

doi: 10.11830/ISSN.1000-5013.201606017



Grover 算法量子处理架构的 设计与模拟

张洪涛, 代永涛, 涂玲英

(湖北工业大学 电气与电子工程学院, 湖北 武汉 430068)

摘要: 针对混合架构经典-量子算法的量子算法处理单元, 设计基于 Grover 算法的量子处理架构. 将一种用于量子计算仿真的量子程序设计语言引入 Grover 量子搜索算法中, 并在 Linux 操作系统中进行执行与模拟. 结果表明: 所提架构可以提高量子搜索算法的执行性能; 利用反馈调节可以有效地实现量子搜索算法的最佳性能.

关键词: Grover 量子搜索算法; 量子处理架构; 量子程序设计语言; 仿真

中图分类号: TP 301 **文献标志码:** A **文章编号:** 1000-5013(2016)06-0749-05

Design and Simulation of Quantum Processing Framework Based on Grover Algorithm

ZHANG Hongtao, DAI Yongtao, TU Lingying

(School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan 430068, China)

Abstract: As for a quantum algorithm processing unit with the hybrid architecture for classical-quantum algorithms, the quantum processing framework based on Grover's algorithm is designed. By applying the quantum programming language which is used in quantum computation to the research of Grover quantum search algorithm, then implemented and simulated the algorithm in Linux operating systems. The results show that the proposed framework can be used to improve the implementation performance of Grover algorithm. And the best performance of Grover algorithm can be achieved by using the feedback regulation.

Keywords: Grover quantum search algorithm; quantum processing framework; quantum programming language; simulation

量子计算机^[1]是一种遵循量子力学规律, 进行高速运算、存储及处理量子信息的物理装置, 计算速度较超级计算机提高数十亿倍. 由于它利用量子系统的可逆运算的特征, 可以有效解决耗热问题. 量子计算机与经典计算机技术相比, 具有较高的计算性能, 所以受到了科学界和高新产业界的青睐^[2]. 近几年, 已有许多学者和公司对其进行了进一步研究及完善, 先后在量子仿真计算框架^[3-4]、量子计算机体系结构^[5-11]、量子处理执行效率^[12]等方面提出了多种改进措施, 并取得了较为瞩目的研究成果. 因此, 量子处理的研究为运行量子算法的量子处理器的体系结构的研究提供了一种新思路, 实现量子保密通信技术在电子商务和数据中心安全方面的应用, 具有一定的军事和经济效益, 应用前景广泛. Grover 量子搜索算法^[13-16]可用于图的着色、最短路径、排序等问题的求解, 还可以有效地破译 DES 密码体系, 已经形

收稿日期: 2016-04-26

通信作者: 张洪涛(1963-), 男, 教授, 博士, 主要从事量子计算与量子信息、嵌入式系统开发的研究. E-mail: zhanght@mail.hbut.edu.cn.

基金项目: 湖北省武汉市科技局资助项目(2013011801010600)

成一个能够适应各种不同搜索需求且较为完整的搜索算法体系. 本文在设计量子计算的核心量子处理器中,采用基于 Grover 量子搜索算法的新思路,提出一种基于 Grover 量子搜索算法的量子处理单元 QAPU 架构的方案.

1 量子算法处理单元

1.1 量子计算机系统

量子算法处理单元(quantum algorithm processing unit, QAPU)^[17-18]是可以运行量子算法的量子装置,它需要一个混合的体系结构执行量子 and 经典操作,其对应操作分别运行于量子计算机和经典计算机上. QAPU 可作为量子计算机系统 中的量子节点,其中,量子计算机系统是由大量的小节点和量子互联总线构成. 节点执行实际的计算,并且每一个节点由量子部分和经典部分两部分组成. 量子部分包含量子数据,经典部分包含实时测量和控制电路的量子装置,相应的操作分别由量子部分的节点和经典部分的节点进行执行,并用 QAPU 和 CPU 代替. 量子计算机系统的原理框图,如图 1 所示. 图 1 中:虚线表示非实时通信;实线表示实时通信.

