

Relatório

Carlos Correia Ramos

Matemática discreta

Relatório a que se refere a alínea b) do artigo 5º do Decreto-Lei 239/2007 publicado no Diário da República, 1ª Série, 116 de 19 de Junho de 2007

Universidade de Évora, novembro de 2024
Agregação
Matemática

Dedicado à Mariana e ao José

Dedicado à Mercês

Conteúdo

Introdução	4
Objetivos	6
Conteúdos programáticos	7
Método de ensino	9
Método de avaliação	11
Estrutura detalhada e planificação	12
Bibliografia comentada	18
Recursos <i>on-line</i>	21
Videos <i>on-line</i>	22

Introdução

Sobre a unidade curricular

Apresenta-se no que se segue um relatório sobre a unidade curricular *matemática discreta*, no ramo do conhecimento de matemática, oferecida pelo departamento de matemática da Universidade de Évora.

A unidade curricular matemática discreta, MAT00932L, 6ECTS, é obrigatória de 2º ano para o curso de engenharia informática. Desde a entrada em funcionamento do curso de matemática aplicada à economia e gestão, em 2014, que a unidade curricular é oferecida também a este curso, como optativa de 3º ano. No ano letivo 2022/2023 entrou em funcionamento o curso de matemática, tendo sido a matemática discreta incluída como obrigatória de 1º ano, no plano de estudos. No ano letivo 2023/2024 entrou em funcionamento o 1º ciclo de inteligência artificial e ciência de dados, curso que inclui também a matemática discreta como obrigatória de 2º ano.

É um desafio articular estas características, em particular, a diferença de anos em que os alunos podem frequentar a unidade curricular. Não se pode esperar que os alunos de matemática, sendo do 1º ano, tenham conhecimento de álgebra linear, análise ou probabilidade e estatística. No outro extremo estão os alunos de matemática aplicada à economia e gestão do 3º ano, em princípio, com muito maior maturidade e conhecimentos matemáticos. Este aspeto condiciona de algum modo a forma de expor os conteúdos e avaliar as aprendizagens.

Por outro lado, tendo em conta o propósito original da unidade curricular de fornecer ao curso de informática ferramentas matemáticas muito variadas é razoável dar menor ênfase a aspetos teóricos de matemática ou formalizados como seria se a disciplina fosse exclusivamente lecionada a cursos de matemática. A grande maioria dos alunos são de engenharia informática, em cada ano entram 60 alunos, a que acrescem agora 20 do curso de inteligência artificial e ciência de dados, face a 15 alunos de matemática e uma dezena de alunos de matemática aplicada à economia e gestão.

Foi introduzida, no ano letivo 2021-2022, uma componente de programação em *python*, que não está formalmente exigida na ficha de disciplina. Esta componente não é avaliada, servindo como ferramenta didática, de aprendizagem voluntária, e valorização do conhecimento dos alunos interessados.

No ano letivo 2022-2023 foi testada uma calendarização e articulação de conteúdos em que o programa mínimo, que consta na ficha de disciplina, é cumprido antes do final do semestre previsto no calendário escolar. Esta antecipação da conclusão do programa mínimo é conseguida à custa de alguns dos tópicos serem lecionados de um modo mais superficial. As semanas remanescentes foram utilizadas precisamente para aprofundar alguns tópicos, recuperar aprendizagens atrasadas de alguns alunos e revisões. Este regime foi útil a vários níveis, em particular permitiu desfazer as avaliações contínuas, tipicamente frequências a meio e no final de semestre, de outras unidades curriculares. Permitiu também que os alunos interessados ganhassem maturidade, aprofundassem conhecimentos e os relacionassem com outros temas à sua escolha, em particular programação ou tópicos mais avançados, aplicados ou teóricos. Este modo de proceder foi repetido no ano 2023-2024.

A unidade curricular tem uma carga horária de quatro horas semanais de contacto, durante quinze semanas, de acordo com o calendário escolar da Universidade de Évora. Das quatro horas de contacto

semanais, duas horas têm componente teórica e as outras duas componente prática. Acresce o horário de acompanhamento que consiste em duas horas semanais agendadas de acordo com as disponibilidades dos alunos e docente.

Os conteúdos mínimos previstos formalmente na ficha de disciplina, são os seguintes:

Noções elementares de conjuntos

Princípio de indução matemática

Combinatória e contagens

Recorrência

Grafos

Algoritmo de Euclides

Aritmética modular

A adaptação dos conteúdos mínimos na unidade curricular, preparada e desenvolvida desde 2021, é indicada na secção *Conteúdos programáticos*.

