

Bacharelado em ciência da computação

Matemática discreta

Lista de exercícios

8 de abril de 2024

## 1 Lógica

1. [CM] Prove que se  $A$ ,  $B$  e  $C$  são proposições, então

- (a)  $F \Rightarrow A$ , ou seja, a partir de uma proposição falsa pode-se concluir qualquer coisa
- (b)  $(A \Rightarrow B) \equiv ((\neg B) \Rightarrow (\neg A))$ , também conhecida como *contrapositiva* da implicação. Uma “prova de  $A \Rightarrow B$  por contrapositiva” é uma prova de que  $((\neg B) \Rightarrow (\neg A))$
- (c)  $(A \Rightarrow F) \equiv \neg A$ , ou seja, uma implicação cujo consequente é falso só pode ser verdadeira se o antecedente é falso. Este é o princípio por baixo das “provas por contradição”
- (d)  $((A \Rightarrow B) \vee (A \Rightarrow C)) \equiv (A \Rightarrow (B \vee C))$  (distributividade da disjunção pela implicação)
- (e)  $((A \Rightarrow B) \wedge (A \Rightarrow C)) \equiv (A \Rightarrow (B \wedge C))$  (distributividade da conjunção pela implicação)
- (f)  $((B \Rightarrow A) \vee (C \Rightarrow A)) \equiv ((B \wedge C) \Rightarrow A)$  (outra distributividade)
- (g)  $((B \Rightarrow A) \wedge (C \Rightarrow A)) \equiv ((B \vee C) \Rightarrow A)$  (outra distributividade)
- (h)  $((A \Rightarrow B) \wedge (A \Rightarrow (\neg B))) \equiv (\neg A)$  (outra maneira de expressar o princípio por baixo de uma prova por contradição)

2. [SDB 3] Mostre que  $p \oplus q$  é equivalente a  $(p \wedge \neg q) \vee (\neg p \wedge q)$

3. [CM] Considere os seguintes predicados

$$I(x) \equiv x \in Z$$

$$P(f, x) \equiv I(x) \Rightarrow I(f(x))$$

$$Q(f, x) \equiv I(f(x)) \Rightarrow I(x)$$

Dê um exemplo de função  $g : R \rightarrow R$  que

- (a) satisfaz o predicado  $P(g, x), \forall x \in R$
  - (b) não satisfaz o predicado  $P(g, x), \forall x \in R$
  - (c) satisfaz o predicado  $\neg(P(g, x), \forall x \in R)$
  - (d) satisfaz o predicado  $Q(g, x), \forall x \in R$
  - (e) não satisfaz o predicado  $Q(g, x), \forall x \in R$
  - (f) satisfaz o predicado  $\neg(Q(g, x), \forall x \in R)$
4. [SDB 3] Construa uma prova de que, se  $m$  é ímpar, então  $m^2$  é ímpar
5. [SDB 3] Prove que, para todos os inteiros  $m$  e  $n$ , se  $m$  é ímpar e  $n$  é ímpar, então  $mn$  é ímpar
6. [SDB 3] Construa uma prova de que, se  $m$  é um inteiro tal que  $m^2$  é par, então  $m$  é par
7. [AL] Construa a tabela verdade para a seguinte proposição:

$$E = (p \vee (\neg p \vee q)) \wedge \neg(q \wedge \neg r)$$

8. [AL] Mostre se as expressões  $E_1$  e  $E_2$  são equivalentes logicamente:

$$E_1 = (s \rightarrow (p \wedge \neg r)) \wedge ((p \rightarrow (r \vee q)) \wedge s)$$

$$E_2 = (p \wedge q \wedge \neg r \wedge s) \vee \neg(p \vee s)$$

9. [AL] Faça a simplificação lógica da seguinte expressão:

$$(p \wedge (\neg(\neg p \vee q))) \vee (p \wedge q)$$

10. [AL] Mostre se o seguinte argumento é válido ou não. Em cada passo, identifique a razão para se obter a conclusão:

(a)  $\neg p \rightarrow (r \wedge \neg s)$

(b)  $t \rightarrow s$

(c)  $u \rightarrow \neg p$

(d)  $\neg w$

(e)  $u \vee w$

(f)  $\therefore \neg t \vee w$

11. [AL] O famoso detetive Percule Hoirot foi chamado para resolver um assassinato misterioso. Ele determinou os seguintes fatos:

(a) Lord Charles, o homem assassinado, foi morto com uma pancada na cabeça com um castiçal

(b) Ou Lady Camila ou a empregada Sara estavam na sala de jantar no momento do assassinato

(c) Se o cozinheiro estava na cozinha no momento do assassinato, então o açougueiro matou Lord Charles com uma dose fatal de arsênico

(d) Se Lady Camila estava na sala de jantar no momento do assassinato, então o motorista matou Lord Charles

(e) Se o cozinheiro não estava na cozinha no momento do assassinato, então Sara não estava na sala de jantar quando o assassinato ocorreu

(f) Se Sara estava na sala de jantar no momento do assassinato, então o ajudante pessoal de Lord Charles o matou

É possível para o detetive Percule Hoirot deduzir quem matou Lord Charles? Se sim, quem é o assassino?

12. [AL] Seja a tabela verdade do operador  $\odot$ :

| $p$ | $q$ | $p \odot q$ |
|-----|-----|-------------|
| $F$ | $F$ | $V$         |
| $F$ | $V$ | $F$         |
| $V$ | $F$ | $F$         |
| $V$ | $V$ | $V$         |

(a) O operador  $\odot$  segue a lei da associatividade com o operador  $\wedge$ ? Ou seja,  $(x \odot y) \wedge z \equiv x \odot (y \wedge z)$ ?

(b) O operador  $\odot$  segue a lei da distributividade com o operador  $\wedge$ ? Ou seja,  $x \odot (y \wedge z) \equiv (x \odot y) \wedge (x \odot z)$ ?

13. [AL] Mostre se o seguinte argumento é válido ou não:

- (a)  $(p \wedge \neg q) \rightarrow r$
  - (b)  $p \vee q$
  - (c)  $q \rightarrow p$
  - (d)  $\therefore r$
14. [AL] Considere a string de números “0204”. Seja a seguinte afirmação:  $\forall x$ , se  $x == 1$  e  $x$  é um caractere na string “0204”, então  $x$  está à esquerda de todos os 0’s na string. Essa afirmação é verdadeira?
15. [AL] Diga se a forma do argumento abaixo é válida ou não, apresentando a justificativa:
- (a) Todas as pessoas saudáveis comem uma banana por dia
  - (b) João não é uma pessoa saudável
  - (c)  $\therefore$  João não come uma banana por dia
16. [AL] Prove que  $\min(x, y) + \max(x, y) = x + y$  para quaisquer números reais  $x$  e  $y$
17. [AL] Prove que se  $n = ab$ , sendo  $a, b \in \mathbb{Z}^+$ , então  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$

