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

QUESTÃO 1: A ideia central da parte "clássica" do Algoritmo de Shor é que fatorar $N = P \cdot Q$ é equivalente a encontar x tal que $x^2 \equiv 1 \pmod{N}$ para para raízes não triviais desta equação. Além disso, encontrar este valor x é equivalente a encontrar o período k da função $f(x) = b^x \pmod{N}$, para algum b adequado que pode ser encontrado com probabilidade exponencialmente alta. Pergunta: Com k em mãos e assumindo que b é uma base adequada, como fazemos para recuperar os fatores P e Q?

QUESTÃO 2: Qual é ideia principal da parte "quântica" do Algoritmo de Shor, ou seja, como fazemos para encontrar o período k (que pode ser exponencialmente grande) da questão anterior? Mostre a parte do circuito que faz esta tarefa (supondo que a base b é adequada).

QUESTÃO 3: Mostre o circuito completo do Algoritmo de Shor qual tarefa realiza cada parte do circuito e indique o estado que o sistema se encontra nestas diferentes partes do circuito.

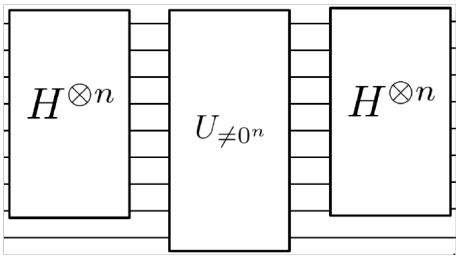
QUESTÃO 4: Vamos executar alguns passos do Algoritmo de Shor para $N = 91$.

(a) Qual é o período k da superposição do algoritmo se a escolha aleatória é $x = 8$?

(b) Usando a resposta da questão (a), qual a raíz de 1 quadrada mod 91

(c) Neste caso o algoritmo calcula $\text{gdc}(y, 91)$. Quais possíveis valores de y podem ser usados para encontrar um fator de 91?

QUESTÃO 5: Apresente a matriz $N \times N$ do circuito quântico $U_{\neq 0^n}$ da figura abaixo. Prove que, uma vez que o qubit mais abaixo seja $|-\rangle$ (i.e., faz-se um "phase kickback" em $U_{\neq 0^n}$), o circuito completo da figura (incluindo as tranformadas de Hadamard) leva a superposição $\sum_x \alpha_x |x\rangle$ para a superposição $\sum_x (2\mu - \alpha_x) |x\rangle$.



QUESTÃO 5: Apresente o circuito quântico completo para o Algoritmo de Grover e indique (não há necessidade de demonstrações matemáticas) qual parte do circuito é a inicialização (ou seja, cria-se todos as strings possíveis), qual parte do circuito é o loop principal e quantas vezes o loop é executado. Finalmente, mostre como é feita a inversão e de fase e que parte do circutio faz a reversão sobre a média.

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).