Universidade Federal do Paraná
Professor Murilo V. G. da Silva
Primeira lista de exercícios

QUESTÃO 1: Com relação a conceitos fundamentais em teoria da computação, responda **V** ou **F**. Justifique sua resposta.

(a) Para todo algoritmo escrito em C, existe uma Máquina de Turing equivalente que resolve o mesmo problema, e vice-versa. Isto é verdade por que embora estes dois formalismos sejam diferentes, ambos são capazes de expressar algoritmos capazes de decidir qualquer linguagem recursiva.

(b) Enquanto Máquinas de Turing são modelos matemáticos formais para representar o que chamamos de algoritmos, uma Máquina de Turing Universal (que é uma Máquina de Turing em particular) é um modelo matemático para representar o que chamamos de um computador.

(c) Autômatos com pilha (PDAs) são formalismos matemáticos usados para descrever certos algoritmos. Entretanto, nem todo algoritmo pode ser expresso em termos de PDAs, sendo que a razão disso é que o conjunto das linguagens livres de contexto (formalismo usado para definir problemas decidíveis por PDAs) é estritamente menor do que o conjunto de linguagens recursivas (formalismo para definir todo problema decidível algoritmicamente, ou seja, todo problema decidível por alguma Máquina de Turing). Em Teoria da Computação diferentes modelos de computação estão associados a diferentes conjuntos de problemas, sendo que tipicamente modelos mais sofisticados (como Máquinas de Turing) são capazes de resolver um conjunto maior de problemas que modelos mais simples (PDAs, autômatos finitos, etc).

(d) Existem formalismos matemáticos que, embora sejam interessantes do ponto de vista teórico, não tem correspondência com objetos físicos (e.g. Máquinas de Turing com Oráculos, Máquinas com fitas contendo "células" capazes de armazenar números com precisão infinita, entre outros). Tais modelos são normalmente chamados de modelos de hipercomputação. Segundo o consenso científico, o modelo de computação quântica não é um modelo de hipercomputação. A razão disso é que existe uma correspondência de um para um entre algoritmos quânticos e o comportamento de objetos físicos, segundo as leis mecânica quântica. A dificuldade de construção de tais máquinas seria um problema de engenharia e não de princípios fundamentais da natureza.

(e) O formalismo matemático que utilizaremos para descrever algoritmos quânticos é chamado de circuito quântico. Neste modelo poderemos escrever circuitos quânticos que não apenas serão equivalentes a qualquer algoritmo concebível, como seremos capazes de escrever circuitos que resolvam problemas que não são recursivos (e.g., problemas semelhantes ao problema da parada).

(f) O conjunto de problemas resolvíveis por circuitos quânticos é o conjunto das linguagens recursivas. Em outras palavras, computação clássica e quântica são equivalentes em termos de computabilidade.

(g) Uma vez que tenhamos computadores quânticos, a Tese de Church-Turing terá sido refutada.

(h) A Tese de Church-Turing Estendida (TCTE) não é aceita na comunidade científica com a mesma credibilidade com que a Tese de Church-Turing (TCT) é aceita. De fato, uma vez que tenhamos computadores quânticos construídos, teremos a evidência para descartar a TCTE. Por outro lado, mesmo neste cenário, a TCT continuará intacta.

(i) Embora computadores quânticos e clássicos sejam equivalentes em termos de computabilidade, um dos pilares da área de computação quântica é a conjectura de que a classe P seja estritamente menor do que a classe BQP. Esta conjectura implica que o conjunto dos problemas decidíveis em tempo polinomial por computadores quânticos é maior do que o conjunto de problemas decidíveis em tempo polinomial por computadores clássicos.

QUESTÃO 2: Com relação a números complexos e conceitos de álgebra linear, resolva os exercícios abaixo

(a) Calcule o módulo do número $-4 + 2i$

(b) Reescreva $1 + i$ na forma polar (i.e., encontre r e θ) e em seguida desenhe o gráfico

(c) Repita o exercício do item anterior para o número $2 + 2\sqrt{3}i$

(d) Seja A uma matriz $n \times n$ e $|v_i\rangle$ um vetor de $\mathbb{C}^n$. Prove que:

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A |v_i\rangle$$

(e) No espaço $\mathbb{C}^2$, quantos vetores unitários de valores **reais** cuja projeção em $|1\rangle$ tem tamanho $\frac{\sqrt{3}}{2}$? E quantos vetores unitários de valores **complexos** cuja projeção em $|1\rangle$ tem tamanho $\frac{\sqrt{3}}{2}$?

QUESTÃO 3: Calcule o produto interno de $|+\rangle$ e $|-\rangle$.

QUESTÃO 4: Medindo o estado $\psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ na base $|+\rangle$ e $|-\rangle$, qual a probabilidade de se obter $-$?.

QUESTÃO 5: Seja $\phi = \frac{1}{2}|0\rangle + \frac{1+\sqrt{2}i}{2}|1\rangle$. (a) Calcule o produto interno $\langle\phi|+\rangle$. (b) Se medirmos $|\phi\rangle$ na base $|+\rangle$, $|-\rangle$, qual a probabilidade de obtermos $+$? (c) Qual a probabilidade de obtermos $-$?

QUESTÃO 6: Suponha que temos um qubit no estado $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Se medirmos os qubit na base $|u\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle, |u^{\perp}\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$, qual é a probabilidade de que o resultado seja u?

