H_2(p) = \frac{p^7 + 1}{p^3 + p^2 + 1} = p^4 + p^3 + p^2 + 1$$

O polinómio recíproco $H_2^*(p)$ torna-se gerador do código dual $(7,3)$, e é dado por $G_{2d}(p) = p^4 + p^2 + p + 1$. Este polinómio gera o código dual correspondente ao código de Hamming gerado por $G_2(p)$.

2. Geração de um código linear de bloco (4,2)

Verifica-se o polinómio $G(p) = p^2 + 1$ é irredutível em $GF(2)$ e divide a expressão $p^4 + 1$ com resto zero, pelo que gera um código linear de bloco $(4,2)$. Efectuando a factorização de $p^4 + 1$ obtemos o polinómio de teste de paridade

$$H(p) = \frac{p^4 + 1}{p^2 + 1} = p^2 + 1$$

Neste caso temos duas coincidências que são as seguintes:

- o polinómio de teste de paridade coincide com o polinómio gerador;
- o recíproco do polinómio de teste de paridade é ele próprio;

A matriz G geradora deste código, na forma sistemática é dada por :

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

A matriz de controlo de paridade H correspondente será :

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

Verificamos que ambas as matrizes coincidem. Este é um caso particular em que o mesmo polinómio gera um código e o respectivo dual, também é um código (4,2). Significa isto que o código coincide com o seu próprio dual.

Conclusão:

Confrontando os resultados obtidos nestes dois exemplos podemos concluir que cada código (n,k) tem o respectivo código dual. Existem códigos que coincidem com os seus próprios duais e designam-se por códigos **auto-duais**.

A figura seguinte mostra a relação existente entre os polinómios geradores dos códigos duais e os polinómios de teste de paridade dos códigos que lhe dão origem, tomando como ponto de partida o código de Hamming referido acima que tem dois polinómios geradores diferentes.

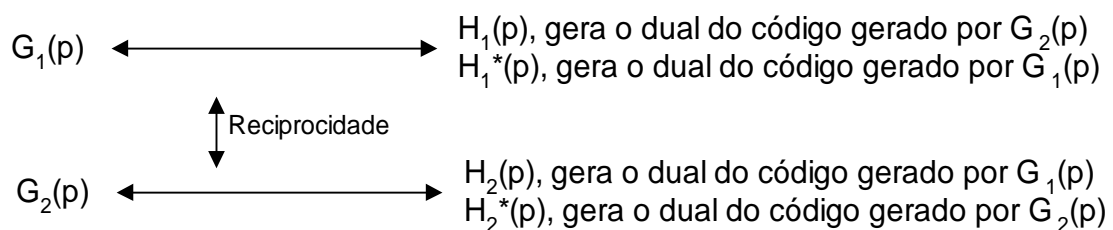


Figura 2 - Relação entre polinómios geradores e de teste de paridade.

6.6.4 Redução

A redução de um código cíclico tem a particularidade de que o código reduzido é obtido com o mesmo polinómio gerador do que o código original.

6.7 Códigos m-ários

Todos os resultados obtidos até ao momento foram feitos tendo como base coeficientes binários, pertencentes a um Campo de ordem 2. É possível extrapolar os resultados obtidos para códigos em que os coeficientes pertencem a Campos de ordem superior.

Exemplo:

Como exemplo da construção de um código cujos coeficientes não são binários, temos o código de bloco linear sistemático quaternário (5,3) de Hamming. A matrizes geradora e de controlo de paridade deste código são as seguintes

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 1 & 3 & 0 & 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \end{bmatrix}$$

O número de síndromas que este código possui é dado por $4^2 - 1 = 15$. O número total de padrões de erro de um símbolo é $3 \cdot 5 = 15$. Verifica-se que é um código perfeito para correcção de erros de um símbolo.

6.8 Critérios de desenho dos códigos BCH

Os códigos BCH são uma família de códigos cíclicos que obedecem a um conjunto de regras no seu desenho.