Objetivos

Adquirir conhecimentos das principais técnicas da combinatória, da matemática discreta e as suas relações com outras áreas da matemática e aplicações, em particular, com a computação e a informática.

Abordar problemas matemáticos e aplicados, de natureza finita ou discreta, empregando técnicas gerais de combinatória e utilizando estratégias próprias para cada problema.

Desenvolver o raciocínio abstrato.

Adquirir autonomia e capacidade de encontrar estratégias para resolver novos problemas.

Adquirir autonomia e capacidade de enunciar novos problemas formulados matematicamente, com base em problemas com origem em aplicações.

Conteúdos programáticos

Noções elementares de conjuntos e funções.

Princípio de indução matemática: *tópico lecionado transversalmente.*

Estruturas combinatórias em conjuntos I: *relações, relações de equivalência, relações de ordem total e parcial, reticulados, conjunto quociente, partições, princípio de inclusão-exclusão.*

Teoria elementar dos números: *algoritmo da divisão, divisores, factorização, máximo divisor comum, mínimo múltiplo comum, algoritmo de Euclides, algoritmo estendido de Euclides, bases numéricas, fração contínua.*

Aritmética modular: *função de Euler, teorema pequeno de Fermat, teorema chinês do resto, exponenciação rápida.*

Estruturas algébricas: *semigrupos, monóides, grupos, anéis, corpos, espaços vetoriais, módulos sobre anéis, álgebras, isomorfismos, teorema do isomorfismo, anéis de polinómios, anéis de matrizes, corpos finitos.*

Grupos de transformações: *permutações, grupos de simetrias, representação de grupos, órbitas, conjuntos invariantes.*

Estruturas combinatórias em conjuntos II: *grafos, árvores, dígrafos, matrizes de adjacência, caminhos, ciclos, caminhos eulerianos, hamiltonianos.*

Funções geradoras: *séries de potências, exponenciais, de Dirichlet, problemas combinatórios.*

Algoritmos: *eficiência, algoritmos de busca, algoritmos de ordenação.*

Linguagens formais e dinâmica discreta: *sistemas de substituição, autómatos celulares. Chip firing games.*

Seguem-se alguns comentários sobre a adaptação do programa mínimo aos conteúdos acima propostos

A indução matemática sendo muito importante é um tópico que dado por si só facilmente consome duas aulas. Por outro lado, é um tópico que é abordado noutras unidades curriculares de um modo ou de outro. Assim opta-se, aqui, por inseri-lo no contexto de outros tópicos ao longo do semestre. Há sempre muitos conteúdos importantes ou interessantes para serem lecionados, é necessário fazer escolhas.

Não está previsto nos conteúdos mínimos o estudo de estruturas algébricas. Nos cursos de engenharia informática e de matemática aplicada à economia e gestão não há unidade curricular onde sejam lecionados estes tópicos. No curso de matemática existem duas unidades curriculares de álgebra. No curso de inteligência artificial e ciência de dados, iniciado este ano, não existe nenhuma unidade curricular que aborde os tópicos referidos. Assim justificou-se e justifica-se a introdução de algumas noções de álgebra no programa adaptado da matemática discreta. Os semigrupos e monóides, além de estruturantes, permitem sistematizar e produzir exemplos e problemas de contagens. A noção de grupo é um dos conceitos centrais em matemática e física e muita da matemática discreta beneficia desta estrutura e das noções acessórias. O estudo da simetria, das permutações, das matrizes, entre outros, utiliza ou beneficia da teoria de grupos. De igual modo, os anéis, além de produzirem muitos exemplos para problemas de contagens e de teoria de números, são importantes para a aritmética modular, para a teoria de matrizes entre outros tópicos. Os corpos finitos entendem-se melhor com contexto algébrico abstrato, para contraste conceptual.

