Aplicações da Matemática

EDITORES:
Acilina Azenha
Maria Amélia Jerónimo
José Alberto Rodrigues

CENTRO DE MATEMÁTICA

Instituto Superior de Engenharia de Lisboa

OFERTA
DO
CENTRO DE MATEMÁTICA

ISEL

APLICAÇÕES DA MATEMÁTICA

Editores

Acilina Azenha , Maria Amélia Jerónimo e José Alberto Rodrigues

CENTRO DE MATEMÁTICA
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Primeira edição, Outubro de 1998

Capa: Helder Soares

Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro
1900 Lisboa
Tel. 831 71 67 - Fax 831 70 01

Impressão: GRAFITESE, Centro Editorial, Lda.
Lisboa

ISSN: 972-97939-0-5

Depósito Legal: 127672/98

PREFÁCIO

Encontram-se aqui reunidos os artigos apresentados nas Jornadas de Aplicações da Matemática, que tiveram lugar nos dias 14, 15 e 16 de Outubro de 1998, no Instituto Superior de Engenharia de Lisboa.

A popularidade da Modelação Matemática tem levado ao aparecimento de novos e mais perfeitos modelos, paralelamente com o incremento das técnicas de simulação de problemas quer académicos quer industriais. Contudo, a proliferação da utilização destas técnicas exige um aumento de robustez e de eficiência nos programas de aplicação. Neste contexto é essencial a colaboração entre peritos com várias formações.

Os artigos apresentados incidem sobre os mais recentes desenvolvimentos efectuados em Modelação Matemática e as suas aplicações realizadas a nível nacional.

Estas actas foram impressas directamente a partir dos textos fornecidos pelos autores, desta forma os editores não são responsáveis por inexactidões, comentários ou opiniões expressas nos artigos.

Os editores pretendem agradecer a participação e cooperação dos autores, sem os quais não seria possível realizar este encontro.

Acilina Azenha Maria Amélia Jerónimo José Alberto Rodrigues

AGRADECIMENTOS

Os editores agradecem o apoio das seguintes entidades:

Conselho Directivo do I.S.E.L.
Área da Matemática do I.S.E.L.
Sociedade Portuguesa de Matemática
Associação para a Divulgação da Ciência e da Tecnologia

PATROCÍNIO EXCLUSIVO

Índice

NOVOS DESAFIOS NO ENSINO DA MATEMÁTICA
- Dos modelos aos conceitos ... -

Teresa Ventura

Universidade Atlântica
Antiga Fábrica da Pólvora de Barcarena
2745 Barcarena

1. Um novo olhar sobre a Matemática...

Todo o professor conhece bem a situação de carência generalizada de conhecimentos de Matemática, por parte dos alunos que ingressam no Ensino Superior. Assim sendo é prática corrente dedicar uma grossa fatia dos *curricula* ao "refrescamento" de conhecimentos, que mais se confunde com "primeira aquisição" dos mesmos.

Ora este refrescamento tem de se complementar, de facto, com novas aquisições sob pena de ser repetitivo também no seu insucesso. Novas aquisições no campo do saber, apenas, ou igualmente do saber fazer e saber ser?

A Matemática é[1], numa primeira (e simples...) definição, a Ciência da qualidade, da quantidade e do espaço, de *como descrevê-los simbolicamente* e *como pensar sobre eles*... Numa abordagem mais profunda poderemos acrescentar que é uma invenção humana, no sentido em que lida com "objectos" inventados pelas mentes humanas.

Conjuntos, funções, sucessões, derivadas, espaços topológicos são realidades ideais (não físicas), mas objectivas (a sua definição e propriedades não dependem da opinião ou consciência individual).

A Matemática não é um jogo, não é técnica de ginástica mental, nem nos foi imposta por poderes supra (ou extra)-humanos. É uma construção da humanidade e, como tal, a inteligibilidade das afirmações que produz só pode ser atingida no contexto do património de conhecimentos partilhado pelas comunidades humanas.

A característica mais marcante que a distingue das outras humanidades - das ideologias ou das diversas formas de arte, por exemplo - é ser suportada, no seu desenvolvimento, por metodologias científicas.
Como qualquer invenção humana a Matemática é falível e susceptível de correcções e reformulações; como qualquer ciência tem significado, é capaz de estabelecer o consenso sobre resultados reprodutíveis.

Julgo que, hoje, um dos primeiros desafios que se colocam ao professor que ensina Matemática é precisamente o de suscitar um novo olhar sobre a Matemática: que reabilite as suas vertentes intuitivas e afectivas a par das cognitivas, que revalorize o erro, a certeza e a incerteza, que a reposicione entre as várias ciências e as várias humanidades, e que promova activamente, a partir desse reposicionamento, uma nova oportunidade para o aluno.

Uma experiência em debate: ... os outdoors no ensino da Matemática... Entre Sherlock Holmes e Maigret ou o conforto ilusório de Carl Sagan...

2. Quem faz Matemática ?

Não há cultura, que não demonstre usar alguma espécie (ainda que primitiva) de matemática. Hoje não há praticamente país no mundo que não inove em matemática: até os países sub-desenvolvidos (...em vias de desenvolvimento...) procuram manter actividade neste domínio. A investigação e inovação matemática realizam-se sobretudo nas universidades ou com o apoio destas, de programas governamentais, de grandes empresas: embora qualquer pessoa isolada possa fazê-la, a actividade não apoiada não tem potencial de inovação suficientemente elevado para ser significativo.

Mas a pergunta "Quem faz Matemática ?" não fica respondida apenas com o que se disser sobre os matemáticos que criam nova matemática: tem sido a interacção entre os "fazedores" e os "utilizadores" de matemática - matemáticos ou não - o fermento que conduz ao aparecimento de novos desenvolvimentos.

Na medida em que todas as crianças aprendem a usar a matemática na sua vida corrente e um número significativo de noções matemáticas entram na linguagem comum, podemos dizer que todos somos utilizadores de matemática, isto é, a matemática está firmemente incorporada no conjunto de instrumentos com que olhamos e operamos sobre a realidade e sobre nós próprios e que, portanto, todos contribuímos para o seu desenvolvimento. Mas os mais exigentes utilizadores das matemáticas são os cientistas e técnicos de outros domínios - físicos, astrónomos, engenheiros e projectistas, nomeadamente na engenharia civil, electrotécnica e electrónica, aeronáutica e aeroespacial, informática, genética,..., economistas e financeiros, gestores e produtores de informação para decisão estratégica ou operacional,...

Podemos dizer que hoje é inconcebível qualquer desenvolvimento científico, técnico ou tecnológico que não envolva forte suporte matemático. Igualmente podemos afirmar que as duas riquíssimas fontes de desenvolvimento da matemática têm sido e são por um lado a interacção com as restantes ciências, técnicas e tecnologias - elas próprias em desenvolvimento - e por outro lado os avanços internos da matemática: cada problema resolvido abre múltiplos novos caminhos a percorrer e problemas a resolver...

Penso, assim, que outro dos novos desafios que se colocam ao professor que ensina Matemática ao nível médio/superior é o de questionar-se sobre a eficácia - também a estes níveis - de uma abordagem psicogenética da aprendizagem Matemática[ii]: que suscite situações de vivência efectiva da interacção interdisciplinar e transdisciplinar geradora do próprio desenvolvimento daquela ciência.

> *Uma experiência em debate: ... a concepção de cenários contextualmente credíveis, de prática científica ou aplicacional, em domínios não matemáticos, como ponto de partida para a busca dos conceitos matemáticos de suporte ... Uso de técnicas da formação profissional[iii]...*

3. Como se faz Matemática ?

Num primeiro tempo poderemos dizer que a maioria dos actores com papel relevante no desenvolvimento e aplicação científica e técnica da Matemática concebem, implementam, testam e exploram Modelos, dado ser a modelação o suporte de desenvolvimento e aplicação das Ciências, das Técnicas e das Tecnologias.

Num segundo tempo deveremos realçar que o fazem, em geral, em trabalho cooperativo: discutindo com os seus pares, trabalhando em equipas pluri-disciplinares, testando hipóteses e soluções em ambiente real.

Num terceiro tempo há que considerar que recorrem cada vez mais e mais às ferramentas tecnológicas da nossa época: o uso das tecnologias da informação e da comunicação são hoje indispensáveis à eficácia e eficiência do trabalho científico e técnico.

Penso assim que o terceiro dos novos desafios que se colocam ao professor que ensina Matemática ao nível médio/superior é o de questionar-se sobre a eficácia - também a estes níveis - da adopção de pedagogias de trabalho cooperativo, em ensino por projecto, suportadas em redes de computadores[iv]: que garantam a possibilidade de resolução de problemas reais, complexos, em equipa, em tempo útil ao ciclo de aprendizagem.

> *Uma experiência em debate: ... a concepção e implementação de um observatório estatístico de... na óptica cliente-servidor...*

4. Dos modelos aos conceitos ?

Um problema está equacionado (ou "bem posto...") se:

- está definido o contexto (tema; características do domínio de enquadramento; condições especiais e limitações...);
- estão bem definidas as questões a que se pretende responder;

- está garantida a existência de solução.

Equacionado o problema (Etapa 1), isto é, estando ele "bem posto", há que percorrer novas etapas:

- Etapa 2: Planeamento da resolução do problema.
- Etapa 3: Execução do plano - procura/construção da(s) solução(ões).
- Etapa 4: Avaliação e eventual reajuste da(s) solução(ões).
- Etapa 5: Visão: Memorização da experiência vivida e extrapolação dessa experiência para novos contextos e/ou para uso comunitário em diferentes situações.

Do equacionamento do problema faz parte a identificação de hipóteses prévias ou adicionais - condicionantes externas, limitações de recursos a usar, etc. No entanto poderemos ser obrigados a acrescentar ou alterar certas hipóteses ao longo das fases subsequentes, nomeadamente porque, ao planear ou ao modelar a situação, poderemos concluir que a adição de novas hipóteses poderá aligeirar o processo de resolução do problema, sem diminuir a eficácia da(s) solução(ões).

Na escolha de caminho(s) a seguir faz-se a selecção dos métodos, a afectação de recursos, a programação de tempos e a distribuição de tarefas e responsabilidades... Inúmeras vezes a resolução de problemas passa pela concepção e implementação de um Modelo da realidade contextual em que o problema se coloca para, através da operação desse modelo, procurar/obter as possíveis soluções.

Mas não se pode finalizar o trabalho com a obtenção da(s) solução(ões). Há que ter em conta que esta(s) foi(ram) condicionada(s) pelas hipóteses formuladas e, provavelmente, só é(são) válida(s) nesse contexto. É, por isso, indispensável uma crítica dos resultados obtidos e dos caminhos percorridos, para se avaliar se a solução não será excessivamente restrita, se poderá ser melhorada em eficácia ou eficiência.

Quando se faz trabalho científico é desta avaliação que, na maior parte dos casos, surgem as melhores pistas para reformulação de concepções ou construção de novos modelos explicativos dos fenómenos observados... Quando se desenvolvem técnicas ou tecnologias é desta fase que, com frequência, surgem os mais fortes contributos para uma maior eficiência.

A etapa final é a de constituição da memória individual e grupal. Esta etapa é realizada por todos nós, numa primeira fase sub-conscientemente: é assim que aprendemos, desde crianças. Mas a memorização/extrapolação da experiência vivida pode não se fazer apenas através dos nossos mecanismos cerebrais: o registo da informação, devidamente classificada para mais fácil acesso e, nomeadamente, o recurso aos computadores veio amplificar fortemente as possibilidades de novos usos, em idênticos contextos e/ou situações e de extrapolação de resultados e processos, para situações e contextos diversos.

Se pretendermos evidenciar as características mais importantes da Modelação diremos que:

- é uma actividade de criação de objectos - os modelos;
- que permite a manipulação e o teste desses objectos para observar o seu funcionamento e avaliar o seu comportamento face a situações-tipo;
- que orienta a correcção das deficiências detectadas;
- e que tem em vista a reprodução do modelo testado e corrigido - para uso repetido, na mesma ou em diferentes situações.

Usamos modelos por razões de mercado: porque o teste do modelo:

- é menos dispendioso do que o teste do produto real...
- é mais seguro do que o teste do produto real...
- facilita a sua optimização ...
- facilita a sua entrada no mercado...
- facilita a sua adaptação rápida a novas situações ...

Usamos modelos por razões científicas e técnicas: porque a concepção, implementação, operação e teste do modelo:

- facilita a compreensão dos fenómenos e situações ...
- facilita a compreensão das condicionantes e limitações do modelo construído...
- facilita a busca de respostas a questões e a procura de soluções...

Em qualquer dos casos o Fazedor de Modelos necessita seguir as diversas etapas de resolução de problemas, neste caso tomando em conta que a modelação será a sua ferramenta privilegiada para encontrar as soluções que procura.

É a riqueza do percurso a seguir ao construir uma representação da realidade - suficientemente simples para que seja facilmente intelígivel o sistema de representação usado, mas suficientemente potente para que a sua operação produza soluções eficazes - que é geradora de uma melhor compreensão dos conceitos de suporte.

Porque uso a Lógica ou a Teoria de Conjuntos para criar um modelo de investigação policial? Porque uso Sucessões para modelar a reprodução de certas espécies em diferentes ambientes? Porque uso Equações Diferenciais em Derivadas Parciais para modelar o comportamento de estruturas de engenharia civil? Porque uso Funções Contínuas para modelar trajectórias de corpos celestes? Como construo o modelo; quais são as propriedades matemáticas da estrutura adoptada que justificam a sua exploração na busca de respostas às questões postas; como interpreto as conclusões? Haverá vários modelos para responder às mesmas questões? Poderá o mesmo modelo ser usado em diferentes contextos e para diferentes situações? Há modelos verdadeiros ou falsos? E melhores ou piores?

Pedagogicamente, a passagem dos modelos aos conceitos pode ser feita, num primeiro tempo, na análise crítica da passagem da realidade para o modelo: passando por uma descrição dos objectos, relações e propriedades relevantes em linguagem natural e evidenciando o que se espera da estrutura-modelo. A avaliação das limitações do modelo reforça a compreensão das diferenças entre a estrutura escolhida e outras, clarificando as ausência de certas características e, em consequência, algum tipo de questões a que não poderá responder.

Num segundo tempo, para estruturas/conceitos mais complexos, pode/deve seguir-se o caminho inverso: com a experiência adquirida na construção e avaliação dos modelos anteriormente referidos, passar à interpretação e avaliação de modelos com valor científico ou técnico reconhecido. Nestes casos poderemos eventualmente ir mais longe nas capacidades operatórias das estruturas adoptadas e no valor da comprovação experimental de resultados.

Penso assim que o quarto dos novos desafios que se colocam ao professor que ensina Matemática ao nível médio/superior é o de questionar-se sobre o balanceamento adequado entre um ensino extensivo das matérias ou um ensino compreensivo/interpretativo. Entre privilegiar a concepção, operação, interpretação e avaliação ou privilegiar a demonstração.

Uma experiência em debate: ... as novas memórias virtuais cooperativas...

5. O que se aprende, o que se ensina ?

As pedagogias de Aprendizagem Cooperativa são hoje consideradas de indiscutível eficácia sobretudo se conjugadas com outras pedagogias, igualmente centradas no aluno mas orientadas para a realização de objectivos finais socialmente estabelecidos como credibilizadores, como é o caso da Pedagogia por Projecto. A aliança das novas tecnologias de trabalho cooperativo sobre redes de computadores (CSCW) veio abrir perspectivas promissoras para uma educação para o século XXI, nomeadamente permitindo o desenvolvimento de novas vertentes bastante eficazes da Pedagogia por Projecto.

No ensino da matemática, a concepção e desenvolvimento de projectos reais (ou aproximadamente reais...), bastante complexos, que exigem os esforços conjugados de uma equipa vasta para serem equacionados e solucionados em tempo útil, usando tecnologias adequadas - projectos que pressupõem *modelar a realidade, implementar, testar e explorar modelos* - potencia enormemente a aquisição de conhecimentos, o domínio das técnicas e a aquisição de uma visão transdisciplinar sobre a própria matemática.

Este trabalho em grupo, se adequadamente orientado, não invalida antes exige e motiva cada elemento do grupo a uma aprendizagem individualizada (auto-controlada e tutelada), que lhe garanta as condições de reconhecimento como membro activo e valioso na equipa.

Aqui também o uso de *software* de apoio às vertentes de ensino individualizado tutelado é garantia de maior qualidade educativa.

É de realçar o facto de que, neste tipo de pedagogia, se adquirem e treinam, também, competências complementares bastante valiosas em liderança de grupos e liderança cooperativa, em partilha de informação em rede, coordenação e realização cooperativa de projectos, na decisão em grupo, na elaboração de documentos em co-autoria, na comunicação e negociação, etc. Estas como aquelas, são competências essenciais a quem trabalha e vive hoje numa sociedade cada dia mais interactiva, globalizada, informacional e ... necessariamente, matematizada...

Uma experiência em debate: Vivmat - Viveiro de Matemática(o)s...
Aprender a aprender, aprender a ensinar: em Matemática, sempre...

---

[i] (1) "A experiência matemática", Philip J. Davis e Reuben Hersh, Colecção Ciência Aberta, GRADIVA, Lisboa, 1995

[ii] "Lógica e conhecimento científico", Jean Piaget e all, Colecção Ponte, Livraria Civilização -Editora, Porto, 1980

[iii] "Guia de métodos e práticas em formação", Edmond Marc, Jacqueline Garcia-Locqueneux, Horizontes Pedagógicos, Instituto Piaget, Lisboa, 1997

[iv] "Implementing computer supported cooperative learning", David McConnell, Kogan Page Limited, London, 1994

Tendencioso, Vago e Inteligente

José Carlos Quadrado
CIPROMEC, ISEL, IPL
R. Conselheiro Emidio Navarro, 1900 Lisboa
Telefone: 8317271 Fax: 8317273
E-mail: jcquadrado@isel.pt

Resumo

O carácter vago e incerto dos sistemas reais tem sido, ao longo de gerações, uma motivação para criar diferentes abordagens com o objectivo de lidar com este carácter vago e incerto. Algumas das abordagens têm sido bem sucedidas, nomeadamente as que recorrem à teoria das probabilidades e à estatística para lidar com sistemas reais com acontecimentos possíveis bem definidos.

Para o caso de sistemas reais onde os acontecimentos possíveis não são bem definidos, criaram-se abordagens que lidam com a dificuldade de uma classificação, sem ser por comparação, associando um certo carácter de incerteza. Para lidar com o carácter vago e incerto existente em alguns sistemas reais, o autor propôs a utilização de objectos matemáticos ditos conjuntos vagos tendenciosos (TSets), e desenvolveu uma teoria para aplicar aos sistemas reais anteriormente referidos, a qual fornece um suporte matemático rigoroso, no qual um fenómeno vago conceptualmente, pode ser estudado de uma maneira precisa e rigorosa, permitindo igualmente a sua utilização em situações em que existem relações, critérios ou fenómenos vagos, quer na modelização, quer no controlo de sistemas reais.

Com o objectivo de sistematizar controladores vagos tendenciosos, apresenta-se, resumidamente, a teoria básica dos conjuntos vagos tendenciosos, e com base nesta, apresenta-se a síntese de um controlador vago tendencioso para um sistema electromecânico e os resultados de implementação do referido controlador.

1 Introdução

A evolução das espécies forçou o desenvolvimento de redes de neurónios, que originaram o comportamento inteligente, permitindo que a evolução da linguagem e a actividade do pensamento alcançassem complexidade.

A actividade do pensamento válido, do raciocínio, é o objecto de estudo da lógica. Os estudos sobre a lógica e a sua organização começaram com Aristóteles nas escolas da antiga Grécia no século IV A.C.. A contribuição de Aristóteles mais importante para a lógica foi a teoria do silogismo [1], considerada pelos pensadores da Idade Média como a mais importante teoria para a lógica. Esta consideração manteve-se até ao século XVIII, culminando com a afirmação do filósofo germânico Kant, "A lógica é uma ciência completa".

No século XIX, o irlandês Boole provou a falsidade da afirmação de Kant, demonstrando que o campo das funções de verdade era bem mais rico do que se supunha, desenvolvendo para tal novos métodos que permitiram generalizar a teoria Aristotélica do silogismo. Ainda neste século, o matemático alemão Frege contribuiu com a teoria da quantificação, para que no início do século XX Whitehead e Russel sistematizassem os novos desenvolvimentos da lógica no seu *Príncipia Matematica*. Nesse trabalho, os autores generalizaram a lógica Aristotélica lidando com mais formas de raciocínio, e utilizando mais simbolismo [1].

Os estudos lógicos mais recentes assumem um carácter semelhante ao da matemática pura e têm mantido o interesse dos investigadores pela lógica. Exemplo disso, a lógica de conjuntos multivalor de Lukasiewicz [2], veio permitir o advento da lógica fuzzy [3], a qual permite elaborar raciocínios num universo linguístico estruturado. Estes raciocínios aumentam o número de elementos lógicos passíveis de serem utilizados, como é o caso da inferência composicional. A lógica fuzzy caracteriza-se sumariamente pela capacidade de efectuar raciocínios aproximados, recorrendo a um suporte linguístico e á lógica de conjuntos multivalor, obtendo desta forma uma relaxação de conceitos.

No entanto ao introduzir-se a relaxação dos conceitos, não se levou este procedimento ao último estágio, "limitando" as funções de pertença das variáveis dos universos linguísticos a funções determinísticas. Posteriormente, foi proposta a noção de conjuntos vagos [4], que apesar de ultrapassar a referida limitação, não eram passíveis de um fácil manuseamento e aplicação a situações reais. Com efeito, a noção de conjuntos vagos consiste numa extensão dos conjuntos fuzzy, através da definição de funções de pertença não determinísticas, caracterizada por um intervalo de graus de pertença para cada valor do universo considerado.

Ao apresentar-se neste trabalho uma variação da teoria dos conjuntos vagos, designada por teoria dos conjuntos vagos tendenciosos [7], procura-se ultrapassar as limitações na utilização dos conjuntos vagos e incorporando simultaneamente outros elementos linguisticos, tais como a ironia, a hipérbole, o ruído de fundo, as perdas de amostragem, entre outros.

2 Definições básicas dos conjuntos vagos tendenciosos

No universo linguístico, a credibilidade que o receptor atribui à mensagem deve ser considerada como um elemento importante, sendo naturalmente incorporada no processamento linguístico. Os TSets procuram incorporar esta credibilidade do receptor linguístico através da

criação de três funções de pertença, nomeadamente a optimista, a pessimista e a tendenciosa, que procuram retractar respectivamente o grau de possibilidade, o grau de impossibilidade, e o grau de certeza de uma dada informação linguística.

2.1 Elementos vagos básicos

Um conjunto vago tendencioso (TSet), é uma colecção de elementos que pertencem a um conjunto suporte X que satisfaz a seguinte definição:

Def. 1: Conjunto vago tendencioso

Seja X um conjunto. $\breve{\breve{A}}$ é um conjunto vago tendencioso em X sse:

$$\breve{\breve{A}} = \left\{\left(x, \left\{\left[\mu^{o}_{\breve{\breve{A}}}(x), \mu^{1-p}_{\breve{\breve{A}}}(x)\right], \mu^{t}_{\breve{\breve{A}}}(x)\right\}\right) | x \in X\right\} \quad (1)$$

sendo $\mu^{o}_{\breve{\breve{A}}}: X \to [0,1]$ uma função de pertença, que mede o grau de pertença optimista de x ao conjunto $\breve{\breve{A}}$, ou seja, dado $x \in X$: $\mu^{o}_{\breve{\breve{A}}}(x) = \text{Grau}(x \in \breve{\breve{A}}) \in [0,1]$; sendo $\mu^{1-p}_{\breve{\breve{A}}}(x) = 1 - \mu^{p}_{\breve{\breve{A}}}(x)$ com $\mu^{p}_{\breve{\breve{A}}}: X \to [0,1]$ uma função de pertença, que mede o grau de pertença pessimista (ou de não pertença) de x ao conjunto $\breve{\breve{A}}$, ou seja, dado $x \in X: \mu^{p}_{\breve{\breve{A}}}(x) = \text{Grau}(x \notin \breve{\breve{A}}) \in [0,1]$, e onde $\mu^{t}_{\breve{\breve{A}}}: X \to [0,1]$, é uma função de pertença, dada pela expressão:

$$\mu^{t}_{\breve{\breve{A}}}(x) = \sqrt[\alpha]{\frac{\left[\mu^{o}_{\breve{\breve{A}}}(x)\right]^{\alpha} + \left[\mu^{1-p}_{\breve{\breve{A}}}(x)\right]^{\alpha}}{2|\alpha|}} \quad \text{com} \quad \alpha \neq 0 \quad (2)$$

que mede o grau de pertença tendencioso (ou de credibilidade tendenciosa) de x ao conjunto $\breve{\breve{A}}$.

O elemento α é o factor de credibilidade, representando a credibilidade de um elemento num conjunto vago, que pode variar do descrédito total ($\alpha \to -\infty$) até ao crédito total ($\alpha \to \infty$).

Nesta teoria as relações seguintes são sempre verificadas, qualquer que seja o valor de x.

$$\begin{aligned} &\mu^{o}_{\breve{\breve{A}}}(x) + \mu^{p}_{\breve{\breve{A}}}(x) \leq 1 \\ &\mu^{o}_{\breve{\breve{A}}}(x) \leq \mu^{t}_{\breve{\breve{A}}}(x) \leq \mu^{1-p}_{\breve{\breve{A}}}(x) \end{aligned} \quad \forall x \in X \quad (3)$$

Pela definição, verifica-se que um TSet é uma generalização de um conjunto vago e por conseguinte uma generalização de um conjunto fuzzy. Assim, se as três funções de pertença (3) tiverem o mesmo grafo, então o TSet identifica-se, naturalmente com um conjunto fuzzy.

Por outro lado se o factor de credibilidade, α, for indefinido então os TSets reduzem-se aos conjuntos vagos, de acordo com a definição [4].

O factor de credibilidade vai ser uma condicionante dos TSets, pois dependo do valor de α

$$\mu_{\tilde{\tilde{A}}}^{t}(x)=\begin{cases}\min(\mu_{\tilde{\tilde{A}}}^{o}(x),\mu_{\tilde{\tilde{A}}}^{1-p}(x)) & \alpha\to-\infty \quad \text{(minimo)}\\ \dfrac{2*\mu_{\tilde{\tilde{A}}}^{o}(x)*\mu_{\tilde{\tilde{A}}}^{1-p}(x)}{\mu_{\tilde{\tilde{A}}}^{o}(x)+\mu_{\tilde{\tilde{A}}}^{1-p}(x)} & \alpha=-1 \quad \text{(media harmonica)}\\ \sqrt{\mu_{\tilde{\tilde{A}}}^{o}(x)*\mu_{\tilde{\tilde{A}}}^{1-p}(x)} & \alpha\to 0 \quad \text{(media geometrica)}\\ \dfrac{\mu_{\tilde{\tilde{A}}}^{o}(x)+\mu_{\tilde{\tilde{A}}}^{1-p}(x)}{2} & \alpha=1 \quad \text{(media aritmetica)}\\ \max(\mu_{\tilde{\tilde{A}}}^{o}(x),\mu_{\tilde{\tilde{A}}}^{1-p}) & \alpha\to\infty \quad \text{(maximo)}\end{cases} \tag{4}$$

2.2 Operações básicas para TSets

As funções de pertença, optimista e pessimista são componentes cruciais dos TSets, pois é através delas que são definidas as operações possíveis com os TSets. A titulo de exemplo, apresentam-se em seguida algumas operações básicas para TSets.

Def. 2: União de dois TSets

Sejam $\tilde{\tilde{A}}$ e $\tilde{\tilde{B}}$ dois TSets. A união de $\tilde{\tilde{A}}$ e $\tilde{\tilde{B}}$ é também um TSet sse as funções de pertença são definidas ponto a ponto por:

$$\begin{aligned}\mu_{(\tilde{\tilde{A}}\cup\tilde{\tilde{B}})}^{o}(x)&=\max\left(\mu_{\tilde{\tilde{A}}}^{o}(x),\mu_{\tilde{\tilde{B}}}^{o}(x)\right)\\ \mu_{(\tilde{\tilde{A}}\cup\tilde{\tilde{B}})}^{1-p}(x)&=\max\left(\mu_{\tilde{\tilde{A}}}^{1-p}(x),\mu_{\tilde{\tilde{B}}}^{1-p}(x)\right)=1-\min\left(\mu_{\tilde{\tilde{A}}}^{p}(x),\mu_{\tilde{\tilde{B}}}^{p}(x)\right)\\ \mu_{(\tilde{\tilde{A}}\cup\tilde{\tilde{B}})}^{t}(x)&=\max\left(\mu_{\tilde{\tilde{A}}}^{t}(x),\mu_{\tilde{\tilde{B}}}^{t}(x)\right)\end{aligned} \tag{5}$$

A figura 1 ilustra a união e a intersecção de dois TSets.

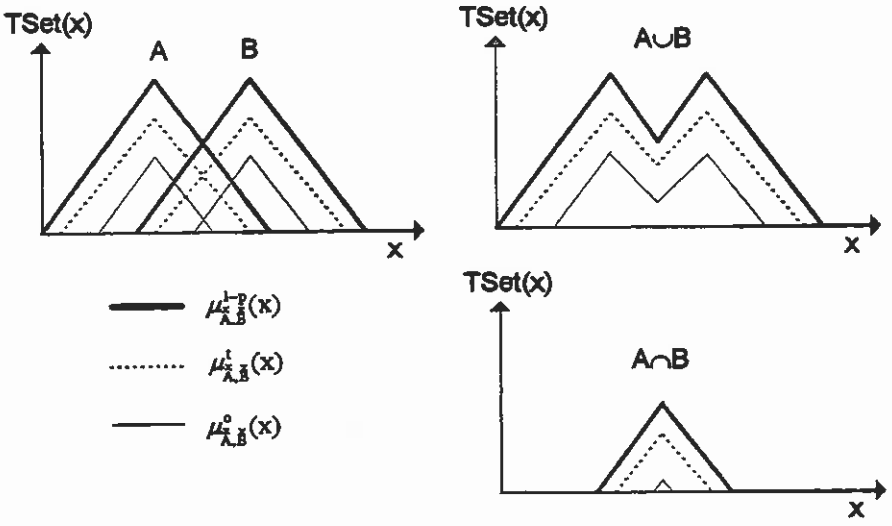


Figura 1 - União e intersecção de dois TSets

Def. 3:Complemento de um TSet

Seja $\tilde{\tilde{A}}$ um TSet. $\complement\tilde{\tilde{A}}$ é o TSet complemento de $\tilde{\tilde{A}}$ sse apresenta as funções de pertença:

$$\begin{aligned}
&\mu^{o}_{\complement\tilde{\tilde{A}}}(x) = 1 - \mu^{1-p}_{\tilde{\tilde{A}}}(x) = 1 - \left[1 - \mu^{p}_{\tilde{\tilde{A}}}(x)\right] = \mu^{p}_{\tilde{\tilde{A}}}(x) \\
&\mu^{1-p}_{\complement\tilde{\tilde{A}}}(x) = 1 - \mu^{o}_{\tilde{\tilde{A}}}(x) \\
&\mu^{t}_{\complement\tilde{\tilde{A}}}(x) = 1 - \mu^{t}_{\tilde{\tilde{A}}}(x)
\end{aligned} \tag{6}$$

Graficamente o complemento de um TSet é o que se apresenta em seguida:

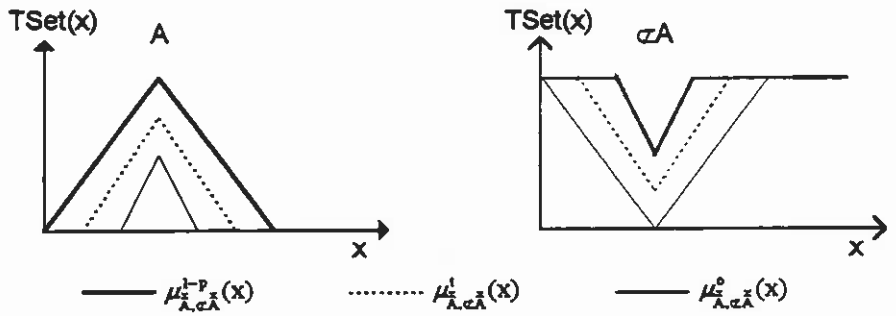


Figura 2.2 - Complemento de um TSet

3 Sistematização da aplicação da lógica vaga tendenciosa

Nos pontos anteriores apresentou-se todo o suporte matemático considerado básico na teoria dos conjuntos vagos tendenciosos. Neste ponto apresentam-se as ferramentas matemáticas necessárias à utilização desta teoria.

Uma das ferramentas básicas na utilização da lógica TSets é a noção de variável linguística, [5]. Uma variável linguística no universo dos TSets pode ser definida como se segue:

Def. 4: Variável linguística

Uma variável linguística é caracterizada por cinco parâmetros (x, T(x), U, G, $\tilde{\tilde{S}}$), onde x é o nome da variável, T(x) o conjunto dos valores linguísticos possíveis dessa variável, U o universo de discurso da variável, G a regra sintáctica (gramática) para gerar os termos da variável, e $\tilde{\tilde{S}}(...)$ a regra semântica para associar a cada termo o seu valor, o qual é um subconjunto vago tendencioso do universo de discurso.

3.1 Raciocínio aproximado

As principais ferramentas do raciocínio são tautologias tais como o *modus ponens*. Esta tautologia foi generalizada [8], criando o chamado *modus ponens* generalizado. Aplicando á lógica vaga tendenciosa o *modus ponens generalizado,* surge a regra de inferência composicional [9], que no domínio dos TSets é definida como:

Def. 5: Regra de inferência composicional

Sendo $\tilde{\tilde{R}}(x)$, $\tilde{\tilde{R}}(x,y)$, e $\tilde{\tilde{R}}(y)$, definidas nos espaços X, X×Y, Y, respectivamente, como restrições nos espaços de x, (x, y), e y respectivamente, com $x \in X$ e $y \in Y$. Sendo ainda $\tilde{\tilde{A}}$ e $\tilde{\tilde{B}}$ dois TSets em X e X×Y respectivamente, então a regra de inferência composicional define a solução das equações de atribuição relacional

$$\tilde{\tilde{R}}(x) = \tilde{\tilde{A}} \tag{7}$$

$$\tilde{\tilde{R}}(x,y) = \tilde{\tilde{B}} \tag{8}$$

como sendo dada por

$$\tilde{\tilde{R}}(y) = \tilde{\tilde{A}} \circ \tilde{\tilde{B}} \tag{9}$$

onde $\tilde{\tilde{A}} \circ \tilde{\tilde{B}}$ é a composição de $\tilde{\tilde{A}}$ e $\tilde{\tilde{B}}$.

Utilizando operadores de união e intersecção, a relação anterior de implicação fica:

$$\tilde{\tilde{R}}(y) = \bigcup_{x} \left\{ I\left[\left(\mu^{o}_{\tilde{\tilde{A}}}, \mu^{1-p}_{\tilde{\tilde{A}}} \right), \mu^{t}_{\tilde{\tilde{A}}}; \left(\mu^{o}_{\tilde{\tilde{B}}}, \mu^{1-p}_{\tilde{\tilde{B}}} \right), \mu^{t}_{\tilde{\tilde{B}}} \right] \right\} \tag{10}$$

Sendo **U** qualquer operador de união, ou seja, que cumpra as normas-t, e **I** qualquer operador intersecção que cumpra as conormas-t. Os operadores mais vulgarmente utilizados são respectivamente o máximo e o mínimo.

3.2 Controlo vago tendencioso

À semelhança do controlo lógico fuzzy [6], o controlo vago tendencioso pretende modelizar o comportamento humano na tomada de decisões, procurando neste segundo caso incluir elementos que não se encontram naturalmente no conteúdo do discurso, mas que influenciam essa tomada de decisões.

A ideia básica do controlo vago tendencioso é incorporar a credibilidade do receptor da mensagem linguística no projecto do controlador. Com base num conjunto de regras linguísticas que descrevem a estratégia de controlo, constrói-se um algoritmo de controlo onde as palavras são definidas como conjuntos vagos tendenciosos. Assim, para além da possibilidade de incorporar no controlador a experiência do operador, ou intuição, ou conhecimentos heurísticos, ou ainda de não precisar do modelo do processo, este tipo de controlo permite ainda uma correcção a esta informação em tempo real através de um factor de credibilidade.

Em termos de diagrama de blocos, o controlador vago tendencioso, é composto pelos blocos que se apresentam na figura seguinte:

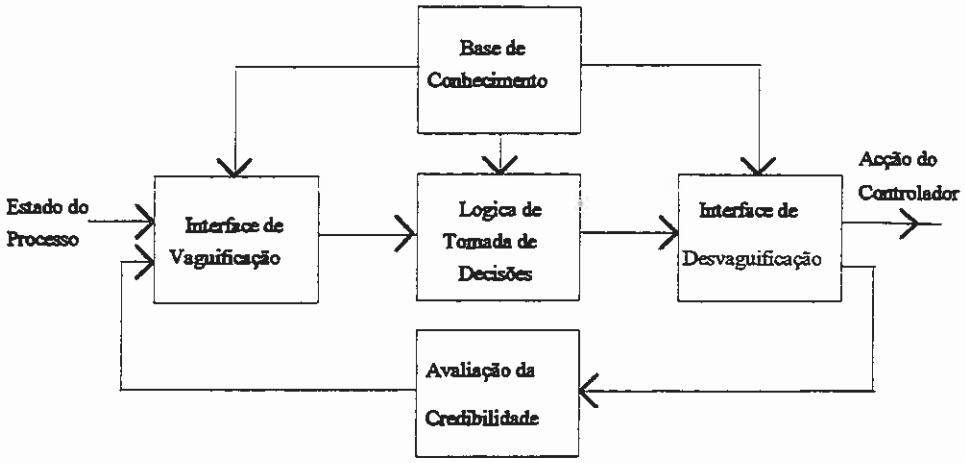


Figura 3 - Diagrama de blocos funcional do controlador vago tendencioso

4 Resultados de Aplicação do Controlador Vago Tendencioso

A aplicação de uma versão discreta simples do controlador vago tendencioso, a um posicionador electromecânico utilizando um motor DC, apresentou os seguintes resultados:

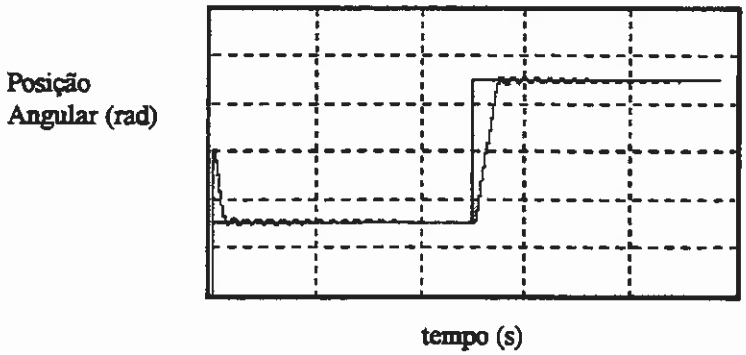


Figura 4 - Posicionador electromecânico inteligente (escalas: vertical 1 [rad]; horizontal 500 [ms])

A saída do controlador na situação de acompanhamento da referencia anterior é a seguinte:

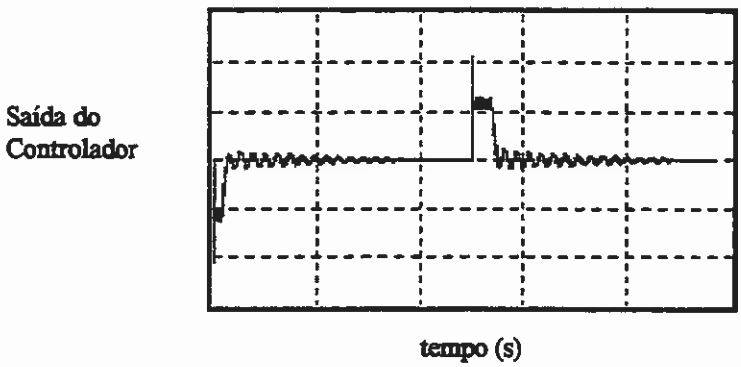


Figura 5 - Comportamento do controlador vago tendencioso (escala horizontal 500 [ms])

A análise dos dois gráficos anteriores permite verificar que o posicionador electromecânico segue a referência sem sobreelevação, reage muito rapidamente a perturbações, e não apresenta erros estáticos, fazendo uma auto-correcção desses erros. No entanto, apresenta um "ripple" excessivo durante a fase de eliminação do erro estático, o qual pode ser resolvido com pequenas

mudanças na determinação do factor de credibilidade, α, mas com custos na simplicidade e velocidade de actuação do controlador.

5 - Conclusões

Neste trabalho, apresentou-se, resumidamente, a teoria dos conjuntos vagos tendenciosos (TSets), procurando realçar os aspectos mais importantes para o estudo do controlo vago tendencioso, e dirigido para o desenvolvimento de controladores vagos tendenciosos.

Verificou-se que os TSets incorporam conceitos que emulam as incertezas do mundo real impossíveis de incluir nos conjuntos fuzzy, particularmente através da atribuição de um grau de credibilidade à informação recebida, à semelhança do comportamento dos seres humanos. Os TSets suportam também todas as operações dos conjuntos fuzzy e ainda outras específicas, tornando fácil a sua implementação no controlo, devido ás suas características internas de auto-correcção, permitindo prescindir por vezes de acções de correcção exteriores ao controlador.

Concluiu-se que a definição deste tipo de controladores não recorre a informação precedente de ensaios laboratoriais, permitindo criar bases de conhecimento universais, ou seja, independentes dos parâmetros do sistema, e que através da utilização de um factor de credibilidade, se incorpora um elemento de aprendizagem que abre o caminho a possíveis incrementos da quantidade de inteligência deste controlador.

Por ultimo, concluiu-se que as possibilidades de incorporação pelos TSets, de incertezas do mundo real, não se esgotam com os elementos apresentados neste capítulo, podendo os TSets incorporar outros elementos do universo linguístico.

Bibliografia

[1] Barker, S. "The Elements of Logic" MacGrawHill,1989.
[2] Giles,R. ; "Lukasiewicz Logic and Fuzzy Theory", International Journal of Man-Machine studies, 8, pp.313-327, 1976.
[3] Zadeh,L.A.; "Fuzzy Sets", Information and Control, vol. 8,pp.338-353, 1965.
[4] Gau e Buhrer, "Vague Sets", IEEE-SMC, vol.23, pp.611-614, 1993.
[5] Zadeh,L.A.; "Outline of a New Approach to the Analysis of Complex Systems and Decision Process", IEEE Trans. Syst. Man Cybern., vol.SMC-3,pp.28-44, 1973.
[6] Mandani,E.H., Efstathiou,H.J. ; "A Comparative Study of Applied Logics", Fuzzy Sets and Systems, 13, pp.35,48, 1984.
[7] Quadrado J.C. e Silva, J.F., "TSets Usage to Incorporate Extra Dialogue Elements", SICE'96 Proceedings, pp. 1373-1376, 1996.
[8] Zadeh,L.A.; "A Fuzzy Algoritm Approach to the Definition of Complex or Imprecise Concepts", International Journal in Man-Machine Studies, vol. 8, pp.249-291, 1976.
[9] Zadeh,L.A. ;"Fuzzy Sets as a Basis for a Theory of Possibility", Fuzzy Sets and Systems, 1, pp.3-28, 1978.

Grafos, Caixeiros Viajantes e Estatística*

Manuel João Cabral Morais

Departamento de Matemática e Centro de Matemática Aplicada, Instituto Superior Técnico

Resumo

A simplicidade de definição, a diversidade de aplicações e a dificuldade de resolução do Problema do Caixeiro Viajante (PCV) constituem algumas das características comuns à maior parte dos problemas que têm vindo a atrair e intrigar os matemáticos.

Por se tratar de um problema $NP-difícil$, o PCV tem vindo a ser esporadicamente abordado sob o ponto de vista estatístico, com o objectivo de obter estimativas quer pontuais, quer intervalares para o custo do percurso óptimo.

No presente trabalho as estimativas do custo do percurso óptimo — parâmetro de localização do modelo Weibull de mínimos tri-paramétrico — são calculadas com base em custos mínimos obtidos em diversas execuções dos algoritmos 2 e $3-optimal$, considerando-se estas soluções aproximadas do PCV como provenientes de tal modelo extremal.

A importância destas estimativas prende-se com o facto de auxiliarem a decidir se é ou não aconselhável prolongar o processo de obtenção de soluções aproximadas.

Palavras-Chave: Problema do Caixeiro Viajante, Algoritmos λ-*optimais*, Teorema de Gnedenko, Estimação Pontual e Intervalar.

1. O Problema do Caixeiro Viajante

Admita-se que um caixeiro viajante pretende visitar uma única vez cada uma das cidades que figuram numa lista e regressar à cidade donde partiu. Admita-se ainda que ele conhece o custo da viagem entre qualquer par de cidades (podendo o custo não ser igual em ambos os sentidos). A obtenção da sequência de cidades que constitui o percurso associado ao custo total mínimo — o percurso óptimo — é usualmente denominada de Problema do Caixeiro Viajante (PCV).

Há razões práticas que justificam a importância do PCV quer num grafo orientado, quer num grafo não orientado: muitos dos problemas reais que, à partida, parecem ser bem distintos do PCV, podem ser formulados como instâncias deste. No capítulo 2 de Lawler *et al.* (1985), p. 18-22, podem encontrar-se algumas das variadíssimas aplicações deste problema, ilustrando assim a versatilidade do PCV; são disso exemplo a sequencialização óptima de tarefas em gestão da produção e o *wiring* óptimo no *design* de computadores e outros sistemas digitais.

O PCV é, à semelhança de um grande número de problemas de optimização combinatória (POC), um problema para o qual não existem algoritmos exactos com complexidade polinomial.[1] Não surpreende pois que o PCV seja o primeiro problema descrito no livro

* Investigação parcialmente suportada pelo Programa Praxis XXI — PCEX/P/MAT/41/96

[1] Recorde-se que o número total de percursos possíveis é igual a $(N-1)!/2$ $((N-1)!)$, caso as distâncias entre as N cidades da lista (não) sejam simétricas.

Computers and Intractability (Garey e Johnson, 1979), seja comum a frase "É tão difícil quanto o *PCV*", ou que de um *reviewww* feito recentemente tenham resultado 505 referências relacionadas com *PCV* e com data de publicação posterior a 1979.

Neste trabalho o destaque vai para a utilização de soluções do *PCV* — soluções essas obtidas recorrendo a algoritmos aproximativos com complexidade polinomial — no cálculo de estimativas pontuais e intervalares para o custo da solução óptima de tal *POC*, provando assim que da estatística e da optimização combinatória pode resultar um casamento interessante.

2. O *PCV* e a Estatística

A análise de um conjunto de soluções de um *PCV* específico, obtidas usando um algoritmo aproximativo, pode ser feita recorrendo a técnicas de inferência estatística que permitam avaliar os desvios entre tais soluções e a solução óptima. Este tipo de análise pressupõe não só a obtenção de uma amostra, como a especificação de um modelo probabilístico que caracterize o comportamento das observações dessa amostra.

A amostra a considerar neste tipo de análise é constituída por n custos dos percursos resultantes de n execuções de um algoritmo aproximativo de melhoramento[2] D para o *PCV*. O custo do percurso resultante da $i-$ésima $(i=1,...,n)$ execução do algoritmo é, por sua vez, o mínimo de um conjunto de m_i custos dos percursos obtidos nas m_i iterações do algoritmo.

A utilização do modelo probabilístico Weibull de mínimos tri-paramétrico (localização, escala e forma), para caracterizar os custos obtidos por intermédio de algoritmos aproximativos para o *PCV*, remonta a McRoberts (1966). Este mesmo modelo foi também utilizado na estimação das soluções exactas de outros *POC's* que vão desde o problema da afectação quadrática (Bruijs (1984)) ao problema de Steiner definido em grafos (Cerdeira (1986)) passando pelos problemas de cobertura (Vasko e Wilson (1984)) e de cobertura generalizada (Gonsalvez *et al.* (1987)).

A função de densidade de probabilidade do modelo Weibull de mínimos tri-paramétrico é dada por

$$f(x)=(c/b)\times\left[(x-a)/b\right]^{c-1}e^{-\left[(x-a)/b\right]^{c}}\times I_{[a,+\infty)}(x) \qquad (1)$$

onde $-\infty<a<+\infty$, $b>0$ e $c>0$ representam os parâmetros de localização, escala e forma, respectivamente. Adiante-se no entanto que, pelo facto de na definição do *PCV* se considerar que a função de custo é não negativa, os valores possíveis para o parâmetro a — que corresponde ao custo do percurso óptimo do *PCV* — restringir-se-ão ao intervalo $[0,+\infty)$.

A aplicação deste modelo à estimação do custo da solução óptima do *PCV* encontra uma justificação — parcial é certo — no teorema de Gnedenko na sua versão para o mínimo.[3] Com

---

[2] Ao contrário dos algoritmos aproximativos de construção, lida-se, em qualquer iteração da execução do algoritmo, com um percurso que inclui todas as cidades.

[3] Este teorema, espécie de teorema do limite central para o mínimo de uma amostra aleatória, afirma que tal mínimo (devidamente estandardizado), caso não convirja para uma distribuição não degenerada, converge para uma das três seguintes distribuições: a Fréchet de mínimos, a Weibull de mínimos ou a Gumbel de mínimos.

efeito lida-se, em cada execução, com o mínimo de um grande número de custos que são limitados à esquerda pelo custo do percurso óptimo, a. Mas, como refere Morais (1998), não basta que o conjunto de valores possíveis para os custos seja limitado à esquerda para que a distribuição de cada um dos n custos mínimos possa ser aproximada pela distribuição Weibull de mínimos, como referem Golden (1977) e outros autores. Esta e outras objecções quanto à aplicação do teorema de Gnedenko e do modelo de Weibull de mínimos ao *PCV* não impediram que alguns autores tivessem obtido resultados, por vezes surpreendentes, na estimação quer pontual, quer intervalar, do custo da solução óptima do *PCV* e de outros *POC*'s.

2.1 Estimativas pontuais

O custo da solução óptima de um *PCV* (ou de qualquer outro *POC* *NP – difícil*) pode considerar-se um "parâmetro desconhecido em tempo polinomial" e por consequência é razoável estimá-lo quer pontual, quer intervalarmente, com base numa amostra de dimensão n de custos de percursos, $\underline{x}=(x_1,\ldots,x_n)$, ou na amostra ordenada $(x_{(1)},\ldots,x_{(n)})$ onde $x_{(1)}=\min_{i=1,\ldots,n} x_i$.

Começa-se por fazer uma breve referência às estimativas de máxima verosimilhança. Estas obtêm-se, tal como o nome indica, maximizando a função de verosimilhança que, para o modelo Weibull de mínimos tri-paramétrico, é igual a

$$L(a,b,c|\underline{x})=(c/b)^n\times\left\{\prod_{i=1}^{n}\left[(x_i-a)/b\right]\right\}^{c-1}\times\exp\left\{-\sum_{i=1}^{n}\left[(x_i-a)/b\right]^c\right\}\times$$
$$\times I_{[0,x_{(1)}]\times(0,+\infty)\times(0,+\infty)}(a,b,c), \qquad (2)$$

onde I_A representa a função indicatriz do conjunto A. Logo a estimativa de máxima verosimilhança do vector de parâmetros do modelo (a,b,c), $(\hat{a},\hat{b},\hat{c})=(\hat{a}(\underline{x}),\hat{b}(\underline{x}),\hat{c}(\underline{x}))$, é caracterizada por ser a escolha mais plausível na região $[0,x_{(1)}]\times(0,+\infty)\times(0,+\infty)$ uma vez obtida a amostra $\underline{x}$.

Surgem algumas dificuldades na obtenção de $(\hat{a},\hat{b},\hat{c})$. Com efeito, Rockette *et al.* (1974) referem — ao contrário do que sugere a leitura de Golden (1977) — que $(\hat{a},\hat{b},\hat{c})$ nem sempre se obtém resolvendo numericamente o sistema de equações de verosimilhança

$$\nabla \ln L(a,b,c|\underline{x})=(0,0,0) \qquad (3)$$

na região $[0,x_{(1)}]\times(0,+\infty)\times(0,+\infty)$. Quando o verdadeiro valor do parâmetro de forma se restringe ao intervalo $(0,1)$ conclui-se que $\hat{a}=x_{(1)}$ e que as estimativas $\hat{b}$ e $\hat{c}$ se obtêm resolvendo as duas últimas equações do sistema em (3). E, caso $c\in[1,+\infty)$ e não exista solução para (3), $\ln L(a,b,c|\underline{x})$ possui ponto de máximo em

$$(\hat{a},\hat{b},\hat{c})=\left(x_{(1)},\frac{1}{n}\sum_{i=1}^{n}(x_i-x_{(1)}),1\right).^4 \qquad (4)$$

---

4 É interessante notar que as estimativas obtidas para o parâmetro de forma, em Golden e Alt (1979), são todas superiores à unidade.

Não admira pois que alguns autores tenham proposto estimativas pontuais alternativas às de máxima verosimilhança para os três parâmetros do modelo; destas alternativas destacam-se as propostas por Zanakis (1979) e Wyckoff *et al.* (1980), que se encontram na Tabela 1 e que têm a particularidade de ser precisas e de cálculo bastante trivial.

Parâmetro	Estimativas	
	Zanakis	Wyckoff-Bain-Engelhardt
a (localização)	$\bar{a} = \dfrac{x_{(1)} \times x_{(n)} - x_{(2)}^2}{x_{(1)} + x_{(n)} - 2 \times x_{(2)}}$	$\tilde{a} = \dfrac{x_{(1)} - \bar{x}/n^{1/\tilde{c}_0}}{1 - 1/n^{1/\tilde{c}_0}}$
b (escala)	$\bar{b} = -\bar{a} + x_{(\lceil 0.63n \rceil^*)}$	$\tilde{b} = \exp\left\{ \gamma/\tilde{c} + \sum_{i=1}^{n} \ln\left[x_{(i)} - \tilde{a} \right]/n \right\}$
c (forma)	$\bar{c} = \dfrac{\ln\left[\dfrac{\ln(1-p_k)}{\ln(1-p_i)} \right]}{\ln\left\{ \dfrac{x_{(\lceil np_k \rceil^*)} - \bar{a}}{x_{(\lceil np_i \rceil^*)} - \bar{a}} \right\}}$	$\tilde{c} = \dfrac{n \times k_n}{-\sum_{i=1}^{s} \ln\left[x_{(i)} - \tilde{a} \right] + \dfrac{s}{n-s} \sum_{i=s+1}^{n} \ln\left[x_{(i)} - \tilde{a} \right]}$

Tabela 1 — Outras estimativas pontuais para o custo da solução óptima do *PCV*

onde: $p_i = 0.16731$ e $p_k = 0.97366$; $[np]^* = [np] + \left[1 - I_{\mathbf{N}_0}(np)\right]$ com $p \in (0,1)$, $[np]$ a parte inteira do real positivo np e $\mathbf{N}_0$ o conjunto de inteiros não negativos; $\tilde{c}_0$ é estimativa rude do parâmetro de forma, calculada com base em observações da amostra ordenada $\left(x_{(1)},\ldots,x_{(n)}\right)$, que se obtém a partir de $\bar{c}$ substituindo $\bar{a}$ por $x_{(1)}$;[5] $\bar{x} = \sum_{i=1}^{n} x_i/n$ é a média amostral; $\gamma = \lim_{m \to +\infty} \left[\sum_{j=1}^{m} 1/j - \ln(m) \right] \approx 0.57721$ é a constante de Euler; $s = [0.84n]$; e k_n é uma constante dependente da dimensão da amostra, tabelada em Engelhardt e Bain (1977), para valores de n de 2 a 60 e para $n = +\infty$.

Importa referir que as estimativas pontuais de Zanakis já foram utilizadas em Cerdeira (1986) no contexto de um *POC* distinto do *PCV*, tendo-se obtido resultados que o autor considerou bastante satisfatórios. Para mais detalhes acerca de todas estas estimativas pontuais consulte-se Morais (1998).

Realce-se por fim a importância do mínimo amostral como estimativa pontual do custo da solução óptima. Apesar de nem sempre se tratar da estimativa de máxima verosimilhança, o mínimo amostral está associado à melhor das soluções aproximadas obtidas. Para além disso é relevante a comparação desta estimativa pontual com outras eventualmente adoptadas — $\hat{a}$, $\bar{a}$ ou $\tilde{a}$ —, já que um mínimo amostral muito maior que qualquer das três estimativas leva a crer que a solução aproximada associada a $x_{(1)}$ ainda pode ser melhorada, sendo por isso aconselhável prolongar o processo de obtenção de soluções aproximadas.

[5] A constante $\tilde{c}_0$ só está bem definida se $x_{(\lceil np_i \rceil^*)} > x_{(1)}$, isto é, se $n > 1/p_i$.

2.2 Estimativas intervalares

Por ser usual acompanhar uma estimativa pontual de um intervalo de valores razoáveis para o parâmetro desconhecido — intervalo este associado a nível de confiança exacto ou aproximado —, segue-se uma tabela de estimativas intervalares para o custo da solução óptima do PCV.

Estimativas intervalares	
Golden-Alt	$IC_{GA}(a)=\left(x_{(1)}-\hat{b};\, x_{(1)}\right)$
Golden-Alt-Zanakis	$IC_{GAZ}(a)=\left(x_{(1)}-\bar{b};\, x_{(1)}\right)$
Golden-Alt-Wyckoff-Bain-Engelhardt	$IC_{GAWBE}(a)=\left(x_{(1)}-\tilde{b};\, x_{(1)}\right)$
Los-Lardinois	$IC_{LL}(a)=\left(x_{(1)}-\hat{b}/\left[-n/\ln(\alpha)\right]^{1/\hat{c}};\, x_{(1)}\right)$
Los-Lardinois-Zanakis	$IC_{LLZ}(a)=\left(x_{(1)}-\bar{b}/\left[-n/\ln(\alpha)\right]^{1/\bar{c}};\, x_{(1)}\right)$
Los-Lardinois-Wyckoff-Bain-Engelhardt	$IC_{LLWBE}(a)=\left(x_{(1)}-\tilde{b}/\left[-n/\ln(\alpha)\right]^{1/\tilde{c}};\, x_{(1)}\right)$

Tabela 2 — Estimativas intervalares para o custo da solução óptima do PCV

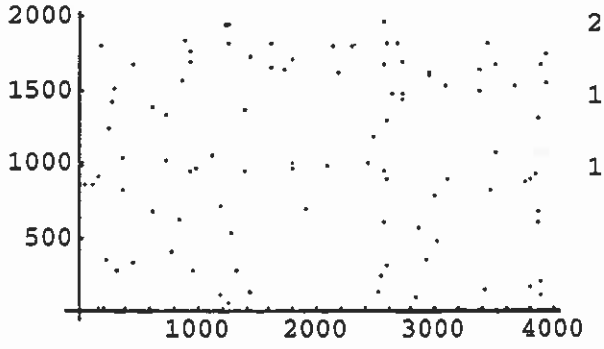
Golden e Alt (1979) constitui aquela que se julga ser a primeira referência em que é feita estimação por intervalos do custo da solução óptima do PCV. Estes autores propuseram que se substituísse o parâmetro de escala b pela sua estimativa de máxima verosimilhança $\hat{b}$ na expressão do intervalo de confiança a $\left(1-e^{-n}\right)\times 100\%$ para o parâmetro de localização a, $IC_{\left(1-e^{-n}\right)\times 100\%}(a)=\left(x_{(1)}-b;\, x_{(1)}\right)$, resultando assim $IC_{GA}(a)$. O segundo e terceiro intervalos de confiança da Tabela 2 foram propostos em Morais (1998) e obtiveram-se substituindo b pelas estimativas de Zanakis e de Wickoff-Bain-Engelhardt, respectivamente.

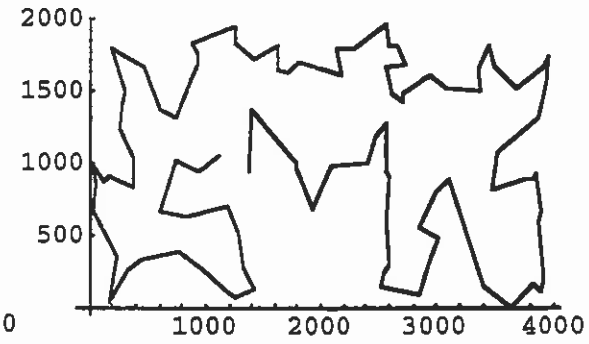
Por seu lado, as três últimas estimativas intervalares da Tabela 2 resultaram da substituição dos parâmetros desconhecidos b e c pelas suas estimativas de máxima verosimilhança (tal como proposto por Los e Lardinois, 1982), de Zanakis e de Wyckoff-Bain-Engelhardt (tal como sugerido por Morais, 1998), na expressão do intervalo de confiança a $(1-\alpha)\times 100\%$ para o custo da solução óptima do PCV, $IC_{(1-\alpha)\times 100\%}(a)=\left(x_{(1)}-b/\left[-n/\ln(\alpha)\right]^{1/c};\, x_{(1)}\right)$. De referir que concretizações do limite inferior de $IAC_{LL}(a)$ já foram utilizadas em Cerdeira (1986), na estimação do custo da solução óptima de um outro POC, o problema de Steiner em grafos.

A substituição de b e c por suas estimativas em $IC_{\left(1-e^{-n}\right)\times 100\%}(a)$ e $IC_{(1-\alpha)\times 100\%}(a)$ altera, naturalmente, o nível de confiança destas duas estimativas intervalares; e, tanto quanto se sabe, nenhum autor determinou os níveis de confiança exactos dos intervalos da Tabela 2. Por este motivo os seis intervalos não possuem um índice indicando o respectivo nível de confiança; possuem antes iniciais que dizem respeito aos autores que propuseram o intervalo original e às estimativas utilizadas.

3. Uma aplicação

Segue-se a análise estatística de uma variação do problema das 100 cidades originalmente descrito em Krolak *et al.* (1971). Na verdade não se tratam de cidades mas de 100 pontos gerados aleatoriamente, que poderiam representar, tal como em Lin e Kernighan (1973), pontos marcados sobre uma placa, onde deve ser efectuada uma pequena perfuração com um *laser* (ver Figura 1).[6] A variação propriamente dita expressa-se sob a forma da seguinte restrição: os pontos de início e de fim da perfuração foram pré-especificados, e coincidem com o 1° e 63° pontos (à esquerda e à direita, respectivamente, na Figura 2);[7] mas atribuindo uma distância não positiva a esse par de pontos, à semelhança do que Crowder e Padberg (1980) sugerem, e somando posteriormente a distância entre esses dois pontos o problema torna-se uma instância do *PCV standard* definido sobre um grafo não orientado.





Figuras 1 e 2 — Pontos do problema das 100 cidades e o percurso óptimo

A escolha deste exemplo prende-se com o facto de Crowder e Padberg (1980) terem estabelecido a optimalidade da solução apresentada por Krolak *et al.* (1971). Deste modo, poder-se-á avaliar objectivamente a precisão das estimativas pontuais e a qualidade dos intervalos de confiança para o custo óptimo do *PCV*, obtidos com base em 100 execuções dos algoritmos 2 e 3 – *optimal*.

Na análise estatística deste *PCV*, que é análoga à efectuada para o problema *standard* das 100 cidades de Krolak *et al.* (1971) em Morais (1998), serão ainda apresentados, para cada um dos dois algoritmos, os valores observados da estatística do teste de ajustamento de Kolmogorov-Smirnov bem como o valor crítico do teste (isto é, o $p-value$) associado; esses valores foram obtidos ao conjecturar três distribuições Weibull que possuem o terno de parâmetros igual a cada uma das três estimativas pontuais do terno de parâmetros desconhecidos.[8]

Começa-se por referir que o percurso com menor custo, nas 100 execuções do algoritmo 3 – *optimal*, se encontra na Figura 2. Este percurso foi obtido na 89ª execução e coincide com o percurso óptimo obtido por Krolak *et al.* (1971) e por Morais (1998). A diferença de três

---

[6] Recorde-se que Lin e Kernighan (1973) consideram um problema análogo com três conjuntos idênticos de 105 pontos e outros três pontos, onde deve ser feita a referida perfuração.

[7] A escolha deste último ponto deve-se ao facto de coincidir com o último ponto do percurso óptimo obtido em Krolak *et al.* (1971) bem como em Morais (1998).

[8] Para detalhes acerca da análise estatística consulte-se Morais (1998).

unidades entre o custo associado ao percurso aqui obtido, que é de aproximadamente 21285 unidades (ver Tabela 3), e o custo do percurso óptimo que se encontra na primeira daquelas referências bem como em Crowder e Padberg (1980) deve-se ao facto de aqueles autores terem aproximado às unidades as distâncias entre os 100 pontos.

