

TEORIA QUÂNTICA DA INFORMAÇÃO

Aluno: Pedro Henrique Milet Pinheiro Pereira

Orientador: Derek Hacon

Introdução

O projeto é dividido em duas partes: na primeira, tratamos da teoria da informação quântica, sendo o objetivo final estudar o Teorema de Schumacher, que é o análogo quântico do Teorema de Shannon. Na segunda parte, estudamos aspectos relacionados à teoria da computação quântica, em particular as propriedades de sistemas compostos emaranhados.

Informação Clássica

A teoria da informação clássica, conhecida há muito tempo, trata do armazenamento, compactação e transmissão de informações utilizando os “bits”. Nessa teoria, destacam-se o conceito de entropia (com várias aplicações na física, mas que na teoria da informação ganha o papel de “dizer como armazenar e transmitir informação de forma mais econômica”) e, em especial, o teorema de Shannon (em que a entropia aparece como a menor razão de compressão de dados que admite um sistema de compressão confiável).

Informação Quântica

Nas últimas décadas do século XX, surgiu a idéia de aplicar mecânica quântica no tratamento da informação.

Sua estrutura básica é o chamado qubit, que é um sistema físico associado a um espaço de Hilbert H de dimensão 2; a grande diferença do qubit para o bit clássico é que, enquanto o segundo pode assumir apenas dois estados diferentes (0 e 1), o primeiro pode assumir infinitos estados, combinações lineares dos estados $|0\rangle$ e $|1\rangle$ (que formam uma base ortonormal de H).

Na informação quântica, existe o conceito de entropia quântica, em analogia com a entropia clássica. Da mesma forma, o recente teorema de Schumacher (que diz que – para n suficientemente grande – a informação contida em n qubits pode ser comprimida em um espaço de Hilbert de dimensão $2^{nS(p)}$, em que $S(p)$ é a entropia do estado p associado a cada qubit) é o paralelo quântico do teorema de Shannon.

Computação Quântica:

A idéia de computação quântica decorre naturalmente da necessidade de miniaturização de componentes eletrônicos, imposta pela indústria de computadores. De fato, chegará um momento em que atingiremos o limite de tecnologia de circuitos integrados, e será necessário enveredar pelos caminhos da mecânica quântica, cujas leis impõem limitações ao tamanho e à performance dos componentes do circuito.

A grande vantagem da computação quântica em relação à clássica é a possibilidade de o computador estar em vários estados ao mesmo tempo (o que é chamado paralelismo quântico). Uma outra grande vantagem da computação quântica é o uso da interferência construtiva entre os qubits, que usa em especial o conceito de emaranhamento (do qual falaremos mais à frente).

Emaranhamento Quântico:

O emaranhamento quântico é o principal fator que diferencia o computador clássico do quântico.

A idéia é a seguinte: considere dois qubits (que podem estar separados por centímetros ou por quilômetros), aos quais está associado um determinado estado ψ . Diz-se que ψ é *separável* quando é possível associar um estado ψ_1 ao primeiro qubit e um estado ψ_2 ao segundo. Nesse caso ψ é o produto tensorial $\psi_1 \otimes \psi_2$. Da mesma forma, diz-se que ψ é *emaranhado* quando não é possível fazer essa separação - e nesse caso se costuma dizer que cada qubit, individualmente, não possui estado físico próprio.

É importante observar que, se o sistema estiver num estado emaranhado, uma medição local em um dos qubits altera todo o sistema.

Uma das mais importantes conseqüências do emaranhamento é a chamada teleportação quântica.

Teleportação Quântica

Criar cópias de estados clássicos é relativamente fácil – basta fazer um número suficiente de observações, tomando o cuidado de não danificá-lo, e usar as informações obtidas para criar uma cópia.

No entanto, no caso quântico, isso não é tão simples. Qualquer tipo de medida feita no sistema altera-o de uma forma incontrolável, destruindo o original.

Uma outra idéia seria tentar fazer “clones” do sistema e medi-las, não destruindo, assim, o original. Mas isso é impossível, como afirma o “Teorema da Não-Clonagem”.

Como transmitir, então, toda informação de um sistema a outro? A resposta é a teleportação quântica, que usa o emaranhamento para transportar um determinado estado de um sistema a outro, e um canal clássico que transmita uma mensagem de apenas 2 bits.

Álgebra de Temperley – Lieb

Alguns autores têm notado alguma semelhança entre a equação de teleportação quântica e a álgebra de Temperley-Lieb, ligada aos grupos de tranças (em Topologia). A idéia é utilizar a álgebra das tranças para simplificar as contas no lado quântico. A área ainda encontra algumas ambigüidades, mas parece bastante promissora.

Referências:

[1] GALINDO, A. e MARTIN-DELGADO, M.A. **Information and Computation: Classical and Quantum Aspects**. Departamento de Física Téorica, Facultad de Ciencias Físicas, Universidad Complutense. Madrid, 2001.

[2] MONDAINI, Débora; SVETLICHNY, George. **A Universalidade do Produto Tensorial e o Teorema de Composicionalidade de Coecke**. Rio de Janeiro, 2006. 64p. Dissertação de Mestrado – Departamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro.

[3] ZHANG, Yong. **Teleportation, Braid Group and Temperley-Lieb Algebra**. Institute of Theoretical Physics, Chinese Academy of Sciences. Beijing, 2006.

[4] LIMA, Bernardo N. B., CIOLETTI, Leandro Martins. CUNHA, Marcelo de O. Terra e BRAGA, Gastão A. **Entropia: Introdução à Teoria Matemática da (des)Informação**. Departamento de Matemática – UFMG. Belo Horizonte, 15 de outubro de 2004.