MAC0317/MAC5920

Introdução ao Processamento de Sinais Digitais

Seção 1.8: Espaços com produto interno e Ortogonalidade

Objetivo dessa seção: formalizar as ferramentas matemáticas necessárias à construção das transformadas de sinais (Fourier, Cosseno, Wavelets)

Definição 1.8.1 (produto interno):

Um *produto interno* sobre um espaço vetorial V é uma função $(\cdot, \cdot)$ de $V \times V$ em $\mathbb{C}$ (ou $\mathbb{R}$) que satisfaz as propriedades abaixo $\forall u, v, w \in V$ e $\forall \alpha, \beta \in \mathbb{C}$ (ou $\mathbb{R}$):

1. $(v, w) = \overline{(w, v)}$ (simetria conjugada)
2. $(\alpha u + \beta v, w) = \alpha(u, w) + \beta(v, w)$ (linearidade no 1° argumento)
3. $(v, v) \geq 0$ e $(v, v) = 0 \iff v = 0$

No caso de espaços vetoriais sobre $\mathbb{R}$ a conjugação complexa não tem efeito, e a condição (1) acima fica simplesmente:

1. $(v, w) = (w, v)$ (simetria)

A condição (3) faz sentido, mesmo em espaços vetoriais sobre $\mathbb{C}$, pois $(v, v) = \overline{(v, v)}$ da condição (1) implica em $(v, v) \in \mathbb{R}$ ($x = \bar{x} \implies \mathfrak{I}(x) = -\mathfrak{I}(x) \implies \mathfrak{I}(x) = 0$).

A linearidade no 1° argumento se estende facilmente para qualquer quantidade finita de termos: basta aplicar repetidamente a propriedade.

Linearidade(s) do produto interno:

A condição

1. $(\alpha u + \beta v, w) = \alpha(u, w) + \beta(v, w)$

se estende facilmente para combinações lineares finitas no primeiro argumento:

$$\left(\sum_{k=0}^{K} \alpha_k u_k, v\right) = \alpha_0(u_0, v) + \left(\sum_{k=1}^{K} \alpha_k u_k, v\right) = \cdots = \sum_{k=0}^{K} \alpha_k (u_k, v)$$

Em relação ao segundo argumento, a propriedade de simetria conjugada implica numa "linearidade conjugada":

$$(w, \alpha u + \beta v) = \overline{(\alpha u + \beta v, w)} = \overline{\alpha(u, w) + \beta(v, w)} = \overline{\alpha(u, w)} + \overline{\beta(v, w)} = \overline{\alpha}(w, u) + \overline{\beta}(w, v)$$

Definição 1.8.2 (norma):

Uma *norma* em um espaço vetorial V é uma função $\|\cdot\|$ de V em $\mathbb{R}$ que satisfaz as propriedades abaixo $\forall v, w \in V$ e $\forall \alpha \in \mathbb{C}$ (ou $\mathbb{R}$):

1. $\|v\| \geq 0$ e $\|v\| = 0 \iff v = 0$
2. $\|\alpha v\| = |\alpha| \|v\|$
3. $\|v + w\| \leq \|v\| + \|w\|$

(Exercício 1.27) Todo produto interno $(\cdot, \cdot)$ sobre V induz uma norma correspondente através da relação:

$$\|v\| = \sqrt{(v, v)}$$

Não se confunda: existem normas definidas diretamente a partir das 3 condições acima mas que não correspondem a nenhum produto interno. Por exemplo, $\|v\|_\infty = \max |v_i|$ e $\|v\|_1 = \sum |v_i|$ satisfazem a definição acima mas não correspondem a nenhum produto interno.

Interpretação de energia em sinais

Frequentemente usamos o valor $\|v\|^2$ como uma medida de energia do sinal. Isso tem origem em analogias com modelos físicos (energia cinética $\propto v^2$, energia potencial $\propto x^2$, energia elétrica dissipada $\propto V^2$).

Em sinais, essa medida de energia tem algumas propriedades importantes, dentre as quais a **Equação de Parseval**, que estabelece que a energia de um sinal equivale à soma das energias de suas componentes (senoidais, exponenciais).