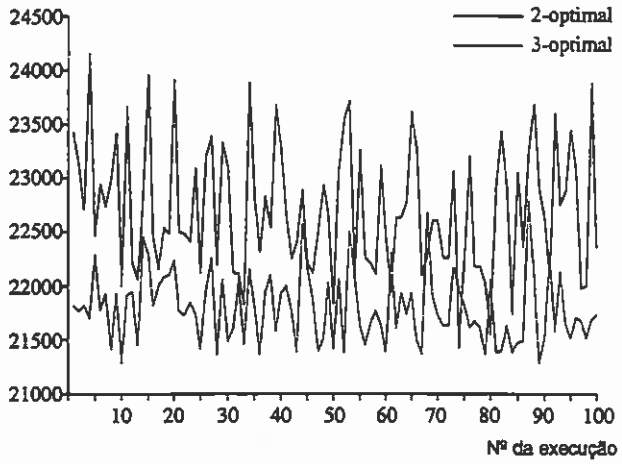


Figura 3 — Custos mínimos em 100 execuções dos algoritmos 2 e 3 – *optimal*

Ao recorrer ao algoritmo 2 – *optimal*, obteve-se o percurso de custo mínimo na 74ª execução de um grupo de 100 execuções; o respectivo custo é de 21426.914 unidades e é, tal como seria de esperar, superior ao do melhor dos 100 percursos 3 – *optimais*.

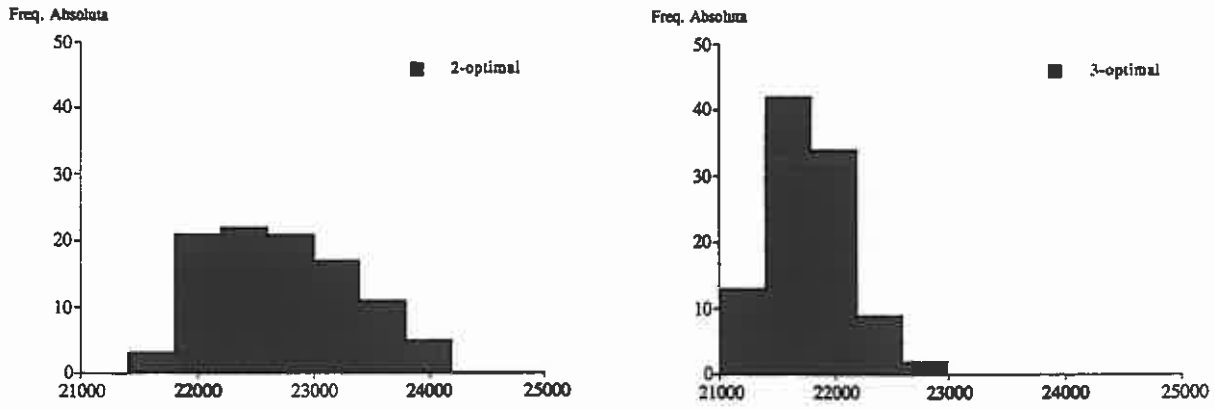


Figura 4 — Histogramas dos custos mínimos em 100 execuções dos algoritmos 2 e 3 – *optimal*

As Figuras 3 e 4 deixam bem claro que os dados associados aos dois procedimentos de melhoramento se distinguem quer em dispersão e quer em forma. Estas diferenças gráficas bem nítidas são consubstanciadas por estimativas pontuais algo discrepantes dos três parâmetros desconhecidos do modelo, bem como intervalos de confiança para o custo mínimo do *PCV* com amplitudes relativas bem distintas (ver Tabelas 3 e 4).

Assim as observações relativas ao algoritmo 2 – *optimal* estão associadas a estimativas do parâmetro de escala pelo menos duas vezes superiores às obtidas pelo algoritmo 3 – *optimal*. E, embora os resultados das execuções dos algoritmos não pareçam ser

provenientes de uma população exponencial bi-paramétrica,[9] os resultados referentes ao algoritmo 3 – *optimal* estão associados a estimativas do parâmetro de forma em torno de 1.5, ao passo que os resultados do algoritmo 2 – *optimal* estão associados a estimativas desse parâmetro que excedem as duas unidades.

	2-optimal			3-optimal		
Estimativas	Localização	Escala	Forma	Localização	Escala	Forma
MV	21403.287	1468.927	2.275	21261.787	593.718	1.646
Zanakis	21420.297	1475.598	2.341	21285.436	612.865	1.468
WBE	21220.674	1688.664	2.641	21262.420	581.948	1.671
Mínimo	21426.914			21285.438		

Tabela 3 — Estimativas pontuais obtidas com base em 100 execuções dos algoritmos 2 e 3 – *optimal*

É importante referir que Morais (1998) constatou que, para o *PCV standard* definido sobre a mesma centena de pontos, os resultados do algoritmo 3 – *optimal* parecem ser exponencialmente distribuídos (as estimativas obtidas para o parâmetro de forma estão muito próximas da unidade) enquanto que os concernentes ao algoritmo 2 – *optimal* são demarcadamente não exponenciais (tais estimativas estão próximas de 2). Este comportamento distinto deve-se essencialmente à introdução da variação acima descrita no problema das 100 cidades de Krolak *et al.* (1998) e ao facto de qualquer das execuções se iniciar com a geração (pseudo-)aleatória de um percurso cujos extremos são os pontos 1 e 63.

Os três tipos de estimativas pontuais do custo óptimo do *PCV* pouco se distinguem quando é utilizado o algoritmo 3 – *optimal*, devendo-se isto à regularidade dos resultados que serviram de base ao cálculo de tais estimativas. Mas o mesmo não acontece com a utilização do algoritmo 2 – *optimal*. Com efeito, ao utilizar o algoritmo 2 – *optimal*, destaca-se de imediato a estimativa de Wyckoff-Bain-Engelhardt do grupo de estimativas do parâmetro de localização; à partida, julgava-se que ela subestimava excessivamente o custo óptimo do *PCV*, no entanto, por se encontrar mais próxima das estimativas obtidas recorrendo ao algoritmo 3 – *optimal*, é a mais razoável das estimativas do referido parâmetro desconhecido quando se utiliza o algoritmo 2 – *optimal*.

Na Tabela 4 figuram as amplitudes relativas dos seis intervalos de confiança para o custo da solução óptima do *PCV*, estando o primeiro e o segundo grupos de três estimativas intervalares associados aos níveis de confiança originais $\left(1-e^{-100}\right)\times 100\% = 100.000\%$ e $(1-\alpha)\times 100\% = 95\%$, respectivamente. Esta tabela permite afirmar que, ao transitar do algoritmo 2 – *optimal* para o algoritmo 3 – *optimal*, ocorre uma clara redução da amplitude relativa de qualquer dos intervalos de confiança, tal como previam Golden e Alt (1979) e se refere em Lawler *et al.* (1985), pag. 249. Estas reduções têm a sua razão de ser: as amplitudes relativa e absoluta dos intervalos de confiança apresentados na subsecção 2.2 são funções

9 Esta população corresponde à *Weibull* de mínimos tri-paramétrica com parâmetro de forma unitário.

crescentes das estimativas dos parâmetros de dispersão ou forma, e as estimativas destes parâmetros são menores quando se utiliza o algoritmo 3 – *optimal*. Acrescente-se ainda que as amplitudes relativas dos intervalos de confiança para os resultados do algoritmo 3 – *optimal* levam a crer que o custo mínimo aqui obtido será dificilmente melhorado (o que é coerente com o resultado de optimalidade de Crowder e Padberg, 1980), não fazendo pois sentido prolongar o processo de obtenção de soluções aproximadas.

	Algoritmo	
Amplitudes relativas dos IC's de	**2-optimal**	**3-optimal**
Golden-Alt	0.068555	0.027893
Golden-Alt-Zanakis	0.068867	0.028793
Golden-Alt-Wyckoff-Bain-Engelhardt	0.078810	0.027340
Los-Lardinois	0.014666	0.003312
Los-Lardinois-Zanakis	0.015393	0.002640
Los-Lardinois-Wyckoff-Bain-Engelhardt	0.020884	0.003348

Tabela 4 — Amplitudes relat. dos IC's para o custo óptimo após 100 exec. dos algorit. 2 e 3 – *optimal*

Ao efectuar-se os testes de ajustamento referidos no início desta secção, obtêm-se *p – values* bastante superiores a qualquer dos níveis usuais de significância — 1%, 5% e.10% — como tal não se deve rejeitar as hipóteses de os dados serem provenientes de populações *Weibull* de mínimos.

	2-optimal		**3-optimal**	
Dist. conjecturada	Valor obs. da estat. de teste	p-value	Valor obs. da estat. de teste	p-value
Weibull-MV	0.065317	0.787080	0.056754	0.904126
Weibull-Zanakis	0.085138	0.463233	0.070050	0.710409
Weibull-WBE	0.077923	0.578266	0.064787	0.795311

Tabela 5 — Resultados do testes de ajustamento com 100 execuções dos algoritmos 2 e 3 – *optimal*

Termina-se referindo que este trabalho constitui mais uma achega à aplicação da abordagem estatística ao *PCV*, a acrescentar aos estudos de autores como Golden (1977), Golden e Alt (1979) e Morais (1998); e reafirmando que os algoritmos 2 e 3 – *optimal* conduzem a resultados distintos, quanto à localização, dispersão, forma e qualidade das estimativas pontuais e intervalares aqui apresentadas, tal como constatou Morais (1998), aquando da análise do problema *standard* das 100 cidades de Krolak *et al.* (1971).

Agradecimentos

Agradeço ao Prof. Orestes Cerdeira o *software* que gentilmente cedeu para obter os ciclos 2 e 3 – *optimais*, e à minha colega Dra. Conceição Amado a disponibilidade em trocar impressões nas alturas mais inoportunas.

Bibliografia

[1] P.A. Bruijs, On the quality of heuristic solutions to a 19×19 quadratic assignement problem, *European Journal of Operational Research*, **17**, 21-30, 1984.

[2] J.O. Cerdeira, *Determinação Estatística de Minorantes para o Problema de Steiner*, Nota N° 8/86, Departamento de Estatística e Investigação Operacional — Faculdade de Ciências de Lisboa, 1986.

[3] H. Crowder e M.W. Padberg, Solving large-scale symmetric travelling salesman problems to optimality, *Management Science*, **26**, 495-509, 1980.

[4] M. Engelhardt e L.J. Bain, Simplified statistical procedures for the Weibull or extreme-value distributions, *Technometrics*, **19**, 323-331, 1977.

[5] M.R. Garey e D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1978.

[6] B.V. Gnedenko, Sur la distribution limite du terme maximum d'une série aléatoire, *Ann. Math.*, **44**, 607-620, 1943.

[7] B.L. Golden, A statistical approach to the TSP. *Networks*, **7**, 209-225, 1977.

[8] B.L. Golden e F.B. Alt, Interval estimation of a global optimum for large combinatorial problems. *Naval Research Logistics Quaterly*, **26**, 69-77, 1979.

[9] D.J. Gonsalvez, N.G. Hall, W.T. Rhee e S.P. Siferd, Heuristic solutions and confidence intervals for the multicovering problem, *European Journal of Operational Research*, **31**, 94-101, 1987.

[10] P.D. Krolak, W. Felts e G. Marble, A man-machine approach toward solving the traveling salesman problem, *Communications of the ACM*, **14**, 327-334, 1971.

[11] E.L. Lawler, J.K. Lenstra, A.H.G. Rinnooy Kan, D. Shmoys (ed.), The Traveling Salesman Problem: A Guide Tour of Combinatorial Optimization, John Wiley & Sons, 1985.

[12] S. Lin e B.W. Kernighan, An effective heuristic algorithm for the traveling-salesman problem, *Operations Research*, **21**, 498-516, 1973.

[13] M. Los e C. Lardinois, Combinatorial programming: statistical optimization and the optimal transportation problem, *Transportation Res. Part B*, **16**, 89-124, 1982.

[14] K.L. McRoberts, *Optimization of Facility Layout*, Ph.D. Thesis, Iowa State University of science and Technology, Ames, Iowa, 1966.

[15] M.J.C. Morais, PCV: um velho problema revisitado estatisticamente. Aceite para publicação em *Actas da V Conferência do CEMAPRE* (Lisboa, 26-28 Maio 1997), 1998.

[16] H. Rockette, C.E. Antle e L.A. Klimko, Maximum likelihood estimation with the Weibull model, *Journal of the American Statistical Society Association*, **69**, 246-249, 1974.

[17] F.J. Vasko e G.R. Wilson, An efficient heuritic for large set covering problems. *Naval Research Logistics Quaterly*, **31**, 163-171, 1984.

[18] J. Wyckoff, L.J. Bain e M. Engelhardt, Some complete and censored sampling results for the three-parameter Weibull distribution, *Journal of Statistical Computation and Simulation*, **11**, 139-151, 1980.

[19] S.H. Zanakis, A simulation study of some simple estimators for the three-parameter Weibull distribution, *Journal of Statistical Computation and Simulation*, **9**, 101-116, 1979.

Métodos Matemáticos para pesquisa de Informação na Internet

J. Ferreira

Departamento de Matemática
Instituto Superior de Engenharia de Lisboa

Sumário: O artigo aborda o problema da pesquisa da informação, no maior sistema de informação existente, a Internet, na perspectiva dos modelos matemáticos usados para o efeito.

1 Introdução

O Homem encontra-se em plena Idade da Informação! Devido às novas tecnologias e em especial à Internet, hoje em dia, a quantidade de informação disponível tem vindo a aumentar de uma forma exponencial. Este aumento deve-se à facilidade com que se acede e se guardam documentos na Internet. Esta situação cria-nos o problema de encontrar a informação pretendida num volume incrivelmente grande! Este problema é abordado em duas vertentes:

- Dado um conjunto de interesses estáveis (perfis) os utilizadores são automaticamente informados de nova informação relevante, (filtragem de Informação).
- Dada uma necessidade de informação os utilizadores vão expressá-la numa 'pergunta' e um sistema irá tentar encontrar os documentos relevantes numa base de dados não estruturada, (pesquisa de informação).

Este problema, devido à complexidade e subjectividade da linguagem Humana está longe de estar resolvido e é um dos pontos onde se tem despendido mais esforço no sentido de desenvolver as técnicas e estratégias para suprir o problema. Abordagem é estruturada em sete Pontos, nos quais se aborda o estado da arte da pesquisa e filtragem da informação:

- Ponto 2: Fundamentos dos sistemas de pesquisa de informação, onde se faz uma analise de blocos dos sistemas de pesquisa;
- Ponto 3: Representação de documentos (Indexação) e 'perguntas'. Processos automáticos, semi-automáticos e manuais de criação de representativos. Métodos para normalizar o espaço dos representativos. Técnicas para guardar\manipular os representativos criados que permitam um acesso rápido e eficaz;
- Ponto 4: Pesquisa, métodos de comparação. São descritos os métodos mais usados para encontrar os documentos relevantes. Estudo da retroação (*"feedback"*) do utilizador;
- Ponto 5: Métodos de avaliação do grau de satisfação proporcionados pelos sistemas de pesquisa;
- Ponto 6: Sistemas e aplicações na Internet, sistemas de pesquisas e de filtragem;
- Ponto 7: Conclusões.

2 Fundamentos

Os sistemas de pesquisa são caracterizados pelos blocos abaixo representados (figura 1). Teremos um repositório de informação onde são guardados os documentos nos mais variados formatados constituindo um espaço heterogéneo de informação. O conteúdo deste espaço é indexado (1) por forma a criar um espaço de menor dimensão representativo do inicial onde se farão as pesquisas de acordo com os métodos em questão.

Os interesses dos utilizadores são representados por um conjunto de palavras (termos) as quais após a devida expansão e normalização de termos se vão comparar com os representativos dos documentos (2) através dum modelo de comparação estabelecido. Os sistemas podem ainda incluir mecanismos que utilizem a retroação (3) dos utilizadores aos resultados da pesquisa, como forma de a melhorar. Dos documentos que o sistema mostra como relevantes o utilizador escolhe os que vai consultar à base de dados dos documentos.

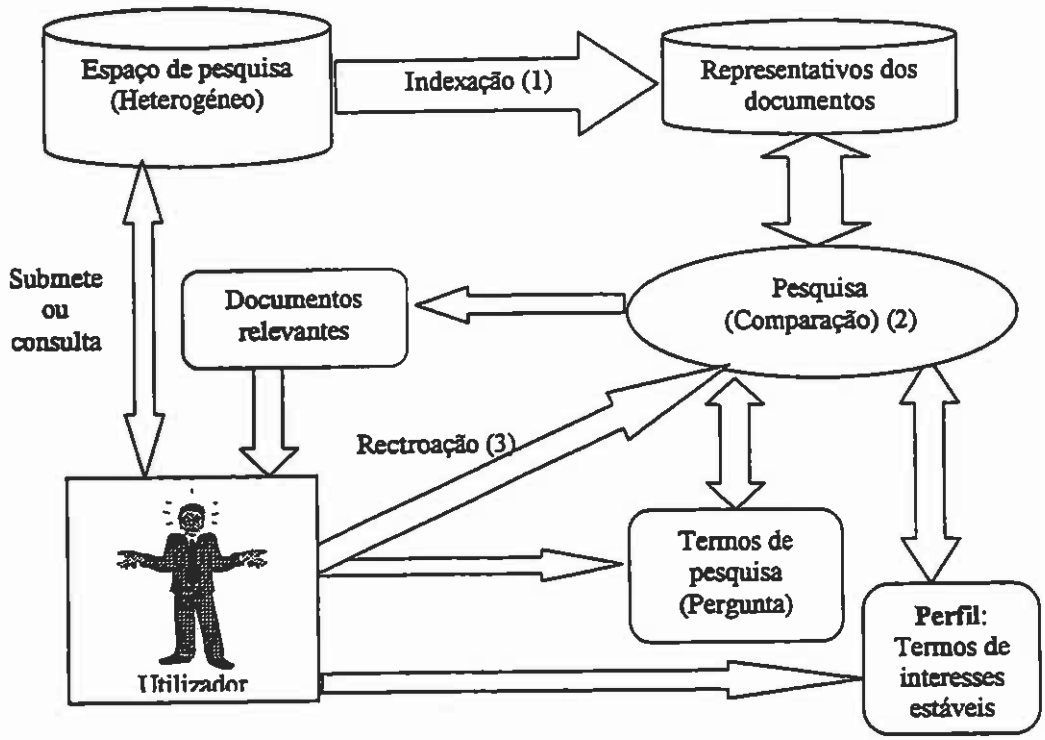


Figura 1: Diagrama dos blocos principais de um sistema de pesquisa de informação.

3 Indexação

Dado o volume de informação existente o primeiro passo é arranjar métodos para representar os documentos reduzindo assim o seu tamanho a um conjunto de termos mínimo que o representem na sua plenitude e que possa ser tratado pelo computador (Indexação). O processo de indexação vai ter em conta o modelo de comparação usado. Uma "boa indexação" cria uma representação que permite uma melhor distinção entre os documentos.

3.1 Mecanismos automáticos

Num processo automático de indexação os representativos são criados de uma forma automática sem qualquer intervenção Humana. Este método baseia-se nos seguintes conjunto de técnicas:

- Remoção das palavras não significativas (consoante a língua existe uma lista predeterminada de palavras). Estas palavras em geral aparecem com uma frequência elevada em todos os documentos.
- Derivação das raízes semânticas das palavras. Neste método pretende-se reduzir as palavras a sua formula mais simples, para posterior comparação. Este método chama-se concatenação.
- Frequência das palavras:
  Técnica existentes para determinar a relevância de um termo num documento.
  A frequência de ocorrência dum termo num documento fornece uma ideia do grau de importância do termo, sendo um factor importante para extrair os termos representativos dos documentos. Os estudos efectuados em documentos mostram que o ordenamento multiplicado pela frequência dos termos é constante (regra de Zipf's). Assim os termos considerados têm uma frequência inferior ao de uma frequência de corte superior e superior a uma frequência de corte inferior.
  Os conceitos mais importantes são:
  - Quantas vezes um termo aparece num documento (f_{ij} – frequência do termo j no documento i).
  - Quantos documentos contém o termo (d_j – numero de documentos que contém o termo j).
  - Número total documentos na colecção N.

  A partir destas definições básicas podem-se derivar outras, nas quais se tenta aferir a importância ou peso do termo em relação aos restantes termos tendo em conta a colecção existente. A diversidade de

definições é grande [1] irá apenas ser referida a mais usada, peso do termo j no documento i que a seguir se apresenta;

$$W_{ij} = f_{ij}\,(log(N/d_j) \quad (1)$$

Esta medida mede o peso deste termo na colecção existente, ao seja um termo é tanto mais relevante quanto menos vezes aparecer noutros documentos da colecção.

A aproximação automática pode ser baseada em termos simples ou múltiplos;

- Termos simples:
  O documento é analisado e são identificadas e retiradas as palavras sem significado (lista predefinida, função da língua em causa). O conjunto de palavras existentes são reduzidas na sua forma mais simples pela remoção dos sufixos, através dum conjunto de algoritmos de concatenação. Estes termos identificados serão contados o numero de vezes que aparecem num documento e guardados num vector.
  O mesmo procedimento é feito para o conjunto dos documentos existentes.
- Termos múltiplos (frases):
  O processo é verificar o numero de vezes que determinados termos aparecem juntos.

$$Coesão(i,j) = Cons\tan te\,\frac{f_{(i,j)}}{f_i \cdot f_j} \quad (2)$$

$f_{(i,j)}$ frequência que os termos i e j aparecerem juntos. $f_{i/j}$ frequência do termo *i/j*.

3.2 Método semi-automático ("*metadata*")

A 'metadata' serve para produzir uma descrição, em formato normalizado, de um documento no momento da sua submissão. Para além da descrição outros campos podem ser preenchidos permitindo outro tipo de pesquisa (ex. Autor, data do documento, etc). O campo de descrição, quando preenchido pelo autor, é uma informação importante a qual pode ser usada na indexação para representação do documento de uma forma semi-automática.

3.3 Método manual

Esta aproximação consiste na criação dos representativos apenas com a intervenção humana. A qualidade desta aproximação manual é superior à automática, mas devido à quantidade de documentos existente esta abordagem torna-se impraticável e dispendiosa.

3.4 Normalização do espaço

Outro aspecto importante na indexação é o controle dos termos usados para representar os documentos tendo em conta que existem diversas palavras para representar o mesmo conceito e que o significado das palavras varia consoante o contexto. Uma forma de minimizar o efeito deste problema complexo é usar as técnicas de pré-coordenação ou pós-coordenação, na qual os termos usados para representar os documentos advenham dum vocabulário controlado. É habitual substituir termos por outros equivalentes, sendo esta relação de equivalência estabelecida por 'thesaurus' ou por sistemas de classificação específicos de cada assunto ou tema. Na pré-coordenação este processo é executado com o processo da indexação e na pós-coordenação é realizado no momento da pesquisa. Aplicações destes métodos demostram que quando aplicados em domínios específicos aumentam a eficiência do sistema de pesquisa sendo uma área onde actualmente se desenvolvem grandes esforços. A existência de sistemas de classificações em varias línguas permite a pesquisa de informação nessas línguas pela equivalência de termos dos mesmos níveis nas diferentes linguagens disponíveis.

3.5 Processamento de representativos.

Serão analisados os diferentes métodos usados para criar um espaço de indexação que permita guardar, manipular os representativos dos documentos criados pela indexação dos documentos originais que permitam um acesso rápido e eficaz durante o processo de comparação com as perguntas.

3.5.1 Agrupamento ("*clusteres*")

Cada documento é representado por um vector num espaço vectorial de dimensão *n*, que reflecte o seu conteúdo, ou seja, os termos que o compõem. O conjunto de vectores *t* pode dar origem a uma matriz *n.t.*

Com o objectivo de reduzir o tempo de pesquisa, estes vectores são agrupados de acordo com as suas semelhança e identificado o vector central do grupo que será usado na pesquisa (ver método vectorial 4.2). os grupos são formados pelo conjunto de documentos semelhantes, sendo esta similaridade dada por:

$$Cos(D_i, D_j) = \frac{\sum_{k=1}^{n} d_{ik} . d_{jk}}{\sqrt{\sum_{k=1}^{n} (d_{ik})^2 . \sum_{k=1}^{n} (d_{jk})^2}} \quad (3)$$

Sempre que este valor for superior a um determinado valor previamente definido o conjunto de documentos nestas circunstancias formam um agrupamento. Este conceito vai permitir acelerar a pesquisa, restringindo o espaço de pesquisa. O valor para o qual se define um grupo é empírico, depende em geral do tamanho da colecção.

Esta determinação de grupos requer um número de comparações proporcional ao quadrado do numero total de documentos na colecção sendo difícil controlar a sobreposição das fronteiras entre os diversos grupos. Estes grupos estão na origem dos catálogos e na pesquisa por temas, sendo este um método automático. Tendo em vista os mesmos conceitos muitas vezes estes catálogos e grupos são determinados manualmente como forma de garantir maior qualidade. Como exemplo disto temos o Yahoo, um dos serviços com mais sucesso na Web, no qual a pesquisa é realizada dentro de determinados tópicos.

3.5.2 Inversão

Este é o método mais usado nos sistema comerciais devido à sua rapidez. O conjunto de termos

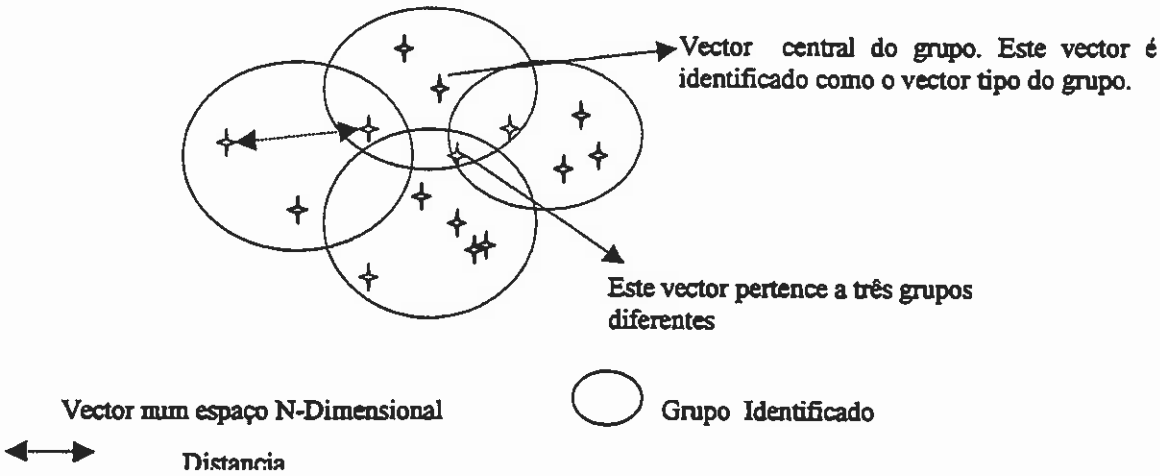


Figura 2: Visualização da criação de grupos num espaço N-dimensional de documentos.

representativos dos documentos são guardados por ordem alfabética num ficheiro indexado onde cada termo tem uma lista de apontadores para os documentos onde este termo é representativo. Os métodos mais sofisticados utilizam B-trees, hashing ou combinações ou variações destes métodos. Como vantagem temos a rapidez, a facilidade com que é implementado e se pode a posterior estabelecer sinónimos. Como desvantagens temos o espaço que ocupa e o tempo despendido para a introdução de novos termos na estrutura.

3.5.3 Assinatura

Os documentos são transformados numa sequência de bits ou assinatura através da utilização de funções hash sobre a codificação dos termos. O ficheiro resultante é mais pequeno e as operações de pesquisa são mais rápidas. Este método apresenta vantagens quando se trabalha com documentos grandes.

4 Pesquisa de informação

Dado uma necessidade de informação por parte do utilizador, pretende-se representar essa necessidade por uma pergunta ao sistema e posteriormente compara-la com os representativos dos documentos com a representação da pergunta formulada. Ao contrario das base de dados, nos sistemas de pesquisa há uma

falta de precisão na representação dos documentos e perguntas dos utilizadores, devido à natureza do problema. Vamos considerar como forma de reduzir o impacto deste problema, o uso de "*thesaurus*" e de sistemas de classificação (já referido em 3.4), e a utilização do retroação dada pelo utilizador (4.3).

4.1 Pergunta

É a forma como se representa o desejo de informação de um utilizador e depende do método de comparação que o sistema usa, podendo-se dividir em duas grandes classes:

- Linguistico: No qual se pretende que o utilizador use a sua própria linguagem, para formular a pergunta ao sistema. Este método requer um sistema complexo de tratamento da pergunta e propõe como modelo de comparação com base num sistema de linguagem natural. Computacionalmente este método é bastante pesado pois requer um grande número de condições linguísticas para processar, nomeadamente ao nível da sintáctica e semântica.
- Estatístico: Tem como base os sistemas estatísticos construídos com base na frequência de termos. Neste método o utilizador tem que fazer um esforço adicional ao expressar a sua necessidade de informação especificando um conjunto de termos que julgue descrever os seus interesses. Se o método de comparação for o modelo boleano o utilizador terá que associar os termos utilizando um conjunto de relações lógicas $(\wedge,\vee,\sim)$. Estes termos serão tratados por forma a possibilitar a sua expansão e normalização para posterior comparação.

4.2 Métodos de comparação

O objectivo dos métodos de comparação criados é definir um conjunto de regras para comparar os termos representativos dos documentos com os das perguntas e assim encontrar um conjunto de documentos que satisfaçam a necessidade de informação expressada na pergunta.

4.2.1 Métodos Gerais

4.2.1.1 Boleano

Embora não seja o método que produz melhores resultados é o método mais usado nos sistemas comerciais existentes. A pergunta é feita com um conjunto de termos ligados através das preposições lógicas $(\wedge,\vee,\sim)$ e o sistema vai procurar documentos onde se encontram estes termos de acordo com as preposições lógicas usadas. Um dos principais problemas deste método é a quantidade enorme de documentos que devolve sem qualquer ordem. O modelo de Fuzzy tenta resolver este problema, com a introdução de operadores lógicos para incluir associação parcial dos termos a classes.
Outro aspecto a considerar é que os utilizadores por vezes tem dificuldade em usar a lógica.

4.2.1.2 Vectorial

Cada documento é representado por um vector num espaço N-dimensional $D_i = (d_{i1},...,d_{in})$ onde são guardados os pesos de cada termo. Um documento é relevante para uma determinada pergunta se for superior a um determinado nível previamente definido:

$$Cos(D_i,q_j) = \frac{\sum_{k=1}^{n} d_{ik}.q_{jk}}{\sqrt{\sum_{k=1}^{n}(d_{ik})^2.\sum_{k=1}^{n}(q_{jk})^2}} \qquad \begin{array}{l} d_{ik} - \text{peso do termo k no doc.i} \\ q_{jk} - \text{peso do termo k na perg. j} \end{array} \qquad (4)$$

Para evitar a comparação dum pergunta com todos os documentos (exigia grande capacidade computacional) faz-se a comparação com os elementos centrais dos grupos de documentos previamente identificados e depois de identificado só dentro desse grupo é que se vão efectuar as comparações. Para um grupo k contendo m documentos o elemento central é:

$$c_j = \frac{1}{m}\sum_{i=1}^{m} d_{ij} \qquad \text{com } D_i \in k \qquad (5)$$

Assume-se que os diferentes termos são ortogonais, ignorando a possível relação entre os termos. Embora computacionalmente mais pesado este método apresenta a vantagem de ordenar os resultados e permitir englobar a retroação do utilizador a uma pergunta feita.
Embora o coseno seja a medida de comparação mais usual, com base neste modelo (vectorial) podemos generalizar obtendo a seguinte expressão de comparação:

$$L_p(D_i,D_j)=\left(\sum_k |d_{ik}-d_{jk}|^p\right)^{1/p} \qquad \text{com } 1\le p\le\infty \tag{6}$$

Para p=2 temos o coseno, para $p=\infty$ temos um comportamento equivalente ao modelo Boleano.

4.2.1.3 Métodos Probabilisticos

Este método tem em conta a relação existente entre os termos. O modelo baseia-se na premissa que os documentos para pesquisa, são aqueles em que, a probabilidade de serem relevantes para uma pergunta é elevado.
No calculo da probabilidade de um documento ser relevante para uma pergunta, quase toda a formulação matemática é baseada no teorema de Bayes.

$$P(w_i/d)=\frac{P(d/w_i)P(w_i)}{P(d)} \qquad i=1,2 \tag{7}$$

$d=(d_1,d_2,...,d_n)$ vector representativo do documento binário $d_i=0\vee 1$ e w_1 = doc. relevante e w_2 =doc. não relevante.
Se os termos forem estocatiscamente independentes vem que:

$$P(d/w_i)=P(d_1,w_i)P(d_2,w_i)..P(d_n,w_i) \tag{8}$$

considerando $p_i=P(d_i=1/w_1)$ e $q_i=P(d_i=1/w_2)$ vem que a relevância dum termo i é dada por:

$$t_i=\log\left(\frac{p_i(1-q_i)}{q_i(1-p_i)}\right) \tag{9}$$

Sendo

	Relevante	Não − Relevante	
$d_i=1$	r	$n-r$	n
$d_i=0$	$R-r$	$N-n-R+r$	$N-n$
	R	$N-R$	N

Assim $p_i=\frac{r}{R}$ e $q_i=\frac{n-r}{N-R}$. Donde vem que:

$$t_i=\log\left(\frac{r/(R-r)}{(n-r)/(N-n-R+r)}\right) \tag{10}$$

O peso do termo i pode ser simplificando, com base na premissa de que o conjunto de documentos relevantes é pequeno comparado com o tamanho da colecção. A probabilidade de ser relevante p_i é assim assumida como constante. Assim a expressão (10) fica reduzida a:

$$t_i=\log\left(\frac{N-R-n+r}{n-r}\right) \tag{11}$$

Como o conjunto de documentos não relevante é aproximadamente igual ao tamanho da colecção N, a probabilidade de não relevância é igual a probabilidade de ocorrência do termo i em toda a colecção, (n_i)

Donde temos que $t_i = \log\left(\frac{N-n}{n}\right) + c$, onde c é uma constante. Este peso é a frequência inversa dum termo, expressão equivalente a (1) onde $n = d_i$ número de vezes que o termo i apareceu no documento.

4.2.2 Métodos, com base num espaço de conceitos previamente definido.

Tendo em vista a normalização dos termos, os métodos abaixo descritos usam um espaço controlado de termos (conceitos) para proceder à comparação, permitindo assim diminuir a dimensão do espaço vectorial e tentar resolver o problema da diversidade de termos empregues com o mesmo significado.

4.2.2.1 Métodos vectoriais/matricial

4.2.2.1.1 Indexação Latente Semântica - LSI ("*Latent Semantic index*")

Para diminuir a dimensão dos espaço vectoriais considerados este método permite a introdução de uma lista controlada de palavras com cariz semântico. Os termos retirados da indexação são projectados num espaço vectorial de dimensão menor. Esta projecção é baseada no método matricial da decomposição singular dos valores (SVD- *Singular Value Decomposition*), técnica relacionada com decomposição de valores próprios. Seja a matriz $X_{t.d}$ (t-linhas que representam os termos e d-colunas que representam cada um dos documentos) em que t>>d, com colunas linearmente independentes e característica *r*. A SVD de $X_{t.d}$ é definida como:

$$X_{t.d} = T_{t.r} S_{r.r} V^T_{r.d} \tag{12}$$

Onde S é uma matriz diagonal com valores próprios positivos ordenados por ordem decrescente ao longo da diagonal principal $S = diag(s_1,...,s_r)$ e as matrizes T e V são vectores próprios.

Pelo Teorema de Echart e Young se $k \le r = p$ a diferença entre as duas matrizes é dada pela seguinte norma:

$$\|X - X_k\|_k^2 = s_{k+1}^2 + ... + s_p^2 \tag{13}$$

onde s_i são os valores próprios de S ordenados por ordem decrescente. A técnica LSI consiste em reconstruir a matriz X eliminando os valores próprios mais pequenos, pois o erro que se comete é pequeno (8). Sendo k a dimensão do sub-espaço que se quer considerar

$$X_k = T_k S_k V_k^T \tag{14}.$$

As perguntas também são projectadas para este sub-espaço no qual se efectuara a comparação:

$$q_k = qT_k S_k^{-1} \tag{15}$$

onde qT_k representa a projecção no sub-espaço e S_k^{-1} a diferença de pesos das duas dimensões.

Assim teremos um espaço conceptual *k* onde $TS^{½}$ representa a projecção dos termos no sub-espaço e respectiva mudança de escala. T representa a projecção e $S^{½}$ a diferença de pesos nas duas dimensões, fazendo a mudança de escala. $VS^{½}$ representa a projecção do espaço vectorial dos documentos duma dimensão d para r e a respectiva mudança de escala.

4.2.2.1.2 Função de mapeamento LLSF (Linear Least Squares Fit)

Este método utiliza um conjunto de documentos que são classificados manualmente. A partir deste trabalho vai-se construir uma função que uma vez aplicada a um representativo de um documento ou a perguntas identifique as categorias de palavras relacionadas com esse documento. Seja A a matriz dos vectores de todos os documentos e B a matriz das categorias o método consiste em determinar uma matriz F que minimize o erro na passagem de A para B. O erro é:

$$\sum_{i=1}^{m}\left\|\vec{e}_i\right\|_2^2 = \left\|F\vec{a}_i^T - \vec{b}_i^T\right\|_2^2 = \left\|FA^T - B^T\right\|_F^2 \qquad (16)$$

onde $F = B^T\left(A^+\right)^T$ e pelo método SVD aplicado a matriz A, fica $F = B^T TS^{-1}V^T$. A transformação F é uma matriz de associação termos categorias onde as colunas são os termos no espaço inicial e as linhas as categorias no espaço resultante.
Qualquer conjunto de termos x pode ser projectado no espaço de conceitos considerado através da transformação F:

$$y = \left(Fx^T\right)^T \qquad (17)$$

4.2.2.2 Métodos probabilisticos

4.2.2.2.1 Redes Neuronais

As redes Neuronais utilizam principalmente os métodos de activação expansiva, como forma de expandir o vocabulário de pesquisa de acordo com o contexto e assim complementar o conjunto de documentos seleccionados. São exemplo deste método a construção de "*thesaurus*".
A técnica usual é construir, manualmente ou automaticamente, dicionários de termos que especifiquem relações entre termos, ou dicionários de palavras que contenham definições e outra informação referente aos termos usados. Nesta expansão são estabelecidas relações entre os documentos. A dificuldade deste método consiste na determinação das relações ou associações que realmente permitem melhorar os resultados da pesquisa. Este método tem sido bem sucedido em domínios especializados. As técnicas de expansão baseiam-se na existência de funções que especificam as relações particulares entre termos e conceitos
Os documentos ou termos são representados por nós numa rede e as relações etiquetadas por arcos entre os nós. Neste modelo de activação expansiva o processo começa por colocar um peso inicial num nó (determinado empiricamente) e os pesos resultantes são resultados de aplicação de técnicas probabilisticas. A mesma rede é constituída para as perguntas. A ligação entre estas duas redes é estabelecida ao nível dos conceitos.

4.2.3 Linguagem natural

Existem vários métodos que empregam a linguagem natural como forma de pesquisa. Estes métodos em geral produzem melhores resultados que os métodos descritos anteriormente só que são difíceis de implementar devido ao elevado numero de condições e relações a considerar. A ideia básica deste método é implementar um conjunto de mecanismos complexos que permitam descobrir a estrutura semântica e sintáctica de um documento, os processos de língua natural (*NLP- "Natural Language Processing"*).

4.3 Retroação do utilizador

A retroação do utilizador em relação aos resultados da pesquisa é uma informação importante que pode ser usada para alterar a representação das perguntas e documentos. O conceito consiste em estabelecer um dialogo entre o sistema e o utilizador a partir das reacções do utilizador aos resultados da pesquisa. Este dialogo pode ser a dois níveis (documentos relevantes e não relevantes) ou de vários níveis, no qual o utilizador estabelece graus de relevância relativa entre os documentos. O modelo vectorial é o que apresenta maiores facilidades na aplicação de algoritmos de retroação usando a informação dos utilizadores para melhorar futuras respostas do sistema. Este processo de retroação é interactivo, o qual deve ter no máximo três a quatro ciclos de interacção e deve apresentar melhorias de uns ciclos para outros, sob pena de o utilizador desistir desmotivado.
A modificação da pergunta:

- Dos pesos dos termos. O retroação positivo pode aumentar o peso dos termos considerados enquanto que o negativo terá o efeito oposto. Esta técnica só e valida em sistemas que permitam pesos de termos diferentes;
- Da expansão dos termos da pergunta pela introdução de termos seleccionados dos documentos com retroação positivo. Pode ser pelo uso de *"thesaurus"* ou por associação de novos termos encontrados

nos documentos considerados relevantes. O mesmo processo de remoção aplica-se ao processo de retroação negativo;
- Da divisão dos termos da pergunta em grupos de acordo com o retroação positivo dado.

Modificação ao nível da representação dos documentos:
- Os vectores que representam o documentos são reajustados, os quais vão originar novos grupos de documentos e novos pesos nos termos. Devido à subjectividade dos utilizadores este método deve introduzir pequenas modificações na representação dos documentos.

No modelo vectorial um dos algoritmos mais usado é o de Rocchio, o qual modifica o peso dos termos da pergunta:

$$Q_1 = Q_0 + \frac{\beta}{n_1} \sum_{\substack{termos \\ relevantes}} d_i - \frac{\gamma}{n_2} \sum_{\substack{termos \\ não-relevantes}} d_i \tag{18}$$

com d_i conjuntos dos termos normalizados que representam o documento, n_1 numero de termos relevantes e n_2 numero de termos não-relevantes. $\beta + \gamma = 1$ e $\beta, \gamma \in [0,1]$

5 Avaliação

Muitos esforços se têm desenvolvido no sentido de medir a eficácia de um sistema de pesquisa e é um problema longe de estar resolvido. Este assunto é coberto pelas seguintes perguntas: Porquê a avaliação? O que avaliar? Como avaliar? A primeira pergunta é uma mera questão social e económica. A segunda pergunta mede-se a capacidade de o sistema satisfazer o utilizador nas suas necessidades de informação e engloba os seguintes pontos:
- O tempo entre a pergunta e a resposta do sistema;
- A cobertura da colecção de documentos;
- A forma como os resultados são apresentados;
- Esforço empregue pelo utilizador para obter os resultados desejados;
- Precisão do sistema, isto é, a percentagem dos documentos obtidos relevantes obtidos, em relação à totalidade dos documentos obtidos nessa operação de pesquisa;
- O "*recall*" é a percentagem dos documentos relevantes, obtidos numa operação de pesquisa em relação a todo o conjunto de documentos relevantes existentes no universo de pesquisa.

Geralmente são estes dois últimos os mais utilizados para medir a eficácia de um método, a precisão e o "*recall*", os quais reflectem a habilidade do sistema para fornecer documentos relevantes em detrimentos dos não relevantes.

$$\text{Precisão} = \frac{Documentos \quad relevantes \quad pesquisados}{Total \quad documentos \quad pesquisados} \tag{19}$$

$$\text{Recall} = \frac{Documentos \quad relevantes \quad pesquisados}{Total \quad documentos \quad relevantes} \tag{20}$$

Enquanto que a pesquisa de um documento aumenta a precisão e o "*recall*", a pesquisa de um documento não-relevante diminui apenas a precisão. A medida exacta do "*recall*" é difícil de obter, pois necessitamos de saber todos os documentos relevantes da colecção, sendo a maior parte das vezes uma medida estatística e portanto imprecisa. Outro aspecto é que o valor destas grandezas depende dos utilizadores e da situação em causa. Quando não se quer perder nenhum documento o recall alto é importante, mas na maior parte das situações os utilizadores preferem uma precisão elevado, pois não desejam encontrar nos resultados da pesquisa documentos não-relevantes. Na maioria dos sistemas estas grandezas têm um comportamento inverso. Se a precisão aumenta, o "*recall*" irá certamente diminuir e vice-versa. É de salientar que a noção de relevante é subjectiva, pois um documento pode ser relevante para um determinado utilizador e não relevante para outro.

A terceira pergunta como avaliar, pode admitir varias respostas técnicas. Dada a extensão do tema não irá ser explorado no presente artigo.

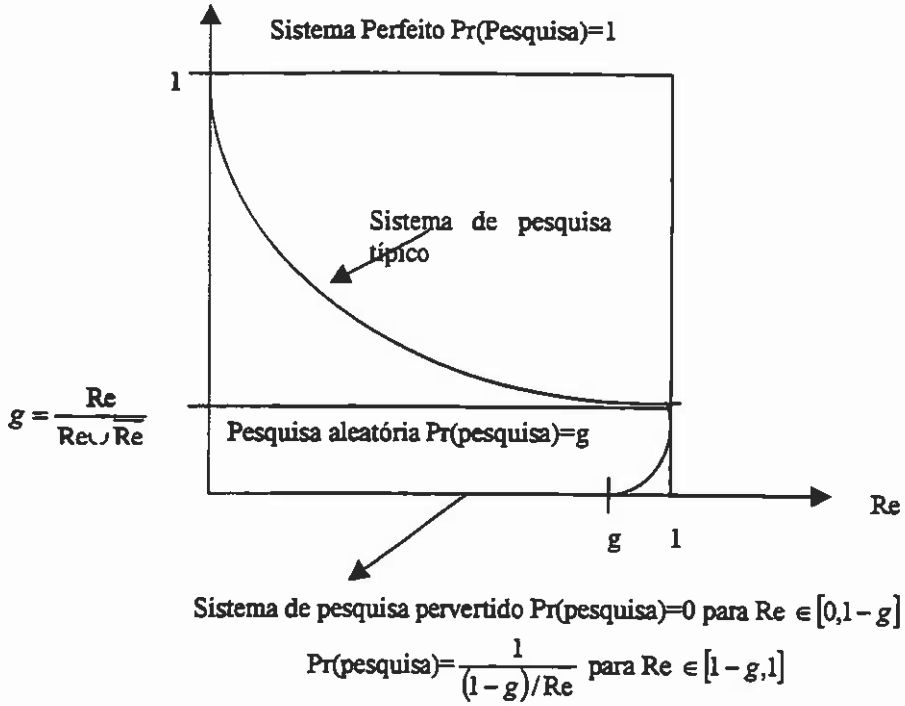


Figura 3: Gráfico da precisão versus 'recall'.

6 Sistemas e aplicações na Internet

6.1 Sistemas de Pesquisa [2]

Muitos dos endereços genéricos de informação na *Internet* têm hoje em dia uma grande quantidade de documentos e/ou outra informação textual. Esta informação torna-se muito mais acessível se existir um sistema de pesquisa que permita encontrar os documentos relevantes para cada utilizador. Assim, os sistemas de pesquisa começaram a ter uma enorme popularidade, existindo mesmo inúmeros endereços na *Internet* com o objectivo praticamente único de facilitar a pesquisa de documentos relevantes. Como exemplos temos o *Yahoo*, o endereço mais visitado da *Internet*, o *Excite*, o *AltaVista*, o *Lycos*, o *Webcraler*, o *Infoseek*, *Hotbot* e muitos outros que se baseiam fundamentalmente em sistemas de pesquisa. Para além destes sistemas comerciais temos sistemas académicos como o *Smart*, *Tapestry*, *Inquery*.

Grande parte dos sistemas comerciais usa o método Boleano sendo a informação guardada em ficheiros invertidos para permitir um rápido acesso. Muitos destes sistemas permitem o acesso a informação distribuída através do uso de mecanismos que visitam os vários endereços e indexam os documentos. Na maior parte dos casos estes mecanismos só consideram o primeiro parágrafo dos documento, pois normalmente ai encontra-se a descrição do documento. A ordenação é feita segundo vários critérios visto usarem um modelo boelano: por exemplo em alguns motores de pesquisa dá-se mais importância aos termos que aparecem nas primeiras linhas, etc. Dos motores comerciais de pesquisa acima referidos apenas o *webcrawler* usa o modelo vectorial. O Smart foi o primeiro sistema construído baseado no método vectorial.

6.2 Filtragem de Informação [3]

Devido ao excesso de informação existente , o numero de sistemas de filtragem tem vindo a aumentar, tendo como objectivo levar a informação correcta às pessoas considerando um conjunto de interesses estáveis. Estes sistemas podem-se dividir em duas categorias principais:

- **Conteúdo:** onde se faz a comparação entre os perfis dos utilizadores e os representativos dos documentos.
- **Colaboração:**
  - Comparação do perfil com outros perfis. Dos perfis mais próximos podem-se tirar, quando existirem, os julgamentos efectuados pelos utilizadores.
  - Comparação do perfil com os perfis tipo das comunidades. Identificação da comunidade a que o utilizador pertence da qual se vai retirar o perfil tipo e assim procurar a informação a enviar ao utilizador (filtragem social).
  - Comparação do perfil com julgamentos explícitos feitos pelos utilizadores em documentos (anotações).

A criação dos perfis pode ser feita duma forma explícita na qual o utilizador introduz um conjunto de termos que julga descreverem os seus interesses. Estes termos serão refinados duma forma implícita usando técnicas de aprendizagem baseados na retroação disponível ou por observação dos comportamentos do utilizador.

Os filtros baseados em conteúdo têm tido apenas sucesso em colecções simples de documentos. O problema principal é a criação eficaz de representativos de documentos num fluxo de informação. Devido a esta complexidade a tarefa é muitas vezes desempenhada por Humanos. Os sistemas colaborativos têm mostrado maior eficiência mas não são capazes de dar informação de documentos que nunca tenha sido lidos e bem como não possui defesas contra utilizadores que dão falsas informações.

Ao longo desta década os sistemas de filtragem têm sido aplicados principalmente a: listas de correio electrónico, relatórios técnicos, noticias de Usenet, robots, música, filmes e vídeo. Hoje em dia estes sistemas estão a ser aplicados a tecnologias emergentes como os jornais personalizados e bibliotecas digitais. Historicamente o primeiro sistema foi o TAPESTRY [4], o qual introduziu a designação de sistemas colaborativos. Este sistema permite duas aproximações, uma automática, baseada no contexto e outra colaborativa. Na tabela 1, é apresentado um sumário de alguns sistemas de filtragem existentes tendo em conta o perfil dos utilizadores e as técnicas de comparação usadas.

Sift e *Newsweeder* são exemplos de sistemas de filtragem (SF) baseado no conteúdo. A grande diferença entre os dois é que o *Newsweeder* usa a experiência passados dos utilizadores para melhor refinar o perfil dos utilizadores. Como exemplo de SF colaborativo temos o *Grouplens*, *Firefly* e *Referralweb* no qual o perfil é comparado com os outros existentes sendo escolhidos os mais próximos.

Perfis				Comparação		
Sistema	**(FI) Fonte de informação**	**Explicito**	**Implícito**	**Técnicas**	**Argumentos**	**Notas**
SIFT (94)	Usenet	lista termos	-	Boleana	(FI) vs (perfil)	Sistema de filtragem (SF)
Grouplens (92)	Usenet	vector numérico	vector numérico (tempo leitura)	Vectorial (coseno)	(perfil) vs (perfis)	SF colaborativo
Newsweeder (94)	Usenet	vector numérico	vector numérico (historia do utilizador)	Vectorial (coseno)	(FI) vs (perfil)	SF baseado no conteúdo
Fab (94)	Web	vector numérico	vector numérico (historia do utilizador)	Vectorial (coseno)	(FI) and (perfis) vs (perfil)	SF colaborativo e baseado no conteúdo
ReferralWeb (94)	Web	referencia a pessoa ou documento			(perfil) vs (perfis-comunidades)	SF colaborativo social
Firefly (94)	Musica, Filmes	vector numérico		Vectorial (coseno)	(perfil) vs (perfis)	SF colaborativo

7 Conclusões

Procurou-se identificar um conjunto de técnicas usadas para resolver o problema da pesquisa de informação. Dada a complexidade do problema existe um conjunto diverso de aproximações sem que haja uma resolução completa do problema.
Duma forma geral nota-se que os sistemas de pesquisa comerciais usam mais o método boleano de comparação enquanto que os sistemas de filtragem usam mais o método vectorial. Isto deve-se à natureza dos sistemas, pois os sistema de pesquisa são executados em tempo real, onde o tempo de resposta é importante e se os resultados não forem muito precisos o utilizador pode reformular a pergunta ou interagir com o sistema. Os sistemas de filtragem correm em batch, informando o utilizador apenas após um evento ou intervalo de tempo definido por este. Neste caso é importante uma precisão mais elevada, pois caso contrario há o risco de o utilizador ficar desmotivado e prescindir do serviço.
Muita da investigação actual faz-se no sentido de encontrar domínios bem definidos para as pesquisas e controlar o vocabulário usado através de "thesaurus" ou lista de autoridades especificas desses domínios. Os sistemas de linguagem Natural apresentam alguns resultados promissores em domínios específicos, mas muito trabalho falta ainda desenvolver.

8 Referencias

[1] - Salton and Buckley. **Term-Weighting Approaches in Automatic Text Retrieval.**

[2] - V.N. Gudivada, V.V.Raghavan, W.I.Grosky and R. Kasanagottu. **Informatiom Retrieval on the World Wide Web**, IEEE Internet Computing, September 1997, 58-66.

[3]- J.Ferreira, J.L.Borbinha, , J.Jorge e J. Delgado. **Using LDAP in a Filtering Service for a Digital Library**, publicado e apresentado no quinto Delos workshop em Budapeste, 10-12 Novembro 1997.

[4] - Foltz, P.W. and Dumais, S.T. **Personalized Information Delivery: An Analysis of Information Filtering Methods.** Communication of ACM, December 1992, Vol. 35, N 12.

[5] –J.L.Borbinha, J.Ferreira, J.Jorge e J. Delgado. **A Digital Library for a Virtual Organization**, publicado na HICSS-31, Hawai, Janeiro 1998.

Novas Orientações na Aplicação da Matemática em Engenharia

Fernando Sousa Pedro Félix

Centro de Cálculo do Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 – 1900 Lisboa
{fsousa, felix}@cc.isel.pt

Resumo

No presente trabalho tratam-se aspectos inerentes ao desenvolvimento de sistemas de comunicação segura. Analisam-se as componentes de codificação de fonte, cifra e codificação de canal, salientando a sua modelação matemática.

A importância desta formulação num contexto matemático, é realçada através das soluções que ela permite: trata-se de aplicações que ilustram novas orientações na aplicação da matemática em engenharia.

1. Introdução

No Centro de Cálculo do Instituto Superior de Engenharia de Lisboa, tem vindo a ser desenvolvida actividade de investigação e desenvolvimento na área das comunicações digitais seguras. A figura 1 representa esquematicamente a estrutura de blocos dessa classe de sistemas [12].

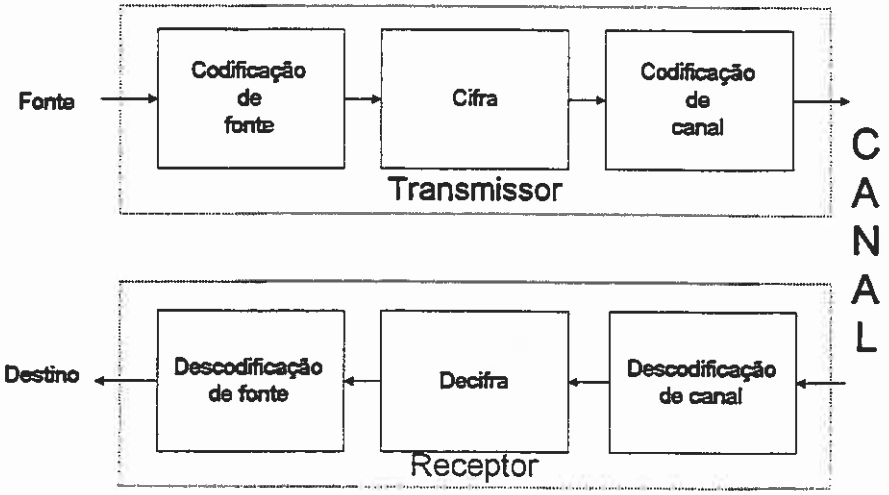


Figura 1. Estrutura genérica dos sistemas de comunicação segura.

Nos casos considerados, a fonte de informação é discreta e modelada por um processo estocástico discreto estacionário. A codificação de fonte tem por objectivo a eliminação da

redundância. O bloco de cifra destina-se a impedir o acesso a utilizadores não autorizados. Na codificação de canal insere-se informação redundante com vista à posterior detecção e/ou correcção de erros no receptor. Os blocos associados ao receptor operam de forma inversa. Considera-se a situação de comunicação em canal discreto, ruidoso e sem memória.

No desenvolvimento destes conceitos tomam-se como exemplo sistemas reais, desenvolvidos em colaboração com outras instituições, ilustrando-se a aplicação de ferramentas matemáticas nessa actividade de investigação e desenvolvimento. Por razões de espaço, os detalhes de implementação são remetidos para a bibliografia.

2. Codificação de fonte

As fontes de informação consideradas neste trabalho são modeladas por processos estocásticos discretos estacionários. A perspectiva adoptada é a da Teoria da Informação proposta por C. Shannon (para maior detalhe sugerem-se as referências [2] e [10]).

Definição 2.1 – Entropia, Entropia Conjunta e Entropia Condicionada

A entropia $H(X)$ de uma variável aleatória (v. a.) discreta X (com espaço de acontecimentos X) é definida por

$H(X) =$ **-Error!**

Sendo X e Y variáveis aleatórias define-se entropia conjunta e entropia condicionada, respectivamente, como

$H(X,Y) =$ **-Error! Error!**

$H(Y|X) =$ **-Error! Error!**

Embora o logaritmo possa ser em qualquer base, é comum utilizar-se a base 2 sendo, neste caso, a entropia medida em bits por símbolo (é também esta a base considerada no presente trabalho).

A taxa de entropia do processo estocástico estacionário $\{X_n, n=0, 1, 2, \ldots\}$ define-se como

$H\{X_n, n=0, 1, 2, \ldots\} = H\{X\} = \lim_{n \to \infty}$**Error!** $H(X_n| X_{n-1}, \ldots, X_1)$.

O limite existe e esta definição corresponde à noção de entropia por símbolo da última v. a. dado o passado. Outra definição equivalente, correspondente à noção de entropia por símbolo de n variáveis aleatórias, é

$H\{X\} = \lim_{n \to \infty}$**Error!** $H(X_1, X_2, \ldots, X_n)$.

A codificação de fonte consiste em atribuir descrições mais curtas para os acontecimentos mais prováveis e, necessariamente, descrições mais longas para os acontecimentos menos

frequentes. O objectivo último é a descrição, de menor comprimento médio, para uma variável aleatória.

A codificação de fonte divide-se em duas classes: sem perda de informação (também designada simplesmente por compressão de dados) e com perda de informação. Nas técnicas de codificação sem perda garante-se a regeneração exacta dos dados após a sequência codificação — descodificação. Por outro lado, na codificação com perdas admite-se distorção, com vista a aumentar a taxa de compressão.

Definição 2.2 – Código de Fonte

Um código de fonte C para a v. a. X é uma transformação de X, o domínio de X, em D* sendo este um conjunto de sequências, de dimensão finita, de símbolos de um alfabeto $_D$.

A palavra de código correspondente a x é $C(x)$, sendo $l_C(x)$ o seu comprimento.

O comprimento esperado de um código de fonte C para a v. a. X, com função de massa de probabilidade $p(x)$, é dado por $L(C) = E_X[l_C(x)]$.

Teorema 2.1 – (Shannon [10]) Codificação de Fonte

Seja L^* o menor valor esperado do comprimento das palavras de um qualquer código unicamente descodificável. O valor L^* satisfaz a seguinte relação

Error! $\leq L^* \leq$ **Error!** + **Error!** para qualquer $n > 0$.

A desigualdade anterior estabelece o valor máximo para a capacidade de compressão de um código, designando-se códigos óptimos os que a verificam [2]. Contudo, não existe forma sistemática para estabelecer códigos óptimos, computacionalmente eficientes, para uma qualquer fonte de informação.

Havendo independência entre as variáveis aleatórias X_i, o que corresponde à modelação de uma fonte de informação sem memória, então

$H\{X\} = H(X_i), \forall i$

A codificação de fontes de informação com memória reduz-se à codificação sem memória introduzindo-se predição adequada [2].

Em [11] ilustra-se a aplicação destas técnicas na implementação de codificadores de fala usando métodos de predição linear.

3. Codificação de Canal

Um canal discreto é um sistema caracterizado por: alfabeto de entrada X (domínio de X), alfabeto de saída Y (domínio de Y) e matriz de transição de probabilidades $p(y|x)$ ($x \in X, y \in Y$)

que exprime a probabilidade de observar o símbolo y dado ter sido enviado o símbolo x (canal: $(\mathrm{X}, p(y|x), \mathrm{Y})$). O canal diz-se sem memória se a distribuição de probabilidades na saída depende apenas da entrada nesse instante e é condicionalmente independente das entradas e saídas anteriores: $p(y_n|x_n, x_{n-1}, .., x_0 y_{n-1}, y_{n-2}, .., y_0) = p(y_n|x_n)$.

Definição 3.1 – Capacidade de Canal

A capacidade de um canal discreto sem memória define-se como

$C =$;max; $p(x)$ $I(X; Y)$,

em que $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y; X)$ é a informação mútua.

Definição 3.2 – Código de Canal

Um código (n, M) para o canal $(\mathrm{X}, p(y|x), \mathrm{Y})$ consiste em:

i) conjunto de índices $\{1, 2, \ldots, M\}$

ii) função de codificação X^n:$\{1, 2, \ldots, M\} \rightarrow \mathrm{X}^n$ dando origem a palavras de código $X^n(1), X^n(2), \ldots, X^n(M)$

iii) função de descodificação g: $\mathrm{Y}^n \rightarrow \{1, 2, \ldots, M\}$ que consiste numa regra determinística que associa um eleito a cada um dos possíveis vectores recebidos.

A taxa R de um código (n, M) define-se como

$R =$ **Error!** bits por símbolo transmitido.

Teorema 3.1 – (Shannon [10]) Codificação de Canal

É possível transmitir informação através de um canal ruidoso a qualquer velocidade inferior à capacidade do canal ($R < C$) com uma probabilidade de erro tão pequena quanto se quiser.

Seja $(S_q)^n$ o conjunto de todos os n-tupletos ordenados $\mathbf{s} = s_1, s_2, \ldots, s_n$ em que cada $s_i \in S_q$. Os elementos $\mathbf{s} \in (S_q)^n$ designam-se vectores ou palavras. A dimensão do conjunto $(S_q)^n$ é q^n. Um código q-ário de comprimento n é um subconjunto de $(S_q)^n$.

A distância de Hamming entre dois vectores $\mathbf{x}$ e $\mathbf{y}$ de $(S_q)^n$ é o número de posições em que os dois vectores diferem (note-se que satisfaz os axiomas de distância [2]).

A distância mínima do código C, designada por $d(C)$, é a menor distância entre quaisquer dois vectores do código, e traduz uma medida da capacidade de correcção de erros do código

$d(C) = \min \{d(x, y) \mid \forall x, y \in C, x \neq y\}$.

Se o código C tem distância mínima d, então o código pode ser usado para: i) detectar até $d - 1$ erros ou ii) corrigir até $\lfloor (d-1) / 2 \rfloor$ erros, em qualquer palavra do código.

No desenho do código (n, M) com distância mínima d, designado por (n, M, d) pretende-se:

i) baixo valor de n (para transmissão rápida da informação);

ii) elevado M (para maximizar a informação por símbolo transmitido);

iii) elevado d (para corrigir muitos erros).

Estes objectivos são contraditórios pelo que, normalmente, a pesquisa de códigos é feita variando apenas um dos parâmetros. É comum a pesquisa do maior código (maior M) dado o comprimento n e a distância mínima d.

Restringindo a pesquisa aos códigos lineares (isto é, q é potência de um número primo sendo, em consequência, S_q um campo de Galois $GF(q)$) simplifica-se a pesquisa e optimiza-se o desenho dos codificadores, devido à estruturação do espaço de pesquisa e dos códigos considerados. Fixando os valores de q e d, o problema da pesquisa do código pode ser enunciado por: dado o comprimento n, determine-se a máxima dimensão k, tal que $M = q^k$, para a qual existe um código $[n, k, d]$ sobre $GF(q)$. A redundância do código $[n, k, d]$ é $r = n - k$.

Exemplo 3.1

Código [4, 3, 3] sobre $GF(3)$

O matriz geradora do código (sub-espaço) é

[1;1;0;0;0;1;1;0;0;0;1;1]

São palavras do código:

0000, 1100, 2200, 0110, 0220, 0011, 0022, 1210, 2010, 1020, 1111, ...

As principais vantagens dos códigos lineares são: simplificação na determinação da distância mínima (M-1 *vs* (1/2)$M(M$-1) operações); para caracterização do código $[n, k, d]$ bastam k palavras do código (a dimensão do sub-espaço é k); existem técnicas simples para codificação e descodificação. São desvantagens: existência de códigos lineares apenas para valores de p que sejam potências inteiras de números primos; eventual existência de códigos não lineares com maior distância mínima. Constata-se contudo que frequentemente os códigos óptimos num certo sentido são lineares.

