

文章编号: 1007-4627(2002)02-0275-03

Brüschweiler 量子搜索算法的改进及其实验实现*

杨晓冬, 魏达秀, 罗 军, 缪希茹

(中国科学院武汉物理与数学研究所, 波谱与原子分子物理国家重点实验室, 湖北 武汉 430071)

摘 要: 量子计算与经典计算相比, 能够极大地提高运算速度, 解决一些经典计算不能解决或很难解决的问题. 对于在无序数据库中进行搜索这类问题, 可以用量子算法, 如 Brüschweiler 量子搜索算法来解决. 与经典算法相比, Brüschweiler 量子算法能够指数次地提高搜索速度.

在 Brüschweiler 提出的算法中, 数据量子位和观测量子位(辅助量子位)是分开的, 属于不同的量子位. 通过研究, 对 Brüschweiler 算法作了改进, 使之不需要用辅助量子位, 就可以达到指数次提高搜索速度的目的. 改进后的 Brüschweiler 量子算法有利于简化实验的设计和实现过程. 同时还利用核磁共振实验, 演示了改进后的 Brüschweiler 量子算法的实现.

关键词: Brüschweiler 算法; 量子计算; 核磁共振

中图分类号: O413 **文献标识码:** A

1 Brüschweiler 量子搜索算法简介

近年来量子计算^[1]的研究已趋于热点, 运用某些特定量子算法的量子计算机能够极大地提高运算速度. 例如, 对于在无序数据库中搜索出某一特定项这类问题来说, 利用 Brüschweiler 量子搜索算法^[2]的量子计算机, 其运算速度比经典算法有了指数量级的提高.

Brüschweiler 量子搜索算法所要解决的问题可以描述为: 考虑给定的由 $N(N=2^n)$ 个数组成的数据库 $x = \{0, 1, 2, 3, \dots, N-1\}$, 其中除一个数 z 满足函数关系 $f(z)=1$ 外, 其它的数均满足 $f(x)=0$, 现要从数据库 x 中找出 z .

用经典算法解决这个问题, 需要 $N=2^n$ 步, 步数 N 随着量子位数 n 的增加而呈指数增加, 而 Brüschweiler 提出的算法是利用 $n+1$ 个量子位, 其中包括 1 个辅助位和 $n(N=2^n)$ 个数据位来实现 n 量子位的搜索, 并且只需要做 n 次操作.

目前, 在诸多实现量子计算机的实验技术中, 核磁共振(NMR)^[3]是在研究量子计算领域取得成果最多、成就最大^[4-7]的一种实验技术, 最近 NMR 实验完成了演示 Shor 因子分解算法的工作^[7]. 我们利用 NMR 实验验证了改进后的 Brüschweiler 量

子搜索算法.

我们以四量子位的体系 I_0, I_1, I_2, I_3 为例(I_0 为辅助位量子位, I_1, I_2, I_3 为数据量子位)来说明原始的 Brüschweiler 算法^[2]在 NMR 实验中的实现. Brüschweiler 算法是利用辅助量子位, I_0 来分别判断数据量子位 $I_i(i=1, 2, 3)$ 的状态, 从而搜索出目标态. 这里假设要搜索的目标态为 $\alpha\beta\alpha$, 即只有当 $z=010$ 时, $f(z)=1$, 其具体过程为: 首先, 以 $I_1^{\uparrow}I_0^{\uparrow}$ 为初始态, 并且 $I_1^{\uparrow}I_0^{\uparrow} = I_1^{\uparrow}(I_2^{\uparrow}I_3^{\uparrow} + I_2^{\downarrow}I_3^{\downarrow} + I_2^{\uparrow}I_3^{\downarrow} + I_2^{\downarrow}I_3^{\uparrow})I_0^{\uparrow}$, 经过一个幺正变换 U_f (U_f 的作用是交换态 $\alpha\beta\alpha$ 和 $\alpha\beta\alpha\beta$, 而其余的态保持不变)后, 体系的状态变为: $\rho = I_1^{\uparrow}I_2^{\uparrow}I_3^{\uparrow}I_0^{\uparrow} + I_1^{\uparrow}I_2^{\downarrow}I_3^{\downarrow}I_0^{\uparrow} + I_1^{\uparrow}I_2^{\uparrow}I_3^{\downarrow}I_0^{\downarrow} + I_1^{\uparrow}I_2^{\downarrow}I_3^{\uparrow}I_0^{\downarrow}$. 对核自旋 I_0 来说, 在幺正变换 U_f 前后, 其谱线强度有变化. 但是如果以 $I_1^{\uparrow}I_0^{\uparrow}$ 为初始态, 那么经过幺正变换后, 体系的状态不变, 此时 I_0 的谱线强度在幺正变换前后也是不变的.