Tal como foi afirmado nas secções anteriores, quando se obtêm um polinómio primitivo para gerar um determinado código cíclico não existe nenhuma garantia que o código desenhado tem uma boa distância mínima, porque não é aplicada nenhuma regra que procure maximizar o peso das palavras do código.

O critério de desenho dos códigos BCH por sua vez assegura que se vai obter pelo menos uma dada distância mínima. Para conseguir este objectivo é necessário introduzir uma condicionante sobre o polinómio gerador. O parâmetro de construção do código que introduz esta condicionante designa-se por distância de desenho.

O valor mínimo para a distância mínima, designado por **limite BCH**, é dado pelos seguintes passos:

Premissas

- Seja C um código cíclico (n,k) com polinómios cujos coeficientes pertencem a um Campo de Galois de ordem q. O polinómio gerador do código é g(x). Seja m o menor inteiro positivo tal que GF(q^m) seja a menor extensão possível de GF(q) que contém uma raiz de ordem n primitiva da unidade, designada por α.

Execução

- Escolhe-se g(x) um polinómio de grau mínimo em GF(q)[x], tal que se verifique a seguinte igualdade:

$$g(\alpha^b) = g(\alpha^{b+1}) = g(\alpha^{b+2}) = \dots = g(\alpha^{b+\delta-2}) = 0, \text{ para os valores inteiros } b \geq 0 \text{ e } \delta \geq 1.$$

Este polinómio g(x) tem como zeros (δ-1) potências consecutivas de α.

Conclusão

O código gerado por g(x) tem uma distância mínima igual ou superior a δ.

O parâmetro δ designa-se por **distância de desenho** definida pelo polinómio gerador $g(x)$.

6.8.1 Algoritmo de construção

O algoritmo de desenho de um código BCH que corrige até t erros é o seguinte:

1. Encontrar uma raiz α de ordem n primitiva da unidade em $GF(q^m)$, onde m é o menor inteiro positivo que efectuar a menor extensão possível de $GF(q)$.
2. Escolher $(\delta-1) = 2t$ potências consecutivas de α , partindo de α^b , com $b \geq 0$.
3. Seja $g(x)$ o menor múltiplo comum dos polinómios mínimos para as potências escolhidas de α em relação a $GF(q)$. Cada polinómio mínimo deve aparecer apenas uma vez no produto.

O primeiro passo do algoritmo segue o processo de desenho genérico definido para os códigos cíclicos. Os passos dois e três garantem o valor do limite BCH, maximizando a distância mínima do código com o menor grau possível para o polinómio gerador, ou seja, com o número mínimo de *bits* de redundância para tentar maximizar a eficiência.

Exemplo:

Existem bastantes códigos BCH com diferentes dimensões de mensagem e de palavras de código que podem ser encontrados em [1]. Ficam aqui alguns exemplos.

- (7,4) ; (15,11) ; (15,7) ; (15,5) ; (31,26) ; (63,57) ; (127,120) ;

6.9 Códigos Reed-Solomon

Existem várias formas de descrever um código Reed-Solomon, uma das quais pode ser a extensão dos códigos BCH. A definição deste código é a seguinte :

“Um código Reed-Solomon é um código BCH q^m -ario com comprimento q^m-1 “

6.9.1 Construção das palavras do código

Como se trata de um código cíclico com características bem determinadas, o seu processo de desenho começa por determinar o polinómio gerador sobre um $GF(q^m)$. A construção das palavras de um código Reed-Solomon, de comprimento q^m-1 com capacidade de correção de t erros é seguinte :

- 1 - Procurar em $GF(q^m)$ a raiz primitiva da unidade de ordem (q^m-1) , designada por α .
- 2 - Encontrar as classes de elementos conjugados módulo (q^m-1) , através da expressão $(s \cdot q^m)$, que pode ser simplificada na forma s módulo (q^m-1) . Temos então conjuntos com um elemento $\{s\}$ e os respectivos polinómios mínimos associados são da forma $(x-\alpha^s)$.