Em [12] descreve-se a aplicação, num sistema de comunicação, do código [8, 4, 3] sobre $GF(2)$. Trata-se de um código linear obtido por extensão do código de Hamming [15].

Por razões de simplificação da pesquisa de códigos e da implementação dos codificadores é ainda comum restringir a pesquisa aos códigos lineares cíclicos (as rotações de palavras do código são palavras do código) [15]. Note-se que o código do exemplo anterior é cíclico. Trata-se de um código óptimo no sentido em que se verifica a igualdade na relação $d \leq r + 1$.

4. Componente criptográfica

O primeiro passo para o estudo dedutivo da criptografia passa pela definição formal de sistema criptográfico.

Definição 4.1 - Sistema criptográfico

Um sistema criptográfico é definido por cinco conjuntos de objectos (P, C, K, E e D) com a seguinte caracterização:

i) P é um conjunto finito de textos ou mensagens;

ii) C é um conjunto finito de criptogramas;

iii) K é um conjunto finito de chaves;

iv) E é um conjunto de funções E: P $\rightarrow$C, designadas por transformações de cifra;

v) D é um conjunto de funções D: C $\rightarrow$P, designadas por transformações de decifra;

vi) Para cada chave $k \in$ K existe uma transformação $E_k \in$ E e uma transformação $D_k \in$ D tal que: $\forall x \in$P, $D_k(E_k(x)) = x$.

As mensagens x, pertencentes ao conjunto P, são transformadas pela função de cifra em criptogramas y pertencentes a C. A regra de cifra é escolhida, de entre as pertencentes ao conjunto E, pela chave k pertencente a K. Essa mesma chave deve ser utilizada no decifrador para escolher, de entre o conjunto D, a regra de decifra a aplicar em y para obter x. Considera-se que o criptoanalista conhece o sistema criptográfico, ou seja, os conjuntos P, C, K, E e D. Munido desta informação e de um criptograma, o seu objectivo é estimar qual a mensagem que lhe deu origem, sem o conhecimento da chave. A definição anterior refere apenas as premissas que o sistema criptográfico tem de respeitar para ser consistente, não o caracterizando em termos da segurança proporcionada. Considerem-se ainda duas variáveis aleatórias: a v.a. X, definida sobre o conjunto P, modela o comportamento estatístico da fonte de mensagens; a v.a. K, definida sobre o conjunto K, modela o gerador de chaves. Com este modelo surge naturalmente a v.a.Y, função de X e K, definida sobre o conjunto C.

Definição 4.2

Um sistema criptográfico possui segurança perfeita [14] se e só se:

$$p(x \mid y) = p(x), \text{ com } y = E_k(x), \forall x \in \mathrm{P} \text{ e } \forall y \in \mathrm{C}$$

A definição anterior implica que a informação mútua entre X e Y seja nula: $I(X; Y) = 0$. A segurança perfeita é igualmente designada de incondicional, uma vez que não são colocadas restrições quanto à caracterização computacional do criptoanalista.

É condição necessária para que um sistema criptográfico possua segurança perfeita, que $H(K) \geq H(X)$. Esta condição estabelece um limite que reduz a aplicabilidade prática deste critério de segurança, obrigando a que a dimensão em bits da chave seja maior ou igual que a dimensão em bits da mensagem.

Exemplo 4.1

Um sistema que possui segurança perfeita é o de Vernam, permitindo a cifra de mensagens com N bits, sendo caracterizado da seguinte forma:

i) $\mathrm{P} = \mathrm{C} = \mathrm{K} = \{0, 1\}^N$,

ii) $y = E_k(x) = (x_1 + k_1 \ mod\ 2, \ldots, x_N + k_N \ mod\ 2)$,

iii) $x = D_k(y) = (y_1 + k_1 \ mod\ 2, \ldots, y_N + k_N \ mod\ 2)$,

iv) $p(k) = 2^{-N}$, $\forall k \in \mathrm{K}$.

Num sistema sem segurança perfeita, o criptoanalista, com recursos computacionais ilimitados, usa o criptograma para reduzir a incerteza sobre a mensagem. Havendo constrições nos recursos computacionais, o sistema criptográfico é caracterizável sob o ponto de vista da segurança condicional ou segurança computacional. Esta caracterização, para além da Teoria da Informação, envolve a Teoria da Complexidade.

Para uma comunicação segura entre dois interlocutores sobre um canal não seguro, há necessidade prévia de troca de chaves. A necessidade de distribuição segura de chaves a todos os utilizadores autorizados é comum a todos os sistemas criptográficos. Na definição de sistema de comunicação segura é utilizado um canal físico seguro para a distribuição das chaves. A necessidade deste canal suplementar constitui forte limitação. O problema da distribuição de chaves agrava-se nas redes de comunicação de larga escala em que o número de ligações evolui em $(n^2 - n)/2$ para n utilizadores. Para valores de n elevados o custo da distribuição de chaves é proibitivo. Assim, na concepção de grandes redes de comunicação segura é-se compelido à utilização de canais não seguros quer para a distribuição das chaves

quer para a subsequente comunicação segura. Este constrangimento leva-nos a uma questão fundamental: como trocar de forma segura as chaves sobre um canal não seguro?

Diffie e Hellman, em [3], propõem uma solução, que passa pela definição de sistema criptográfico assimétrico. No que se segue, iremos focar a nossa atenção no desenho, análise e realização desta classe de sistemas.

Definição 4.3

Um sistema criptográfico assimétrico respeita a definição de sistema criptográfico (4.1), acrescida do seguinte: para qualquer $k \in \mathrm{K}$ é "computacionalmente difícil" obter a função D_k, conhecendo-se apenas a função E_k. Contudo, é "computacionalmente fácil" obter pares (E_k, D_k), bem como realizar essas operações.

Neste contexto, a função E_k é designada por transformação pública e a função D_k é designada por transformação privada. Tipicamente a chave é dividida em duas componentes: pública e privada. A componente pública é suficiente para a realização da função E_k. Em contrapartida, num sistema simétrico, o conhecimento da função E_k é equivalente ao conhecimento da função D_k.

A formulação de sistemas assimétricos passa assim pela criação de funções, designadas de *one-way functions with trapdoor*. Esta funções são caracterizadas como sendo fáceis de calcular, mas difíceis de inverter, a menos que se possua informação adicional não pública (*trapdoor*).

Apresentamos de seguida dois sistemas baseados em dois problemas clássicos da Teoria Computacional dos Números: a factorização de números inteiros e o cálculo de logaritmos discretos.

Definição 4.4 - Sistema assimétrico de Rivest-Shamir-Adleman (RSA [9])

Sejam p e q dois números primos:

$\mathrm{K} = \{(e, d, n): n = pq \text{ e } ed \equiv 1 \ mod\ ((p-1)(q-1))\}$.

$\mathrm{P} = \mathrm{C} = \mathbf{Z}/n\mathbf{Z}$

$y = E_k(x) = x^e \ mod\ n$

$x = D_k(y) = y^d \ mod\ n$

A componente pública da chave, que permite caracterizar a transformação de cifra é (e, n), e a componente privada é d. A segurança do sistema RSA é condicionada à dificuldade da factorização de um número composto.

Definição 4.5 - Sistema assimétrico de ElGamal [14]

Seja $G = (G, o)$ um grupo finito, seja α um elemento de G e seja H o subgrupo gerado por α, tal que o cálculo de logaritmos discretos em H seja difícil.

$K = \{(\alpha, a, \beta): \beta = \alpha^a\}$

$P = G$

$C = G \times G$

$y = (y_1, y_2) = E_k(x) : y_1 = \alpha^r, y_2 = x \circ \beta^r$, em que r é um número aleatório que deve permanecer secreto.

$x = D_k(y) = y_2 \circ (y_1^a)^{-1}$.

A componente pública da chave é (α, β) e a componente privada é a. Normalmente é utilizado é o grupo multiplicativo Zp^*, com p inteiro primo.

A implementação e utilização de um sistema assimétrico como o RSA num sistema de comunicação seguro, coloca problemas a vários níveis: geração de parâmetros e chaves, implementação das transformações de cifra e decifra, correcta utilização no desenho de protocolos de comunicação.

A forma de utilização do sistema criptográfico condiciona o nível de segurança do sistema de comunicação. Tipicamente, as falhas dos protocolos criptográficos devem-se, não a deficiências dos sistemas criptográficos, mas à sua incorrecta utilização. Esta depende não só da classificação do sistema (simétrico *vs* assimétrico) mas também das suas características internas, i.e., da teoria matemática que o suporta. Ilustramos de seguida este aspecto com um exemplo paradigmático.

Exemplo 4.2

No sistema RSA, para optimização computacional da transformação pública ($x^e \ mod \ n$), é corrente a utilização do expoente público 3 ($e = 3$). O criptoanalista, dispondo de três criptogramas resultantes da cifra de uma mesma mensagem com três chaves diferentes (com $e = 3$), obtém facilmente a mensagem. Este cenário é vulgar em situações de *broadcast*. A metodologia do ataque baseia-se num teorema clássico da Teoria Elementar dos Números.

Teorema 4.2 - Teorema Chinês do Resto (TCR [6], [14])

Seja $M = n_1.n_2 \ldots n_N$, tal que $\text{mdc}(n_i, n_j) = 1$, com $i \neq j$. O sistema de equações congruenciais: $x \equiv r_i \ mod \ n_i$, $i = 1, \ldots, N$; possui uma e só uma solução no conjunto $\{0, \ldots, M\text{-}1\}$. Essa solução é dada por

$$x = \textbf{Error!} \bmod M, \text{ com } M_i = \textbf{Error!} \text{ e } y_i \equiv M_i^{-1} \bmod n_i$$

O coeficientes M_i são calculados através de divisões e os coeficientes y_i são calculados usando a extensão do algoritmo de Euclides.

Sejam $y_i = x^3 \bmod n_i$, com $i = 1, 2$ e 3, os criptogramas resultantes da cifra de x utilizando as chaves públicas $(3, n_1)$, $(3, n_2)$ e $(3, n_3)$. Se os três módulos não forem relativamente primos (situação altamente improvável) a factorização de um dos módulos é trivial. Caso contrário, o Teorema Chinês do Resto é aplicável, e o valor $x^3 \bmod M = x^3$ é facilmente calculado. Para finalmente se obter x basta calcular uma raiz cúbica (não modular).

Este método é facilmente estendido a qualquer exponente público e, necessitando-se para tal de e criptogramas.

A optimização computacional das transformações pública e privada representa outro dos desafios na implementação do RSA. Apresentamos de seguida um conjunto de optimizações, numa abordagem *top-down* do problema.

Tipicamente, o expoente público é pequeno, pelo que a transformação pública é bastante mais rápida de efectuar do que a transformação privada. Um dos métodos mais eficientes de optimização desta última, proposto por Quisquater e Couvreur [8], baseia-se igualmente no TCR.

Para o cálculo de $y^d \bmod n$, com $n = pq$, pode-se calcular $r_p = y^d \bmod p$ e $r_q = y^d \bmod q$ e de seguida utilizar o TCR. O cálculo de r_p, tal como o de r_q, pode ser optimizado da seguinte forma:

$$y^d \bmod p = y^{k(p-1)+ d \bmod (p-1)} \bmod p = (y^{(p-1)})^k y^{d \bmod (p-1)} \bmod p, k \in \mathbf{Z}.$$

Se p não dividir y temos, pelo Teorema de Fermat [5], que $y^{(p-1)} \equiv 1 \bmod p$, ou seja, $y^d \equiv y^{d \bmod (p-1)} \bmod p$. Se p dividir y a congruência anterior é igualmente verificada.

A operação $y^{d \bmod (p-1)} \bmod p$ tem complexidade $\mathbf{O}(\log^3(p))$, enquanto que $y^d \bmod n$ tem complexidade $\mathbf{O}(\log^3(n))$. Sendo $\log(p)$ aproximadamente metade de $\log(n)$ obtemos uma redução assimptótica de 8 no tempo de processamento. Como são necessárias duas exponenciações modulares, e o peso computacional do TCR é desprezável face a estas, obtemos um ganho assimptótico de 4 no cálculo da transformação privada.

Para a realização de uma exponenciação modular é necessário calcular uma sucessão de multiplicações modulares. Uma forma de diminuir o número de operações passa pela utilização de cadeias de adição [4]. Seja d um número inteiro, a cadeia de adição de d é a sequência de inteiros $a_0, a_1, \ldots, a_r$ tal que

$a_0 = 1$; $a_r = d$ e $a_i = a_j + a_k$ para $0 \leq k \leq j < i \leq r$.

A cadeia de adição para o expoente estabelece a sequência de multiplicações modulares que é necessário realizar. A minimização do comprimento da cadeia minimiza igualmente o número de multiplicações. Encontrar a cadeia de menor dimensão para um qualquer inteiro é considerado um problema *NP-hard*, contudo existem soluções sub-óptimas, com complexidade polinomial, nomeadamente: cadeias binárias e M-árias, janela deslizante, etc.

Em [13] ilustra-se a aplicação da cadeia M-ária no cálculo da exponenciação modular. Cohen, em [1], descreve algoritmos bem como a determinação do valor de M óptimo.

O método proposto por Quisquater e Couvreur [8] (baseado no TCR) diminui a dimensão dos operandos da exponenciação modular. A utilização das cadeias de adição reduz o número de multiplicações necessárias para a realização dessa operação. Contudo, o cálculo de uma multiplicação modular, realizado da forma mais imediata, envolve uma divisão no passo de redução. Montgomery, em [7], propôs um método de redução sem divisões.

Sejam n e r inteiros positivos tal que $r > n$ e mdc(n, r) = 1. Defina-se o *n-residue* de um inteiro $x < n$ como sendo $x' = T_{n,r}(x) = xr \ mod \ n$, em que $T_{n,r}$: $\mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$. Como mdc($n$, r) = 1, existe a transformação inversa $T^{-1}_{n,r}(x) = xr^{-1} \ mod \ n$, com $rr^{-1} \equiv 1 \ mod \ n$. Consideremos a transformação $R_r(x) = xr^{-1} \ mod \ n$, com $0 \leq x < nr$, normalmente designada por redução de Montgomery. Temos que

$R_r(x'y') = (xr \ mod \ n) \ (yr \ mod \ n) \ r^{-1} \ mod \ n = (\mathrm{nr})(\mathrm{yr})\mathrm{r}^{-1} \ mod \ n = xyr \ mod \ n = T_{n,r}(xy)$.

Assim, as operações de multiplicação modular podem ser realizadas no domínio dos *n-residue* utilizando a transformação R_r. A optimização advém da existência dum algoritmo sem divisões para o cálculo de R_r.

Algoritmo 4.1

Seja t um inteiro tal que $0 \leq t < nr$, representado na base b: $t = (t_{N-1},\ldots,t_0)_b$; $nn' \equiv -1 \bmod b$ e $r = b^N$; um algoritmo para o cálculo de $R_r(t)$ é:

```
1.  a ← t.
2.  Desde i = 0 até N-1:
    2.1. α ← a_i n' mod b.
    2.2. a ← a + αnb^i.
3.  a ← a / b^N.
4.  Se a ≥ n então a ← a - n.
5.  Devolver a.
```

Para provarmos a correcção do algoritmo temos que mostrar que o valor de a no final do passo 3 é: inteiro; congruente com $tr^{-1} \bmod n$ e que se encontra no intervalo $0 \leq t < 2n$.

No passo 2.2, a é sempre adicionado com um múltiplo de n pelo que no final do passo 2 temos que $a \equiv t \bmod n$. Assim no final do passo 3 temos $a \equiv tr^{-1} \bmod n$.

O valor αn é igual a $kb + (\alpha n \bmod b)$, com $k \in \mathbb{Z}$, que simplifica para $kb + (-a_i) \bmod b = kb - a_i$. Temos assim que no final do passo 2.2 e para cada iteração i, o valor de a é divisível por b^{i+1}.

No final de do passo 2 temos que

$$0 \leq a \leq t + n(b\text{-}1)\textbf{Error!} \Leftrightarrow 0 \leq a < nr + nr,$$

uma vez que $(b\text{-}1)\textbf{Error!} < b^N$. Assim no final do passo 3 temos $0 \leq a < 2n$.

As três optimizações descritas ilustram a aplicação de aspectos da teoria dos números num problema clássico de engenharia: desenho de algoritmos eficientes para resolução de um problema. Utilizaram-se aspectos elementares dessa teoria, nomeadamente: noção de congruência, teorema de Fermat e Teorema Chinês do Resto. Outros temas, tais como a geração de números primos e o desenho de sistemas assimétricos baseados em curvas elípticas, constituem exemplos de aplicação de outros conceitos da teoria dos números. Estas técnicas foram ferramenta indispensável no desenvolvimento de uma biblioteca, em linguagem "C", para realização de operações sobre inteiros em precisão estendida.

5. Conclusões e comentários finais

No presente trabalho tratam-se aspectos inerentes ao desenvolvimento de sistemas de comunicação segura. Analisam-se as componentes de codificação de fonte, cifra e codificação de canal, salientando a sua modelação matemática.

A importância desta formulação num contexto matemático, é realçada através das soluções que ela permite: trata-se de aplicações de áreas da matemática como probabilidades, álgebra linear, álgebra abstracta e teoria dos números. Ilustram-se assim novas orientações na aplicação da matemática em engenharia.

A realização das operações criptográficas é exemplo paradigmático: a utilização de resultados da teoria dos números, permitiu satisfazer requisitos funcionais previamente estabelecidos, só doutra forma alcançáveis se adoptadas plataformas computacionais mais onerosas.

Os temas abordados constituem ainda áreas de investigação, onde a aplicação da matemática em engenharia, não só é natural como essencial.

6. Bibliografia

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993.

[2] T. Cover, J. Thomas, Elements of Information Theory, John Wiley & Sons, 1991.

[3] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, November 1976.

[4] D. Knuth, The Art of Computer Programming, Vol 2: Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1981.

[5] N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

[6] J. Nechvatal, "Public Key Cryptography" in Contemporary Cryptology, edited by Gustavus J. Simmons, IEEE Press, 1992.

[7] P. Montgomery, "Modular multiplication without trial division", Mathematics of Computation, vol. 44, pp. 519-521, 1985.

[8] J-J Quisquater, C. Couvreur, "Fast Decipherment algorithm for RSA Public-Key Cryptosystem", Electronics Letters, vol. 18, N° 21, pp. 905-907, 1982.

[9] R. Rivest, A. Shamir, A. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM vol. 21, no. 2, pp. 120-126, 1978.

[10] C. Shannon, "A Mathematical Theory of Communication", Bell Systems Technical Journal, Vol. 27, pp. 379-423, 1948.

[11] F. Sousa, "DSP-Based Secure Systems for Digital Speech Communication over PSTN and via Radio", Proceedings of The International Conference on Signal Processing Applications & Technology – ICSPAT94, Dallas, Vol. II, pp. 1405-1410, 1994.

[12] F. Sousa, P. Félix, "DSP Based Secure Communication Systems", Proceedings of The First European DSP Education and Research Conference, Paris, 1996.

[13] —, "The Computation of Extended-Modular Exponentiation on a DSP Architecture", Proceedings of The International Conference on Signal Processing Applications & Technology – ICSPAT96, Boston, 1996.

[14] D. Stinson, Cryptography Theory and Practice, CRC Press, 1995.

[15] S. Wicker, Error Control Systems for Digital Communication and Storage, Prentice-Hall, 1995.

Análise Dinâmica de Permutadores de Fluxo Cruzado

José Emílio da Costa Cruces

Instituto Superior de Engenharia de Lisboa

Resumo

Deduz-se a equação diferencial parcial que governa o comportamento térmico de um permutador de calor de fluxo cruzado.

Integra-se analiticamente a referida equação para temperaturas e caudais variáveis.

Estudam-se os esquemas numéricos de diferenças finitas mais adequados para a resolução do problema, em termos de simplicidade, precisão e estabilidade.

Apresenta-se a representação gráfica dos resultados obtidos.

1. Introdução

O balanço entálpico para um pequeno troço do permutador de comprimento Δx, durante um curto intervalo de tempo Δt, conduz a:

$$\rho \cdot C \cdot \frac{\pi \cdot D^2}{4} \cdot \Delta x \cdot u\Big|_{x,t} - \rho \cdot C \cdot \frac{\pi \cdot D^2}{4} \cdot \Delta x \cdot u\Big|_{x,t+\Delta t} +$$
$$+ \rho \cdot C \cdot Q \cdot \Delta t \cdot u\Big|_{x,t} - \rho \cdot C \cdot Q \cdot \Delta t \cdot u\Big|_{x+\Delta x,t} +$$
$$+ U \cdot \pi \cdot D \cdot \Delta x \cdot \Delta t \cdot (u - u_o) = 0$$

em que:

C - capacidade calorífica,

D - diâmetro da tubagem em que circula o fluido que se deseja arrefecer/aquecer,

Q - caudal de fluido que se deseja arrefecer/aquecer,

U - coeficiente global de transferência de calor,

u - temperatura do fluido que se deseja arrefecer/aquecer,

u_o - temperatura do fluido de arrefecimento/aquecimento,

ρ - massa volumíca.

Se D for constante e se C, U e ρ não tiverem variações significativas ao longo do permutador, situação relativamente frequente, dividindo ambos os membros da equação por $\rho \cdot C \cdot \frac{\pi \cdot D^2}{4} \cdot \Delta x \cdot \Delta t$, tendo em conta que $v = \frac{4 \cdot Q}{\pi \cdot D^2}$ é a velocidade do fluido que se deseja arrefecer/aquecer e fazendo $k = \frac{4 \cdot U}{\rho \cdot C \cdot D}$, vem:

$$\frac{u(x,t)-u(x,t+\Delta t)}{\Delta t}+v\cdot\frac{u(x,t)-u(x+\Delta x,t)}{\Delta x}+k\cdot(u-u_o)=0$$

Nestas condições, quando $\Delta x \to 0$ e $\Delta t \to 0$, chega-se a:

$$\frac{\partial u}{\partial t}+v\cdot\frac{\partial u}{\partial x}+k\cdot(u-u_o)=0$$

Trata-se de uma equação diferencial parcial do tipo hiperbólico, cuja solução analítica geral se obtém com relativa facilidade quando u_o e v são constantes:

$$u(x,t)=u_o+\exp\left[-\frac{k}{2}\cdot\left(t+\frac{x}{v}\right)\right]\cdot f\left(t-\frac{x}{v}\right)$$

Se, por exemplo, a condição inicial corresponder ao estado estacionário:

$$u(x,0)=u_o+(u_e-u_o)\cdot\exp\left(-\frac{k\cdot x}{v}\right)$$

e a condição fronteira equivaler a uma variação sinusoidal da temperatura de entrada do fluido que se quer arrefecer /aquecer, com o tempo:

$$u(0,t)=u_e+u_a\cdot\sin\left(\frac{2\cdot\pi\cdot t}{T}\right)$$

onde:

T - período da variação de temperatura de entrada do fluido que se deseja arrefecer/aquecer,

u_a - amplitude da variação de temperatura de entrada do fluido que se deseja arrefecer/aquecer,

u_e - temperatura média de entrada do fluido que se deseja arrefecer/aquecer,

a solução do problema escreve-se:

$$u(x,t)=u_o+\left[(u_e-u_o)+u_a\cdot H\left(t-\frac{x}{v}\right)\cdot\sin\frac{2\cdot\pi\cdot\left(t-\frac{x}{v}\right)}{T}\right]\cdot\exp\left(-\frac{k\cdot x}{v}\right)$$

na qual:

$$H(y)=\begin{cases}0 & y\le 0\\ 1 & y>0\end{cases}$$

Quando v depende de t a obtenção de uma solução analítica torna-se mais difícil. Todavia, pode verificar-se que, para uma variação sinusoidal:

$$v=v_e+v_a\cdot\sin\frac{2\cdot\pi\cdot t}{T}$$

onde:

T - período da variação da velocidade do fluido que se deseja arrefecer/aquecer,

v_a - amplitude da variação da velocidade do fluido que se deseja arrefecer/aquecer,

v_e - velocidade média do fluido que se deseja arrefecer/aquecer,

associada a uma condição inicial idêntica à do caso anterior:

$$u(x,0)=u_o+(u_e-u_o)\cdot\exp\left(-\frac{k\cdot x}{v}\right)$$

e a uma condição fronteira representativa de uma temperatura constante de entrada do fluido que se pretende arrefecer/aquecer:

$$u(0,t)=u_e$$

se tem:

$$u(x,t)=u_o+(u_e-u_o)\cdot\exp[-k\cdot(t-\theta)]$$

em que:

$$\theta=t+\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\left(1-\cos\frac{2\cdot\pi\cdot t}{T}\right)-\frac{x}{v_e} \qquad \theta\le 0$$

$$\theta-\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot\theta}{T}=t-\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot t}{T}-\frac{x}{v_e} \qquad \theta>0$$

Para compreender a forma da solução obtida, válida para $v_e>|v_a|$, deve ter-se em atenção que:

$$\frac{dx}{dt}=v=v_e+v_a\cdot\sin\frac{2\cdot\pi\cdot t}{T}\rightarrow x-x_0=v_e\cdot t+\frac{T\cdot v_a}{2\cdot\pi}\cdot\left(1-\cos\frac{2\cdot\pi\cdot t}{T}\right)$$

Por outro lado, como não se consegue resolver formalmente a equação:

$$\theta-\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot\theta}{T}=t-\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot t}{T}-\frac{x}{v_e}$$

há que recorrer a métodos numéricos. Se se optar pelo método de Newton, pode-se escrever:

$$f(\theta)=\theta-\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot\theta}{T}-t+\frac{T\cdot v_a}{2\cdot\pi\cdot v_e}\cdot\cos\frac{2\cdot\pi\cdot t}{T}+\frac{x}{v_e}$$

Depois faz-se, sucessivamente:

$$\theta_{k+1}=\theta_k-\frac{f(\theta_k)}{f'(\theta_k)}$$

até obter a precisão desejada. Claro que:

$$f'(\theta)=1+\frac{v_a}{v_e}\cdot\sin\frac{2\cdot\pi\cdot\theta}{T}$$

2. Esquemas Numéricos

O conhecimento das soluções analíticas apresentadas em 1. permite testar, de uma forma objectiva, diversos esquemas alternativos de discretização numérica, para a integração da equação diferencial parcial em estudo.

Embora a análise efectuada se tenha estendido a um leque mais vasto de opções, por questões de simplicidade e brevidade, vai-se considerar, em primeiro lugar, o caso em que a velocidade se mantém constante, o permutador se encontra no estado estacionário no instante inicial e a temperatura de entrada do fluido que se deseja arrefecer/aquecer tem uma variação sinusoidal, aplicando-lhe as seguintes discretizações:

- Método de Euler para a frente no tempo, método de Euler para trás no espaço

$$u_{i,1} = u\left((i-1)\cdot\Delta x, 0\right) \quad (i = 1,\ldots,I)$$

$$u_{1,j} = u\left(0,(j-1)\cdot\Delta t\right) \quad (j = 2,\ldots,J)$$

$$\frac{u_{i,j}-u_{i,j-1}}{\Delta t} + v\cdot\frac{u_{i,j-1}-u_{i-1,j-1}}{\Delta x} = k\cdot\left(u_o - u_{i,j-1}\right)\rightarrow$$

$$\rightarrow u_{i,j} = \Delta t\cdot\left[k\cdot u_o + \frac{v}{\Delta x}\cdot u_{i-1,j-1} + \left(\frac{1}{\Delta t} - \frac{v}{\Delta x} - k\right)\cdot u_{i,j-1}\right] \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$

- Método de Runge-Kutta (4.ª ordem) para a frente no tempo, método de Euler para trás no espaço

$$u_{i,1} = u\left((i-1)\cdot\Delta x, 0\right) \quad (i = 1,\ldots,I)$$

$$u_{1,j} = u\left(0,(j-1)\cdot\Delta t\right) \quad (j = 2,\ldots,J)$$

$$k1_1 = k2_1 = k3_1 = k4_1 = 0$$

$$\frac{du_i}{dt} + v\cdot\frac{u_i - u_{i-1}}{\Delta x} = k\cdot\left(u_o - u_i\right)\rightarrow$$

$$\rightarrow\begin{cases} k1_i = \Delta t\cdot\left[k\cdot u_o + \dfrac{v}{\Delta x}\cdot u_{i-1,j-1} - \left(\dfrac{v}{\Delta x}+k\right)\cdot u_{i,j-1}\right] \\ k2_i = \Delta t\cdot\left[k\cdot u_o + \dfrac{v}{\Delta x}\cdot\left(u_{i-1,j-1} + \dfrac{k1_{i-1}}{2}\right) - \left(\dfrac{v}{\Delta x}+k\right)\cdot\left(u_{i,j-1} + \dfrac{k1_i}{2}\right)\right] \\ k3_i = \Delta t\cdot\left[k\cdot u_o + \dfrac{v}{\Delta x}\cdot\left(u_{i-1,j-1} + \dfrac{k2_{i-1}}{2}\right) - \left(\dfrac{v}{\Delta x}+k\right)\cdot\left(u_{i,j-1} + \dfrac{k2_i}{2}\right)\right] \\ k4_i = \Delta t\cdot\left[k\cdot u_o + \dfrac{v}{\Delta x}\cdot\left(u_{i-1,j-1} + k3_{i-1}\right) - \left(\dfrac{v}{\Delta x}+k\right)\cdot\left(u_{i,j-1} + k3_i\right)\right] \\ u_{i,j} = u_{i,j-1} + \dfrac{k1_i + 2\cdot k2_i + 2\cdot k3_i + k4_i}{6} \end{cases}$$

$$(i = 2,\ldots,I; j = 2,\ldots,J)$$

- Método de Euler para trás no tempo, método de Euler para trás no espaço

$$u_{i,1} = u((i-1)\cdot\Delta x, 0) \quad (i = 1,\ldots,I)$$
$$u_{1,j} = u(0,(j-1)\cdot\Delta t) \quad (j = 2,\ldots,J)$$
$$\frac{u_{i,j} - u_{i,j-1}}{\Delta t} + v\cdot\frac{u_{i,j} - u_{i-1,j}}{\Delta x} = k\cdot(u_o - u_{i,j}) \rightarrow$$
$$\rightarrow u_{i,j} = \frac{k\cdot u_o + \frac{u_{i,j-1}}{\Delta t} + \frac{v}{\Delta x}\cdot u_{i-1,j}}{k + \frac{1}{\Delta t} + \frac{v}{\Delta x}} \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$

- Método de Euler para trás no tempo, método das diferenças centrais no espaço

$$u_{i,1} = u((i-1)\cdot\Delta x, 0) \quad (i = 1,\ldots,I)$$
$$u_{1,j} = u(0,(j-1)\cdot\Delta t) \quad (j = 2,\ldots,J)$$
$$\frac{u_{i,j} - u_{i,j-1}}{\Delta t} + v\cdot\frac{u_{i+1,j} - u_{i-1,j}}{2\cdot\Delta x} = k\cdot(u_o - u_{i,j}) \rightarrow$$
$$\rightarrow -\frac{v}{2\cdot\Delta x}\cdot u_{i-1,j} + \left(k + \frac{1}{\Delta t}\right)\cdot u_{i,j} + \frac{v}{2\cdot\Delta x}\cdot u_{i+1,j} = k\cdot u_o + \frac{u_{i,j-1}}{\Delta t} \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$
$$u_{I+1,j} = 2\cdot u_{I,j} - u_{I-1,j}$$

- Método das características de Euler

$$u_{i,1} = u((i-1)\cdot\Delta x, 0) \quad (i = 1,\ldots,I)$$
$$u_{1,j} = u(0,(j-1)\cdot\Delta t) \quad (j = 2,\ldots,J)$$
$$\frac{x_i - x_{i-1}}{\Delta t} = v \wedge x_1 = 0 \rightarrow x_i = v\cdot\Delta t\cdot(i-1) \quad (i = 2,\ldots,I)$$
$$\frac{u_{i,j} - u_{i-1,j-1}}{\Delta t} = k\cdot(u_o - u_{i-1,j-1}) \rightarrow u_{i,j} = k\cdot u_o + \left(\frac{1}{\Delta t} - k\right)\cdot u_{i-1,j-1} \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$

- Método das características de Runge-Kutta (4.ª ordem)

$$u_{i,1} = u\left((i-1)\cdot \Delta x, 0\right) \quad (i = 1,\ldots, I)$$

$$u_{1,j} = u\left(0, (j-1)\cdot \Delta t\right) \quad (j = 2,\ldots, J)$$

$$\frac{x_i - x_{i-1}}{\Delta t} = v \wedge x_1 = 0 \rightarrow x_i = v\cdot \Delta t\cdot (i-1) \quad (i = 2,\ldots, I)$$

$$\frac{du_{i-1}}{dt} = k\cdot (u_o - u_{i-1}) \rightarrow \begin{cases} k1 = \Delta t\cdot k\cdot \left(u_o - u_{i-1,j-1}\right) \\ k2 = \Delta t\cdot k\cdot \left(u_o - \left(u_{i-1,j-1} + \frac{k1}{2}\right)\right) \\ k3 = \Delta t\cdot k\cdot \left(u_o - \left(u_{i-1,j-1} + \frac{k2}{2}\right)\right) \\ k4 = \Delta t\cdot k\cdot \left(u_o - \left(u_{i-1,j-1} + k3\right)\right) \\ u_{i,j} = u_{i-1,j-1} + \frac{k1 + 2\cdot k2 + 2\cdot k3 + k4}{6} \end{cases}$$

$$(i = 2,\ldots, I; j = 2,\ldots, J)$$

Do ponto de vista teórico, sem entrar em grandes detalhes, o método de Euler para a frente no tempo, método de Euler para trás no espaço, bem como o método de Runge-Kutta (4.ª ordem) para a frente no tempo, método de Euler para trás no espaço, são métodos simples, sobretudo o primeiro, cuja estabilidade, todavia, depende do valor do parâmetro $\frac{v\cdot \Delta t}{\Delta x}$, o qual deve ser menor que a unidade, quando a equação diferencial parcial tem a forma:

$$\frac{\partial u}{\partial t} + v\cdot \frac{\partial u}{\partial x} = 0$$

O método de Euler para trás no tempo, método de Euler para trás no espaço e o método de Euler para trás no tempo, método das diferenças centrais no espaço, não sofrem desse defeito, que costuma obrigar a uma utilização de valores de Δt demasiado pequenos, ou de Δx excessivamente grandes. O principal óbice dos métodos para trás no tempo costuma residir na necessidade da resolução sucessiva de um sistema de equações lineares, o que não acontece, porém, na presente situação, para o método de Euler para trás no tempo, método de Euler para trás no espaço. Relativamente ao método de Euler para trás no tempo, método das diferenças centrais no espaço, significativamente mais exacto que o anterior, além da dificuldade já mencionada, existe a necessidade de introdução de uma condição fronteira artificial, que permita a determinação das temperaturas do fluido que se está a arrefecer/aquecer. No presente caso, admitiu-se que se estendia a malha para além fronteira no sentido dos x crescentes e se fazia:

$$u_{I+1,j} = 2\cdot u_{I,j} - u_{I-1,j} \quad (j = 2,\ldots, J)$$

O método das características de Euler e o método das características de Runge-Kutta (4.ª ordem), por sua vez, embora de implementação simples, especialmente o primeiro, e gozando de razoável precisão, particularmente o segundo, apresentam uma grande limitação, visto imporem que:

$$\Delta x = v \cdot \Delta t$$

Face a tudo o que ficou exposto, que, como se verá, é suportado pelos resultados a que se chegou, decidiu-se limitar a análise do caso de variação sinusoidal da velocidade do fluido a arrefecer/aquecer aos seguintes esquemas:

- Método de Euler para trás no tempo, método de Euler para trás no espaço

$$u_{i,1} = u\left((i-1)\cdot \Delta x, 0\right) \quad (i = 1,\ldots,I)$$

$$u_{1,j} = u\left(0,(j-1)\cdot \Delta t\right) \quad (j = 2,\ldots,J)$$

$$\frac{u_{i,j} - u_{i,j-1}}{\Delta t} + v_j \cdot \frac{u_{i,j} - u_{i-1,j}}{\Delta x} = k \cdot \left(u_o - u_{i,j}\right) \rightarrow$$

$$\rightarrow u_{i,j} = \frac{k \cdot u_o + \frac{u_{i,j-1}}{\Delta t} + \frac{v_j}{\Delta x} \cdot u_{i-1,j}}{k + \frac{1}{\Delta t} + \frac{v_j}{\Delta x}} \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$

- Método de Euler para trás no tempo, método das diferenças centrais no espaço

$$u_{i,1} = u\left((i-1)\cdot \Delta x, 0\right) \quad (i = 1,\ldots,I)$$

$$u_{1,j} = u\left(0,(j-1)\cdot \Delta t\right) \quad (j = 2,\ldots,J)$$

$$\frac{u_{i,j} - u_{i,j-1}}{\Delta t} + v_j \cdot \frac{u_{i+1,j} - u_{i-1,j}}{2 \cdot \Delta x} = k \cdot \left(u_o - u_{i,j}\right) \rightarrow$$

$$\rightarrow -\frac{v_j}{2 \cdot \Delta x} \cdot u_{i-1,j} + \left(k + \frac{1}{\Delta t}\right) \cdot u_{i,j} + \frac{v_j}{2 \cdot \Delta x} \cdot u_{i+1,j} = k \cdot u_o + \frac{u_{i,j-1}}{\Delta t} \quad (i = 2,\ldots,I; j = 2,\ldots,J)$$

$$u_{I+1,j} = 2 \cdot u_{I,j} - u_{I-1,j}$$

Convém sublinhar, que a aplicação de métodos das características com v variável, além de bastante complexa, não produz uma malha uniforme. Serviu, no entanto, para estabelecer a solução analítica apresentada anteriormente.

3. Resultados

A fim de estudar os esquemas numéricos apresentados, na situação de temperatura de entrada variável e velocidade constante do fluido que se deseja arrefecer/aquecer, escreveram-se programas em MATLAB, adoptando os seguintes valores para os parâmetros intervenientes: $L = 10; \Delta x = 1; \Delta t = 0{,}5; u_o = 25; v = 2; k = 0{,}05; u_e = 75; u_a = 10; T = 100$. As unidades utilizadas são as do Sistema Internacional (S. I.).

Os erros quadráticos médios das temperaturas do fluido que se quer arrefecer/aquecer, à saída do permutador, em relação à solução analítica, cifram-se em:

a) método de Euler para a frente no tempo, método de Euler para trás no espaço - $\sigma^2 = 0{,}0062$;

b) método de Runge-Kutta (4.ª ordem) para a frente no tempo, método de Euler para trás no espaço - $\sigma^2 = 0{,}0113$;

c) método de Euler para trás no tempo, método de Euler para trás no espaço - $\sigma^2 = 0{,}0079$;

d) método de Euler para trás no tempo, método das diferenças centrais no espaço - $\sigma^2 = 0{,}0007$;

e) método das características de Euler - $\sigma^2 = 0{,}0060$;

f) método das características de Runge-Kutta (4.ª ordem) - $\sigma^2 = 0{,}0000$.

Uma análise de estabilidade mostra que dos métodos para a frente no tempo, método de Euler para trás no espaço, o de Euler se torna instável quando $\frac{v \cdot \Delta t}{\Delta x} > 1$, enquanto para o de Runge-Kutta (4.ª ordem) a situação só ocorre se $\frac{v \cdot \Delta t}{\Delta x} > 1{,}5$. Por outro lado, os métodos de Euler para trás no tempo, método de Euler para trás, ou das diferenças centrais, no espaço, são ambos intrinsecamente estáveis. Finalmente, os métodos das características, quer de Euler, quer de Runge-Kutta (4.ª ordem), obrigam a que $\frac{v \cdot \Delta t}{\Delta x} = 1$, conforme já foi explicado.

Os resultados obtidos correspondem, mais ou menos, ao que seria de esperar, com a notável excepção de os valores de σ^2 do método de Euler para a frente no tempo, método de Euler para trás no espaço serem inferiores aos do método de Runge-Kutta (4.ª ordem) para a frente no tempo, método de Euler para trás no espaço. A explicação do facto, prende-se com uma descontinuidade na derivada em ordem ao tempo, que se verifica alguns momentos após o instante inicial, quando a perturbação da temperatura chega ao ponto em estudo. Como é lógico, um método de aproximação linear das derivadas em ordem ao tempo, tipo Euler, acompanha melhor um tal fenómeno, que outro de ordem mais elevada!

Apresenta-se, em seguida, um gráfico dos resultados, usando o método de Euler para trás no tempo (M. E. T. T.), método das diferenças centrais no espaço (M. D. C. E.), mas com uma malha menos apertada do ponto de vista temporal - $\Delta t = 2$ - que evita a sobrecarga da imagem e demonstra, simultaneamente, a estabilidade do esquema para $\frac{v \cdot \Delta t}{\Delta x} > 1$:

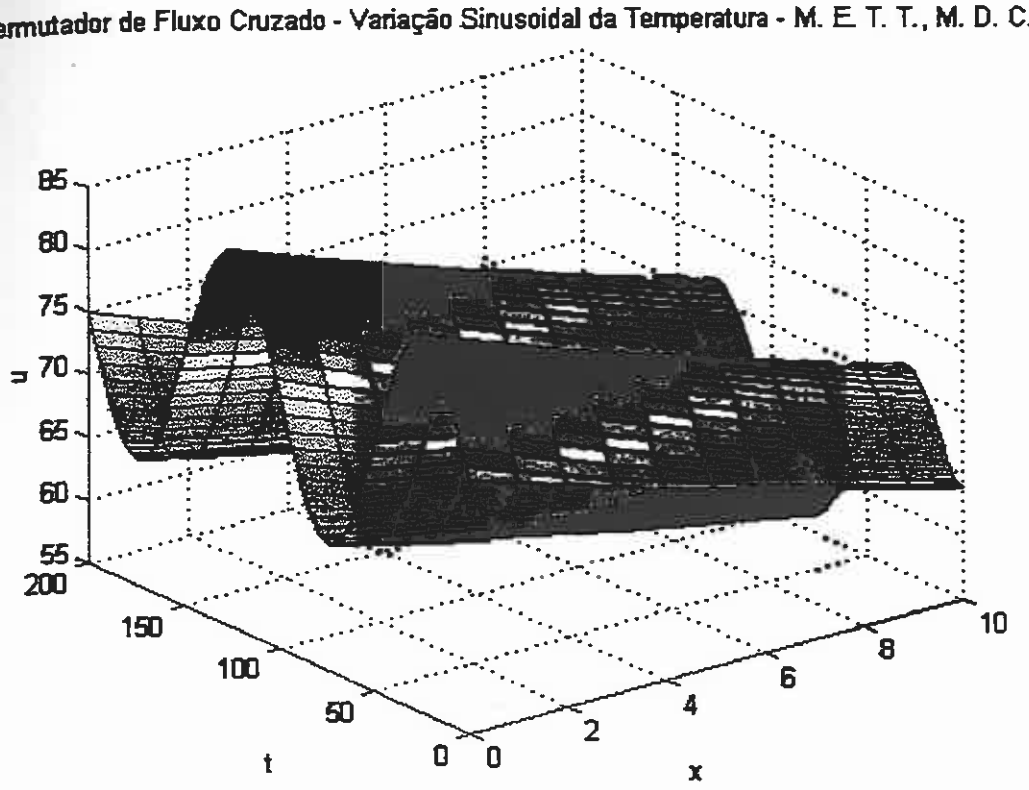


Figura 1

Quando a temperatura de entrada do fluido que se deseja arrefecer/aquecer permanece constante, mas as sua velocidade varia, supôs-se, sempre em unidades S. I., que: $L = 10; \Delta x = 1; \Delta t = 0{,}5; u_o = 25; v_e = 2; v_a = 0{,}8; k = 0{,}05; u_e = 75; T = 100$.

Usando sempre a mesma linguagem, escreveram-se outros programas e determinaram-se, também relativamente à solução analítica, os novos erros quadráticos médios, cujos valores são:

a) método de Euler para trás no tempo, método de Euler para trás no espaço - $\sigma^2 = 0{,}0136$;

b) método de Euler para trás no tempo, método das diferenças centrais no espaço - $\sigma^2 = 0{,}0001$.

Inclui-se, em continuação, uma representação gráfica dos resultados gerados pela aplicação do método de Euler para trás no tempo, método das diferenças centrais no espaço, onde se fez $\Delta t = 4$, a fim de evitar um detalhe excessivo que torna a imagem menos legível e prova, mais uma vez, a estabilidade do esquema quando $\frac{v \cdot \Delta t}{\Delta x} > 1$:

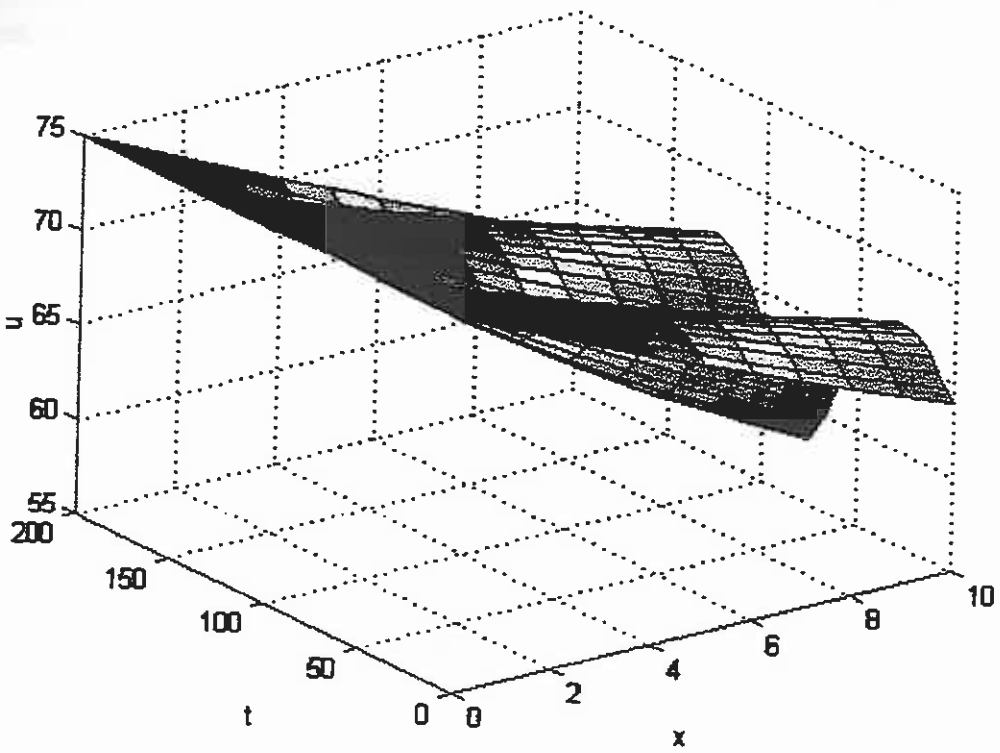


Figura 2

4. Conclusões

O estudo efectuado mostra que, na integração de equações diferenciais parciais do tipo considerado, o esquema numérico de diferenças finitas correspondente ao método de Euler para trás no tempo, método das diferenças centrais no espaço, apresenta vantagens significativas, em termos quer de estabilidade, quer de precisão.

No que diz respeito ao primeiro aspecto, tratando-se de um método para trás no tempo, não tem competição, excepto por parte do outro que pertence ao mesmo grupo, como seria de esperar. Quanto ao segundo, o único esquema alternativo que mostrou superioridade foi o método das características de Runge-Kutta (4.ª ordem). Infelizmente, este método não se adapta bem aos casos, de significativa importância prática, em que o caudal e, portanto, a velocidade do fluido a arrefecer/aquecer dependem do tempo.

Finalmente, a desvantagem decorrente da necessidade de resolver uma sucessão de sistemas de equações algébricas lineares, não constitui óbice significativo, porque a respectiva matriz dos coeficientes é tridiagonal, o que permite a utilização de métodos de resolução que diminuem significativamente a complexidade computacional do problema.

Bibliografia

[1] – Cruces, J. – Transient Analysis of Heat Exchangers, incluída na lista oficial das comunicações da conferência Matlab'97, realizada em Outubro de 1997, em San Jose, California, U. S. A.

[2] – Nakamura, S. – Applied Numerical Methods with Software, Prentice-Hall Inc., Englewood Cliffs, N.J., 1991.

[3] – Foust, A.; Wenzel, L.; Clump, C.; Maus, L.; Andersen, L. – Principles of Unit Operations, John Wiley & Sons, Inc., New York, 1960.

Computação simbólica e numérica – um caso paradigmático

Heitor L. Pina
Instituto Superior Técnico

Resumo

Neste artigo apresenta-se um caso de aplicação da computação simbólica à resolução aproximada das equações da Dinâmica de Fluidos aplicadas concretamente à modelação de um lago solar. São realçadas as vantagens deste procedimento e sublinhadas as principais diferenças relativamente aos métodos puramente numéricos.

1 Introdução

Um lago solar é uma bacia de água que absorve e armazena a energia solar. Esta absorção de energia cria um gradiente de temperatura na direcção vertical o qual tende a produzir movimentos de convecção que reduzem a capacidade de armazenamento do lago (ver a Fig. 1.1). Assim, para aumentar a eficácia do lago como dispositivo armezenador, é necessário contrariar estas correntes convectivas o que é feito estabelecendo artificialmente um gradiente salino que aumenta a densidade da água na zona mais quente, o fundo do lago. Resultam daqui dois problemas interessantes:

- o estudo da estabilidade do lago perante duas tendências opostas: o gradiente de temperatura (desestabilizador) e o gradiente salino (estabilizador);
- a modelação da dinâmica do lago em condições realistas e por períodos de tempo longos, tipicamente, um a dois anos.

Portugal teve um lago solar experimental entre 1982 e 1990 que permitiu recolher um volume razoável de dados. Em 1995 foi iniciado um programa de investigação com vista a estudar por via teórica a estabilidade do lago e a construir um modelo analítico-numérico que possibilitasse a simulação do seu comportamento

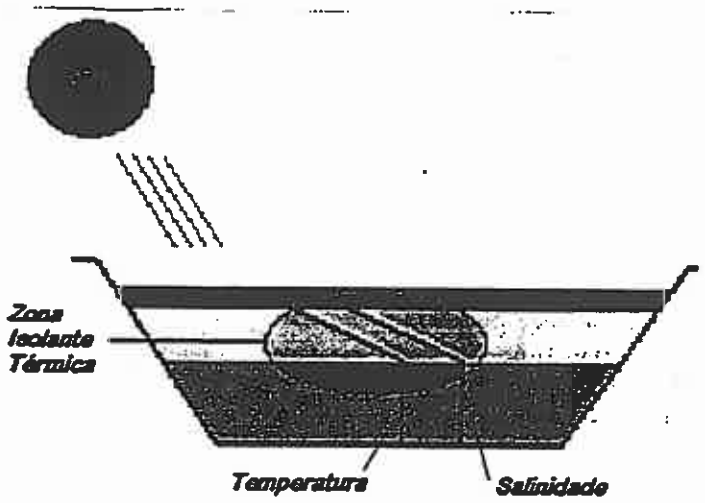


Figura 1.1: Esquema de um lago solar

2 Modelo matemático

Para efeitos de modelação o lago vai ser considerado como possuindo uma geometria rectangular, com coordenada horizontal x e vertical z. A dinâmica do lago é regida pelas equações de Navier-Stokes bidimensionais com a aproximação de Boussinesq (para o desenvolvimento detalhado, consultar (4) e (2)). Assim, temos:

$$\begin{aligned}
&\text{(Balanço de massa)} && \nabla \cdot \mathbf{v} = 0 \\
&\text{(Balanço de momento linear)} && \partial_t \mathbf{v} + (\mathbf{v}\cdot\nabla)\mathbf{v} = -\frac{1}{\rho_m}\nabla p + g(\alpha T - \beta S)\mathbf{k} + \nu\nabla^2\mathbf{v} \\
&\text{(Difusão do calor)} && \partial_t T + \mathbf{v}\cdot\nabla T = K_T\nabla^2 T + \frac{q}{\rho C_p} \\
&\text{(Difusão do sal)} && \partial_t S + \mathbf{v}\cdot\nabla S = K_S\nabla^2 S \\
&\text{(Equação de estado)} && \rho = \rho_m(1 - \alpha T + \beta S) \\
&\text{com} && \alpha = -\frac{1}{\rho}\partial_T\rho, \qquad \beta = \frac{1}{\rho}\partial_S\rho
\end{aligned} \tag{2.1}$$

As variáveis independentes são x, z e o tempo t. A velocidade $\mathbf{v}$, a temperatura T e a concentração salina S são funções das variáveis independentes a determinar mediante a solução deste sistema de equações às derivadas parciais, complementado com condições iniciais

$$\begin{aligned}
\mathbf{v}(x,z,0) &= \mathbf{v}_0(x,z) \\
T(x,z,0) &= T_0(x,z) \\
S(x,z,0) &= S_0(x,z)
\end{aligned} \tag{2.2}$$

e condições de fronteira apropriadas (consultar (3), (4) e (2) para mais detalhes).

A equação do balanço de massa pode ser satisfeita identicamente se exprimirmos a velocidade em termos da função de corrente ψ,

$$\mathbf{v} = (u, v, w) = (\partial_z \psi, 0, -\partial_x \psi) \tag{2.3}$$

e sendo, deste modo, eliminada do sistema (2.1). As variáveis dependentes ficam assim a ser os campos escalares ψ, T e S.

3 Método de solução

Tradicionalmente, os problemas envolvendo equações diferenciais são resolvidos tentando métodos analíticos (leia-se exactos). No entanto esta via só se mostra frutuosa nos casos mais simples. O problema formulado, como aliás quase todos os que envolvem equações diferenciais não-lineares, é demasiado complicado para estes métodos poderem ser aplicados pelo que se desenvolveram métodos aproximados, numéricos, de que se destacam o método das diferenças finitas e, mais recentemente, o método dos elementos finitos.

Com o aparecimento e desenvolvimento, sobretudo nas décadas de 70 e 80, de manipuladores simbólicos ou sistemas de álgebra computacional (por exemplo: AXIOM (6), MAPLE (1), MATHEMATICA (9)), tornou-se possível efectuar em computador muitas das tarefas laboriosas susceptíveis a erros humanos, requeridas pelos métodos analíticos. A disponibilidade desta nova ferramenta veio relançar o interesse por estes métodos ou, pelo menos, pela combinação destes com os métodos numéricos propriamente ditos. A ideia orientadora desta nova via de solução é a de levar tão longe quanto possível o trabalho analítico deixando para a via numérica a parte que, de todo em todo, não pode ser resolvida exactamente. Um ponto de partida para apreciar o desenvolvimento desta abordagem na área da Mecânica Computacional é a referência (7).

Dada a geometria simples (rectangular) Ω do problema em causa optou-se por usar um método estectral de aproximação, i.e., cada variável dependente é aproximada num subespaço de funções de classe C^∞ e cujo suporte é $\bar{\Omega}$. Note-se que este tipo de aproximação é possível graças à simplicidade da geometria; num domínio mais complicado a satisfação das condições de fronteira do problema obrigaria a recorrer a um método de diferenças finitas, ou, melhor, a um método de elementos finitos.

Por exemplo, a salinidade S é aproximada por

$$S_n(x, z, t) = \sum_{i=1}^{n} a_i(t)\phi_i(x, z) \tag{3.1}$$

em que os $\phi_i(x, z)$ são escolhidos de modo a respeitar as condições de fronteira (essenciais) apropriadas para esta variável; expressões semelhantes são propostas para a função de corrente e para a temperatura. Assim, uma vez fixados os $\phi_i(x, z)$ o problema fica reduzido à determinação dos coeficientes $a_i(t)$ que determinam a aproximação $S_n(x, z, t)$.

Para obter estes coeficientes foi empregue o método dos resíduos ponderados, ou de Galerkin, que consiste em substituir a formulação do problema em termos das equações às derivadas parciais (2.1) por uma *formulação fraca* que consiste em obrigar o *resíduo* a ser ortogonal ao um subespaço apropriado. Exemplificando com a equação da salinidade, temos que

$$\left(\partial_t S_n + \mathbf{v}\cdot\nabla S_n - K_S\nabla^2 S_n, \phi_i\right), \qquad i = 1,\ldots,n \tag{3.2}$$

onde

$$(f,g) \equiv \int_\Omega f(x,z)g(x,z)\,\mathrm{d}x\,\mathrm{d}z$$

designa o produto interno e Ω o domínio rectangular do lago. Efectuando os cálculos necessários, os quais envolvem algiumas integrações por partes e a introdução das condições de fronteira, cujos detalhes se omitem por brevidade (ver (3), (4) e (2)), chegamos à seguinte relação

$$(\partial_t S_n, \phi_i) + \tau\,(\nabla S_n\cdot\nabla\phi_i, 1) + (\partial_x\psi_n, \phi_i) - (J(\psi_n, S_n), \phi_i) = 0, \qquad i = 1,\ldots,n \tag{3.3}$$

em que

$$J(f,g) = \partial_x f\partial_z g - \partial_z f\partial_x g$$

e $\tau = K_S/K_T$ é o inverso do número de Schmidt.

Uma vantagem da formulação fraca reside no facto de apenas as condições de fronteira *essenciais* necessitarem de ser satisfeitas à partida pelas funções S_n o que dá mais liberdade na escolha das formas admissíveis para estas funções.

Aplicado o procedimento acabado de descrever a todas as equações de (2.1), obtem-se como resultado final um sistema de equações diferenciais ordinárias não-linear nos coeficientes $a_i(t),\ldots$ o qual pode ser resolvido por um método numérico adequado, por exemplo, Runge-Kutta de quarta ordem com controlo de passo (RK45, (8)).

Uma análise de (3.3) revela que, admitindo que todas as aproximações recorrem a n termos, o esforço computacional para formar o sistema de equações diferenciais ordinárias se centra em calcular $\mathcal{O}(n^3)$ integrais resultantes do termo $(J(\psi_n, S_n), \phi_i)$ e $\mathcal{O}(3n^2)$ integrais resultantes dos restantes termos. Para os valores de n em vista – da ordem da dezena – o esforço computacional é pois dominado pelo termo do jacobiano.

4 Alguns aspectos

Uma vez estabelecida a formulação fraca, a tarefa seguinte á da escolha das funções de aproximação. No caso presente, dadas as condições de fronteira do problema, optou-se por tomar como funções tentativa e teste funções do tipo

$$\phi_i = \xi^{r_i}\sin(\xi)^{p_i}\cos(\xi)^{q_i} \tag{4.1}$$

em que ξ é uma versão adimensionalizada de x ou de z e τ_i, p_i, q_i são expoentes inteiros não negativos. Atendendo a que estas funções entram nos produtos internos que figuram em (3.3), torna-se necessário calcular integrais da forma

$$(\phi_i, \phi_j) = \int_\Omega \xi^{\tau_i} \sin(\xi)^{p_i} \cos(\xi)^{q_i} \xi^{\tau_j} \sin(\xi)^{p_j} \cos(\xi)^{q_j} \, \mathrm{d}\Omega \tag{4.2}$$

os quais, por separação de variáveis, se podem reduzir ao cálculo de integrais do tipo

$$\int \xi^{\tau} \sin(\xi)^{p} \cos(\xi)^{q} \, \mathrm{d}\xi \tag{4.3}$$

Mesmo para uma aproximação modesta, o número de integrais que é necessário calcular é enorme. Por exemplo, para uma aproximação com 6 funções por cada uma das variáveis dependentes Ψ, T e S, no total de 18 graus de liberdade, conduzindo portanto a 18 EDO's, este número é da ordem de 10^4. Uma aplicação directa do procedimento de integração `int` do Maple revelou-se desastrosa. Não só o tempo de cálculo atingia facilmente a dezena de horas (num PC a 200 MHz) como o comprimento das expressões intermédias crescia de tal modo que a memóra disponível era facilmente excedida, com o consequente bloqueio da execução do programa.

Todas as tentativas de simplificação ou não resultaram ou produziram melhorias marginais. A solução encontrada foi a de tirar partido da estrutura especial dos integrais (4.3), que permitia que fossem calculados utilizando as fórmulas de recorrência de (5). Para tal torna-se necessário 'ensinar' o programa a reconhecer aquelas fórmulas e a identificar os expoentes τ, p e q. A solução encontrada consta dos procedimentos que se incluem nas Figs. 4.1, 4.2 e 4.3. O tempo de cálculo foi reduzido a alguns minutos, deste modo viabilizando a abordagem adoptada para o problema.

5 Conclusões e comentários finais

Um aspecto interessante que merece um comentário é o da complexidade computacional. Em programs puramente numéricos, a complexidade de um algoritmo é geralmente medida pela memória gasta e pelo número de operações aritméticas envolvidas (em flops). Em computação simbólica, estes parâmetros continuam naturalmente a ser importantes, sobretudo o segundo se a aritmética em ponto flutuante for simulada por *software* em vez de ser efectuada por *hardware* nativo. Todavia, surge uma outra dimensão que pode assumir um papel dominante que é o do crescimento das expressões matemáticas, ou, melhor dizendo, da sua representação pelo sistema de computação simbólica. Este crescimento tende a ser exponencial e, se não forem tomadas as devidas precauções, pode facilmente esgotar a memória disponível ou conduzir a tempos de cálculo incomportáveis. Este aspecto é um dos que mais surpreende os analistas numéricos recém chegados à computação simbólica.

Agradecimentos

O presente trabalho foi apoiado pelo IST, INETI e IDMEC, Lisboa e pelo Programa PRAXIS e resulta de uma colaboração com M. Giestas e A. Joyce.

Referências

[1] B. W. Char, K. O. Geddes, G. H. Gonnet, B. L. Leong, M. B. Monagan, and S. M. Watt. *MAPLE V: Language Reference Manual.* Springer-Verlag, 1991.

[2] M. Giestas, A. Joyce, and H. Pina. The influence of non-constant diffusivities on solar pond stability. *Int. J. Heat Mass Transfer*, 40(18):4379–4391, 1997.

[3] M. Giestas, H. Pina, and A. Joyce. The use of symbolic computayion in fluid stability problems. In Arantes e Oliveira, J. Bento, and G. Maier, editors, *Proc. of EPMESC V*, volume 2, pages 13377–1343. Techno Press, 1995.

[4] M. Giestas, H. Pina, and A. Joyce. The influence of radiation absortion on solar pond stability. *Int. J. Heat Mass Transfer*, 39(18):3873–3885, 1996.

[5] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals, Series and Products.* Academic Press, 1980.

[6] R. D. Jenks and R. S. Sutor. *AXIOM – The Scientific Computation System.* Springer-Verlag, 1992.

[7] A. K. Noor. List of books, monographs, conference proceedings and short courses on symbolic computations. In A. K. Noor, I. Elishakov, and G. Hulbert, editors, *1990 Winter Annual Meeting of the American Society of Mechanical Engineers*, pages vii–xii. ASME, 1990.

[8] Heitor Pina. *Métodos Numéricos.* McGraw Hill, 1995.