QUESTÃO 7: Queremos medir o estado $|\phi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ na base $\{\cos\theta|0\rangle + \sin\theta|1\rangle, \sin\theta|0\rangle - \cos\theta|1\rangle\}$. Se quisermos que os dois possíveis resultados sejam equiprováveis, qual deve ser o valor de θ em graus?

QUESTÃO 8: Rescreva $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$ na base $|+\rangle, |-\rangle$.

QUESTÃO 9: Considere o estado $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$. Vamos estimar a fase θ fazendo uma medida na base $|+\rangle, |-\rangle$. Qual é a probabilidade do resultado ser $+$? Dica: $e^{i\theta} = \cos\theta + i\sin\theta$.

QUESTÃO 10: A base padrão (base computacional) para um sistema com dois qubits é $|00\rangle, |01\rangle, |10\rangle, |11\rangle$? Verdadeiro ou Falso?

QUESTÃO 11: Todo sistema de dois qubits pode ser escrito como $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$, onde $a, b, c, d \in \mathbb{C}$. Em caso afirmativo, prove. Em caso negativo, forneça um contra-exemplo.

QUESTÃO 12: Dois qubits estão emaranhados se o sistema pode ser escrito como $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$, onde $a, b, c, d \in \mathbb{C}$. Verdadeiro ou falso?

QUESTÃO 13: Para quaisquer $a, b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$, é verdade que $a|00\rangle + b|11\rangle = a|++\rangle + b|--\rangle$? Justifique sua resposta.

QUESTÃO 14: Calcule o produto interno $(\frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle, |+\rangle)$. Com isso em mãos, calcule a probabilidade de se obter $+$ fazendo uma medida de um sistema quântico $|\Psi\rangle = \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle$ na base $|+\rangle$, $|-\rangle$.

QUESTÃO 15: Reescreva $\frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle$ na base $|+\rangle$, $|-\rangle$.

QUESTÃO 16: Suponha que um qubit está no estado $|\phi\rangle = a|0\rangle + \sqrt{1-a^2}|1\rangle$ onde $a \in [-1, 1]$. Se primeiro fazemos uma medida na base padrão e depois medimos na base $|u\rangle, |u^\perp\rangle$, onde $|u\rangle = b|0\rangle + \sqrt{1-b^2}|1\rangle$, para algum $b \in [-1, 1]$, qual é a probabilidade de que o resultado da segunda medida seja u, em termos de a e b?

QUESTÃO 17: Quais conjuntos de vetores abaixo **NÃO** é uma base válida para um sistema de dois qubits?

- $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- $|++\rangle, |+-\rangle, |-+\rangle, |--\rangle$
- $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, $\frac{1}{\sqrt{2}}|++\rangle + \frac{1}{\sqrt{2}}|--\rangle$, $\frac{1}{\sqrt{2}}|+-\rangle + \frac{1}{\sqrt{2}}|-+\rangle$
- $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

QUESTÃO 18: Se o primeiro qubit está no estado $\frac{\sqrt{2}}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$ e segundo qubit está no estado $\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle$, qual é o estado do sistema composto?

QUESTÃO 19: Fatore $\frac{1}{2\sqrt{2}}|00\rangle - \frac{1}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|10\rangle - \frac{\sqrt{3}}{2\sqrt{2}}|11\rangle$ em $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$, onde $|a|^2 + |b|^2 = 1$ e $|c|^2 + |d|^2 = 1$. Qual o valor de $|a|$?

QUESTÃO 20: Suponha que temos dois qubits em um estado $\alpha|00\rangle + \beta|11\rangle$.

(a) Se medirmos o primeiro qubit na base $|+\rangle, |-\rangle$, qual a probabilidade de se obter $+$?

(b) Obtendo-se o resultado do item (a), qual o estado do segundo qubit?

QUESTÃO 21: Um sisetma de dois qubits estava originalmente no estado $\frac{1}{5}|00\rangle + \frac{2}{5}|01\rangle + \frac{4}{5}|10\rangle - \frac{2}{5}|11\rangle$. Mediu-se o primeiro qubit e obteve-se 0. Se medirmos o segundo qubit, qual a probabilidade de se obter 0?

QUESTÃO 22: No sistema $|\Psi\rangle = |0+\rangle$ temos dois qubits emaranhados?

QUESTÃO 23: Temos um sistema com dois qubits no estado $|0+\rangle$. Digamos que queiramos obter um sistema em que os dois qubits estejam emaranhados. Para tal queremos fazer uma medida do sistema. Em qual base abaixo devemos fazer a medida?

- $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- $|++\rangle, |+-\rangle, |-+\rangle, |--\rangle$
- $|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle$
- $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle, \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle, \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$
- Não é possível emaranhar o sistema com um precesso de medida.

QUESTÃO 24: Temos um sistema com dois qubits no estado $|0+\rangle$. Digamos que queiramos obter um sistema em que os dois qubits etejam emaranhados. Para tal queremos fazer uma medida **parcial** do sistema, medindo apenas o primeiro qubit. Em qual base abaixo devemos fazer a medida?

- $|0\rangle, |1\rangle$
- $|+\rangle, |-\rangle$
- $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle, -\frac{i}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- $\frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle, \frac{i}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- Não é possível emaranhar o sistema com um precesso de medida.

Obs: Alguns dos exercícios desta lista contém questões de prova de edições do curso "Quantum Mechanics and Quantum Computation" (Professor Umesh Vazirani, Universidade de Berkeley).