As funções geradoras são uma ferramenta eficaz, articulada com a análise matemática – certos aspetos de teoria das funções e séries - e que permite resolver problemas de combinatória e de matemática discreta de modo quase surpreendente. Constituem um tópico muito relevante, que aparece em enumeração combinatória, em sistemas dinâmicos, probabilidade, entre muitas outras áreas da matemática. Justifica-se a introdução deste tópico ainda que lecionado de modo introdutório e superficial. Uma referência útil e acessível é a obra de Wilf

H. Wilf, *Generatingfunctionology*, Academic Press 1994.

Sobre o tópico do estudo de algoritmos, optou-se por introduzi-lo essencialmente de modo transversal, articulando com a aritmética modular e outros temas como os grafos e dígrafos, fazendo o estudo dos algoritmos integrado nos algoritmos concretos estudados. Exemplos: o aparecimento do número de ouro na quota para o tempo no algoritmo Euclides estendido; o algoritmo de exponenciação rápida, que pode ser utilizado para aritmética modular, ou para produtos de polinómios ou matrizes. Mas além disso, havendo tempo, dedica-se uma aula sobre este tópico, para discutir a eficiência de algoritmos em abstrato e discutir algoritmos de ordenação, relacionando com o primeiro tópico lecionado de relações de ordens em conjuntos.

As linguagens formais facilmente são lecionadas no contexto da combinatória, em particular, tendo em conta a perspetiva mais focado para a computação na unidade curricular aqui descrita. Logo no início podem ser introduzidas dando certos exemplos no contexto das relações de equivalência e das relações de ordem parciais. Podem ser abordadas, novamente, no âmbito dos exemplos de semigrupos e monóides, o conjunto das palavras com a operação concatenação. No contexto de caminhos em grafos e dígrafos são utilizadas para a enumeração de palavras e fala-se em palavras admissíveis e não admissíveis, associadas a caminhos e a ciclos dos dígrafos. Pode ainda relacionar-se com a enumeração de palavras por recorrências e funções geradoras. Em seguida é possível definir sistemas de reescrita, sistemas de substituição e autómatos celulares, neste contexto. Certos autómatos celulares podem ainda ser definidos utilizando aritmética modular. Deste modo, são tópicos encarados como de síntese, com uma componente computacional muito forte e simultaneamente apelativos. Definido certos autómatos celulares sobre os vértices de grafos obtêm-se os chamados *chip firing games*, *sand pile models* e outras variantes. Estes modelos permitem novas possibilidades de aplicações e simultaneamente amadurecer conteúdos passados, mostrando por exemplo a importância das configurações críticas e o grupo crítico de grafo. Este tipo de tópicos sendo acessíveis do ponto de vista de técnica matemática permitem colocar problemas de investigação atuais.

Método de ensino

Contexto formal

A unidade curricular em causa – matemática discreta - não tem um corpo teórico formalizado, estruturado completo, podendo ser constituída por uma variedade grande de conteúdos relacionados com diferentes áreas da matemática como a combinatória enumerativa, teoria dos números, análise, probabilidade, álgebra, teoria de grafos, entre muitos outros. Tendo em conta o número de alunos e que grande parte dos alunos são de informática, seria aconselhável que a tipologia de aulas fosse $2 \times 2hTP + 2 \times 2hTP$, com duas turmas distintas, com exposição sintética de conteúdos, operacionalização rápida, exercícios de prática e articulação com outros conteúdos. Com entrada em funcionamento do curso de inteligência artificial e ciência de dados serão necessárias três turmas distintas.

Por ocasião da proposta formal da unidade curricular ficou estipulado o figurino $1 \times 2hT + 2 \times 2PL$, a aula teórica com as duas turmas juntas e as práticas-laboratoriais em duas turmas separadas. Apesar de em sala de aula estarem presentes muitos alunos, tem sido sempre possível tornar a aula teórica um pouco prática. Enunciam-se alguns exercícios, consideram-se e propõem-se problemas que surjam de perguntas de alunos e que tornam a aula teórica mais dinâmica e valiosa para quem nela participa. Por outro lado, para ser possível avançar nos conteúdos, as aulas práticas não são puramente práticas, sendo sempre que possível lecionados conteúdos. Havendo neste caso o cuidado de seguir a mesma preparação em ambas as turmas práticas.

No ano letivo, 2023/2024, as turmas ficaram separadas, $2 \times 2hT + 2 \times 2hPL$, tanto nas aulas teóricas como práticas. Uma turma de alunos de engenharia informática e uma turma de alunos de matemática e de matemática aplicada à economia e gestão. Deste modo, tornaram-se informalmente teórico-práticas, apesar do elevado número de alunos por aula, em particular na turma de engenharia informática.