[9] S. Wolfram. *Mathematica — A System for Doing Mathematics by Computer.* Addison-Wesley, 1988.

```
# Proc IXMSN computes int (xi^m*sin(xi)^n, xi=a..b)
#
IXMSN := proc(m, n)
local a, b, val, aux, auxa, auxb, auxab;
option remember;
     a := 0; b := Pi;
    if m*n = 0 then val := int(xi^m*sin(xi)^n, xi = a .. b)
    elif m*n = 1 then val := int(xi*sin(xi), xi = a .. b)
    elif 1 < m*n then
    aux := xi^(m - 1)*sin(xi)^(n - 1)*(m*sin(xi) - n*xi*cos(xi)) /n^2;
        auxa := subs(xi = a, aux);
        auxb := subs(xi = b, aux);
        auxab := eval(auxb - auxa);
        if n = 1 then val := auxab - m*(m - 1)*IXMSN(m - 2, 1) fi ;
        if m = 1 then val := auxab + (n - 1)*IXMSN(1, n - 2)/n fi ;
        if 1 < m and 1 < n then
          val := auxab + (n - 1)*IXMSN(m, n - 2)/n - m*(m - 1)*IXMSN(m - 2, n)/n
        fi;
        val := evalf(val)
end
#
# Proc IXMCN computes int (xi^m*cos(xi)^n, xi=a..b)
*
IXMCN := proc(m, n)
local a, b, val, aux, auxa, auxb, auxab;
option remember;
    a := 0;
    b := Pi;
    if m*n = 0 then val := int(xi^m*cos(xi)^n, xi = a .. b)
    elif m*n = 1 then val := int(xi*cos(xi), xi = a .. b)
    elif 1 < m*n then
      aux := xi^(m - 1)*cos(xi)^(n - 1)*(m*cos(xi) + n*xi*sin(xi)) /n^2;
      auxa := subs(xi = a, aux);
      auxb := subs(xi = b, aux);
      auxab := eval(auxb - auxa);
      if n = 1 then val := auxab - m*(m - 1)*IXMCN(m - 2, 1) fi ;
      if m = 1 then val := auxab + (n - 1)*IXMCN(1, n - 2)/n fi ;
      if 1 < m and 1 < n then
        val := auxab + (n - 1)*IXMCN(m, n - 2)/n - m*(m -1)*IXMCN(m - 2, n)/n^2
      fi:
    fi;
    val := evalf(val)
end
```

Figura 5.1: Fragmento do programa em Maple

```
#
# Proc IXRSPCQ computes int (xi^r * sin(xi)^p * cos(xi)^q, xi=a..b)
#
IXRSPCQ := proc(r, p, q)
local a, b, val, aux, auxa, auxb, auxab;
option remember;
    a := 0;
    b := Pi;
    if p = 0 then val := IXMCN(r, q)
    elif q = 0 then val := IXMSN(r, p)
    elif 0 < p and 0 < q then
        aux := (p + q)*xi^r*sin(xi)^(p + 1)*cos(xi)^(q - 1)
             + r*xi^(r - 1)*sin(xi)^p*cos(xi)^q;
        auxa := subs(xi = a, aux);
        auxb := subs(xi = b, aux);
        auxab := eval(auxb - auxa);
        if r = 0 then
            if q = 1 then val := auxab; val := val/(p + q)^2
            else
              val := auxab + (q - 1)*(p + q)*IXRSPCQ(r, p, q - 2);
              val := val/(p + q)^2
            fi
        elif r = 1 then
            if q = 1 then
                val := auxab - r*p*IXRSPCQ(r - 1, p - 1, q - 1);
                val := val/(p + q)^2
            else
                val := auxab - r*p*IXRSPCQ(r - 1, p - 1, q - 1)
                     + (q - 1)*(p + q)*IXRSPCQ(r, p, q - 2);
                val := val/(p + q)^2
            fi
        elif 1 < r then
            if q = 1 then
                val := auxab - r*p*IXRSPCQ(r - 1, p - 1, q - 1)
                     - r*(r - 1)*IXRSPCQ(r - 2, p, q);
                val := val/(p + q)^2
            else

                val := auxab - r*p*IXRSPCQ(r - 1, p - 1, q - 1)
                     - r*(r - 1)*IXRSPCQ(r - 2, p, q)
                     + (q - 1)*(p + q)*IXRSPCQ(r, p, q - 2);
                val := val/(p + q)^2
            fi
        fi
    fi;
    val := evalf(val)
end
#
```

```
INTXSC := proc(func)
#
local nterms, s, i, fun, op1, const, td, dsxi, dseta, dcxi, dceta,
dxi, deta,ixi,ieta;
  if hastype(func, '+') then  nterms := nops(func)
  else nterms := 1 fi;
  s:= 0;
  for i to nterms do
  if nterms = 1 then fun := func; else fun := op(i,func);  fi;
  if type (fun,numeric) then const := fun
  elif type(op(1,fun),numeric) then const := op(1,fun);
   else const:=1  fi;
   else const:=1 fi;
          td:= degree(fun);
          dsxi:= degree(fun,sin(xi));
          dseta:= degree(fun,sin(eta));
          dcxi:= degree(fun, cos(xi));
          dceta:= degree(fun, cos(eta));
          dxi:= degree(fun/sin(xi)^dsxi/cos(xi)^dcxi,xi);
          deta:= degree(fun/sin(eta)^dseta/cos(eta)^dceta,eta);
   ixi:=IXRSPCQ(dxi,dsxi,dcxi);
   ieta:=IXRSPCQ(deta,dseta,dceta);
   s:= s + evalf(const*ixi*ieta)
  od;
end;
```

Figura 5.3: Fragmento do programa em Maple (cont.)

A Investigação Operacional e suas aplicações nos aspectos tácticos e logísticos das operações militares

Marçal Lourenço

Comando Logística – E. M. E.
Av. Infante Santo, 49
1350 Lisboa

"A protecção com revestimentos de metal é menos importante que cereais e alimentos"

Esta afirmação é referida por SUN TZU no seu livro A Arte da Guerra , tratado militar escrito na China 500 anos antes de Cristo e considerado como muito marcante no pensamento militar Japonês.

Ela revela a necessidade já nessa altura sentida , da importância de uma disciplina que tivesse como objectivo fundamental proporcionar os meios às forças armadas.

Foi Henry Jomini, escritor militar suíço e coronel ao serviço de Napoleão quem no seu livro "Precis de l'art de la Guerre" usou pela primeira vez a palavra Logística definindo-a como "tudo o que inclui a preparação e manutenção das campanhas" iniciando assim um novo ramo de conhecimentos militares.

Nos exércitos antigos dava-se mais realce aos aspectos tácticos e estratégicos do que à logística . Napoleão, embora reconhecendo importância aos aspectos logísticos não os levava por vezes em consideração, sendo, segundo vários historiadores, uma das razões de algumas das suas derrotas, nomeadamente nas campanhas da Rússia onde falharam os abastecimentos às tropas .

Verifica-se que até à 1ª Guerra Mundial o uso que se fez da expressão Logística foi bastante limitado e o estudo da logística e o conceito moderno que lhe anda ligado, resultaram do largo uso que da mesma se fez e do amplo significado que lhe atribuíram as forças armadas dos Estados Unidos durante a 2ª Guerra Mundial .

Muitos de vós com certeza viram filmes sobre a 2ª Guerra Mundial . nomeadamente mostrando o desembarque aliado na Normandia , (muito recentemente estreou um filme de Spilberg focando o mesmo tema) mas não sei é se conseguiremos apercebermo-nos das

quantidades astronómicas de homens e abastecimentos que foi preciso colocar no continente Europeu em espaço e tempo reduzidos .

Mas é o eclodir da Guerra do Golfo que vem mostrar ainda mais o quanto é importante a Logística chegando alguns autores a considerá-la como elemento fundamental no desenvolvimento do combate, alterando a filosofia que até aí existia.

Esta considerava que a logística devia apoiar o desenrolar das operações . Pensa-se agora que a logística determina até que ponto se pode desenvolver o aspecto operacional. A título de exemplo, refira-se o pré-posicionamento de munições como factor determinante para os êxitos da artilharia, e a necessidade de abastecimento de água e outros materiais para satisfazer em qualidade e em quantidade no momento e lugar oportuno as exigências do combate

Constatou-se na Guerra do Golfo que os dois primeiros soldados americanos feitos prisioneiros pertenciam à área da Logística e não às tropas combatentes como era usual nos conflitos anteriores, e que o oficial que mais condecorações recebeu foi o general comandante da Logística.

A aplicação de alguns modelos e técnicas de Investigação Operacional. têm sido a solução aos obstáculos e a resposta cabal para os objectivos destas missões.

Embora alguns modelos e técnicas de Investigação Operacional possam ser considerados muito mais recuados é geralmente aceite que a disciplina começou durante a 2ª Guerra Mundial.

Muitos problemas estratégicos e tácticos associados ao esforço militar dos aliados que se consideravam bastante complicados foram de uma maneira simples resolvidos por vezes por apenas um indivíduo ou por uma pequena equipa.

Quando a Marinha dos Estados Unidos concebeu o projecto do Submarino Polaris não só tinha que se preocupar com os problemas técnicos e científicos mas também com a coordenação e controlo do enorme esforço a despender.. Neste projecto havia 250 empreitadas directas e mais de 9000 subempreitadas . Era necessário encontrar uma nova técnica para concluir o projecto com eficiência dentro de um nível aceitável de custo e tempo . Em colaboração com uma empresa da especialidade iniciaram-se os conceitos básicos do método PERT (Project Evaluation and Review Technic) como instrumento de planeamento, controlo e informação .

Da aplicação desta nova técnica resultou o avanço de 2 anos num projecto com a duração total de 5 anos .

Curioso é notar que anos volvidos a aplicação de Investigação Operacional na condução das operações militares foi extraordinariamente reduzida e por vezes até esquecida, sendo em contrapartida a sua aplicação nas indústrias ditas civis o seu campo normal de aplicação.

Na maioria dos livros que abordam assuntos relacionados com Investigação Operacional os exemplos já não são relacionados com aspectos tácticos ou estratégicos de âmbito militar e a maioria das vezes nem as indústrias de defesa são focadas ..

No caso dos problemas militares verifica-se que é na área do apoio logístico que a Investigação Operacional. vai fazendo o seu regresso ao ambiente militar, desenvolvendo-se algoritmos que poderão apoiar a tomada de decisão do comandante, sendo a própria teoria da decisão uma matéria que também se está a generalizar.

O desenvolvimento e utilização vulgarizada do computador veio permitir maior facilidade e rapidez de cálculo com recurso a grande número de algoritmos de apoio á Investigação Operacional.

Exemplos de algoritmos de apoio á Investigação Operacional utilizados no campo da Logística.

Suponhamos que queremos encher um contentor com vários objectos seleccionados entre vários possíveis , de modo a utilizar o máximo de objectos e o máximo de volume á nossa disposição

Este problema pode ser formulado matematicamente numerando os objectos de 1 a **n** e introduzindo um vector de variáveis binárias x_j (j = 1... n) tendo o seguinte significado

$$x_j = \begin{cases} 1 & \text{se selecciono o objecto} \\ 0 & \text{no caso contrario} \end{cases}$$

Então se p_j for a medida da "necessidade" dada para o objecto **j** , w_j o seu tamanho e **c** o tamanho do contentor, o nosso problema será seleccionar de entre todos os vectores binários **x** satisfazendo a restrição

$$\sum_{j=1}^{n} w_j x_j \leq c$$

aquele que maximiza a função objectivo

$$\sum_{j=1}^{n} p_j x_j$$

Este algoritmo é conhecido pelo problema do Knapsack (saco mochila) e tem sido intensamente estudado , atraindo teóricos e práticos.

Vê-se que ele é fundamental para resolver situações de carregamento de navios ou aviões, mas também está a ser amplamente estudado na aplicação de verbas em investimentos.

Outro dos aspectos fundamentais da Logística é o transporte de munições, combustíveis e víveres, com economia de custos.

O "Problema de Transporte" envolve a optimização do transporte e a distribuição de bens e serviços a partir de várias origens para vários destinos É evidente que existem sempre diferentes modalidades de encaminhamento Origem-Destino, com custos diferentes.

A solução do problema obriga a que sejam calculadas quantas unidades devem ser encaminhadas de cada origem para cada destino, satisfazendo as necessidades destes com o custo total mínimo

Estrutura matemática do problema

Considerando m Origens dispondo da quantidade a_i de um bem (**i =1,...m**)

Considerando ainda **n** Destinos necessitando da quantidade b_j daquele bem (**j=1,...n**)
Existe um custo unitário c_{ij} correspondente ao transporte de uma unidade do bem de cada origem para cada destino
De cada origem **i** será transportado para cada destino **j** a quantidade x_{ij}

O modelo de PL é então

$$\text{Min } f(x)= \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\, x_{ij}$$

Restrições : 1) Da " Oferta"

$$\sum_{j=1}^{n} x_{ij} = a_i \quad (a > 0 \text{ , } i=1,...m)$$

2) Da "Procura"

$$\sum_{i=1}^{m} x_{ij} = b_j \quad (b > 0 \text{ , } j=1,...n)$$

3) Lógicas

$$x_{ij} \geq 0 \quad \text{e inteiro}$$

Num modelo equilibrado considera-se

$$\sum_{i=1}^{m} a_i = \sum_{j=1}^{n} = b_j$$

Significando que a totalidade da "Oferta" das Origens iguala a totalidade da "Procura" nos Destinos (quando a "Procura" difere da "Oferta" é necessário equilibrar o modelo)

Um dos aspectos que é de importância capital quando há necessidade de ligar várias origens com vários destinos é a obtenção das distancias mínimas.

O algoritmo Floyd-Warshall permite-nos obter as distancias mínimas e a descrição dos caminhos correspondentes a cada uma .

Este algoritmo é de extrema utilidade pois permite obter as distancias mínimas tanto no emprego de pipe-lines como no lançamento de fio telefónico ou deslocação de munições, por exemplo.

Assim seja o grafo G = (X,A) um grafo conexo, x_1 o vértice inicial, x_n o vértice final e consideremos os custos $c_{ij} \geq 0$ associados aos arcos (x_i,x_j)de G. O problema do caminho mais curto consiste em determinar o caminho entre o vértice origem x_1 e o vértice destino x_n cuja soma dos custos c_{ij} associados aos arcos que o constituem é mínima

Apresentei apenas exemplos de algoritmos que têm aplicação directa em acções logísticas , nomeadamente no que respeita á função Transporte, mas praticamente toda a teoria de Investigação Operacional é aplicada com grande utilidade na área Logística.

A logística nos tempos actuais tem nas operações militares tanta importância quanto os aspectos tácticos e melhora cabalmente os seus procedimentos apoiando-se na Investigação Operacional

No nosso país hoje em dia , felizmente , a solicitação feita ás Forças Armadas tem sido sobretudo nas operações de manutenção de paz e acções humanitárias . São do domínio público as acções desenvolvidas pelas Forças Armadas Portuguesas na Bósnia e em África.

Estas situações apoiam-se grandemente na componente logística , dando-lhe actualidade e exigindo aos profissionais de logística um elevado grau de perícia em várias especialidades tais como , stocks, transportes, gestão de manutenção , caminhos críticos , controlo , planeamento de factores humanos etc....

Muito útil e louvável seria que a comunidade científica e a militar juntassem esforços no sentido de produzir um efeito sinergético na optimização das acções logísticas

Bibliografia

Langford, John W , Principles and Applications McGraw-Hill, Logistics Series 1995

Logistica, edição do Instituto de Altos Estudos Militares- IAEM ME3000

TZU,SUN, A Arte da Guerra , tratado militar escrito há mais de 2000 mil anos , Europa América

Cañado, Santiago Guerra - El Conflito del Golfo Persico , Política y Estrategia - Abril 1991

Martello, Silvano and Toth, Paolo - Knapsack Problems, John Wiley & Sons Ltd - 1990

Chuen-Tao, Luis Yo, - PERT e CPM aplicações práticas - Pórtico

Rardin, Ronald L. ,Optimizations in Operations Research , Prentice-Hall, Inc.1998.

Ravindran, A. - Phillip, Don T. , Solberg, James J. , - Operations Research John Wiley & Sons

Limites das Propriedades Efectivas de Materiais Celulares.

Z. Dimitrovová[†] and L. Faria[‡]

Resumo.

Apresenta-se nova metodologia para o estabelecimento de limites das propriedades mecânicas efectivas de materiais celulares constituídos por células abertas. Essa metodologia foi aplicada a casos bidimensionais em [7], verificando resultados conhecidos. O trabalho presente trata modelos tridimensionais, em que os limites obtidos são novos. A metodologia apresentada permite estabelecer condições para microestruturas óptimas, que em alguns casos podem ser especificadas geometricamente.

1 Introdução

Materiais celulares têm propriedades úteis que permitem múltiplas aplicações, como absorsores de energia cinética, como isoladores térmicos, etc. Alguns destes materiais são naturais (cortiça e madeira), outros podem ser fabricados.

Um material celular é composto por uma rede de barras e cascas sólidas interligadas, formando células, que se repetem, talvez com algumas modificações, no meio celular. Materiais celulares podem ser divididos em materiais com células abertas, quando apenas barras sólidas estão presentes; e os com células fechadas, que contêm partes de cascas. De ponto de vista de estudo de propriedades mecânicas, podem ser considerados como compósitos de duas fases: sólida e vazia.

A monografia mais detalhada sobre sólidos celulares foi publicada por Gibson e Ashby, [10], mas o problema de estabelecimento de limites das propriedades efectivas não está lá tratado.

O estabelecimento de limites das propriedades mecânicas efectivas de compósitos é um assunto de investigação considerável há muitos anos. No trabalho presente estimativas de [12]-[13] e de [2] para compósitos efectivamente isotrópicos ou com simetria cúbica efectiva, respectivamente, são utilizados.

[†] IDMEC, Instituto Superior Técnico, Av. Rovisco Pais 1, 1096 Lisboa, (zdimitro@dem.ist.utl.pt ou zuzanadimitrovova@yahoo.com).

[‡] Departamento de Engenharia Mecânica, Instituto Superior Técnico, Av. Rovisco Pais 1, 1096 Lisboa.

Um dos mais importantes parâmetros que descreve um material celular particular é a densidade relativa, s, definida como razão entre a densidade de meio celular e densidade de material de fase sólida. Há duas características principais que determinam sólidos celulares:

- Dimensão das partes vazias é muito pequena em relação à dimensão do meio, o que permite utilização de teoria de homogeneização, ver [3]-[4], [9], [11], [15], [17].
- Densidade relativa é baixa, habitualmente está considerada até s=0.3, ver [10], consequentemente uma das dimensões ao nível das células é pequena, permitindo simplificação dos cálculos da teoria de homogeneização utilizando teorias estruturais como está demonstrado em [5]-[6].

Naturalmente, limites das propriedades mecânicas efectivas de materiais celulares podem ser calculados usando limites para compósitos de duas fases, introduzindo propriedades zero das partes vazias e possivelmente com posterior linearização em relação à densidade relativa. Assim podem ser obtidos limites para casos bidimensionais, onde meios celulares podem ser compostos apenas por uma rede de barras sólidas. Para o caso tridimensional foi provado em [1] que estruturas óptimas têm que conter partes de cascas. Por isso limites para materiais celulares de celular abertas têm que ser estritamente inferiores e a necessidade da nova metodologia está estabelecida.

A contribuição deste trabalho é na determinação destes limites até agora não publicados, e na especificação detalhada das microestruturas óptimas em forma de condições necessárias e suficientes, que podem ser em alguns casos especificadas geometricamente.

2 A Nova Metodologia

Como já foi dito, a metodologia foi apresentada em [7], mas apenas para o caso bidimensional.

De ponto vista de simplificação do problema, vamos assumir que o material da fase sólida é isotrópico homogéneo. Sem restrição na generalidade podemos também assumir que a microestrutura dos meios celulares em consideração é periódica. Apenas materiais efectivamente isotrópicos ou com simetria cúbica efectiva são considerados neste trabalho. A matriz de rigidez efectiva, $\mathbf{C}^*$, nestes casos tem a forma seguinte:

$$\mathbf{C}^* = \begin{bmatrix} \mathbf{C}_1^* & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2^* \end{bmatrix}, \text{ onde } \mathbf{C}_1^* = \begin{bmatrix} K^*+4^1G^*/3 & K^*-2^1G^*/3 & K^*-2^1G^*/3 \\ & K^*+4^1G^*/3 & K^*-2^1G^*/3 \\ \text{sim.} & & K^*+4^1G^*/3 \end{bmatrix} \text{ e}$$

$$\mathbf{C}_2^* = \begin{bmatrix} {}^2G^* & 0 & 0 \\ & {}^2G^* & 0 \\ \text{sim.} & & {}^2G^* \end{bmatrix}.$$

K^* representa módulo de Young, ${}^1G^*$ e ${}^2G^*$ os módulos de corte com condição de isotropia: ${}^1G^*={}^2G^*=G^*$. Asterisco determina não só propriedade efectiva mas também o facto que as constantes são adimensionadas em relação ao módulo de Young da fase sólida E_s.

De ponto de vista de modelo estrutural barras são modeladas pelas vigas e para junções dois tipos de modelação são possíveis: ou articulação ou junta rígida. De acordo com [16] termos micro-estruturas (quando vigas possivelmente curvas são ligadas principalmente pelas juntas rígidas) ou micro-treliças (quando vigas directas, de facto barras, são ligadas somente pelas articulações) são introduzidos.

A metodologia nova está baseada na expressão da energia de deformação efectiva, que pode ter forma (Σ é tensão efectiva):

$$W = \frac{1}{2}\left(\frac{\Sigma_M^2}{K^*} + \frac{\Sigma_D : \Sigma_D}{2G^*}\right) \text{ ou}$$

$$W = \frac{1}{2}\left(\frac{\Sigma_M^2}{K^*} + \frac{\Sigma_{D,12}^2 + \Sigma_{D,13}^2 + \Sigma_{D,23}^2}{{}^2G^*} + \frac{(\Sigma_{D,11} - \Sigma_{D,22})^2 + (\Sigma_{D,11} - \Sigma_{D,33})^2 + (\Sigma_{D,22} - \Sigma_{D,33})^2}{6\,{}^1G^*}\right) \quad (1)$$

para materiais efectivamente isotrópicos ou com simetria cúbica efectiva, respectivamente. Para poder exprimir desta formula uma propriedade constitutiva efectiva, a carga teste tem que ser introduzida em termos de componentes de tensão efectiva. Consequentemente componentes de deformação efectiva tem que satisfazer algumas condições, ver Tabela 1.

Carga teste	Propriedade constitutiva	Especificação de Σ	Especificação de $\mathbf{E}$
Σ^K	K^*	$\Sigma_{11}=\Sigma_{22}=\Sigma_{33}\neq 0$, $\Sigma_{ij}=0\ \forall i\neq j$	$E_{11}=E_{22}=E_{33}\neq 0$, $E_{ij}=0\ \forall i\neq j$
Σ^{1G}	${}^1G^*$	$\Sigma_{11}+\Sigma_{22}+\Sigma_{33}=0$, $\exists k$; $\Sigma_{kk}\neq 0$, $\Sigma_{ij}=0\ \forall i\neq j$	$E_{11}+E_{22}+E_{33}=0$, $\exists k$; $E_{kk}\neq 0$, $E_{ij}=0\ \forall i\neq j$
Σ^{2G}	${}^2G^*$	$\Sigma_{11}=\Sigma_{22}=\Sigma_{33}=0$, $\exists i\neq j$; $\Sigma_{ij}\neq 0$	$E_{11}=E_{22}=E_{33}=0$, $\exists i\neq j$; $E_{ij}\neq 0$
Σ^G	G^*	$\Sigma_{11}+\Sigma_{22}+\Sigma_{33}=0$, $\exists k$; $\Sigma_{kk}\neq 0$, $\exists i\neq j$; $\Sigma_{ij}\neq 0$ $\Sigma_{kk}/\Sigma_{ij}=\gamma_{ij}\ \forall i\neq j$ when $\Sigma_{ij}\neq 0$	$E_{11}+E_{22}+E_{33}=0$, $\exists k$; $E_{kk}\neq 0$, $\exists i\neq j$; $E_{ij}\neq 0$ $E_{kk}/E_{ij}=\gamma_{ij}\ \forall i\neq j$ when $E_{ij}\neq 0$

Tabela 1 – Cargas testes e especificação correspondente de componetes de tensão e deformação efectiva

Para expressão de Σ e W o operador de média sobre célula básica pode ser usado:

$$\Sigma = \frac{1}{|V|}\int_{v^*}\sigma dy = \frac{1}{|V|}\sum_i \int_{v^*_i}\sigma^i dy = \sum_i \langle \sigma^i \rangle,$$
$$\Sigma_{jk} = \sum_i \langle \sigma^i_{jk} \rangle,\ W = \sum_i \langle w^i \rangle,$$

onde σ^i e w^i são tensão e energia de deformação local, que correspondem a viga-i com volume $|V^*_i|$. O volume total da célula básica é $|V|$ e o volume da fase sólida é designado por $|V^*|$. No passo seguinte as contribuições da viga-i $\langle \sigma^i \rangle$ e $\langle w^i \rangle$ são exprimidas em termos de forças internas generalizadas.

A metodologia nova é mais fácil de aplicar quando apenas micro-treliças são consideradas. Primeiro, é possível provar que, em relação a estruturas óptimas, vigas rectilineas com área de secção transversal constante são preferíveis a vigas curvas, ver [8]. Segundo, usando conclusões formuladas em [7], apenas no caso da carga teste Σ^G estruturas óptimas de grupo das micro-treliças têm modulo de corte G* mais elevado quando micro-estrutura relacionada é considerada. Este aumento é causado pela contribuição de flexão, é diferente para diferentes estruturas G*-óptimas mas não é significativo, e a tangente em s=0 coincide com modulo G* anterior, i.e. para micro-treliça.

3 A Nova Metodologia Aplicada Dentro de Micro-Treliças

Vamos considerar uma célula básica composta pelas n barras com área de secção transversal constante ao longo da barra. A barra-i tem comprimento l_i, área de secção transversal A_i, força normal interna N_i e a sua posição está determinada pelos ângulos $\theta_i \in \langle 0, \pi)$ e $\varphi_i \in \langle 0, 2\pi)$ em relação às coordenadas y_j, j=1,2,3, ver Figura 1. Depois:

$$\langle \sigma^i \rangle = \frac{N_i l_i}{|V|}\begin{bmatrix} \cos^2\varphi_i \sin^2\theta_i; & \sin\varphi_i \cos\varphi_i \sin^2\theta_i; & \cos\varphi_i \sin\theta_i \cos\theta_i \\ & \sin^2\varphi_i \sin^2\theta_i; & \sin\varphi_i \sin\theta_i \cos\theta_i \\ \text{sim.} & & \cos^2\theta_i \end{bmatrix} \text{ e}$$

$$\langle w^i \rangle = \frac{1}{2|V|E_s}\left(N_i^2 \frac{l_i}{A_i}\right).$$

É conveniente usar notação:

$${}^1\Omega_i = \cos^2\varphi_i \sin^2\theta_i,\ {}^2\Omega_i = \sin^2\varphi_i \sin^2\theta_i,\ {}^3\Omega_i = \cos^2\theta_i;$$
$${}^1\Phi_i = \sin\varphi_i \sin\theta_i \cos\theta_i,\ {}^2\Phi_i = \cos\varphi_i \sin\theta_i \cos\theta_i,\ {}^3\Phi_i = \sin\varphi_i \cos\varphi_i \sin^2\theta_i;$$
$${}^1\Psi_i = \sin^2\varphi_i \sin^2\theta_i - \cos^2\theta_i,\ {}^2\Psi_i = \cos^2\theta_i - \cos^2\varphi_i \sin^2\theta_i,\ {}^3\Psi_i = \cos(2\varphi_i)\sin^2\theta_i;$$

e introduzir os vectores seguintes, ver [7]:

$$\mathbf{N}=\left\{\mathrm{N}_1\sqrt{\frac{l_1}{\mathrm{A}_1}},\mathrm{N}_2\sqrt{\frac{l_2}{\mathrm{A}_2}},\ldots,\mathrm{N}_n\sqrt{\frac{l_n}{\mathrm{A}_n}}\right\},$$

$${}^{j}\mathbf{R}=\left\{{}^{j}\Omega_1\sqrt{l_1\mathrm{A}_1},{}^{j}\Omega_2\sqrt{l_2\mathrm{A}_2},\ldots,{}^{j}\Omega_n\sqrt{l_n\mathrm{A}_n}\right\},\ \mathrm{j}=1,2,3,$$

$${}^{j}\mathbf{Q}=\left\{{}^{j}\Phi_1\sqrt{l_1\mathrm{A}_1},{}^{j}\Phi_2\sqrt{l_2\mathrm{A}_2},\ldots,{}^{j}\Phi_n\sqrt{l_n\mathrm{A}_n}\right\},\ \mathrm{j}=1,2,3,$$

$$\mathbf{L}=\left\{\sqrt{l_1\mathrm{A}_1},\sqrt{l_2\mathrm{A}_2},\ldots,\sqrt{l_n\mathrm{A}_n}\right\},$$

$${}^{1}\mathbf{P}={}^{2}\mathbf{R}-{}^{3}\mathbf{R},\ {}^{2}\mathbf{P}={}^{3}\mathbf{R}-{}^{1}\mathbf{R},\ {}^{3}\mathbf{P}={}^{1}\mathbf{R}-{}^{2}\mathbf{R}.$$

Obviamente:

$${}^{j}\mathbf{P}=\left\{{}^{j}\Psi_1\sqrt{l_1\mathrm{A}_1},{}^{j}\Psi_2\sqrt{l_2\mathrm{A}_2},\ldots,{}^{j}\Psi_n\sqrt{l_n\mathrm{A}_n}\right\},\ \mathrm{j}=1,2,3\ \text{e}$$

$${}^{1}\mathbf{P}+{}^{2}\mathbf{P}+{}^{3}\mathbf{P}=\mathbf{0},\ {}^{1}\mathbf{R}+{}^{2}\mathbf{R}+{}^{3}\mathbf{R}=\mathbf{L},$$

$$\left\|{}^{1}\mathbf{P}\right\|^2+\left\|{}^{2}\mathbf{P}\right\|^2+\left\|{}^{3}\mathbf{P}\right\|^2+\left\|{}^{1}\mathbf{Q}\right\|^2+\left\|{}^{2}\mathbf{Q}\right\|^2+\left\|{}^{3}\mathbf{Q}\right\|^2=2\|\mathbf{L}\|^2,$$

$$\mathrm{s}=\|\mathbf{L}\|^2/|\mathrm{V}|,$$

onde $\|\ \|$ é norma Euclidean. A tensão efectiva pode ser exprimida como:

$$\Sigma^{\mathrm{T}}=\frac{1}{|\mathrm{V}|}\mathbf{S}\cdot\mathbf{N}^{\mathrm{T}}=\frac{1}{|\mathrm{V}|}\left\{{}^{1}\mathbf{R},{}^{2}\mathbf{R},{}^{3}\mathbf{R},{}^{1}\mathbf{Q},{}^{2}\mathbf{Q},{}^{3}\mathbf{Q}\right\}^{\mathrm{T}}\cdot\mathbf{N}^{\mathrm{T}},\qquad(2)$$

onde $\Sigma=\{\Sigma_{11},\Sigma_{22},\Sigma_{33},\Sigma_{23},\Sigma_{31},\Sigma_{12}\}$, $\mathbf{S}$ é matriz estática modificada e "·" designa multiplicação de matrizes. Estas formulas são suficientes para poder exprimir a razão que define uma das propriedades constitutivas de formula (1) e condições adicionais nas forças normais internas usando formula (2) e coluna 3 da Tabela 1. Condições de maximalidade são obtidas como condições que asseguram igualdade em posteriores estimativas dessa razão. Nas estimativas são utilizadas basicamente desigualdade de Schwarz e alguns factos de algebra linear. Mas estas estimativas não podiam ser desenvolvidas geralmente sem utilização de mais um pressuposto relacionado com limite de Voight, ver [14], que pode ser escrito em forma:

$$\mathbf{S}^{\mathrm{T}}\cdot\mathbf{E}=\mathbf{N}/\mathrm{E}_s,$$

onde $\mathbf{E}=\{\mathrm{E}_{11},\mathrm{E}_{22},\mathrm{E}_{33},2\mathrm{E}_{23},2\mathrm{E}_{31},2\mathrm{E}_{12}\}$. A condição de maximalidade é obtida pela introdução das condições especificadas na coluna 4 da Tabela 1.

Os resultados obtidos são presentes em Tabela 2. As provas para casos de ${}^{1}G^*$ e ${}^{2}G^*$ são bastante compridas, mas permitem uma descrição única de micro-treliças óptimas. Os meios mais simples destes grupos estão nas Figuras 2 e 3. O G*-limite foi estabelecido usando sobreposição dos resultados anteriores, que pode ser usada em alguns casos, ver [7].

Constante constitutiva	Limite	Condições de maximalidade	Condições adicionais
K^*	s/9	$N//L$	$^1R\cdot L^T=^2R\cdot L^T=^3R\cdot L^T$ & $^iQ\perp L\ \forall i$
$^1G^*$	s/6	Possível especificação geométrica	
$^2G^*$	s/9	Possível especificação geométrica	
G^*	s/15	$N=\lambda_i{}^iP+\mu_j{}^jQ$	$\left\|^1R\right\|=\left\|^2R\right\|=\left\|^3R\right\|$ & $\cos(^1R,^2R)=\cos(^2R,^3R)=\cos(^3R,^1R)$ & $^iQ\perp{}^jR\ \forall i,j$ & $^1Q\perp{}^2Q\perp{}^3Q$ & $\left\|^1Q\right\|=\left\|^2Q\right\|=\left\|^3Q\right\|$

Tabela 2 – Limites e condições necessárias e suficientes para micro-treliças óptimas

4 Conclusão

A metodologia nova apresentada neste trabalho é completamente geral para materiais celulares de células abertas e permite estabelecer valores limites de propriedades mecânicas ainda não encontradas. Em relação a direcções principais das cargas testes examinadas neste trabalho, pode-se concluir que apenas no caso de Σ^{1G} este conhecimento é útil, porque só neste caso as direcções principais de Σ^{1G} concordam com as direcções das barras das estruturas Σ^{1G}–óptimas.

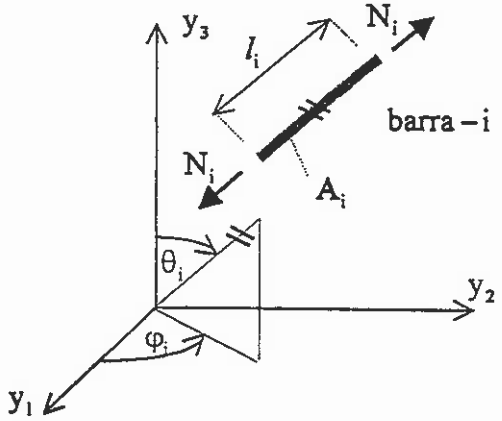


Figura 1 – Especificação da barra-i

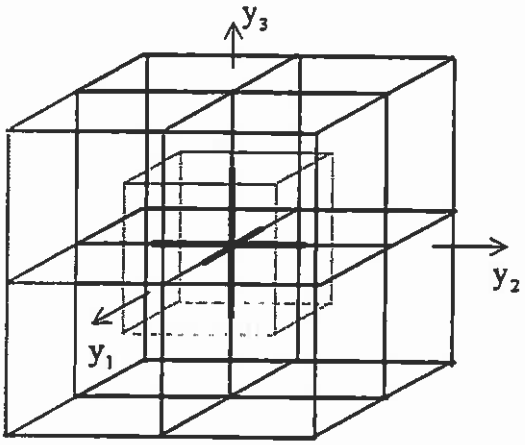


Figura 2 – Micro-treliça mais simples [1] G-óptima, a célula básica possível tem barras mais grosas*

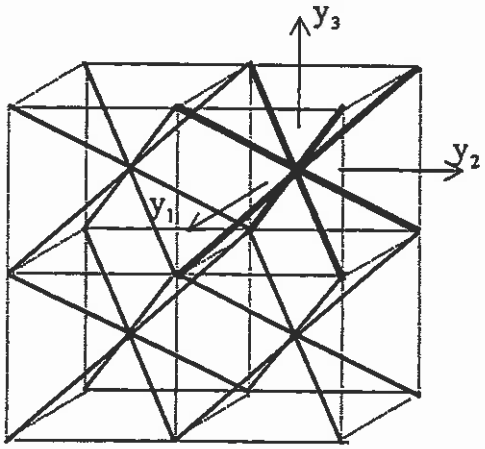


Figura 3 – Micro-treliça mais simples [2] G-óptima, a célula básica possível tem barras mais grosas*

Bibliografia

[1] G. Allaire e R. V. Kohn, Optimal Design for Minimum Weight and Compliance in Plane Stress Using Extremal Microstructures, *Eur. J. Mech., A/Solids*, vol. 12, pp. 839-878, 1993.

[2] M. Avellaneda, Optimal Bounds and Microgeometries for Elastic Two-Phase Composites, *J. Appl. Math., SIAM*, vol. 47, pp. 1216-1228, 1987.

[3] N. Bakhvalov e G. Panasenko, *Homogenization: Averaging Processes in Periodic Media*, Dordrecht, Boston, London, Kluwer Academic Publishers, 1989.

[4] A. Bensoussan, J. L. Lions e G. Papanicolau, *Asymptotic Analysis for Periodic Structures*, North Holland, Amsterdam, 1978.

[5] Z. Dimitrovová e L. Faria, Mechanical Behavior of the Cellular Solids in the Linear Range, Part I – Determination of Effective Properties Using Structural Theories, *Eur. J. Mech., A/Solids*, (submetido), 1998.

[6] Z. Dimitrovová e L. Faria, Mechanical Behavior of the Cellular Solids in the Linear Range, Part II – Classification According to Structure and Properties, *Eur. J. Mech., A/Solids*, (submetido), 1998.

[7] Z. Dimitrovová e L. Faria, New Methodology to Establish Bounds on Effective Properties of Cellular Solids, *J. Mech. Comp. Mat. Str.*, (aceite para publicação), 1998.

[8] Z. Dimitrovová e L. Faria, Bounds on Effective Properties of Open-Cell Foams, *J. Mech. Phys. Solids*, (a ser submetido), 1998.

[9] G. Duvaut, Homogeneization et Materiaux Composite, em *Theoretical and Applied Mechanics*, P. Ciarlet e M. Rouseau (eds.), Amsterdam, North-Holland, 1976.

[10] L. J. Gibson e M. F. Ashby, *Cellular Solids. Structure and Properties*, Pergamon Press, Oxford, 1988.

[11] J. M. Guedes, *Nonlinear Computational Models for Composite Materials Using Homogenization*, Ph.D. Dissertation, Ann Arbor: The University of Michigan, USA, 1990.

[12] Z. Hashin, Theory of Composite Materials, em *Mechanics of Composite Materials*, F. W. Wendt, H. Liebowitz e N. Perrone (eds.), Pergamon Press, Oxford, pp. 201-242, 1970.

[13] Z. Hashin, Analysis of Composite Materials - A Survey, *J. Appl. Mech., ASME*, vol. 50, pp. 481-505, 1983.

[14] R. Hill, Elastic Properties of Reinforced Solids: Some Theoretical Principles, *J. Mech. Phys. Solids*, vol. **11**, pp. 357-372, 1963.

[15] S. Nemat-Nasser e M. Hori, *Micromechanics: Overall Properties of Heterogeneous Materials*, North-Holland Series in Applied Mathematics and Mechanics, vol. **37**, J. D. Achenbach, B. Budiansky, H. A. Lauwerier, P. G. Saffman, L. Van Wijngaarden e J. R. Willis (eds.), North-Holland-Amsterdam, London, New York, Tokyo, 1993.

[16] O. Sigmund, Tailoring Materials with Prescribed Elastic Properties, Report N°480, The Danish Center for Applied Mathematics and Mechanics, Denmark, 1994.

[17] P. M. Suquet, Elements of Homogenization for Inelastic Solid Mechanics, em *Homogenization Techniques for Composite Media* (Proceedings, Udine, Italy 1985), E. Sanchez-Palencia e A. Zaoui (eds.), Lecture Notes in Physics, 272, Springer-Verlag, pp. 193-278, 1985.

Detecção não destrutiva

Carlos J. S. Alves
Departamento de Matemática, Instituto Superior Técnico,
Av. Rovisco Pais 1, 1096 LISBOA Codex
(e-mail: calves@math.ist.utl.pt)

Resumo

A utilização de raios X para detecção é uma prática de uso corrente que é utilizada na medicina através de radiografias ou tomografia axial computadorizada, ou no controlo de segurança nos aeroportos. No entanto não podemos falar de uma detecção completamente não destrutiva, pois trata-se da emissão de radiação de alta frequência. Neste artigo, apresentaremos recentes técnicas matemáticas que abordam o problema de detecção (para qualquer frequência) como um problema inverso de difracção.

1. Introdução

Com o objectivo de apresentar o contexto actual em que se situa a investigação no campo da detecção não destrutiva, começamos por apresentar exemplos em diferentes domínios científicos.

Medicina. O primeiro caso notável de detecção não destrutiva é a descoberta da radiografia por Roentgen no final do século XIX. A emissão de ondas electromagnéticas de alta frequência (os denominados Raios X) permite obter uma reconstituição fotográfica de objectos opacos contidos num corpo transparente através da sua sombra. É o caso das radiografias em que, a determinada frequência, os tecidos subcutâneos são transparentes e o objecto a analisar (um osso, ou algum órgão) provoca alguma sombra. Situação semelhante ocorre com as ecografias, só que neste caso são utilizadas ondas acústicas de alta frequência, os ultra-sons, em vez de ondas electromagnéticas.

A utilização das ecografias é mais benigna, mas a técnica implementada não permite imagens nítidas e não há muitas soluções quando os órgãos a examinar são transparentes a essas altas frequências. Um processo desagradável consiste em utilizar substâncias que se infiltram nesses órgãos e os tornam momentaneamente opacos à radiação.

No entanto, há muitas circunstâncias em que não há solução aparente. Um caso habitual é a detecção de um tumor situado na medula óssea, causador de leucemia. O osso sendo opaco à alta radiação não permite a sua detecção pelos processos vulgares. A recente abordagem deste caso por D. Colton e P. Monk [4], encarando-o como um problema inverso de difracção levou à obtenção de resultados promissores do ponto vista teórico... Com efeito, até à presente data ainda não foi construído o simulador com o qual a Força Aérea Norte-Americana pretende realizar experiências.

Materiais. Um outro aspecto importante é a detecção não destrutiva de defeitos em materiais, mais concretamente a detecção de fissuras, cavidades ou impurezas em materiais. Uma vez construída uma peça, é importante assegurar a sua qualidade com um processo que não comprometa a própria peça!

Um processo pode ser a difracção de ondas (elásticas ou electromagnéticas), ou a aplicação de tensões superficiais e subsequente medição dos efeitos.

Um problema real é a junção ou colagem de dois componentes que são peças de um reactor nuclear. Caso haja uma fissura ou uma cavidade entre eles essa junção é instável às altas temperaturas a que está submetida e pode pôr em perigo o funcionamento de uma central nuclear.

Convém notar que a inspecção da qualidade de pequenas peças através de Raios X é bastante usual. No entanto, podendo permitir a detecção de cavidades no material, não permite a

detecção de fissuras (podemos entender fissura como sendo uma cavidade em que a sua espessura é bastante inferior ao comprimento de onda).

Geofísica. A pesquisa geológica é outro assunto em que a detecção é factor fundamental. Aqui não há sequer a possibilidade real de que a detecção seja fortemente destrutiva.

A explosão de cargas no subsolo (no contexto, encarada como minimamente destrutiva) gera ondas elásticas que se propagam com velocidades diferentes nos diversos estratos. A medição do resultado dessa difracção permite, actualmente, apenas testar teorias acerca da localização de estratos e falhas na crosta terrestre. Um tratamento matemático completo do assunto é neste caso demasiado complexo devido ao grande número de graus de liberdade existente e à escassa informação que é possível reunir através de sismógrafos.

Radar e Sonar. O radar é outra aplicação importante, popularizado pela eficácia revelada na II Guerra Mundial. Permite a detecção de aparelhos no espaço aéreo (aviões) ou marítimo (submarinos) e também a detecção de materiais enterrados a pouca profundidade (por exemplo, minas). O sonar, por sua vez, tem também grande aplicação a nível marítimo, nomeadamente para a localização da pesca. A qualidade da informação obtida pela reflexão das ondas (acústicas, no caso do sonar, e electromagnéticas no caso do radar) é, no entanto, bastante deficiente.

2. Problemas Directo e Inverso

Chamamos *problema directo* ao problema que consiste em emitir uma onda e determinar o resultado da sua difracção num obstáculo conhecido (ver Figura 1). O obstáculo considerado não tem que ser conexo, pode ter várias componentes separadas no espaço, mas a fronteira é suficientemente regular (sem cantos), sendo normalmente consideradas fronteiras C^1. Trata-se de um problema bem posto (cf. [3]), pelo que pequenas alterações na emissão conduzem a pequenas alterações na recepção e reciprocamente (supõe-se o obstáculo fixo).

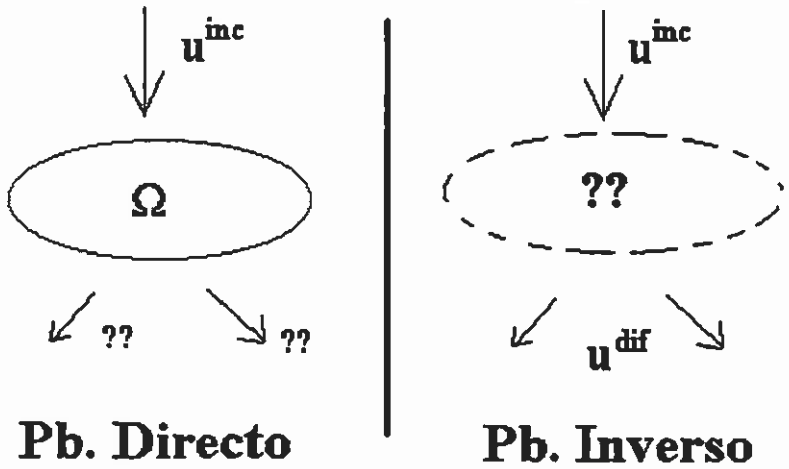


Figura 1. Esquematicamente, os problemas directo e inverso.

O mesmo não se passa com o problema inverso. Entendemos por *problema inverso*, o problema em que o obstáculo é desconhecido, e apenas conhecemos as ondas incidente e difractada (ver Figura 1). As restrições impostas à regularidade da fronteira do obstáculo são as mesmas que no problema directo, normalmente trabalhamos com regularidade C^1, ou mesmo C^2. O problema inverso é mal posto, já que se mantivermos a mesma onda incidente, e fizermos uma pequena alteração na forma do objecto, podemos obter uma onda difractada completamente diferente. Assim, também pequenas alterações na medição da amplitude da onda difractada, próprias do aparelho de medida, podem comprometer a identificação da forma.

3. O Problema Directo

3.1 Equação de Helmholtz

Vamos modelizar matematicamente um problema simples. Consideramos a difracção de ondas acústicas planas (harmónicas no tempo) por um obstáculo tridimensional e medimos a amplitude da onda difractada.

Sejam $u^{inc}(x) = e^{i\omega x.\theta}$, ondas planas incidentes cuja direcção de deslocamento é um vector θ unitário e onde ω é a frequência da onda. A onda difractada pelo objecto Ω verifica a equação de Helmholtz[1]:

$$\Delta u + \omega^2 u = 0 \text{ em } R^3 \setminus \bar{\Omega}$$

e são impostas condições na fronteira do objecto, consoante as suas propriedades de impedância. Num caso razoavelmente geral, podemos considerar uma condição de Robin:

$$(\frac{\partial}{\partial n} + iZ)(u + u^{inc})(x) = 0 \text{ em } \partial\Omega,$$

em que Z é a impedância. O comportamento da onda difractada quando $\|x\| \to \infty$ é determinado pela amplitude limite A, tendo-se (a partir da condição de radiação de Sommerfeld)

$$u(x) = \frac{e^{i\omega\|x\|}}{\|x\|}\left(A(\frac{x}{\|x\|}) + O(\|x\|^{-1}) \right).$$

É a partir do conhecimento de A, uma função analítica definida sobre a superfície esférica unitária (ver Figura 2), que se pretende determinar a forma do objecto.

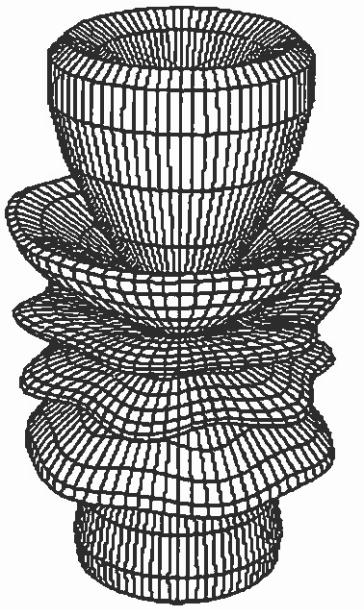


Figura 2. Padrão do módulo da amplitude limite num caso de incidência de ondas elásticas.

[1] Convém referir que assumimos aqui um meio homogéneo em que a velocidade de propagação da onda é constante e define a unidade. Num caso geral a equação de Helmholtz fica

$$\Delta u + \left(\frac{\omega}{c(x)}\right)^2 u = 0 \text{ em } IR^3 \setminus \bar{\Omega}$$

em que $c(x)$ é a velocidade no ponto x. Isto introduz um outro tipo de problema inverso em que a distribuição da velocidade $c(x)$ passa a ser a incógnita a determinar.

3.2 Resolução numérica do problema directo.

Ao pretender resolver numericamente o problema directo com o método dos elementos finitos, e como pretenderemos usar o mesmo método para a resolução do problema inverso, debatemo-nos com um problema imediato que é o facto dos nossos domínios serem o exterior de obstáculos Ω. Como se tratam de domínios infinitos, a única possibilidade é considerar um domínio artificial suficientemente grande que contenha Ω, o que pode levar a malhagens de grande dimensão e exageradamente complexas.

Uma solução razoável e eficaz é discretizar o problema com o método do elementos de fronteira. Para esse efeito precisamos de estabelecer equações integrais associadas ao problema directo. No caso de considerarmos objectos rígidos, a condição de fronteira é a condição de Neumann,

$$\frac{\partial}{\partial n}(u+u^{inc})(x)=0, \text{ em } \partial\Omega,$$

e podemos obter a fórmula de representação integral em $\partial\Omega$, através de um potencial de camada dupla

$$u(x)=\int_{\partial\Omega}\varphi(y)\frac{\partial}{\partial n_y}\Phi(x-y)ds(y),$$

em que φ é uma densidade em $\partial\Omega$, e $\Phi(x-y)=\frac{e^{ik|x-y|}}{4\pi|x-y|}$ é uma solução fundamental da equação de Helmholtz em R^3. A densidade φ é determinada resolvendo a equação integral

$$\frac{\partial}{\partial n_x}\int_{\partial\Omega}\varphi(y)\frac{\partial}{\partial n_y}\Phi(x-y)ds(y)=\frac{\partial}{\partial n}u^{inc}(x) \text{ em } \partial\Omega,$$

que tem, no entanto, um núcleo hiper-singular. Todavia, usando um método de elementos finitos de fronteira, é possível obter uma formulação variacional equivalente em que a forma bilinear já apresenta integrais com núcleo fracamente singular, numericamente calculáveis. Uma outra hipótese é obter uma equação integral derivada de um potencial de camada simples

$$u(x)=\int_{\partial\Omega}\psi(y)\Phi(x-y)ds(y),$$

e aplicar um método de quadratura de Nyström, como em [3].

4. O Problema Inverso

O estudo do problema inverso de difracção é consideravelmente recente, e sofreu um grande impulso com os trabalhos de D. Colton e R. Kress nos anos 80, [2, 3].

Já referimos que se trata de um problema mal posto, em primeiro lugar, porque pequenas alterações na forma do obstáculo podem provocar enormes alterações na amplitude da onda difractada (ver Figura 3), e em segundo lugar, porque não se pode sequer falar em existência de solução, por falta de um espaço conveniente. Basta reparar que a amplitude é uma função analítica e não podemos esperar efectuar medições analíticas, já que devemos sempre contar com 'ruído', imprecisões inerentes a qualquer medição. No entanto, temos um resultado de densidade que é importante a este nível:

***Teorema 1:** A amplitude limite gerada pela difracção de uma infinidade de ondas planas incidentes é densa no espaço das funções L^2 definidas sobre a superfície esférica.*

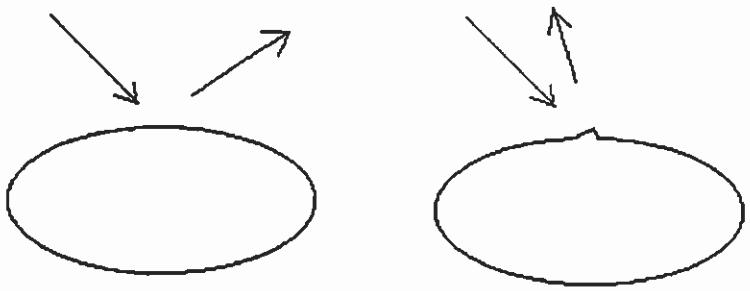


Figura 3. Uma pequena alteração no domínio provoca uma grande alteração na onda difractada (pressupõe-se neste esquema ilustrativo uma reflexão perfeita de um raio, assumindo alta frequência)

4.1 O problema da unicidade.

É muito importante saber se é possível determinar univocamente o objecto a partir da difracção que provoca e, caso afirmativo, saber quantas ondas incidentes são necessárias para o fazer.

O primeiro resultado que se conhece acerca de unicidade para o problema inverso é um resultado comunicado por Schiffer a Lax e Phillips ([7]), cujo argumento se baseia numa propriedade dos valores próprios que é apenas válida quando na fronteira dos objectos se verifica a condição de Dirichlet $u = u^{inc}$. O resultado de Schiffer assegurava unicidade, caso se dispusesse das amplitudes limite de uma infinidade de ondas incidentes, mas este resultado foi melhorado por Colton e Sleeman [CS], que conseguiram mesmo estabelecer unicidade usando uma única onda incidente, caso se soubesse que os obstáculos estavam contidos numa bola de raio $r < \pi/\omega$.

Até 1990 o problema de unicidade para a condição de Neumann ficou por provar, mas uma nova demonstração de unicidade para o problema de Dirichlet, por V. Isakov [5], permitiu a Kirsch e Kress [6] assegurar a unicidade para o problema de Neumann através da incidência de uma infinidade de ondas planas (ainda é um problema em aberto saber se é possível obter unicidade com um número finito de ondas incidentes).

Em qualquer destas demonstrações é assumido que os obstáculos possuem fronteiras regulares (pelo menos C^1) e foi o excluído o caso de obstáculos que podem incluir fissuras. Mais recentemente (cf. [1]), foi demonstrada a unicidade para o caso mais geral em que também se incluem fissuras e é considerada uma condição de fronteira de Robin, em que a própria impedância é desconhecida. Também neste caso é exigido o conhecimento da amplitude limite gerada pela incidência de uma infinidade de ondas planas.

Teorema 2: *Sejam $A_1(.;\theta)$ e $A_2(.;\theta)$ as amplitudes limite geradas por obstáculos D_1 e D_2 (respectivamente), após a incidência de uma onda plana de direcção θ.*

Se $A_1(.;\theta) = A_2(.;\theta)$, $\forall\theta$, então $D_1 = D_2$ e $Z_1 = Z_2$ (em que Z_1, Z_2 são as respectivas impedâncias).

Convém referir aqui que, apesar de se assumir que parte de D_1 ou D_2 pode ser uma fissura, estamos ainda a considerar superfícies regulares. Estabelecer estes resultados para objectos com 'cantos' é ainda um problema em aberto.

4.2 Resolução numérica do problema inverso.

Como se trata de um problema mal posto, resolver numericamente o problema inverso é uma tarefa complicada e portanto é normalmente necessário usar técnicas de regularização para inverter operadores compactos, nomeadamente usando os resultados de Tikhonov (e.g.[3]).

As técnicas numéricas encaram o problema inverso como um problema de minimização, já que, sendo impossível obter a forma exacta (... a menos que se caia num '*inverse crime*', como alertado em [3]), procura-se obter a forma $\tilde{D}$ que melhor aproxima D, no sentido de minimizar

$$\| A_D - A_{\tilde{D}} \|_{L^2(S)}$$

em que S é a superfície esférica e A_D , $A_{\tilde{D}}$ são as respectivas amplitudes limite.

Actualmente, os processos de resolução numérica tratam apenas da recuperação da forma de um único objecto conexo, normalmente um domínio 'estrelado', cuja fronteira de $\tilde{D}$ é descrita pelos pontos

$$x = r(\theta)\theta \quad (\theta \in S),$$

em que S é a superfície esférica e r é uma função contínua definida em S.

Para aproximar r, considera-se uma família de funções densa nas funções contínuas em S. Isto pode ser obtido usando vários tipos de funções base, no quais se incluem funções trigonométricas.

O método de minimização normalmente utilizado é um método do tipo 'mínimos quadrados', uma variante do método de Gauss-Newton, conhecido como Levenberg-Marquardt.

Uma outra maneira de proceder à minimização é obter a derivada de Fréchet do operador A_D, relativamente ao domínio, trata-se de uma derivada de domínio, cujo valor pode ser obtido através da resolução de um problema semelhante ao da difracção, como foi provado por Kirsch (cf. [3]). Tendo a derivada de Fréchet pode ser implementado um método de Newton para o operador A_D.

No entanto, em qualquer dos casos, existe um problema difícil de solucionar na minimização, que é o da boa escolha da aproximação inicial, já que é difícil contornar a existência de mínimos locais, que nos afastam da forma pretendida - o mínimo global. Mas, como normalmente há uma informação '*a priori*' acerca da localização aproximada do objecto, os resultados actualmente obtidos são prometedores para uma implementação experimental, já que asseguram bons resultados, mesmo com um erro experimental nas medições de 10%.

Bibliografia:

[1] Alves, C. J. S., Ha Duong T., On Inverse Scattering by Screens. *Inverse Problems*, **13**, 1161-76, 1997.

[2] Colton, D., Kress, R., *Integral Equation Methods in Scattering Theory*. Wiley, New York, 1983

[3] Colton, D., Kress, R., *Inverse Acoustic and Electromagnetic Scattering Theory*. Appl. Math. Sc. **93**, Springer-Verlag, 2nd.ed., 1997

[4] Colton, D., Monk, P., Kress, R., A New Algorithm in Electromagnetic Inverse Scattering Theory with an Application to Medical Imaging. *Math. Meth. Appl. Sc.*, **20**, 385-401, 1997

[5] Isakov, V., On uniqueness on the inverse transmission scattering problem. *Comm. Part. Diff. Eq.*, **15**, 1565-87, 1990

[6] Kirsch, A., Kress, R., Uniqueness in inverse obstacle scattering. *Inverse Problems*, **9**, 285-299, 1993

[7] Lax, P., Phillips R., *Scattering Theory*, Academic Press, New York, 1967.

Utilização de Modelos Matemáticos em Problemas de Engenharia Costeira

Adélio J. R. Silva*

Resumo

A utilização da modelação matemática em engenharia costeira representa actualmente um valor acrescentado inprescindível na abordagem destes problemas. A utilização dos modelos contribui decisivamente para uma melhor comprensão dos sistemas e funciona como ferramenta de apoio à decisão na análise de possíveis alternativas no campo da engenharia.

Nesta comunicação apresenta-se uma descrição básica do processo de implementação de um modelo matemático e de alguma da experiência acumulada pela Hidromod no desenvolvimento e implementação de modelos matemáticos para diversos campos de actuação da engenharia costeira.

Palavras-Chave: Modelos matemáticos, Modelação, Engenharia Costeira

* Eng. Civil, Doutor.
Hidromod, Modelação em Engenharia, Lda
Taguspark, Núcleo Central, 349, 2780 Oeiras, Portugal
Tel: (351 1) 4213173 – Fax (351 1) 4211272 – Email:asilva.hidromod@taguspark.pt

Introdução

Em zonas ecologicamente sensíveis como é o caso dos meios aquáticos, as acções de planeamento e gestão ou os projectos e execução de trabalhos de engenharia devem ser antecedidos por um planeamento cuidado que minimize os impactes sobre o meio. No entanto, para que se atinja este objectivo é necessário ter um conhecimento profundo dos sistemas, de modo a ser possível prever como estes irão reagir às novas condições.

Com o aparecimento dos computadores surgiu uma ferramenta capaz de processar grandes volumes de informação, que rapidamente se tornou num auxiliar essencial na integração do conhecimento. Esta "nova" ferramenta permitiu a estruturação da informação de um modo intuitivo e de fácil acesso (SIG – Sistema de Informação Geográfica), permitiu a divulgação à escala mundial dessa mesma informação (internet) e permitiu que os modelos conceptuais desenvolvidos ao longo de décadas a partir da análise experimental por biólogos, químicos, físicos pudessem ser acoplados e aplicados de uma forma generalizada a casos reais.

Nesta perspectiva, os modelos matemáticos representam actualmente uma ferramenta imprescindível na abordagem destes problemas, contribuindo decisivamente para uma melhor compreensão dos fenómenos envolvidos e fazer o diagnóstico das situações, permitindo tomar decisões ao nível das soluções de engenharia e efectuar uma análise dos impactes associados. O campo de aplicação dos modelos é bastante vasto, podendo simular fenómenos que vão desde a hidrodinâmica ao transporte de sedimentos, à qualidade da água e ecologia.

Nesta comunicação apresentam-se alguns exemplos de aplicação de modelos matemáticos a problemas de engenharia costeira, envolvendo problemas de hidrodinâmica, transporte de sedimentos e qualidade de água.

Os Modelos Matemáticos

Um modelo matemático, na perspectiva em que é aqui apresentado, pretende ser a representação matemática de uma realidade física. Estas representações matemáticas podem ser derivadas directamente das equações fundamentais que descrevem os fenómenos (com ou sem simplificações) ou resultar de modelos empíricos construídos em torno de observações sistemáticas da natureza.

Implementação de um modelo matemático

A implementação de um modelo matemático passa por diversas fases. Numa primeira fase é necessário proceder a uma recolha de informação sobre o local. Elementos sobre batimetria, dados de correntes e níveis para a calibração da hidrodinâmica, dados relativos ao problema específico que se pretende modelar (e.g. qualidade da água, sedimentos, etc). No caso dos elementos não existirem será necessário definir um programa de trabalhos para recolha de dados de campo que permitam a definição da geometria, uma verificação e posterior calibração do modelo.

Com base na informação recolhida, nomeadamente da batimetria, é então possível definir uma malha de cálculo. Este procedimento consiste na interpolação da

informação existente para os pontos de uma malha onde irão ser calculadas as variáveis do problema (velocidades, níveis, taxas de transporte, etc).

Verificação, Calibração e Validação dos Modelos

A qualidade dos resultados de um modelo depende da qualidade do modelo propriamente dito (equações, método numérico e código) e dos cuidados tidos durante a implementação (qualidade dos dados, da calibração e da validação). A verificação do modelo é feita através da comparação dos seus resultados com casos com solução analítica, ou através da análise qualitativa dos resultados em casos teste. Este processo permite verificar a capacidade para as equações resolverem o problema em análise, verificar a qualidade do método numérico utilizado e identificar erros do programa. No caso de um modelo hidrodinâmico as equações e o seu domínio de validade são normalmente conhecidos, mas no caso da qualidade da água, ou mesmo do transporte de sedimentos o grau de confiança é menor.

A qualidade dos resultados de um modelo que tenha passado a fase de verificação depende da qualidade da implementação, a qual está dependente da qualidade dos dados utilizados para definir as condições aos limites e proceder à calibração (batimetria, marés na fronteira aberta, caudal do rio, características dos sedimentos, etc.). Durante a fase de calibração são ajustados os parâmetros do modelo, de forma a que este reproduza o conjunto de dados utilizados para o efeito.

A validação consiste na verificação dos resultados através da sua comparação com um conjunto de dados independente dos utilizados na calibração. Num modelo hidrodinâmico a validade dos resultados é normalmente assegurada através de uma calibração cuidada. No caso dos modelos de qualidade da água o número de parâmetros é normalmente muito elevado. A validação dos resultados, utilizando um conjunto de dados independente, é assim essencial para garantir que através da calibração não estamos fazer um simples ajustamento aos dados de campo disponíveis e que o modelo mantém a capacidade de previsão.

A calibração e validação da hidrodinâmica é em geral relativamente simples. Normalmente é neste campo que existem mais medidas disponíveis e, mesmo não existindo, a execução de uma campanha de medidas (níveis e correntes) envolve meios relativamente pouco dispendiosos, sendo possível obter elevados graus de concordância entre os resultados dos modelos e as medidas.

Já no que respeita à simulação do transporte de sedimentos ou da qualidade da água, a calibração e validação dos modelos é bastante mais difícil. Estas dificuldades adicionais têm a ver tanto com a própria complexidade dos fenómenos como com limitações no que respeita à disponibilidade de dados, quer em quantidade quer em qualidade.

Exemplo das dificuldades no que respeita ao conhecimento dos fenómenos é, entre muitos outros, a descrição dos processos de troca entre a coluna de água e o fundo, a determinação dos campos de correntes produzidos por acção combinada de ondas e correntes e dos volumes de erosão-sedimentação associados aos fenómenos de transporte.

Estas limitações não devem no entanto ser encaradas liminarmente como impeditivas da utilização dos modelos, uma vez que os resultados que são possíveis de obter podem conduzir a ganhos significativos de qualidade no que toca ao conhecimento dos sistemas e ao tipo de resposta a esperar na sequência de determinada acção, mesmo que só possam ser encarados do ponto de vista qualitativo.

Exemplos de Aplicação

A aplicação de modelos matemáticos em problemas de engenharia costeira tem-se generalizado ao longo dos últimos anos, na medida que o custo dos computadores tem vindo a decrescer e a capacidade de cálculo a aumentar.

Com efeito, a utilização dos modelo é hoje considerada imprescindível na generalidade dos problemas, para efectuar diagnóstico de situações, integrar resultados de medidas pontuais, aumentar a comprensão sobre o funcionamento dos sistemas ou avaliar os possíveis impactes associados a determinado tipo de intervenção que se pretenda fazer.

Ao longo dos últimos anos a Hidromod, em resultado da participação num grande número de trabalhos, envolvendo problemas relacionados com a hidrodinâmica, transporte de sedimentos, qualidade de água, dispersão de poluentes, propagação de ondas, etc., acumulou uma larga experiência na aplicação de modelo a zonas costeiras.

A título de exemplo presentam-se de seguida alguns exemplos de aplicação dos modelos à simulação de diferentes problemas.

Avaliação dos impactes de construção de estruturas ou dragagem de canais

A utilização dos modelos matemáticos como forma de avaliar o nível dos impactes associados a diferentes possibilidades de intervenção, conduz a ganhos significativos na compreensão da dinâmica dos sistemas e, consequentemente, a uma perspectiva objectiva do tipo de reacção a esperar de cada uma das acções propostas, permitindo nomeadamente:

- Avaliar as alterações esperadas ao nível da hidrodinâmica e da qualidade da água;
- Caracterizar a forma como se processa o trânsito de areias por acção combinada de ondas e correntes;
- Avaliar os impactes de diferentes opções construtivas, tanto no que respeita à geometria como às respectivas metodologias de construção;
- Avaliar possíveis riscos decorrentes das obras propostas (e.g. contaminação de zonas vizinhas, possibilidade de agravamento de problemas de cheias, etc.).

