

Entregue apenas a folha de respostas. As questões não precisam estar em ordem e podem ser respondidas à lápis ou caneta. Na correção, símbolos ou palavras ilegíveis não serão considerados. Justifique todas as respostas a menos de menção em contrário.

Coloque o seu nome na folha de resposta, o mais acima possível na folha. Não coloque o RA. Se você não quiser que a sua nota seja divulgada publicamente, escreva apenas NÃO depois do seu nome.

No final da prova há um pequeno resumo da matéria.

1. (2,0) Prove que a linguagem $\{2n : n \in \mathbb{N}\}$ sobre $\{0,1\}$ é uma linguagem recursivamente enumerável. Siga a definição de recursivamente enumerável dada no fim desta prova. Não é necessário definir formalmente a MT. Apenas descreva o seu funcionamento no mesmo nível de detalhe das descrições de MT do livro do Sipser.
2. (2,5) Explique como uma MT com uma única fita pode simular a execução de uma MT com duas fitas.
3. (3,0) Explique o que é uma MT Universal. A sua resposta deve responder às seguintes questões: o que uma MT universal U toma como entrada? O que produz como saída? Ela sempre pára? Justifique! A codificação de uma máquina de Turing é utilizada em algum lugar? O que é mesmo codificação? Não é preciso explicar com detalhes esta última pergunta, apenas especifique o que é.
4. (2,5) Suponha que $SAT \leq_P K$ para certa linguagem $K \in NP$. Prove que K é NP-completa. Se houver um algoritmo polinomial para decidir SAT então haverá um algoritmo polinomial que decide K ? E o contrário?
5. (2,5) Seja S o conjunto das linguagens sobre $\{0,1\}$ e T o conjunto de todas as máquinas de Turing (ou codificações no conjunto \mathbb{N} de todas as MTs). Pergunta-se:
 - (a) S é equipotente a qual conjunto? Não é preciso justificar;
 - (b) T é equipotente a qual conjunto? Não é preciso justificar;
 - (c) $S \sim T$? Justifique. O que isto significa?

Resumo

Sendo Σ um conjunto finito de símbolos, uma cadeia sobre Σ é a concatenação de um conjunto finito de símbolos de Σ . Definimos $\Sigma^n = \{a_1 a_2 \dots a_n : a_i \in \Sigma, 1 \leq i \leq n\}$, o conjunto de todas as cadeias sobre Σ de tamanho n . Usamos ϵ para a cadeia com zero elementos. Logo $\Sigma^0 = \{\epsilon\}$. Definimos Σ^* como

$$\bigcup_{n \geq 0} \Sigma^n$$

Uma linguagem L sobre Σ é um subconjunto de Σ^* .

Uma máquina de Turing M é uma 7-tupla $(Q, \Sigma, \Gamma, \delta, q_0, q_A, q_R)$ na qual Q, Σ, Γ são conjuntos finitos. Q é um conjunto de estados, Σ é o alfabeto de entrada ($\sqcup \in \Sigma$), Γ é o alfabeto da fita ($\sqcup \in \Gamma$ e $\Sigma \subset \Gamma$), $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R, S\}$ é a função de transição, $q_0 \in Q$ é o estado inicial, q_A é o estado de aceitação e q_R é o estado de rejeição. Sempre que o estado corrente for q_A ou q_R a máquina pára (e estes são os únicos estados finais). Para facilitar as provas, assuma que sempre que o estado corrente for q_A o valor de retorno da máquina será 1. Idem para q_R e 0.

Uma MT de decisão sempre termina o seu processamento e retorna 0 ou 1. A menos de menção em contrário, todas as MT aceitam um inteiro em binário como entrada. Uma MT M decide uma linguagem L sobre Σ se M é uma MT de decisão e $x \in L$ se e somente se $M(x) = 1$. Uma linguagem L sobre Σ é recursivamente enumerável se existe uma MT M tal que

$$x \in L \implies M(x) = 1$$

$$x \notin L \implies M(x) \uparrow$$

Uma linguagem $L \in \text{NP}$ se existe uma MT não determinística N que decide L em tempo polinomial; isto é, se $x \in L$, então existe uma sequência de escolhas não determinísticas na computação $N(x)$ de tal forma que o resultado seja $N(x) = 1$. Uma linguagem $L \in \text{P}$ se existe uma MT M que decide L em tempo polinomial. Isto é, $L \in \text{TIME}(n^k)$ para algum $k \in \mathbb{N}$. SAT é a linguagem $\{\langle \varphi \rangle : \varphi \text{ está na FNC e é satisfazível}\}$. SAT é NP-completa. Isto é, $\text{SAT} \in \text{NP}$ e para toda $L \in \text{NP}$, $L \leq_P \text{SAT}$ ($L \leq_P K$ se existe uma MT R que executa em tempo polinomial tal que $x \in L$ sse $R(x) \in K$). A relação \leq_P é transitiva: se $L_1 \leq_P L_2$ e $L_2 \leq_P L_3$ então $L_1 \leq_P L_3$.

$A \sim B$ se existe uma função bijetora entre A e B .