

MATEMÁTICA DISCRETA

Conceitos e Tópicos Principais

Prof. Cícero Costa Quarto
Departamento de Engenharia de Computação
Universidade Estadual do Maranhão
cicero@engcomp.uema.br

1 Introdução

Conhecer e entender Matemática Discreta é fundamental para ser um bom profissional da Computação em suas diversas áreas, como as que seguem: *Ciência da Computação, Teoria da Computação, Criptografia, Teoria dos Jogos, Análise de Algoritmos, Raciocínio Lógico, Teoria dos Conjuntos, Teoria dos Grafos, Teoria das Árvores e Contagem.*

1.1 Ciência da Computação

É o estudo teórico e prático da computação, focado em algoritmos, desenvolvimento de softwares, inteligência artificial, banco de dados e sistemas de informação, formando profissionais para criar soluções tecnológicas, otimizar processos e inovar, atuando em diversas áreas como TI, Finanças, saúde e pesquisa, com uma formação generalista que permite especialização futura.

1.2 Teoria da Computação

É um campo fundamental da Ciência da Computação que estuda os limites e capacidades da computação através de modelos abstratos, focando em autômatos (máquinas), computabilidade (o que pode ser resolvido), complexidade (o quão rápido) e linguagens formais (regras para linguagens), fornecendo a base teórica para processadores, compiladores, algoritmos e o próprio funcionamento dos computadores.

1.3 Criptografia

É a prática e o estudo de técnicas para comunicação segura na presença de comportamento adversário. De forma mais geral, a criptografia trata da construção e análise de protocolos que impedem terceiros ou o público de ler mensagens privadas. A criptografia moderna existe na intersecção das disciplinas Matemática, Ciência da Computação, Segurança da Informação, Engenharia Elétrica, Processamento de Sinais Digitais, Física e outras.

Conceitos básicos relacionados à segurança da informação (confidencialidade de dados, integridade de dados, autenticação e não repúdio) também são centrais para a criptografia. As aplicações práticas da criptografia incluem comércio eletrônico, cartões de pagamento baseados em chip, moedas digitais, senhas de computador e comunicações militares.

1.4 Teoria dos Jogos

É um ramo da matemática aplicada que estuda situações estratégicas onde jogadores escolhem diferentes ações na tentativa de melhorar seu retorno. A Teoria dos Jogos tornou-se um ramo proeminente da matemática na década de 1930, especialmente depois da publicação em 1944 de *The Theory of Games and Economic Behavior* de John Von Neumann e Oscar Morgenstern. A Teoria dos Jogos distingui-se na Economia na medida em que procura encontrar estratégias racionais em situações em que o resultado depende não só da estratégia própria de um agente e das condições de mercado, mas também das estratégias escolhidas por outros agentes que possivelmente têm estratégias diferentes, mas objetivos comuns.

Os resultados da Teoria dos Jogos tanto podem ser aplicados a simples jogos de entretenimento como aspectos significativos da vida em sociedade. Um exemplo deste último tipo de aplicação é o Dilema do Prisioneiro, tendo sua primeira análise no ano de 1953 popularizado pelo matemático Albert W. Tucker, e que tem muitas implicações no estudo da cooperação entre indivíduos. O Dilema dos Prisioneiros é um jogo classificado como jogo de soma não zero, pois o ganho de um jogador não implica que os outros percam.

Suponhamos que você e seu comparsa foram presos. Convencido da culpa de ambos, mas não dispondo de provas para condená-los, o acusador coloca cada um numa cela e propõe a ambos o mesmo acordo. Cada um pode confessar (trair o comparsa) ou ficar calado (se manter fiel). Isolados, ambos não tem como saber ou combinar a resposta um do outro, e não há um histórico de lealdade e honra entre os mesmos. Nessa situação, como você agiria?



Tabela 1: O Dilema do Prisioneiro

	PRISIONEIRO B	
PRISIONEIRO A	Meu comparsa fica em silêncio	Meu comparsa confessa
Eu fico em silêncio	Eu = 6 meses Ele = 6 meses	Eu = 10 anos Ele = Livre
Eu confesso	Eu = Livre Ele = 10 anos	Eu = 6 anos Ele = 6 anos

Fonte: (2011).