Este tipo de tecnologias tem sido aplicado com sucesso a diferentes estudos, dos quais se podem destacar, pela sua complexidade, os relacionados com as dragagens do canal de acesso ao porto de Setúbal e com a possibilidade de construção dos esporões à entrada do estuário do Douro.

Em ambos os casos a utilização da modelação matemática desempenhou um papel determinante tanto ao nível da escolha das soluções de engenharia como da avaliação dos possíveis impactes sobre o meio físico aquático.

No que respeita ao caso do estuário do Douro (Figura 1) foi possível simular sete diferentes soluções para uma futura possível configuração da barra, tendo a solução final proposta tido em consideração os possíveis efeitos sobre:

- A segurança da navegação;
- transporte de areias;

- A inundação das zonas ribeirinhas em situação de cheias;
- As alterações de salinidade no estuário.

Esta abordagem do problema permitiu assim pôr em evidência aspectos que de outra forma não seria possível avaliar.

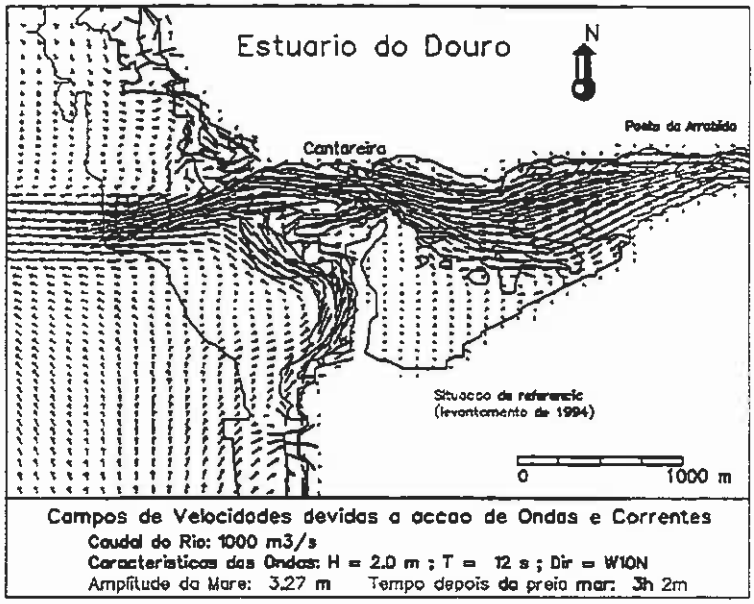


Figura 1 – campo de correntes produzido por **acção combinada de ondas, maré e caudal do rio Douro na situação** de referência

No caso do estuário do Sado a Hidromod tem participado em diversos estudos relacionados com a operação e expansão do porto de Setúbal. Estes estudos iniciaram-se genericamente com a avaliação dos impactes relacionados com a construção do terminal da Ford-VW e têm vindo sucessivamente a envolver outros aspectos.

Recentemente foi concluído um estudo envolvendo a aplicação de um modelo tridimensional para o estuário, que apresenta aspectos importantes em termos de inovação tecnológica. Esta aplicação teve por objectivo efectuar uma avaliação dos impactes resultantes de um possível aprofundamento do actual canal sobre o transporte de sedimentos em suspensão (Figura 2) e sobre a distribuição de salinidade no estuário. Como resultado foi possível pôr em evidência alguns aspectos relacionados com a tridimensionalidade do escoamento, nomeadamente alguns efeitos de curvatura, que não seria possível avaliar com recurso a um modelo bidimensional (Figura 3).

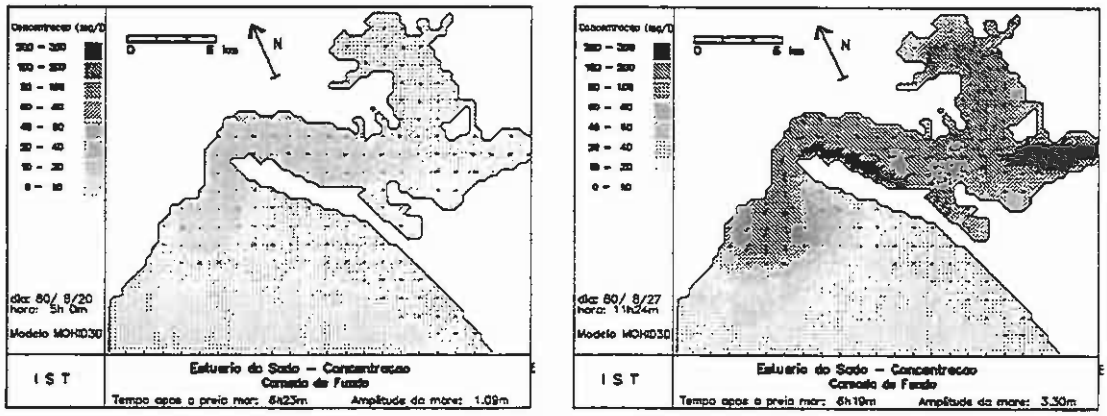


Figura 2 – a) Concentração de sedimentos coesivos durante uma baixa-mar com uma amplitude de maré de 1.09 m (maré morta). b) Concentração de sedimentos coesivos durante uma baixa-mar com uma amplitude de maré de 3.30 m (maré viva).

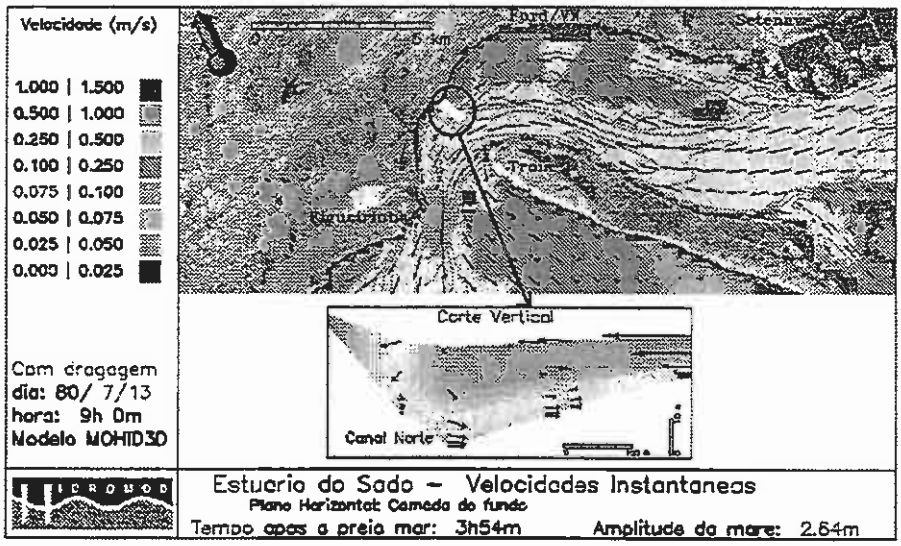


Figura 3 – Campo de correntes na camada de fundo e corte vertical à entrada do canal norte.

Avaliação de diferentes alternativas para a construção de uma estrutura de protecção

A construção de uma estrutura de abrigo, para protecção da agitação incidente, implica sempre a execução de estruturas pesadas em que cada metro de estrutura tem um elevado custo de construção.

A utilização de modelos matemáticos para avaliação das condições de abrigo proporcionadas por determinado tipo e estrutura, permitindo testar rapidamente e a custos reduzidos diferentes soluções alternativas, permite conduzir a ganhos que podem ser significativos.

A Hidromod tem efectuado diversos estudos visando a determinação das condições de abrigo propocionadas pela construção de molhes de protecção, especialmente em pequenos portos de pesca ou de recreio.

Como resultado das possibilidades oferecidas pela capacidade de simulação de múltiplas configurações tem sido possível fornecer dados ao projectista que lhe permitem optimizar a estrutura, reduzindo substancialmente os custos de construção.

Avallação das condições de dispersão de um efluente.

A rejeição de efluentes em meio aquático põe sempre problemas do ponto de vista ambiental. Estes problemas podem tanto ter origem a montante do sistema, como seja o caso das afluências de ribeiras com elevadas cargas poluentes, como ser produzidos localmente.

Mesmo em caso de necessidade de construção de uma estação de tratamento, continua a ser necessário descarregar nalgum ponto o efluente tratado, podendo neste caso a escolha correcta do local da rejeição ser de fundamental importância para o sucesso do projecto, sobretudo em estuários e outras zonas sensíveis. Em qualquer caso será sempre necessário garantir a manutenção de valores legais ao nível da qualidade da água e demonstrar a capacidade do meio receptor para dispersar o efluente rejeitado.

A modelação matemática pode nestes casos ser importante quer para caracterização dos sistemas (ex. Figura 4) quer para simular os impactes de possíveis soluções ou de novos projectos que se pretendam desenvolver em determinada zona.

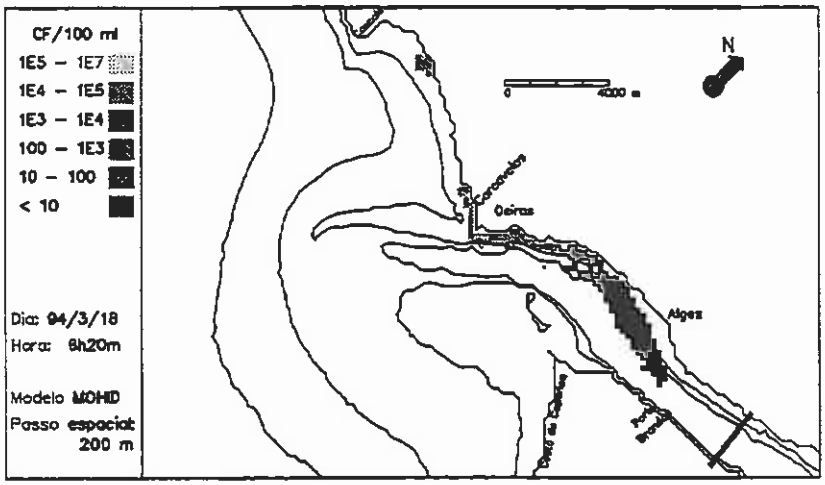


Figura 4 - Estudo da dispersão de coliformes fecais na costa do Estoril. Localização da pluma 30 minutos após a preia mar

Conclusões

Nesta comunicação apresenta-se uma descrição de alguns dos meios matemáticos actualmente à disposição da comunidade técnica e científica capazes de dar um contributo importante na caracterização e avaliação dos impactes resultantes de intervenções em estuários e zonas costeiras.

Dos modelos e exemplos de aplicação aqui descritos pode verificar-se que este tipo de tecnologias, criteriosamente utilizadas, possui um carácter integrador único que permite obter uma visão ao nível global do estuário (ou zona costeira afectada) de possíveis impactes resultantes de alterações introduzidas quer no meio físico quer no ecossistema. Este carácter integrador associado à capacidade de simulação de múltiplos cenários e da comparação relativa entre eles, permite estabelecer critérios com bases objectivas que podem constituir um precioso auxiliar no processo de tomada de decisão.

Método de Domínios Fictícios para problemas Elípticos

Luís R. Borges
Área de Matemática-ISEL e Centro de Matemática Aplicada-IST
José A. Rodrigues
Área de Matemática-ISEL e Centro de Matemática Aplicada-IST
Adélia Sequeira
Departamento de Matemática-IST e Centro de Matemática Aplicada-IST

18 de Setembro de 1998

1 Introdução

O Método de Domínios Fictícios aplicado à resolução numérica de equações com derivadas parciais tem-se revelado muito útil na aplicação a problemas industriais de geometria complexa. Para este sucesso contribui fundamentalmente a possibilidade de se poder eliminar as dificuldades impostas pela geometria do domínio, mergulhando-o num outro de geometria mais simples e permitindo assim a utilização dos métodos numéricos clássicos.

Com base nos artigos [7], [4] e [3] apresentamos neste trabalho uma resolução numérica de um problema do tipo Poisson com condições de fronteira de Dirichlet não homogéneas, recorrendo ao Método de Domínios Fictícios.
Começamos por mergulhar o domínio, onde é formulado o problema, num mais regular. Posteriormente damos nova formulação ao problema inicial impondo a condição de fronteira com recurso a multiplicadores de Lagrange. Na última secção apresentamos resultados numéricos para vários exemplos.

No que se segue utilizaremos os seguintes espaços de Sobolev:

$$\begin{aligned} H^1(\Omega) &= \left\{ v \in L^2(\Omega) : \frac{\partial v}{\partial x_i} \in L^2(\Omega), i = 1,2 \right\} \\ H_0^1(\Omega) &= \left\{ v \in H^1(\Omega) : v = 0 \text{ sobre } \partial\Omega \right\}, \\ H^{\frac{1}{2}}(\partial\Omega) &= \left\{ \varphi \in L^2(\partial\Omega) : \exists v \in H^1(\Omega), v\,|_{\partial\Omega} = \varphi \right\} \end{aligned}$$

com as respectivas normas

$$\begin{aligned} \|v\|_{H^1(\Omega)} &= \left(\|v\|^2_{L^2(\Omega)} + \|\nabla v\|^2_{L^2(\Omega)}\right)^{\frac{1}{2}} \\ \|\mu\|_{H^{\frac{1}{2}}(\Gamma)} &= \inf_{u \in H^1(\Omega):\, \gamma_0(u)=\mu} \|u\|_{H^1(\Omega)} \end{aligned}$$

além destes consideramos também o espaço $H^{-\frac{1}{2}}(\Gamma)$, o dual de $H^{\frac{1}{2}}(\Gamma)$ com a norma

$$\|\mu\|_{H^{-\frac{1}{2}}(\Gamma)} = \sup_{\psi \in H^{\frac{1}{2}}(\Gamma)} \langle \mu, \psi \rangle .$$

2 Formulação de um problema de Dirichlet

Seja Ω um domínio limitado de $\mathbb{R}^2$ com fronteira $\partial\Omega = \Gamma$, que se supõe Lipschitziana e n a normal exterior em Γ.

Consideremos o seguinte problema de Dirichlet:

Dados f em $H^{-1}(\Omega)$ e g em $H^{\frac{1}{2}}(\Gamma)$, determinar u tal que

$$(Q) \begin{cases} \alpha u - \nu \Delta u &= f \text{ em } \Omega \\ u &= g \text{ sobre } \Gamma, \end{cases}$$

onde $\alpha \geq 0$ e $\nu > 0$.

O problema (Q) admite solução única $u \in H^1(\Omega)$. (cf. [5]).

Introduzimos a seguinte forma bilinear contínua

$$a_\Omega(.,.) : H^1_0(\Omega) \times H^1_0(\Omega) \longrightarrow \mathbb{R},$$

definida do seguinte modo:

$$a_\Omega(u,v) = \int_\Omega \alpha\, u\, v + \nu\, \nabla u\, \nabla v\, dx, \ \forall u, v \in H^1_0(\Omega).$$

Integrando por partes a primeira equação do problema (Q) podemos escrever este problema com uma nova formulação que designaremos por (P):

$$(P) \begin{cases} \text{Determinar } u \in V(g) \text{ tal que} \\ a_\Omega(u,v) = < f, v >, \ \forall v \in H^1_0(\Omega), \end{cases}$$

onde $V(g) = \{v \in H^1(\Omega) : \ v = g \ \text{ sobre } \Gamma\}$ e $< .,. >$ representa a dualidade entre $H^{-1}(\Omega)$ e $H^1_0(\Omega)$.

3 Uma Formulação em Domínios Fictícios

Seja $\mathcal{O}$ um subconjunto poligonal de $\mathbb{R}^2$ tal que $\overline{\Omega} \subset \mathcal{O}$ e designemos a sua fronteira por γ.

Vamos considerar uma extensão ao domínio $\mathcal{O}$ do problema (Q), formulado sobre Ω: determinar $\tilde{u}$ tal que

$$(QF)\begin{cases} \alpha\tilde{u} - \nu\Delta\tilde{u} &= \tilde{f} \text{ em } \mathcal{O} \\ \tilde{u} &= g \text{ sobre } \Gamma \\ \tilde{u} &= 0 \text{ sobre } \gamma, \end{cases}$$

onde $\tilde{f}\,|_\Omega = f$ e $\tilde{u}\,|_\Omega$ é solução do problema (Q).

A fim de apresentar uma formulação variacional do problema (QF) introduzimos o seguinte operador de projeção:

$$T : H_0^1(\mathcal{O}) \longrightarrow H^{\frac{1}{2}}(\Gamma)$$

que, para cada $v \in H_0^1(\mathcal{O})$, satisfaz

$$\langle T(v) - v,\, \mu\rangle_\Gamma = 0, \forall \mu \in H^{-\frac{1}{2}}(\Gamma). \tag{3.1}$$

onde $< .,. >_\Gamma$ designa agora a dualidade entre $H^{-\frac{1}{2}}(\Gamma)$ e $H^{\frac{1}{2}}(\Gamma)$

Propomos assim a seguinte formulação variacional:
determinar $(\tilde{u}, \lambda) \in H_0^1(\Omega) \times H^{-\frac{1}{2}}(\Gamma)$ tal que

$$(PF)\begin{cases} \int_\mathcal{O} \alpha\tilde{u}v + \nu\nabla\tilde{u}\nabla v\,dx &= \int_\mathcal{O} \tilde{f}v\,dx + \langle \lambda T(v)\rangle\,,\ \forall v \in H_0^1(\mathcal{O}) \\ \langle T(v) - v,\, \mu\rangle_\Gamma &= 0,\ \forall \mu \in H^{-\frac{1}{2}}(\Gamma), \end{cases}$$

onde $\tilde{u}\,|_\Omega = u$(solução do problema (P)) e λ é o multiplicador de Lagrange associado à restrição $\tilde{u} = g$ sobre Γ, isto é, $\lambda = -\nu\left[\frac{\partial\tilde{u}}{\partial n}\right]$, onde [.] representa o salto em Γ.
Definimos as seguintes formas bilineares:

$$a_\mathcal{O} : H_0^1(\mathcal{O}) \times H_0^1(\mathcal{O}) \longrightarrow \mathbb{R} \quad \text{e} \quad b : H_0^1(\mathcal{O}) \times H^{-\frac{1}{2}}(\Gamma) \longrightarrow \mathbb{R},$$

respectivamente por

$$a_\mathcal{O}(u,v) = \int_\mathcal{O} (\alpha u v + \nu\nabla u\nabla v)\,dx,\ \forall u, v \in H_0^1(\mathcal{O}).$$

$$b(v,\mu) = \langle v,\, \mu\rangle\,,\ \forall v \in H_0^1(\mathcal{O}),\ \forall \mu \in L^2(\Gamma).$$

A forma bilinear $a(.,.)$ é $H_0^1(\mathcal{O})$-elíptica e a forma bilinear $b(.,.)$ satisfaz a condição *inf-sup*: existe uma constante positiva β^* tal que

$$\inf_{\mu\in H^{-\frac{1}{2}}(\Gamma)} \sup_{v\in H_0^1(\mathcal{O})} \frac{b(v,\mu)}{\|v\|_{1,\mathcal{O}}\,\|\mu\|_{-\frac{1}{2},\Gamma}} \geq \beta^*. \tag{3.2}$$

Nestas condições podemos garantir existência e unicidade de solução para o problema misto (PF). (cf. [4])

4 Discretização

Por uma questão de simplicação consideramos agora $\bar{f} \in L^2(\mathcal{O})$. Discretizando o problema (PF) pelo Método dos Elementos Finitos obtemos o seguinte problema que designaremos por (PF_h):
Determinar $(\bar{u}_h, \lambda_h) \in V_h \times M_h$ tal que

$$(PF_h) \begin{cases} a_{\mathcal{O}}(\bar{u}_h, v_h) =< \bar{f}, v_h > + \int_\Gamma \lambda_h v_h \, d\sigma, \ \forall v_h \in V_h \\ \int_\Gamma (T(\bar{u}_h) - g_h) \mu_h \, d\sigma = 0, \ \forall \mu_h \in M_h, \end{cases}$$

onde V_h e M_h são, dois espaços de elementos finitos, subespaços de dimensão finita de $H_0^1(\mathcal{O})$ e $L^2(\Gamma)$, respectivamente, definidos por:

$$V_h = \left\{ v_h \in C(\mathcal{O}) \cap H_0^1(\mathcal{O}) : v_h \mid_K \in I\!P_1, \ \forall K \in \mathcal{T}_h \right\} (VER) \tag{4.3}$$

$$M_h = \left\{ q_h \in L^2(\Gamma) : q_h \mid_{K \cap \Gamma} \in I\!P_0, \ \forall K \in \mathcal{T}_h \right\}. \tag{4.4}$$

Onde $I\!P_k$ designa o espaço dos polinómios de duas variáveis de grau menor o igual a k.

Para que a solução do problema (PF_h) convirja (quando $h \to 0$), é suficiente que a condição "*inf-sup*" discreta se verifique para os espaços de elementos finitos escolhidos, isto é, que exista uma constante positiva β independente de h tal que

$$\inf_{q_h \in M_h} \sup_{v_h \in V_h} \frac{\int_\Gamma v_h \, q_h \, d\sigma}{\|v_h\|_{1,\mathcal{O}} \, \|q_h\|_{0,\Gamma}} \geq \beta. \tag{4.5}$$

Nestas condições e para uma triangulação uniformemente regular de $\mathcal{O}$ temos que

$$\lim_{h \to 0} \|\bar{u}_h - \bar{u}\|_{H^1(\mathcal{O})} = 0$$

Se para a descritização da fronteira utilizarmos uma malha cujo o diâmetro seja pelo menos o dobro ou triplo do diâmetro da malha do domínio, prova-se que se obtém uma estimativa de erro na ordem de h (cf.[4]). No presente trabalho não pretendemos comprovar esta ordem de convergência.

5 Algoritmo de Gradiente Conjugado

Na resolução do problema discreto usamos o seguinte algoritmo de Gradiente Conjugado:

1. Dado $\lambda_0 \in M_h$
   determinar $u_0 \in V_h$ tal que $a_{\mathcal{O}}(u_0, v_h) =< \bar{f}, v > + \int_\Gamma \lambda_0 v_h \, d\sigma, \ \forall v_h \in V_h,$
2. determinar $g_0 \in M_h$ tal que $\int_\Gamma g_0 \mu_h \, d\sigma = \int_\Gamma (u_0 - g) \mu_h \, d\sigma, \ \forall \mu_h \in M_h,$

3. considerar $w_0 = g_0$.

4. Início do ciclo
   Para $n \geq 0$, conhecidos λ_n, g_n, w_n determinar λ_{n+1}, g_{n+1}, w_{n+1}

   (a) determinar $\overline{u}_n \in V$ tal que $\tilde{a}(\overline{u}_n, v) = \int_\Gamma w_n\, v\, d\sigma$, $\forall v \in V_h$,

   (b) calcular $\rho_n = \frac{\int_\Gamma |g_n|^2\, d\sigma}{\int_\Gamma \overline{u}_n\, w_n\, d\sigma}$,

   (c) fazer $\lambda_{n+1} = \lambda_n - \rho_n w_n, \quad u_{n+1} = u_n - \rho_n \overline{u}_n$,

   (d) determinar $g_{n+1} \in M_h$, tal que

$$\int_\Gamma g_{n+1}\, \mu\, d\sigma \;=\; \int_\Gamma g_n\, \nu\, d\sigma - \rho_n \int_\Gamma \overline{u}_n\, \nu\, d\sigma,\ \forall \mu \in M_h$$

   (e) Se $\frac{\|g_{n+1}\|_{L^2(\Gamma)}}{\|g_0\|_{L^2(\Gamma)}} \leq \varepsilon$, então fazer

$$\lambda = \lambda_{n+1} \qquad u = u_{n+1},$$

   (f) caso contrário, calcular $\gamma_n = \frac{\|g_{n+1}\|^2_{L^2(\Gamma)}}{\|g_n\|^2_{L^2(\Gamma)}}$ e considerar

$$w_{n+1} = g_{n+1} + \gamma_n\, w_n.$$

   (g) Voltar ao início do ciclo.

6 Resultados Numéricos

Nesta secção pretendemos validar o método descrito anteriormente apresentando resultados numéricos para um problema particular. Consideremos o problema de Dirichlet com $\Omega = [0,1] \times [0,1]$ e $\mathcal{O} = [-1,2] \times [-1,2] (Fig.1)$:
determinar u tal que

$$\begin{cases} \alpha\, u - \nu \Delta\, u &= f \text{ em } \Omega \\ u &= 0 \text{ sobre } \Gamma, \end{cases}$$

com $\alpha = 1$, $\nu = 1$ e $f(x,y) = x(x-1)y(y-1) - 2(x^2 + y^2 - x - y)$. Para estes dados é conhecida a solução exacta

$$u = x(x-1)y(y-1),$$

que iremos posteriormente comparar com a solução numérica obtida.

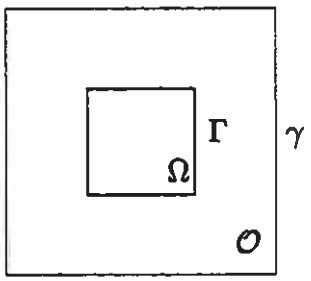


Fig. 1: Domínio fictício

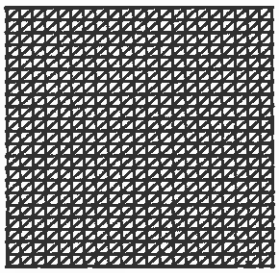


Fig. 2: Malha

Utilizando o algoritmo descrito na secção 5 com o critério de paragem $\varepsilon = 10^{-6}$, obtemos os seguintes resultados:

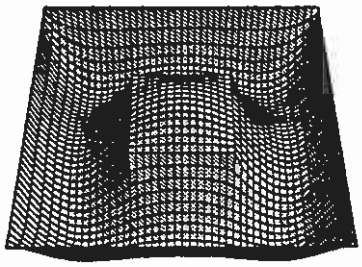


Fig. 3: Solução numérica em O.

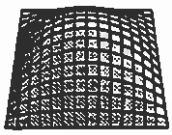


Fig. 4: Solução exacta em Ω.

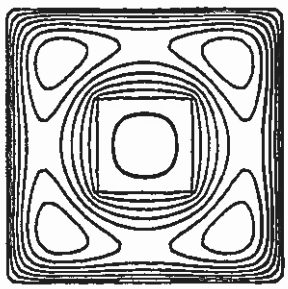


Fig. 5: Curvas de nível da solução numérica em O.

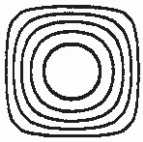


Fig. 6: Curvas de nível em Ω

A tabela seguinte apresenta os erros obtidos entre u e u_h, respectivamente a solução exacta do problema e a solução discreta correspondente, para três malhas diferentes, obtida pelo o Método de Domínios Fictícios.

malhas	h	$n.^o$ de iter.	$\|u-u_h\|_{\infty,\Omega}$	$\|u-u_h\|_{0,\Omega}$
(10×10)	$4,71 \times 10^{-1}$	4	$3,63 \times 10^{-3}$	$7,23 \times 10^{-3}$
(16×16)	$2,83 \times 10^{-1}$	5	$1,52 \times 10^{-3}$	$4,59 \times 10^{-3}$
(28×28)	$1,57 \times 10^{-1}$	8	$5,0 \times 10^{-4}$	$2,98 \times 10^{-3}$
(43×43)	$1,01 \times 10^{-1}$	11	$2,1 \times 10^{-4}$	$1,67 \times 10^{-3}$

Apresentamos mais um exemplo de aplicação do Método de Domínios Fictícios a domínios de fronteira seccionalmente Lipchitziana. Consideremos agora o mesmos problema formulado num domínio em forma de L e com f=2. Como sempre a solução obtida é independente da geometria do domínio $\mathcal{O}$.

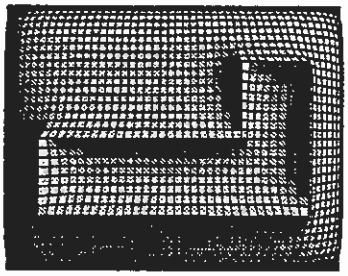


Fig. 7: Solução em $\mathcal{O}$.

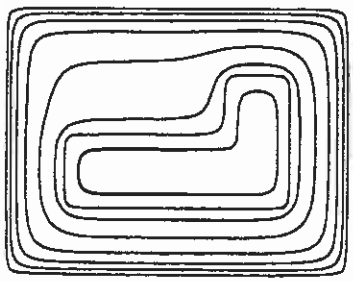


Fig. 8: Curvas de nível em Ω

7 Conclusão

Neste traballho apresentamos uma abordagem numérica do Método de Domínios Fictícios aplicado a um problema particular. A utilização de um multiplicador de Lagrange, associado à condição de fronteira do domínio genuino, permiti-nos o uso do algoritmo de gradiente conjugado trabalhando sempre no espaço do multiplicador, M_h. Esta técnica elimina as eventuais restrições geométricas existentes em Ω, sendo deste modo bem adaptado a problemas industriais onde as geometrias são geralmente complexas. As estimativas teóricas do erro são analisadas em [1].

Bibliografia

[1] Borges, L. R.:*Método de Domínios Fictícios para um problema de Stokes*, Tese de Mestrado, Instituto Superior Técnico, Lisboa(em preparação).

[2] Brezzi, F. e M. Fortin:*Mixed and Hybrid Finite Elements Methods*, Springer, New York (1991).

[3] Dinh, Q. V., e Glowinski, R., e He, J., e Kwock, V., and Pan, T. W., e J. Périaux *Lagrange Multiplier Approach to Fictitious Domain Methods: Application to Fluid Dynamics and Electro-Magnetics*, Domain Decomposition Methods for partial differential equations, SIAM, Philadelphia, Pa, 151-194 (1992).

[4] Girault, V.:*Error Analysis of a Fictitious Domain Method Applied to a Dirichlet Problem*, Japan J. Indust. Appl. Math., 12, 487-514 (1995).

[5] Girault, V. and Raviart, P. A.: *Finite Elements Methods For Navier-Stokes Equations*, Springer Series in Computational Mathematics (1986).

[6] Glowinski, R.:*Numerical Methods for Nonlinear Variational Problems*, Springer Series in Computational Physics, New York (1984).

[7] Glowinski, R.: *A fictitious domain method for Dirichlet problem and aplications*, Computer methods in Applied Mechanics and Engeneering 111, North-Holland, 283-303 (1994).

[8] Golub, G. , Loan V.:*Matrix Computations*, North Oxford Academic (1986).

[9] Quarteroni, A. e A. Valli:*Numerical Approximation of Partial differential Equations*, Springer Series in Computational Mathematics (1997).

Uma Aplicação do Teorema dos Resíduos

Miguel Moreira
Escola Superior de Tecnologia de Setúbal
SAM

José Vieira Antunes
Instituto Tecnológico e Nuclear
LDA

Heitor Pina
Instituto Superior Técnico
DEM

15 de Outubro de 1998*

Resumo

O movimento rotativo de um rotor numa região confinada determina o escoamento do fluído envolvente e o desenvolvimento de forças de interacção fluído-estrutura, cujo conhecimento é essencial na previsão do comportamento dinâmico deste sistema. A determinação explícita das força referidas a partir das equações de Navier-Stokes conduz à necessidade de resolução de integrais definidos do tipo,

$$G_k^{ij}(H,X,Y) = \int_0^{2\pi} \frac{\sin^i\theta\cos^j\theta}{(H - X\cos\theta - Y\sin\theta)^k}d\theta,$$

em que H, X, e Y são constantes tais que $X^2+Y^2 < H^2$ e i,j e k são parâmetros inteiros que podem variar entre zero e quatro.

A aplicação de uma forma particular do teorema dos resíduos da análise complexa constitui a solução natural do problema anterior, concretizada recorrendo ao auxílio de um manipulador simbólico para fazer face à extensão das manipulações algébricas necessárias.

1 Introdução

1.1 Formulação do Problema

Consideremos as forças resultantes do escoamento de fluído na região anular representada na figura 1, determinado pela rotação Ω do veio circular interno de raio R. A determinação destas forças (também designadas fluído-elásticas) é essencial no estudo do comportamento vibratório dos veios e rotores de equipamentos rotativos em geral. Em Antunes *et al.* [1], por

*Comunicação apresentada nas Jornadas de Aplicações da Matemática no Centro de Matemática do ISEL

exemplo, pode encontrar-se uma completa discussão teórica e a motivação para o estudo deste assunto.

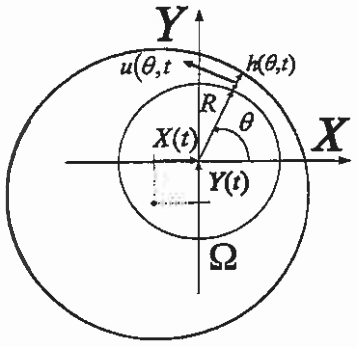


Figura 1: Geometria do escoamento

No apêndice B faz-se referência ao significado da simbologia utilizada. De referir que a *folga* $h(\theta,t)$, representada na figura indicada, pode ser bem aproximada recorrendo à seguinte equação,

$$h(\theta,t) = H - X(t)\cos\theta - Y(t)\sin\theta, \tag{1}$$

em que X e Y representam factores associados à excentricidade do sistema (posição do centro do veio interior) e H representa a folga que existiria se a excentricidade instantânea referida fosse nula. Naturalmente e para que o veio interior não entre em contacto com a superfície do *estator* supõe-se que, $X(t)^2 + Y(t)^2 < H^2$.

As equações de conservação da massa e do momento que permitem modelar (simplificadamente) o escoamento referido são (ver Antunes *et al.* [1]):

$$\frac{\partial h}{\partial t} + \frac{1}{R}\frac{\partial (hu)}{\partial \theta} = 0, \tag{2}$$

$$\rho\left\{\frac{\partial (hu)}{\partial t} + \frac{1}{R}\frac{\partial \left(hu^2\right)}{\partial \theta}\right\} + \tau + \frac{h}{R}\frac{\partial p}{\partial \theta} = 0, \tag{3}$$

em que $u(\theta,t)$ representa uma velocidade tangencial do fluído (valor médio na folga) e $\tau(\theta,t)$ as tensões de natureza dissipativa. Estas últimas podem ser descritas recorrendo à formulação semi-empírica

$$\begin{aligned}\tau(u) &= \tau_r(u) + \tau_s(u)\\ &= -\frac{1}{2}\rho f(\Omega R - u)^2 + \frac{1}{2}\rho f u^2\\ &= \rho f \Omega R u - \frac{1}{2}\rho f \Omega^2 R^2\end{aligned} \tag{4}$$

onde f representa um apropriado coeficiente de fricção.

Observe-se que reescrevendo a equação da continuidade (2) como, $\frac{\partial u}{\partial \theta} + \frac{u}{h}\frac{\partial h}{\partial \theta} = -\frac{R}{h}\frac{\partial h}{\partial t}$ deduz-se,

$$u(\theta,t) = \frac{R}{h}\left(-\int\left(\frac{\partial h}{\partial t}\right)d\theta\right) = \frac{R\left(\dot{X}\sin\theta - \dot{Y}\cos\theta + C\right)}{H - X\cos\theta - Y\sin\theta}, \qquad (5)$$

tendo em conta (1). De assinalar a presença da constante de integração, $C(t)$, na expressão da velocidade (5),assim obtida.

1.2 Determinação das Forças Fluído-elásticas

Denotando por $F_X(t)$ e $F_Y(t)$ as componentes segundo X e Y da força resultante que o fluído exerce no rotor, pode mostrar-se que

$$F_X(t) = -LR\int_0^{2\pi} p(\theta,t)\cos\theta d\theta = LR\int_0^{2\pi}\frac{\partial p(\theta,t)}{\partial\theta}\sin\theta d\theta, \qquad (6)$$

$$F_Y(t) = -LR\int_0^{2\pi} p(\theta,t)\sin\theta d\theta = -LR\int_0^{2\pi}\frac{\partial p(\theta,t)}{\partial\theta}\cos\theta d\theta, \qquad (7)$$

em que R e L representam o raio e o comprimento do rotor. Assim, integrando entre 0 e 2π, as seguintes formas equivalentes da equação (3),

$$-\frac{\partial p}{\partial\theta}\sin\theta = \left\{\rho\left\{R\frac{\partial(hu)}{h\partial t} + \frac{\partial(hu^2)}{h\partial\theta}\right\} + R\frac{\tau(u)}{h}\right\}\sin\theta, \qquad (8)$$

$$-\frac{\partial p}{\partial\theta}\cos\theta = \left\{\rho\left\{R\frac{\partial(hu)}{h\partial t} + \frac{\partial(hu^2)}{h\partial\theta}\right\} + R\frac{\tau(u)}{h}\right\}\cos\theta, \qquad (9)$$

deduz-se,

$$F_X(t) = -\rho R^2 L\int_0^{2\pi}\frac{\partial(hu)}{h\partial t}\sin\theta d\theta - \rho RL\int_0^{2\pi}\frac{\partial\left(hu^2\right)}{h\partial\theta}\sin\theta d\theta \qquad (10)$$
$$-R^2L\int_0^{2\pi}\frac{\tau(u)}{h}\sin\theta d\theta,$$

$$F_Y(t) = \rho R^2 L\int_0^{2\pi}\frac{\partial(hu)}{h\partial t}\cos\theta d\theta + \rho RL\int_0^{2\pi}\frac{\partial\left(hu^2\right)}{h\partial\theta}\cos\theta d\theta \qquad (11)$$
$$+R^2L\int_0^{2\pi}\frac{\tau(u)}{h}\cos\theta d\theta.$$

Tendo em conta a expressão conhecida da velocidade (5), facilmente se verifica que cada um dos integrais definidos representados nas equações (10) e (11), pode ser descrito com base em integrais definidos elementares do tipo,

$$G_k^{ij}(H,X,Y) = \int_0^{2\pi}\frac{\sin^i\theta\cos^j\theta}{(H - X\cos\theta - Y\sin\theta)^k}d\theta,\ 0\le i,j,k\le 4. \qquad (12)$$

A título de exemplo apresentamos a representação de um dos integrais definidos indicados:

$$\int_0^{2\pi} \frac{\partial(hu^2)}{h\partial\theta} \sin\theta d\theta = 2R^2 \left(\left(\left(\dot{X}\right)^2 - \left(\dot{Y}\right)^2 \right) G_2^{21} + 2\dot{X}\dot{Y}\, G_2^{30} \right)$$
$$+2R^2 \left(-\dot{X}\dot{Y}\, G_2^{10} + C\left(\dot{X}\, G_2^{11} + \dot{Y}\, G_2^{20}\right)\right)$$
$$-R^2 \left(\left(\dot{X}\right)^2 X G_3^{40} + X\left(\dot{Y}\right)^2 G_3^{22} - 2X\,\dot{X}\dot{Y}\, G_3^{31} \right)$$
$$-R^2 \left(C^2 X G_3^{20} + 2CX\left(\dot{X}\, G_3^{30} - \dot{Y}\, G_3^{21}\right)\right)$$
$$-R^2 \left(-\left(\dot{X}\right)^2 Y G_3^{31} - Y\left(\dot{Y}\right)^2 G_3^{13} + 2\,\dot{X}\, Y\, \dot{Y}\, G_3^{22} \right)$$
$$-R^2 \left(-C^2 Y G_3^{11} - 2CY\left(\dot{X}\, G_3^{21} - \dot{Y}\, G_3^{12}\right)\right).$$

Torna-se assim claro que a obtenção de expressões analíticas que descrevam $F_X(t)$ e $F_Y(t)$ está dependente do cálculo dos integrais definidos do tipo (12) em função dos parâmetros H, X e Y.

Refira-se que o seu cálculo recorrendo às técnicas da análise real dependente da computação prévia das primitivas envolvidas não é uma tarefa fácil, conduzindo frequentemente a expressões muito pesadas.

2 A aplicação do Teorema dos Resíduos

O procedimento natural para calcular estes integrais definidos (12) consiste na utilização do resultado elementar (consequência do teorema dos resíduos) da análise complexa (proposição 2.1) que seguidamente se expõe.

Proposição 2.1 *Seja $R(x,y)$ uma função racional em x e y cujo denominador não se anula na circunferência centrada na origem e de raio unitário. Então*

$$\int_0^{2\pi} R(\cos\theta, \sin\theta)\, d\theta = 2\pi i \sum [\textit{resíduos de } f(z) \textit{ no interior de } D] \quad (13)$$

em que

$$f(z) = \frac{R\left(\frac{1}{2}\left(z+\frac{1}{z}\right), \frac{1}{2i}\left(z-\frac{1}{z}\right)\right)}{iz} \quad (14)$$

e D representa o interior do círculo unitário centrado na origem.

Demonstração. Consultar Marsden [2], pg 302, por exemplo. ■

Pode encontrar-se também em Marsden [2] a definição dos conceitos de *resíduo*, *polo* e *ordem de um polo* de utilização necessária. A proposição 2.2 apresenta um resultado a partir do qual se torna possível a determinação de resíduos associados a polos de ordem arbitrária.

Proposição 2.2 *Suponha-se que f tem um polo de ordem k em z_0. Então*

$$Res(f, z_0) = \lim_{z \to z_0} \frac{\Phi^{(k-1)}(z)}{(k-1)!},$$

em que $\Phi(z) = (z - z_0)^k f(z)$.

Demonstração. Consultar Marsden [2], pg 272. ■

2.1 Exemplo de Aplicação

Ilustremos a aplicação destes resultados no cálculo de

$$G_3^{00}(H, X, Y) = \int_0^{2\pi} \frac{1}{(H - X\cos\theta - Y\sin\theta)^3} d\theta,$$

supondo naturalmente que $H > 0$ e $X^2 + Y^2 < H^2$.

1. Comecemos por determinar a função $f(z)$ nos termos da proposição 2.1,

$$\begin{aligned} f(z) &= \frac{R\left(\frac{1}{2}\left(z + \frac{1}{z}\right), \frac{1}{2i}\left(z - \frac{1}{z}\right)\right)}{iz} \\ &= \frac{1}{iz\left(H - X\frac{1}{2}\left(z + \frac{1}{z}\right) - Y\frac{1}{2i}\left(z - \frac{1}{z}\right)\right)^3} \\ &= \frac{-8z^2}{i\left((X - iY)z^2 - 2Hz + X + iY\right)^3} \\ &= \frac{-8z^2}{i(X - iY)^3 (z - z_1)^3 (z - z_2)^3}, \end{aligned}$$

   em que

$$z_1 = \frac{1}{(X - iY)}\left(H + \sqrt{H^2 - X^2 - Y^2}\right)$$

   e

$$z_2 = \frac{1}{(X - iY)}\left(H - \sqrt{H^2 - X^2 - Y^2}\right)$$

   são polos de ordem 3.

2. Repare-se que z_2 é o único polo que se localiza no interior do círculo unitário. Calculemos então o resíduo de f em z_2 com base na proposição 2.2. Seja,

$$\Phi(z) = \frac{-8z^2}{i(X - iY)^3 (z - z_1)^3},$$

   então

$$\text{Res}(f; z_2) = \frac{1}{2} \lim_{z \to z_2} \Phi''(z).$$

Concluíndo-se,

$$\mathrm{Res}(f; z_2) = i\frac{-16z_2^2 - 16z_1^2 - 64z_1z_2}{2(X-iY)^3(z_1-z_2)^5}.$$

3. Substituindo em (13) e simplificando obtemos finalmente o resultado desejado:

$$\begin{aligned}\int_0^{2\pi} \frac{1}{(H - X\cos\theta - Y\sin\theta)^3} d\theta &= \pi\frac{16z_2^2 + 16z_1^2 + 64z_1z_2}{(X-iY)^3(z_1-z_2)^5} \\ &= \frac{\pi\left(2H^2 + X^2 + Y^2\right)}{\left(\sqrt{H^2 - X^2 - Y^2}\right)^5}. \quad (15)\end{aligned}$$

3 Conclusões

No apêndice A podem encontrar-se os integrais definidos do tipo G_k^{ij} calculados pela via apresentada.

De referir que a metodologia referida se bem que conceptualmente simples exige a realização de computações algébricas extensas e pesadas que só puderam ser facilmente ultrapassadas com o recurso a um manipulador simbólico.

Este trabalho reforça a ideia da importância de se considerar na formação do Engenheiro uma sólida preparação matemática (nomeadamente e em particular o conhecimento de alguns resultados elementares da análise complexa) e a familiaridade na utilização das ferramentas computacionais de manipulação simbólica actualmente disponíveis.

Referências

[1] Antunes, J., Axisa, F. and Grunenwald, T., *Dynamics of rotors immersed in eccentric annular flow. Part1:Theory*, Journal of Fluid and Structures (1996), 10, 893-918.

[2] Marsden, J. E. and Hoffman, M. J., *Basic Complex Analysis*, Second Edition, Freeman, 1987.

A Integrais Azimutais

$$G_1^{00} = \frac{2\pi}{\sqrt{H^2 - X^2 - Y^2}} \quad (16)$$

$$G_1^{01} = \begin{cases} 0 \text{ se } X = Y = 0 \\ 2\pi X \frac{H - \sqrt{(H^2 - X^2 - Y^2)}}{(X^2+Y^2)\sqrt{(H^2 - X^2 - Y^2)}} \text{ c.c.} \end{cases} \quad (17)$$

$$G_1^{10} = \begin{cases} 0 \text{ se } X = Y = 0 \\ 2\pi Y \frac{H - \sqrt{(H^2 - X^2 - Y^2)}}{(X^2+Y^2)\sqrt{(H^2-X^2-Y^2)}}, \text{ c.c.} \end{cases} \tag{18}$$

$$G_1^{11} = \begin{cases} 0 \text{ se } X = Y = 0 \\ -2\pi Y X \frac{X^2+Y^2-2H^2+2\sqrt{(H^2-X^2-Y^2)}H}{(X^2+Y^2)^2\sqrt{(H^2-X^2-Y^2)}}, \text{ c.c.} \end{cases} \tag{19}$$

$$G_1^{20} = \begin{cases} \frac{\pi}{H} \text{ se } X = Y = 0 \\ 2\pi \frac{X^2(X^2+Y^2) - H^2(X^2-Y^2) + H(X^2-Y^2)\sqrt{(H^2-X^2-Y^2)}}{(X^2+Y^2)^2\sqrt{(H^2-X^2-Y^2)}}, \text{ c.c} \end{cases} \tag{20}$$

$$G_1^{02} = G_1^{00} - G_1^{20} =$$

$$= \begin{cases} \frac{\pi}{H} \text{ se } X = Y = 0, \\ 2\pi \frac{X^2Y^2+Y^4+H^2X^2-H^2Y^2-H\sqrt{(H^2-X^2-Y^2)}X^2+H\sqrt{(H^2-X^2-Y^2)}Y^2}{(X^2+Y^2)^2\sqrt{(H^2-X^2-Y^2)}}, \text{ c.c.} \end{cases} \tag{21}$$

$$G_2^{00} = 2\pi H \frac{\sqrt{(H^2 - X^2 - Y^2)}}{(H^2 - X^2 - Y^2)^2} \tag{22}$$

$$G_2^{01} = 2\pi X \frac{\sqrt{(H^2 - X^2 - Y^2)}}{(H^2 - X^2 - Y^2)^2} \tag{23}$$

$$G_2^{10} = 2\pi Y \frac{\sqrt{(H^2 - X^2 - Y^2)}}{(H^2 - X^2 - Y^2)^2} \tag{24}$$

$$G_2^{20} = \begin{cases} \frac{\pi}{H^2} \text{ se } X = Y = 0 \\ 2\pi \frac{HY^2(Y^2+X^2) + (H^2(X^2-Y^2) - X^4 + Y^4)\left(H - \sqrt{(H^2-X^2-Y^2)}\right)}{(X^2+Y^2)^2\left(\sqrt{(H^2-X^2-Y^2)}\right)^3}, \text{ c.c.} \end{cases} \tag{25}$$

$$G_2^{02} = G_2^{00} - G_2^{20} \tag{26}$$

$$G_2^{11} = \begin{cases} 0 \text{ se } X = Y = 0 \\ 2\pi XY \frac{H\left(-2H^2+3(X^2+Y^2)\right)+2(H^2-Y^2-X^2)\sqrt{(H^2-X^2-Y^2)}}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^3(X^2+Y^2)^2}, \text{ c.c.} \end{cases} \tag{27}$$

$$G_2^{30} = 2\pi Y \frac{-3\sqrt{(H^2-X^2-Y^2)}X^2-3HX^2-2HY^2+3\sqrt{(H^2-X^2-Y^2)}H^2+3H^3}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^3\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^3} \quad (28)$$

$$G_2^{03} = 2\pi X \frac{-3\sqrt{(H^2-X^2-Y^2)}Y^2-3HY^2-2HX^2+3\sqrt{(H^2-X^2-Y^2)}H^2+3H^3}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^3\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^3} \quad (29)$$

$$G_2^{12} = G_2^{10} - G_2^{30} \quad (30)$$

$$G_2^{21} = G_2^{01} - G_2^{03} \quad (31)$$

$$G_3^{00} = \left(2H^2 + X^2 + Y^2\right) \frac{\pi}{\left(\sqrt{(H^2 - X^2 - Y^2)}\right)^5} \quad (32)$$

$$G_3^{20} = \pi \frac{H^2 - X^2 + 2Y^2}{\left(\sqrt{(H^2 - X^2 - Y^2)}\right)^5} \quad (33)$$

$$G_3^{02} = G_3^{00} - G_3^{20} \quad (34)$$

$$G_3^{11} = \pi \frac{3XY}{\left(\sqrt{(H^2 - X^2 - Y^2)}\right)^5} \quad (35)$$

$$G_3^{10} = 3\pi \frac{HY}{\left(\sqrt{(H^2 - X^2 - Y^2)}\right)^5} \quad (36)$$

$$G_3^{01} = 3\pi \frac{HX}{\left(\sqrt{(H^2 - X^2 - Y^2)}\right)^5} \quad (37)$$

$$G_3^{30} = \pi Y \frac{\left(9H^4+9\sqrt{(H^2-X^2-Y^2)}\left(H^3-X^2H\right)-4H^2Y^2-15H^2X^2-2Y^4+4Y^2X^2+6X^4\right)}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^5\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^3} \quad (38)$$

$$G_3^{12} = G_3^{10} - G_3^{30} \quad (39)$$

$$G_3^{03} = \pi X \frac{\left(9H^4+9\sqrt{(H^2-X^2-Y^2)}\left(H^3-Y^2H\right)-4H^2X^2-15H^2Y^2-2X^4+4Y^2X^2+6Y^4\right)}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^5\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^3} \quad (40)$$

$$G_3^{21} = G_3^{01} - G_3^{03} \quad (41)$$

$$G_3^{40} = 3\pi\frac{\left(2H^6-5H^4X^2+4H^2X^4-X^6+3H^4Y^2-6H^2X^2Y^2+3X^4Y^2-4H^2Y^4+4X^2Y^4\right)}{\left(\sqrt{(H^2-X^2-Y^2)}\right)^5\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^4} + 3\pi\frac{2H\left(H^4-2H^2X^2+X^4+2H^2Y^2-2X^2Y^2-Y^4\right)}{(H^2-X^2-Y^2)^2\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^4} \quad (42)$$

$$G_3^{04} = G_3^{00} - 2G_3^{20} + G_3^{40} \quad (43)$$

$$G_3^{22} = G_3^{20} - G_3^{40} \quad (44)$$

$$G_3^{31} = 3\pi XY\frac{3X^4+X^2Y^2-7H^2X^2-2Y^4-H^2Y^2+4H^4}{\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^4\left(\sqrt{(H^2-X^2-Y^2)}\right)^5} + 3\pi XY\frac{4H\left(H^2-X^2\right)}{\left(H+\sqrt{(H^2-X^2-Y^2)}\right)^4(H^2-X^2-Y^2)^2} \quad (45)$$

$$G_3^{13} = G_3^{11} - G_3^{31} \quad (46)$$

B Simbologia Utilizada

$C(t)$ –Constante (dependente do tempo) associada à integração da equação da continuidade;
f–Coeficiente de fricção na parede do rotor/parede do estator;
$F_X(t), F_Y(t)$–Forças fluidoelásticas;
$h(\theta,t)$–Folga local;
L–Comprimento mergulhado do veio (rotor);
$p(\theta,t)$–Pressão azimutal;
R–Raio do veio (rotor) imerso;
t–Tempo;
$u(\theta,t)$–Velocidade tangencial local;
$X(t), Y(t)$–Posição do veio (rotor);
θ–Ângulo azimutal;
ρ–Massa volúmica do fluído;
$\tau(u)$ –Tensão de corte total (como função de u);
$\tau_r(u)$ –Tensão de corte na parede do rotor (como função de u);
$\tau_s(u)$ –Tensão de corte na parede do estator (como função de u);
Ω–Velocidade angular do rotor;
μ–Viscosidade dinâmica do fluído em escoamento;

Aplicações da Teoria Matemática da Comunicação

David P. Coutinho Fernando M. G. Sousa

Centro de Cálculo,
DEEC, ISEL
E-mail: {davidpc,fsousa}@ cc.isel.pt

Resumo

O presente artigo visa dar resposta unificada às questões do que é a informação, da transmissão de dados com segurança e da compressão de dados, usando a Teoria da Informação. Aplicando os conceitos da Teoria das Probabilidades e o conceito de entropia, ilustra-se como é possível demonstrar que existem sistemas com segurança perfeita e aborda-se o problema da compressão e dos seus limites; discute-se a possibilidade de compressão de ficheiros face às suas características estatísticas e como tirar partido destas na compressão.

1. Introdução

Nos anos 40, C. E. Shannon introduziu a Teoria Matemática da Comunicação, ou Teoria da Informação, motivado pelo problema das comunicações com segurança "verdadeira". Concentrou-se inicialmente no estudo da estrutura matemática genérica e propriedades dos sistemas de comunicação com segurança. Na sequência deste estudo [1][1], estabeleceu um modelo de sistema de comunicação genérico e formalizou os conceitos de medida de informação, de capacidade de transferência de informação sobre um canal e de codificação [2].

Um dos resultados mais importante do seu trabalho foi a formalização da ideia (abstracta) de incerteza ou informação. Para ilustrar este conceito, considere-se o seguinte exemplo: o resultado da corrida de dois cavalos "iguais" é menos incerto do que de outra corrida com 8 cavalos "iguais". Antes da corrida temos incerteza em relação ao resultado, depois de sabermos o resultado temos informação, que pode ser vista como a resolução da incerteza e está relacionada com o inverso da probabilidade desse resultado.

Mas como medir informação? A entropia pode ser entendida como uma medida matemática da informação necessária, em média, para descrever uma variável aleatória (v.a.) ou como uma medida da incerteza acerca desta. Seja X uma v.a. discreta que toma valores de

[1] Trabalho inicialmente publicado em 1945 mas classificado como confidencial.

um conjunto finito X, de acordo com uma distribuição de probabilidades p(X). Define-se entropia (ou incerteza) de uma v.a. X por

$$H(X) = \sum_{x \in X} p(x) \log_2 [1 / p(x)] \qquad (1.1)$$

e satisfaz $0 \leq H(X) \leq \log_2 n$

(sendo n a cardinalidade de X) com igualdade à esquerda sse $\exists x \in X : p(x)=1$ e à direita (máxima entropia) sse $\forall x \in X : p(x)=1/n$, isto é, se X tomar todos os valores com igual probabilidade. A entropia é um número real que depende apenas do conjunto de valores diferentes de zero de p(x) e vem expressa em bits[2] por concretização da v.a. X ou seja bits/símbolo.

Nas secções seguintes ilustra-se a aplicação deste conceito em áreas como a criptografia e a compressão de dados.

2. Transmissão de dados com segurança perfeita

É possível enviar pela Internet dados relativos a uma compra electrónica, garantido a confidencialidade dos mesmos? Ou por outras palavras, existe transmissão de dados com segurança perfeita? A resposta a estas perguntas é dada pela Criptologia. Os assuntos abordados por esta ciência podem ser divididos em criptoanálise e criptografia.

O objectivo fundamental da criptografia é permitir que duas pessoas, geralmente referidas por Alice e Bob, comuniquem através dum canal inseguro, no sentido em que um "estranho" (Oscar) não consiga perceber o que está a ser "dito". Esse canal pode ser a Internet, por exemplo. A informação que Alice pretende enviar para Bob, designa-se por texto em claro, pode ser um texto em língua portuguesa, dados numéricos, ou qualquer outra coisa. Alice cifra o texto em claro usando uma chave predeterminada e envia o resultante texto cifrado pelo canal. Com base neste, Oscar não consegue determinar o texto em claro, ao contrário de Bob que conhece a chave.

Em termos matemáticos sistema criptográfico define-se como sendo o quintupleto (P,C,K,E,D) onde P é o conjunto finito de possíveis textos em claro (espaço de textos em claro), C é conjunto finito de possíveis textos cifrados, K é o conjunto finito de possíveis chaves, E é o conjunto de regras de cifra e finalmente D é o conjunto de regras de decifra. Para cada $k \in K$, existe uma regra de cifra $e_k \in E$ e a correspondente regra de decifra $d_k \in D$. Cada $e_k : P \rightarrow C$ e $d_k: C \rightarrow P$ são funções tais que $d_k(e_k(x)) = x$ para $\forall x \in P$.

---

[2] Não confundir com a contracção das palavras *binary digits* (*bits*).

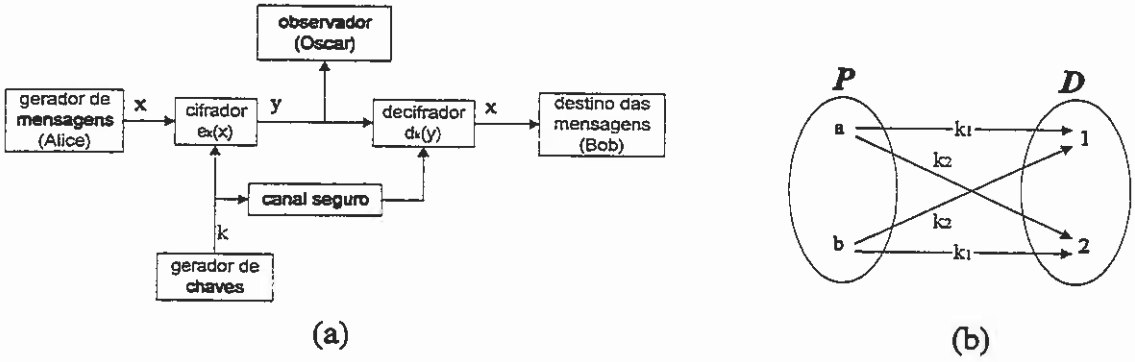


Fig.1 a) Modelo genérico proposto por Shannon para os sistemas criptográficos.
b) Diagrama dum sistema criptográfico exemplo.

Como primeiro passo para a análise matemática dos sistemas criptográficos Shannon idealizou um modelo genérico, tal com o que se representa na figura 1.a). Existem no entanto outras representações mais conveniente para efeitos ilustrativos. Para isso considere-se por exemplo o sistema criptográfico representado sob a forma de diagrama na figura 1.b).

O conceito de segurança perfeita pode-se definir informalmente como sendo a impossibilidade de Oscar obter informação acerca do texto em claro por observação do texto cifrado. Formalmente diz-se que um sistema criptográfico tem segurança perfeita se

$$H(x|y) = H(x) \quad \text{para todo o } x \in \boldsymbol{P}, y \in \boldsymbol{C}.$$

Analisemos o sistema da figura 1.b) em termos de entropia, para determinarmos se permite segurança perfeita. Antes porém, façamos algumas considerações. Cada texto e cada chave é constituído apenas por um símbolo. Uma chave em particular não é usada para cifrar mais do que um texto, pelo que o número de chaves é pelo menos igual ao número de textos a cifrar. Existe uma distribuição de probabilidades que caracteriza completamente uma v.a. discreta X, que toma valores no espaço de textos em claro, $\boldsymbol{P}$. Seja p(x) a probabilidade à priori do texto x ocorrer. Admita-se que a chave k é escolhida, de forma aleatória pela Alice e pelo Bob, de acordo com uma distribuição fixa, designada por p(k). Note-se que a chave é escolhida antes de se saber qual o texto a transmitir, por isso é razoável assumir que a chave k e o texto são acontecimentos independentes. Finalmente, existe uma distribuição de probabilidades que caracteriza completamente uma v.a. discreta Y, que toma valores no espaço de textos cifrados, $\boldsymbol{C}$.

As distribuições de probabilidades de $\boldsymbol{P}$ e $\boldsymbol{K}$ induzem a distribuição de probabilidades de $\boldsymbol{C}$. Donde, é possível calcular a probabilidade p(y) em que y é o texto cifrado. Assim para todo o $y \in \boldsymbol{C}$ temos que

$$p(y) = \sum_{i,j} p(x_i)\, p(k_j) \quad \text{para todo } x_i \text{ e } k_j \text{ tal que } e_{kj}(x_i) = y \qquad (2.1)$$

A probabilidade de ser y o texto cifrado dado que x é o texto em claro calcula-se por

$$p(y|x) = \sum_{j} p(k_j) \quad \text{para todo } k_j \text{ tal que } e_{kj}(x) = y \qquad (2.2)$$

Admitamos então que são conhecidas as probabilidades à priori dos textos em claro e das chaves, respectivamente p(a) = 0,25 e p(k1) = 0,5 (cada chave é usada com igual probabilidade). Aplicando a definição de entropia, expressão (1.1), determina-se que a incerteza em relação aos textos em claro e a incerteza das chaves é, em média, $H(X) \approx 0{,}81$ bits/símbolo e H(K) = 1 bit/símbolo. Para se determinar a incerteza relativamente aos textos cifrados H(Y), é necessário determinar primeiro p(y) para todo o $y \in C$, aplicando a expressão (2.1). Determinada esta distribuição de probabilidades vem que H(Y) = 1 bits/símbolo.

De seguida observemos qual a quantidade de informação necessária, em média, para descrever os textos em claro e os cifrados, ou seja o par de v.a. X e Y. Para isso aplica-se a definição de entropia conjunta [3]

$$H(X,Y) = \sum_{i,j} p(x_i, y_j)\, \log_2 [\, 1/\, p(x_i, y_j)\,]$$

sendo necessário calcular primeiro a probabilidade conjunta p(x,y). Os resultados desses cálculos apresentam-se na tabela 1. Com bases neles determina-se então que $H(X,Y) \approx 1{,}81$. Como se observa H(X,Y) = H(X) + H(Y). Mas este é um resultado que é válido apenas se X e Y forem estatisticamente independentes. Logo conclui-se que neste sistema, e nas condições descritas, os textos em claro são independentes dos cifrados.

$p(x_i, y_j)$	1	2
a	1/8	1/8
b	3/8	3/8

Tabela 1

$p(x_i \mid y_j)$	1	2
a	1/4	1/4
b	3/4	3/4

Tabela 2

Determine-se agora qual a incerteza em relação aos textos em claro depois de observados os textos cifrados. Para tal aplica-se a definição de entropia condicionada [3]

$$H(X|Y) = \sum_{i,j} p(x_i, y_j)\, \log_2 [\, 1/\, p(x_i \mid y_j)\,].$$

A probabilidade condicionada $p(x_i \mid y_j)$ pode ser obtida aplicando a lei de Bayes. Dessa forma obtêm-se os resultados apresentados na tabela 2. Com base nestes determina-se que

$$H(X|Y) \approx 0,81 = H(X).$$

Ou seja, a incerteza sobre o texto em claro mantém-se antes e depois de observarmos o texto cifrado, logo "mais vale tentarmos adivinhar qual foi o texto em claro independentemente das observações". Esta conclusão pode ser reforçada, se calcularmos a informação mútua das v.a. X e Y, porque é uma medida da quantidade de informação média que a v.a. X contém acerca da v.a. Y. Usando a relação entre a entropia e a informação mútua, de acordo com [3]

$$I(X;Y) = H(X)-H(X|Y)$$

vem que $I(X;Y) = 0$ neste caso, porque como vimos $H(X|Y) = H(X)$. Por isso, não existe redução da incerteza de X por conhecimento de Y, ou seja, não há "ganho" de informação acerca do texto em claro por observação do cifrado, logo este sistema tem segurança perfeita.

Shannon deu-nos um exemplo simples de cifrador perfeito, o designado por *One Time Pad* proposto, sem prova de segurança, por Vernam em 1926. Consiste em "esconder" um texto binário em claro adicionando módulo 2 (XOR) uma chave secreta binária aleatória com a mesma dimensão do texto a cifrar. Este sistema tem como modelo o diagrama da figura 1.b), já analisado e para o qual se fez prova de segurança.