由以上的讨论可知, 设初始态为 $I_i^{\uparrow}I_0^{\uparrow}(i=1, 2, 3)$, 如果我们事先假设的数据量子位 I_i 的状态是正确的, 则辅助量子位 I_0 的谱线强度在幺正变换 U_f 前后会发生变化; 反之, 若 I_0 的谱线强度没有变化, 则说明原先假设的数据量子位 I_i 的状态不

收稿日期: 2002-03-05; 修改日期: 2002-03-20

* 基金项目: 国家自然科学基金资助项目(19974064)

作者简介: 杨晓冬(1977-), 男(汉族), 湖北襄樊人, 博士, 从事核磁共振量子计算研究.

对.

若对数据量子位 $I_i (i = 1, 2, 3)$ 依次做如上所示的操作, 即可对数据位 I_i 逐位判断出我们要搜索的目标态.

由以上过程可知, Bruschweiler 算法利用 $n+1$ 个量子位实现了 n 个量子位的搜索.

2 Bruschweiler 量子搜索算法的改进

在文献[2]中, Bruschweiler 提出利用辅助量子位可以帮助实现 n 次搜索出目标态. 我们经过研究, 提出了一种改进后的方法, 该方法不需要用到辅助量子位, 而是通过观测数据量子位谱线强度的变化来实现量子搜索.

在 Bruschweiler 算法中, 我们分析了 U_f 的作用, 发现通过改变 U_f 的形式, 使之变为 U'_f , 可以用 n 量子位实现 n 量子位的搜索. 上节提到的 U_f 可以分解成: $U_f = (\pi/2)_y^3 P(\pi/2)_{-y}^3$, 式中 $\pi/2$ 表示磁化强度矢量翻转角为 $\pi/2$ 的射频脉冲, 上标 I_3 表示射频脉冲所作用的核自旋, 下标 y 表示射频脉冲的相位. 这里仍设 $z=010$, 对应的 P 的矩阵形式为

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

改进后的 Bruschweiler 算法的实现过程可表述为:

(1) 以 $I_1^a I_3^a$ 为初始态, 以 I_3 为观测核, 因为 $I_1^a I_3^a = I_1^a (I_2^a + I_2^b) I_3^a$, 经过 U_f 变换后, 如果核自旋 I_3 的谱线强度发生变化, 则可判断 I_1 处于 I_1^a 是正确的.

(2) 以 $I_2^a I_3^a$ 为初始态, 以 I_3 为观测核, 因为 $I_2^a I_3^a = (I_1^a + I_1^b) I_2^a I_3^a$, 经过 U_f 变换后, 如果 I_3 的谱线强度不变, 则可知 I_2 应处于 I_2^a ; 否则, 若强度发生变化, 则 I_2 应处于 I_2^b 态.

(3) 若已经知道了 I_1, I_2 的状态, 要想判断 I_3 的状态, 可以采用如下的方法: 以 $I_1^a I_3^a$ 为初始态, 以 I_1 为观测核, 因为 $I_1^a I_3^a = I_1^a (I_2^a + I_2^b) I_3^a$, 运用幺正变换 U'_f , 系统的状态变为

$$I_1^a I_3^a = I_1^a (I_2^a + I_2^b) I_3^a = I_1^a I_2^a I_3^a + I_1^a I_2^b I_3^a$$

$$\xrightarrow{U'_f} I_1^a I_2^a I_3^a + I_1^b I_2^a I_3^a.$$

这时观察核自旋 I_1 的谱线, 如果其谱线强度发生变化, 说明我们最初假定 I_3 处于 I_3^a 是正确的, 如果谱线强度不变, 则 I_3 处于 I_3^b .