Metodologia

São disponibilizados no *moodle*, aos alunos, *slides* e outros materiais para cada semana, mas as aulas são expositivas de quadro e giz. Parte do interesse da aula teórica e prática depende muito da interação com os alunos a quem são propostos problemas e desafios, frequentemente decorrentes de perguntas e dúvidas colocadas. Existem dúvidas, previsíveis, que a cada ano aparecem recorrentemente. Mas, com frequência, criando o ambiente correto, aparecem também dúvidas surpreendentes, pertinentes e algumas vezes soluções propostas por alunos muito inovadoras que permitem conduzir a aula de um modo não previsto inicialmente.

Deste modo a aula presencial seja teórica ou prática é única e irrepetível. Mas não é imprescindível para se ter aproveitamento uma vez que a matéria alvo de avaliação está disponibilizada nos *slides*, ficheiros, e nas listas de exercícios, assim como *notebooks* em *python* que ilustram e complementam os exemplos trabalhados em aula. Este aspeto é muito importante pois existe a cada ano um número razoável de alunos trabalhadores-estudantes, que não podendo frequentar as aulas presencialmente, são empenhados.

Por cada semana é entregue uma ficha de exercícios. Alguns serão realizados nas aulas práticas outros ficam para trabalho autónomo dos alunos. Na semana seguinte à entrega da ficha é disponibilizada no *moodle* a resolução.

A cada semana são também disponibilizados no *moodle links* de alguns vídeos *youtube* de conteúdos relevantes sobre o que se está a discutir na semana.

Prevê-se que os conteúdos programados sejam lecionados todos em 11 a 12 semanas. Deste modo nas semanas que sobram são realizadas revisões, lecionados conteúdos novos de síntese, que não são avaliados, mas que permitem obter perspetiva global e amadurecer os conteúdos lecionados. Também são propostos exercícios e trabalho com *python*. Neste período, os alunos aperfeiçoam os conhecimentos e alunos que tenham perdido matéria têm oportunidade de recuperar. Serve ainda, este período, para preparação do teste final ou exame.

Exemplos de conteúdos suplementares e síntese, que podem ser lecionados, nas semanas remanescentes:

◊ Transformada de Fourier discreta: sendo dado de modo muito prático e muito operacionalizado, articulam-se conhecimentos de aritmética modular, álgebra linear, funções geradoras.

◊ Quadrados latinos: articulam-se conhecimentos de funções geradores, grupos, contagens.

◊ Sistemas criptográficos: Cifras afins, RSA. Articulam-se conhecimentos de aritmética modular, algoritmo de Euclides, algoritmo de exponenciação rápida, teorema pequeno de Fermat.

◊ Geradores de números pseudo-aleatórios – articulam-se conhecimentos de probabilidade, recorrências, contagens, aritmética modular.

◊ Iteradas de aplicações do intervalo e elementos de dinâmica simbólica: Relaciona-se com as expansões numéricas, com dígrafos e linguagens formais. Enumeração de órbitas periódicas. Ordem de Sharkovsky (exemplo de uma ordenação dos números naturais não trivial).

◊ Outros.

Método de avaliação

A avaliação segue dois regimes: avaliação contínua ou avaliação por exame. A avaliação contínua consiste na realização de testes frequentes, minitestest-*pergunta em aula*, durante o semestre, em sala de aula-prática, com duração de 10 a 15 minutos e um teste final cobrindo toda a matéria.

Os minitestest têm a função de manter a atenção e a prática nos conteúdos à medida que são lecionados, e uma certa segurança na nota. O teste final assegura que os conhecimentos são adquiridos razoavelmente.

A avaliação por exame pressupõe a realização do exame em data a estipular, cobrindo toda a matéria lecionada durante o ano.

O número de minitestest a realizar durante o semestre é ajustável a cada ano. A razão prende-se com alguma incerteza, que se verifica sempre, em relação ao início do ano letivo. Os horários são disponibilizados apenas no início das aulas. Os tipos de salas disponíveis para as aulas práticas só são conhecidos nessa altura. O número de alunos por turma também. Considera-se um número mínimo de 5 minitestest, podendo também serem feitos em todas as aulas práticas.

A nota do conjunto de minitestest é obtida somando as notas e normalizando a 20 valores. Considera-se ainda a possibilidade de não contar para a soma um dos minitestest com pior nota, para também salvaguardar algum imprevisto ou falta não justificada à aula prática. O peso do conjunto de minitestest é 30% sendo o peso do teste final 70%. A nota final é a média ponderada destas duas notas parciais.