Distância induzida por uma norma

As propriedades que caracterizam distâncias em geral são $\forall u, v, w$

1. $d(v,w) \geq 0$ e $d(v,w) = 0 \iff v = w$
2. $d(v,w) = d(w,v)$
3. $d(v,w) \leq d(v,u) + d(u,w)$

A partir de uma norma qualquer $\|\cdot\|$ pode-se definir uma distância induzida por

$$d(v,w) = \|v - w\|$$

Exemplos de espaços com produtos internos e normas correspondentes

Exemplo 1.12

Em $\mathbb{R}^N$ o produto interno mais comum (canônico) é

$$(x, y) = \sum_{i=0}^{N-1} x_i y_i = x_0 y_0 + x_1 y_1 + \cdots + x_{N-1} y_{N-1}$$

A norma correspondente é

$$\|x\| = \left(\sum_{i=0}^{N-1} x_i x_i \right)^{\frac{1}{2}} = \left(x_0^2 + x_1^2 + \cdots + x_{N-1}^2 \right)^{\frac{1}{2}}$$

e é chamada de *Norma Euclideana*.

Exemplo 1.13

Em $\mathbb{C}^N$ o produto interno canônico é

$$(x, y) = \sum_{i=0}^{N-1} x_i \overline{y_i} = x_0 \overline{y_0} + x_1 \overline{y_1} + \cdots + x_{N-1} \overline{y_{N-1}}$$

cuja norma correspondente é

$$\|x\| = \left(\sum_{i=0}^{N-1} x_i \overline{x_i} \right)^{\frac{1}{2}} = \left(|x_0|^2 + |x_1|^2 + \cdots + |x_{N-1}|^2 \right)^{\frac{1}{2}}$$

Atenção: tanto as conjugações complexas quanto os valores absolutos nas equações acima são importantes! Note que para qualquer $z \in \mathbb{C}$, considerando sua representação polar $z = Ae^{i\varphi}$ (onde $A = |z|$ e $\varphi = \measuredangle z$) temos
$z\overline{z} = Ae^{i\varphi}\overline{Ae^{i\varphi}} = Ae^{i\varphi}Ae^{-i\varphi} = A^2e^0 = |z|^2$.

Verificação:

1. $\overline{(x, y)} = \overline{\sum_{i=0}^{N-1} x_i \overline{y_i}} = \sum_{i=0}^{N-1} \overline{x_i \overline{y_i}} = \sum_{i=0}^{N-1} \overline{x_i} y_i = (y, x)$
2. $(\alpha x + \beta y, z) = \sum_{i=0}^{N-1} (\alpha x_i + \beta y_i) \overline{z_i} = \alpha \sum_{i=0}^{N-1} x_i \overline{z_i} + \beta \sum_{i=0}^{N-1} y_i \overline{z_i}$

   $= \alpha(x, z) + \beta(y, z)$
3. $(x, x) = \sum_{i=0}^{N-1} x_i \overline{x_i} = \sum_{i=0}^{N-1} |x_i|^2 \geq 0$

   e $(x, x) = 0 \iff |x_i|^2 = 0 \forall i \iff x = 0$

Exemplo 1.14

Em $\mathcal{M}_{M,N}(\mathbb{C}) = \mathbb{C}^{M\times N}$ o produto interno canônico é

$$(A, B) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} A_{ij}\overline{B_{ij}}$$

cuja norma correspondente, conhecida como *Norma de Frobenius* é

$$\|A\| = \left(\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |A_{ij}|^2 \right)^{\frac{1}{2}}$$

O espaço $\mathbb{C}^{M\times N}$ é essencialmente o mesmo que $\mathbb{C}^{MN}$ (serialização de linhas ou colunas).

Observação: pulamos os exemplos 1.15 a 1.17.

Ortogonalidade

Da geometria elementar em 2D ou 3D sabemos que

$$(v, w) = \|v\| \|w\| \cos(\theta)$$

onde θ é o ângulo formado entre os vetores v e w. Daí segue que se $v, w \neq 0$ então

$$v \perp w \iff \theta = \frac{\pi}{2} \iff \cos(\theta) = 0 \iff (v, w) = 0.$$

Isso motiva a

Definição 1.8.3

Num espaço vetorial com produto interno, dizemos que $v \neq 0$ e $w \neq 0$ são *ortogonais* ($v \perp w$) se $(v, w) = 0$.