1.2 量子处理单元的架构

量子处理单元的架构,如图 2 所示. 图 2 中: $|x\rangle$ 和 $|y\rangle$ 分别表示控制寄存器和目标寄存器的输入, G_c 和 G_t 为 Hadamard 变换或量子傅里叶变换; G'_c 为 Hadamard 变换或量子傅里叶变换的逆变换(QFT⁻¹); U_f 为一种么正变换; $|x,y\rangle\overset{U_f}{\longrightarrow}|x,y\oplus f(x)\rangle$, \oplus 表示按位模 2 加法;开关 S_0, S_1, S_2 和 S_3 用于控制反馈迭代.

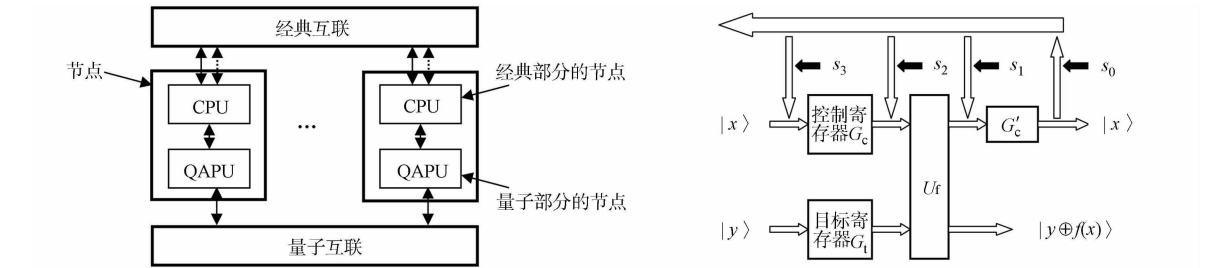


图 1 量子计算机系统的原理框图

图 2 量子处理单元的架构

Fig. 1 Block diagram of quantum computer system

Fig. 2 Framework of quantum algorithm processing unit

2 架构设计与模拟实现

2.1 量子处理架构的设计

Grover 量子搜索算法包括不同量子态的 n 量子比特的 $|x\rangle$ 和 1 量子比特的 $|y\rangle$,分别对应于控制寄存器和目标寄存器的输入. 作为该算法的量子电路,算法从计算机的初态 $|0\rangle^{\otimes n}$ 开始,用 Hadamard 变换使计算机处于均衡叠加态,即

$$|\psi\rangle = \frac{1}{N^{1/2}}(|0\rangle + |1\rangle + \cdots + |\tau\rangle + \cdots + |N-1\rangle) = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle.$$

式中: $|\tau\rangle$ 为寻找的标记态; $N=2^n$ 为元素个数.

量子搜索算法由反复应用 Grover 迭代(G)或 Grover 算子的量子子程序组成,即

$$G = G'_c U_f = H^{\otimes n} U_0 \perp H^{\otimes n} U_f.$$

式中: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ 表示 Hadamard 变换; $H^{\otimes n}$ 表示 n 量子比特 Hadamard 变换的并行运算; U_f 的作用是将 $|x\rangle \rightarrow -|x\rangle$ (如果 x 是一个搜索解),否则,不变; U_0 的作用是变 $|0\rangle \rightarrow -|0\rangle$,且保持其他所有的计算基不变.

为了确保经过 $O(\sqrt{N})$ 次 Grover 迭代^[19],需要一个反馈完成搜索过程,而通过使用开关 S_0, S_1, S_2 和 S_3 就可以很容易地实现这种反馈. 在 Grover 量子搜索算法中,这种反馈调节需要关闭 S_0 和 S_2 ,打

开 S_1 和 S_3 (此处省略, 说明开关为打开状态). 在设计构架中, 可以通过反馈机制将 Grover 迭代过程中相位反转的结果反馈给控制寄存器的输入, 进而确保均值反演操作的有效执行, 从而有效实现量子搜索算法的最佳性能. 其量子处理框架, 如图 3 所示.

