

# 量子线路仿真的分治算法

薛希玲<sup>1</sup>, 陈汉武<sup>1</sup>, 刘志昊<sup>1</sup>, 李志强<sup>1,2</sup>

(1. 东南大学计算机科学与工程学院, 江苏南京 210096; 2. 扬州大学信息工程学院, 江苏扬州 225009)

**摘要:** 本文将通用量子线路分为两类, 给出了每类中两种线路的酉算子表达式; 根据矩阵张量积转置相似定理, 实现了两类线路酉算子间的转换. 引入矩阵的直和运算并将其扩展到向量上, 以简洁的形式直观地表示出量子线路对输入向量的作用. 在将量子线路抽象为受控酉运算嵌套的基础上, 提出了仿真量子线路的分治算法. 相较于其他基于状态向量的仿真算法, 该算法避免了通过张量积运算生成酉矩阵, 从而节省了存储空间; 并且在仿真非平凡的量子线路时具有更好的时间复杂度.

**关键词:** 量子线路; 仿真技术; 状态向量; 分治算法

**中图分类号:** TP387      **文献标识码:** A      **文章编号:** 0372-2112 (2010) 02-0439-04

## Divide and Conquer Algorithms for Quantum Circuit Simulation

XUE Xi-ling<sup>1</sup>, CHEN Han-wu<sup>1</sup>, LIU Zhi-hao<sup>1</sup>, LI Zhi-qiang<sup>1,2</sup>

(1. School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China;

2. College of Information Engineering, Yangzhou University, Yangzhou, Jiangsu 225009, China)

**Abstract:** Quantum circuits are divided into two classes, and unitary operator expressions for two kinds of circuits in each class are offered. Transformation of unitary operators between two classes is presented according to tensor product transposition similarity theory. Besides, direct sum operation of matrices is adopted and expanded to vectors to elegantly represent the functions of quantum circuits on input vectors. On the basis of abstracting quantum circuits as controlled unitary operations, divide and conquer algorithms are proposed to simulate quantum circuits. In contrast to other algorithms based on state vector, our algorithms avoid generating matrix operators by tensor product, thus are considerably economy of memory space; and we also show that they are more time-efficient while simulating nontrivial quantum circuits.

**Key words:** quantum circuit; simulation technique; state vector; divide and conquer algorithm

## 1 引言

为降低量子仿真算法的复杂度, 或者用更有效的数据结构代替状态向量表示, 或者采取适当的压缩技术以减少状态向量和酉算子所需存储空间. 针对前者有稳定子形式方法、矩阵乘积状态表示 (MPS) 和带权图状态等<sup>[1]</sup>, 这类数据结构可以在经典计算机上有效地仿真特定的线路. 但据我们所知, 所有通用的量子仿真技术都基于状态向量表示.

迄今主要的仿真算法均采用基于 BDD 的结构来表示酉算子和状态向量, 如 QMDD<sup>[2]</sup> 和 QuIDD<sup>[3,4]</sup>, 仿真中用到的线性代数运算如矩阵-向量乘法可以在操作数规模二次方的时间内完成. 此类算法可以有效地仿真具有特定属性的状态向量和量子线路, 但在仿真非平凡线路时, 算法的复杂度仍将呈指数级增长. 最近 Samoladas 提出使用投影算子符号化地描述量子线路的方法<sup>[5]</sup> 提高

仿真算法的效率, 该算法仍然基于 BDD 结构.

本文将量子线路抽象为嵌套的受控酉运算, 并给出相应的酉算子表达式. 根据这种形式化的描述层层解析量子线路来确定线路上的受控量子门对状态向量的作用, 实现量子线路的仿真. 这种直接根据线路构造确定对输入状态的作用的方法避免了通过张量积运算生成酉算子, 从而节省了存储空间. 在时间复杂度上, 针对不能优化的非平凡电路, 我们将证明该算法的效率优于上述各算法.

## 2 预备知识

### 2.1 矩阵和向量的直和运算

为了能够直观地表示出酉算子的结构特点, 引入矩阵的直和运算  $\oplus$  并限定其操作数为两个同阶复方阵. 定义向量的直和运算为两个等长向量  $a$  与  $b$  的连接. 该运算将操作数的线性空间合在一起, 构成维数为两个操作

数维数之和的线性空间. 本文将用到直和运算的一个重要性质  $(A \oplus B)(a \oplus b) = (Aa) \oplus (Bb)$ .

