CÓDIGOS QUÂNTICOS CORRETORES DE ERROS

Júlio César OLIVEIRA AGUIAR (1); Selma Rozane VIEIRA (2); Rodrigo GUSMÃO CAVALCANTE (3)

(1) IFBA – Campus Vitória da Conquista, Av. Amazonas, 3150, Zabelê , CEP 45030-220
Vitória da Conquista - BA, telefax: (77) 3426-2421, e-mail: jc-aguiar@hotmail.com
(2) IFBA – Campus Vitória da Conquista, Av. Amazonas, 3150, Zabelê , CEP 45030-220
Vitória da Conquista - BA, telefax: (77) 3426-2421, e-mail: srozane@ifba.edu.br
(3) IFBA – Campus Salvador, Rua Emídio dos Santos, s/n, Barbalho, CEP 40301-015
Salvador - BA, telefax: (71) 2102-9516, e-mail: rodgcav@ifba.edu.br

RESUMO

Neste artigo, apresentamos parte do nosso projeto desenvolvido na Iniciação Científica. Trata-se de um trabalho sobre códigos quânticos corretores de erros. Na presente contribuição analisamos um código quântico já conhecido na literatura, o código de Shor, assim como também propomos um novo código quântico da classe CSS.

Palavras-chave: computação quântica, informação quântica, códigos quânticos, corretores de erros.

1 INTRODUÇÃO

Na computação clássica a unidade básica da informação é o *bit*, variável aleatória que pode assumir valores lógicos 0 (zero) ou 1 (um). Na computação quântica a unidade básica da informação é o *qubit* (bit quântico). O qubit pode existir em um dos estados distintos, $|0\rangle$ e $|1\rangle$, correspondentes aos estados clássicos 0 e 1, e também na superposição destes estados, sem análogo clássico. Foi no início dos anos 1980 que conexões entre mecânica quântica e computação começaram a ser formalizadas, dando origem a um novo campo de pesquisa: a computação quântica e a informação quântica. Em grosso modo, podemos dizer que a teoria da computação trata dos recursos necessários para a execução de algoritmos (recursos de tempo, memória etc.), bem como da análise da complexidade dos problemas computacionais. Já a teoria da informação é responsável pelas formas e os recursos necessários para o envio da informação por canais de comunicação. Uma revisão sobre este tema pode ser encontrada no livro de Nielsen e Chuang [2005].

Embora a história da computação quântica e da informação quântica tenha começado na virada do século XX, atualmente, na prática não contamos com computadores quânticos em pleno funcionamento, quem sabe no futuro próximo. Desde dezembro de 2001, quando cientistas do Centro de Pesquisa da IBM anunciaram terem conseguido construir um computador quântico de 7 qubits [IBM, 2001], pesquisas tecnológicas envolvendo novos computadores vem crescendo consideravelmente. Em fevereiro de 2007 a empresa canadense D-Ware divulga a construção de *Orion*, um computador quântico híbrido de 16 qubits [INFO online]. Em novembro 2009, pesquisadores do Instituto Nacional de Padrões e Tecnologia (sigla em inglês, NIST), em Boulder, no Colorado, exibiram o primeiro computador quântico programável. Testes realizados com essa máquina indicaram um índice de precisão de 79 por cento, indicando que o computador precisa ser melhorado [NewScientist, 2009].

Enquanto aguardamos estas fantásticas máquinas, os computadores quânticos, disponíveis em nossas mesas, cientistas ao redor do mundo vêm trabalhando em pesquisas básicas, teóricas e experimentais, em particular, com estados emaranhados. “O emaranhamento é considerado um *recurso natural* para a computação quântica” [Oliveira, 2005]. Como exemplo de pesquisa básica experimental nesta linha podemos citar o trabalho “Three-Color Entanglement” publicado na revista Science [COELHO et. al., 2009]. Este trabalho foi divulgado na Folha de São Paulo com o título “Experimento na USP mostra base de Internet do futuro” [FolhaOnline, 2009].

Este trabalho está organizado como segue: na seção 2, breve histórico da computação quântica, na seção 3, codificação quânticas, na seção 4, códigos corretores de erros e por fim, na seção 5, as considerações finais.

