Título: Introdução à Computação Quântica
Instrutor: Prof. Fernando J. O. Souza (Dept. de Matemática, UFPE)

Resumo: A computação quântica é um paradigma de computação ainda em desenvolvimento. Nela, enriquece-se a computação clássica com recursos da física quântica, tentando-se ganhar eficiência (no sentido de complexidade computacional). Ela começou na década de 1980, e envolve tanto a criação de algorítmos e modelos de computação que tomam vantagem de efeitos quânticos como o desenvolvimento de maquinaria ("hardware") que permite o uso daqueles recursos (em geral, explorando propriedades quânticas de partículas convenientes). Um dos mais célebres sucessos desta jovem área é o algorítmo devido a Peter Shor (1994) para a fatoração inteira eficiente (em tempo polinomial), um problema para o qual se suspeita ser impossível a obtenção de um algorítmo clássico eficiente. Isto é de enorme importância estratégica porque a suposta ineficiência da fatoração inteira é amplamente utilizada na criptografia de chave pública (especificamente, no algorítmo RSA, usado na internet). O algorítmo de Shor foi generalizado para algorítmos que determinam propriedades de grupos (em álgebra). Há também algorítmos quânticos mais eficientes que os clássicos, por exemplo, para busca (numa lista), na topologia de baixa dimensão, e na simulação de alguns sistemas quânticos (esta, uma das motivações originais para a computação quântica).

Para se ter uma idéia da diferença entre a computação clássica e a quântica, recorde-se que um circuito booleano clássico processa cadeias de dígitos, cada um igual a zero ou um (tais cadeias representam informação). Já um circuito quântico manipula, paralelamente, diversas cadeias de zeros e uns, as quais estão combinadas em superposições (*estados quânticos*) através de números complexos (*amplitudes*). Contudo, enquanto informação clássica pode ser recuperada à vontade, estados quânticos podem sofrer modificações ao serem acessados, fornecem informação probabilisticamente, dependendo das amplitudes, e sua natureza não é local. Esta última característica (*emaranhamento quântico*) se traduz no fato de que a observação de zero ou um numa posição das cadeias pode afetar as probabilidades para as demais posições. Há também o problema tecnológico da interação do computador quântico com o ambiente (um fenomeno denominado *decoerência quântica*), a qual funciona como uma observação de estados quânticos, levando à perda de informação. Assim, poderosa e delicada, a computação quântica exige o uso adequado (e nada trivial) da natureza quântica da informação processada

durante a solução engenhosa dos problemas que admitem solução eficiente por meio de computadores quânticos.

Iniciaremos este mini-curso com uma breve visão geral da área. Logo depois, faremos um resumo dos elementos de mecânica quântica necessários, revisando os conceitos e resultados matemáticos apropriados. Então, serão discutidos: o modelo de computação por circuitos quânticos; alguns algorítmos quânticos à luz da teoria da complexidade computacional; e a correção de erros quânticos. Ao longo desta discussão, os paradigmas quântico e clássico (determinístico e probabilístico) serão contrastados. Se houver interesse e o tempo permitir, outros temas poderão ser comentados rapidamente. Ex.: outros modelos de computação quântica; propostas para a implementação física de um computador quântico; linguagens de programação quânticas; teoria da informação quântica e, em particular, criptografia quântica; etc.

Os pré-requisitos para este mini-curso são: fluência em números complexos e propriedades de polinômios a nível de ensino médio; e um primeiro curso sobre álgebra linear a nível de graduação.