## 2 Teoria dos números

1. [JG] Mostre que, se  $m, n, p, q$  forem inteiros tais que  $n \mid p$  e  $m \mid q$ , então  $nm \mid pq$
2. [JG] Mostre que, se  $n = 25, 100$  ou  $169$ , então  $n$  é um quadrado perfeito e é uma soma de *outros* dois quadrados perfeitos
3. [JG] Mostre que, para todo inteiro  $n$ , o número  $3(n^2 + 2n + 3) - 2n^2$  é um quadrado perfeito
4. [SDB] Se  $a \cdot 133 - 2m \cdot 277 = 1$ , isso garante que  $a$  tenha um inverso multiplicativo em  $\text{mod } m$ ? Se sim, qual seria? Se não, por quê?
5. [SDB] Calcule o MDC de 210 e 126 usando o algoritmo de Euclides (mostrar o passo-a-passo)
6. [SDB] Escreva um pseudocódigo que, dados os inteiros  $a, b, n$  em  $\mathbb{Z}_n$ , calcule um  $x$  tal que  $a \cdot_n x = b$  ou conclua que não existe tal  $x$
7. [SDB] Encontre uma equação da forma  $a \cdot_n x = b$  em  $\mathbb{Z}_n$  que tenha uma única solução, mas sem que  $a$  e  $n$  sejam primos entre si, ou prove que essa equação não existe. Em outras palavras, prove a afirmação de que, se  $a \cdot_n x = b$  tem uma única solução em  $\mathbb{Z}_n$ , então  $a$  e  $n$  são primos entre si, ou encontre um contraexemplo
8. [SDB] Escreva a tabela de multiplicação  $\cdot_7$  para  $\mathbb{Z}_7$
9. [SDB] Os números 29 e 43 são primos. Calcule:
  - (a) o valor de  $(29 - 1)(43 - 1)$
  - (b) o valor de  $199 \cdot 1111$  em  $\mathbb{Z}_{1176}$
  - (c) o valor de  $(23^{1111})^{199}$  em  $\mathbb{Z}_{29}$
  - (d) o valor de  $(23^{1111})^{199}$  em  $\mathbb{Z}_{43}$
  - (e) o valor de  $(23^{1111})^{199}$  em  $\mathbb{Z}_{1247}$

10. [SDB] Quantas soluções com  $x$  entre 0 e 34 existem para o sistema de equações

$$\begin{cases} x = 4 \bmod 5 \\ x = 5 \bmod 7 \end{cases}$$

? Quais são essas soluções?

11. [SDB] Mostre que em  $\mathbb{Z}_p$ , se  $a^i \bmod p = 1$ , então  $a^n \bmod p = a^{n \bmod i} \bmod p$
12. [SDB] A relação de “congruência do módulo  $n$ ” é indicada por  $\equiv$ , e definida por  $x \equiv y \pmod{n}$  se, e somente se,  $x \bmod n = y \bmod n$ . Mostre que a congruência do módulo  $n$  é uma relação de equivalência ao indicar que ela é reflexiva, simétrica e transitiva
13. [SDB] Determine todos os números, se houver,  $a \in \mathbb{Z}_9$  diferentes de 1 e 8 (note que  $-1 \bmod 9 = 8$ ) de tal forma que  $a^8 \bmod 9 = 1$
14. Implemente (em C ou C++) o algoritmo de Euclides estendido que recebe como entrada dois números inteiros  $a, b$  e imprime a equação  $a \cdot i + b \cdot j = \text{MDC}(a, b)$ . Note que o programa deve imprimir a equação “por extenso”, onde seja possível visualizar os valores de  $i, j, \text{MDC}(a, b)$ , que são as saídas do programa. Para este exercício em particular, envie o arquivo `.c` ou `.cpp` para o email do professor até o início da aula na data de entrega.

### 3 Indução e recorrência

1. [EM] Note que  $1 \equiv 1 \bmod 3$ ,  $10 \equiv 1 \bmod 3$ ,  $100 \equiv 1 \bmod 3$ . Prove por indução que  $10^n \equiv 1 \bmod 3$  para todo  $n \geq 0$
2. [JG] Prove por indução que, para todo inteiro  $n > 1$ :

$$2^{n+1} < 3^n$$

3. [JG] Prove por indução que, para todo inteiro  $n \geq 1$ :

$$2 + 6 + 10 + \dots + (4n - 2) = 2n^2$$

4. [JG] Prove por indução que, para todo inteiro  $n \geq 1$ :

$$2 + 4 + 6 + \dots + 2n = n(n + 1)$$

5. [JG] Prove por indução que, para todo inteiro  $n \geq 1$ :

$$1 + 3 + 6 + \dots + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{6}$$

6. [JG] Prove por indução que, para todo inteiro  $n > 1$  e  $r \neq 1$ :

$$a + ar + ar^2 + \dots + ar^{n-1} = \frac{a - ar^n}{1 - r}$$

(soma dos  $n$  primeiros termos de uma progressão geométrica)