O objectivo principal de Oscar é determinar a chave para assim poder "escutar" tudo. Para avaliarmos a incerteza acerca da chave quando se conhece o texto cifrado, aplica-se a definição de equívoco da chave, tal como vem em [4],

$$H(K|Y) = H(K) + H(X) - H(Y)$$

assumindo que K e X determinam um único Y, $H(Y|K,X) = 0$, e que K e Y determinam um único X, ou seja $H(X|K,Y) = 0$. Aplicando esta expressão ao exemplo analisado vem que

$$H(K|Y) = 1 + 0,81 - 1 = 0,81$$

verificando-se que é menor do que H(K), sendo a diferença a quantidade de informação revelada pelo texto cifrado, pelo simples facto de os textos em claro não serem equiprováveis, neste caso (senão teríamos $H(K|Y) = 1 + 1 - 1 = 1$). Usando sempre a mesma chave o equivoco vai sendo cada vez menor, porque a distribuição de probabilidades dos textos em claro reflecte-se nos textos cifrados e fica cada vez mais "visível". Mas isto pode ser evitado se maximizarmos H(X), fazendo dessa forma com que $H(K|Y) = H(K)$.

Levanta-se assim o problema da representação dos textos em claro x, que de acordo com Shannon deve ser tratado separadamente. Para isso introduziu e formalizou o conceito de codificação de fonte ou compressão de dados, que veremos de seguida.

3. Compressão de dados

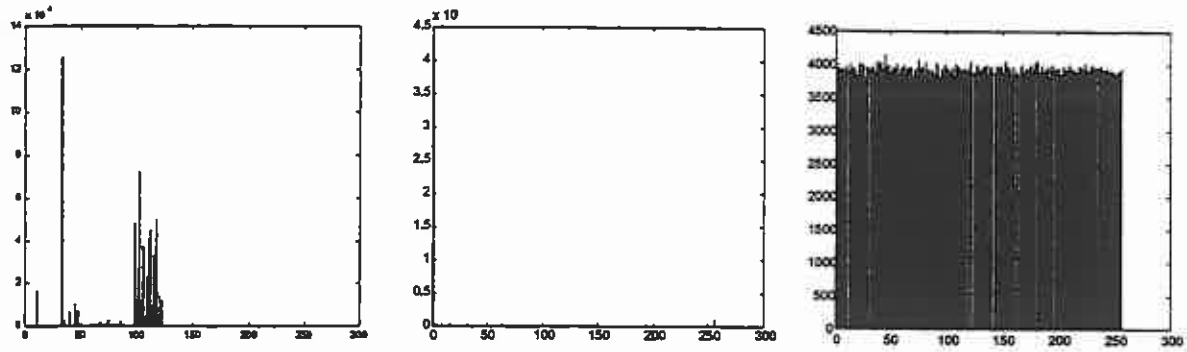
É possível reduzir a dimensão de todo e qualquer ficheiro, sem que haja perda de informação, recorrendo à compressão? A resposta é negativa. Segundo Shannon não é possível representar, sem perdas, os dados contidos num ficheiro[3], por exemplo, com um número médio de dígitos binários por cada símbolo, inferior ao da entropia desse ficheiro (informação média contida em cada símbolo). Este é outro resultado fundamental do seu trabalho [2] - os limites da compressão.

Fig.2 - O paradigma da compressão.

O objectivo da compressão de dados é eliminar a redundância (da fonte) dos dados. Na figura 2 representa-se um dos modelos mais comuns para descrever o paradigma da compressão [5]. Consiste num codificador que com base num modelo faz a tradução da mensagem numa sequência de dígitos binários, formada por códigos de dimensão variável. Idealmente o comprimento médio dos códigos gerados será igual à entropia da mensagem (codificador óptimo). O descodificador traduz essa sequência para recuperar a mensagem original, utilizando um modelo idêntico elaborado a partir de mensagens anteriores. O modelo recebe símbolos da mensagem e produz estimativas de probabilidades de acordo com determinado conjunto de dados e regras. A exactidão dessas estimativas dependem de quanto conhecimento de contexto se utiliza na obtenção das probabilidades dos símbolos.

A possibilidade de compressão de ficheiros relaciona-se com as suas características estatísticas e portanto com a entropia. Analise-se alguns tipos de ficheiros. Consideremos por exemplo, o seguintes ficheiros: BOOK1 (750 K*byte*) - texto na língua inglesa, PIC (501 K*byte*) - - *bit-map* duma imagem, e RAND.256 (977 K*byte*) - dados "pseudo" aleatórios. Na figura 3 ilustram-se os histogramas respectivos.

[3] Sequência de símbolos



a) b) c)

Fig.3 - Histogramas de ficheiros tipo a) texto em língua inglesa b) *bit-map* duma imagem c) dados "pseudo" aleatórios.

A análise dos histogramas revela que o ficheiro RAND.256 aproxima-se da situação de máxima entropia, uma vez que os valores dos símbolos constituintes são quase equiprováveis. Este facto confirma-se com os resultados da entropia estimada ($\hat{E}$) a partir dos histogramas:

$\hat{E}(X)_{BOOK1} = 4{,}5$ bits/símbolo, $\hat{E}(X)_{PIC} = 1{,}2$ bits/símbolo e $\hat{E}(X)_{RAND256} = 8$ bits/símbolo.

Então, não é possível comprimir o ficheiro, facto que se verifica na prática (mesmo com o Pkzip), confirmando-se assim os limites da compressão de Shannon.

Por outro lado constata-se que no ficheiro PIC existe um símbolo (o zero) que é muito mais provável do que os restantes, não sendo tão grande o desequilíbrio no ficheiro BOOK1. Ora o facto de existir tão grande desequilíbrio reflecte-se na entropia, justificando a diferença dos valores obtidos para estes dois ficheiros. Porque a entropia da imagem é muito menor do que a do texto, ou seja a redundância é maior na imagem, então é expectável que a compressão desta permita representações sem perda com menos dígitos binários/símbolo, em média, o que também se verifica na prática. Portanto, quanto maior a redundância na representação dos dados maior a possibilidade de compressão.

Para se estimar a entropia duma linguagem, ou de qualquer tipo de dados "estruturados" onde exista relação entre os símbolos, deve-se utilizar estatísticas referentes ao conjunto de n letras ou símbolos (n-gramas), com $n \to \infty$. Por exemplo, determine-se uma estimativa da entropia do Inglês a partir de BOOK1, considerando apenas as 26 letras do alfabeto. Resulta em

$\hat{E}(X) = 4{,}18$ bits/símbolo, $\hat{E}(X,Y)/2 = 3{,}90$ bits/símbolo e $\hat{E}(X,Y,Z)/3 = 3{,}65$ bits/símbolo.

Por limitações computacionais considerou-se até trigramas, o que é insuficiente para se obter uma boa estimativa porque existem palavras com mais de 3 letras e as primeiras condicionam sempre as últimas. Note-se que o valor empírico da entropia do Inglês é 1,25 bits/símbolo, segundo Stinson [4], sendo muito inferior aos resultados obtidos.

Aplicando a definição de entropia conjunta, conhecendo a distribuição de probabilidades dos digramas que constituem os ficheiros BOOK1 e PIC, estima-se que

$$\hat{E}(X,Y)_{BOOK1}/2 = 4{,}1 \text{ bits/símbolo e } \hat{E}(X,Y)_{PIC}/2 = 1{,}0 \text{ bits/símbolo.}$$

Estes valores são inferiores aos anteriormente calculados para $\hat{E}(X)_{BOOK1}$ e $\hat{E}(X)_{PIC}$, concluindo-se por isso que os símbolos nestes ficheiros não são independentes, porque senão a informação somava-se e a entropia ao nível do par de símbolos dividida por dois era igual à entropia ao nível do símbolo. Relativamente ao ficheiro RAND.256 vem que

$$\hat{E}(X,Y)_{RAND256}/2 = 7{,}98 \text{ bits/símbolo}$$

o que revela o seu carácter "pseudo" aleatório, ou seja, os símbolos estão de alguma forma relacionados.

Um exemplo de como tirar partido das características estatísticas e da relação entre os símbolos num ficheiro, está patente no novo programa de compressão BZIP2 (mais eficaz do que o Pkzip). Trata-se da transformada de Burrows-Wheeler [6].

A transformada de Burrows-Wheeler (BWT) é um algoritmo que a partir dum bloco com símbolos o rearranja usando um algoritmo de ordenação. O bloco daí resultante contém exactamente os mesmos símbolos que tinha inicialmente diferindo apenas na sua ordem (e no índice adicionado no final do bloco [7]). Agora, tem uma particularidade caso os símbolos estejam originalmente relacionados (não sejam independentes): a probabilidade dum símbolo ser igual ao anterior é grande. Então o bloco resultante desta transformação tem mais redundância, logo menor informação (entropia), permitindo por isso maior compressão que o bloco original. A transformada é reversível, o que significa que a ordem original dos símbolos pode ser reposta sem perda de fidelidade.

Na tabela 3 apresentam-se os resultados, expressos em bits/símbolo, da entropia estimada para os ficheiros constituintes do Calgary Corpus[4], antes e depois de aplicada a BWT. Observe-se que $\hat{E}(X)$ mantém-se (sendo expectável um ligeiro aumento pois foi adicionado um índice) enquanto que do ponto de vista dos digramas a redução de $\hat{E}(X,Y)/2$ é notória. Este facto é fundamental na interpretação dos resultados da compressão destes ficheiros com codificadores de entropia (estatísticos), apresentados na tabela 4. Note-se que os resultados são valores médios expressos em dígitos binários (*bits*) por grupo de oito *bits* (*byte*).

[4] Conjunto normalizado de ficheiros, preparado na Universidade de Calgary (Canadá), utilizado na investigação em compressão de dados.

Calgary Corpus	$\hat{E}(X)$	$\hat{E}_{BWT}(X)$	$\hat{E}(X,Y)/2$	$\hat{E}_{BWT}(X,Y)/2$
BIB	5,20	5,20	4,28	3,74
BOOK1	4,53	4,53	4,06	3,83
BOOK2	4,79	4,79	4,27	3,75
GEO	5,65	5,65	4,96	4,75
NEWS	5,19	5,19	4,64	4,12
OBJ1	5,95	5,95	4,71	4,57
OBJ2	6,26	6,26	5,07	4,44
PAPER1	4,98	4,99	4,31	3,86
PAPER2	4,60	4,60	4,06	3,69
PAPER3	4,67	4,67	4,11	3,81
PAPER4	4,70	4,71	4,09	3,88
PAPER5	4,94	4,94	4,23	3,99
PAPER6	5,01	5,01	4,31	3,87
PIC	1,21	1,21	1,02	1,00
PROGC	5,20	5,20	4,40	3,94
PROGL	4,77	4,77	3,99	3,36
PROGP	4,87	4,87	4,03	3,36
TRANS/BWT	5,53	5,53	4,44	3,57
valor médio	4,89	4,89	4,17	3,75

Tabela 3

Tipo de Compressor	Calg. Corpus [*bits/byte*]	**BWT**(Calg. Corpus) [*bits/byte*]
Codificador de Huffamn	4,99	5,00
Codificador Aritmético	4,95	4,96
Codificador Aritmético (digramas)	4,16	3,30

tabela 4

Utilizando um codificador de Huffman ou um Aritmético, com modelo estatístico ao nível do símbolo, antes e depois da BWT o resultado é praticamente igual, porque os símbolos são os mesmos, a distribuição estatística é igual, logo o código também é igual.

Com um codificador Aritmético usando um modelo estatístico ao nível dos digramas, verifica-se que depois da transformada a compressão é maior. Como a entropia estimada é menor para os digramas depois da BWT, então tem menos informação e por isso pode-se comprimir mais.

Mark Nelson em [7] faz a análise da BWT, complementado-a com uma implementação, na linguagem 'C', da nova técnica de compressão baseada nesta transformada.

4. Conclusão

Este artigo ilustra a aplicação da Teoria da Informação na criptografia e na compressão de dados. Na secção 2 recorrendo a um exemplo fez-se a análise do sistema criptográfico *One Tima Pad* de Vernam, para se verificar em termos de entropia que tem segurança perfeita. Desta forma evidenciou-se o papel importante que a Teoria da Informação tem na avaliação da segurança provável dos sistemas criptográficos, independentemente da capacidade computacional do observador (pode ser infinita). Por último fez-se a ligação da criptografia com a compressão de dados ilustrando a sua importância na segurança da chave.

Na secção 3 analisaram-se três ficheiros, de tipos diferentes, para ilustrar a relação entre as suas características estatísticas, a entropia e a possibilidade de compressão. Finalmente analisou-se a transformada de Burrows-Wheeler, para exemplificar como na compressão se pode tirar partido das características estatísticas dos dados. Observou-se o seu efeito sobre o conjunto de ficheiros normalizado Calgary Corpus e constatou-se o aumento de eficácia na compressão deste conjunto após esta transformada.

5. Bibliografia

[1] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, **28**, pp. 656-715, 1949.

[2] C. E. Shannon, "A mathematical theory of communication", Bell System Technical Journal, **27**, pp. 379-423, pp. 623-656, 1948

[3] T. M. Cover, J. A. Thomas, Elements of Information Theory, John Wiley & Sons, Inc., 1991.

[4] D. R. Stinson, Cryptography: theory and practice, CRC Press, Inc., 1995.

[5] T. C. Bell, I. H. Witten and J. G. Cleary, "Modeling for text compression", ACM Computing Surveys, vol. 21, nº 4, pp. 557-591, Dec. 1989.

[6] M. Burrows, D.J. Wheeler, "A Block-sorting Lossless Data Compression Algorithm", Digital Systems Research Center Research Report 124, May 1994.

[7] M. Nelson, "Data Compression with the Burrows-Wheeler Transform", Dr. Dobb's Journal, Sept. 1996.

Análise multivariada: uma ferramenta a ter sempre ao "pé"

M. Rosário de Oliveira* e José A. Maia**

* Departamento de Matemática e Centro de Matemática Aplicada, Instituto Superior Técnico. Universidade Técnica de Lisboa

** Laboratório de Cineantropometria. Faculdade de Ciências do Desporto e de Educação Física. Universidade do Porto.

Resumo

Correntemente o analista, depois de formular o seu problema, delinea a experiência e recolhe os dados. Ao trabalhá-los, é frequentemente assaltado pela dificuldade em encontrar significado (estatístico) para os resultados obtidos, que corrobore, ou não, as suas expectativas. A natureza multivariada dos dados é, em geral, responsável por este facto.

Neste trabalho apresenta-se um estudo sobre a selecção de jovens futebolistas, problema real em que a intervenção da análise multivariada teve um papel preponderante. Dada a inexistência de estudos desta natureza em Futebol, em Portugal, contrastaram-se três grupos etários distintos de jovens futebolistas de nível médio a elevado com jovens da mesma idade, cuja prática motora estava limitada às aulas curriculares de Educação Física. As nossas preocupações centraram-se em encontrar distinções entre os dois grupos de indivíduos, nas diferentes faixas etárias e procurar estabelecer relações entre os domínios motor e somático.

Palavras Chave: Matrizes de correlações, função discriminante, correlações canónicas.

1. Introdução

A modelação do desempenho desportivo-motor apresenta-se como o problema fundamental da pesquisa em Ciências do Desporto na vertente do rendimento. A pesquisa nesta matéria tem-se centrado na identificação das características óptimas do sujeito que se pensa estar intimamente associada à *performance*.

Este trabalho concentra-se numa faceta de um problema fulcral para os treinadores - o da selecção: como escolher os mais aptos, de um vasto conjunto de candidatos, que ofereçam elevadas possibilidades de (i) resposta adequada ao treino e (ii) sucesso competitivo. Este problema não tem solução fácil. Contudo, a identificação da relevância dos traços somáticos, motores, psicológicos e outros de atletas que "sobrevivem" ao treino e competição pode ser um auxiliar precioso neste processo.

Apesar do fascínio colectivo pelo Futebol, esta modalidade permanece, paradoxalmente,

menos investigada pelos pesquisadores das Ciências do Desporto (Silva, 1997). Em Portugal, e nos escalões mais baixos, o panorama é deveras desolador. Se nos deslocarmos para o domínio da selecção, então o quadro é ainda mais delicado, apesar das exigências colocadas aos jovens futebolistas em termos de resposta ao treino e à competição.

Alguns dos especialistas na matéria manifestam a necessidade da utilização adequada de ferramentas estatísticas de natureza multivariada, que possam ajudar a esclarecer os resultados dos estudos que têm sido desenvolvidos sobre o assunto.

2. Objectivo do estudo

Este estudo prende-se com objectivos de natureza analítica e substantiva:

- reduzir o conjunto original de variáveis a um outro que contenha a informação relevante na identificação de aspectos da selecção e da resposta ao treino em Futebol;
- identificar a eventual presença de um padrão de indicadores de selecção e resposta ao treino nas três faixas etárias consideradas no estudo;
- relacionar os domínios somático e motor nas diferentes faixas etárias.

3. Material e métodos

3.1 Amostra

A amostra deste estudo está dividida em dois grupos de contraste (futebolistas *versus* não futebolistas, designados por "sedentários") em cada um de três intervalos de idade.

Tabela 1: Dimensões dos sub-grupos da amostra em estudo.

Categoria	**Limites de idade**	**Dimensão da amostra**
Infantil (10-12 anos)	futebolistas	n_1=46
	"sedentários"	n_2=28
Iniciado (13-14 anos)	futebolistas	n_1=47
	"sedentários"	n_2=29
Juvenil (15-16 anos)	futebolistas	n_1=46
	"sedentários"	n_2=28

Os sujeitos "sedentários" são alunos de diferentes escolas do distrito do Porto que não realizam qualquer prática formal de desporto para além das aulas de Educação Física curricular.

Os futebolistas pertencem a clubes do distrito do Porto. A sua prática de treino é, no mínimo, de 3 treinos semanais e de um jogo-competição ao Sábado. Todos possuem, no mínimo, 2 anos de treino.

3.2 Medidas somáticas

Para calcular o somatótipo (*i.e.* a configuração morfológica externa presente do sujeito) foram obtidas 10 medidas somáticas: peso, altura, diâmetros bicondio-humeral e femoral,

perímetros braquial tenso e geminal, pregas de adiposidade subcutânea tricipital, subescapular, ilíaca e geminal. O procedimento de medição utilizado foi proposto pelo Grupo Internacional para o avanço da Cineantropometria (Ross e Marfell-Jones, 1983). As fórmulas usadas para calcular as componentes do somatótipo foram propostas por Carter e Heath (1990). O somatótipo é representado por três componentes derivadas dos três folhetos embrionários: a endomorfia (Endo) expressa o grau de gordura-magreza, a mesomorfia (Meso) o desenvolvimento musculo-esquelético relativamente à altura e Ectomorfia (Ecto) o desenvolvimento da linearidade dos segmentos.

3.3 Medidas motoras

Utilizou-se a bateria de testes proposta pela *American Alliance for Health Physical Education Recreation and Dance*. A sua estrutura é a seguinte:

Tabela 2: Variáveis motoras.

Componentes da aptidão física	**Testes**	**Representação da variável**
Força média	Número de abdominais	Abdom
Força inferior	Salto horizontal	Shoriz
Agilidade	Corrida vai-vem	Agilid
Velocidade	Corrida de 50 metros	50m
Resistência	Corrida de 12 minutos	12min

3.4 Análise estatística: métodos de interesse para o problema em estudo

Utilizou-se a análise discriminante (vide Seber, 1984) para perceber o que distingue os futebolistas dos "sedentários" nas várias faixas etárias. No caso do domínio motor utilizou-se a taxa de erro aparente como indicador para a escolha da melhor função discriminante, o que conduziu à redução do número de variáveis iniciais.

A análise de correlações canónicas (vide Gittings, 1980) foi empregue na tentativa de entender as relações lineares entre os dois domínios em estudo.

4. Metodologia

Ambos as ferramentas estatísticas utilizadas pressupõem a hipótese de normalidade multivariada dos dados. Esta foi verificada recorrendo ao papel de normalidade (Krzanowski, 1988). No caso da análise discriminante utilizou-se um método robusto, já que o papel de normalidade levantou algumas questões quanto a esta hipótese. Foram realizados testes de igualdade das matrizes de covariâncias dos dois grupos considerados (futebolistas e "sedentários"), hipótese rejeitada em todos os casos. Assim optou-se pela estimação da função discriminante linear por um método denominado pela autora (Pires, 1995) por *discriminante projection pursuit*. Para mais detalhes sobre a metodologia empregue neste trabalho vide Oliveira *et al.* (1998).

5. Resultados

5.1 Análise discriminante

i. Domínio motor

Para escolher o conjunto de variáveis motoras que conduziu à melhor função discriminante linear obtiveram-se todas as funções discriminantes possíveis. Entre estas foi escolhida aquela que apresentava uma menor taxa de erro aparente (um indicador optimista da qualidade do ajuste do modelo). Esta abordagem foi possível dado ao baixo número de variáveis envolvidas: 5, para cada faixa etária (vide tabela 2).

As funções discriminantes seleccionadas assim como as taxas de erro aparente correspondentes estão sintetizadas na tabela 3.

Tabela 3: Funções discriminantes para o domínio motor.

Faixa etária	**Função discrininante**	**Taxa de erro aparente**
Infantil	4.280 - 0.143Agilid - 0.199(50m) + 0.024Abdom - 0.969Shoriz	10.81%
Iniciado	3.198 - 0.930Agilid - 0.272(50m) + 0.147Abdom	14.47%
Juvenil	6.213 + 0.024Agilid - 0.989(50m)	7.90%

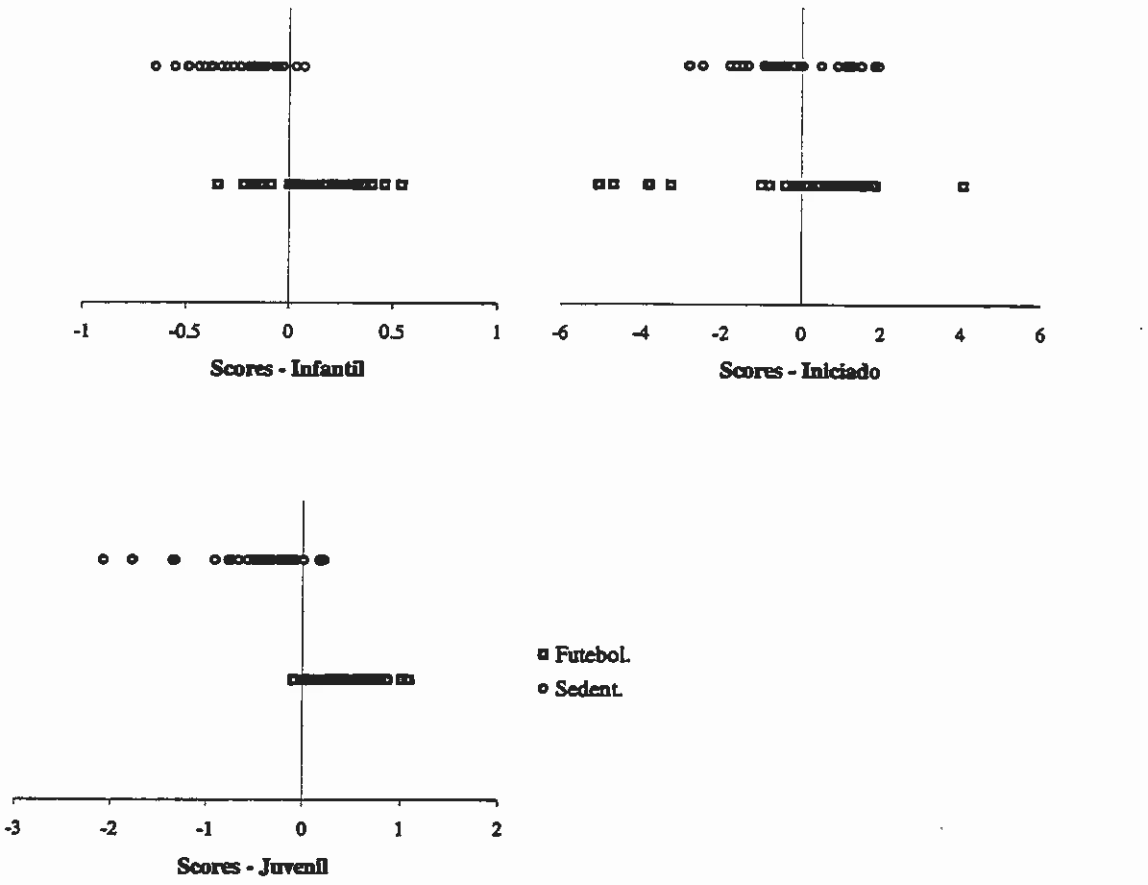


Figura 1: *Scores* discriminantes para o domínio motor.

A tabela 3 permite concluir que à medida que os indivíduos têm mais anos de treino as variáveis importantes para os distinguir são cada vez menos (menos uma que no escalão anterior). As variáveis agilidade (Agilid) e 50 metros (50m), que fazem sempre parte das três funções discriminantes, traduzem a noção de velocidade e deslocamento. A importância destas variáveis está bem clara no âmbito das exigências físicas colocadas pelo jogo de futebol.

É ainda importante realçar que a taxa de erro aparente é menor nos juvenis. Este facto é devido ao aumento das exigências do jogo, e ao carácter mais fino que a agilidade e a velocidade traduzem nas mudanças de direcção, fintas, arranques e desmarcações.

A figura 1 ilustra os resultados da reclassificação da amostra inicial. Um futebolista está bem classificado se o seu *score* fôr superior a zero e um sedentário está bem classificado se o seu *score* fôr negativo. Pode então afirmar-se que para os infantis a regra tende a maiores erros na classificação de futebolistas. A categoria iniciado é o caso em que a taxa de erro aparente é mais elevada. É nos juvenis que a função discriminante apresenta um melhor ajuste, e parece comportar-se igualmente bem nos dois casos.

ii. Domínio somático

Uma vez que no domínio somático se decidiu trabalhar apenas com 3 variáveis (Endo, Meso e Ecto) não se fez qualquer selecção destas.

Para os infantis não se encontrou diferenças médias significativas entre os dois grupos: futebolistas e "sedentários". Assim conclui-se que estas três variáveis só por si, não distinguem os indivíduos nesta faixa etária. Note-se que ao usar as variáveis somáticas medidas directamente nos indivíduos encontraram-se diferenças e conseguiu-se construir uma regra discriminante, apesar de ter uma taxa de erro aparente elevada: 25.68% (vide Oliveira *et al.*, 1998).

As funções discriminantes, e respectivas taxas de erro, para os iniciados e juvenis estão apresentadas na tabela 4.

Tabela 4: Funções discriminantes para o domínio somático.

Faixa etária	Função discriminante	Taxa de erro aparente
Iniciado	4.381 – 0.914Endo – 0.181Meso –0.363Ecto	25.00%
Juvenil	4.636 – 0.464Endo – 0.256Meso –0.848Ecto	27.03%

A tabela 4 parece evidenciar que a variável com maior peso na função discriminante para os iniciados é a endomorfia. No caso dos juvenis, a variável com maior peso passa a ser ectomorfia. A variável que em ambos os casos tem menor peso é sempre a mesomorfia.

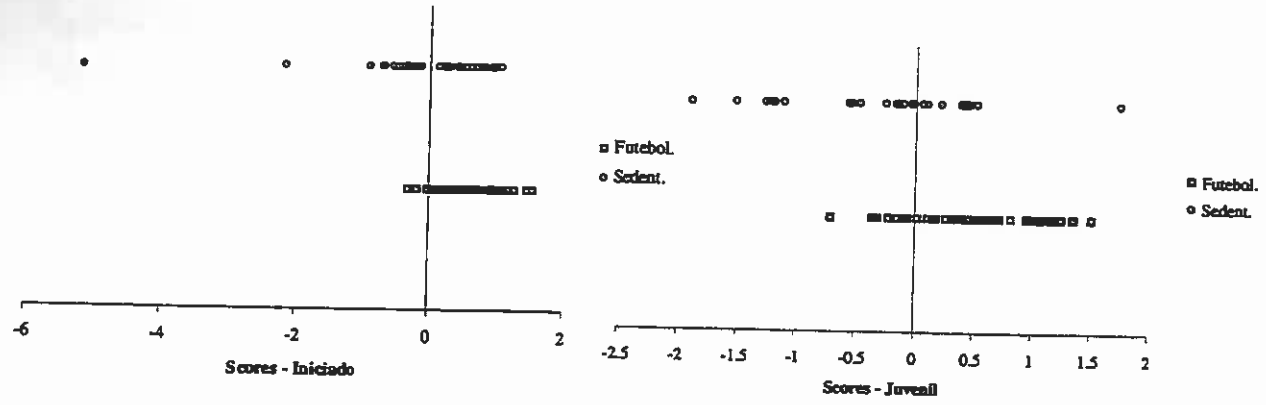


Figura 2: *Scores* discriminantes para o domínio somático.

A figura 2 permite-nos concluir que é o grupo dos "sedentários" aquele em que ambas as regras cometem mais erros, sendo problemático no caso dos iniciados (percentagem de indivíduos mal classificados do grupo dos "sedentários": 57.14%). Estes resultados permitem-nos concluir que estas três variáveis não conduzem a regras discriminantes satisfatórias.

5.2 Análise de correlações canónicas

Nas três faixas etárias em estudo, o teste de Bartlett (Cliff, 1987) sugere que se extraia apenas um par de variáveis canónicas. Representar-se-á por U_1 a variável canónica, do primeiro par, associada às variáveis somáticas, e V_1 a variável canónica, do primeiro par, associada às variáveis motoras.

Em todos os casos o coeficiente de correlação, ρ, entre o primeiro par de variáveis canónicas é elevado, assim como a percentagem de variância explicada pelas variáveis canónicas. Apenas no caso das variáveis somáticas se registam valores um pouco mais baixos.

i. Infantil

De acordo com a tabela 5, a variável canónica U_1 é dominada pelo valor da variável endomorfia, uma medida da gordura/magreza de um indivíduo. A variável V_1 está muito correlacionada com todas as variáveis motoras excepto com a agilidade, tendo os 50m um papel preponderante na definição da variável canónica. Da observação da figura 3 pode concluir-se que, em geral, os futebolistas tem valores baixos nas duas variáveis canónicas: são os mais "magros", os mais rápidos e os mais resistentes (embora a agilidade tenha um peso canónico negativo, o que indicaria que os futebolistas eram pouco ágeis, esta variável está pouco correlacionada com a variável canónica, logo não será tida em conta na interpretação da mesma). O que se esperaria era uma grande concentração de "sedentários" no primeiro quadrante (os mais "pesados", menos ágeis, mais lentos e os menos

resistentes) o que não acontece. O que se verifica é uma distribuição quase uniforme nos três primeiros quadrantes. Note que o facto de o quarto quadrante contêr poucas observações apenas significa que há poucos indivíduos com maior tendência para ser mais "pesado" e conseguir ser ágil e resistente, simultaneamente.

Tabela 5: Análise de correlações canónicas para a categoria infantil.

X_i (estandard.)	Y_i (estandard.)	Pesos Canónicos	$Corr(\bullet, U_1)$	$Corr(\bullet, V_1)$	% variância explicada por U_1	% variância explicada por V_1
Endo		0.965	0.997	0.589	33.13	12.35
Meso		-0.105	0.555	0.339	10.27	3.83
Ecto		-0.126	-0.758	-0.423	19.15	7.14
	Abdom	-0.145	-0.325	-0.532	2.11	5.66
	Agilid	-0.534	0.180	0.294	0.64	1.73
	Shoriz	-0.087	-0.424	-0.694	3.59	9.63
	50m	0.774	0.499	0.818	4.99	13.38
	12min	-0.514	-0.458	-0.751	4.20	11.28

V^2_{X,U_1} = % da variância total dos X's explicada por $U_1 = 62.55\%$

V^2_{Y,V_1} = % da variância total dos Y's explicada por $V_1 = 41.68\%$

V^2_{X,U_1} = % da variância total dos X's explicada por $V_1 = 23.32\%$

V^2_{X,U_1} = % da variância total dos Y's explicada por $U_1 = 15.53\%$

$\rho = 0.610$

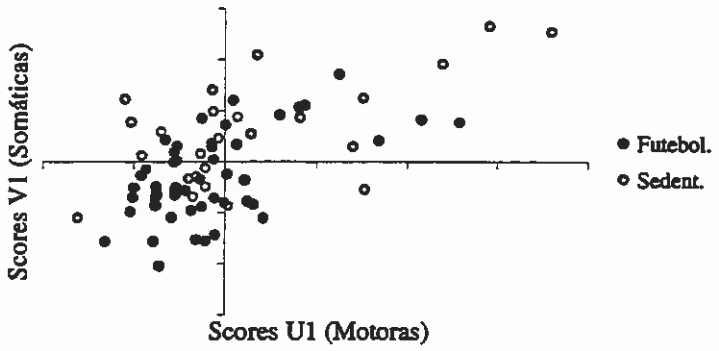


Figura 3: *Scores* dos infantis no primeiro par de variáveis canónicas.

ii. Iniciado

Tal como anteriormente, a tabela 6 indica que a variável canónica U_1 é dominada pelo valor da variável endomorfia. A variável V_1 pode ser interpretada como uma média ponderada das variáveis motoras. A figura 4 ilustra bem, que os futebolistas estão quase todos no terceiro quadrante, estando apenas 9 (em 47) numa vizinhança da origem (e fora do terceiro quadrante). Assim pode afirmar-se que, em geral, os futebolistas são mais magros e que conseguem fazer mais abdominais, ser mais ágeis, com melhores resultados na prova de salto horizontal, mais velozes e mais resistentes. Os "sedentários" localizam-se, na sua maioria, no primeiro e segundo quadrante, o que significa que têm maior tendência a ter resultados inferiores nas provas de aptidão, mas não se distinguem dos futebolistas pela sua

medida de gordura/magreza.

Tabela 6: Análise de correlações canónicas para a categoria iniciado.

X_i (estandard.)	Y_i (estandard.)	Pesos Canónicos	$Corr(\bullet, U_1)$	$Corr(\bullet, V_1)$	% variância explicada por U_1	% variância explicada por V_1
Endo		1.092	0.979	0.676	31.95	15.23
Meso		0.083	0.202	0.140	1.36	0.65
Ecto		0.267	-0.322	-0.222	3.46	1.65
	Abdom	-0.286	-0.525	-0.761	5.52	11.58
	Agilid	0.209	0.501	0.726	5.02	10.54
	Shoriz	-0.262	-0.517	-0.749	5.35	11.22
	50m	0.258	0.614	0.890	7.55	15.84
	12min	-0.298	0.475	-0.688	4.51	9.47

$V^2_{X,U_1} = 36.77\%,\ V^2_{Y,V_1} = 58.65\%,\ V^2_{X,U_{11}} = 17.53\%,\ V^2_{X,U_1} = 27.95\%,\ \rho = 0.690$

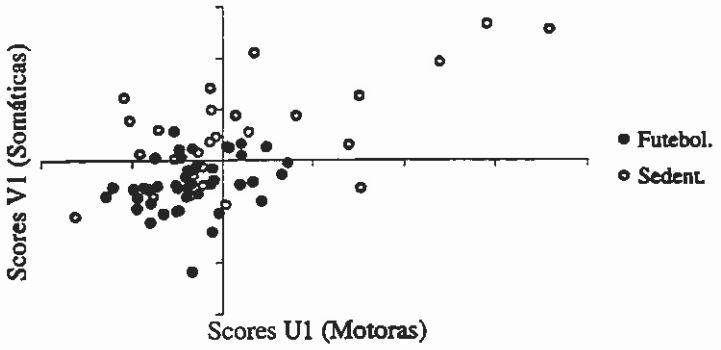


Figura 4: *Scores* dos iniciados no primeiro par de variáveis canónicas.

iii. Juvenil

Pela tabela 6 pode afirmar-se que variável canónica U_1 é dominada pelo valor da variável endomorfia e ectomorfia, ou seja com valores positivos teremos indivíduos altos e "pesados" e com valores negativos indivíduos magros mas com tendência para ser mais baixos. Esta nova variável não parece distinguir entre os dois grupos de indivíduos. A variável V_1 é essencialmente definida à custa da agilidade e salto horizontal. Não se considera a prova de resistência (12min), para interpretar V_1, uma vez que está pouco correlacionada com esta. A figura 5 ilustra bem que os futebolistas podem-se considerar quase todos com bons níveis de agilidade e de força nos membros inferiores. Sobre os "sedentários" apenas se pode afirmar que quase não existem indivíduos altos, "pesados", que sejam rápidos e com valores elevados da força dos membros inferiores (*i.e.* com localização no terceiro e quarto quadrantes).

Tabela 6: Análise de correlações canónicas para a categoria juvenil.

X_i (estandard.)	Y_i (estandard.)	Pesos Canónicos	$Corr(\bullet, U_1)$	$Corr(\bullet, V_1)$	% variância explicada por U_1	% variância explicada por V_1
Endo		1.101	0.543	0.335	9.82	3.74
Meso		-0.188	-0.362	-0.223	4.37	1.66
Ecto		0.842	0.397	-0.245	5.25	2.00
	Abdom	-0.079	0.397	-0.643	3.15	8.27
	Agilid	0.336	0.464	0.752	4.31	11.31
	Shoriz	-0.683	0.573	-0.928	6.56	17.22
	50m	0.169	0.441	0.715	3.89	10.22
	12min	0.320	0.112	-0.181	0.00	0.01

$V^2_{X,U_1} = 19.44\%,\ V^2_{Y,V_1} = 47.03\%,\ V^2_{X,U_1} = 7.40\%,\ V^2_{X,U_1} = 17.91\%,\ \rho = 0.617$

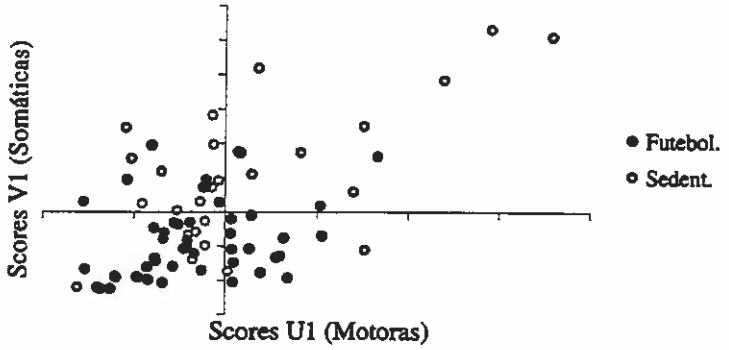


Figura 5: *Scores* dos juvenis no primeiro par de variáveis canónicas.

Agradecimentos

Agradeço à Prof. Ana M. Pires ter disponibilizado o seu *software* para a estimação robusta em análise discriminante, bem como pelos esclarecimentos que nos prestou.

Bibliografia

[1] J. E. L. Carter e B. H. Heath, *Somatotyping - development and applications*. Cambridge University Press, 1990.

[2] N. Cliff, *Analyzing multivariate data*. Harcout Brace Jovanivich Publishers, 1987.

[3] R. Gittings, *Canonical analysis. A review with applications in ecology*. Springer-Verlag, 1980.

[4] W. J. Krzanowski, *Principles of multivariate analysis. A user's perspective*. Clarendon Press, 1988.

[5] M. R. Oliveira, J. A. Maia e J. A. Branco, Análise dos efeitos do treino em jovens futebolistas. Submetido para publicação em *Actas do VI Congresso da Sociedade Portuguesa de Estatística*, Tomar, 1998.

[6] A. M. Pires, *Análise discriminante. Novos métodos robustos de estimação.*

Dissertação de Doutoramento, Universidade Técnica de Lisboa, 1995.

[7] W. Ross, e M. Marfell-Jones, *Kinanthropometry*. Em J. McDouglas, H. Wenger e H. Green (eds), *Physiological testing of the elite athlete*, 75-115. Mouvement Publications, Inc., 1983

[8] J. M. G. Silva, *Modelação táctica do jogo de futebol: estudo da organização da fase ofensiva em equipas de alto rendimento*. Dissertação de Doutoramento. FCDEF. Universidade do Porto. 1997.

[9] G. A. F. Seber, *Multivariate Observations*, John Wiley & Sons, 1984.

Modelos de Markov Não-Observáveis no Reconhecimento Automático de Fala e no Reconhecimento de Objectos em Imagens

João B. Sousa (jbs@cedet.isel.pt) Pedro M. Jorge (pmj@isel.pt)
Instituto Superior de Engenharia de Lisboa (ISEL)
DEEC / CEDET (tel: 8317235)

Resumo

Os Modelos de Markov Não-Observáveis são um modelo matemático probabilístico de sequências de observações, que constitui uma ferramenta matemática bastante versátil e que proporciona bons resultados quando aplicados a problemas de reconhecimento.

No presente artigo descreve-se brevemente os Modelos de Markov Não-Observáveis e ilustra-se a sua aplicação nos domínios do reconhecimento automático de fala e do reconhecimento de objectos em imagens.

1. Introdução

Os modelos de Markov Não-Observáveis (*Hidden Markov Models* - HMM) são muito utilizados em reconhecimento automático de fala [1][2] e, mais recentemente, noutros contextos, nomeadamente no reconhecimento de objectos bidimensionais [3][4]. Essencialmente porque são modelos probabilísticos que permitem lidar com a incerteza inerente a problemas de reconhecimento de padrões, possuem um suporte matemático muito rico que lhes confere uma grande versatilidade e proporcionam bons resultados de reconhecimento.

Este artigo está organizado da seguinte forma: na secção 2 é apresentado um resumo da teoria dos modelos de Markov não-observáveis; as secções 3 e 4 ilustram a aplicação dos modelos ao reconhecimento de fala e ao reconhecimento de objectos bidimensionais em imagens onde se apresentam também alguns resultados experimentais; as conclusões são apresentadas na secção 5.

2. Modelos de Markov Não-Observáveis

Um HMM é constituído por uma cadeia de Markov estacionária com um número finito de estado. Associada a cada estado existe uma função densidade de probabilidade de observação.

A utilização dos HMM's em sistemas de reconhecimento de padrões passa pela resolução dos seguintes problemas: determinar a probabilidade do HMM gerar uma sequência de observações (problema da determinação); estimar os parâmetros do HMM de modo a maximizar a probabilidade de gerar um conjunto de sequências de observações (problema da

estimação); determinar qual a sequência de estados que gera uma sequência de observações com maior probabilidade (problema da descodificação).

2.1. Os parâmetros do HMM

Uma cadeia de Markov estacionária é um processo estocástico discreto que verifica a propriedade de Markov - a probabilidade do processo assumir um dado valor q_k (que denominaremos por estado) no instante *t*, condicionada ao facto dos estados assumidos nos instantes anteriores (*t*-1, *t*-2,...) serem q_a, q_b, ... é igual à probabilidade do processo assumir o estado q_k no instante *t*, condicionada apenas ao facto do estado assumido no instante *t*-1 ser q_a, ou seja:

$$P[q_t = q_k | q_{t-1} = q_a, q_{t-2} = q_b, \ldots] = P[q_t = q_k | q_{t-1} = q_a].$$

A cadeia de Markov com N estados é definida por uma matriz de probabilidades de transição entre estados (de dimensão NxN) designada por matriz A. Cada um dos seus elementos a_{ij} representa a probabilidade do processo assumir o estado q_j dado que no instante anterior assumiu o estado q_i.

A evolução temporal da cadeia por entre os seus estados depende, não só das probabilidades de transição entre estados, como também do estado ocupado no instante inicial (*t*=1). As probabilidades de ocupação inicial dos estados são representadas por um vector (de dimensão N), designado por Π. Cada um dos seus elementos π_i representa a probabilidade da cadeia assumir o estado q_i no instante inicial.

Caso o espaço de observações seja finito de dimensão M (existem apenas M observações distintas), as funções densidade de probabilidade de observação associadas aos estados são discretas e representadas por uma matriz B (de dimensão NxM). Cada um dos seus elementos b_{ij} representa a probabilidade da observação j ser observada no estado i.

De acordo com a definição de probabilidade, os parâmetros do HMM, $\lambda=(A, B, \Pi)$ verificam as restrições estocásticas: $a_{ij} \geq 0$, $\pi_i \geq 0$ e $b_{ij} \geq 0$; $\sum_{j=1}^{N} a_{ij} = 1$, $\sum_{i=1}^{N} \pi_i = 1$ e $\sum_{j=1}^{N} b_{ij} = 1$.

2.2. Problema da Determinação

Pretende-se determinar $P(O|\lambda)$, a probabilidade do modelo λ gerar a sequência de observações $O = \{o_1, o_2, ..., o_T\}$ de comprimento T.

Considerando uma sequência de estados $Q = \{q_1, q_2, ...q_T\}$, e assumindo independência entre as observações, a probabilidade da sequência O ser gerada pela sequência Q é dada por:

$$P(O|Q,\lambda) = b_{q_1}(o_1) \cdot b_{q_2}(o_2) \cdot \ldots \cdot b_{q_T}(o_T) = \prod_{t=1}^{T} b_{q_t}(o_t)$$

Por outro lado, a probabilidade da sequência Q ocorrer, é dada por:

$$P(Q|\lambda) = \pi_{q_1} \cdot a_{q_1 q_2} \cdot a_{q_2 q_3} \cdot \ldots \cdot a_{q_{T-1} q_T} = \prod_{t=1}^{T} a_{q_{t-1} q_t} \text{ (onde se fez } \pi_{q_1} = a_{q_0 q_1}).$$

A probabilidade da sequência O ser gerada pelo modelo λ segundo a sua sequência de estados Q, vem:

$$P(O,Q|\lambda) = P(O|Q,\lambda) \cdot P(Q|\lambda) = \prod_{t=1}^{T} a_{q_{t-1} q_t} \cdot b_{q_t}(o_t)_T$$

Em virtude da sequência de observações poder ser gerada pelo HMM segundo qualquer uma das suas sequências de estados com o mesmo comprimento, não é possível determinar a sequência de estados que gerou a sequência de observações. Por esta razão, diz-se que a sequência de estados não é observável, e denominam-se estes modelos de modelos de Markov não-observáveis. Assim, a probabilidade do modelo λ gerar a sequência de observações O é dada pela soma das probabilidades do modelo gerar essa sequência de observações segundo cada uma das suas sequências de estados de comprimento T. Deste modo, designando por Q_T todas as sequências de estados do modelo, de comprimento T , vem:

$$P(O|\lambda) = \sum_{Q_T} P(O|Q,\lambda) \cdot P(Q|\lambda)$$

Note-se que existem N^T sequências de estados de comprimento T, o que torna a aplicação directa da expressão anterior muito exigente do ponto de vista computacional. Existe, no entanto, uma forma eficiente de efectuar este cálculo, recorrendo às probabilidades progressiva e regressiva (*Forward-Backward*) [5] determinadas de um modo recursivo.

2.3. Problema da Estimação

Pretende-se determinar os parâmetros A, B e Π do modelo λ de forma a maximizar a probabilidade do modelo gerar uma sequência de observações O. Esta maximização é efectuada recorrendo a uma função auxiliar $Q(\bar{\lambda},\lambda)$ definida por [5]:

$$Q(\bar{\lambda},\lambda) = \sum_{Q_T} P(O,q|\lambda) \ln P(O,q|\bar{\lambda})$$

Atendendo à desigualdade $\ln(x) \leq x - 1$, pode verificar-se que:

$$Q(\bar{\lambda},\lambda) - Q(\lambda,\lambda) \leq P(O|\bar{\lambda}) - P(O|\lambda)$$

pelo que os parâmetros serão determinados de forma a que a função $Q(\bar{\lambda},\lambda)$ atinja o seu máximo. Esta função sujeita às restrições estocásticas atinge o seu valor máximo quando :

$$\overline{\pi}_{q_1=i} = \frac{P(O,q_1=i|\lambda)}{\sum_{i=1}^{N} P(O,q_1=i|\lambda)} \qquad \overline{a}_{q_t=i q_{t+1}=j} = \frac{\sum_{t=1}^{T} P(O,q_t=i,q_{t+1}=j|\lambda)}{\sum_{j=1}^{N}\sum_{t=1}^{T} P(O,q_t=i,q_{t+1}=j|\lambda)}$$

$$\overline{b}_{q_t=i}(o_t=v_k) = \frac{\sum_{t=1}^{T} P(O,q_t=i,o_t=v_k|\lambda)}{\sum_{k=1}^{K}\sum_{t=1}^{T} P(O,q_t=i,o_t=v_k|\lambda)}$$

Estas equações, reescritas utilizando as probabilidades progressiva e regressiva de modo a proporcionarem maior eficiência computacional, são conhecidas por equações de reestimação de Baum-Welch.

2.3.1. Treino dos modelos

As equações apresentadas na secção anterior garantem que os novos parâmetros do modelo correspondem a um máximo da função $Q(\overline{\lambda},\lambda)$ e não a um máximo da probabilidade P(O|λ). Por esta razão, a obtenção dos parâmetros dos modelos efectua-se repetindo a aplicação das referidas equações sucessivamente aos modelos obtidos, até que se atinja um máximo (que em geral é um máximo local) de P(O|λ). Este processo de treino é efectuado sobre um modelo inicial cujos parâmetros são obtidos de um modo heurístico ou mesmo aleatório.

2.4. Problema da Descodificação

Embora não seja possível determinar a sequência de estados que gerou uma dada sequência de observações, é possível, no entanto, determinar a sequência de estados que gerou a sequência de observações com maior probabilidade. A determinação desta sequência é efectuada recorrendo ao algoritmo de Viterbi [1], que consiste num processo recursivo semelhante ao da determinação da probabilidade progressiva/regressiva, em que se faz uma maximização de probabilidades em vez de uma soma. Memorizando ao longo do processo os estados que conduzem à maximização referida, pode determinar-se a sequência de estados pretendida.
Com base nesta sequência podem deduzir-se outras equações de reestimação dos parâmetros dos HMM's - treino de Viterbi.

2.5. Classificação com HMM's

Para a utilização de HMM's em reconhecimento, é necessário transformar o padrão que se pretende classificar, numa sequência de observações. Em geral, o classificador é constituído por um HMM por cada classe de padrões. Os parâmetros destes HMM's são convenientemente estimados de forma a maximizar a probabilidade de cada um gerar as sequências de observações correspondentes aos padrões da classe que representam (fase de

treino). Para classificar um padrão, determina-se a probabilidade de cada modelo gerar a sequência de observações correspondente e escolhe-se a classe representada pelo modelo que exibe a maior probabilidade.

3. Reconhecimento Automático de Fala com HMM's

Foi desenvolvido um sistema de reconhecimento de palavras isoladas dependente do orador com 128 nomes próprios portugueses pronunciados por um único orador. O sinal de fala foi adquirido digitalmente a uma frequência de amostragem de 16KHz num ambiente sem ruído. Utilizaram-se modelos esquerda-direita [1] (numerando os estados da cadeia de Markov, as únicas probabilidades de transição não nulas são para o próprio estado e para o estado seguinte) treinados com o método de Viterbi com 5 repetições de cada palavra. Para testar o sistema usaram-se outras cinco repetições. A sequência de observações correspondente a cada repetição de cada palavra consiste em símbolos obtidos por quantificação vectorial [6] dos coeficientes de predição linear [7](LPC) de segmentos de 30 ms de sinal de fala espaçados entre si de 20 ms. A tabela seguinte mostra as taxas de reconhecimento obtidas para diversos números de estados, e diversos números de símbolos.

	Número de Estados								
	3			6			9		
Símbolos	treino	teste	total	treino	teste	total	treino	teste	total
16	99,2	80,8	90	99,8	86,4	93,1	99,8	90	94,9
32	100	86,7	93,4	100	90,9	95,5	100	93,4	96,7
64	100	89,7	94,8	100	93,6	96,8	100	94,1	97
128	100	94,7	97,3	100	96,1	98	100	95,9	98

Tabela 1 - Taxas de reconhecimento de palavras isoladas

4. Reconhecimento de Objectos com HMM's

Para a aplicação dos HMM's no reconhecimento de objectos bidimensionais, é necessário transformar o objecto presente na imagem numa sequência de observações. Neste estudo é utilizada a silhueta do objecto para a geração da sequência de observações [4]. Para esta geração procedeu-se a uma segmentação da imagem que contém o objecto, seguida de uma extracção do contorno e finalmente a caracterização deste.

Para a segmentação foi escolhido um algoritmo de limiar em que o nível de decisão é ponderado analisando o histograma da imagem [8].

A extracção do contorno é realizada com base na análise das mudanças na imagem binária [9] depois de aplicado um algoritmo de fecho morfógico [10], que permite suavizar o contorno do objecto e torna mais robusta a sua caracterização.

Para se obter a sequência de observações, o contorno exterior do objecto é dividido num número de segmentos com igual comprimento. Em seguida, cada segmento é aproximado por

um segmento de recta, unindo os seus pontos extremos. O conjunto de todos os segmentos forma um aproximação poligonal da silhueta do objecto. A partir da aproximação poligonal é gerada uma sequência de observações do tipo *chain code* [11], contendo o ângulo que cada troço faz com o troço anterior quantificado uniformemente. A figura 1 mostra como é calculado o ângulo entre dois segmentos de recta consecutivos da aproximação poligonal do objecto, e a observação gerada (a sombreado) para 8 níveis de quantificação. A figura 2 exemplifica algumas etapas da geração da sequência de observações.

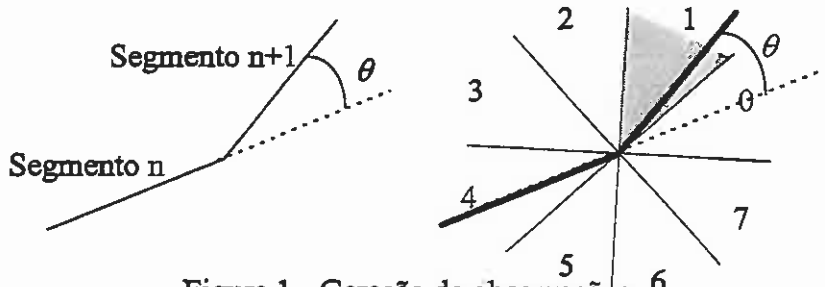
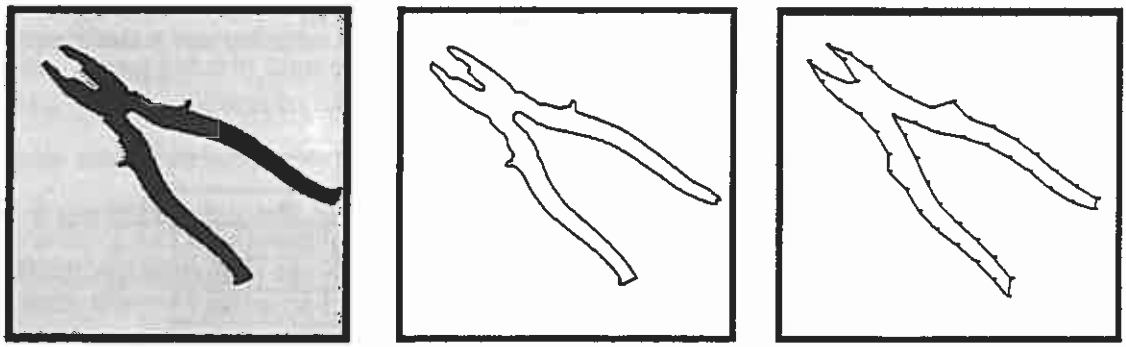


Figura 1 - Geração de observações.



a) b) c)

d) 0000000050000000100004012050000161000007600000003

Figura 2 - Etapas da geração da sequência de observações : a) imagem original, b) silhueta do objecto, c) aproximação poligonal com 50 segmentos, d) sequência de observações.

Foi desenvolvido um sistema de reconhecimento de 15 ferramentas e peças mecânicas. A base de dados experimental contém entre 34 e 62 imagens de cada objecto com diferentes translações, rotações, escalamentos e formas (no caso de objectos com partes móveis).

Para o reconhecimento foram utilizados duas topologias dos HMM's : 1) modelos totalmente ligados (todas as probabilidades de transição entre estados são não nulas) com 10 estados, 16 símbolos por estado e com sequências de 30 observações; 2) modelos esquerda-direita com 20 estados, 16 símbolos por estado e com sequências de 30 observações. Os modelos foram treinados com o treino de Baum-Welch e com 25 sequências de cada objecto. As restantes sequências de cada objecto, num total de 298, foram utilizadas para testar os modelos. Os resultados de reconhecimento encontram-se na tabela seguinte.

	Taxa de Reconhecimento
Classificador 1	99,3%
Classificador 2	100%

Tabela 2 - Taxas de reconhecimentos para os diferentes classificadores.

5. Conclusões

Neste artigo apresenta-se um resumo sobre modelos de Markov não-observáveis, salientando os resultados matemáticos que permitem a sua utilização, nomeadamente no que diz respeito ao treino dos modelos. A sua aplicação em duas áreas distintas como são o reconhecimento de fala e o reconhecimento de objectos em imagens e os bons resultados obtidos, permitem constatar a grande versatilidade que os HMM's proporcionam.

Bibliografia

[1] L.R. Rabiber and B. Juang, *Fundamental of Speech Recognition*, Prentice-Hall,1994.

[2] A. Serralheiro, *Metodologias probabilísticas no reconhecimento de palavras isoladas*, Tese de Doutoramento, 1990.

[3] Y. He, A. Kundu, 2-D shape classification using hidden Markov model, *IEEE Trans. On Pattern Anal. Mach. Intell*, Vol PAMI-13, nº 11 (Nov.), pp. 1172-1184, 1991.

[4] P. Jorge, *Reconhecimento de objectos bidimensionais baseado em modelos de Markov não-observáveis*, Tese de Mestrado, 1995.

[5] L. Baum, An inequaly and associated maximization technique in statistical estimation for probabilistic function of Markov processes. *Inequalities*, Vol. 3, pp 1-8, 1972.

[6] Y. Linde, A. Buzu e R. Gray, An algoritm for vector quantize design, *IEEE Trans. on Communication*, Vol. COM-28, nº1 (Jan.), pp. 84-95, 1980.

[7] J. Makhoul, Linear Prediction: A Tutorial Review, *Proc. of the IEEE*, Vol. 63, nº 4, April 1975.

[8] N. Otsu, A treshold selection method from gray-level histogram, *IEEE Trans. on System Man Cyber.*, Vol SMC-9, nº 1 (Jan.), pp. 63-66, 1979.

[9] R. Shalkoff, *Digital Image Processing and Computer Vision*, John Whiley & Sons, 1989.

[10] J. Serra, Introduction to mathematical morphology, *Comp. Vision, Graphics, and Image Processing*, 35, 3 (Set.), pp. 283-305, 1986.

[11] W. Pratt, *Digital Image Processing*, 2nd Edition, Whiley-Interscience, 1991.

Soluções numéricas das equações de Emden-Fowler e suas aplicações

Pedro Lima
Departamento de Matemática
Instituto Superior Técnico
Lisboa

1. Introdução

São conhecidas como equações de Emden-Fowler generalizadas [10] as equações diferenciais ordinárias de segunda ordem da seguinte forma:

$$y''(x) + c\,x^p\,y^q = 0, \qquad (1)$$

onde **c, p** e **q** são números reais, $x \geq 0$. Segundo alguns autores [14], também se consideram equações de Emden-Fowler generalizadas as que têm a forma

$$y''(x) + a(x)\,y^q = 0, \qquad (1a)$$

onde **a(x)** é uma função absolutamente contínua e não negativa.

Equações deste tipo surgem em diversos domínios da Mecânica e da Física, dando origem a diferentes problemas, consoante os valores das constantes e as condições iniciais ou de fronteira que são impostas à solução .

Historicamente, foi o astrofísico Emden quem primeiro se interessou por equações deste tipo, no princípio deste século. Ao estudar o problema do equilíbrio de uma esfera de gás, ele deduziu a seguinte equação diferencial ordinária:

$$y''(x) = -x^{1-n}\,y^n, \qquad (2)$$

onde **n** é um número positivo. O problema que o interessava consistia em determinar a solução da equação (2) que satisfizesse as condições iniciais

$$\lim_{x\to 0} y(x) = 0, \qquad \lim_{x\to 0} y'(x) = 1. \qquad (3)$$

A mais pequena raiz desta solução dá o raio duma esfera de gás em equilíbrio.

Mais tarde, equações do mesmo tipo voltariam a surgir nos modelos estatísticos da estrutura do átomo. Nestes modelos, a função que representa o potencial do campo eléctrico no seio do átomo satisfaz a chamada equação de Thomas-Fermi:

$$y''(x) = x^{-1/2}\,y^{3/2}, \qquad (4)$$

que também é um caso particular da equação (1). A solução do problema de Thomas-Fermi é uma função *y*, não negativa e contínua num certo intervalo (ou no semi-eixo positivo) e que satisfaz a equação (4) no interior desse intervalo. Existem três tipos de condições de fronteira com significado físico para a equação (4):

$$\lim_{x\to 0} y(x) = 1, \quad \lim_{x\to\infty} y(x) = 0 \qquad (4a)$$

no caso de um átomo neutro isolado;

$$\lim_{x\to 0} y(x) = 1, \; y(b) - by'(b) = 0, \qquad (4b)$$

no caso de um átomo neutro, com raio de Bohr igual a b, inserido numa estrutura cristalina;

$$\lim_{x\to 0} y(x) = 1, \; y(1) = 0, \qquad (4c)$$

no caso de um átomo ionizado.

Outros exemplos de aplicação das equações de Emden-Fowler generalizadas podem ser encontrados em Mecânica dos Fluidos [13], Física do Plasma [7] e no estudo de reacções químicas [6].

É interessante notar que, apesar do seu estudo datar de há tanto tempo e do seu aspecto ser simples, as equações de Emden-Fowler levantam uma série de problemas interessantes, alguns deles ainda por resolver, que continuam até hoje a atrair a atenção de muitos matemáticos e físicos.

Neste trabalho, vamos expor alguns resultados relacionados com a aproximação numérica de equações de Emden-Fowler, obtidos por vários autores. Na segunda parte, ocupar-nos-emos da equação de Thomas-Fermi e de algumas das suas generalizações, enquanto a terceira parte será dedicada a um problema de valores de fronteira com aplicação na mecânica dos fluidos.

2. Equação de Thomas-Fermi e suas generalizações

Consideremos a equação (1), com $c=-1$, $p<0$ e $q>1$. No caso particular de $p=-1/2$ e $q=3/2$, como já foi dito, temos a equação de Thomas-Fermi. Sabe-se que esta equação tem uma única solução que satisfaz as condições de fronteira (4c) . De acordo com Mooney [10], a equação (1) com as mesmas condições de fronteira continua a ter uma única solução se considerarmos qualquer valor de p superior a -2. Estes problemas com valores negativos de p têm em comum a propriedade de as respectivas soluções serem singulares em $x=0$. Como resulta da própria equação (1) , y'' é ilimitada quando $x\to 0$ e, se $p\leq -1$, o mesmo acontece com y'. Esta propriedade cria certas dificuldades à aproximação numérica da solução do problema (cuja solução exacta não é conhecida); contudo foi possível ultrapassar essas dificuldades e obter aproximações de grande precisão (ver [10],[11],[2] [3]). Vamos descrever em linhas gerais os métodos que foram utilizados nestes trabalhos para aproximar a solução.

Em primeiro lugar, a equação (1) é reduzida a uma sucessão de equações lineares através de um método iterativo. Se optarmos pelo método de Picard , de acordo com Mooney, devemos reescrever a equação (1) na forma

$$y''(x) - q\,x^p\,y(x) = x^p\,y^q(x) - q\,x^p\,y(x). \qquad (1b)$$

Se aplicarmos um esquema iterativo de ponto fixo à equação (1b) e representarmos cada iterada por y_ν , a equação das iteradas vai ter a forma

$$y_\nu''(x) - q\,x^p\,y_\nu(x) = x^p\,(y_{\nu-1}(x)^q - q\,y_{\nu-1}(x)), \quad \nu=1,2,\ldots \qquad (5)$$

Cada iterada deverá satisfazer as condições de fronteira correspondentes a (4a), (4b) ou (4c), conforme o caso. Embora muitos dos resultados sejam extensíveis aos outros casos, vamos deter-nos no caso do átomo ionizado, pelo que consideraremos as condições

$$y_\nu(0)=1 \; ; \; y_\nu(1)=0. \qquad (5a)$$

Mooney provou que, partindo da aproximação inicial $y_0(x)\equiv 0$, se obtem uma sucessão de iteradas tais que

$$y_0(x) \le y_1(x) \le \ldots \le y_\nu(x) \le y(x) \; , \quad 0 \le x \le 1$$

e esta sucessão converge uniformemente para y (solução exacta do problema não-linear) em [0,1].

Por outro lado, se partirmos da aproximação inicial $y_0(x) = 1 - x$, a sucessão das iteradas satisfaz

$$y_0(x) \ge y_1(x) \ge \ldots \ge y_\nu(x) \ge y(x) \; , \quad 0 \le x \le 1$$

verificando-se igualmente convergência uniforme para a solução exacta. Este método permite-nos, portanto, obter aproximações tão exactas quanto quisermos da solução, assim como enquadrá-la entre um minorante e um majorante.