Um subconjunto $S \subseteq V$ é *ortogonal por pares* (ou simplesmente *ortogonal*) se $v \perp w, \ \forall v, w \in S \backslash \{0\}$.

Exemplo 1.18

Seja $S = \{e_i | i = 0, \dots, N-1\} \subset \mathbb{R}^N$ onde

$$e_i = (0, \dots, 0, \overbrace{1}^{ind=i}, 0, \dots, 0) \quad \text{ou equivalentemente} \quad (e_i)_j = 0 \iff i = j.$$

Então S é ortogonal, pois se $i \neq j$

$$(e_i, e_j) = \sum_{k=0}^{N-1} (e_i)_k (e_j)_k = 0,$$

já que não podem valer $i = k$ e $j = k$ ao mesmo tempo.

Exemplo 1.18 (cont.)

O mesmo conjunto $S = \{e_i | i = 0, \dots, N-1\}$ visto como subconjunto de $\mathbb{C}^N$ também é ortogonal, pois se $i \neq j$:

$$(e_i, e_j) = \sum_{k=0}^{N-1} (e_i)_k \overline{(e_j)_k} = \sum_{k=0}^{N-1} (e_i)_k (e_j)_k = 0,$$

onde a penúltima igualadade vale porque $(e_j)_k \in \{0, 1\}$.

Observação: pulamos o exemplo 1.19

Exemplo 1.20

Seja $S = \{E_k | k = 0, \dots, N-1\}$ como definidos anteriormente, onde

$$(E_k)_n = e^{i2\pi k \frac{n}{N}}.$$

Então S é ortogonal:

$$(E_k, E_l) = \sum_{n=0}^{N-1} e^{i2\pi k \frac{n}{N}} \overline{e^{i2\pi l \frac{n}{N}}} = \sum_{n=0}^{N-1} e^{i2\pi k \frac{n}{N}} e^{-i2\pi l \frac{n}{N}} = \sum_{n=0}^{N-1} e^{i2\pi (k-l) \frac{n}{N}} =$$

$$\sum_{n=0}^{N-1} \left(e^{i2\pi (k-l) \frac{1}{N}} \right)^n = \cdots$$

A última equação pode ser desenvolvida lembrando da equação de soma dos termos de uma Progressão Geométrica:

$$X = 1 + z + z^2 + \cdots + z^{N-1} \implies X = 1 + zX - z^N \implies X = \frac{1 - z^N}{1 - z},$$

Substituindo $z = e^{i2\pi(k-l)\frac{1}{N}}$ em

$$(E_k, E_l) = \sum_{n=0}^{N-1} \left(e^{i2\pi(k-l)\frac{1}{N}} \right)^n$$

e usando $z \neq 1$ (pois $0 \leq k, l < N$ e $k \neq l$) temos

$$(E_k, E_l) = \frac{1 - \left(e^{i2\pi(k-l)\frac{1}{N}} \right)^N}{1 - e^{i2\pi(k-l)\frac{1}{N}}} = \frac{1 - e^{i2\pi(k-l)}}{1 - e^{i2\pi(k-l)\frac{1}{N}}} = 0$$

(a última equação segue de $e^{i2\pi(k-l)\frac{1}{N}} = 1$).

Comentário 1.10: Usando essencialmente o mesmo argumento pode-se provar que a mesma ortogonalidade vale entre as matrizes básicas $E_{k,l}$, ou seja, dados k, l, r, s com $k \neq r$ ou $l \neq s$, então $(E_{k,l}, E_{r,s}) = 0$ usando o produto interno do Exemplo 1.14.

Teorema 1.8.1 (Desigualdade de Cauchy-Schwarz)

Dados v e w em um espaço vetorial V, temos

$$|(v, w)| \leq \|v\|\|w\|,$$

onde a norma do lado direito é aquela induzida pelo produto interno do lado esquerdo.