只有在张量积运算的结果不呈指数级增长时, QMDD 和 QuIDD 才能有效地仿真量子线路, 限制了算法所能仿真的线路类型. 此外, 这种表示方式在线性代数运算时需要频繁地引用行列变量在图中的下标, 操作非常繁琐且容易出错. 本文分析量子线路中张量积运算自身的特点, 用酉矩阵和状态向量的直和运算直观地表示出量子线路对输入向量的作用, 用形式化的分析代替了具体的线性代数操作.

## 2.2 张量积矩阵的相似性

引理<sup>[6]</sup>  $B \otimes A = P^T(m, n)(A \otimes B)P(m, n)$ ,  $\forall A \in \mathcal{M}^{m \times m}, B \in \mathcal{M}^{n \times n}$ . 即  $A$  和  $B$  都是方阵时,  $B \otimes A$  置换相似于  $A \otimes B$ , 且置换矩阵  $P(m, n) \in \mathcal{M}^{m \times mn}$  仅依赖维数  $m$  和  $n$ ,  $P(m, n) = \sum_{i=1}^m \sum_{j=1}^n E_{ij} \otimes E_{ij}^T$ , 每个  $E_{ij} \in \mathcal{M}^{m \times n}$  在  $(i, j)$  位置的元素为 1, 其余元素为 0. 可知

$$P^T(m, n) = P^{-1}(m, n). \text{ 例如 } P(2, 2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

更一般地, 设  $A_1, \dots, A_k \in \mathcal{M}^{m \times m}, B_1, \dots, B_k \in \mathcal{M}^{n \times n}$ , 则  $B_1 \otimes A_1 + \dots + B_k \otimes A_k = P^T(m, n)(A_1 \otimes B_1 + \dots + A_k \otimes B_k)P(m, n)$ .

矩阵张量积运算的转置相似性是我们应用直和运算表示所有量子线路的基础. 利用这一性质将不能直接用该运算表示的酉算子转置后用直和运算表示, 统一了量子线路的表示形式. 特别地, 当  $m=2, n=2^k$  时, 置换矩阵  $P$  和  $P^T$  对向量的作用如下所示:

$$P(2, 2^{k-1})(x_0 x_1 x_2 \dots x_{n-3} x_{n-2} x_{n-1})^T = (x_0 x_2 \dots x_{n-2} x_1 \dots x_{n-3} x_{n-1})^T \quad (1)$$

操作结果为向量偶数项和奇数项的连接.

$$P^T(2, 2^{k-1})(x_0 x_1 \dots x_{n/2-1} x_{n/2} x_{n/2+1} \dots x_{n-2} x_{n-1})^T = (x_0 x_{n/2} x_1 x_{n/2+1} \dots x_{n-2} x_{n/2-1} x_{n-1})^T \quad (2)$$

即将向量的后  $n/2$  项分别插入到前  $n/2$  项之后.

$n$  阶矩阵-向量乘法操作需要  $O(n^2)$  的乘法操作, 而转置矩阵  $P(2, 2^{k-1})$  和  $P^T(2, 2^{k-1})$  与向量乘积的结果只需将该向量作  $O(n)$  次移位即可实现, 降低了算法的时间复杂度.

## 3 量子线路

### 3.1 量子线路的形式化表示

我们称包含量子门受控端的量子线路为门线路, 记为  $U$ . 在由门线路  $U$  和量子连线构成的量子线路中, 根据门线路上方的量子连线上是否有控制点, 可以将

此类线路分为两种, 如图 1 所示.

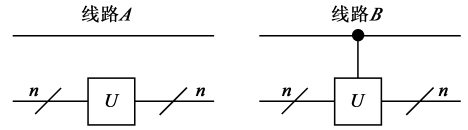


图1 门线路在下方的两种量子线路

线路  $A$  的酉算子表达式为

$$U_A = I_1 \otimes U_n = \begin{pmatrix} U_n & 0 \\ 0 & U_n \end{pmatrix} \quad (3)$$

线路  $B$  中的门为受控酉门, 其酉算子表达式比线路  $A$  的略复杂,

$$U_B = |0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes U_n = \begin{pmatrix} I_n & 0 \\ 0 & U_n \end{pmatrix} \quad (4)$$

这里  $I_k$  和  $U_n$  分别表示  $2^k$  阶单位阵和  $2^n$  阶酉矩阵.