O ideal, havendo condições em sala de aula, será no início de cada aula prática a realização de um miniteste cotado a 2 valores, com uma pergunta, durante 10 minutos. Neste caso, havendo o incentivo de cada aluno rever a matéria antes da aula prática permite melhor aprendizagem e rendimento na própria aula.

[illegible]

De seguida descreve-se algum detalhe do programa e da forma como é articulado ao longo do semestre. Em particular explicita-se a forma como os mesmos conteúdos vão sendo abordados diversas vezes em diferentes contextos.

Semana 1

Estruturas combinatórias em conjuntos I.

Revisão de conjuntos. Enumeração de conjuntos. Cardinais. Princípio de inclusão-exclusão. Relações binárias. Relações de equivalência. Conjunto quociente. Relações de ordem parcial, total. Diagrama de Hasse.

São dados exemplos de relações de equivalência relacionados com números. Relação de congruência $\text{mod } n$. Relação de equivalência em conjuntos de palavras, num dado alfabeto. Isto permite ir preparando terreno para desenvolver estes conceitos mais tarde.

Exemplos de relações de ordem relacionados com números: relação divide nos naturais. Relação contido no conjunto das partes de um conjunto dado. Exemplos de relações de ordem dadas em linguística. Explorar informalmente a factorização em números primos e a estruturas de relação de ordem que se obtém. Informalmente explorar as semelhanças (aqui começar a trabalhar a noção de isomorfismo de grafos) de diferentes diagramas de Hasse para diferentes factorizações de números.

Exemplos de uso do princípio de inclusão-exclusão. Referir o seu uso na probabilidade.

Introdução informal de diversos diagramas que representam conjuntos e relações de equivalência. Em particular grafos.

Semana 2

Funções.

Funções injectivas, sobrejectivas, invertíveis. Funções definidas em conjuntos finitos. Composição de funções. Permutações. Conjuntos invariantes. Conjuntos invariantes primitivos. Diferentes notações para permutações. Ciclos. Transposições. Noção informal de órbita. Noção informal de semigrupo, monóide e grupo.

Exemplos variados de funções em diferentes contextos. Enumerar funções em conjuntos finitos dados. Composição de funções usando a notação das permutações.

Explorar através dos exemplos de funções em conjuntos finitos, a existência de elemento neutro, de inverso, de comutatividade, com a operação composição. Determinar órbitas explicitamente através de funções definidas em conjuntos finitos. Introduzir informalmente diagrama de dígrafo para explicitar as órbitas. Introduzir informalmente a noção de ordem de um elemento, neste caso usando permutações. Relacionar a ordem com os conjuntos invariantes existentes. Classificar os conjuntos invariantes, como primitivos e não primitivos.

Semana 3

Teoria elementar dos números.

Factorização em números primos. Máximo divisor comum e mínimo múltiplo comum. Algoritmo da divisão. Algoritmo de Euclides, algoritmo de Euclides estendido. Bases numéricas. Frações contínuas. Números naturais, racionais, algébricos quadráticos, algébricos, reais, complexos. Dízimas.

Algoritmo da divisão. Diferentes métodos para determinar o máximo divisor comum e mínimo múltiplo comum. Factorização de números primos. Iteradas de aplicações do intervalo e expansão em base n . Iteradas de aplicações e fração contínua. Dízimas, números racionais e irracionais. Números quadráticos. Fração contínua

Semana 4

Aritmética modular I.

Determinação de elementos inversos em $\mathbb{Z}_n$. Divisores de zero em $\mathbb{Z}_n$. Função de Euler. Teorema pequeno de Fermat. Grupos de invertíveis, subgrupos, anéis modulares e corpos finitos.

Aprofundamento da aritmética modular introduzida na semana 3. Neste caso considera-se o problema de determinar os elementos invertíveis e os seus inversos em $\mathbb{Z}_n$. Este problema pode ser considerado e relacionado com o algoritmo de Euclides, com o teorema pequeno de Fermat e mais tarde com o algoritmo de exponenciação rápida. São também introduzidos os divisores de zero. Fica aberto o caminho para introduzir as estruturas algébricas formalmente, neste caso no contexto de $\mathbb{Z}_n$. Tabelas da multiplicação e os seus padrões podem ser considerados e analisados de muitos pontos de vista.

Propriedades da função de Euler: exemplo de uso do princípio de inclusão-exclusão.