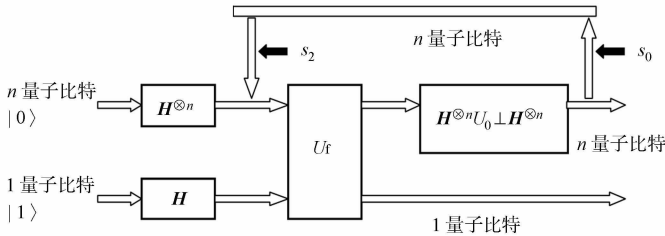


图 3 Grover 量子搜索算法的量子处理框架

Fig. 3 Quantum processing framework for Grover's quantum search algorithm

一般来说, 在最坏情况下要识别标记项, 对于确定性算法需要查询 $2^n - 1$ 次, 概率性算法也需要查询 $O(2^n)$ 次, 但是对于 Grover 量子搜索算法却只需要查询 $O(\sqrt{2^n})$ 次, 并且已被证明是最优的^[20].

对于 N 个元素、搜索问题解 $M=1$ 的搜索空间, 其运行时间为 $O(\sqrt{2^n})$ 次运算, 以 $O(1)$ 概率成功, 需应用 Grover 迭代的次数为

$$R \approx \lceil \pi \sqrt{2^n} / 4 \rceil.$$

2.2 量子模拟平台的搭建及相关配置

QCL(quantum computation language)^[21-22] 是一个结构化命令式量子程序设计语言, 其语法和 C/Pascal 类似. 它提供了基本的量子运算符和量子态的表示方法, 能实现量子位的各种么正变换及测量操作. 在 Linux 操作系统中有如下 5 个安装过程.

- 1) 下载 QCL 的安装包.
- 2) 下载并安装 bison 和 flex 工具.
- 3) 安装依赖库, 如 libplot2c2 和 libplot-dev 等.
- 4) 下载一个最新的 readline 文件, 然后解压并安装. `tar xvzf readline-5.2.tar.gz; ./configure; make; make install.`
- 5) 将 qcl-0.6.4.tar.gz 解压后, 进入所在文件夹; 然后, 直接运行 make 命令就会在当前文件夹中生成 qcl 可执行文件, 至此说明 qcl 已经安装成功; 最后, 直接运行. /qcl, 就可以进入 qcl 量子模拟环境.

2.3 实验结果及分析

当 $n=100, 10\,000, 10\,000\,00$ 时, Grover 量子搜索算法搜索结果, 分别如图 4(a), (b), (c) 所示. 为了更直观地反映该算法的成功率, 通过数据模拟得到算法的成功率 P 与搜索问题的解在整个搜索空间中所占的比例 M/N 之间的关系, 如图 4(e) 所示.

为了进一步说明搜索过程中幅值变化情况, 在 $n=20$ 量子比特的搜索空间 $N=2^{20}=1\,048\,576$ 中搜索某特定元素 1 000 000, 特定元素(所需记录)和非特定元素(其他记录)的幅值随迭代次数的变化关系, 如图 4(d), (f) 所示.

由图 4(a), (b), (c) 可知: Grover 量子搜索算法每搜索一次, 可同时检查所有 N 个数, 且利用量子叠加和量子纠缠的特性, 量子干涉效应引起的操作运算重复 \sqrt{N} 次后, 平均获得正确答案的概率为 $1/2$. 如果依此, 再多重复进行几次操作, 便可以以较高的概率(接近于 1)找到正确答案, 这与算法的实例化是一致的.

由图 4(d) 可知: 执行此次搜索问题所需的量子比特数和迭代次数分别为 20 和 805.

由图 4(e) 可知: Grover 算法仅在若干离散点处的成功率为 1, 随着 M/N 的增大, 成功率迅速下降, 直至失效. 当要搜索的目标数目超过数据库中记录总数的 $1/4$ 时(如 $N=10\,000$), Grover 量子搜索算法搜索成功的概率呈下降趋势; 且当要搜索的目标数目超过数据库记录的一半时(如 $N=1\,000\,000$), 算法几乎失效.

```
root@ubuntu:/home/qcl/qcl-0.6.4# ls
CHANGES  dump.h  extern.cc  Makefile  plot.o  quheap.cc  syntax.o
cond.cc   dump.o  extern.h  options.cc  print.cc  quheap.h  typcheck.cc
cond.h    error.cc  extern.o  options.h  print.o  quheap.o  typcheck.o
cond.o    error.h  format.cc  options.o  qcl      README    types.cc
COPYING   error.o  format.h  parse.cc   qcl      symbols.cc  types.h
debug.cc  eval.cc  format.o  parse.h    qcl.cc   symbols.h  types.o
debug.h   eval.o  lex.cc    parse.o    qcl.lex  symbols.o  yacc.cc
debug.o   exec.cc  lex.o     plot.cc    qcl.o    syntax.cc  yacc.h
dump.cc   exec.o  lib       plot.h     qcl.y    syntax.h  yacc.o

root@ubuntu:/home/qcl/qcl-0.6.4# ./qcl
QCL Quantum Computation Language (32 qubits, seed 1437373081)
[0/32] 1 |0>
qcl> include "grover.qcl"
qcl> grover(100)
: 7 qubits, using 5 iterations
: measured 100
[0/32] 1 |0>
qcl>
```