Em alternativa, a solução da equação (1) também pode ser aproximada pelo método de Newton. Neste caso, a equação das iteradas tem a forma

$$y_\nu''(x) - q\, x^p\, y_{\nu-1}(x)^{q-1}\, y_\nu(x) = x^p\,(1-q)\,y_{\nu-1}(x)^q, \quad \nu=1,2,\ldots \qquad (6)$$

com as condições de fronteira (5a). Partindo da aproximação inicial $y_0(x) = 1 - x$, obtém-se uma sucessão decrescente de funções que converge uniformemente para y(x). Como é do conhecimento geral, o método Newton tem convergência quadrática, (em contraste com o método de Picard que tem simplesmente convergência linear), o que significa, na prática, que usando o esquema (6) se consegue obter a aproximação desejada com um menor número de iterações.

Uma vez reduzido o problema não-linear (1) a uma sucessão de problemas lineares, pelo método de Picard ou pelo de Newton, torna-se necessário escolher um método numérico adequado para aproximar as soluções dos problemas lineares (5) ou (6), já que estes também não se podem resolver analiticamente. Um dos métodos mais simples e eficientes para resolver este problema é o método das diferenças finitas, que foi aplicado, por exemplo, em [10] e [2] . A principal dificuldade , neste caso, resulta da descontinuidade da segunda derivada em x=0 , o que diminui significativamente a precisão do método. Com efeito, sendo h o passo da rede utilizada, o esquema de diferenças finitas mais comum (com aproximação da segunda derivada por diferenças centrais) garantiria, num problema sem singularidades, uma aproximação com erro $O(h^2)$. No entanto, na presença de singularidade, o erro passa a ser da ordem de h^{p+2}, conforme foi estudado detalhadamente nos trabalhos acima citados. Para conseguir que o erro de discretização fosse da ordem de $O(h^2)$, Mooney introduziu, em [10] e [11], uma modificação do método das diferenças finitas que entra em conta com a singularidade do problema considerado. Em [2], para ultrapassar esta dificuldade, propusemos um método alternativo que consiste em utilizar o método das diferenças

finitas comum e acelerar a convergência dos resultados obtidos através de métodos de extrapolação. Para isso, foi necessário deduzir desenvolvimentos assimptóticos do erro de discretização, com base nos quais se pode aplicar o algoritmo-E de Brezinski [1]. Essa abordagem permitiu-nos obter aproximações com cerca de 10 algarismos significativos, para a equação de Thomas-Fermi, e com cerca de 8, para as suas generalizações (com p=-1 e p=-1.25).

No caso de valores de p próximos de -2, no entanto, as técnicas acima descritas não permitem obter uma precisão satisfatória . Estes casos foram estudados por Mooney em [12] e por nós em [3]. Neste último trabalho, foi analisado o comportamento assimptótico das iteradas de Picard e da solução exacta da equação(1). Em particular, conclui-se que, para valores de p, entre -2 e -1, a solução da equação (1) que satisfaz as condições de fronteira (4c) , quando x é próximo de 0, tem o comportamento assimptótico

$$y(x) \sim 1 + ax^{p+2} + o(x^{p+2}) \quad (a - \text{constante}),$$

donde resulta que a primeira derivada tende para infinito junto da origem. Este facto, naturalmente, faz com que a aproximação pelo método das diferenças finitas, para tais valores de p, se torne insatisfatória. Com base nesta análise, no trabalho citado foi proposta a aplicação de uma substituição de variável às equações (5) e (6) e a discretização das equações na nova variável. A substituição de variável proposta foi

$$t = x^{p+2},$$

no caso de p ser irracional, e

$$t = x^{1/n},$$

no caso de $p = -m/n$. A vantagem destas substituições consiste em transformar as soluções da equação (1) da equação (5) em funções que são continuamente diferenciáveis em $x=0$, apresentando, portanto, um comportamento regular em todo o segmento [0,1]. Os resultados apresentados em [3] confirmam que esta substituição de variável permite melhorar drasticamente a precisão da aproximação numérica.

Na fig.1 pode ver-se o gráfico da solução aproximada da equação (1) com as condições de fronteira (4c), no caso de p=-1.5, q=2.5, bem como algumas das iteradas de Picard correspondentes. A fig. 2 ilustra a aplicação da substituição de variável no caso do problema considerado na fig.1. Como se pode ver pelos gráficos das funções (que são as transformadas das funções da fig.1 quando é aplicada a substituição $t = x^{1/2}$) o seu comportamento torna-se regular junto da origem.

Title:
Clipboard
Creator:
(Mathematica Microsoft Windows 3.0)
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Fig.1 Reprentação gráfica das iteradas de Picard y_1, y_2 e da solução y da equação (1) no caso de c=-1, p=-1.5 , q=2.5. Tomou-se como aproximação inicial $y_0 \equiv 0$.

Fig.2 . Gráficos das funções da fig.1 quando é aplicada a substituição de variável $t= x^{1/2}$.

A utilização da substituição de variável permitiu aumentar substancialmente a precisão dos resultados. No caso de p=-1.7, por exemplo, o número de algarismos significativos passa de 4 para cerca de 12.

3.Problema singular da mecânica dos fluidos não-newtonianos.

Como segundo exemplo de aplicação das equações de Emden-Fowler, vamos expor alguns resultados referentes a um problema de valores de fonteira que surge na mecânica de fluidos. Mais precisamente, considere-se um escoamento sobre uma superfície plana impermeável de um fluido incompressível que satisfaz a lei potencial

$$\tau= k(\partial u / \partial y)^n ,$$

onde τ é a tensão de cisalhamento, u é a componente da velocidade segundo o eixo dos x, k é uma constante de e n é um parâmetro característico do fluido. Conforme o valor de n, o fluido diz-se pseudodplástico (quando $n<1$), dilatante (quando $n>1$) ou newtoniano (quando $n=1$). A equação da camada de fronteira num escoamento deste tipo conduz, após algumas transformações [8] , ao problema de determinar uma solução positiva da equação

$$y''(x) =1/q \; x\, y^{q}, \quad 0 < x <1, \tag{7}$$

onde $q=-1/n$, que satisfaça as condições

$$y'(0)= 0 , \; y(1)=0.$$

Facilmente se vê que a equação (7) é um caso particular da equação (1), desta vez com uma singularidade em $x=1$, já que y se anula neste ponto e q é negativo. A existência e unicidade de solução deste problema foi demonstrada por Luning e Perry [8], para o caso de $-1 < q < 0$, e por Nachman e Callegari [13], para o caso de $q<-1$. Num trabalho recente [4], analisámos este problema e tentámos obter aproximações numéricas utilizando métodos semelhantes aos que foram aplicados no caso de outras equações de Emden-Fowler.

Tal como no caso anterior, começámos por reduzir o problema a uma sucessão de equações lineares. Com este fim, propusemo-nos utilizar igualmente os esquemas iterativos de Picard e Newton. Neste caso, porém, é necessário prestar especial

atenção à escolha das aproximações iniciais, já que a hipótese de $y_0(x)=0$ está excluída por q ser negativo, e a função $y_0(x)=1-x$ também não garante a convergência.

Detivemo-nos portanto na determinação de sub-soluções e supersoluções da equação (7), como passo inicial para a resolução do problema. Seguindo Mooney [9], chamaremos *subsolução* do problema (7), com as condições de fronteira (7a), a uma função da classe $C^2(]0,1[)\cap C([0,1])\cap C^1([0,1[)$, tal que

$$-y''(x) + 1/q\ x\, y^q \leq 0, \quad 0 < x < 1,$$
$$y'(0) \leq 0\ ,\ y(1)=0. \tag{8}$$

Invertendo os sinais das desigualdades (8), obtém-se a definição de uma *supersolução*.

Após uma análise do problema, verificámos que, para qualquer valor de q, tal que $q<-1$, existem sub-soluções e supersoluções do problema (7) com a forma geral

$$y(x) = B\,(1 - x^3)^{\gamma}, \tag{9}$$

onde $\gamma = 2/(1-q)$ e B é uma constante real positiva. Assim, para $q\leq -5$, prova-se que uma função da forma (9) é uma sub-solução de (7) se

$$B \leq (9\gamma(\gamma-1)q)^{-1/(1-q)} \tag{10a}$$

e é uma supersolução se

$$B \geq (-6\gamma q)^{-1/(1-q)}\ . \tag{10b}$$

Por outro lado, no caso de $-1 > q \geq -5$, uma função da forma (9) é uma sub-solução de (7) se

$$B \leq (-6\gamma q)^{-1/(1-q)} \tag{11a}$$

e é uma supersolução se

$$B \geq (9\gamma(\gamma-1)q)^{-1/(1-q)}\ . \tag{11b}$$

No caso de $q=-5$ $(\gamma = 1/3)$, verifica-se que $(-6\gamma q)^{-1/(1-q)} = (9\gamma(\gamma-1)q)^{-1/(1-q)} = 10^{-1/6}$. Por conseguinte, a função

$$y(x) = 10^{-1/6}\,(1 - x^3)^{1/3}$$

é simultaneamente uma sub-solução e uma supersolução do problema considerado. Substituindo na equação, verifica-se que se trata da solução exacta. É este o único valor de q para o qual é conhecida a solução exacta.

No que diz respeito ao caso de $0>q>-1$, consegue-se provar que uma função da forma

$$y(x) = B\,(1 - x^3)$$

é uma subsolução de (7) se

$$B \leq (-6\gamma q)^{-1/(1-q)}$$

mas não foi possível determinar supersoluções da mesma forma.

O conhecimento de uma subsolução da equação (7) permitiu-nos generalizar a teoria de Mooney [9] para o caso desta equação, quando q>-1, e provar que o método de Newton, tomando essa subsolução como aproximação inicial , gera uma sucessão crescente de funções que converge uniformemente para a solução exacta.

Neste caso, a equação das iteradas do método de Newton tem a forma

$$y_\nu''(x) - x^p y_{\nu-1}(x)^{q-1} y_\nu(x) = 1/q \; x\,(1-q) y_{\nu-1}(x)^q, \quad \nu=1,2,\ldots \qquad (12)$$

e as condições de fronteira a aplicar são

$$y_\nu'(0) = 0 \,, \; y_\nu(1) = 0. \qquad (12a)$$

Também se pode aplicar um esquema iterativo do tipo de Picard que, para este caso, terá a forma

$$y_\nu''(x) - x^p \underline{y}(x)^{q-1} y_\nu(x) = 1/q \; x\,(y_{\nu-1}(x)^q - q\,\underline{y}(x)^{q-1} y_\nu(x)), \qquad (13)$$

onde $\underline{y}(x)$ representa uma subsolução da equação (7).

Para os valores de *q*, inferiores a -1, uma vez determinada uma subsolução e uma supersolução (usando as desigualdades (10a) e (10b) ou (11a) e (11b), conforme o caso), pode utilizar-se a teoria desenvolvida por Mooney e generalizá-la de modo a provar que a solução exacta está enquadrada entre aquelas (tal como, no caso da equação de Thomas-Fermi, a solução exacta está enquadrada entre a função nula e a função *1-x*). Além disso, é possível provar que os métodos de Newton e Picard, definidos respectivamente pelas equações (12) e (13) , se tomarmos uma subsolução como aproximação inicial, geram sucessões crescentes de funções que convergem uniformemente para a solução. A demonstração destas afirmações, para o caso de $q<-1$, ainda não está terminada, embora os resultados numéricos obtidos indiquem que a aplicação dos métodos com estes valores de *q* continue a ser válida.

Para a discretização das equações lineares (12) e (13), usámos esquemas de diferenças finitas, análogos aos que foram utilizados para as equações (5) e (6). Como seria de esperar, devido à presença da singularidade em $x=1$, a precisão das aproximações numéricas é baixa. Mais precisamente, estimativas a posteriori mostraram que, para valores de *q* situados entre -1 e 0, o erro de discretização é da ordem de h^{q+2}, enquanto que, para $q<-1$, é aproximadamente da ordem de *h*.

Tal como no caso das equações consideradas na primeira parte, é possível melhorar a aproximação numérica das equações (12) e (13) recorrendo a uma substituição de variável. Num trabalho recente [5], propusemos, no caso de q<-1, a aplicação de uma substituição de variável do tipo $t = (1 - x)^{1/(1-q)}$,inspirada na forma das sub-soluções e supersoluções.

Tal como as substituições propostas para as outras equações, acreditamos (nao foi ainda provado) que esta substituição tem a propriedade de converter as soluções das equações (12) e (13) (e, por conseguinte, da equação (7)) em funções continuamente diferenciáveis em [0,1].

Para testar os métodos propostos, foram realizadas várias experiências numéricas. Em particular, no caso de q=-5, em que a solução exacta é conhecida, foi possível determinar o erro das aproximações e tirar conclusões quanto à sua precisão. Assim, chegámos às seguintes conclusões:

a) os resultados obtidos quando se aplica a substituição de variável têm um erro da ordem de h^2 (sem a substituição, o erro é da ordem de h);
b) se obtivermos aproximações com diferentes passos (usando a substituição de variável) e aplicarmos a extrapolação de Richardson, podemos obter resultados de alta precisão (até 10-11 algarismos significativos) .

Na fig.3, estão representadas graficamente algumas iteradas do método de Newton e a solução exacta no caso de $q=-5$. Estes gráficos evidenciam a singularidade das funções representadas em $x=1$. Quando é aplicada a substituição de variável $t = (1-x)^{1/6}$, as funções correspondentes adquirem um comportamenro regular em todo o intervalo [0,1] , como se pode ver na fig. 4.

Title:
Clipboard
Creator:
(Mathematica Microsoft Windows 3.0)
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Fig.3 . Gráficos da solução exacta e das duas primeiras iteradas de Newton da equação (7) no caso de q=-5. A aproximação inicial neste caso é $y_0(x) = 0.5\,(1 - x^3)^{1/3}$.

Title:
Clipboard
Creator:
(Mathematica Microsoft Windows 3.0)
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Fig.4. Quando é aplicada a substituição de variável $t=(1-x)^{1/6}$, as funções representadas na fig.3 adquirem esta forma.

4. Conclusões

Os resultados até agora obtidos levam-nos a concluir que as técnicas de cálculo aqui discutidas constituem uma ferramenta eficaz para o tratamento numérico das equações de Emden-Fowler, já que permitem obter resultados de alta precisão sem grande esforço computacional. De notar que todos os cálculos podem ser efectuados num computador pessoal de capacidade média em poucos segundos. Assim, tencionamos continuar a aplicá-las na resolução de novos problemas.

ERRATA

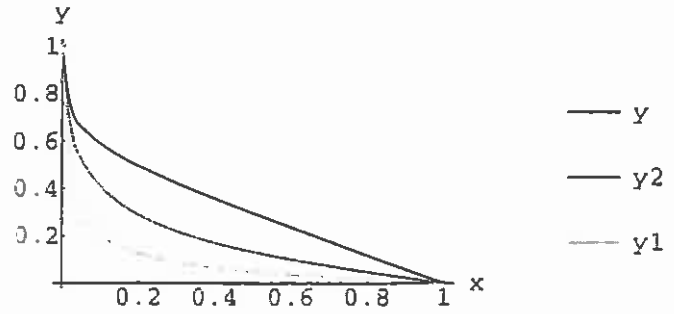


Fig.1 Reprentação gráfica das iteradas de Picard y_1, y_2 e da solução y da equação (1) no caso de c=-1. p=-1.5 . q=2.5. Tomou-se como aproximação inicial $y_0 \equiv 0$.

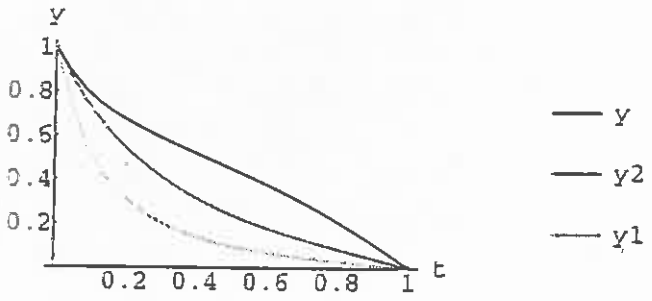


Fig.2 . Gráficos das funções da fig.1 quando é aplicada a substituição de variável $t = x^{1/2}$.

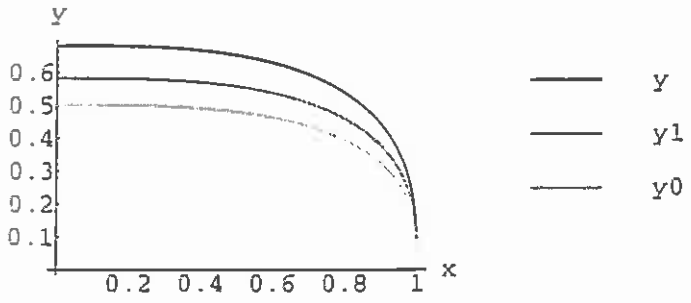


Fig.3 . Gráficos da solução exacta e das duas primeiras iteradas de Newton da equação (7) no caso de q=-5. A aproximação inicial neste caso é $y_0(x) = 0.5\ (1 - x^3)^{1/3}$.

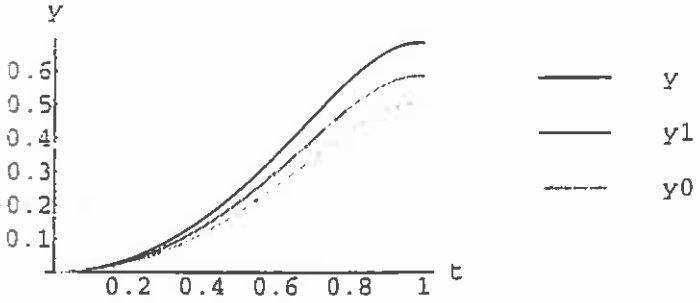


Fig.4. Quando é aplicada a substituição de variável $t=(1-x)^{1/3}$, as funções representadas na fig.3 adquirem esta forma.

Bibliografia:

[1] C.Brezinski , A general extrapolation algorithm, Numer. Math. 35 (1980),175-187.

[2] P.M.Lima , Numerical methods and asymptotic error expansions for the Emden-Fowler equations, J. Comp. Appl. Math. 70 (1996), 245-266.

[3] P.M.Lima and M.P.Carpentier, Asymptotic expansions and numerical approximation of non-linear degenerate boundary-value problems, Appl. Num. Math. (a publicar).

[4] P.M.Lima and M.P.Carpentier, Iterative methods for a nonlinear singular boundary-value problem, J. Comp. Appl. Math. (a publicar)

[5] P.M.Lima and M.P.Carpentier, Numerical solution of a singular boundary-value problem in non-newtonian fluid mechanics, Comp. Phys. Commun. (a publicar)

[6] C.D. Luning and W.L.Perry, A monotone iterative technique for solution of p-th order ($p<0$) reaction-diffusion problems in permeable catalysis, J.Comp. Chem. 5 (1984) 353-357.

[7] C.D. Luning and W.L.Perry, Shape functions for separable solutions to cross-field diffusion problems, J. Math. Phys. 25 (1984) 2374-2376.

[8] C.D. Luning and W.L.Perry, An iterative method for solution of a boundary value problem in non-newtonian fluid flow.J. Non-Newtonian Fluid Mechanics, 15 (1984) 145-154.

[9]J.W. Mooney, A unified appproach to the solution of certain classes of nonlinear boundary value problems using monotone iterations, Nonlinear Analysis, TM&A, 3 (1979) 449-465.

[10] J.W. Mooney, Numerical schemes for degenerate boundary-value problems. J. Phys A 26 (1993), L413-L421.

[11] J.W. Mooney, Solution of a Thomas-Fermi problem using linear approximants. Comp: Phys. Comm. 76 (1993) 51-57.

[12] J.W. Mooney, Solution of Emden-type problems using accurate, efficient discretization schemes, Comp. Phys. Comm. 83 (1994) 245-254.

[13] A. Nachman and A. Callegari, A nonlinear singular boundary-value problem in the theory of pseudoplastic fluids, SIAM J. Appl. Math., 38 (1980) 275-281.

[14] J.W.Wong, On the generalizaed Emden-Fowler equation, SIAM review 17 (1975), 339-360.

Analogia entre Sinais e Vectores

Isabel Milho Fernando Sousa

Centro de Cálculo, ISEL

DEEC, ISEL

isabel@cc.isel.pt fsousa@cc.isel.pt

Resumo

Este artigo propõe-se ilustrar a analogia entre sinais e vectores aplicada na resolução e compreensão de problemas em áreas como a análise de sinais e o desenho de sistemas de comunicação. Desta analogia resulta a reinterpretação (aplicada) das operações vectoriais, nomeadamente: produto interno, norma, desigualdades, ortogonalidade, projecções de vectores, base ortogonal, procedimento de Gram-Schmidt. Evidenciam-se as vantagens desta perspectiva na análise de problemas tipo.

1 Introdução

Através da descrição de sinais como vectores num espaço multi-dimensional, as operações e relações vectoriais são aplicadas na resolução de problemas em áreas como a análise de sinais e o desenho de sistemas de comunicação. São exemplos de aplicação: compreensão da série de Fourier, extracção de características, compressão de dados, representação de sinais com base num conjunto reduzido de sinais, interpretação da amostragem, medidas de semelhança entre sinais, detecção de sinais na presença de ruído, funções de Walsh.

A aplicação desta ferramenta consiste na reinterpretação (aplicada) das operações vectoriais, nomeadamente: produto interno (medida de semelhança entre dois sinais), norma (energia ou potência, conforme se trate de sinal de energia ou de potência), desigualdades (relações de energia ou potência entre sinais), ortogonalidade (quando a medida de semelhança entre dois sinais é nula), projecções de vectores (representação de sinais segundo outros), base ortogonal de vectores (base ortogonal de sinais), procedimento de Gram-Schmidt (obtenção da base ortonormada para representar quaisquer M sinais de energia).

Este artigo propõe-se ilustrar esta analogia (entre Espaços Vectoriais e Espaços de Sinais) e evidenciar as vantagens desta perspectiva na análise de problemas tipo. Na secção 2 descrevem-se de modo informal as operações e relações dos Espaços Vectoriais. Na secção seguinte ilustram-se alguns exemplos de aplicação destas relações e operações aos sinais, salientando-se a simplicidade desta abordagem. Finalmente na secção 4 apresentam-se de forma conclusiva as vantagens desta perspectiva na área de análise de sinais.

2 Espaços Vectoriais

A apresentação da teoria de espaços vectoriais é feita de modo informal e compacto[1]. No entanto, considera-se essencial esta descrição para maior simplicidade e compreensão da exposição na secção seguinte (Aplicações de Espaços de Sinais).

Um espaço vectorial (ou espaço linear) S é formado por um conjunto de elementos designados por vectores. A partir de quaisquer dois vectores v e w e dois escalares α e β forma-se outro vector $z=\alpha v+\beta w$ que pertence também ao espaço vectorial S. Por outras palavras, o conjunto de todos os elementos de S é fechado sobre combinação linear. As operações de adição e multiplicação em S são definidas de modo usual existindo o vector nulo θ tal que $v+\theta=v$ e $\theta\cdot v=\theta$.

2.1 Produto Interno, (v,w)

O produto interno, simbolizado por (v,w), é um número complexo associado a um par de vectores v e w pertencentes a S, com as seguintes propriedades

$$(v,\theta)=0 \tag{1}$$

$$(v,w)=(w,v)^* \tag{2}$$

$$(\alpha v,\beta w)=\alpha\beta^*(v,w) \tag{3}$$

$$(v+w,x+y)=(v,x)+(v,y)+(w,x)+(w,y) \tag{4}$$

O valor do produto interno representa uma medida de semelhança entre vectores, nomeadamente o ângulo relativo.

2.2 Norma, $\|v\|$

A norma de qualquer vector v é um valor real definido por

$$\|v\|=(v,v)^{1/2} \tag{5}$$

Representa a medida do seu comprimento e verifica as seguintes propriedades:

$$\|v\|\geq 0 \tag{6}$$

$$\|v\|=0 \quad \text{sse} \quad v=\theta \tag{7}$$

$$\|\alpha v\|=|\alpha|\cdot\|v\| \tag{8}$$

[1] Sugere-se o texto de Apostol [1] para maior rigor e detalhe.

2.3 Desigualdades e Ortogonalidade

Usando as propriedades do produto interno e da norma de vectores derivam-se várias relações importantes [1], [2].

2.3.1 Desigualdade de Schwarz's

$$|(v,w)| \leq \|v\| \, \|w\| \tag{9}$$

Relaciona o produto interno entre dois vectores com o produto das respectivas normas. A igualdade verifica-se para o caso de v e w serem colineares ($v = \alpha w$).

2.3.2 Teorema de Pitágoras e Ortogonalidade

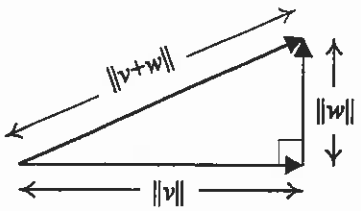


Figura 1 – Representação vectorial de dois vectores v e w ortogonais.

Na Figura 1, os vectores v e w são ortogonais, ou perpendiculares. Como o produto interno (v,w) entre dois vectores ortogonais é nulo, verifica-se o Teorema de Pitágoras. Ou seja,

$$\|v+w\|^2 = \|v\|^2 + \|w\|^2 \quad \text{se } (v,w) = 0 \tag{10}$$

2.4 Projecção Vectorial

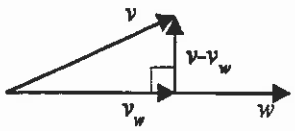


Figura 2 – Projecção vectorial de v sobre w.

Na Figura 2, ilustra-se a projecção do vector v sobre o vector w. O vector que resulta da projecção ortogonal de v sobre w designa-se por v_w e é definido pelas propriedades $v_w = \alpha v$ e $(v - v_w, w) = 0$, tal que

$$\text{proj}_w v = v_w = \frac{(v,w)}{\|w\|^2} w \tag{11}$$

A norma do vector projecção v_w é nula quando os vectores v e w são perpendiculares e é máxima quando são colineares (proporcionais). Na Figura 2, note que $v - v_w$ é ortogonal a w (a

sua semelhança com w é nula) e que $\|v - v_w\|$ é distância mais curta entre a extremidade do vector v e qualquer ponto ao longo do vector w.

2.5 Base vectorial

O conceito de base vectorial realça a interpretação geométrica de um espaço vectorial. Seja S um espaço vectorial que inclui um conjunto de K vectores linearmente independentes ϕ_k, com k=1, 2, ..., K, tal que qualquer vector v pertencente ao espaço S é expresso da seguinte forma

$$v = \sum_{k=1}^{K} \alpha_k \cdot \phi_k \tag{12}$$

Deste modo diz-se que o espaço S tem K dimensões e os vectores ϕ_k formam uma base vectorial. Os escalares α_k designam-se por coordenadas de v na base ϕ e são determinados segundo v e ϕ_k, tal que

$$\alpha_k = (v, \phi_k) \tag{13}$$

Para que a base ϕ_k seja ortonormada tem de verificar a condição

$$(\phi_k, \phi_m) = \begin{cases} 1 & m = k \\ 0 & m \neq k \end{cases} \tag{14}$$

que garante-se que os vectores ϕ_k são ortogonais e de norma unitária.

2.5.1 Procedimento de Gram-Schmidt

Para gerar uma base ortonormada de vectores ϕ_k que represente um determinado conjunto de vectores segue-se o procedimento sequencial de Gram-Schmidt. Segundo este, a base ortonormada que representa o conjunto de vectores z_k, com k=1, 2, ..., K, é formada tal que

$$\phi_k = \frac{g_k}{\|g_k\|} \tag{15a}$$

onde

$$\begin{aligned} g_1 &= z_1 \\ g_k &= z_k - \sum_{m=1}^{k-1} (z_k, \phi_m) \cdot \phi_m \qquad 2 \leq k \leq K \end{aligned} \tag{15b}$$

Verifique que $(z_k, \phi_m) \cdot \phi_m$, em (15b), é precisamente a projecção de z_k sobre ϕ_m, dado que $\|\phi_m\|^2 = 1$. O procedimento está ilustrado na Figura 3, onde se observa que g_k é ortogonal a ϕ_1, ϕ_2, ..., ϕ_{k-1} com k=2, 3; note que a coordenada α_{km} representa o valor de (z_k, ϕ_m) em (15b).

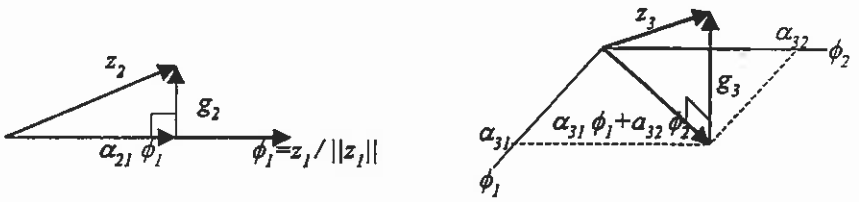


Figura 3 – Geração de vectores ortonormados segundo o procedimento de Gram-Schmidt.

Na geração da base ortonormada segundo este procedimento, se os vectores z_k não forem linearmente independentes, então um ou mais vectores ϕ_k serão nulos e a dimensão da base será menor que *K*.

2.5.2 *Produto Interno e Norma*

O produto interno entre dois vectores z_i e z_j definidos pelas suas coordenadas numa base ortonormada vem igual a

$$\left(z_i, z_j\right)=\left(\sum_{k=1}^{K}\alpha_{ik}\cdot\phi_k \quad , \quad \sum_{l=1}^{K}\alpha_{jl}\cdot\phi_l\right)=\sum_{k=1}^{K}\alpha_{ik}\cdot\alpha_{jk}^{*} \tag{16a}$$

Fazendo *j=i* , obtem-se a norma de z_i

$$\|z_i\|^2=\left(z_i, z_j\right)=\sum_{k=1}^{K}|\alpha_{ik}|^2 \tag{16b}$$

que exprime o Teorema de Pitágoras de dimensão *K*.

3 Aplicações de Espaços de Sinais

Através da descrição de sinais como vectores, as operações e relações vectoriais são aplicadas na resolução de problemas em áreas como a análise de sinais e o desenho de sistemas de comunicação. A ligação entre vectores e sinais é estabelecida através da definição adequada do produto interno (depois de ser identificado o conjunto de sinais, fechado sobre combinação linear). Esta ligação permite a reinterpretação das operações e relações vectoriais, nomeadamente: produto interno (medida de semelhança entre dois sinais), norma (energia ou potência, conforme se trate de sinal de energia ou de potência), desigualdades (relações de energia ou potência entre sinais), ortogonalidade (quando a medida de semelhança entre dois sinais é nula), projecções de vectores (representação de sinais segundo outros), base ortogonal de vectores (base ortogonal de sinais), procedimento de Gram-Schmidt (obtenção da base ortonormada para representar quaisquer M sinais de energia).

Para iniciar a apresentação de exemplos de aplicação de Espaços de Sinais começa-se por definir a ligação (produto interno) para as classes de sinais de energia e de potência[2]. De seguida apresenta-se a classe de sinais de potência descrita segundo a série de Fourier. Finalmente, referem-se os exemplos seguintes: transformada de Fourier, descritores de Fourier para extracção de características, compressão de dados, representação de sinais com base num conjunto reduzido de sinais, interpretação da amostragem, medidas de semelhança entre sinais, detecção de sinais na presença de ruído, funções de Walsh.

3.1 Sinais de Energia

O conjunto de todos os sinais de energia define um espaço de sinais. A definição de produto interno entre dois sinais de energia vem igual a

$$(v,w)=\int_{-\infty}^{\infty} v(t)\cdot w^{*}(t)\,dt \tag{17}$$

Esta definição estabelece a ligação dos sinais de energia aos vectores. Tal como no espaço vectorial, este escalar representa uma medida de semelhança entre dois sinais. Veja-se que a definição em (17) verifica as propriedades descritas na subsecção 2.1.

Deste modo, com a definição do produto interno, deduzem-se todas as operações e relações da secção 2. Para definir a norma de v faz-se w igual v em (17) tal que

$$\|v\|^2=(v,v)=\int_{-\infty}^{\infty} v(t)\cdot v^{*}(t)\,dt=\int_{-\infty}^{\infty}|v(t)|^2\,dt=E_v \tag{18}$$

onde se verifica que o valor quadrático da norma de um sinal de energia é igual ao valor da sua energia. De salientar o Teorema de Pitágoras em (10) e (16b) aplicado aos sinais de energia em (19): a sobreposição de sinais implica a sobreposição das energias quando se verifica a ortogonalidade.

$$E_{v+w}=E_v+E_w \qquad \text{se } (v,w)=0 \tag{19}$$

3.2 Sinais de Potência

O conjunto de sinais de potência periódicos em T_0 define outro espaço de sinais. A definição de produto interno entre dois sinais de potência vem igual a

$$(v,w)=\frac{1}{T_0}\int_{T_0} v(t)\cdot w^{*}(t)\,dt \tag{20}$$

De igual modo para os sinais de potência, define-se a norma de v fazendo, em (20), w igual

[2] Em vários autores se encontra a definição de sinais de energia e de potência [2], [4], [6].

a v tal que

$$\|v\|^2 = (v,v) = \frac{1}{T_0}\int_{T_0} v(t)\cdot v^*(t)\,dt = \frac{1}{T_0}\int_{T_0} |v(t)|^2\,dt = P_v \tag{21}$$

onde se constata que o valor quadrático da norma de um sinal de potência é igual ao valor da sua potência.

Aos sinais de potência ortogonais também se aplica o Teorema de Pitágoras de modo que

$$P_{v+w} = P_v + P_w \qquad \text{se } (v,w) = 0 \tag{22}$$

3.3 Série de Fourier

A Série de Fourier que representa os sinais de potência periódicos em T_0 pode ser facilmente compreendida usando a ferramenta vectorial. Considere-se a base ortonormada de dimensão igual a $2K+1$

$$\phi_k(t) = e^{\frac{j2\pi kt}{T_0}} \qquad \text{com } k = 0,\pm 1,\pm 2,...,\pm K \tag{23}$$

Considerando o sinal $\hat{v}(t)$ como a projecção de $v(t)$ sobre a base $\phi_k(t)$, vem que

$$\hat{v}(t) = \sum_{k=-K}^{K} \alpha_k \cdot \phi_k(t) = \sum_{k=-K}^{K} \alpha_k \cdot e^{\frac{j2\pi kt}{T_0}} \tag{24a}$$

onde

$$\alpha_k = (v,\phi_k) = \frac{1}{T_0}\int_{T_0} v(t)\cdot e^{\frac{-j2\pi kt}{T_0}}\,dt \tag{24b}$$

Observe-se em (24a) que $\hat{v}(t)$ representa os primeiros $2K+1$ termos da série de Fourier e as coordenadas α_k são os coeficientes da série de Fourier. Fazendo $K = \infty$ em (24a) tem-se $\hat{v}(t) = v(t)$, que é a forma de $v(t)$ descrito na série de Fourier, em (25).

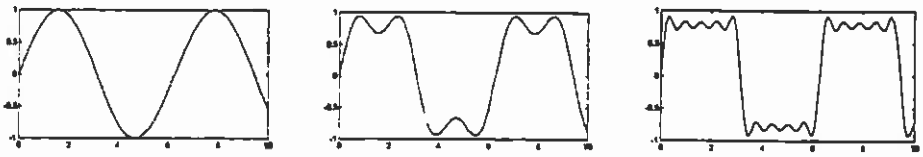
$$v(t) = \sum_{k=-\infty}^{\infty} \alpha_k \cdot e^{\frac{j2\pi kt}{T_0}} \tag{25}$$

Deste modo interpreta-se a série de Fourier como sendo a projecção do sinal $v(t)$ na base ϕ_k de dimensão infinita mas contável.

Os coeficientes de Fourier significam as coordenadas do sinal $v(t)$ sobre cada sinal $\phi_k(t)$ da base; fisicamente, cada coordenada tem significado espectral correspondente a uma determinada frequência múltipla da fundamental $f_0 = 1/T_0$, dado que, desenvolvendo (23), vem

$$\phi_k(t) = e^{\frac{j2\pi kt}{T_0}} = e^{j2\pi k f_0 t} = \cos(2\pi k f_0 t) + j\,\mathrm{sen}(2\pi k f_0 t) \tag{26}$$

Veja-se o exemplo da Figura 4 que ilustra a geração da onda quadrada (sinal periódico de potência) a partir da soma sucessiva de sinusóides.



(a) (b) (c)

Figura 4 – Geração da onda quadrada a partir da soma sucessiva de sinusóides, correspondentes aos primeiros $2K+1$ coeficientes da série de Fourier. (a) K=1; (b) K=4; (c) K=10.

Observe-se a semelhança do sinal com a onda quadrada à medida que K aumenta: o sinal da Figura 4(c) foi gerado com os primeiros 21 termos da série de Fourier da onda quadrada respectiva. De salientar que, quando o sinal $v(t)$ é real, os coeficientes de Fourier têm simetria complexa e $\hat{v}(t)$ definido em (24a) vem expresso em função da soma de sinusóides, na forma

$$\hat{v}(t) = \sum_{k=-K}^{K} \alpha_k \cdot \phi_k(t) = \alpha_0 + \sum_{k=1}^{K} 2|\alpha_k| \cdot \cos(2\pi k f_0 t + \arg \alpha_k) \tag{27}$$

Ainda em relação à série de Fourier, cada coeficiente de Fourier (coordenada α_k) tem significado físico em termos de potência, tal que $|\alpha_k|^2$ representa a distribuição de potência ao longo das diferentes frequências (múltiplas da fundamental f_0). Como a potência tem analogia com a norma então, usando (16b), tem-se

$$P_v = \|v\|^2 = \sum_{k=1}^{K} |\alpha_k|^2 \tag{28}$$

que exprime o Teorema de potência de Parseval.

Para ilustrarmos o significado físico dos coeficientes α_k considere-se $v(t)$ na Figura 5.

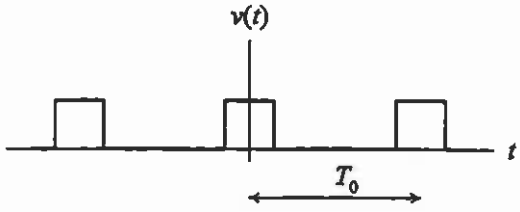


Figura 5 – Onda quadrada de frequência $f_0 = 1/T_0$.

Os coeficientes de Fourier (ou as coordenadas da projecção do sinal sobre as exponenciais complexas ϕ_k) representam a contribuição de cada frequência na geração do sinal.

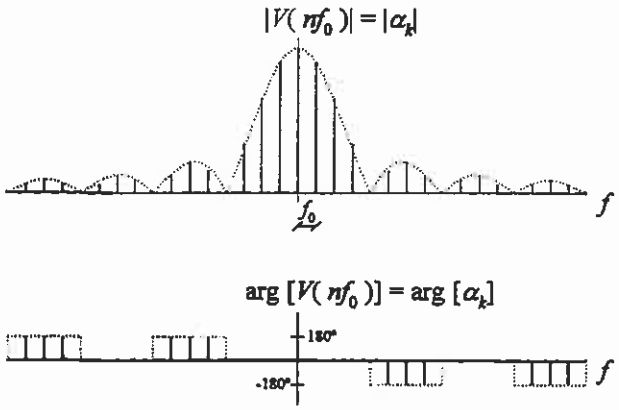


Figura 6 – Espectro da onda quadrada com *duty cycle* igual a 25%. (a) Amplitude; (b) fase.

Analisando a Figura 6, veja-se que a contribuição das exponenciais complexas ϕ_4 e ϕ_{-4} é nula, uma vez que $\alpha_4 = \alpha_{-4} = 0$. Conclui-se então que: a sinusóide de frequência igual a $4f_0$ não afecta a geração da onda $v(t)$; a projecção de $v(t)$ sobre a sinusóide de frequência $4f_0$ é nula; a medida de semelhança $(v(t), \cos(2\pi 4 f_0 t))$ é nula.

3.4 Outros exemplos

Outros exemplos, onde são evidentes as vantagens em aplicar a analogia entre sinais e vectores, são referidos de modo resumido:

- Transformada de Fourier – análoga à série de Fourier, para sinais de energia [10];
- Descritores de Fourier – para extracção de características em processamento de imagem [7], [8], [9];
- DCT (*Discrete Cosine Transform*) – utilizada na compressão de imagem do JPEG (*Joint Photographers Expert Group*) [7];
- Amostragem de sinais – interpretação dos valores das amostras como coordenadas da projecção do sinal sobre uma base ortonormada formada por funções *sinc* [10], [11];
- Funções de correlação – sua interpretação como funções dos valores do produto interno entre sinais [2], [10];
- Desenho de sistemas de comunicação digital [3], [4];
- Análise da desmodulação de sinais na presença de ruído [2], [4];
- Representação de sinais com base nas Funções de Walsh [11].

4 Conclusões

A simplicidade das operações e relações vectoriais facilita a compreensão de algumas operações de análise e processamento de sinais como a série de Fourier ou as funções de correlação entre sinais. A nossa experiência diz-nos que depois de sensibilizar professores e alunos para a utilidade desta ferramenta (analogia entre sinais e vectores) os assuntos são apresentados e compreendidos com maior simplicidade e clareza. Assim, conclui-se que a Teoria de Espaços Vectoriais é de extrema importância na formação básica do engenheiro, permitindo o constante e essencial recurso à ferramenta "analogia entre sinais e vectores" ao longo da sua restante formação relacionada com a análise de sinais.

Bibliografia

[1] T. M. Apostol, *Calculus*, Vol. I, Second Edition, Wiley International Edition, 1967.

[2] A. B. Carlson, *Communication Systems*, 3rd Edition, McGraw-Hill, 1986.

[3] J. G. Proakis, *Digital Communications*, 3rd Edition, McGraw-Hill, 1995.

[4] S. Haykin, *Communication Systems*, John Wiley & Sons, 1994.

[5] L. L. Scharf, *Statistical Signal Processing*, Addison-Wesley, 1991.

[6] A. V. Oppenheim and A. S. Willsky, *Signal & Systems*, 2nd Edition, Prentice Hall, 1997.

[7] J. C. Russ, *The Image Processing Handbook*, 2nd Edition, IEEE Press, 1995.

[8] A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall, 1989.

[9] R. G. Matteson, *Introduction to Document Image Processing Techniques*, Artech House, 1995.

[10] I. Milho, *Folhas de Apoio a Teoria dos Sinais e dos Sistemas*, DEEC-ISEL, Outubro-1998. Disponível na internet em http://www.cc.isel.pt/Pessoais/IsabelMilho/index.htm.

[11] F. Coulon, *Théorie et Traitement des Signaux*, Vol. VI, Presses Polytechniques romandes, Lausanne, 1984.

Condução Automática de Veículos Terrestres através de Redes Neuronais

Gonçalo Xufre Silva
ISEL – INESC

Resumo

O projecto ALVINN (*Autonomous Land Vehicle In a Neural Network*) [4] tem mostrado que as técnicas de redes neuronais apresentam boas condições para a condução automática de veículos terrestres. Neste artigo fazemos uma introdução às redes neuronais artificias e apresentamos uma das suas aplicações práticas com maior sucesso: a condução automática de veículos terrestres.

1 Redes Neuronais Artificiais

1.1 Introdução

As redes neuronais artificiais têm sido motivo de estudo nos últimos anos, na tentativa de alcançar performances próximas das conseguidas pelo cérebro humano em muitos campos, tais como a análise de fala e o processamento de imagens. Na verdade, o cérebro humano desempenha um conjunto de actividades, das quais a mais destacável talvez seja o processamento de imagem, de modo muito mais eficiente e rápido do que o melhor dos super computadores. As redes neuronais artificiais foram inspiradas no pouco conhecimento que temos do funcionamento do cérebro, que naturalmente, é muito mais complexo que o descrito por estes modelos.

As redes neuronais têm uma enorme e variada aplicação que envolve campos desde o reconhecimento de fala e imagem, até ao controlo de pequenas acções domésticas. São geralmente utilizadas em contextos onde o conhecimento *a priori*, acerca do sistema envolvido, não é total e muitas vezes quase inexistente, sendo necessário uma constante adaptação a frequentes variações desse mesmo sistema. Algumas das sua características são:

- A capacidade de aprender a desempenhar determinadas tarefas

- O conseguir extrair características dos dados que lhe são apresentados, que lhes permite classificar em classes distintas ou estabelecer relações implícitas entre os mesmos.
- A facilidade em lidar com informação ruidosa, conseguindo separar de forma bastante aceitável, o ruído das características principais que compõem a informação.
- Processamento da informação em paralelo.

Uma descrição bastante simples, no entanto algo insuficiente, poderia ser: uma rede neuronal é constituída por um conjunto de unidades (neurónios) que processam informação, estando ligadas entre si, através de canais de comunicação unidireccionais que transportam dados numéricos. Cada unidade opera sobre os dados que recebe através das ligações e, possivelmente sobre a sua memória local. A família das redes é muito vasta, e os diferentes modelos podem ser classificados em diferentes classes consoante as suas características:

- ***Redes estáticas***. Nas redes estáticas, a saída de cada unidade (neurónio) depende apenas do valor actual das suas entradas.
- ***Redes dinâmicas***. Nas redes dinâmicas as unidades são regidas por equações diferenciais ou às diferenças. Assim, a classificação das redes está relacionada com o facto destas serem ou não, dispositivos com memória.

O sistema implementado por uma rede neuronal é ditado pelos diferentes valores dos parâmetros que a compõem. Os parâmetros mais importantes numa rede, são os valores numéricos atribuídos a cada ligação, a que damos o nome de *pesos* e que definem o ganho fornecido pelas respectivas ligações entre as unidades. As redes neuronais artificiais possuem regras de treino, através das quais, os parâmetros da rede são ajustados por forma a que esta desempenhe as acções pretendidas. Essa *adaptação*, *treino* ou *aprendizagem* é feita com base em padrões que vão sendo apresentados à rede e, por essa razão, diz-se que uma rede neuronal é um dispositivo de processamento que tem a capacidade de aprender a partir de exemplos.

- ***Aprendizagem supervisionada***. Quando se usa a aprendizagem supervisionada, vão-se apresentando à rede pares de vectores (*entrada* e *saída desejada*) e os seus parâmetros vão sendo ajustados por forma a diminuir alguma função pré-definida de erro entre a saída que a rede produz e a saída desejada. A este tipo de aprendizagem chama-se aprender com um professor.

- ***Aprendizagem não supervisionada***. Na aprendizagem não supervisionada, apresentam-se à rede apenas os vectores de entrada e a rede é treinada de modo a desenvolver um comportamento desejado, como por exemplo identificar classes de dados estruturalmente diferentes.

Neste artigo iremos apenas referir o perceptrão multicamada, uma rede pertencente à classe das redes estáticas, sendo talvez a rede mais utilizada e cujas características mais interesse tem despertado no seio dos investigadores de redes neuronais artificiais. O perceptrão multicamada apresenta como regra de treino o algoritmo da retropropagação dos erros pertencente ao grupo dos algoritmos de treino supervisionado.

1.2 Perceptrão multicamada

O Perceptrão multicamada é o género de rede mais conhecido, e que mais e melhores tipos de capacidades apresenta. Um Perceptrão multicamada é uma rede que contém uma ou mais camadas de unidades entre os nós de entrada e os nós de saída da rede. Cada unidade individual é um perceptrão (figura 1) composto por um elemento que faz a soma ponderada (pelos pesos) das suas entrada e que posteriormente lhe aplica uma função não linear $f(x)$, conhecida como função de activação, que origina o valor de saída da unidade. As camadas que não estão directamente ligadas aos nós de saída chamam-se camadas escondidas. Na figura 2 podemos observar um perceptrão multicamada com uma camada escondida. Hornik et al. [2] demonstram que um Perceptrão multicamada com uma camada escondida, desde que se possa variar sem restrições o número de unidades nessa camada, consegue aproximar com precisão desejada qualquer tipo de função.

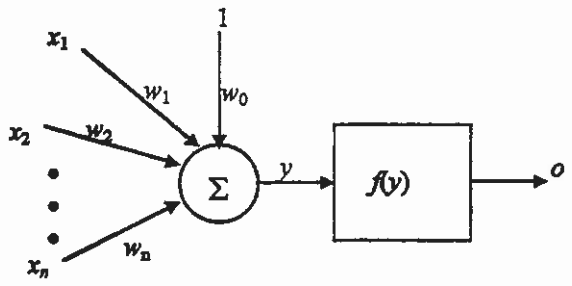


Figura 1 – Perceptrão

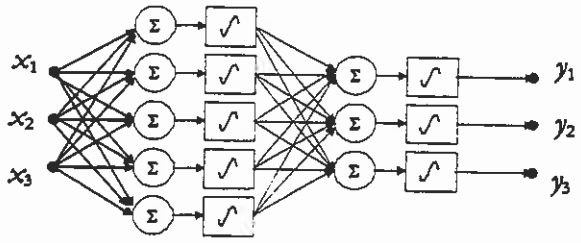


Figura 2 – Perceptrão multicamada

1.3 Algoritmo da retropropagação dos erros

Uma rede neuronal é um modelo matemático que tem a capacidade de adaptar os seus parâmetros por forma a aproximar o mais possível as saídas geradas por cada padrão de entrada, dos valores desejados. Para essa adaptação existem várias regras ou algoritmos, sendo a mais utilizada em perceptrões multicamada, o algoritmo da retropropagação dos erros. Trata-se de um algoritmo que pode ser utilizado em qualquer rede cujas ligações não formem ciclos e cujas unidades tenham funções continuas e diferenciáveis como funções de activação. É um algoritmo baseado no cálculo do gradiente de uma função de custo, geralmente o somatório dos erros ao quadrado, com respeito aos diferentes parâmetros da rede (pesos das ligações). A inovação que ele apresenta, centra-se na forma fácil e rápida do ponto de vista computacional, com que nos permite calcular as derivadas parciais da função de custo. Uma demonstração simples e bastante descritiva do algoritmo pode ser encontrada em [6]. Depois de na iteração n, se ter calculado o gradiente da função de custo relativamente aos pesos da rede, $\frac{\partial(E^2_{total})}{\partial w_{ij}}$, estes são actualizados de acordo com a seguinte regra de actualização:

$$\Delta w_{ij}(n+1) = -\eta \cdot \frac{\partial(E^2_{total})}{\partial w_{ij}} + \alpha \cdot \Delta w_{ij}(n) \qquad (1)$$

onde $\Delta w_{ij}(n) = w_{ij}^{(n)} - w_{ij}^{(n-1)}$, e α representa o parâmetro do termo de momento [1], que tipicamente apresenta um valor entre 0.5 e 0.9 e que pretende garantir a estabilidade de convergência do processo de aprendizagem (convergência para um mínimo local da função de custo, pois os métodos baseados em técnicas de cálculo do gradiente não garantem a convergência para mínimos globais), através da introdução de uma "memória" sobra a

actualização efectuada na iteração anterior. O parâmetro η representa o passo de aprendizagem, tendo sido proposto em [3] um método de passos adaptativos que usa um passo de aprendizagem distinto para cada peso da rede, e que apresenta excelentes resultados em termos de velocidade de convergência do algoritmo [5].

2 Projecto ALVINN

O projecto ALVINN é um projecto inicialmente desenvolvido por Dean A. Pomerlau e Todd M. Jochem em 1992 [4] onde o objectivo principal é conseguir que uma rede neuronal artificial conduza sozinha, um veiculo terrestre numa situação real, fazendo a sua aprendizagem através da observação de uma pessoa a conduzir. A arquitectura da rede que podemos observar na figura 3 consiste numa camada de entrada com 960 unidades correspondentes a uma retina de 30x32 que recebe como entradas as imagens de vídeo fornecidas por uma câmara no topo do veículo. Cada entrada está ligada a todas as unidades da camada escondida que por sua vez estão ligadas a todas as unidades de saída. A camada escondida tem 9 unidades e a de saída 45. A camada de saída é uma representação linear da direcção a que o veiculo se deve deslocar de modo a manter-se na estrada. De modo a que a rede conduza o veículo, a imagem da câmara é injectada nas entradas da rede e uma ordem de comando relativamente ao volante é obtida da camada de saída.

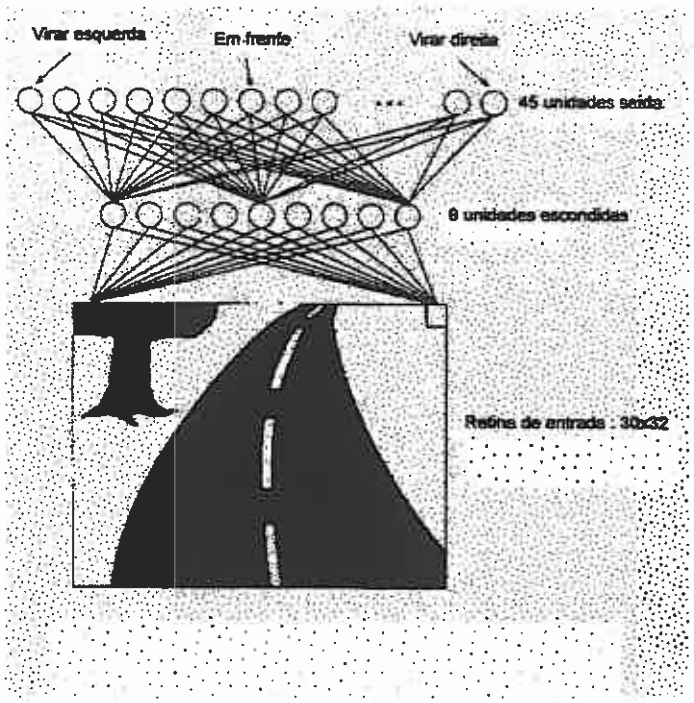


Figura 3 : Arquitectura da rede neuronal ALVINN

A unidade de saída mais activa determina a direcção em que se deve colocar o veiculo. Na figura 4 temos uma fotografia do carro de teste conduzido pelo ALVINN onde se pode observar a câmara de vídeo instalada na parte superior da cabina de condução.

Figura 4 – Veiculo de teste conduzido pelo ALVINN

Por forma a ensinar a rede a conduzir, são lhe fornecidas algumas imagens, enquanto uma pessoa conduz, e é lhe fornecido a informação relativamente à posição do volante em cada instante da condução. O algoritmo da retropropagação do erros adapta os pesos das ligações entre as diferentes unidades, de modo a que a rede produza uma resposta adequada quando lhe é apresentada uma imagem da estrada à frente do veiculo. Podemos observar na figura 5 exemplos de imagens que são apresentadas à rede (as imagens recolhidas pela câmara sofrem um pré-processamento onde são transformadas em imagens de níveis de cinzentos).

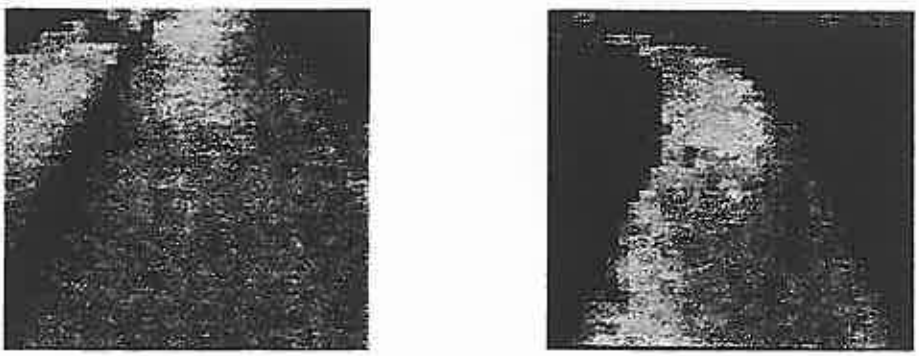


Figura 5 – Dois exemplos das imagens apresentadas à rede

Após 3 minutos de observação o ALVINN é capaz de tomar o controlo da situação e conduzir sozinho. Devido à sua capacidade de aprender as características importantes das imagens para conduzir numa situação particular, o ALVINN tem sido treinado com sucesso numa maior variedade de situações do qualquer outro sistema autónomo de navegação, que geralmente requerem situações pré-definidas e de características fixas. As situações em que o ALVINN tem conduzido, incluem estradas simples de uma faixa com pavimento sujo, estradas de uma faixa com faixa para bicicletas, estradas de duas faixas e auto-estradas. Neste último domínio, o ALVINN conduziu com sucesso distâncias superiores a 90 milhas e velocidades até 70 milhas por hora, numa auto-estrada pública a norte de Pittsburg.

Redes especificas são treinadas para cada situação e além de fornecerem uma posição para o volante fornecem uma estimativa da sua fiabilidade. O ALVINN usa estas estimativas para seleccionar a rede mais apropriada para o tipo de estrada em que se encontra, e para mudar de rede à medida que o tipo de estradas vai variando.

3 Conclusão

Neste artigo, fizemos uma breve apresentação das redes neuronais artificiais que têm sofrido um considerável aumento de interesse nos últimos anos. Os investigadores têm descoberto características importantes nas redes neuronais, que lhes permite em algumas situações obter performances parecidas com as alcançadas pelo cérebro humano.

Apresentámos como caso de sucesso o projecto ALVINN, onde uma rede neuronal consegue conduzir de forma automática um veiculo de terrestre. Inúmeras outras situações existem, nas quais as redes neuronais conseguem desempenhar tarefas onde os computadores devido ao seu processamento sequencial e à sua necessidade de evoluir em situações pré-definidas têm-se revelado incapazes.

Bibliografia

[1] D. E. Rumelhart, G. E. Hinton e R. J. Williams, Learning Internal Representations by Error Propagation, *ICS Report 8506*, Universidade Califórnia, 1985.

[2] K. Hornik, M. Stinchcombe e H. White, Multilayer feedforward networks are universal approximators, *Neural Networks* nº 2, pp. 359-366, 1989.

[3] F. M. Silva e L. B. Almeida, Speeding up Backpropagation, em *Advances in Neural Information Processing Systems*, nº 3, pp. 213-225, 1991.

[4] D. A. Pomerleau, Neural Network Perception for Mobile Robot Guidance, *Tese de Doutoramento*, Universidade de Carnegie Mellon, 1992.

[5] J. D. Amaral, Técnicas de aceleração do algoritmo da retropropagação, *Tese de Mestrado em Engª Electrotécnica e Computadores* no Instituto Superior Técnico, 1993.

[6] G. X. Silva, Redes Neuronais Recorrentes em Processamento Temporal de Informação, *Tese de Mestrado em Engª Electrotécnica e Computadores* no Instituto Superior Técnico, 1996.

Predição linear – Aplicações na Codificação de Fala.

Carlos Eduardo de Meneses Ribeiro

Instituto Superior de Engenharia de Lisboa

DEEC-CEDET-INESC

Tel: + 1.8317281 E-mail: cmr@isel.pt

Resumo

Este artigo apresenta a predição linear, um dos métodos mais importantes para modelação e extracção de características do sinal de fala. Será dado maior ênfase à estimação e interpretação do modelo e serão apresentadas aplicações na codificação de sinais de fala com débito binário baixo, tendo em especial atenção o *vocoder* (*voice coder*) como modelo aproximado de produção da fala. Embora a estimação do modelo seja feita por minimização do erro quadrático no domínio do tempo, serão apresentadas interpretações no domínio da autocorrelação e da frequência.

1 Introdução

Um dos métodos mais poderosos de análise e caracterização de sinais de fala é o da predição linear. Este método tornou-se dominante para estimar parâmetros do sinal de fala numa trama em que se considera o sinal estacionário, devido à variação lenta do tracto vocal. A ideia básica da predição linear é a de que o valor de uma amostra pode ser aproximado (predito) por combinação linear dos valores das amostras anteriores, tirando partido da correlação entre estas, resultando num modelo autoregressivo. Os pesos da combinação linear ou coeficientes LPC (Linear Predictive Coding) são estimados por minimização do erro quadrático entre a amostra actual e a sua predição. Será apresentada a formulação desta estimação e os resultados interpretados quer no domínio da autocorrelação quer no da frequência. O filtro resultante simula o tracto vocal, pelo que são apresentadas analogias entre este método e a produção da fala.

Embora não se limite ao processamento de sinais de fala, as aplicações da predição linear em processamento de fala são inúmeras. No contexto da codificação de fala, além dos parâmetros LPC é transmitido o erro de predição, com menor gama dinâmica do que o sinal de entrada e, portanto, capaz de ser quantificado de um modo mais eficiente. Exemplos de outras aplicações são a estimação de formantes, o reconhecimento e síntese de fala e a identificação e verificação do orador.

Além desta introdução, este artigo apresenta a estimação do modelo na secção 2, sendo a interpretação no domínio da autocorrelação apresentado conjuntamente com a estimação do ganho do modelo. Na secção 3 é apresentada a interpretação no domínio da frequência e a justificação da necessidade de pré-ênfase. Na secção 4 é apresentada a utilização da predição linear na codificação de sinais terminando a secção 5 com um conjunto de breves conclusões.

2. Estimação do Modelo

O sinal de fala é não estacionário, sendo no entanto possível considerá-lo quase estacionário (localmente estacionário) numa trama do sinal, em que o valor de uma amostra s[n] pode ser predito por combinação linear do valor de p amostras passadas, mais um termo correspondente ao erro de predição ou resíduo e[n]

$$s[n]=\sum_{k=1}^{p}a_k s[n-k]+e[n] \tag{1}$$

em que a_k são os pesos da combinação linear. O sistema descrito por esta equação pode ser especificado no domínio da frequência, aplicando a transformada z a ambos os lados da equação e admitindo uma entrada u[n], tal que e[n]=Gu[n], em que G é o ganho do modelo

$$H(z)=\frac{S(z)}{U(z)}=\frac{G}{1-\sum_{k=1}^{p}a_k z^{-k}} \tag{2}$$

O filtro resultante é um filtro só de pólos, correspondentes às raízes do polinómio do denominador. Este tipo de modelos são também conhecidos por modelos autoregressivos (AR).

2.1 Estimação dos coeficientes de LPC - Minimização do erro quadrático

Dado um sinal s[n] e considerando a trama índice m, os pesos ou coeficientes de predição são calculados minimizando o erro quadrático do resíduo, dado por

$$E_m=\sum_n e^2[n]=\sum_n\left(s[n]-\sum_{k=1}^{p}a_k s[n-k]\right)^2 \tag{3}$$

O intervalo para o qual se minimiza o erro quadrático é deixado para já indefinido, mas recairá naturalmente sobre a trama em análise. Em aplicações de codificação de sinais de fala com frequência de amostragem a 8 KHz, valores típicos para a ordem de predição p variam entre os 8 e os 12, sendo os coeficientes de predição obtidos por minimização do erro quadrático em ordem aos diversos coeficientes a_k,

$$\frac{\partial E_m}{\partial a_k}=0 \qquad k=1,\ldots,p \tag{4}$$

pelo que resulta, juntamente com a equação 3, no sistema de p equações a p incógnitas

$$\sum_{k=1}^{p}a_k\sum_n s[n-k]s[n-i]=\sum_n s[n]s[n-i] \qquad i=1,\ldots,p \tag{5}$$

Esta equações, na terminologia da minimização do erro quadrático, são conhecidas como equações normais. Para se calcular os coeficientes de predição deve-se resolver o sistema (5) de p equações a p incógnitas, havendo para isso basicamente dois métodos, baseados em definições diversas dos limites do intervalo de minimização: o método da autocorrelação e o método da covariância.

2.2.1 Método da autocorrelação - Considere-se que o sinal x[n] é nulo fora da janela de análise, o que pode ser descrito por

$$s_m[n] = s[m+n]w[n] \tag{6}$$

sendo w[n] uma janela de duração N, com valores zero fora do intervalo $0 \leq n \leq N\text{-}1$. Os limites dos somatórios das equações (5) serão entre $-\infty$ e $+\infty$ e os somatórios corresponderão à função de autocorrelação R(i) do sinal depois de multiplicado pela janela, que dá nome a este método.

O sistema de equações colocado sobre a forma matricial dá origem a uma matriz de Toeplitz [pxp], em que todos os coeficientes ao longo das diagonais são idênticos. Sendo a matriz de Toeplitz, é possível resolver este sistema de equações de um modo recursivo e portanto computacionalmente eficiente [Makhoul (75)].

2.2.2 Método da covariância - Minimizando o erro E numa trama de dimensão N, os limites do somatório passam a ser entre 0 e N-1. Se para além desta imposição nada se supuser sobre o sinal fora dessa trama, os somatórios das equações (5) deixam de representar a correlação do sinal multiplicado pela janela. A matriz resultante embora simétrica deixa de ser de Toeplitz, pelo que a sua solução é computacionalmente mais pesada. Este método, conhecido por método da covariância, é mais exacto uma vez que os erros no início e fim da trama não são tão grandes como no método da autocorrelação.

2.3 Estimação do ganho do modelo

A resposta em frequência dada pela equação (2) assume um ganho G tal que Gu[n]=e[n], ou seja, a excitação deverá ser proporcional ao erro de predição, sem o qual o sinal de saída não será igual ao sinal original. No entanto, este sinal será sempre uma versão quantificada, pelo que o ganho do modelo deverá ser estimado tendo em consideração que a energia do sinal de saída deverá ser igual à energia do sinal a modelar. Iremos considerar dois tipos de entrada: Um impulso correspondente à modelação da abertura da glote nas zonas vozeadas (com vibração das cordas vocais) e ruído branco estacionário correspondente à modelação das zonas não vozeadas (ar saído dos pulmões com a glote completamente aberta).