Semana 5

Aritmética modular II.

Algoritmo de exponenciação rápida. Teorema chinês do resto

Algoritmo de exponenciação rápida no contexto da aritmética modular. Determinação de inversos. Algoritmo de exponenciação rápida noutros grupos como matrizes, ou grupos de invertíveis em anéis do tipo $\mathbb{Q}[\beta]$. Teorema chinês do resto.

Semana 6

Estruturas algébricas I.

Semigrupo, monóide, grupo, anel, corpo, espaço linear. Isomorfismos.

Início do estudo formal das estruturas algébricas. Definições: Operações binárias. Semigrupos. Monóides. Grupos. Anéis, Corpos. Exemplos concretos de estruturas algébricas que aparecem em diversas áreas da matemática. Definição e discussão de espaços lineares e álgebras. Breve referência aos quatérnios. Propriedades básicas de estruturas algébricas. Isomorfismo de estruturas algébricas, com ênfase no caso dos grupos e dos anéis. Exemplos de anéis e corpos do tipo $\mathbb{Q}[\beta]$. São explorados os subgrupos, conjuntos geradores, conjuntos geradores minimais, ordem de elementos.

Semana 7

Estruturas algébricas II.

Grupos. Subgrupos. Ordem de um elemento. Conjuntos geradores. Grupos de transformações. Simetrias. Simetrias dos polígonos regulares. Simetrias de poliedros regulares.

Aprofundamento dos conceitos de teoria de grupos. Definições de subgrupos. Muitos exemplos serão fornecidos em contextos matemáticos muito variados. Ordem de elemento. Conjunto gerador, conjunto gerador minimal. Exemplos de grupos de matrizes, exemplos de grupos e subgrupos de permutações. Grupos de transformações geométricas. Conjuntos invariantes revisitados e simetrias de figuras do plano e figuras no espaço. São explorados os subgrupos, conjuntos geradores, conjuntos geradores minimais, ordem de elementos. Isomorfismos de grupos do tipo $\mathbb{Z}_n^*$ com grupos de simetrias de polígonos.

Semana 8

Estruturas combinatórias em conjuntos II

Grafos. Caminhos, árvores. Isomorfismo de grafos. Caminhos eulerianos, caminhos hamiltonianos. Matriz de adjacência.

Definição de grafo, partindo de conjuntos de vértices e de conjuntos de partes de cardinal 2. Noções elementares, caminhos, ciclos, grafos conexos, árvores, grau de vértice. Isomorfismo de grafos. Invariantes para grafos. Subgrafos, grafo complementar. Caminhos eulerianos e hamiltonianos, condições de existência. Matriz de adjacência. Propriedades algébricas. Relações de equivalência revisitadas.

Semana 9

Estruturas combinatórias em conjuntos III

Digrafos. Caminhos. Ciclos. Matrizes de adjacência. Número de caminhos de comprimento fixo entre vértices dados. Caminhos fechados de comprimento fixo. Matrizes redutíveis, irredutíveis, primitivas.

Definição de digrafo, partindo de conjuntos de vértices e de pares ordenados. Noções elementares, caminhos, ciclos, digrafos conexos e fortemente conexos. Matriz de adjacência. Propriedades algébricas. Estudo do semigrupo dos ciclos de um digrafo. Recorrências e fórmula matricial. Relações de ordem e de equivalência revisitadas.

Semana 10

Funções geradoras.

Séries de potências. Solução de equações às diferenças lineares. Exemplos de problemas de combinatória. Função geradora do número de ciclos num digrafo de comprimento $k \in \mathbb{N}$. Funções geradoras exponenciais, exemplos de problemas de combinatória. Funções geradoras de Dirichlet. Função zeta de Riemann. Função de Mobius. Funções multiplicativas. Função de Euler revisitada.

Semana 11

Algoritmos.

Eficiência. Taxas de crescimento. Comparação de algoritmos

Algoritmos. Operações elementares. Número de operações/memória necessária. Taxas de crescimento notação O . Comparação de diferentes algoritmos. Rever algoritmos lecionados. Algoritmos de ordenação. Algoritmos de grafos.

Semana 12

Linguagens formais - sistemas dinâmicos discretos.

Sistemas de substituição. Autômatos celulares.