2 BREVE HISTÓRICO

Abaixo um resumo dos principais fatos ocorridos na área da computação quântica

1980 – Y. Manin sugere que computadores quânticos poderiam simular sistemas quânticos mais rápidos do que os computadores clássicos;

1981 –Richard Feynman apontou que os sistemas clássicos não seriam capazes de modelar eficientemente os sistemas quânticos. Ele sugeriu (independentemente do trabalho de Manin) que computadores baseados nas leis da mecânica quântica ao invés das leis clássicas poderiam ser usados para modelar sistemas quânticos. Esta proposta foi apresentada na Primeira Conferência de Computação Física no MIT (Massachusetts Institute of Technology), e publicada no Int. J. Theor. Phys em 1982.

1984 – Charles Bennett e Gilles Brassard descobrem o protocolo de criptografia quântica BB84.

1985 – David Deutsch definiu aparatos computacionais, com base nos princípios da mecânica quântica, que fossem capazes de simular eficientemente qualquer sistema físico. Esses aparatos eram análogos quânticos das máquinas definidas por Turing 49 anos antes. Deutsch foi, também, o primeiro a publicar um algoritmo quântico, o Problema de Dois Bits de Deutsch (1987).

1994 - Peter Shor publica resultados demonstrando que um computador quântico resolveria eficientemente dois problemas importantes – o de encontrar os fatores primos de um número inteiro e o "problema do logaritmo discreto". O Algoritmo de Shor poderia, em tese, quebrar muito dos sistemas criptográficos em uso atual.

1995 – Lov Grover mostrou que o problema de se realizar uma busca em uma lista desordenada poderia ser revolvido mais rapidamente em um computador quântico.

1996 – Um grupo da IBM demonstra experimentalmente o BB84 utilizando fótons enviados por fibras comerciais de telecomunicação.

1997 – Neil Gershenfeld e Issac Chuang descobrem os estados pseudopuros.

1998 – Considerado o ano da computação quântica por ressonância magnética nuclear (RMN). Implementações de várias chaves lógicas quânticas são demonstradas através da RMN. Neste mesmo ano são demonstrados os algoritmos de busca e de teleporte, também por RMN.

3 CODIFICAÇÃO QUÂNTICA

O ruído é um sinal indesejado que interfere no processamento e na transmissão de informação, tanto nos sistemas clássicos quanto quânticos. Sempre que possível os sistemas são construídos de modo a evitar completamente o ruído, e quando isso não é possível, tenta-se pelo menos protegê-los dos seus efeitos. A idéia é que se quisermos proteger uma mensagem contra os efeitos de ruídos, devemos codificá-la adicionando informação redundante. Assim, mesmo que alguma informação seja corrompida pelo ruído, a redundância tornará possível a decodificação, de forma que a mensagem original seja recuperada. Para compreendermos como os esquemas de correção agem, vejamos um exemplo no caso clássico. Suponha que se queira enviar um bit de um local para outro através de um canal de comunicação ruidoso. O efeito do ruído no canal é inverter o bit que está sendo enviado com probabilidade $p > 0$. Logo, o bit será transmitido sem erro com probabilidade igual a $1 - p$. Um canal que possui esta característica é conhecido como ***canal binário simétrico*** – **BSC**. Uma forma usual de proteger o bit contra a ação do ruído é substituí-lo por três cópias (código de repetição), antes de enviá-lo pelo canal, isto é, $0 \to 000$ e $1 \to 111$.

Embora a teoria clássica de correção de erros seja bem fundamentada, ela não pode ser usada diretamente na teoria quântica. No caso quântico existem barreiras que dificultam a correção de erros. Contudo, nenhum deles é fatal.

Uma medida em mecânica quântica destrói o estado quântico sob observação, o que torna sua recuperação impossível. Para contornar isso as medidas realizadas sobre os estados quânticos não devem fornecer informação sobre as amplitudes do estado quântico codificado. Desse modo a superposição não será destruída. Em códigos quânticos corretores de erros o resultado das medidas realizadas sobre os estados para a verificação da ocorrência de erro são chamados de síndrome de erro e não apresentam informação sobre as amplitudes do estado, preservando-o.