3 - Pelo limite BCH temos $2t$ potências consecutivas de α como zeros do polinómio gerador $g(x)$, para uma capacidade de correcção de t erros. O polinómio gerador $g(x)$ é constituído pelo produto de polinómios mínimos associados:

$$g(x) = (x-\alpha^b).(x-\alpha^{b+1}).(x-\alpha^{b+2}) \dots (x-\alpha^{b+2t-1})$$

Consegue-se provar que um código Reed-Solomon tem uma distância mínima dada por $n-k+1$ ou de outra forma $q+1$. Este é o máximo valor possível para a distância mínima, designado por limite de Singleton. Códigos nestas condições são designados por **maximum-distance separable (MDS)** [1].

Exemplo:

Construção de um código Reed-Solomon 8-ário com palavras de comprimento 7 e capacidade de correcção de $t=2$ erros.

Dado o polinómio primitivo $g(x) = x^3 + x + 1$ em $GF(2)$, podemos construir $GF(8)$ tal como apresentado na secção 6.6.1 onde ficou descrita a sua construção, tal como apresentada na tabela seguinte :

Representação exponencial	Representação polinomial
α^0	1
α	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$
α^7	1

Tabela 7 - Representação de $GF(8)$.

Pelo limite BCH, se pretendermos um código com capacidade de correcção de $t=2$ erros, é necessário termos as primeiras $2t=4$ potências consecutivas de α , para a construção do polinómio gerador. Desta forma ficamos com o seguinte polinómio :

$$\begin{aligned} g(x) &= (x-\alpha).(x-\alpha^2).(x-\alpha^3).(x-\alpha^4) \\ &= x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 \end{aligned}$$

Temos um polinómio gerador para um código $(7,3)$, que tem $8^3=512$ palavras. Tanto os códigos BCH como Reed-Solomon podem ter as suas dimensões alteradas[1] tal como referido na secção anterior para o caso dos códigos cíclicos em geral.

7. Bibliografia e referências

- [1] Error Control Coding for Digital Communication and Storage, Stephen B. Wicker, Prentice Hall, 1995.
- [2] Abstract Algebra, David S. Dummit, Richard M. Foote, Prentice Hall, 1991.
- [3] Communication Systems, A. Bruce Carlson, McGraw-Hill, 1986.
- [4] Communication Systems, Symon Haykin, John Wiley & Sons, 1994.
- [5] Algebra Linear, Luís Magalhães, Texto Editora, 1997.

Apêndice A

Geração de um espaço vectorial

Propriedades da relação entre conjuntos de vectores e campos de escalares.

Neste Apêndice apresentam-se as propriedades que um conjunto de vectores e um campo de escalares devem apresentar de forma a que o conjunto de vectores possa ser classificado como Espaço Vectorial sobre o conjunto de escalares. A introdução destas propriedades em Apêndice visa complementar o texto apresentado.

Seja V um conjunto não vazio constituído por vectores, e F um conjunto de escalares. Existem duas operações definidas sobre os elementos de V , que são a adição de vectores e multiplicação por escalares, respectivamente “+” e “.”, definidas da seguinte forma :

i) Soma de dois vectores: $u + v = (u_0+v_0, u_1+v_1, \dots, u_n+v_n)$;

ii) Multiplicação por um escalar: $\alpha.u = (\alpha u_0, \alpha.u_1, \dots, \alpha.u_n)$;

Para que V seja um espaço vectorial sobre F têm que se verificar as seguintes propriedades :

- $(V,+)$ é um grupo comutativo;
- Para qualquer escalar $a \in F$ e para qualquer vector $v \in V$, verifica-se que $a.v = u \in V$;
- As operações “.” e “+” são distributivas :

$$a.(u + v) = au + a.v, (a + b).v = a.v + b.v \forall a, \forall b \in F, \forall u, \forall v \in V$$
- A operação “.” é associativa :

$$(a.b).v = a.(b.v), \forall a, \forall b \in F, \forall v \in V$$
- O elemento identidade do campo F , funciona como elemento identidade na multiplicação por um vector $v \in V$;

Apêndice B

Domínios Euclidianos

Um Domínio Euclidiano é um conjunto D com duas operações binárias “+” e “.”, que satisfazem as seguintes condições:

$(D, “+”, “.”)$ é um anel comutativo aditivo com identidade.