Prova do teorema 1.8.1

Essencialmente ela parte da observação de que a *distância* entre um vetor v e sua projeção ortogonal cw sobre w (aqui c é um escalar) é sempre ≥ 0, ou equivalentemente, $\|v - cw\|^2 \geq 0$. Note que

$$\begin{aligned} \|v - cw\|^2 &= (v - cw, v - cw) = (v, v) - c(w, v) - \bar{c}(v, w) + c\bar{c}(w, w) \\ &= \|v\|^2 + |c|^2\|w\|^2 - (c\overline{(v, w)} + \bar{c}(v, w)). \end{aligned}$$

Agora, pela propriedade da projeção ortogonal, $(v - cw, w) = 0$, ou seja, $c = \frac{(v,w)}{\|w\|^2}$.

Substituindo este c na equação anterior,

$$\begin{aligned} \|v\|^2 &+ \frac{|(v,w)|^2}{\|w\|^4}\|w\|^2 - \left(\frac{(v,w)}{\|w\|^2}(w, v) + \frac{\overline{(v,w)}}{\|w\|^2}(v, w)\right) \\ &= \|v\|^2 + \frac{|(v,w)|^2}{\|w\|^2} - 2\frac{|(v,w)|^2}{\|w\|^2} \\ &= \|v\|^2 - \frac{|(v,w)|^2}{\|w\|^2} \geq 0, \end{aligned}$$

de onde sai a equação de Cauchy-Schwarz $|(v, w)| \leq \|v\|\|w\|$.

Bases

Vimos no Exemplo 1.18 como o conjunto $S = \{e_i | i = 0, \dots, N-1\}$ onde

$$e_i = (0, \dots, 0, \overbrace{1}^{ind=i}, 0, \dots, 0) \quad \text{ou equivalentemente} \quad (e_i)_j = 0 \iff i = j$$

era ortogonal. Esse conjunto é chamado de base canônica e serve tanto para $\mathbb{R}^N$ quanto $\mathbb{C}^N$, pois qualquer vetor $x = (x_0, x_1, \dots, x_{N-1})$ de um desses espaços pode ser escrito como combinação linear dos elementos de S, mais especificamente,

$$x = \sum_{i=0}^{N-1} x_i e_i.$$

Assim S é um conjunto que permite a construção de qualquer elemento de $\mathbb{R}^N$ ou $\mathbb{C}^N$ como combinações lineares de S, e é minimal pois nenhum conjunto com menos de N vetores tem essa propriedade.

Definição 1.8.4 (conjunto gerador)

Dizemos que um subconjunto $S \subset V$ (finito ou infinito) em um espaço vetorial V é um *conjunto gerador* de V se qualquer $x \in V$ pode ser representado como uma combinação linear finita de elementos de S, ou seja, se existem $K \in \mathbb{N}$, escalares $a_i,\ i = 0, \ldots, K-1$ e vetores $v_i \in S,\ i = 0, \ldots, K-1$ tais que

$$x = \sum_{i=0}^{K-1} a_i v_i.$$

Definição 1.8.5 (conjunto linearmente independente)

Dizemos que um subconjunto $S \subset V$ (finito ou infinito) em um espaço vetorial V é um *conjunto linearmente independente* se para qualquer subconjunto finito $\{v_i,\ i = 0, \dots, K-1\} \subseteq S$, a única solução do sistema homogêneo

$$\sum_{i=0}^{K-1} a_i v_i = 0$$

é a solução trivial $a_0 = a_1 = \cdots = a_{K-1} = 0$.

Definição 1.8.6 (base)

Dizemos que um subconjunto $S \subset V$ (finito ou infinito) é uma *base* de V se S é um conjunto gerador e linearmente independente.

Observação: ainda que S possa ter infinitos elementos, a definição acima exige que todos os elementos de V possam ser representados como combinações lineares *finitas*, ou seja, usando subconjuntos finitos de S. O nome técnico para isso é *Base de Hamel*, e exclui por exemplos conjuntos como a extensão da base canônica para sinais infinitos ou bi-infinitos ($e_i = (\dots, 0, 1, 0, \dots)$), que demandariam combinações lineares infinitas (séries).