7. [JG] Prove por indução que, para todo inteiro  $n > 1$ ,  $3^{2n} + 7$  é divisível por 8

8. [JG] Prove por indução que, para todo inteiro  $n > 1$ ,  $n^3 - n$  é divisível por 3
9. [JG] O que está errado na seguinte demonstração por indução? Vamos provar que, para qualquer inteiro positivo  $n$ ,  $n = 1 + n$ . Suponha que  $P(k) : k = k + 1$  é verdadeira. Somando 1 aos dois lados da equação, obtemos  $k + 1 = k + 2$ . Portanto,  $P(k + 1)$  é verdadeira.
10. [JG] Prove a seguinte propriedade dos números de Fibonnaci para  $n \geq 1$ :

$$F(n + 6) = 4F(n + 3) + F(n)$$

11. [JG] Uma sequência é definida por recorrência por

$$\begin{cases} S(0) = 1 \\ S(1) = 1 \\ S(n) = 2S(n - 1) + S(n - 2), \text{ para } n \geq 2 \end{cases}$$

Mostre que  $S(n) < 6S(n - 2)$  para  $n \geq 4$

12. [JG] Dê uma definição recorrente para o fatorial  $(n!)$ , para  $n \geq 1$
13. [JG] Resolva a recorrência:

$$\begin{cases} S(1) = 1 \\ S(n) = S(n - 1) + 2n - 1, \text{ para } n \geq 2 \end{cases}$$

14. [JG] Resolva a recorrência:

$$\begin{cases} P(1) = 1 \\ P(n) = 2P(\frac{n}{2}) + n^2, \text{ para } n \geq 2, n = 2^m \end{cases}$$

## 4 Combinatória e máquinas de estado finita

### Instruções para entrega dos exercícios desta seção

- Escreva, à mão, a resolução das questões em folhas de caderno/sulfite, como nas outras listas. Não é necessário copiar os enunciados.
- Tire uma foto por página da resolução, com cuidado para gerar imagens nítidas nas quais o conteúdo das suas resoluções esteja legível.
- As imagens podem estar no formato **jpg** ou **png**. Se preferir, também pode enviar arquivos **pdf**.
- Enumere os arquivos para indicar a ordem de leitura. Por exemplo, **1.jpg**, **2.jpg**, ...
- Envie as imagens anexadas para o email do professor até o início da aula na data de entrega estipulada.
- O professor enviará uma confirmação de que recebeu sua entrega. Se isso não acontecer em algumas horas, envie um novo email para o professor para resolver a situação.

1. [CM] Um *palíndromo* sobre um conjunto  $A$  é uma sequência  $(a_1, \dots, a_k)$  de elementos de  $A$  que “permanece a mesma quando lida na ordem reversa”, ou seja,