Propriedade do cancelamento: $a.b = b.c$, $b \neq 0$, então $a=c$.

Cada elemento $a \in D$ tem uma métrica $g(a)$, tal que:

$g(a) \leq g(a.b)$, para todos os elementos $b \neq 0$, com $b \in D$.

para todos os elementos $a \neq 0$, $b \neq 0$, com $a, b \in D$, $g(a) > g(b)$, então existem valores q e r tal que $a = q.b + r$ com $r=0$ ou $g(r) < g(b)$. O valor q é o quociente e o valor r é o resto.

Algoritmo de Euclides no cálculo de GCD(a,b)

O algoritmo de Euclides implementa uma forma rápida de cálculo do máximo divisor comum entre dois elementos quaisquer que pertencem a um Domínio Euclidiano.

1. Sejam a e b dois elementos que pertencem a um Domínio Euclidiano D , tal que $g(a) > g(b)$.
2. Consideram-se as variáveis r_{-1} e r_0 . Faz-se $r_{-1} = a$ e $r_0 = b$.
3. Proceder de forma recursiva :
Se $r_{-1} \neq 0$, então $r_i = r_{i-2} - q_i.r_{i-1}$, com $g(r_i) < g(r_{i-1})$. Repetir o processamento até $r_i = 0$. No final, o valor em r_0 é o GCD(a,b).

Nota:

Quando se calcula o GCD(a,b) com a e b dois números inteiros, a métrica associada ao número poderá ser o próprio número.

Apêndice C

Algoritmo estendido de Euclides

Tal como o próprio nome indica, este algoritmo representa uma extensão do anterior. Para além de encontrar o máximo divisor comum (GCD) entre dois elementos, obtém ainda os coeficientes da combinação linear formada por ambos, que origina também o GCD.

1. Pretende-se encontrar dois valores s e t , tal que $\text{GCD}(a,b) = s.a + t.b$. É necessário considerar um conjunto de variáveis $\{r_i, s_i, t_i\}$ tal que :

$$r_{-1} = a \quad r_0 = b$$

$$s_{-1} = 1 \quad s_0 = 0$$

$$t_{-1} = 0 \quad t_0 = 1$$

2. Se $r_{i-1} \neq 0$, então faz-se $q_i = r_{i-2} / r_{i-1}$, $r_i = r_{i-2} - q_i \cdot r_{i-1}$, $g(r_i) < g(r_{i-1})$

3. Fazer $s_i = s_{i-2} - q_i \cdot r_{i-1}$, com q_i tendo o valor do passo anterior.

4. Fazer $t_i = t_{i-2} - q_i \cdot t_{i-1}$, com q_i tendo o valor do passo anterior.

5. Repetir os passos 2 a 4 inclusivé, até obter $r_i=0$. Nesta altura tem-se a combinação linear pretendida:

$$r_{i-1} = \text{GCD}(a, b) = a \cdot s_{i-1} + b \cdot t_{i-1}$$

Apêndice D

Código de Hamming (7,4) e respectivo dual (7,3)

Neste anexo exemplifica-se uma matriz geradora de um código de Hamming(7,4) e respectiva matriz de teste de paridade. Analisa-se também o correspondente código dual e suas matrizes. Note-se que existem 24 possibilidades de estabelecer códigos de Hamming(7,4) diferentes, que correspondem ao número de combinações possíveis das quatro linhas da submatriz geradora de paridade designada por P. O número de combinações é dado por $4! = 24$.

