Lógica e Computabilidade 2024-2

Hugo Nobrega

Lista de Exercícios 3+4

As entregas podem ser feitas em duplas, mas lembre-se que
não poderá haver repetição de duplas em listas diferentes!
Entregue todas as questões marcadas com * até
13/12 às 20:00

Questão 1. Considere uma assinatura com dois símbolos para relações: P (unário) e R (binário). Prove ou refute o que é afirmado em cada item abaixo. Lembrete: nossos modelos sempre têm universos não vazios.

a. $P(x) \vDash P(x)$

b. $P(x) \vDash P(y)$

c. $P(x) \vDash \forall x\, P(x)$

d. $\forall x\, P(x) \vDash P(x)$

e. $\forall x\, P(x) \vDash \exists x\, P(x)$

f. $\exists x\, P(x) \vDash \forall x\, P(x)$

g. $\forall x\, \exists y\, (xRy) \vDash \exists x\, \forall y\, (xRy)$

* **h.** $\exists x\, \forall y\, (xRy) \vDash \forall x\, \exists y\, (xRy)$

i. $\vDash \exists x\, (P(x) \to \forall y\, (P(y)))$

j. $\varphi \vDash \forall x\, \varphi$

* **k.** Se x não ocorre livre em φ, então $\varphi \vDash \forall x\, \varphi$

l. $\vDash \varphi$ se, e somente se, $\vDash \forall x\, \varphi$

Questão 2. Chamamos de *modelagem* o processo de formalizar (simbolizar) frases ou argumentos da linguagem natural para a LPO usando alguma assinatura apropriada. Deve-se indicar a correspondência entre os componentes da frase de linguagem natural e os símbolos da linguagem formal.

Por exemplo, para a frase “eu nunca como manga e bebo leite no mesmo dia”, poderíamos ter:

Lingugem natural	Simbólico
eu como manga no dia x	$M(x)$
eu bebo leite no dia x	$L(x)$

também estipulando que as variáveis $x, y, z, \ldots$ correspondem a dias.

De acordo com essa correspondência, a frase dada cima pode ser modelada por

$$\forall x \, \neg(M(x) \wedge L(x)).$$

Cada frase pode ser modelada de diversas formas diferentes.

Dê modelagens para cada frase abaixo.

a. "Ninguém gosta de todo mundo", usando

Linguagem natural	Simbólico
x gosta de y	$G(x, y)$

*** b.** "Toda pessoa que tem um filho deveria ser carinhosa com ele", usando

Linguagem natural	Simbólico
x é pai de y	$P(x, y)$
x deveria ser carinhoso com y	$C(x, y)$

c. "Você consegue enganar algumas pessoas em alguns momentos, mas não consegue enganar todas as pessoas em todos os momentos", usando

Linguagem natural	Simbólico
x é uma pessoa	$P(x)$
x é um momento	$M(x)$
você consegue enganar x em y	$E(x, y)$

d. "Nem toda fruta é gostosa, algumas são, mas nenhuma fruta cítrica é", usando

Linguagem natural	Simbólico
x é gostosa	$G(x)$
x é cítrica	$C(x)$

Questão 3. Em cada item abaixo, defina uma assinatura e encontre uma sentença φ dessa assinatura com a propriedade desejada. Lembre-se de que você tem liberdade de colocar os símbolos que quiser na assinatura, podendo então usar φ para fazê-los "se comportarem" de alguma forma desejada em cada modelo.

Por exemplo, para "os modelos de φ têm exatamente 1 elemento", poderíamos ter uma assinatura vazia e fazer φ ser $\forall x \, \forall y \, (x = y)$.

a. Para um dado $k \geqslant 1$ fixo: os modelos de φ são grafos (direcionados[1]) k-coloríveis[2].

[1]Aqui, *grafos direcionados* são compostos por um conjunto não-vazio de vértices e uma relação binária sobre eles. Permitimos laços.

[2]Um grafo direcionado é k-colorível se existe um forma de colorir seus vértices usando no máximo k cores, de forma que vértices distintos vizinhos recebam cores distintas.

b. Os modelos de φ são *torneios* (grafos direcionados, sem laços, tais que entre qualquer par de vértices distintos existe exatamente uma aresta direcionada)

* **c.** Os modelos de φ são grafos direcionados acíclicos (*DAGs*).

