A PROGRAMAÇÃO QUÂNTICA: APROVEITANDO OS CÓDIGOS CLÁSSICOS

Carlos A. Lungarzo

Um computador processa um ente especial lógico/físico, a **informação**, que é codificada em dígitos binários, transportada por objetos lógicos do sistema, os programas, e operada pelas **portas** lógicas que usam a lógica proposicional clássica. Os componentes lógicos se traduzem em fenômenos elétricos (tensões) que fazem possível sua execução pelo processador.

O computador quântico (CQ) preserva a relação entre lógica e física, pois também recebe informação (**bits quânticos** ≡ **qubits**) e a transforma em fenômenos. O diferente é o suporte físico: a porta lógica clássica é um circuito sob as leis clássicas do eletromagnetismo, mas a porta quântica está regida pela mecânica quântica (MQ). Assim, também os **estados** são diferentes: enquanto os clássicos são tensões elétricas, medidas de maneira independente, os estados quânticos nem sempre são **puros**, pois podem consistir na **superposição** de outros.

Usualmente, um sistema quântico é representado por um 'espaço de Hilbert': um espaço vetorial complexo com produto escalar, de dimensão talvez infinita. As portas lógicas quânticas não são circuitos, mas **operadores** (matrizes) aplicados aos vetores de um (sub) espaço bi-dimensional: H^2. Por sua vez, as unidades de informação não são os bits 0 e 1 que indicam o estado (aberto/fechado) do circuito, mas os qubits $|0\rangle$, $|1\rangle$ que indicam estados ortogonais em H^n ($2 \leq n$).

A base de informação quântica também é binária, pois os qubits básicos são $|0\rangle$ $|1\rangle$, mas eles não são os únicos possíveis. Todo objeto $E = \boldsymbol{\alpha}|0\rangle + \boldsymbol{\beta}|1\rangle$, com $|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = 1$, é um estado, mas, se ambos $|\alpha|,|\beta| > 0$, então E já não é puro, pois é superposição dos básicos.

Os computadores quânticos precisarão de programas especiais, mas alguns deles podem ser simulados no paradigma clássico

A superposição é comum a diversos processos ondulatórios, mas esta forma é típica da MQ. Na mecânica clássica, os estados são conjuntos **mensuráveis** do espaço de configuração (de dimensão finita) e formam uma álgebra de Boole, de característica 2. Portanto, não existe um equivalente da combinação linear de vetores, nem da superposição de estados.

A existência de 'bits' quânticos superpostos é a principal causa do interesse nos CQ's, pois um CQ poderia utilizar não apenas os estados básicos $\{|0\rangle,|1\rangle\}$, mas também os estados de superposição, que também correspondem a qubits. Isso permitiria processamentos **fortemente paralelos**, pois a informação se distribuiria entre os diversos estados de maneira simultânea. Ora, para que as leis quânticas se tornem relevantes, o processador deve ter grandezas de ordem compatível com a constante de Planck, o que exige objetos nanoscópicos. Uma escolha natural deveria incluir átomos, íons, partículas, etc. O modelo constituído por íons aprisionados em campos magnéticos é um dos mais aceitos (1).

As atuais tendências da pesquisa se dirigem, por um lado, à construção de um CQ real e, por outro, à formulação dos programas que rodariam nesses CQ's.

O primitivo otimismo sobre a possibilidade de fabricar CQ's reais foi arrefecendo por causa de observações (2) sobre a sensibilidade da informação quântica ao ambiente e o caráter quase inevitável de erros de inicialização. Recentemente, foram conjeturados métodos para inibir essas perturbações, e no começo do ano, foi criada uma porta lógica robusta, usando dois íons de berílio aprisionados (3). Mas, a possibilidade de um computador quântico "pleno" é ainda confusa. Existe um estudo recente da atividade brasileira neste campo (4).

As outras tendências de pesquisa seguem a direção lógica: construção de linguagens e programas.

Mesmo em alto nível, a formalização da estrutura de um programa exige conhecer as variedades de organização dos CQ's, para saber de que maneira a parte lógica deve ser expressada pela parte física. No entanto, até que apareça uma arquitetura completa, especificar uma linguagem com grande detalhe será difícil.

É possível, porém, uma aproximação clássica, motivada pela maneira em que um 'programa' para um computador clássico (a máquina de Turing) foi projetado antes da construção do computador físico. A possibilidade de estender essa máquina ao caso quântico já é conhecida (5). Existem algumas propostas de linguagem experimental (6) que utilizam esse caráter ideal do CQ.

As atuais pesquisas estão centradas em linguagens procedimentais estruturadas, que implementam programas que são tratados

como meta-programas clássicos, e cujo "objeto" é um CQ ideal. A linguagem de montagem é o formalismo dos operadores, ou seja, sua lógica é a lógica quântica em sentido estrito, abstraída das propriedades algébricas dos espaços de Hilbert, mas isso não é suficiente para implementar algoritmos quânticos, que precisam de uma linguagem de alto nível que, por sua vez, supõe linguagens livres de contexto não deterministas.

Uma máquina é determinista se cada estado possui um único estado "sucessor", enquanto que, numa máquina probabilística, podem existir vários "sucessores" com uma certa probabilidade. A máquina probabilística usará o meta-programa para controlar o CQ e processar as medições dos dados de saída.