当门线路在量子连线上方时, 同样根据底层量子连线上是否有控制点分为两种, 如图 2 所示.

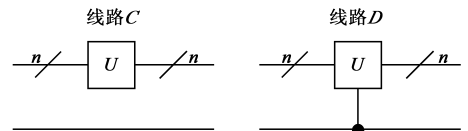


图2 门线路在上方的两种量子线路

我们发现, 线路  $C$  的酉算子表示形式可由线路  $A$  的表达式交换  $\otimes$  操作的两个操作数得到, 即:

$$U_C = U_n \otimes I_1 \quad (5)$$

同样, 线路  $D$  的酉算子表示形式可由线路  $B$  的表达式交换  $\otimes$  操作的两个操作数得到:

$$U_D = I_n \otimes |0\rangle\langle 0| + U_n \otimes |1\rangle\langle 1| \quad (6)$$

若子线路  $U$  中受控端量子门与量子连线的组合方式为上述四种线路中的任一种, 受控端量子门也可以是多量子比特门, 则线路  $A \sim D$  实现了用嵌套的方式描述通用量子线路. 实际量子线路由上述四种线路级联而成. 基于 BDD 表示的算法适于仿真特定的量子线路, 不具有通用性; 而基于上述形式化描述的仿真算法对线路结构、门的种类及输入向量等没有特殊要求, 适用于仿真通用量子线路.

### 3.2 量子线路功能的分解

分析式(3)和(4)矩阵张量积运算的结果可知, 线路  $A$  和线路  $B$  的酉算子用矩阵的直和运算表示为:

$$U_A = U_n \oplus U_n, \quad U_B = I_n \oplus U_n$$

同时, 将长度为  $2^{n+1}$  的状态向量  $|\varphi\rangle$  用等分的子向量  $|\varphi\rangle_0$  和  $|\varphi\rangle_1$  的直和运算表示为  $|\varphi\rangle = |\varphi\rangle_0 \oplus |\varphi\rangle_1$ .

应用直和运算的性质, 线路  $A$  和线路  $B$  对输入向量  $|\varphi\rangle$  的作用可分别表示如下:

$$U_A |\varphi\rangle = (U_n \oplus U_n)(|\varphi\rangle_0 \oplus |\varphi\rangle_1) = U_n |\varphi\rangle_0 \oplus U_n |\varphi\rangle_1 \quad (7)$$

$$U_B|\varphi\rangle = (I_n \oplus U_n)(|\varphi\rangle_0 \oplus |\varphi\rangle_1) = I_n|\varphi\rangle_0 \oplus U_n|\varphi\rangle_1 \quad (8)$$

线路  $C$  和线路  $D$  所对应矩阵形式较复杂,无法直接对其应用直和运算. 如当  $U = \begin{pmatrix} u_0 & u_1 \\ u_2 & u_3 \end{pmatrix}$  时,二者的酉算子描述分别为:

$$U_C = \begin{pmatrix} u_0 & 0 & u_1 & 0 \\ 0 & u_0 & 0 & u_1 \\ u_2 & 0 & u_3 & 0 \\ 0 & u_2 & 0 & u_3 \end{pmatrix}, \quad U_D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & u_0 & 0 & u_1 \\ 0 & 0 & 1 & 0 \\ 0 & u_2 & 0 & u_3 \end{pmatrix}$$

由 2.2 节矩阵张量积的转置相似性可知,  $U_n \otimes I = P^T(I \otimes U_n)P$ , 故线路  $C$  作用于状态向量  $|\varphi\rangle$  可以表示为:  $U_C|\varphi\rangle = P^T(I \otimes U_n)P|\varphi\rangle$ , 记  $|\varphi\rangle^P = P|\varphi\rangle$ , 则

$$U_C|\varphi\rangle = P^T(U_n|\varphi\rangle_0^P \oplus U_n|\varphi\rangle_1^P) \quad (9)$$

同理,线路  $D$  作用于状态向量  $|\varphi\rangle$  可以表示为:

$$U_D|\varphi\rangle = P^T(I_n|\varphi\rangle_0^P \oplus U_n|\varphi\rangle_1^P) \quad (10)$$

通过以上分析,式(7)~(10)将  $n+1$  比特的量子线路对输入向量的酉运算等价于  $n$  比特子线路或恒等线路分别对两个子向量作酉变换;而这里的子线路和子向量又可以继续递归分解直至量子门的受控端.