Você pode usar o seguinte teorema que nós não provamos: um grafo direcionado é acíclico sse possui uma *ordenação topológica*, que é uma ordenação de seus vértices de maneira que, para toda aresta direcionada $u \to v$, temos que u vem antes de v na ordenação.

d. Os modelos de φ são cografos (definição dada na Lista 1).

Você pode usar o seguinte teorema que nós não provamos: todo grafo que não possui P_4 como subgrafo induzido é um cografo.

e. Os modelos de φ são grupos abelianos.

Questão 4. Sejam $\mathcal{A}$ uma assinatura e $\$_0$, $\$_1$ estruturas para $\mathcal{A}$. Dizemos que $\$_0$ é uma *subestrutura* de $\$_1$ se

- o domínio $D(\$_0)$ de $\$_0$ é um subconjunto do domínio $D(\$_1)$ de $\$_1$, i.e.,

$$D(\$_0) \subseteq D(\$_1)$$

- para cada símbolo para constante c de $\mathcal{A}$, temos

$$c^{\$_0} = c^{\$_1}$$

- para cada símbolo para operação n-ária op de $\mathcal{A}$ e cada $d_0, \ldots, d_{n-1} \in D(\$_0)$, temos

$$\mathrm{op}^{\$_0}(d_0, \ldots, d_{n-1}) = \mathrm{op}^{\$_1}(d_0, \ldots, d_{n-1})$$

- para cada símbolo para relação n-ária R de $\mathcal{A}$ e cada $d_0, \ldots, d_{n-1} \in D(\$_0)$, temos

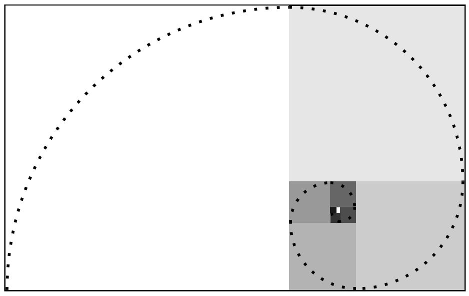
$$R^{\$_0}(d_0, \ldots, d_{n-1}) \text{ é verdadeira} \quad \Longleftrightarrow \quad R^{\$_1}(d_0, \ldots, d_{n-1}) \text{ é verdadeira}$$

Suponha que $\$_0$ seja subsestrutura de $\$_1$ e seja φ uma fórmula da LPO na assinatura $\mathcal{A}$, sem ocorrências de quantificadores, e tal que $\exists x\, \varphi$ é uma sentença.

Prove que se $\$_0 \vDash \exists x\, \varphi$ então $\$_1 \vDash \exists x\, \varphi$, mas que a recíproca não é necessariamente verdadeira.

Questão 5. Seja $\mathcal{A}$ uma assinatura com um símbolo para constante u, com dois símbolos para operações binárias $\oplus$, $\odot$ e um símbolo para relação binária $\lhd$. Seja $\$_{\mathbb{R}}$ a estrutura para essa assinatura que tem o conjunto dos reais $\mathbb{R}$ como domínio e que interpreta u como 1, as operações $\oplus$, $\odot$ respectivamente como adição e multiplicação, e a relação $\lhd$ como "estritamente menor que".

a. A equação $x^2 = x+1$ tem duas soluções reais; a maior delas é um número chamado *razão áurea.* Esse número é famoso pois, por exemplo, a sua n-ésima potência se aproxima do n-ésimo número de Fibonacci conforme $n \to \infty$, e também por supostamente ser "agradável" para os olhos: a razão áurea é a proporção do retângulo do qual, se retirarmos do "canto" do retângulo um quadrado de lado igual ao menor lado do retângulo, o retângulo restante tem a mesma proporção do original:



Escreva uma fórmula da assinatura $\mathcal{A}$ que defina a razão áurea em $\$_{\mathbb{R}}$.

*** b.** Prove que todo número inteiro é definível em $\$_{\mathbb{R}}$.
Dica: não se preocupe em fazer uma definição "eficiente" ou "esperta"!

*** c.** Um número *racional* é um número que pode ser escrito como uma fração com numerador e denominador inteiros.
Prove que todo racional é definível em $\$_{\mathbb{R}}$.

*** d.** Prove que *qualquer* raiz[3] de polinômio com coeficientes racionais é definível em $\$_{\mathbb{R}}$.
Dica: primeiro mostre que a *maior* raiz de um dado polinômio com coeficientes racionais é definível, depois que a *segunda maior* raiz também é definível, etc.

