目录

量子信息与量子计算

量子有限自动机

量子下推自动机

量子图灵机

第十四章
量子自动机

姚　刚

中国科学院信息工程研究所

目录

目录

量子信息与量子计算

量子有限自动机

量子下推自动机

量子图灵机

1 量子信息与量子计算

2 量子有限自动机

3 量子下推自动机

4 量子图灵机

量子信息科学

量子信息科学研究如何运用量子力学基本原理进行信息的存储、通信与处理，为未来的量子计算机和量子通信技术建立坚实的理论基础和保证。

量子信息科学的研究几乎覆盖现有信息科学的所有方面。

量子信息科学

就量子计算基础理论研究而言，包括量子计算的数学模型研究、量子软件的理论和方法研究、量子计算机体系结构研究、量子计算与人工智能领域的交叉研究等。

就量子通信基础理论研究而言，包括量子信道容量理论研究、量子密码术理论研究、量子中继器理论研究、量子隐形传态理论研究、量子网络理论研究、量子存储技术理论研究、量子纠缠态理论研究、量子控制理论研究等。

量子计算理论

量子计算理论属于量子信息科学研究领域的一个分支，它的研究划分大致为4个研究方向：

- 量子自动机与量子形式语言理论；
- 量子可计算性理论；
- 量子计算复杂性理论；
- 量子算法设计技术。

可逆计算

量子计算研究源于对可逆计算的研究，而研究可逆计算是为了克服计算机的能耗问题。

1961年，Landauer提出一个问题：逻辑不可逆是计算机的一个不可避免的特征吗？他的回答是肯定的，并且表明：无论什么时候，只要一个计算机扔掉它的前一个状态的信息，那么它就一定会生成相应量的熵。而且，扔掉或删除一个比特的信息，计算机将消耗至少$kT\ln 2$的能量。这就是著名的Landauer原理。

可逆计算机

1973年，Bennett令人惊奇地表明通用可逆图灵机是存在的！所有经典不可逆的计算机都可以改造为可逆计算机，而且不影响其计算能力。此外，这样的逻辑可逆计算至少在理论上，在适当的硬件条件下，能够以热动力学可逆的方式实现。

提出了两种通用可逆逻辑门：Toffili门和Fredkin门，表明通用可逆逻辑门确实是存在的。

量子图灵机

1980年，Benioff研究了图灵机的量子力学Hamilto型，详细地阐述了一个量子系统怎样模拟经典可逆图灵机的行为。

1982年，Feynman进一步问：量子物理能够由经典的通用计算机确切而又有效地模拟吗？他的回答是否定的，并且指出：按照量子力学原理建造的新型计算机对解决某些问题可能比常规计算机更有效。

1983年，Albert描述了一种所谓的量子力学测量自动机，它有一个经典自动机所没有的自测的性质。

量子图灵机

Deutsch在1985年和1989年分别提出了量子计算机的两种模型：量子图灵机模型和量子电路模型。

量子图灵机模型主要是作为研究量子计算的效率的数学模型，而量子电路模型主要是作为实现量子计算的物理模型。

1993年，Yao给出了能在多项式时间内模拟任何量子图灵机的通用量子图灵机模型，同时也证明了量子图灵机和量子电路的等价性。

量子自动机

1997年，Moore和Crutchfield为了理解量子计算，把经典计算理论中的概念推广到量子情形。

他们定义了量子有限状态自动机、量子下推自动机、正规量子文法和量子上下文无关文法，并且建立了它们之间的对应关系。

此后，提出了多种量子自动机模型。

量子图灵机

1994年，Shor发现了在量子计算机上的大数因子分解的多项式时间算法。

因为目前广泛采用的RSA公钥密码体系是建立在大数因子分解是难解问题这一假定的基础上的，所以，如果能建造出真正实用的量子计算机，那么使用大数因子分解的Shor量子算法，就将直接破解现有的RSA公钥密码体系。

Shor的量子算法，极大地推动了量子信息科学，特别是量子计算的发展。

参考文献

量子计算与量子信息：

M. A. Nielsen, I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press. 2000.

Moore-Crutchfield量子自动机：

C. Moore, J. P. Crutchfield. Quantum Automata and Quantum Grammars. Theoretical Computer Science, 237: 275-306. 2000.

改写的有限自动机定义

定义 (确定型有限自动机)

一个确定型有限自动机由五部分构成：

1. 一个有限状态集S；
2. 一个初始状态$s_{init} \in S$；
3. 一个接收状态集$S_{accept} \subset S$；
4. 一个输入字母表A；
5. 一个状态转移函数$F : S \times A \to S$。

实时量子自动机

定义 (实时量子自动机)

一个实时量子自动机$(QA)Q$由五部分构成：

1. 一个$Hilbert$空间H；
2. 一个初始状态向量$\langle s_{init}| \in H$且满足$|s_{init}|^2 = 1$；
3. 一个子空间$H_{accept} \subset H$和一个投影到该子空间的算子P_{accept}；
4. 一个输入字母表A；
5. 对于每一个字母$a \in A$都对应一个酉转移矩阵U_a。