## 4 仿真算法

基于上述思想,采用分治法实现量子线路仿真算法. 设线路中只有受控端为单量子比特的量子门,两个核心算法的伪代码如下所示. 当线路中存在受控端为  $k$  量子比特的量子门时,只需将递归终结处定义为  $n=k$  即可.

函数的输入参数  $tline$  表示当前处理线路的第一条量子连线  $x_i \in \{x_0, x_1, \dots, x_{n-1}\}$ ,  $n$  为当前子线路条数,  $sbit$  为对应状态向量的起始下标,  $N=2^n$  是其长度.  $ApplyDown$  和  $ApplyUp$  均直接对状态向量作变换.

```

ApplyDown(tline, n, sbit) {
  if(n == 1) //受控端为单量子比特门
  ApplyGate(SglGate, sbit);
  else if (Circuit[tline] == NONE) {
    //量子线上无控制点处
    ApplyDown(tline + 1, n - 1, sbit);
  }
  else if (Circuit[tline] == CTRL) {
    //量子线上有控制点
    ApplyDown(tline + 1, n - 1, sbit + N/2);
  }
  else if (Circuit[tline] is a gate)
    ApplyUp(tline, LineNum, sbit);
}

ApplyUp(tline, n, sbit) {
  if(n == 1)
    ApplyGate(SglGate, sbit);
  else if (Circuit[tline] is a gate)
    TransPermute(sbit, N);
  else if (Circuit[tline + n - 1] == NONE) {
    ApplyUp(tline, n - 1, sbit);
  }
  else if (Circuit[tline + n - 1] == CTRL)
    ApplyUp(tline, n - 1, sbit + N/2);
}

```

$ApplyDown$ : 从第一条线开始自上而下逐层分解量

子线路,在无控制点处按式(7)递归向下,在控制点处按式(8)递归向下,直至  $n=1$  时应用单量子比特受控门(或  $n>1$  时应用多量子比特受控门)到对应向量;若在递归过程中遇到量子门,则调用  $ApplyUp$ .

$ApplyUp$ : 从下往上分解电路,过程与  $ApplyDown$  相似,不同之处在于根据式(9)和式(10)在递归开始之前先对状态向量应用置换  $P$ ,其操作如式(1)所示;递归返回之后对应状态向量应用置换  $P^T$ ,其操作如式(2)所示. 两次置换分别由内联函数  $Permute$  和  $TransPermute$  来完成.

设输入向量长度为  $N$ ,则在函数  $ApplyDown$  中,全部递归均按式(7)递归,最多执行次数  $T(N) = 2T(N/2)$ ,故最坏情况时间复杂度为  $O(N)$ ;在函数  $ApplyUp$  中增加了对状态向量的置换操作,由 2.2 节可知,两次置换共耗时  $2N$ ,  $T(N) = 2T(N/2) + 2N$ ,最坏情况时间复杂度为  $O(N \log N)$ .

## 5 实验结果分析

实验仿真量子傅立叶变换(QFT)<sup>[7]</sup>,其线路如图 3 所示.  $n$  量子 QFT 线路的长度(即包含量子门的个数)为  $n(n+1)/2$ . Hadamard 门的酉算子为  $U_H = \frac{1}{\sqrt{2}}$

$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ ,  $R_k$  的酉算子为  $U_{R_k} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}$ . 表 1 给出了仿真实验结果. 由表中可知,运行时间符合上述给出的分析,这里还要考虑当  $n$  增大时,线路长度亦随之增加.