$$a_i = a_{k-i+1}, \text{ para todo } 1 \leq i \leq k$$

- (a) Enumere todos os palíndromos de tamanho 4 sobre  $a, b, c$
  - (b) Enumere todos os palíndromos de tamanho 5 sobre  $a, b, c$
  - (c) Qual o número de palíndromos de tamanho  $k$  sobre um conjunto de  $n$  elementos?
2. [SDB] Um clube de tênis possui  $2n$  membros. Queremos emparelhar os membros para partidas individuais. (simplifique o máximo possível das expressões obtidas)
    - (a) De quantas maneiras podemos emparelhar os membros do clube?
    - (b) Agora suponha que, além de especificar quem joga com quem, também queremos determinar quem saca primeiro em cada partida. De quantas maneiras podemos especificar nossos pares?
  3. [AL] Um grupo de oito pessoas está indo ao cinema e todos vão sentar na mesma fileira. Duas dessas pessoas não querem sentar uma ao lado da outra. De quantas formas diferentes as oito pessoas podem ser dispostas na fileira?
  4. [JG] Uma senha para acessar um sistema computacional consiste em três letras seguidas de dois dígitos. Quantas senhas diferentes existem para acessar esse sistema? E se diferenciarmos maiúsculas de minúsculas?
  5. [JG] Uma rede de computadores é composta pelos nós  $A, B, C, D$ . Existem dois caminhos entre  $A$  e  $C$ , dois entre  $B$  e  $D$ , três entre  $A$  e  $B$  e quatro entre  $C$  e  $D$ . Por quantas rotas diferentes pode-se mandar uma mensagem de  $A$  para  $D$ ?
  6. [JG] Um prédio comprou um novo sistema de fechadura para seus 175 apartamentos. Uma fechadura é aberta digitando um código de dois algarismos. O síndico do edifício fez uma compra inteligente? Justifique com os cálculos de contagem que vimos na disciplina.
  7. [CM] Um protocolo de comunicação usa três tipos de pacotes de dados,  $T_1, T_2, T_3$ , diferenciados por um campo inicial que identifica o tipo do pacote. Os pacotes do tipo  $T_1$  possuem 4 bits de dados após o campo inicial, os pacotes do tipo  $T_2$  tem 8 bits de dados e os pacotes do tipo  $T_3$  tem 10 bits de dados. Qual o número de pacotes distintos que existem nesse protocolo?
  8. [CM] Quantos são os inteiros positivos menores ou iguais a 1000 que são divisíveis por 3 ou por 5 ou por 7? (dica: utilize o princípio da inclusão-exclusão)
  9. [JG] Considere um baralho padrão, com 52 cartas divididas em 4 naipes:
    - (a) Quantas cartas devem ser retiradas para se obter, com certeza, duas cartas do mesmo naipe?
    - (b) Quantas cartas devem ser retiradas para se obter, com certeza, uma carta de naipe preto?
  10. [JG] Considere uma rede de computadores com 60 nós, projetada para suportar a falha de até 2 nós. De quantas maneiras 1 ou 2 nós podem falhar, de forma que a rede ainda vai continuar funcionando?
  11. [JG] Um elevador em um prédio de três andares serve os andares 1, 2 e 3. Um sinal indica para que o elevador suba ou desça (S ou D) e o andar de onde o elevador foi requisitado. O elevador responde ao sinal de entrada movendo-se para o andar correto. Por exemplo, se o elevador estiver no andar 1 e receber um sinal D-3, ele se move para o andar 3. Desenhe a máquina de estados finita que descreve o comportamento do elevador.
  12. [JG] Construa uma máquina de estados finita que reconheça cadeias compostas inteiramente de qualquer quantidade (inclusive nenhum) de pares "01" ou cadeias compostas inteiramente por dois algarismos "1" seguidos de qualquer quantidade (inclusive nenhum) de algarismos "0".

13. [JG] Considere uma máquina de estados finita que retarda a entrada, com os alfabetos de entrada e saída iguais a  $0, 1$ . Por exemplo, se a entrada for  $a_1a_2a_3 \dots$ , a saída deve ser  $00a_1a_2a_3 \dots$  (o primeiro zero é o da primeira execução do estado inicial, que ignoramos, e o segundo zero efetivamente retarda a entrada).
- (a) Construa a máquina descrita
  - (b) Explique, intuitivamente, por que não é possível construir uma máquina de estados finita que produza, para qualquer entrada  $a_1a_2a_3 \dots$ , a sequência de saída  $0a_10a_20a_3 \dots$
14. [JG] Construa uma máquina de estados finita que calcula o complemento de dois<sup>1</sup> de um número binário. Considere que a entrada começa pelos bits menos significativos.
- (a) Use a máquina construída para encontrar os complementos de dois de  $010101$  e de  $110011$

---

<sup>1</sup>Veja [https://pt.wikipedia.org/wiki/Complemento\\_para\\_dois](https://pt.wikipedia.org/wiki/Complemento_para_dois)