Exemplo 1.21

No espaço $\mathcal{M}_{m,n}(\mathbb{C}) = \mathbb{C}^{m\times n}$ de matrizes complexas $m \times n$, considere as mn matrizes $A_{i,j}$ definidas por

$$\left(A_{p,q}\right)_{i,j} = 1 \text{ se } p, q = i, j, \text{ e } 0 \text{ caso contrário.}$$

Então o conjunto $S = \{A_{p,q} \mid 0 \le p \le m-1,\ 0 \le q \le n-1\}$ forma uma base de $\mathcal{M}_{m,n}$, já que qualquer matriz $X \in \mathcal{M}_{m,n}$ satisfaz

$$X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} A_{i,j}.$$

Exemplo 1.22

Seja P o conjunto de todas os polinômios de grau n, ou seja, funções da forma

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Então P é um espaço vetorial (usando a soma de polinômios e o produto por escalar usuais -- fica como exercício) e o conjunto infinito

$$S = \{1, x, \ldots, x^n, \ldots\}$$

é uma base para P. De fato S gera P por construção, e o conjunto S é linearmente independente, pois a única maneira de uma equação da forma

$$a_0 + a_1 x + \cdots + a_n x^n = 0,\ \forall x$$

valer é quando $a_i = 0,\ \forall i$.

Base e dimensão

Se S é uma base finita para V, o tamanho $N = |S|$ de S é denominado **dimensão** de V, e é possível provar que qualquer outra base de V precisa possuir exatamente N elementos. Mais ainda, em um espaço N dimensional, qualquer conjunto de N vetores linearmente independentes é necessariamente uma base.

Pelos exemplos acima podemos estabelecer que tanto $\mathbb{R}^N$ quanto $\mathbb{C}^N$ são espaços N-dimensionais, e que tanto $\mathcal{M}_{m,n}(\mathbb{R})$ quanto $\mathcal{M}_{m,n}(\mathbb{C})$ são espaços mn-dimensionais. Por outro lado, o espaço P dos polinômios possui dimensão infinita.

Não se confunda: apesar de representarmos o conjunto $\mathbb{C}$ dos complexos em um plano, como espaço vetorial $\mathbb{C}$ tem dimensão 1, pois qualquer elemento de $\mathbb{C}$ pode ser escrito como $\alpha \cdot (1)$, onde $\alpha \in \mathbb{C}$; pela mesma razão, os N elementos da base canônica de $\mathbb{C}^N$ são suficientes para produzir qualquer vetor com N componentes complexas, pois os *escalares* nesse caso são eles próprios complexos, e então a dimensão de $\mathbb{C}^N$ é de fato N (e não $2N$).

Bases ortogonais e ortonormais

Em um espaço N dimensional, qualquer conjunto ortogonal de N vetores não-nulos é necessariamente uma base. Isso decorre do seguinte fato:

Teorema 1.8.2: Se $\mathcal{S} \subset \mathcal{V} \backslash \{\mathbf{0}\}$ é ortogonal, então $\mathcal{S}$ é linearmente independente.

Prova: seja $\{v_0, v_1, \ldots, v_{N-1}\} \subset S$ com $v_i \neq 0,\ \forall i$ e $(v_i, v_j) = 0,\ \forall v_i, v_j \in S,\ i \neq j$; então o sistema $\displaystyle\sum_{i=0}^{K-1} a_i v_i = 0$ pode ser resolvido fazendo produtos internos com cada v_j:

$$\left(\sum_{i=0}^{K-1} a_i v_i, v_j\right) = \sum_{i=0}^{K-1} a_i (v_i, v_j) = a_j (v_j, v_j) = 0,$$

onde o somatório desaparece porque $(v_i, v_j) = 0$ para todo $i \neq j$. Pela última equação, como $(v_j, v_j) = \|v_j\|^2 \neq 0$ segue que $a_j = 0$ (esse argumento vale $\forall j$).