Um outro problema para a correção quântica de erros em relação à clássica é abordado pelo teorema da não-clonagem, que demonstra a impossibilidade de clonagem dos estados quânticos. Logo, os códigos quânticos corretores de erros devem utilizar outras técnicas que não utilizem a clonagem de estados. Embora os erros possam ocorrer de forma contínua em um qubit, todos esses erros podem ser sanados corrigindo-se apenas um subconjunto discreto de erros; todos os outros erros possíveis ficarão automaticamente corrigidos. A discretização de erros é fundamental para explicar a eficácia das correções quânticas.

4 CÓDIGO CORRETORES DE ERROS

Um corretor de erro quântico é uma função de *k*-qubits sobre *n*-qubits (espaços vetoriais complexos de dimensões 2^k e 2^n), onde $n > k$. Este *k* qubits são designado qubits de informação são eles que devem ser protegidos de erros. Os $n-k$ qubits adicionais formam a redundância necessária para proteger a informação. Suponha que qubits sejam enviados através de um canal que os deixa inalterados com probabilidade $1-p$ e os inverte com probabilidade p. Isto é, com probabilidade p o estado $|\psi\rangle$ é levado para $X|\psi\rangle$, onde *X* é o operador inversão de bit. Esse canal é chamado de canal de *inversão de bit* ou canal *bit flip*. Suponha que o estado de um qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ tenha sido codificado com três qubits em, $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$. Cada um dos três bits é enviado através de uma cópia independente do canal de inversão de bit. Admitindo-se que uma inversão tenha ocorrido com no máximo um qubit. Como recuperar o estado quântico? Existe um procedimento de correção de erro em dois estágios, a saber:

Diagnóstico de síndrome: Medidas que detectam erro, caso haja algum, são realizadas sobre o estado quântico. O resultado da medida é chamado de *síndrome de erro*. Para um canal de inversão de bit existem quatro síndromes de erro, que corresponde aos quatros operadores de projeção:

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{sem erro}$$
$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{inversão do primeiro q-bit}$$
$$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{inversão do segundo q-bit}$$
$$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{inversão do terceiro q-bit}$$

Vale ressaltar, que a medida da síndrome não altera o estado que está sendo observado, pois ela exibe apenas a informação de que ocorreu erro sem interferir nos valores α e β que determinam o estado inicial. Ou seja, a síndrome não contém informações sobre o estado a ser protegido dos erros.

Recuperação: O valor da síndrome de erro é útil para sabermos qual procedimento a ser adotado para recuperar o estado inicial. No caso de uma síndrome e erro igual a 1 (2 ou 3), medida sobre o projetor P_1 (P_2 ou P_3), indica que um erro bit flip corrompeu o primeiro (segundo ou terceiro) qubit, inverte-se o qubit novamente, recuperando assim o estado inicial com exatidão.

4.1 Código de Shor

O código de Shor [1995] (em homenagem ao inventor) trata-se de um código quântico capaz de proteger contra os efeitos de um erro arbitrário em um qubit. Este código é uma combinação de um código para inversão de qubit com um código de três qubit para inversão de fase. Primeiramente codifica-se o qubit pelo código de inversão de fase: $|0\rangle \to |+++\rangle$ e $|1\rangle \to |---\rangle$ depois, codifica-se cada um dos qubits usando o código de três qubtis de inversão de bit: $|+\rangle \to \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ e $|-\rangle \to \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. O resultado é um código de nove qubtis com dois estados lógicos dados por:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \quad \text{[Eq.01a]}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \quad \text{[Eq.01b]}$$

Aplicando o formalismo dos estabilizadores ao código de Shor, teremos uma representação mais compacta e uma forma mais simples de descrever os erros nos qubits. Os geradores relacionados na tabela 1 geram um estabilizador para o espaço dos qubits codificados pelo código de Shor. Aplicando qualquer um dos geradores ao estado zero lógico, obteremos o mesmo estado como resultado. O mesmo acontece para o um lógico. Esse resultado mostra que os estados zero lógico e um lógico são estabilizados pelos geradores descritos na tabela 1.