2.3.1 Impulso à entrada - Se a excitação do filtro corresponder a um impulso de área unitária, a saída do sistema será a resposta impulsiva h [n], calculada através da equação (1)

$$h[n] = \sum_{k=1}^{p} a_k h[n-k] + G\delta[n] \tag{7}$$

Multiplicando ambos os membros desta equação por h[n-i] e somando para todo o n, resulta a seguinte recursão para o cálculo da autocorrelação da resposta impulsiva,

$$\hat{R}(i) = \sum_{k=1}^{p} a_k \hat{R}(i-k) \tag{8}$$

em que a autocorrelação de ordem zero correspondente à energia e é dada por,

$$\hat{R}(0) = \sum_{k=1}^{p} a_k \hat{R}(k) + G^2 \tag{9}$$

Impondo a condição de que a energia da resposta impulsiva deverá ser igual à energia do sinal de entrada, e tomando em consideração a recursividade imposta por (8), conclui-se que

$$\hat{R}(i) = R(i) \quad 0 \le i \le p \tag{10}$$

pelo que se pode reinterpertrar a estimação do modelo de LPC como o de estimar os coeficientes de um filtro só de polos, tal que os p+1 primeiros valores da autocorrelação sejam iguais aos do sinal que se quer modelar. Das equações (9) e (10) obtêm-se o ganho G do modelo,

$$G^2 = R(0) - \sum_{k=1}^{p} a_k R(k) \tag{11}$$

2.3.2 Ruído branco à entrada - Assumindo que a entrada u[n] corresponde a ruído branco estacionário com valor médio nulo e variância unitária e aplicando a equação (1), a saída s´[n] correspondente será dada por

$$s'[n] = \sum_{k=1}^{p} a_k s'[n-k] + Gu[n] \tag{12}$$

Multiplique-se ambos os membros desta equação por s´[n-i] e some-se para todo o n. Tendo em consideração que u[n] e s´[n] são incorrelacionados, a condição de impor a mesma energia entre o sinal de saída e o sinal a modelar faz resultar quer para o ganho quer para a autocorrelação as mesmas equações (10) e (11) já obtidas para o caso de ter à entrada um impulso. Este resultado era de esperar já que ambas as entradas têm a mesma autocorrelação e espectro plano.

3 Envolvente espectral - Estimação do tracto vocal

Foi provado através da equação (10) que os primeiros p+1 coeficientes de autocorrelação do sinal de saída do modelo são idênticos aos do sinal que se quer modelar. São estes valores que contribuem primordialmente para a definição da envolvente espectral, pelo que esta condição impõe uma aproximação da resposta em frequência do filtro de LPC à envolvente espectral do sinal a modelar, como é mostrado na figura 1 (c)(d).

Na produção de fala contribuem dois tipos de excitação do tracto vocal: a excitação vozeada, com vibração periódica das cordas vocais que se dá por abertura e fecho da glote; e a não vozeada em o ar flúi livremente para o tracto vocal. A excitação vozeada tem uma característica aproximadamente passa-baixo de segunda ordem, enquanto que a excitação não vozeada é do tipo ruído branco, com espectro plano. Do outro lado do tracto vocal a radiação nos lábios tem uma característica essencialmente passa-alto, que poderá ser modelada por um zero muito perto da origem, eliminando a contribuição de um dos pólos da excitação nas zonas vozeadas.

É normal antes da estimação do modelo LPC introduzir um filtro de pré-ênfase das altas frequências do tipo,

$$P(z) = 1 - \mu z^{-1} \tag{16}$$

em que μ tem tipicamente um valorentre 0.9 e 1. Este filtro retira a contribuição do segundo pólo nas zonas vozeadas, pelo que o filtro LPC resultante é uma estimativa do tracto vocal.

A razão da utilização do filtro de pré-ênfase é dar maior peso às altas frequências dos sinais a modelar, atenuadas devido ao espectro da forma de onda glotal nas zonas vozeadas, que faz aparecer um declive (*tilt*) ao longo do espectro do sinal, como é mostrado na figura 1(c). Com a utilização do filtro de pré-ênfase o declive espectral diminui, como é mostrado na figura 1(d) e apresenta uma menor gama dinâmica. Da comparação destas figuras verifica-se ainda que o filtro de LPC segue melhor o sinal com pré-ênfase, estando as formantes (zonas de ressonância do tracto vocal) melhor marcadas. Nas zonas não vozeadas o filtro de pré-ênfase não deverá ser utilizado, embora não seja notada degradação da qualidade caso este se aplique. Na síntese dos sinais de fala deverá ser colocado à saída do filtro LPC um filtro de de-ênfase, com a característica inversa do da equação (16).

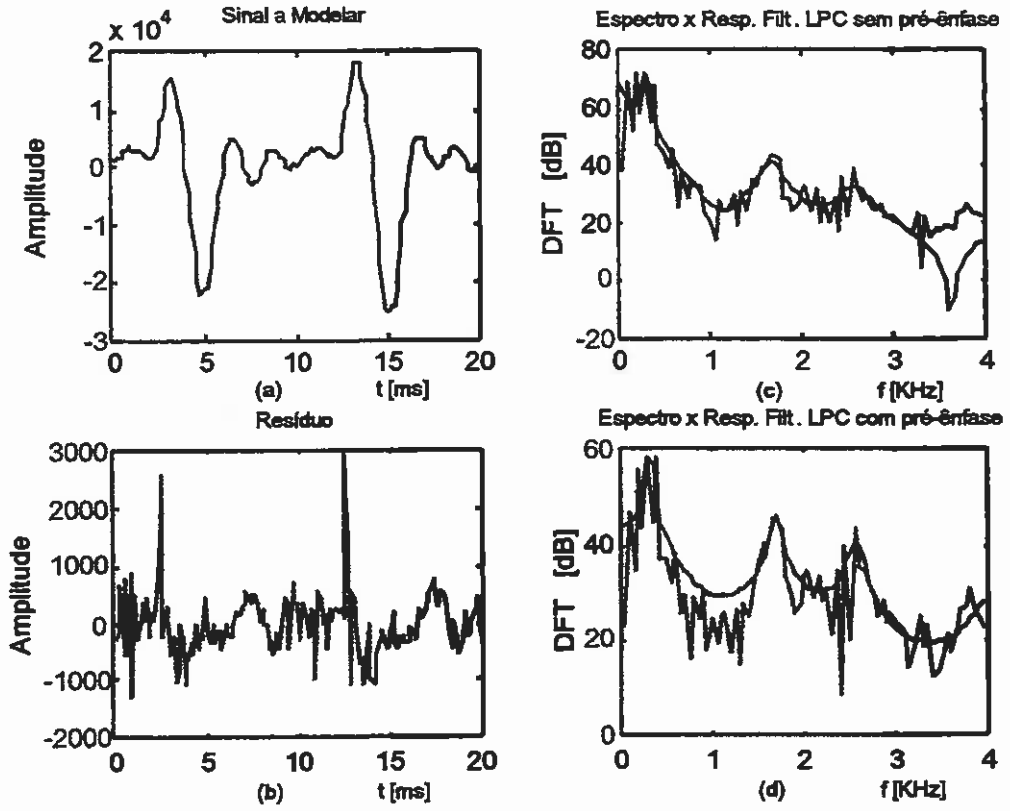


Figura 1

(a) Sinal a modelar.

(b) Resíduo de predição - ordem 10 com pré-ênfase (μ=0.95).

(c) Espectro do sinal a modelar versus resposta do filtro de LPC sem pré-ênfase.

(d) Espectro do sinal a modelar versus resposta do filtro de LPC com pré-ênfase.

A resposta do filtro pode ser distinguida da DFT do sinal a modelar por ser contínua e com andamento suave, enquanto que esta última é discreta, embora afectada pela janela de análise.

4 Codificação de sinais de fala utilizando predição linear

A figura 1 mostra o sinal a modelar em (a) e o respectivo resíduo de predição (erro de predição) em (b). Pode-se verificar a existência no resíduo da mesma periodicidade do sinal original, que corresponde à frequência fundamental de vibração das cordas vocais (*pitch*), mas com muito menor gama dinâmica, podendo ser quantificado de uma forma mais eficiente que o sinal a modelar. É exactamente esta característica que torna a predição linear atractiva em temos da redução do débito binário. Repare-se que, nas zonas vozeadas, pode-se ainda tirar partido da periodicidade (com um atraso correspondente à frequência fundamental) para minimizar ainda mais o resíduo.

O primeiro codificador a utilizar um preditor linear adaptativo foi proposto por Atal em 1970 [Atal (70)], com o nome de APC - *Adaptive Predictive Coding*. Consistia num modulador delta adaptado (ADM), com um preditor LPC de ordem 9. Entretanto, diversas estratégias foram propostas para quantificar o resíduo: Multi-Pulso [Atal (82)] que modela o resíduo com um número finito de pulsos e funcionando na gama dos 13 aos 16 kbit/s; O RPE -Excitação regular de pulsos [Deprettere (85)], que codifica vectorialmente a posição dos pulsos mais importantes e que é utilizado no sistema GSM de transmissão digital móvel europeia [Vary (88)] a 13 Kbit/s; e o CELP - *Code Excited Linear Prediction* [Schroeder (84)], que quantifica vectorialmente as amplitudes do resíduo, funcionando na gama dos 4.8 a 8 Kbit/s. Este último método tem vindo a merecer especial atenção devido à relação qualidade débito binário, sendo a base de diversas normas de codificação.

Os *vocoders* (*Voice Coders*) LPC usam um modelo simplificado do mecanismo humano de produção da fala. Como ilustra a figura 2, um filtro de síntese LPC simulando o trato vocal, seguido do filtro representando a radiação nos lábios, é excitado por um de dois tipos de sinal: sinal da glote com período igual ao do período da frequência fundamental se o som for vozeado; ruído branco se o som for não vozeado.

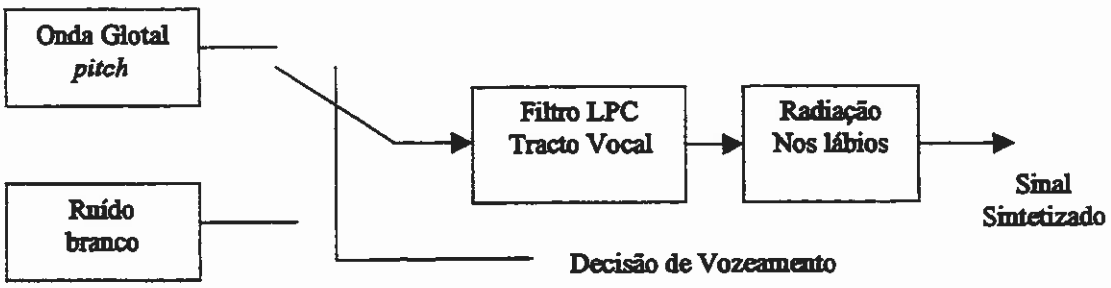


Figura 2
Esquema de blocos da síntese em *vocoders*
utilizando um modelo simplificado de produção da fala

Devido ao pequeno número de parâmetros deste codificador (parâmetros LPC, ganho, decisão de vozeamento e frequência fundamental) obtêm-se débitos binários bastante baixos, sendo no entanto pouco robusto, dado que o modelo da excitação é demasiado simples e por possíveis erros na decisão

de vozeamento e estimação da frequência fundamental. Este tipo de codificador, puramente paramétrico, apenas preserva a amplitude espectral de curta duração e não a fase.

Baseado neste modelo simplificado de produção de fala, a norma do departamento de defesa (DoD) dos Estados Unidos da América FS-1015 [Tremaen (82)], codifica a fala a 2.4 kbit/s. Esta norma, também conhecida por LPC-10, embora proposta já em 1982 tem sido uma referência obrigatória em toda a investigação posterior na área da codificação de fala a um débito binário baixo.

5 Conclusões

Foi apresentado o modelo de predição linear e apresentado o método de estimação dos diversos parâmetros. Embora seja um método no domínio do tempo, foi interpretado no domínio da autocorrelação e da frequência. Sendo um modelo autoregressivo de minimização do erro, este poderá ser representado com maior eficiência do que o sinal a modelar e portanto com uma melhoria na relação *qualidade - débito binário*. Foram ainda abordadas algumas estratégias de representação do erro de predição, e apresentado o *vocoder* como modelo simplificado de produção da fala.

Bibliografia

[Atal (70)] - Atal B. S., Schroeder M. R., "Adaptive Predictive Coding of Speech Signals", Bell Sys. Tech. Jour., vol. 49, pp.1973-1986, Outubro de 1970.

[Atal (82)] - Atal B. S., Remde J. R., "A New Model of LPC Excitation for Producing Natural-Sounding Speech at Low Bit Rates", Proc. IEEE, ICASSP, pp.6124-6127, 1982.

[Atal (89)] - Atal B. S., Cox R. V., Kroon P., "Spectral Quantization and Interpolation for CELP Coding", Proc. IEEE, ICASSP, 1989.

[Deller (93)] J. R. Deller Jr., J. G. Proakis, J. H. L. Hansen, "Discrete-Time Processing of Speech Signals", Macmillan, 1993.

[Deprettere (85)] - Deprettere Ed F., Kroon P., "Regular Excitation Reduction for Effective and Efficient LP-Coding of Speech", Proc. IEEE, ICASSP, pp.25.8.1-25.8.4, 1985.

[Makhoul (75)] - Makhoul J. , "Linear Prediction: A Tutorial Review", Proc IEEE, vol. 63, pp.561-580, Abril de 1975.

[Meneses(97)] - C. Meneses Ribeiro, "Codificação de Sinais", apontamentos da disciplina de Sistemas de Comunicação Digital, I.S.E.L., 1997.

[Schroeder (84)] - Schroeder M. R., Atal B. S., "Code-Excited Linear Prediction (CELP): High-Quality Speech at Very Low Bit Rates", Proc. Int. Conf. Com..,pp.1610-1613, 1984.

[Tremaen (82)] - Tremain T. E., "The Government Standard Linear Predictive Coding Algorithm: LPC-10", Speech Technology, Vol.1 N°2, pp.40, Abril de 1982.

[Vary (88)] - Vary P., Hellwing K., Hofmann R., Sluyter R. J., Galand C., Rosso M., "Speech Coded for the European Mobile Radio System", Proc. IEEE, ICASSP, pp.227-230, 1988.

Telecomunicações: Um Desafio às Probabilidades

Cláudia Nunes
Departamento de Matemática, Centro de Matemática Aplicada,
Instituto Superior Técnico

O desenvolvimento crescente na área de Telecomunicações tem estado na origem de novas técnicas probabilistícas, ao mesmo tempo que se assiste à aplicação de métodos estatísticos e probabilísticos já sobejamente conhecidos em novos problemas do domínio das comunicações. Esta dicotomia tem-se mostrado particularmente fértil: a aplicação de modelação estocástica, embora de grande dificuldade, tem-se mostrado muito importante quer no planeamento dos sistemas de comunicação quer na avaliação do seu desempenho, ao mesmo tempo que novos métodos probabilísticos têm sido desenvolvidos para responder a novas situações, contribuindo assim para a evolução da área dos processos estocásticos.
Neste trabalho propomos ilustrar esta dicotomia, apresentando alguns breves exemplos.

1. Os Novos Modelos de Comunicação

Nos dias correntes a atenção no domínio das telecomunicações está essencialmente centrada sobre modelos de comunicação móveis : os vulgos telemóveis. Este mercado tem assistido a um rápido desenvolvimento não só a nível técnico como a nível comercial. Este ritmo de crescimento representa por si só fonte de desafio para os engenheiros e técnicos associados ao negócio das comunicações móveis: dado que o número de clientes e serviços requeridos regista aumentos anuais muito significativos, impõem-se sofisticadas estratégias de design e planeamento de rede. Em particular, é necessário construir sucessivos modelos que descrevam arquitecturas de sistemas e protocolos capazes de lidar com novos objectivos, restrições e parâmetros de qualidade.
Ao contrário de uma rede de telefones fixos, uma rede de telefones móveis serve clientes "dinâmicos", isto é, clientes que se movem temporal e espacialmente. Devido a esta mobilidade, tanto o local como a duração das chamadas afectam os recursos presentes na rede que suporta a comunicação. Este aspecto é uma das particularidades mais "visíveis" destes modelos [1].
Outro aspecto que merece toda a atenção dos profissionais das comunicações actuais é a necessidade de estabelecer fluxos de informação eficientes; estes fluxos são suportados por estruturas complexas, cuja presença deverá passar despercebida ao comum dos utilizadores. Exemplos desta situação são os mecanismos de redes de transporte de alta velocidade, dos

quais ATM (*assyncronous transfer mode*) é o mais conhecido, que permitem a utilização de tecnologias que suportam novos serviços de comunicação (serviços multimédia, por exemplo). Seja qual for a situação (redes móveis, modelos de tráfego rápido, etc), o design e as decisões de gestão destes serviços requerem previsões sobre o desempenho da rede que os suporta; decisões baseadas em previsões erradas podem ser catastróficas. Existe uma panóplia considerável de métodos utilizados na avaliação e comparação de designs de redes e protocolos: técnicas analíticas (equações diferenciais, por exemplo), técnicas de simulação, projecções baseadas em dados existentes, análise de séries temporais, etc. Mas seja qual for a técnica utilizada, estaremos sempre em presença de um problema sobre o qual não dispomos de informação completa, existindo sempre - em maior ou menor grau - conhecimento incompleto da dinâmica dos clientes e do próprio sistema em si. E é precisamente fruto deste conhecimento incompleto que as probabilidades se têm mostrado de importância fulcral.

Neste artigo ilustraremos, de forma necessariamente breve e incompleta, alguns problemas recentes no domínio das telecomunicações e quais as vias probabilísticas encontradas para a sua solução. Na secção 2 daremos exemplos de situações ligadas aos serviços de comunicações móveis e na secção 3 ilustraremos um dos problemas associado aos serviços de transmissão de dados. Dado o objectivo deste trabalho e da sua reduzida dimensão, os exemplos apresentados são notoriamente escassos e pouco desenvolvidos, pelo que indicaremos bibliografia considerada relevante.

2. Serviços de Comunicações Móveis (SCM)

Nesta secção procuraremos descrever brevemente duas técnicas de modelação presentes no planeamento de serviços de comunicação móveis (abreviadamente designado por SCM).

Um SCM é composto por estações de base, onde são processadas as chamadas. A cada base corresponde uma área geográfica coberta pelo sinal emitido/recebido pela base; esta área geográfica constitui uma célula. Uma célula tem c canais, onde cada canal representa uma dada banda de frequência, que será atribuída a cada chamada. Um conjunto de células que forma uma área geográfica contínua designa-se por área de registo (AR). Para que um assinante da rede emita/receba uma chamada é necessário identificar a AR associada à chamada [2].

Numa rede de comunicações móveis as estações de base necessitam de gerir de forma eficiente a largura de banda - o recurso mais escasso e dispendioso - devendo ter em linha de conta dois objectivos que estão de certa forma em conflito: *utilizar ao máximo os recursos disponíveis* vs *reservar recursos de forma a que a taxa de recusa de serviços, devido a insuficiência de recursos, seja mantida abaixo de um nível aceitável*. Na prática tal significa

que por vezes uma estação de base terá que reservar recursos para eventuais chamadas que estão nesse preciso momento a decorrer fora da sua área geográfica de influência mas que brevemente poderão entrar nos seus "domínios", mesmo que tal signifique rejeitar o acesso de rede a novas chamadas. Tal balanço, que se repercute na percentagem de chamadas "caídas" e chamadas "recusadas", é usualmente medido em termos de um parâmetro usualmente designado de "Qualidade de Serviço" (QoS, sigla utilizada na literatura anglo-saxónica). Algumas das questões mais pertinentes a nível do planeamento de recursos de um SCM:

1. Dado que o número de assinantes destes serviços aumenta drasticamente, dever-se-à planear os recursos de forma que a probabilidade de que todos os canais estejam ocupados quando uma nova chamada é pedida (e que será recusada) seja mantida abaixo de um dado limite;
2. Deverão ser considerados modelos distintos para populações de baixa mobilidade e de alta mobilidade;
3. Tem-se registado uma diminuição na duração média de uma chamada (de acordo com dados divulgados pelo CTIA, a duração média de uma chamada passou de 2.24 min, em 1990, para 2.15 min, em 1996), pelo que no planeamento da rede dever-se-à ter em linha de conta tal facto;
4. Dado o aumento do número de utilizadores de redes fixas, regista-se igualmente aumento de comunicações de rede fixa/rede móvel, pelo que é necessário estudar tais alterações e propor novos protocolos e métodos de avaliação/gestão de tráfego.

Vários modelos de gestão de rede têm sido propostos (por exemplo, em [4] e [5]). Uma das grandes dificuldades registadas na elaboração de tais modelos prende-se com o insuficiente conhecimento da população e respectiva dinâmica.

Um SCM pode ser estudado de duas formas: através de simulação ou de métodos analíticos. As técnicas de simulação apresentam o inconveniente de requererem recursos computacionais substanciais, pelo que é desejável encontrar técnicas analíticas que reduzam o esforço requerido no estudo do comportamento de SCM e seus utilizadores. Existem vários modelos que procuram satisfazer este requerimento; de entre esses modelos destacam-se os designados Modelo de População e Modelo de Movimento:

a) Modelo de População

Este modelo permite a determinação da distribuição em equilíbrio do número de chamadas afectadas a uma dada célula. Para tal assume a seguinte hipótese: *a taxa a que novos utilizadores* ***entram*** *na área geográfica correspondente a uma célula é igual à taxa a que utilizadores* ***deixam*** *essa área* ***(taxa de entrada=taxa de saída)***. Considere-se a população formada

pelos utilizadores de um SCM. Seja N o número esperado de utilizadores de uma célula e $F(.)$ a distribuição (genérica) do tempo em que um utilizador permanece nesta célula, com valor esperado $1/\eta$. Assume-se que o processo de chegadas de clientes a uma célula pode ser aproximado por um processo de Poisson, com taxa de chegada $\lambda^* = N\eta$ e que durante a realização de uma chamada a probabilidade do utilizador se deslocar, saindo da área de influência da célula inicial, é negligível. Com estas hipóteses e com o facto de se assumir que a taxa de entrada é igual à taxa de saída de chamadas de uma célula (esta hipótese permitirá, em particular, considerar as equações de balanço de um sistema de filas de espera), podemos considerar que a população afectada a uma dada célula pode ser modelada por um sistema do tipo $M/G/\infty$ (designação usual para filas de espera com processo de chegadas regido por um processo de Poisson, distribuição de serviços genérica e infinitos servidores), com taxa de chegada λ^* e taxa de serviço η. Seja π_n a probabilidade, estando o sistema em equilíbrio, de existirem n clientes numa célula; então é possível provar [12] que $\pi_n = \frac{N^n e^{-N}}{n!}$, seja qual for a distribuição da duração das chamadas. Esta insensibilidade à distribuição da duração do serviço (não só da sua lei como até da duração média de cada chamada) parece surpreendente mas estudos de simulação corroboram tal facto (vide [7], onde são apresentados resultados de simulação para durações exponenciais e uniformes).

Este modelo pode servir para inferir sobre determinados parâmetros importantes da população. Um dos exemplos mais significativos é a probabilidade de bloqueio p_b - probabilidade de uma chamada não ser efectuada por a célula a que está afectada estar totalmente ocupada (porque todos os canais estão a ser utilizados). De facto este é um dos parâmetros mais significativos na determinação do índice QoS, pelo que na gestão e planeamento de redes de SCM um dos objectivos que se deverá ter sempre em linha de conta é a minimização da probabilidade de bloqueio.

Pela lei das probabilidades totais, vem que:

$$p_b = \sum_{c \le n < \infty} P(\textit{bloqueio} \mid \textit{existem } n \textit{ clientes na célula})\pi_n \equiv \sum_{c \le n < \infty} p_b^{(n)} \pi_n$$

Como calcular $p_b^{(n)}$? Dado que existem n clientes na célula, ocorre bloqueio quando c estão em chamada e ocorre um pedido de chamada antes de algum desses c clientes terminar a sua chamada. Se as chamadas ocorrem de acordo com um processo de Poisson, se estas tiverem duração com distribuição exponencial e se a mobilidade da população for negligível (isto é, o número de utilizadores que no decorrer de uma chamada o cliente saiem da área de influência

da célula original é negligível), é possível derivar uma expressão para $p_b^{(n)}$ [12] e consequentemente determinar a probabilidade de bloqueio.

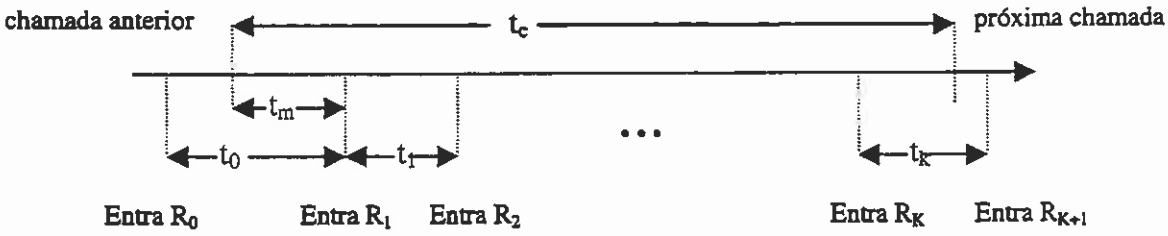
b) Modelo de Movimento

É necessário distinguir duas situações: um cliente pode apresentar pouca mobilidade durante a realização de uma chamada mas ser móvel entre duas chamadas consecutivas. É este segundo "tipo" de mobilidade a que seguidamente dedicaremos atenção.

Designe-se por $\alpha(K)$ a probabilidade de um cliente se deslocar ao longo de K AR entre duas chamadas consecutivas e t_c o intervalo de tempo entre duas chamadas consecutivas desse mesmo cliente. Suponhamos que aquando da primeira chamada o cliente se encontra na AR R_0; depois desta chamada o cliente passa por outras K AR, sendo t_i o tempo em que se encontra na AR i $(0 \le i \le K)$; seja ainda t_m o tempo que decorre entre a primeira chamada e o tempo até sair da AR R_0. Assumem-se as seguintes hipóteses:

1. chamadas realizadas pelo cliente decorrem segundo um processo de Poisson; nesse caso t tem distribuição Exponencial de média $E[t_c] = 1/\lambda$;
2. Os t 's são v.a. independentes e identicamente distribuídas, com função densidade genérica $f(t_i)$ e valor esperado $E[t_i] = 1/\eta$.

A relação entre os diversos tempos pode ser representada esquematicamente da seguinte forma:



Utilizando o facto de que as chamadas ocorrem de acordo com um processo de Poisson é possível provar que [7]:

$$\alpha(K) = \begin{cases} \dfrac{P\left(t_m + t_1 + \ldots + t_K < t_c < t_m + t_1 + \ldots + t_K\right)}{P\left(t_c < t_m\right)} & K \ge 1 \\ & K = 0 \end{cases} = \begin{cases} \dfrac{\eta}{\lambda}\left[1 - f^*(\lambda)\right]^2 \left[f^*(\lambda)\right]^{K-1} & K \ge 1 \\ 1 - \dfrac{\eta}{\lambda}\left[1 - f^*(\lambda)\right] & K = 0 \end{cases}$$

onde $f^*(s) = \int_0^\infty e^{-st} f(t)dt$ é a transformada de Laplace-Stieljes de $f(\,)$, cujos valores estão tabelados para a maior parte das distribuições comuns. Casos de especial interesse são o exponencial ($f^*(s) = \eta/(\eta + \lambda)$), e o uniforme ($f^*(s) = \eta/(2\lambda)\left(1 - e^{-(2\lambda)/\eta}\right)$).

Este modelo permite estudar outro parâmetro do índice de QoS: a probabilidade de terminação de chamadas. Quando um cliente se move durante a realização de uma chamada, de tal forma

que a chamada tem de ser processada por outra célula diferente da inicial, há sempre a hipótese de não haver canal disponível na nova célula, pelo que a chamada será bruscamente terminada. Esta incapacidade do sistema processar a chamada na sua totalidade é muito grave, sendo este facto ainda menos desejável que a ocorrência de bloqueio.

Suponhamos que tanto a ocorrência de novas chamadas como a *transferência* de chamadas (adoptaremos esta terminologia para designar o efeito de mudança de célula responsável pelo processamento das chamadas) ocorrem de acordo com processos de Poisson independentes, de taxas λ_{nc} e λ_{tc}. Designa-se por p_0 a probabilidade de ocorrer bloqueio por ocorrência de nova chamada e p_f a probabilidade de terminação forçada da chamada (chamada "caída). Assumindo que os tempos que as chamadas permanecem em cada célula são v.a. i.i.d., é possível estabelecer a seguinte relação ([7], [5]):

$$\lambda_{tc} = (1-p_0)\frac{\eta\left[1-f^*(\mu)\right]}{\mu\left[1-(1-p_f)f^*(\mu)\right]}\lambda_{nc}$$

a qual permite derivar p_0 e p_f iterativamente: atribuir um valor inicial a λ_{tc} e iterar a expressão anterior até convergência (afim de assegurar convergência do processo iterativo, é relevante qual o valor inicial para λ_{tc}, vide [5]).

3. Transmissão de Dados

No âmbito de modelos de transmissão de informação, uma das técnicas correntemente utilizadas é o chamado *Modo de Transmissão Assíncrono* (cuja sigla, de origem anglo-saxónica, é ATM) [10]. A tecnologia ATM caracteriza-se por uma grande versatilidade e flexibilidade que permite, por exemplo, integrar serviços de baixo ritmo (como a voz e alguns tipos de dados), serviços de alto débito (como o vídeo), incluindo serviços de ritmo constante, variável, com ou sem relação temporal. A forma mais usual de modelar as diversas fontes de sinal a que correspondem diferentes classes de serviços é por um processo MMPP. O MMPP (*Markov Modulated Poisson Process*) é um processo de Poisson duplamente estocástico cuja intensidade é controlada por uma cadeia de Markov, vulgarmente designada de *ambiente*. Por exemplo, quando o número de estados da cadeia de Markov é dois, o processo condicional de chegadas é Poisson de taxa λ_0 (λ_1) se o ambiente está no estado 0 (1). Na maior parte das aplicações em que nos deparamos com MMPP's o ambiente não é observável, pelo que ao "utilizador" não é facultada a possibilidade de observar directamente as transições entre estados do ambiente.

Associado a um MMPP existe um conjunto de parâmetros que, a menos de permutações na numeração dos estados, define univocamente o processo, e que é composto por: taxas de chegada $\Lambda = \{\lambda_1, \lambda_2, ..., \lambda_M\}$ (λ_j designa a taxa de chegada ao processo quando a cadeia de Markov está no estado j, sendo M o número de estados da cadeia) e taxas de transição

$$\Sigma = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1M} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2M} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{M1} & \sigma_{M2} & \cdots & \sigma_{MM} \end{bmatrix}$$ (onde σ_{ij} designa a taxa de transição do estado i para o estado j da cadeia de Markov, com $\sigma_{ii} = -\sum_{j \neq i} \sigma_{ij}$).

É sobre estes parâmetros que incide um dos problemas estatísticos mais relevantes: a sua estimação. Usualmente dispõe-se dos seguintes dados: *instantes de ocorrência de pedidos de serviço* e *duração do serviço*.

Na literatura são mencionados métodos que se enquadram numa das seguintes categorias:

- Métodos baseados no método dos momentos;
- Métodos baseados na verosimilhança.

O método dos momentos foi o primeiro a ser aplicado a este problema [8]. Após determinação da função geradora de probabilidades de um MMPP, são determinados os momentos de diversa ordem; de seguida, os parâmetros do modelo são escolhidos de forma a que estes momentos sejam numericamente iguais aos momentos empíricos dos dados recolhidos. Porém este método de estimação apresenta dois tipos de problemas:

1. Baseia-se num critério de estimação "pobre" e por vezes conduz a estimadores com "más" propriedades (e.g., a nível de consistência, [3]).
2. Quando o número de estados do ambiente do MMPP é superior a 2, esta escolha – que na prática significa a resolução de um sistema de M^2 equações – pode ser numericamente difícil.

Quanto aos estimadores baseados na função de verosimilhança: em situações em que as suas propriedades são conhecidas (poucas, infelizmente), apresentam características desejáveis (em particular, são consistentes e têm distribuição assimptótica normal, facto que permite a elaboração de testes de hipóteses e intervalos de confiança). De entre os estimadores pertencentes a esta categoria, distinguem-se:

- **Estimadores EM** : estimadores obtidos iterativamente. Cada iteração é composta por duas etapas (etapa **E** – obtenção do valor esperado da função de verosimilhança em ordem à parte não observada do ambiente; etapa **M** – maximização deste valor esperada).

- **Estimadores Recursivos:** Um procedimento recursivo para estimação de um vector paramétrico arbitrário, que designaremos genericamente por Ψ, assenta na seguinte relação:

$$\Psi^{(n+1)} = \Psi^{(n)} + \gamma_n H_n h\left(y_1, y_2, ..., y_{n+1}; \Psi^{(n)}\right)$$

onde $\Psi^{(k)}$ representa a estimativa de Ψ após k observações, $\{\gamma_n\}$ é uma sucessão de números positivos que tende para zero, H_n é uma matriz dita adaptativa (e que deverá ser *convenientemente escolhida*) e $h(\bullet;\Psi)$ designa-se por vector *score*. Diferentes escolhas de H_n e de $h(\bullet;\Psi)$ são possíveis, levando a métodos e resultados eventualmente distintos; exemplos de tal são os métodos de Holst e Lindgren – vide [6], o de Krishnamurthy e Moore e o de Rydén – vide [11] para uma comparação destes três métodos.

- **Estimador de Discretização Temporal:** Este método deve-se a Deng e Mark [3] e constitui uma alternativa à estimação paramétrica de um MMPP baseada no princípio da máxima verosimilhança. Trata-se de um método iterativo e pode ser visto como uma aplicação do algoritmo EM. Seja $]0,x]$ o intervalo temporal em que se observa o processo; fixa-se uma unidade temporal h e divide-se o intervalo em $\lceil x/h \rceil$ subintervalos. A cada subintervalo é atribuído o valor 1 ou 0 consoante nele se registar ou não uma ocorrência de evento (h deverá ser escolhido de forma a assegurar que não ocorre mais de um evento em cada subintervalo). Após a discretização, obtemos uma sequência binária $O = \{O_1, O_2, ..., O_{\lfloor x/h \rfloor}\}$ para a qual é possível construir um algoritmo EM de mais fácil implementação que para os dados originais e com resultados numéricos animadores (vide [3] e [9]).

- **Estimador Bi-etápico:** diversos estudos de simulação têm mostrado que é difícil estimar *simultaneamente* e *bem* as taxas de chegada e de transição, uma vez que nas aplicações de maior interesse as taxas de chegada são de ordem superior às de transição. Geralmente os dois conjuntos de parâmetros são simultaneamente estimados. Porém, tal como proposto em [9], os resultados são francamente melhores se primeiramente se estimar as taxas de transição e seguidamente, fixadas estas, se estimar as taxas de chegada. Resultados de simulação evidenciam a superioridade numérica deste procedimento, ao mesmo tempo que indiciam os seguintes factos:

  - as estimativas das taxas de transição no método da discretização temporal apresentam regiões de estabilidade muito notórias, isto é, existe uma gama variada de h's que conduzem a estimativas semelhantes; a partir de certo limiar, tais estimativas são

notoriamente diferentes. Em termos práticos, quando os parâmetros do modelo forem desconhecidos, sugere-se que se estime as taxas de transição para uma gama variada de h's, se reconheça a zona de estabilidade e se tome como estimativa final uma função das estimativas nessa zona, como seja, por exemplo, a média dessas estimativas.

- as estimativas das taxas de chegada não são muito influenciadas pelas estimativas das taxas de transição, desde que estas últimas não assumam valores muito díspares dos verdadeiros.

4. Comentários Finais

A cooperação da engenharia com as probabilidades têm já um passado histórico relevante e é de prever um futuro risonho. Os problemas levantados aos probabilistas (nomeadamente a nível de processos estocásticos) pelas telecomunicações constituem verdadeiros desafios, permitindo o avanço de ambas as áreas do conhecimento. Esta cooperação é extensível a outros domínios da matemática: a estatística, sistemas dinâmicos e análise numérica são outros exemplos desta situação.

Referências

[1] N. Antunes, R. Rocha, P. Pinto e A. Pacheco, Impact of Next-Generation Wireless Networks Requirements on Teletraffic Modeling, *Interoperable Communication Networks*, Vol. 1 (1998), n°2-4, Ed: Dr. Stathya Rao, Publ: Baltzer Science Publishers, Julho 1998.

[2] D. Cox, Wireless Personal Communications: What Is It?, *IEEE Pers. Commun.*, pg. 20-35, Abril 1995.

[3] L. Deng e J. Mark. Parameter estimation for Markov modulated Poisson processes via the EM algorithm with time discretization. *Telecomm. Syst.*, 1, p. 321-338, 1993.

[4] J. Ho, I. Akyldiz, Local Anchor Scheme for Reducing Signaling Cost in Personal Communication Networks, *IEEE/ACM Trans. Networking*, 1996.

[5] D. Hong e S. Rappaport, Trafic Model and Performance Analysis for Cellular Mobile Radio Telephone Systems with Prioritized and Non-Protection Handoff Procedure, *IEEE Trans. Vehic. Tech.*, vol VT-35, n° 3, Ag. 1986.

[6] U. Holst e G. Lindgren, Recursive estimation in mixture models with Markov regime. *IEEE Trans. Inform. Theory*, vol. 37, n°6, p. 1683-1690, 1991.

[7] Y. Lin, Modeling Techniques for Large-Scale PCS Networks, *IEEE Comm. Mag.*, Fev. 1997.

[8] M. Neuts, A versatile Markovian point process. *J. Appl. Prob.* 16, p. 746-779, 1979.

[9] C. Nunes e A. Pacheco, Estimação Paramétrica em MMPP's, a publicar nas Actas do VI Congresso SPE, Tomar.

[10] J.P. Rebelo. *Aproximação de Processos ON-OFF por um Processo MMPP para Análise do Atraso Médio numa Fila de Espera ATM*. Tese de Mestrado, Instituto Superior Técnico, Lisboa, 1997.

[11] T. Rydén. On recursive estimation of hidden Markov models. *Stochast. Process. Appl.*, 66, p. 79-96, 1997.

[12] S. Ross, *Stochastic Processes*, John Wiley & Sons, 1983.

MODELAÇÃO MATEMÁTICA DE CÂMARAS FRIGORÍFICAS

R. A. Pitarma*, J. E. Ramos** e M. G. Carvalho***

(*) Dept.Eng.Mecânica; Instituto Politécnico da Guarda-ESTG
Av.Francisco Sá Carneiro, Nº50, 6300 Guarda;
E-mail: rpitarma@ipg.pt
(**) Dept.Eng.Mecânica; Instituto Politécnico de Leiria-ESTG
Morro do Lena, Alto Vieiro, 2400 Leiria;
E-mail: jramos@estg.iplei.pt
(***) Dept.Eng.Mecânica; Instituto Superior Técnico
Av.Rovisco Pais, 1096 Lisboa Codex;
E-mail: maria@navier.ist.utl.pt

Sumário

O presente artigo descreve um modelo computacional para a caracterização de ambientes interiores em câmaras frigoríficas. O modelo consiste num procedimento de cálculo para resolução, por diferenças finitas, das equações diferenciais de derivadas parciais exprimindo a conservação de massa, de quantidade de movimento, de energia e de concentração de espécies no ar. O transporte turbulento é modelado através do modelo a duas equações k-ε. O modelo computacional foi validado através da confrontação de previsões numéricas com valores experimentais obtidos em modelo laboratorial.

1 - Introdução

O projecto de instalações frigoríficas desenvolve-se, regra geral, de um modo empírico, prevalecendo a experiência do projectista e o sucesso adquirido em projectos similares precedentes. As câmaras frigoríficas representam, actualmente, o acumular de anos de experiência e de evolução tecnológica, desempenhando de forma mais ou menos satisfatória as suas funções.

Não obstante, como resultado das maiores exigências ao nível das condições de frio e da utilização racional de energia, nos últimos anos a metodologia seguida começou a ser questionada. Assumem aqui particular importância os métodos de distribuição de ar nas câmaras. Com efeito, face à natureza complexa da movimentação do ar nos recintos refrigerados, estes observam uma distribuição não uniforme dos campos de velocidade, de temperatura e de humidade relativa do ar, tornando heterogéneas as condições de frio a que os géneros armazenados estão expostos.

O desenvolvimento dos métodos computacionais aplicados à Mecânica de Fluidos, associado ao constante aumento da capacidade de cálculo e à redução de custo dos computadores, têm permitido criar ferramentas avançadas de cálculo de escoamentos de fluidos em geometrias mais ou menos complexas. Estas ferramentas apresentam enormes potencialidades no domínio da refrigeração de espaços, permitindo ao projectista antecipar e corrigir deficiências na fase de projecto ou optimizar instalações já em operação. Merecem referência, por exemplo, os estudos de [1] e [2].

Neste artigo apresenta-se um modelo computacional, implementado e validado por [3], que permite prever as condições climáticas de ambientes interiores em câmaras frigoríficas.

2 - Modelo Matemático

O modelo matemático que descreve o escoamento tridimensional turbulento em câmaras frigoríficas, consiste num conjunto de equações diferenciais de derivadas parciais, exprimindo a conservação de massa, de quantidade de movimento, de energia e de concentração de espécies. A turbulência, sendo um fenómeno quase aleatório, tridimensional e dependente do tempo, está ainda longe de um perfeito entendimento. Porém, para a maioria dos problemas de engenharia, tal como o que aqui é estudado, o conhecimento dos valores médios temporais das propriedades sobrepõe-se ao conhecimento dos detalhes da turbulência. Deste modo, em substituição das equações exactas, são resolvidas as equações expressas em função de valores médios temporais. Estas equações podem ser representadas segundo uma mesma equação geral de transporte, definida por

$$\frac{\partial}{\partial x_i}(\rho U_i \phi) = \frac{\partial}{\partial x_i}\left(\Gamma_\phi \frac{\partial \phi}{\partial x_i}\right) + S_\phi \qquad (1)$$

em que

U_i	é a componente da velocidade média na direcção x_i
ϕ	representa a variável dependente
Γ_ϕ	é o coeficiente de difusão da variável ϕ
S_ϕ	constitui o termo fonte

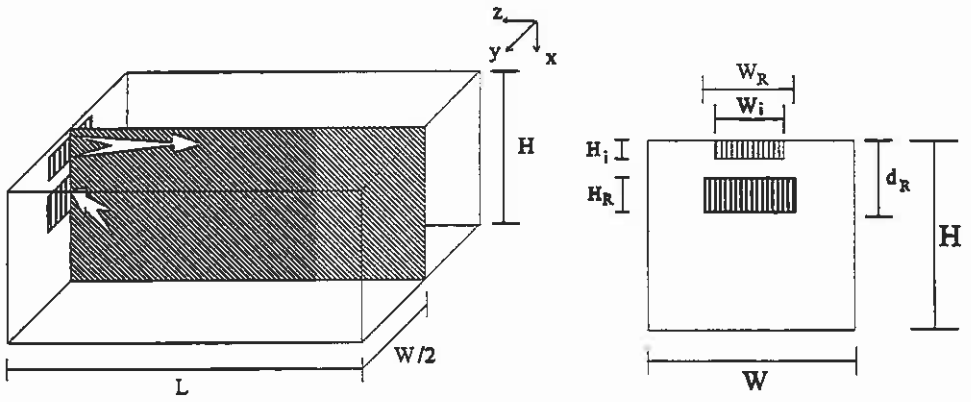
Nas equações para a continuidade, quantidade de movimento, energia térmica e concentração de espécies, a variável ϕ toma, respectivamente, os valores 1, U_i (velocidade média na direcção x_i), h (entalpia específica) e m_V (humidade específica). O efeito da turbulência é modelado por recurso ao modelo de turbulência k-ε [5]. Assim, torna-se necessário resolver adicionalmente duas equações diferenciais de transporte, correspondentes à energia cinética turbulenta (k) e à sua taxa de dissipação (ε). Os efeitos de impulsão são contabilizados, quer na componente vertical da equação de conservação de quantidade de movimento, quer no modelo de turbulência. O estabelecimento das condições de fronteira nas paredes é feito por recurso às leis de parede [5].

A discretização das equações diferenciais é obtida por diferenças finitas, formulação do volume de controlo, com os termos convectivos e difusivos tratados conjuntamente segundo o esquema híbrido. Para assegurar a satisfação da equação da continuidade, as equações anteriores são resolvidas sequencialmente, num processo iterativo, de acordo com o algoritmo SIMPLE [6]. O sistema de equações algébricas resultantes da discretização é resolvido por um

método iterativo linha-a-linha, que combina o algoritmo de Thomas para matrizes tri-diagonais (TDMA) com o de Gauss-Seidel [7].

3 - Modelo Laboratorial

Os ensaios para a validação experimental do modelo computacional foram realizados num compartimento à escala laboratorial com 1,52x0,72x0,66m^3 (Figura 1). As paredes do modelo são em Perspex com 6mm de espessura e isolamento térmico em poliestireno expandido com 100mm de espessura. A temperatura no exterior foi estabilizada a 25°C. A fonte de calor correspondente à taxa de metabolismo dos produtos armazenados foi admitida uniforme e proveniente do pavimento com o valor aproximado de 50W. O ar de circulação foi insuflado no compartimento, à temperatura estabilizada de 5°C e com uma velocidade média de 3,1m/s, através de uma abertura rectangular localizada numa parede junto ao tecto. O retorno foi realizado por uma abertura mais ampla, igualmente rectangular, localizada por baixo da insuflação. As medições da temperatura do ar foram realizadas com termopares do tipo T, de 200μm, conectados a um sistema de aquisição DT 2811-PGL / DT756-Y.



L	H	W	H_i	H_R	W_i	W_R	d_R	
1,52	0,66	0,72	0,06	0,12	0,24	0,32	0,24	[m]

Figura 1 - Geometria simplificada do modelo laboratorial, com o plano de simetria e o sistema de coordenadas adoptado

4 - Resultados e Discussão

A figura 2 apresenta o campo de temperatura previsto no plano de simetria do compartimento experimental. É possível observar uma zona sob influência do escoamento do ar insuflado, com trajectória descendente junto da parede posterior, e outra zona caracterizada pela circulação de retorno. Na zona sob influência do "jacto" de entrada verificam-se valores baixos da temperatura do ar. Note-se que a utilização de jactos parietais de tecto com elevada velocidade de descarga permitem, coadjuvados pelo efeito de Coanda, manter o jacto junto ao tecto até ao extremo do compartimento, onde deflecte em direcção ao pavimento. Assim, na

região inferior da câmara regista-se um aumento gradual do nível da temperatura do ar entre as paredes posterior e anterior como resultado do efeito convectivo da circulação de retorno junto ao pavimento. Deste modo, a zona útil localizada junto da parede anterior revela-se mais crítica do ponto de vista das condições de frio. Conclui-se, por conseguinte, que deve ser considerada uma especial atenção neste tipo de instalações — regra geral refrigeradas por escoamentos de mistura — no que se refere ao posicionamento e à seleção das grelhas de insuflação, assim como na especificação dos valores do caudal do ar de circulação.

Na figura 3 são confrontados, sob a forma de perfis, valores medidos e calculados da temperatura do ar. Os valores da temperatura foram adimensionalizados tomando como referência a temperatura do ar de insuflação (5°C). Senão de uma forma quantitativa exacta, que se revelou muito satisfatória, é possível observar uma boa previsão qualitativa, o que, na prática, representa uma forte contribuição para a compreensão do escoamento no compartimento. Uma eventual inadequada modelação do transporte turbulento em zonas caracterizadas por baixos números de Reynolds, pode estar na origem da ausência de uma melhor concordância entre as previsões e os valores experimentais.

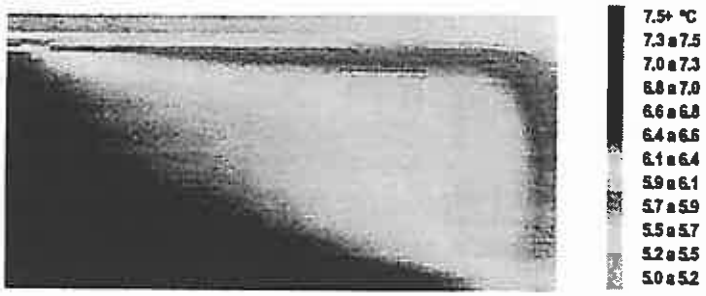


Figura 2 - Previsão da temperatura do ar no plano de simetria

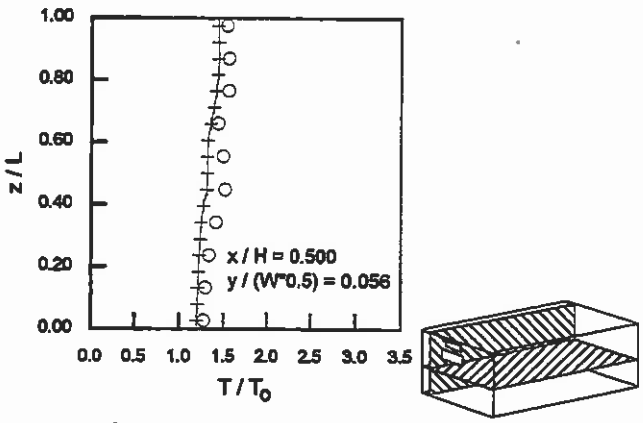


Figura 3 - Perfis comparativos de temperatura adimensional
(o : experimental ; — : numérico)

5 - Nota Conclusiva

Foi apresentado um modelo computacional para a simulação de escoamentos tridimensionais turbulentos, com transmissão de calor, em câmaras frigoríficas. A validação do modelo teórico foi empreendida através de ensaios experimentais realizados num modelo laboratorial, tendo-se revelado muito satisfatória para aplicações de engenharia. Alguns resultados do estudo foram apresentados e discutidos. A extensa informação recolhida, patente na ilustração apresentada, permite constatar que a simulação computacional de ambientes interiores em câmaras frigoríficas representa uma solução eficiente e económica para o estudo de problemas neste domínio.

Referências

[1] M.G. Carvalho, R.A. Pitarma, F.D. Pereira e J.E. Ramos, "Dynamic analysis of a refrigerated room", Ventilation'94, part 2, pp. 545-550, Stockholm, 1994.

[2] H. Wang e S. Touber, "Distributed dynamic modelling of a refrigerated room", International Journal of Refrigeration, vol. 13, Julho, 1990.

[3] R.A. Pitarma, "Modelação matemática e experimental de câmaras frigoríficas de veículos", Tese de Doutoramento, IST, Lisboa, 1998.

[4] B.E. Launder e D.B. Spalding, "The numerical computation of turbulent flows", Computer Methods in Applied Mechanics and Engineering, vol. 3, pp. 269-289, 1974.

[5] B.E. Launder e D.B. Spalding, "Mathematical models of turbulence", Academic Press, London, 1972.

[6] S.V. Patankar e D.B Spalding, "A calculation procedure for heat, mass and momentum transfer in three-dimensional parabolic flows", International Journal of Heat and Mass Transfer, vol. 15, pp. 1787-1806, 1972.

[7] S.V. Patankar, "Numerical heat transfer and fluid flow", Hemisphere Publishing Corporation, Washington, 1980.

[8] ASHRAE Handbook - Refrigeration Systems and Applications, 1994, SI Edition, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc; Atlanta.

Bloco-Valores Singulares: Que Aplicações?

Cecília COSTA* Teresa P. de LIMA† Manuela S. SILVA‡
José VITÓRIA§

1. Introdução

Nesta comunicação centramos a nossa atenção em matrizes bloco-companheiras e estudamos alguns aspectos relacionados com valores singulares e bloco-valores singulares [5] daquelas matrizes.

Os valores singulares de matrizes têm assumido, nos últimos anos, uma grande importância, dado que se tornaram numa ferramenta eficiente na resolução de problemas em diversas áreas de investigação, nomeadamente, na Álgebra Linear Numérica [2], em Análise Estatística, no Processamento de Sinal e Imagem, em Teoria de Controlo [3] e em Engenharia Biomédica [1, 5].

Em particular, neste último caso, é sabido que a decomposição em valores singulares da matriz cujos elementos são as diferenças de potencial captadas pelos eléctrodos cutâneos colocados no tórax e no abdómen de uma mulher grávida, permite obter o electrocardiograma fetal [1, 5].

Por outro lado, as matrizes bloco-companheiras desempenham papel importante no estudo de equações diferenciais (e de diferenças) com coeficientes matriciais [6].

Finalmente, o conceito (original) de bloco-valor singular foi elaborado recentemente [5], tendo sido estabelecida uma relação entre valor singular (escalar) e bloco-valor singular [7].

Esta nota está organizada da seguinte maneira: na secção 2, consideramos matrizes bloco-companheiras, cujos blocos são matrizes quadradas reais e apresentamos limites superiores para os valores singulares; na secção 3, onde os blocos (matrizes simétricas reais) comutam dois a dois, damos fórmulas para os bloco-valores singulares e, a partir destes, encontramos os valores singulares (escalares).

* Secção de Matemática, UTAD, Vila Real, e I.S.R. (Coimbra)
† Faculdade de Economia, Universidade de Coimbra, e I.S.R. (Coimbra)
‡ Faculdade de Economia, Universidade de Coimbra, e I.S.R. (Coimbra)
§ Departamento de Matemática, Universidade de Coimbra, e I.S.R. (Coimbra)

2. Caso Não Comutativo [4]

Neste parágrafo, apresentamos limites superiores para os (quadrados dos) valores singulares da matriz bloco-companheira

$$F = \begin{bmatrix} 0 & \cdots & 0 & -A_0 \\ I & \cdots & 0 & -A_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & I & -A_{n-1} \end{bmatrix}$$

em que os blocos A_i, $i = 0, 1, ..., n-1$, são matrizes quadradas reais, de ordem p.

Tomando a norma (escalar) $\|\cdot\cdot\|_\infty$ de cada bloco de F^TF, obtemos uma norma matricial $\Phi_\infty\left(F^TF\right)$. Temos a desigualdade seguinte, envolvendo matrizes não-negativas:

$$\Phi_\infty\left(F^TF\right) \leq \begin{bmatrix} I & 0 & \cdots & 0 & \|A_1\|_\infty \\ \vdots & \ddots & & \vdots & \|A_2\|_\infty \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I & \|A_{n-1}\|_\infty \\ \left\|A_1^T\right\|_\infty & \left\|A_2^T\right\|_\infty & & \left\|A_{n-1}^T\right\|_\infty & \sum_{j=0}^{n-1}\left\|A_j^T\right\|_\infty \|A_j\|_\infty \end{bmatrix} := G$$

A chave para a obtenção dos resultados deste parágrafo é a lista seguinte de desigualdades, onde estão envolvidos os conceitos de raio espectral ρ, de norma (escalar) $\|\cdot\cdot\|_1$, de norma matricial Φ_∞ e de matriz não-negativa:

$$\rho\left(F^TF\right) \leq \rho\left[\Phi_\infty\left(F^TF\right)\right] \leq \rho(G) \leq \|G\|_1$$

Apresentamos duas desigualdades envolvendo os valores singulares s_μ, $\mu = 1, 2, ..., pn$, da matriz F:

- Partindo de $\|G\|_1$:

$$s_\mu^2 \leq 1 + \sum_{q=0}^{n-1}\left\|A_q^T\right\|_\infty \|A_q\|_\infty$$

- - Usando uma técnica ligeiramente diferente:

$$s_\mu^2 \leq \frac{1 + \sum_{q=0}^{n-1}\left\|A_q^T\right\|_\infty \|A_q\|_\infty + \sqrt{\left(1 + \sum_{q=0}^{n-1}\left\|A_q^T\right\|_\infty \|A_q\|_\infty\right)^2 - 4\left\|A_0^T\right\|_\infty \|A_0\|_\infty}}{2}$$

3. Caso Comutativo [7]

Consideremos, de novo, a matriz bloco-companheira F, em que, agora, A_i, $i = 0, 1, ..., n-1$, são matrizes simétricas reais, de ordem p, e $A_iA_j = A_jA_i$, $i, j = 0, 1, ..., n-1$.

Usamos uma versão matricial do conceito de valor singular, que designamos por bloco-valor singular. Mais concretamente, seguindo [5], definimos:

> Uma matriz normal S, quadrada, de ordem p, é dita um bloco-valor singular da matriz F, se S^2 for tal que $F^TFV = VS^2$, em que o vector de blocos V é de característica máxima.
>
> Nestas condições, a V chamamos vector singular de blocos associado ao bloco-valor singular S.

No contexto deste parágrafo — e admitindo que a matriz radicando é semi-definida positiva — temos as fórmulas seguintes para os bloco-valores singulares, S_1, S_α, S_n, $\alpha = 2, ..., n-1$, da matriz F:

$$S_1^2 = \frac{\sum_{k=0}^{n-1} A_k^TA_k + I + \sqrt{\left(\sum_{k=0}^{n-1} A_k^TA_k + I\right)^2 - 4A_0^TA_0}}{2}$$

$S_\alpha = I$, de multiplicidade $n-2$

$$S_n^2 = \frac{\sum_{k=0}^{n-1} A_k^TA_k + I - \sqrt{\left(\sum_{k=0}^{n-1} A_k^TA_k + I\right)^2 - 4A_0^TA_0}}{2}$$

É importante salientar que, neste caso concreto, os valores singulares (escalares), s_μ, $\mu = 1, 2, ..., pn$, de F, são os valores próprios dos bloco-valores singulares, S_1, S_α, S_n, $\alpha = 2, ..., n-1$, de F.

4. Notas e Conclusões

Foram apresentadas duas abordagens para o estudo dos valores singulares (escalares). Em ambos os casos tratados, foram usados dois conceitos não muito divulgados: norma matricial de matriz — que é uma matriz não-negativa; bloco-valor singular — que é uma matriz normal.

Quanto às aplicações: ainda que bastante se saiba a respeito dos valores singulares escalares, nada conhecemos no tocante a bloco-valores singulares [excepto, é claro, que os valores próprios dos bloco-valores singulares são — para já, somente no contexto da secção 3! — valores singulares escalares].

Referências

[1] D. Callaerts; B. de Moor; J. Vandewalle, W. Sansen; G.Vantrappen; J. Janssens, Comparison of SVD Methods to Extract the Foetal Electrocardiogram from Cutaneous Electrode Signals, *Med. Biol. Eng. Comput.* **28**: 217–224 (1990)

[2] R. N. Datta, *Numerical Linear Algebra*, Cole Publishing Company, New York, 1995.

[3] C. Kenney and A. J. Laub, Controllability and Stability Radii for Companion Form Sytems, *Math. Control Signals Systems*, **1**: 239–256 (1988)

[4] T. P. Lima; J. Vitória, Bounds for the Singular Values of Block Companion Matrices, *Linear Algebra Applications*, **170**: 225–228 (1992)

[5] M. S. Silva, *Valores Singulares — Algumas considerações sobre a sua utilidade do ponto de vista estético, científico e tecnológico.* Dissertação de Mestrado, Faculdade de Economia, Universidade de Coimbra, 1997.

[6] J. Vitória, Singular e Non-Singularizable Higher-Order Differential Matrix Equations, *Linear Algebra Applications*, **121**: 687–691 (1989).

[7] J. Vitória; T. P. Lima; C. Costa, On Block Singular Values of Block Companion Matrices, Proceedings of CONTROLO'98, 3rd Portuguese Conference on Automatic Control, Coimbra, Portugal, 9–11 September, 1998, vol.1, pp 69–73.

Introdução ao Maple V (Release 5)

J. F. Aguilar Madeira

Instituto Superior de
Engenharia de Lisboa

Maple é um programa para pessoas que trabalham com matemática. O seu ambiente computacional integrado permite realizar uma grande variedade de operações matemáticas de carácter simbólico, numérico e gráfico.

O Maple permite resolver uma grande variedade de problemas que podem ir desde problemas simples de aritmética elementar até aos problemas complexos da relatividade geral.

A utilização do Maple na verificação dos cálculos, permite uma maior concentração nos conceitos e evitar erros de cálculo.

O Maple é constituído por cerca de 3000 instruções cada uma delas comportando diversas opções. As instruções mais utilizadas em álgebra, analise, etc. formam a "main Library", enquanto as mais especializadas estão agrupadas em "packages" que cobrem entre outras áreas: ensino da matemática, álgebra linear, equações diferenciais, geometria e estatística.

O Maple também oferece uma linguagem completa de programação, que ajuda a estender as suas capacidades e permite satisfazer as necessidades específicas.

Nas jornadas de matemática pretende-se dar a conhecer o Maple como uma "ferramenta matemática" no ensino e na resolução de problemas. Para tal os pontos a evidenciar nas jornadas de matemática serão:

- Introdução a linguagem do Maple;
- A estrutura interna do Maple;
- Potencialidades do Maple no ensino e na resolução de problemas;
- Cuidados a ter com o Maple.

Começo por apresentar uma breve referência a certas instruções do Maple.

Breve Referência do Maple V (Release 5)

Abreviaturas e símbolos utilizados frequentemente

+	adição	=	igual
-	subtracção	>=	maior ou igual
*	multiplicação	<	menor
&*	Multiplicação não comutativa	<>	diferente
/	divisão	@	composição
** ou ^	potenciação	%	última instrução executada
!	factorial	->	"arrow"(para definir funções)
:=	"assignment"	?	Ajuda
.	"concatenationn" ou decimal	..	Especificar o tamanho de um intervalo

Comandos utilizados frequentemente

Tópico	Exemplo	Comando
Definir uma função	Definir $f(x)=\frac{x^2}{x^2+1}$	`f:=x->x^2/(x^2+1);`
Calcular um limite	Calcular $\lim_{x\to 2}\frac{x^2+x-6}{x^2+2x-8}$	`limit((x^2+x-6)/ ( x^2+2*x-8),x=2);`
Decompor uma fracção	Decompor a fracção $\frac{x}{x^2-3x-4}$	`convert(x/(x^2-3*x-4),parfrac,x);`
Simplificar uma fracção	Simplificar $\frac{x-1}{x^2-1}$	`simplify((x-1)/(x^2-1));`
Mostrar uma expressão como uma única fracção	Escrever $1+\frac{1}{x}$ como uma única fracção	`simplify(1+1/x);`
Derivar uma expressão	Calcular $\frac{d}{dx}(x\sin x)$	`diff(x*sin(x),x);`
Integral indefinido	Calcular $\int x\sin x\,dx$	`int(x*sin(x),x);`
Factorizar um polinómio	Factorizar $5x^2-8x-4$	`factor(5*x^2-8*x-4);`
Multiplicar uma expressão algébrica	Calcular $(5x+2)(x-2)$	`expand ((5*x+2)*(x-2));`
Resolver uma equação	Resolver $x^2-4x-5=0$	`solve(x^2-4*x-5=0);`
Resolver um sistema de equações	Resolver $\begin{cases}2x-y=7\\4x+2y=2\end{cases}$	`solve({2*x-y=7, 4*x+2*y=2});`
Resolver uma equação diferencial	Resolver $y'=1+y$	`dsolve(diff(y(x),x)= 1+y(x),y(x));`

Definir uma matriz	Definir $A=\begin{bmatrix}4 & 3\\ 5 & 0\end{bmatrix}$	`A:=array([[4,3],[5,0]]);`
Calcular um determinante	Calcular $\begin{vmatrix}5 & -3\\ 2 & 2\end{vmatrix}$	`with(linalg):` `det([[5,-3],[2,2]]);`
Calcular uma série de potências	Calcular os cinco primeiros termos da série de potências $\sin x$ no ponto 0	`series(sin(x),x=0,5);`

Calcular os valores próprios e os os correspondentes vectores próprios de uma matriz	Calcular os valores próprios e os os correspondentes vectores próprios de $\begin{bmatrix}-17 & -15\\ 20 & 18\end{bmatrix}$	`with(linalg):`
		`eigenvects([[-17,-15],`
		`[20,18]]);`

Calcular a inversa de uma matriz	Calcular a inversa da matriz $\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$	`with(linalg):`
		`inverse([[1,2],`
		`[3,4]]);`

Visualizar o gráfico de uma função	Gráfico de $\frac{x}{x^2+1}$ no intervalo $[-6,6]$	`plot(x/(x^2+1),` `x=-6..6);`
Gráfico de uma função com duas variáveis em três dimensões	Gráfico da função $\sin x \cos y$ com $0\le x\le 4\pi$ e $0\le y\le 2\pi$	`plot3d(sin(x)*cos(y),` `x=0..4*Pi,y=0..2*Pi);`
Gráfico de equações paramétricas	Gráfico de $\begin{cases}x=\cos t\\ y=4\sin t\end{cases}$ com $0\le t\le 2\pi$	`plot([cos(t),4*sin(t)` `,t=0..2*Pi]);`
Gráfico de diversas funções	Gráfico de $\sin x^2$ e $\sin^2 x$ no intervalo $[0,2\pi]$	`plot({sin(x^2),` `sin(x)^2},x=0..2*Pi);`

Multiplicar duas matrizes	Calcular AB com $A=\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$ e $B=\begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}$	`A:=array([[1,2],[3,4]]);`
		`B:=array([[1,2],[1,3]]);`
		`evalm(A&*B);`