广义实时量子自动机

定义 (广义实时量子自动机)

一个广义实时量子自动机是一个广义实时量子自动机，其中初始状态s_{init}的范数不必为1，U_a不必为酉矩阵。

对于任意$w = a_1 a_2 \cdots a_n \in A^*$，对应的酉转移矩阵$U_w = U_{a_1} U_{a_2} \cdots U_{a_n}$。

量子语言

定义 (广义实时量子自动机)

量子自动机Q识别的量子语言为函数

$$f_Q : A^* \to [0, 1]。$$

式中，对于任意$w \in A^*$，$f_Q(w) = |s_{init} U_w P_{accept}|^2$。

量子语言

开始时，初始状态为$\langle s_{init}|$，然后按照在字符串w中字符a_i出现的顺序，依次将对应的酉矩阵U_{a_i}作用于$\langle s_{init}|$，最后将投影算子P_{accept}作用于$\langle s_{init}|U_w$，并测量其范数$|s_{init}U_wP_{accept}|^2$，这即为最终状态出现在子空间$H_{accept}$中的概率。

量子有限状态自动机

定义 (Moore-Crutchfield量子有限状态自动机)

一个量子有限状态自动机(*QFA*)是一个实时量子自动机，其中H、s_{init}和U_a的维数都是有限维数n。

定义 (量子正规语言)

称量子有限状态自动机识别的语言为量子正规语言(*QRL*)。

量子正规语言的性质

定理

如果Q和R是QFA，并且如果$|a|^2 + |b|^2 = 1$，那么$aQ \oplus bR$也是QFA，并且$f_{aQ \oplus bR} = |a|^2 f_Q + |b|^2 f_R$。因此，如果$f_1, f_2, \cdots, f_n$是$QRL$，那么对于任意满足条件$\sum_{i=1}^{n} c_i = 1$的实数$c_i > 0$，$\sum_{i=1}^{n} c_i f_i$都是$QRL$。

量子正规语言的性质

定理

如果Q和R是QFA，那么$Q \otimes R$也是QFA，并且$f_{Q\otimes R} = f_Q f_R$。因此，任意数目的QRL的乘积都是QRL。

定理

对于任意常数$c \in [0,1]$，常数函数$f(w) = c$是QRL。

定理

如果f是QRL，那么$\bar{f} = 1 - f$也是QRL。

量子正规语言的性质

定理 (泵引理)

若f是QRL，则对于任意字w和任意的$\varepsilon > 0$，存在一个k，使得对于任意字u和v，有

$$|f(uw^k v) - f(uv) \leq \varepsilon。$$

而且，如果f的自动机是n维的，那么存在一个常数c，使得$k \leq (c\varepsilon)^{-n}$。

量子正规语言的性质

定理

如果一个正规语言L是QRL，那么识别L的极小化自动机DFA的转移矩阵M_a生成一个群$\{M_a\}$。所以，存在正规语言(RL)不是量子正规语言(QRL)。

推论

$QRL \neq RL$。

量子下推自动机

定义 (Moore-Crutchfield量子下推自动机)

一个量子下推自动机$(QPDA)P$也是一个实时量子自动机，其中：

- $Hilbert$空间$H = Q \otimes \Sigma$，其中，Q是一个有限维状态空间，它的基向量是有限控制器的状态集，Σ是一个无限维栈空间，它的基向量对应栈字母表T上的有限字集；

量子下推自动机

定义 (Moore-Crutchfield量子下推自动机)

- 无限维的初始状态向量$\langle s_{init}| \in H$是一个叠加态，它是有限个不同的初始控制状态和栈状态的叠加态；
- $H_{accept} = Q_{accept} \otimes \{\varepsilon\}$。

量子下推自动机

因为栈的后进先出结构，所以仅有某些转移能够发生。如果$q_1, q_2 \in Q$是控制状态，并且$\sigma_1, \sigma_2 \in T^*$是栈状态，那么对应的转移幅度$\langle (q_1, \sigma_1) | U_a | (q_2, \sigma_2) \rangle$不等于零当且仅当对于某个$t \in T$，$t\sigma_1 = \sigma_2$，$\sigma_1 = t\sigma_2$，或$\sigma_1 = \sigma_2$。

如果不要求转移矩阵U_a是酉的，则称为广义量子下推自动机。

量子文法

定义 (Moore-Crutchfield量子文法)

一个量子文法G由四部分构成：

1. 一个变元字母表V；
2. 一个终止字母表T；
3. 一个初始变元$I \in V$；
4. 一个有限的生成式集合$P = \{\alpha \to \beta : \alpha \in V^*, \beta \in (V \cup T)^*\}$，并且对于$P$的每一个生成式$\alpha \to \beta \in P$，都有$n$个复幅度，即有$c_k(\alpha \to \beta) \in C$，$1 \leq k \leq n$，这里$n$是该文法的维数。