Mudanças de representação para bases ortogonais

Se S é uma base qualquer para V, temos uma garantia de que é possível representar qualquer $x \in V$ como $x = \sum_{i=0}^{N-1} a_i v_i$ (Eq. I). Uma pergunta razoável é: "como encontrar os a_i's?". Um solução muito simples existe quando S é uma base ortogonal:

Teorema 1.8.3: Se $\boldsymbol{S = \{v_0, v_1, \ldots, v_{N-1}\}}$ é uma base ortogonal para $\boldsymbol{V}$, então qualquer $\boldsymbol{x \in V}$ pode ser escrito como $\boldsymbol{x = \sum_{i=0}^{N-1} a_i v_i}$ onde $\boldsymbol{a_j = \frac{(x, v_j)}{(v_j, v_j)}}$.

Prova: podemos proceder outra vez por eliminação, fazendo produtos internos da Eq. I com cada v_j:

$$(x, v_j) = \left(\sum_{i=0}^{N-1} a_i v_i, v_j \right) = \sum_{i=0}^{N-1} a_i (v_i, v_j) = a_j (v_j, v_j),$$

de onde segue que

Bases ortonormais

Definição 1.8.7: Um conjunto ortogonal S é dito ortonormal se $\|v\| = 1, \ \forall v \in S$.

Observação 1.11: É sempre possível normalizar um conjunto ortogonal S para obter um conjunto ortonormal S' substituindo cada $v \in S$ por

$$v' = \frac{v}{\|v\|}.$$

Isso garante que $\|v'\| = \left\| \frac{v}{\|v\|} \right\| = \frac{\|v\|}{\|v\|} = 1.$

No caso de uma base ortonormal S, os coeficientes a_i da representação de $x = \sum_{i=0}^{N-1} a_i v_i$ podem ser obtidos como

$$a_i = (x, v_k).$$

Exemplo 1.23

Considere o conjunto $S = \{E_k | k = 0, \dots, N-1\} \subset \mathbb{C}^N$. No Exemplo 1.20 vimos que eles são ortogonais, logo linearmente independentes, e como $|S| = N$, segue que S é uma base de $\mathbb{C}^N$. Pelo teorema 1.8.3, segue que qualquer $x \in \mathbb{C}^N$ pode ser escrito como $x = \sum_{k=0}^{N-1} a_k E_k$ com $a_k = (x, E_k)/(E_k, E_k) = (x, E_k)/N$ (pois $(E_k, E_k) = N$, veja o Exercício 1.30). Isso mostra que qualquer $x \in \mathbb{C}^N$ pode ser escrito como:

$$x = \frac{1}{N} \sum_{k=0}^{N-1} (x, E_k) E_k.$$

Essa equação é a conhecida *Transformada de Fourier*, que será estudada em profundidade nos capítulos 2 e 3.

Exemplo 1.24

Usando exatamente o mesmo argumento do exemplo anterior, verificamos que qualquer matriz $A \in \mathcal{M}_{m,n}(\mathbb{C})$ pode ser escrita como

$$A = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} \frac{(A, E_{k,l})}{(E_{k,l}, E_{k,l})} E_{k,l} = \frac{1}{mn} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} (A, E_{k,l}) E_{k,l},$$

onde usamos o fato de que $(E_{k,l}, E_{k,l}) = mn$ (Exercício 1.31).

Identidade de Parseval

Quando $S = \{v_0, v_1, \ldots, v_{N-1}\}$ é uma base ortonormal para V (ou seja, $\|v_j\| = 1,\ \forall j$, temos que qualquer $x \in V$ pode ser escrito como $x = \sum_j a_j v_j$ e além disso

$$\begin{aligned} \|x\|^2 &= (x, x) = \left(\sum_j a_j v_j, \sum_k a_k v_k\right) \\ &= \sum_j \sum_k a_j \overline{a_k} (v_j, v_k) = \sum_j a_j \overline{a_j} = \sum_j |a_j|^2, \end{aligned}$$

onde a penúltima equação segue do fato que $(v_j, v_k) = 0$ se $j \neq k$ e $(v_j, v_j) = 1$. Essa é a *Identidade de Parseval*, que estabelece que se a_j são os coeficientes de x em uma base ortonormal qualquer, então

$$\|x\|^2 = \sum_j |x_j|^2 = \sum_j |a_j|^2,$$

mostrando que o conceito de *energia* associado à quantidade $\|x\|^2$ não depende da base ortonormal utilizada.