Indivualmente, a melhor situação é aquela em que você sai livre por ter traído enquanto seu comparsa fica calado, mas se ele pensar o mesmo e também trair, vocês dois ficam presos por seis anos. A melhor solução para ambos é se vocês dois ficarem calados, pois ambos ganharão seis meses de prisão. Entretanto, você arriscaria optar por se calar, sabendo que se o comparsa o trair você ficará dez anos preso. O exemplo do Dilema do Prisioneiro mostra como a Teoria dos Jogos apoia a compreensão de situações reais e orienta os atores em suas ações e decisões. Em relação à colaboração, a Teoria dos Jogos esclarece conceitos nem sempre bem compreendidos como autointeresse, matriz de ganhos, incentivo e jogos de soma não zero. Ao aplicá-los em situações reais, cresce a nossa capacidade de avaliar, propor e agir em cenários de trabalho, estudo e lazer em grupo. Um exemplo é a capacidade de alterar a matriz de ganhos para introduzir incentivos que promovam a colaboração. A Teoria dos Jogos possibilita o aprofundamento da compreensão e a análise mais apurada de situações reais envolvendo a tomada de decisões.

1.5 Análise de Algoritmos

Área da Ciência da Computação que estuda e avalia o desempenho e os recursos (tempo e memória) necessários para executar um algoritmo, usando notação assintótica (**Big O**¹, **Big Theta**²) para medir sua eficiência em relação ao tamanho de entrada (n).

1.5.1 Conceitos Chave da Análise de Algoritmos

- **Objetivos:** Medir eficiência (tempo de execução) e uso de memória (complexidade espacial) de forma independente da máquina;
- **Complexidade de tempo** (Ordem de Grandeza): Mede o número de passos/instruções. O pior caso é frequentemente utilizado para garantir segurança no desempenho;
- **Notação Assintótica** (θ, Θ, Ω): Representa como o tempo de execução cresce com o aumento do *input*, ex: $\theta(1), \theta(\log n), \theta(n), \theta(n^2)$;
- **Casos de Análise**
 - Pior Caso (θ): Máximo de recursos necessários;
 - Melhor Caso (Ω): Mínimo de recursos necessários;
 - Caso Médio (Θ): Comportamento esperado.
- **Modelo Computacional:** Assume-se tempo constante para operações básicas (aritmética, comparações, atribuições);
- **Exemplos de Complexidade:** Busca binária é $\theta(\log n)$, enquanto algoritmos de ordenação simples como Bubble Sort são $\theta(n^2)$.

A análise permite escolher a melhor abordagem (divisão e conquista, programa dinâmica, busca local) para resolver problemas computacionais, garantindo que o algoritmo seja prático e eficiente.

¹Notação matemática usada em Ciência da Computação para descrever a escalabilidade e a eficiência de algoritmos.

²Descreve o comportamento de funções ou sistemas à medida que uma variável (geralmente o tamanho de entrada (n), com n crescendo indefinidamente.

1.6 Raciocínio Lógico

É a habilidade de analisar informações de forma estruturada, identificar padrões e usar a lógica para chegar a conclusões coerentes e racionais, fundamental para resolver problemas, tomar decisões e compreender relações complexas, baseando-se em premissas (verdadeiras ou falsas) para formar argumentos válidos e sendo um conceito central na disciplina de lógica.

1.6.1 Estrutura Funcional

- **Análise de Premissas:** Parte de afirmações (proposições) que podem ser verdadeiras ou falsas. Exemplos:
 - A terra é um planeta;
 - Todas as plantas realizam fotossíntese;
 - O sol é uma estrela;
 - A lua é um satélite;
 - Todo homem é mortal;
 - Todos os políticos são corruptos.
- **Conectivos Lógicos:** Usa "E (AND)", "OU (OR)", "SE ... ENTÃO (IF ... THEN)" para formar argumentos mais complexos, como em "Se chover (p), então a rua ficará molhada (q)".
- **Linguagem Bivalente:** Opera com valores de "verdadeiro" ou "falso", mesmo que o valor real seja desconhecido, mais existente como "Há vida em outro planeta do sistema solar sem ser a Terra".
- **Inferência:** A partir de premissas, faz inferências para chegar a uma conclusão que é apoiada pelas premissas originais, formando um argumento.

Referências Bibliográficas

- Pimentel, Mariano e Fuks, Hugo (Organizadores). Sistemas Colaborativos - Rio de Janeiro: Elsevier, 2011.
- Internet: Google e Wikipedia