***Questão 6.** Prove que $\varphi, \psi \vdash \beta$, onde

$$\begin{aligned}
\varphi &:= \forall x\, [(F(x) \wedge G(x)) \to H(x)] \quad \to \quad \exists x\, [F(x) \wedge (\neg G(x))] \\
\psi &:= \forall x\, [F(x) \to G(x)] \quad \vee \quad \forall x\, [F(x) \to H(x)] \\
\beta &:= \forall x\, [(F(x) \wedge H(x)) \to G(x)] \quad \to \quad \exists x\, [\langle F(x) \wedge G(x) \rangle \wedge \neg H(x)]
\end{aligned}$$

Questão 7. Em cada item abaixo, escreva uma máquina de Turing que aceite a linguagem dada.

*** a.** $\{w \in \{x, y\}^* \text{ ; as quantidades de } x\text{'s e de } y\text{'s em } w \text{ são iguais}\}$.

b. $\{w \in \{x, y, z\}^* \text{ ; } \exists n \in \mathbb{N} \,.\, w = x^n y^n z^n\}$

[3] *Lembrete*: uma *raiz* de um polinômio p é um número r tal que $p(r) = 0$.

*** c.** $\{w \in \Sigma^* \ ; \ w$ é um palíndromo$\}$ (um *palíndromo* é uma palavra que é igual ao seu próprio reverso, i.e., é uma palavra que é igual lida de frente pra trás ou de trás pra frente, como "socorram-me, subi no ônibus em Marrocos" se você ignorar acentos, pontuação, espaços e se as letras são maiúsculas/minúsculas).

***Questão 8.** Considere a MT que tem estado inicial q_0, estado terminal q_f, e a seguinte função de transição:

ao ler	no estado	escreva	vá para o estado	ande para
0	q_0	X	q_0	$\rightarrow$
1	q_0	X	q_1	$\rightarrow$
0	q_1	X	q_2	$\rightarrow$
1	q_1	X	q_1	$\rightarrow$
0	q_2	X	q_2	$\rightarrow$
1	q_2	X	q_3	$\rightarrow$
B	q_2	X	q_f	$\rightarrow$
0	q_3	X	q_0	$\rightarrow$
1	q_3	X	q_3	$\rightarrow$
B	q_3	X	q_f	$\rightarrow$

Descreva de maneira sucinta a linguagem $L \subseteq \{0,1\}^*$ que essa MT aceita.

***Questão 9.** Considere a seguinte noção levemente alterada de Máquina de Turing:

> **Definição.** Um *enumerador* é uma MT com 2 fitas, uma chamada *fita de trabalho* e a outra chamada *fita de enumeração*, e um estado especial chamado *estado de enumeração* (que não é terminal).
>
> A *execução de enumeração* de um enumerador E começa com ambas as fitas vazias. Durante essa execução, sempre que E entra no estado de enumeração, se as células não-vazias da fita de enumeração formam um bloco contíguo, consideramos que a palavra formada por essas células foi *enumerada*.

Note que a execução de enumeração de E pode enumerar diversas, talvez infinitas, palavras (a execução pode, ou não, terminar).

Prove que uma linguagem $L \subseteq \{0,1\}^*$ é recursivamente enumerável (i.e., aceita por alguma MT comum) se, e somente se, existe um enumerador E tal que L é exatamente o conjunto das palavras enumeradas por E.

Questão 10. Diga se cada uma das linguagens abaixo é decidível (i.e., reconhecida por alguma máquina de Turing que sempre para) ou não, e prove sua resposta.

*** a.** PASSOS $:= \{c \in \{0,1\}^* \mid c$ codifica alguma máquina M, alguma entrada x para M e algum $n \in \mathbb{N}$, tais que M para em no máximo n passos quando executada com entrada $x\}$

*** b.** FINITO $:= \{c \in \{0,1\}^* \mid c$ codifica máquina M tal que M aceita apenas uma quantidade finita de entradas$\}$

c. EQUIVALENTES $:= \{c \in \{0,1\}^* \mid c$ codifica máquinas M e N que aceitam exatamente as mesmas entradas$\}$

Questão 11. Seja $f : (\{0,1\}^*)^n \to \{0,1\}^*$ uma função n-ária parcial (i.e., uma função cujas saídas são sempre elementos de $\{0,1\}^*$ e cujos argumentos de entrada são n elementos de $\{0,1\}^*$, para algum $n > 0$, mas não necessariamente *todas* as n-uplas desse tipo são entradas aceitas). Dizemos que uma máquina M *computa* f se:

- M tem como alfabeto de entrada $\{0, 1, \texttt{\#}\}$;
- M tem pelo menos 2 fitas: uma fita *de entrada* e uma fita *de saída*, mais alguma quantidade finita (talvez zero) de fitas *de rascunho*;
- no início de qualquer execução de M, todas as fitas exceto a de entrada estão vazias;
- quando $(c_0, \dots, c_{n-1}) \in (\{0,1\}^*)^n$ é uma entrada possível para f, então M chega a um estado terminal quando executada com $c_0\texttt{\#}c_1\texttt{\#}\cdots\texttt{\#}c_{n-1}$ inicialmente na fita de entrada;
- quando $(c_0, \dots, c_{n-1}) \in (\{0,1\}^*)^n$ é uma entrada possível para f, e M é executada com $c_0\texttt{\#}c_1\texttt{\#}\cdots\texttt{\#}c_{n-1}$ inicialmente na fita de entrada, então quando M chega ao seu estado terminal, o conteúdo da fita de saída é exatamente $f(c_0, \dots, c_{n-1})$.

Note: quando $(c_0, \dots, c_{n-1}) \in (\{0,1\}^*)^n$ **não** é uma entrada possível para f e M é executada com $(c_0, \dots, c_{n-1})$ inicialmente na fita de entrada, **nada afirmamos** sobre o comportamento de M (não importa o que acontece nesse caso)! Além disso, a máquina pode usar no seu alfabeto de fita quaisquer outros símbolos além de $0, 1, \texttt{\#}, B$ (“blank”, símbolo representando o vazio).

Prove que as funções a seguir são computáveis:

a. “Soma em base unária”: $f(1^x, 1^y) = 1^{x+y}$. Aqui, f só tem como entradas pares de palavras sem ocorrências de 0.

b. “Dobro em base unária”: $f(1^x) = 1^{2x}$. Aqui, f só tem como entradas palavras sem ocorrências de 0.

*** c.** “Sucessor em base binária”: $f(c)$ é o binário que representa o sucessor do número natural cuja representação binária é c. Aqui, f tem como entrada qualquer c não-vazia.

d. “Dobro em base binária”: $f(c)$ é o binário que representa o dobro do número natural cuja representação binária é c. Aqui, f tem como entrada qualquer c não-vazia.

e. "Fatorial em base unária": $f(1^n) = 1^{n!}$, sendo $n!$ o *fatorial* de n. Aqui, f só tem como entradas palavras sem ocorrências de 0.

Questão 12. Dê exemplo de função parcial $f : (\{0,1\}^*)^n \to \{0,1\}^*$ que não seja computável, para algum $n \in \mathbb{N}$ (e prove que ela não é computável).

Questão 13 (Busy Beaver, o "castor ocupado")**.** É fato (e você não precisa provar!) que para cada $n \in \mathbb{N}$, existe uma quantidade finita de máquinas de Turing M satisfazendo:

- M tem exatamente n estados *além* do seu estado terminal;
- M tem apenas 1 fita;
- M tem alfabeto de entrada $\varnothing$ (vazio) e de fita $\{1, B\}$;
- quando executada com sua fita vazia (i.e., com B em todas as células), M **sempre chega ao estado terminal** após um número finito de passos.

Assim, para cada $n \in \mathbb{N}$, há uma máquina com essas propriedades que deixa uma quantidade *máxima* de 1s escrita na fita ao parar (não necessariamente todos juntos); chamamos de *número de Busy Beaver de n*, denotado $\mathsf{BB}(n)$, essa quantidade (algumas fontes usam a notação $\Sigma(n)$ para o que estamos denotando por $\mathsf{BB}(n)$). Até hoje só se conhecem os valores exatos de $\mathsf{BB}(n)$ para $n \leqslant 4$. Por exemplo, $\mathsf{BB}(3) = 6$, $\mathsf{BB}(4) = 13$, $\mathsf{BB}(5) \geqslant 4098$, e $\mathsf{BB}(6)$ certamente não caberia nessa página: ele é maior do que o número

$$10 \uparrow\uparrow 15 := 10 \text{ elevado a } (10 \text{ elevado a } (10 \text{ elevado a } (\ldots \text{ elevado a } 10)))$$

com 15 números 10 aparecendo na expressão!

a. Encontre (e prove que estão corretos) os valores de $\mathsf{BB}(0)$ e $\mathsf{BB}(1)$.

b. Prove que $\mathsf{BB}(2) \geqslant 4$.