(a) $n=100$

```
root@ubuntu:/home/qcl/qcl-0.6.4# ./qcl
QCL Quantum Computation Language (32 qubits, seed 1437373853)
[0/32] 1 |0>
qcl> include "grover.qcl"
qcl> grover(100000)
: 14 qubits, using 51 iterations
: measured 8848
: measured 5631
: measured 10000
[0/32] 1 |0>
qcl> grover(10000)
: 14 qubits, using 51 iterations
: measured 8569
: measured 3734
: measured 10000
[0/32] 1 |0>
qcl> grover(10000)
: 14 qubits, using 51 iterations
: measured 10000
[0/32] 1 |0>
qcl>
```

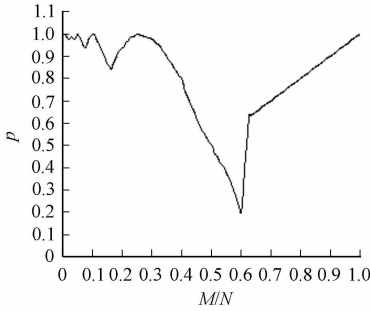
(b) $n=10\ 000$

```
root@ubuntu:/home/qcl/qcl-0.6.4# ./qcl
QCL Quantum Computation Language (32 qubits, seed 1437375474)
[0/32] 1 |0>
qcl> include "grover.qcl"
qcl> grover(1000000)
: 17 qubits, using 143 iterations
: measured 82148
: measured 124261
: measured 87794
: measured 5391
: measured 100000
[0/32] 1 |0>
qcl> grover(1000000)
: 20 qubits, using 403 iterations
```

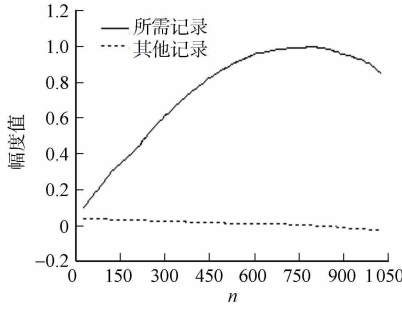
(c) $n=1\ 000\ 000$

```
root@ubuntu:/home/qcl/qcl-0.6.4# ./qcl
QCL Quantum Computation Language (32 qubits, seed 1450699357)
[0/32] 1 |0>
qcl> include "grover.qcl"
qcl> grover(1048576)
: 20 qubits, using 805 iterations
```

(d) 所需量子比特数和迭代次数



(e) 成功率与 M/N 的关系



(f) 幅值随迭代次数的变化关系

图 4 Grover 量子搜索算法的模拟仿真

Fig. 4 Simulation of Grover quantum search algorithm

由图 4(f)可知:当迭代次数小于 805 时,所需记录的幅值曲线收敛于 1.0,而其他记录的幅值曲线收敛于 0.在经过 805 次迭代后,其他记录的幅值变为 0,而所需记录的幅值达到 1,此时搜索到真解,直到运行 1 024 次迭代才停止搜索.这与理论计算搜索到特定元素所需的迭代次数为 $(\pi/4)\sqrt{N}\approx/805$,总运行时间为 $O(\sqrt{N})=1\ 024$ 次迭代是一致的.同时,该搜索过程可以形象地反映 Grover 量子搜索算法中幅度值变化情况、所需迭代次数和总运行时间.