表 1 仿真 QFT 实验结果

量子比特	13	14	15	16	17	18	19	20	21
时间(s)	1	3	7	16	34	89	197	435	918

量子线路的构成与算法的复杂度之间有如下关系:(1)线路中量子门的控制点越多,算法效率越高. 因为在有控制点的量子线上  $U_n|\varphi\rangle = |\varphi\rangle_0 \oplus U_{n-1}|\varphi\rangle_1$ , 递归只在一个分支进行,退化为线性算法;(2)受控量子门在线路越底层,算法效率越高. 此时  $ApplyUp$  函数的执行次数减少,附加的置换操作减少. 在较好地满足以上条件的情况下,算法的复杂度降低至与输入规模成正比的线性关系. 而就最一般的线路而言,在使用状

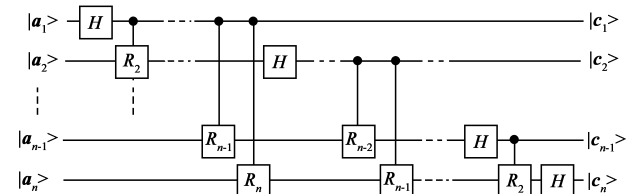


图3  $n$ 量子比特QFT电路逻辑图

态向量表示的情况下,量子线路状态向量大小为  $N$ ,对输入进行变换处理的量子线路仿真算法复杂度至少为  $N$ , ApplyDown 函数已达到此下界.

QuIDD 仿真算法<sup>[3]</sup>中,若酉算子用  $m$  个节点表示,作用于大小为  $N$  的状态向量,则运行时间的上界为  $O(m^2 N^2)$ . Samoladas 同样采用量子线路符号化表示,但仍使用 MTBDD 表示状态向量<sup>[5]</sup>,其最坏时间复杂度为  $O(|F| N^2)$ ,其中  $|F|$  是布尔投影算子的大小.在通用量子线路仿真过程中,线路和输入向量均无特定结构,将酉算子和状态向量表示成 BDD 图并不能得到有效的压缩,此时应用我们的算法效率将得到很大提高.

## 6 结论

本文提出了一种仿真通用量子线路的分治算法.该算法利用量子线路中构造酉算子时张量积运算自身的特点,引入酉算子和状态向量的直和运算来直观地表示出量子线路对输入向量的作用.我们利用矩阵张量积运算的相似性定理,用形式化地分析代替了具体的线性代数操作,使得利用分治思想仿真量子线路成为可能.该算法避免了基于 BDD 的结构仿真算法中出现的张量积运算和复杂的指标引用,更为简洁、直观.在仿真通用量子线路时,相较于复杂性极大依赖于量子线路的结构特点的其他仿真算法,我们论证了该算法的效率更高.

## 参考文献:

- [1] BROWNE D E. Efficient classical simulation of the quantum Fourier transform[J]. New Journal of Physics, 2007, 9(146): 1-7.
- [2] MILLER D M, et al. QMDD: A decision diagram structure for reversible and quantum circuits[A]. IEEE International Symposium on Multiple-Valued Logic (ISMVL)[C]. Washington, D C: IEEE Computer Society, 2006. 30-30.

- [3] VIAMONTES G F. Efficient Quantum Circuit Simulation. PhD thesis[D]. America: University of Michigan, 2007.
- [4] VIAMONTES G F, et al. Improving gate-level simulation of quantum circuits[J]. Quantum Information Processing, 2003, 2(5): 347-380.
- [5] SAMOLADAS V. Improved BDD Algorithms for the simulation of quantum circuits[A]. Proceedings of the 16th annual European Symposium on Algorithms (ESA)[C]. Heidelberg: Springer-Verlag, 2008. 720-731.
- [6] 陈景良, 陈向晖. 特殊矩阵[M]. 北京: 清华大学出版社, 2001. 434-437.
- [7] NIELSEN M A, CHUANG I L, Quantum Computation and Quantum Information[M]. Beijing: Higher Education Press, 2003. 217-220.

## 作者简介:



薛希玲 女, 1985 年 1 月出生于山东临沂, 硕士研究生. 2006 年始就读于东南大学计算机科学与工程学院. 主要研究方向为量子计算、量子算法与仿真.  
E-mail: xuexiling@gmail.com



陈汉武 男, 1955 年 11 月出生于江苏南京. 现为东南大学教授、博士生导师. 主要研究领域为经典信息论, 量子信息与量子计算, 数理解析.  
E-mail: hw\_chen@seu.edu.cn

刘志昊 男, 1982 年 10 月出生于湖南邵阳. 现为东南大学博士生, 主要从事量子信息和量子通信方面的研究.

李志强 男, 1974 年生于江苏姜堰, 博士研究生, 副教授. 主要研究方向为量子计算、可逆电路综合与测试.