Código de Hamming(7,4)

Matriz geradora

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

Matriz de teste de paridade

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

Código dual (7,3)

Matriz geradora

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

Matriz de teste de paridade

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

Se analisarmos as matrizes geradoras como base de um sub-espaço vectorial verificamos que temos para o primeiro caso temos um espaço de dimensão de 4, e no segundo temos dimensão 3. Pelo Teorema da Dimensão podemos obter a dimensão do espaço vectorial composto por ambos.

$$\dim(V) = \dim(S) + \dim(S^\perp) = 4 + 3 = 7$$

Apêndice E

Código de Hamming (7,4) original não sistemático

Message	Check	Weigth
0 0 0 0	0 0 0	0
1 0 0 1	1 1 0	4
1 0 1 0	0 1 0	3
0 0 1 1	1 0 0	3
1 1 0 0	1 0 0	3
0 1 0 1	0 1 0	3
0 1 1 0	1 1 0	4
1 1 1 1	0 0 0	4
0 0 0 0	1 1 1	3
1 0 0 1	0 0 1	3
1 0 1 0	1 0 1	4
0 0 1 1	0 1 1	4
1 1 0 0	0 1 1	4
0 1 0 1	1 0 1	4
0 1 1 0	0 0 1	3
1 1 1 1	1 1 1	7

Matriz geradora

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

Matriz de teste de paridade

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

As palavras estão organizadas na forma $X = [c_1 \ c_2 \ m_1 \ c_3 \ m_2 \ m_3 \ m_4]$.

As equações dos *bits* de paridade são as seguintes :

$$\begin{cases} c_1 = m_1 \oplus m_2 \oplus m_4 \\ c_2 = m_1 \oplus m_3 \oplus m_4 \\ c_3 = m_2 \oplus m_3 \oplus m_4 \end{cases}$$

Matriz de teste de paridade transposta

$$H^T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Tabela de síndromas

S_1	S_2	S_3	E_1	E_2	E_3	E_4	E_5	E_6	E_7
0	0	0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0	0	0
0	1	0	0	1	0	0	0	0	0
0	1	1	0	0	1	0	0	0	0
1	0	0	0	0	0	1	0	0	0
1	0	1	0	0	0	0	1	0	0
1	1	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	1

Apêndice F

Códigos lineares de bloco (7,4) obtidos por dois polinómios geradores diferentes.

Código de bloco linear **sistemático cíclico** Hamming(7,4). $G(p) = p^3 + p + 1$

Message	Check	Weigth
0 0 0 0	0 0 0	0
0 0 0 1	0 1 1	3
0 0 1 0	1 1 0	3
0 0 1 1	1 0 1	4
0 1 0 0	1 1 1	4
0 1 0 1	1 0 0	3
0 1 1 0	0 0 1	3
0 1 1 1	0 1 0	4
1 0 0 0	1 0 1	3
1 0 0 1	1 1 0	4
1 0 1 0	0 1 1	4
1 0 1 1	0 0 0	3
1 1 0 0	0 1 0	3
1 1 0 1	0 0 1	4
1 1 1 0	1 0 0	4
1 1 1 1	1 1 1	7

Código de bloco linear **sistemático cíclico** (7,4). $G(p) = p^3 + p^2 + 1$.

Message	Check	Weigth
0 0 0 0	0 0 0	0
0 0 0 1	1 0 1	3
0 0 1 0	1 1 1	4
0 0 1 1	0 1 0	3
0 1 0 0	0 1 1	3
0 1 0 1	1 1 0	4
0 1 1 0	1 0 0	3
0 1 1 1	0 0 1	4
1 0 0 0	1 1 0	3
1 0 0 1	0 1 1	4
1 0 1 0	0 0 1	3
1 0 1 1	1 0 0	4
1 1 0 0	1 0 1	4
1 1 0 1	0 0 0	3
1 1 1 0	0 1 0	4
1 1 1 1	1 1 1	7