3 结 束 语

提出一种基于 Grover 量子搜索算法的量子处理架构的方案,在 Linux 操作系统中,通过量子程序设计语言 QCL 模拟实现了 Grover 量子搜索算法,并通过实验数据说明了 Grover 量子搜索算法存在的缺陷与不足,以及 Grover 量子搜索算法中幅度值与迭代次数的变化情况.该架构可以用来提高量子搜索算法的的执行性能,利用反馈调节可以有效保证经过 $O(\sqrt{N})$ 次 Grover 迭代完成搜索过程,为运行量子算法的量子处理器的体系结构的研究提供了一种新思路.

参考文献:

[1] 方粮,刘汝霖.量子计算机:量子算法与物理实现[J].计算机工程与科学,2012,34(8):32-43.

- [2] WEIMER H, ULLER M, LESANOVSKY I, et al. A rydberg quantum simulator[J]. *Nature Physics*, 2010, 6(5): 382-388.
- [3] AGHAEI M R S, ZUKARNAIN Z A, MAMAT A, et al. An architectural framework for quantum algorithms processing unit[J]. *Lecture Notes in Engineering and Computer Science*, 2010, 2180(1): 303-309.
- [4] LEE Y H, KHALIL-HANI M, MARSONO M N. An FPGA-based quantum computing emulation framework based on serial-parallel architecture[J]. *International Journal of Reconfigurable Computing*, 2016, 2016(5): 1-18.
- [5] WANG Anming. Quantum central processing unit and quantum algorithm[J]. *Chinese Physics Letters*, 2002, 19(5): 620-622.
- [6] 薛飞. 量子计算的核磁共振实验实现及量子 CPU 的设计[D]. 合肥: 中国科学技术大学, 2004: 90-96.
- [7] BRIAN R L C, COREY I O, GRANVILLE E O, et al. Classical emulation of a quantum computer[J]. *International Journal of Quantum Information*, 2016, 14(1): 1-12.
- [8] METER R V, OSKIN O. Architectural implications of quantum computing technologies[J]. *ACM Journal on Emerging Technologies in Computing Systems*, 2006, 2(1): 31-63.
- [9] RONNOW T F, WANG Z, JOB J, et al. Defining and detecting quantum speedup[J]. *Science*, 2014, 345(6195): 420-424.
- [10] TÉLLEZ V H, CAMPERO A, LUGA C, et al. An architecture of quantum CPU[J]. *NSTI-Nanotech*, 2007(3): 205-208.
- [11] 吴楠, 宋方敏. 一种高效容错的通用量子计算机体系结构[J]. *计算机学报*, 2009, 32(1): 161-168.
- [12] 宋辉. 量子计算机体系结构及模拟技术的研究与实现[D]. 长沙: 国防科学技术大学, 2003: 25-33.
- [13] GROVER L K. A fast quantum mechanical algorithm for database search[C]//28th Annual ACM Symposium on the Theory of Computation. New York: ACM Press, 1996: 212-219.
- [14] 卢春红. 3 量子位的 Grover 量子搜索算法的核磁共振的仿真实现[D]. 无锡: 江南大学, 2007: 5-21.
- [15] 马宏源, 王洪福, 张寿. 在热腔中实现 Grover 量子搜索算法[J]. *延边大学学报*, 2008, 34(1): 27-30.
- [16] 韩广甫. Grover 量子搜索算法的改进及其在图像检索中的应用[D]. 南京: 南京邮电大学, 2013: 13-34.
- [17] AGHAEI M R S, ZUKARNAIN Z A. A quantum processing framework for quantum algorithms[J]. *Majlesi Journal of Electrical Engineering*, 2012, 6(3): 1-7.
- [18] AGHAEI M R S, ZUKARNAIN Z A. A hybrid architecture approach for quantum algorithms[J]. *Journal of Computer Science*, 2009, 5(10): 725-731.
- [19] MICHAEL A N, CHUANG I L. 量子计算和量子信息(一)[M]. 赵千川, 译. 北京: 清华大学出版社, 2003: 228-231.
- [20] ZALKA C. Grover's quantum searching algorithm is optimal[J]. *Physical Review A*, 1997, 60(4): 2746-2751.
- [21] ÖMER B. A procedural formalism for quantum computing[D]. Vienna: Technical University of Vienna, 1998: 16-83.
- [22] ÖMER B. Structured quantum programming[D]. Vienna: Technical University of Vienna, 2003: 45-102.

(责任编辑: 陈志贤 英文审校: 吴逢铁)