Para manter a coerência entre ambas formas de programação, deve existir alguma correspondência entre computadores clássicos e CQ's[7]. O CQ ideal processa informação codificada em qubits, a transforma com suas portas lógicas e produz uma saída, que é a medida do estado final do CQ (vide figura). Nos computadores convencionais, o "último passo" do processamento é um estado elétrico que oscila usualmente entre 0 e 5 volts. Para o operador, a informação se apresenta em alto nível, onde esse estado é ignorado. Para o observador macroscópico, uma saída é um caractere, um som, uma imagem, mas não um estado elétrico.

No CQ considerado como objeto de programação por um meta-computador clássico, a saída é um estado que deve ser medido de maneira probabilística (eventualmente, usando a função de onda). O meta-computador de controle deve decidir se a medida é ou não correta para o problema dado. Neste enfoque da programação quântica é importante descrever os elementos do CQ que executam funções análogas aos componentes clássicos. Isto poderia ser evitado se programássemos o CQ no nível de montagem, mas esse método esbarra com vários problemas: os escassos recursos da arquitetura quântica para o usuário, a dificuldade de preparar os qubits e o risco de produzir perturbações (como a perda de informação).

O meta-programa de controle pode ser escrito numa linguagem clássica, como PASCAL ou C. Portanto, não é surpreendente que a linguagem quântica utilize os tipos e variáveis dessas linguagens. Não obstante, nem sempre uma variável ou um tipo poderá ser interpretado da mesma maneira que na computação clássica, pois o objetivo do programa é processar resultados de medições do CQ, que são obtidas em função das leis da MQ e não da clássica.

Assumimos que o CQ foi descrito por sua função ψ, e que a dimensão do espaço de Hilbert associado é 2^n. Para cada número $k \leq n$, um vetor de dimensão k que pertence a um estado específico do CQ, é chamado registrador de comprimento k. Os registradores assumem o papel das variáveis na computação convencional.

Os procedimentos de um programa convencional correspondem aos operadores (matrizes) unitários no modelo matemático do CQ. Um operador unitário é inversível e, ainda, seu inverso é igual ao resultado de trocar seus componentes complexos pelos seus conjugados (e. g. (a+ib) por (a-ib)), e suas colunas pelas filas horizontais.

Um enunciado clássico do tipo "`if... else`" corresponde ao uso de um operador condicional. A aplicação desses operadores a um qubit é o resultado que depende de que um novo qubit (equivalente à condição booleana do enunciado clássico) seja habilitado.

Linhas de código de programas para CQ's têm aparência similar às linhas de linguagens clássicas, como C. Mas, dentro dos tipos de dados, alguns são específicos do CQ e não teriam função no caso clássico. Por exemplo, a expressão '`qureg`' refere-se a um tipo de dado cuja semântica contém os registradores quânticos.

Uma linguagem para programas de QC's deve poder implementar um algoritmo quântico. Para certos problemas, já foi possível encontrar algoritmos que, se implementados quanticamente, seriam mais eficientes que os clássicos (8). O que permite implementar um algoritmo em linguagens para CQ's, é a presença, nessas linguagens, de categorias formais (funções, operações, etc) que representem a matemática interna do CQ, ou seja, a própria lógica quântica.

Os problemas mais ricos da lógica dos CQ's estão relacionados com a implementação e redução da complexidade temporal de algoritmos. Uma proposta recente de otimização é a de aumentar a valência das portas lógicas. As portas clássicas são binárias, com os valores 0 e 1, como também são as quânticas com: $|0\rangle$ $|1\rangle$. No entanto, nas portas clássicas, a extensão ao caso polivalente não aparece como necessidade atual, mas, nas portas quânticas, pode simplificar alguns algoritmos (9).

Carlos Lungarzo é professor titular aposentado da área de lógica da Universidade Estadual de Campinas.

O autor agradece as vitais observações dos professores Alfredo Pereira Jr. E Sílvio Senho Chibene. Algumas não puderam ser aproveitadas por causa do espaço.

(1) SACKETT, C. et al. *Nature*, 404, 256 (2000)
(2) BENIOFF, P. *Superlattices and Microstructures*, vol. 23, N. 3/4, 1998, p. 408-417
(3) STEANE, A. *Nature*, 422, mar 2003, 387-8
(4) ZORZETTO, R. *Pesquisa Fapesp*, Abril 2003, num. 86, p.54-59.
(5) BENIOFF, P., Physica D, 1998, 12-19.
(6) ÖMER, B., A Procedural Formalism for Quantum Computing (Master Dissertation, Tech. Univ. Vienna, 1998)
(7) WALLACE, J., "Quantum Computer Simulators", in Partial Proceedings of the 4th Int. Conference CASYS 2000
(8) VAN DAM & SEROUSSI, Efficient Quantum Algorithms for Estimating Gauss Sums 2002, in *http://www.hpl.hp.com/techreports/2002/HPL-2002-208.pdf*
(9) LUNGARZO C., Lógicas polivalentes na representação de portas clássicas e quânticas (Campinas, XIII EBL, 2003), em processo de publicação.