Definição de linguagens formais, partindo de conjuntos de palavras num dado alfabeto. Recuperação das noções já introduzidas de operação de concatenação, no âmbito das estruturas algébricas. Condições de admissibilidade. Exemplos de cadeias de Markov topológicas, definidas por uma matriz de transição. Digrafos e linguagens formais. Enumeração de palavras, funções geradoras. Sistemas de substituição. Enumeração. Autômatos celulares. Simulações. Autômatos celulares definidos por funções em aritmética modular. Definição de *chip firing game*. Estudo e simulação de exemplos.

Semana 13

Revisões, aprofundamento de conteúdos, código *python*.

Semana 14

Revisões, aprofundamento de conteúdos, código *python*.

Semana 15

Revisões, aprofundamento de conteúdos, código *python*, preparação para o teste final/exame

Bibliografia comentada

Em geral os livros e as referências são pouco consultados por parte dos alunos. Isso não significa que não se insista e que não se forneçam referências apropriadas. Existe um esforço de seguir partes dos conteúdos de modo próximo a obras de referência, para que os alunos possam ter acesso a material adicional se precisarem, e dominarem diferentes notações e abordagens.

No entanto o material disponibilizado no *moodle* é suficiente para aprovação na unidade curricular. Os recursos disponíveis *on-line* são valiosos e abundantes, em particular vídeos, pelo que existe uma constante atualização de *links*, sendo os alunos incentivados a descobrir novos e a partilharem em fórum *moodle*.

A experiência de anos anteriores dá indicações que vídeos curtos sintéticos são os mais eficazes no progresso do aluno e na aprendizagem. Vídeos mais longos, por mais bem feitos que estejam, tornam-se pouco apelativos e pouco utilizados.

Referências principais

[B] Norman Biggs, Discrete Mathematics, Oxford Science Publications. Reprinted 1993.

[C] Peter Cameron, Combinatorics, Topics, Techniques, Algorithms, Cambridge University Press, 1994

Referências avançadas ou complementares

[RLF-MR] Rui Loja Fernandes, Manuel Ricou, *Introdução à álgebra*, IST Press 15. ()

[M] Elementos de Álgebra - Luiz Monteiro, IMPA
<https://edisciplinas.usp.br/mod/resource/view.php?id=2926192&forceview=1>

[Buch] Johannes Buchmann, *Introduction to cryptography*, Springer Verlag. (2001)

[JHL-RMW] Lint, Wilson, *A course in combinatorics*, Cambridge, 2Ed. (2001)

[CKY] Chee Keng Yap, *Fundamental problems of algorithmic algebra*, Oxford. (2000)

Sobre as referências indicadas

[B] Capítulos com temas abordados. Os conteúdos desenvolvidos em cada um destes capítulos vai muito além do que é necessário para a unidade curricular. De qualquer modo esta referência é mais acessível e completa em relação ao pretendido na unidade curricular do que a [C].

1. Integers
2. Functions and counting
3. principles of counting
5. Partition, classification, and distribution
6. Modular arithmetic
7. Algorithms and their efficiency
8. Graphs
- 9 Trees, sorting and searching
- 11 Digraphs, networks and flows
- 13 Groups
- 14 Groups of permutations
- 15 Rings, fields and polynomials
- 18 Generating functions

[C] Capítulos com temas abordados. Os conteúdos desenvolvidos em cada um destes capítulos vai muito além do que é necessário para a unidade curricular.

2. On numbers and counting
3. Subsets, partitions, permutations.
4. Recurrence relations and generating functions

5. The principle of inclusion exclusion.

11. Graphs

12. Posets, lattices and matroids

14. Automorphism groups and permutation groups

[RLF-MR] Livro complementar à matéria lecionada nos conteúdos de álgebra. Muitos exemplos variados, relações com outras áreas da matemática, por exemplo a geometria e aritmética, exercícios, e tópicos avançados expostos de modo completo e acessível.

[M] Livro complementar à matéria lecionada em particular nos tópicos: Conjuntos, Anéis e corpos: páginas 166-190, Grupos: Introdução, Propriedades gerais dos grupos, grupos cíclicos e grupos de permutações 444-477.

Recursos *on-line*

Uma série de recursos digitais são disponibilizados. A título de exemplo seguem-se os principais:

Python - plataforma Anaconda

IDE: *Jupyter*, *Spyder*.

<https://www.anaconda.com/products/individual>

Anaconda é uma plataforma de distribuição de linguagens de programação *Python*, *R*, entre outras aplicações de tratamento de dados, visualização gráfica, etc.