量子文法

对于每一个导出式$\alpha \Rightarrow \beta$，定义它的第k个幅度c_k为该导出链中每个生成式的第k个幅度的乘积；定义$c_k(\alpha \Rightarrow \beta)$为从$\alpha$导出$\beta$的所有导出式的第$k$个幅度$c_k$的和；对任意字符串$w \in T^*$，定义$w$的幅度为$c_k(w) = c_k(I \Rightarrow w)$，并且指派给该字符串$w$的概率$f(w)$为$f(w) = \sum_{i=1}^{n} |c_k(w)|^2$，并且称量子文法$G$生成量子语言$f$。

量子文法

定义 (等价)

如果两个量子文法G_1和G_2生成相同的语言，即对任意的$w \in T^*$，都有$f_1(w) = f_2(w)$，则称G_1和G_2等价。

量子文法

定义 (Moore-Crutchfield量子上下文无关文法)

一个量子文法G是上下文无关的，如果G的生成式$\alpha \to \beta$有非零幅度，当且仅当α为单个变元。量子上下文无关文法生成的语言称为量子上下文无关语言$(QCFL)$。

量子文法

定理

任意量子上下文无关语言都能被一个广义量子下推自动机识别。

定理

任意广义量子下推自动机识别的语言都是量子上下文无关语言。

量子文法

定义 (Moore-Crutchfield量子正规文法)

一个量子文法G是正规的，当且仅当在G的生成式中，只有形式为$v_1 \to wv_2$和$v_1 \to w$的生成式有非零幅度，其中$v_1, v_2 \in V$，$w \in T^*$。

定理

一个量子语言是一个广义量子正规语言，当且仅当它能由一个正规量子文法生成。

量子上下文无关语言性质

定理

如果f是一个量子上下文无关语言，g是一个量子正规语言，那么fg是一个量子上下文无关语言。

定理

如果f和g是量子上下文无关语言，那么$f+g$是一个量子上下文无关语言。

量子上下文无关语言性质

定理

存在量子上下文无关语言$(QCFL)$不是上下文无关语言(CFL)。

推论

$QCFL \neq CFL$。

量子图灵机

定义 (Bernstein-Vazirani量子图灵机)

一个量子图灵机(QTM)是一个三元组$M = (\Sigma, Q, \delta)$，其中：

1. Σ是一个有限字母表；
2. Q是一个有限状态集；
3. δ是一个量子转移函数：

$$\delta : Q \times \Sigma \times \Sigma \times Q \times \{L, R\} \to C。$$

式中，符号L和R代表带头向左、向右移动。

量子图灵机

量子转移函数$\delta(p,\sigma,\tau,q,d)$表示当量子图灵机在状态$p$读到一个$\sigma$时，将写下一个$\tau$，进入状态$q$，并向$d$方向移动的幅度。

良构量子图灵机

与量子有限自动机类似，量子有限状态转移函数δ也诱导出一个时间进化算子。

定义 (良构量子图灵机)

一个量子图灵机$(QTM)M = (\Sigma, Q, \delta)$是良构的，如果它的(量子转移函数$\delta$诱导出的)时间进化算子$U_M$保持欧氏长度。

良构量子图灵机

定理

一个量子图灵机$(QTM)M = (\Sigma, Q, \delta)$是良构的，当且仅当它的(量子转移函数$\delta$诱导出的)时间进化算子$U_M$是酉的。

Yao定理

定义 (Yao量子图灵机)

一个量子图灵机(QTM)是一个三元组$M = (\Sigma, Q, \delta)$，其中：

1. Σ是一个有限字母表；
2. Q是一个有限状态集；
3. δ是一个量子转移函数：

$$\delta : Q \times \Sigma \times \Sigma \times Q \times \{\leftarrow, o, \rightarrow\} \rightarrow C。$$

式中，符号$\leftarrow$和$\rightarrow$代表带头向左、向右移动，而o代表带头不移动。

Yao定理

定理 (Yao定理)

设M是一个量子图灵机，n和t是正整数。那么，存在一个$\mathrm{poly}(n,t)$ 尺度的量子布尔电路K，它能(n,t)-模拟M。

推论

量子计算的两种模型—量子图灵机模型和量子电路模型，从复杂性理论的观点看，它们的计算能力是相同的。

Yao定理

定理

存在一个通用量子图灵机能在多项式时间内模拟任意给定的量子图灵机。

Church-Turing-Deutsch原理

1985年，Deutsch从物理学的角度重新考虑了Church-Turing论题，提出了Church-Turing论题的一个物理版本：

Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means（每一个有限的可实现的物理系统都能被一台通用量子计算机以有限方式的操作来完全地模拟）。

谢谢！

主 讲 人： 姚 刚

电子邮箱： yaogang@iie.ac.cn