以上步骤中, U_f, U'_f 可表示为如下形式:

$$U_f = \left(\frac{\pi}{2}\right)_y^{I_3} P\left(\frac{\pi}{2}\right)_{-y}^{I_3},$$

$$U'_f = \left(\frac{\pi}{2}\right)_y^{I_1} P\left(\frac{\pi}{2}\right)_{-y}^{I_1},$$

这样, 利用数据量子位同时作为观测量子位, 可以实现不需辅助量子位的量子搜索. 这种改进后的方法可以类似地推广至更多量子位的核自旋体系中, 并且还可用于其它的物理体系.

另外, 我们在 NMR 实验中, 用 3 量子位体系, 演示了改进后的 Bruschweiler 量子搜索算法的运算过程.

3 结论

我们分析了 Bruschweiler 量子搜索算法的结构, 提出了不用辅助量子位的方法来实现搜索无序数据库中某一目标态. 这种改进后的 Bruschweiler 算法仍是以指数量级地提高了搜索速度, 并减少了实验所需的量子位, 从而降低了实验的复杂程度. 同时我们用 NMR 实验验证了改进后的 Bruschweiler 量子搜索算法.

参 考 文 献:

[1] Bennett C H, DiVincenzo D P. Quantum Information and Computation[J]. Nature, 2000, 404: 247.

[2] Bruschweiler R. Novel Strategy for Database Searching in Spin Liouville Space by NMR Ensemble Computing[J]. Phys Rev Lett, 2000, 85: 4 815.

[3] Jones J A. NMR Quantum Computation[J]. Prog NMR Spec-

- trosc, 2001, **38**: 325.
- [4] Marx R, Fahmy A F, Myers J M, *et al.* Approaching Five-bit NMR Quantum Computing[J]. Phys Rev , 2000, **A62**(1): 012310.
- [5] Knill E, Laflamme R, Matinez R, *et al.* An Algorithmic Benchmark for Quantum Information Processing[J]. Nature, 2000, **404**: 368.
- [6] Nielsen M A, Knill E, Laflamme R. Complete Quantum Teleportation Using Nuclear Magnetic Resonance [J]. Nature, 1998, **396**: 52.
- [7] Vandersypen L M K, Steffen M, Breyta G, *et al.* Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance[J]. Nature, 2001, **414**: 883.

Modification of Brüscheiler Quantum Searching Algorithm and Realization by NMR Experiment^{*}

YANG Xiao-dong, WEI Da-xiu, LUO Jun, MIAO Xi-jia

(*State Key Laboratory of Magnetic Resonance and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, China*)

Abstract: In recent years, quantum computing research has made big progress, which exploit quantum mechanical laws, such as interference, superposition and parallelism, to perform computing tasks. The most inducing thing is that the quantum computing can provide large rise to the speedup in quantum algorithm. Quantum computing can solve some problems, which are impossible or difficult for the classical computing.

The problem of searching for a specific item in an unsorted database can be solved with certain quantum algorithm, for example, Grover quantum algorithm and Brüscheiler quantum algorithm. The former gives a quadratic speedup, and the latter gives an exponential speedup comparing with the corresponding classical algorithm.

In Brüscheiler quantum searching algorithm, the data qubit and the read-out qubit (the ancilla qubit) are different qubits. We have studied Brüscheiler algorithm and proposed a modified version, in which no ancilla qubit is needed to reach exponential speedup in the searching, the data and the read-out qubit are the same qubits. The modified Brüscheiler algorithm can be easier to design and realize. We also demonstrate the modified Brüscheiler algorithm in a 3-qubit molecular system by Nuclear Magnetic Resonance (NMR) experiment.

Key words: Brüscheiler algorithm; quantum computing; nuclear magnetic resonance

* **Foundation item:** National Natural Science Foundation of China(19974064)