Tabela 1: Geradores do código de Shor

NOME	OPERADOR
g1	Z Z I I I I I I I
g2	I Z Z I I I I I I
g3	I I I Z Z I I I I
g4	I I I I Z Z I I I
g5	I I I I I I Z Z I
g6	I I I I I I I Z Z
g7	X X X X X X I I I
g8	I I I X X X X X X

Para o código ser capaz de corrigir um determinado erro, este deve anticomutar com pelo menos um dos geradores do estabilizador do código. Como os geradores do código de Shor anticomutam com os erros representados pelos operadores de Pauli, desde que aconteçam somente sobre um qubit, o código é capaz de corrigir esses erros e qualquer combinação linear entre eles, ou seja, um erro arbitrário sobre um qubit. Desta forma fica claro que é bem mais fácil encontrar os erros corrigíveis por determinado código utilizando seus estabilizadores do que através dos vetores de estado.

Na subseção a seguir apresentamos um novo código quântico corretor de erro, da classe CSS.

4.2 Novo código quântico

Uma classe de códigos quânticos de correção de erros bastante ampla é a classe dos códigos de *Calderbank-Shor-Steane*, ou simplesmente códigos CSS. Tal classe de códigos é definida da seguinte maneira: sejam C_1 e C_2 códigos clássicos lineares $[n, k_1]$ e $[n, k_2]$, tais que $C_2 \subset C_1$ e C_1 e $C_2^{\perp}$ corrigem ambos t erros. Define-se um código quântico CSS(C_1, C_2) , $[n, k_1 - k_2]$, capaz de corrigir erros em t qubits, por meio da seguinte construção. Seja $x \in C_1$ uma codificação no código C_1. Define-se o estado quântico $|x + C_2\rangle$ por:

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \quad \text{[Eq.02]}$$

com "+" indicando adição binária módulo 2.

O código proposto neste trabalho pertence à classe de código CSS que foi construído a partir de um código linear clássico $[k, n, d] = [11, 20, 5]$ cuja matriz verificadora de paridade é:

$$H = \begin{bmatrix}
0&0&1&1&1&0&1&0&1&1&0&1&0&0&0&0&0&0&0&0\\
0&1&1&0&1&1&1&0&1&0&1&0&1&0&0&0&0&0&0&0\\
0&0&1&1&0&1&0&1&1&0&1&0&0&1&0&0&0&0&0&0\\
1&0&1&1&1&0&1&1&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&1&0&1&1&0&1&1&1&0&0&0&0&0&1&0&0&0&0\\
1&1&0&1&1&1&1&0&1&1&1&0&0&0&0&0&1&0&0&0\\
1&1&1&0&0&0&1&1&1&0&0&0&0&0&0&0&0&1&0&0\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
1&1&1&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

Suponha que se rotule esse código por *C*, e se defina $C_1 \equiv C$ e $C_2 \equiv C^{\perp}$. A fim de se usar esses códigos para definir um código CSS, é possível realizar permutações nas linhas da matriz geradora de C_2 de forma que a condição $C_2 \subset C_1$ seja satisfeita.

Por definição, a matriz verificadora de paridade de $C_2 = C^{\perp}$ é igual à transposta da matriz geradora de $C_1 = C$:

$$H[C_2] = G[C_1]^T = \begin{bmatrix}
0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&1&1&1&0&1&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&0&1&1&1&0&0&1&0&0&0&0&0&0&0&0\\
1&0&1&1&0&1&0&1&1&0&0&0&1&0&0&0&0&0&0&0\\
1&1&0&1&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&1&0&1&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0\\
1&1&0&1&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&1&1&0&1&1&1&0&1&0&0&0&0&0&0&0&0&1&0&0\\
1&0&0&0&1&1&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&1&1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

Como $C_2^{\perp} = (C^{\perp})^{\perp} = C$, de onde se vê que C_1 e $C_2^{\perp}$ são códigos com distância 5, capazes de corrigir erros em dois bits. Dessa forma, como C_1 é um código [11, 20, 5] e C_2 é um código [9, 20, 6], segue que o código CSS(C_1, C_2) é um código quântico [20,2] capaz de corrigir erros em dois qubits.