Jupyter - Vantagem do uso integrado, num *notebook*, de código, texto *markdown* ou *LaTeX*.

Package *python* apropriada para grafos, digrafos ou redes complexas: *Networkx*

<https://networkx.org/documentation/stable/>

Editor de *LaTeX* - processador de texto matemático.

<https://miktex.org/>

Editor de *Latex Overleaf*

<https://www.overleaf.com/>

Sociedade portuguesa de matemática

<https://www.spm.pt/>

Impa – Instituto de matemática pura e aplicada - Brasil

<https://impa.br/>

Math.stackexchange-

<https://math.stackexchange.com/>

Fórum de perguntas e repostas sobre matemática. Existem fóruns equivalentes para outras áreas como informática, física e outras. Especialistas de topo ou curiosos respondem às perguntas mais variadas, das mais simples às mais complicadas. Muito útil. Fortemente recomendado.

Repositório *on-line* de pré-publicações - ArXiv

Nas áreas da matemática, computação, física, entre outras.

<https://arxiv.org/>

GitHub - plataforma de partilha de código.

<https://github.com/>

GitHub é uma plataforma de partilha de código que permite a gestão de versões, de atualizações e de desenvolvimento de código em colaboração. Para aplicações à matemática existem muitos códigos específicos em *python*, ou outras linguagens, de livre acesso.

Videos *on-line*

Ligações sobre temas específicos

Divisibilidade, máximo divisor comum, algoritmo de Euclides(40 min)

<https://www.youtube.com/watch?v=o7axlIFY3Ko>

Congruências, pequeno teorema de Fermat(21min)

<https://www.youtube.com/watch?v=qYqusyUOtFO>

Sobre o pequeno teorema de Fermat(11min)

<https://www.youtube.com/watch?v=eYzxLI9pc-8>

Aplicações do pequeno teorema de Fermat(5min)

https://www.youtube.com/watch?v=m_69JCcCkCs

Cálculo de exponenciação rápida(21min)

<https://www.youtube.com/watch?v=nEloSK0VhEM>

Sistemas de congruências(8min)

<https://www.youtube.com/watch?v=E0g4DxccC6M>

Teorema chinês do resto(11min)

<https://www.youtube.com/watch?v=ZJcd8t2z8dQ>

Grupos(15min)

https://www.youtube.com/watch?v=g7L_r6zw4-c&t=142s

Tabelas de multiplicação – grupos(7min)

<https://www.youtube.com/watch?v=BwHspSCXFNM>

Subgrupos – teorema de Lagrange(9min)

https://www.youtube.com/watch?v=TCcSZEL_3CQ

Permutações-ciclos(12min)

<https://www.youtube.com/watch?v=MpKG6FmclHk>

Corpos e anéis(7min)

https://www.youtube.com/watch?v=_RTHvweHlhE

Grupos simétricos(5min)

<https://www.youtube.com/watch?v=3aNeCWRjh8I>

Unidades em anéis(7min)

<https://www.youtube.com/watch?v=HHpODrFZ4YQ>

Grafos(16min)

<https://www.youtube.com/watch?v=LFKZLXVO-Dg>

Notação O – programadores(20min)

<https://www.youtube.com/watch?v=BgLTDT03QtU>

Ligações sobre temas de interesse

Computadores mecânicos. Computadores analógicos. Computadores digitais. Veritasium.

<https://www.youtube.com/watch?v=IgF3OX8nT0w>

Integração mecânica. Computação mecânica.

https://www.youtube.com/watch?v=s-y_InzWQjk

Equação logística. Teoria do caos. Veritasium.

<https://www.youtube.com/watch?v=ovJcsL7vyrk>

Mandelbolbo – quaterniões.

<https://www.youtube.com/watch?v=xO5fXGqeM5c>

Conjunto de Mandelbrot – complexos.

<https://vimeo.com/349434513>

FFT – fast Fourier transform. Um dos algoritmos mais importantes para aplicações e teoria.

<https://www.youtube.com/watch?v=nmgFG7PUHfo>

<https://www.youtube.com/watch?v=h7apO7q16V0>

Exposição intuitiva da série de Fourier – síntese.

<https://www.youtube.com/watch?v=ds0cmAV-Yek>

Interpretação visual da transformada de Fourier. Exemplo de filtros de som.

<https://www.youtube.com/watch?v=spUNpyF58BY>

Carlos Ramos

Universidade de Évora, novembro de 2024