Devido ao fato dos valores de *k* e *n* dos códigos clássicos C_1 e C_2 serem altos, então não é possível descrever explicitamente aqui os elementos lógicos codificados, $|00_L\rangle$, $|01_L\rangle$, $|10_L\rangle$ e $|11_L\rangle$, para o código quântico proposto.

5 CONSIDERAÇÕES FINAIS

Os computadores atuais baseados na arquitetura de Von Neumann são, atualmente, a melhor opção na realização da maioria dos cálculos matemáticos, na editoração de textos ou para "navegarmos" na Internet. Contudo, em áreas como inteligência artificial, seria interessante a utilização de outros tipos de computadores e arquitetura. Devido o poder de processamento paralelo, computadores quânticos seria uma boa opção.

Enquanto aguardamos estes computadores disponíveis em nossas casas, cientistas ao redor do mundo vêm trabalhando em pesquisas básicas que sejam aplicadas ao seu desenvolvimento. Existem no Brasil laboratórios que realizam experiências com átomos frio (UFPE, USP, UNICAMP), fótons emaranhados

(UFMG, UFAL, UFRJ, USP-SP,UFF), com pinças óticas (UFMG, UNICAMP, UFRJ), pontos quânticos (LNLS) e ressonância magnética nuclear (CBPF, UFPE, USP-São Carlos). Grupos teóricos no CBPF, UFRJ, UFSCar, UNICAMP e UFMG pesquisam propostas de realização de operações elementares de computação quântica em diversos sistemas físicos, propriedades de estados emaranhados, efeitos do ambiente em sistemas quânticos e algoritmos computacionais.

Alem dos grupos acima citados existem grupos menores espalhados em diversas outras instituições do país, trabalhando com temas relacionados à computação quântica e informação quântica. Um exemplo é o trabalho aqui exposto pelos representantes do IFBA.

AGRADECIMENTOS

Os autores agradecem a Fundação de Amparo à Pesquisa do Estado da Bahia – FAPESB pelo financiamento de bolsa de Iniciação Científica.

REFERÊNCIAS

BENNETT, C.H., BRASSARD, G., **Quantum cryptography,** In Proccedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175-179, New York, 1984. IEEE Bangalore, India, December 1984.

COELHO, A.S.; BARBOSA, F.A.S; CASSEMIRO, K.N; VILLAR, A.S.; MARTINELLI, M e NUSSENZVEIG, P. **Three-Color Entanglement.** Science, n. 6, 2009, vol. 326., pp. 823 – 826.

DEUTSCH, D. **Quantum theory, the Church-Turing Principle and the universal quantum computer.** Pro. R. Soc. Lond. A, 400:97, 1985.

FEYNMAN, R.P. **Simulating physics with computers.** Int. J. Theor. Phys., 21:467, 1982.

FOLHAONLINE **- Experimento na USP mostra base de Internet do futuro** Disponível em: <http://www1.folha.uol.com.br/folha/ciencia/ult306u625766.shtml>

IBM's **Test-Tube Quantum Computer Makes History** - Disponível em: <http://www-03.ibm.com/press/us/en/pressrelease/965.wss>.

INFO online **- Computador quântico já funciona.** Disponível em: <http://info.abril.com.br/aberto/infonews/022007/15022007-3.shl>.

NewScientist - **Cientistas anunciam primeiro computador quântico programável.** Disponível em: <http://www.newscientist.com/article/dn18154-first-universal-programmable-quantum-computer-unveiled.html>.

MANIN, Y. **Computable and uncomputable** (*in Russian*), Sovetskoye Radio, Moscou, 1980.

NIELSEN, M.A; CHUANG, I.L. **Computação Quântica e Informação Quântica** (tradução Ivan S. Oliveira), Porto Alegre, Bookman Cia, 2005.

OLIVEIRA, I.S. **Física Moderna para iniciantes, interessados e aficionados**, vol. II, São Paulo, Editora da Física, 2005.

SHOR, P.W. **Scheme for reducing decoherence in quantum computer memory**, Physical Review A, n. 4, 1995, vol. 52.