1000-9825/2003/14(01)0009 ©2003 Journal of Software 软 件 学 报 Vol.14, No.1

量子自动机的刻画*

邱道文+

(中山大学 计算机科学系,广东 广州 510275)
(清华大学 计算机科学与技术系,北京 100084)
(清华大学 智能技术与系统国家重点实验室,北京 100084)

Characterizations of Quantum Automata

QIU Dao-Wen+

(Department of Computer Science, Zhongshan University, Guangzhou 510275, China)
Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)
(State Key Laboratory of Intelligent Technology and Systems, Tsinghua University, Beijing 100084, China)
+ Corresponding author: Phn: 86-20-38458089, E-mail: issqdw@zsu.edu.cn
http://www.zsu.edu.cn
Received 2001-07-24; Accepted 2001-10-16

Qiu DW. Characterizations of quantum automata. *Journal of Software*, 2003,14(1):9~15.

Abstract: The relationships among various quantum automata are clarified, and in particular, variously equivalent characterizations of quantum automata are established. The G-quantum automata, g-quantum automata, (generalized) quantum automata, G-quantum grammars and g-quantum grammars are presented, and their connections to some of the other existing quantum automata are expounded. Under a certain condition, the equivalence between the G(g)-quantum automata and G(g)-quantum grammars is discussed. Therefore the problem of quantum grammars generating quantum regular languages is solved. The relation between quantum and regular languages is dealt with, and particularly, two open problems proposed by Gudder are answered. Finally, the method of decreasing the dimensions of spaces of states on quantum automata is given.
Key words: Hilbert space; quantum computation; automata; grammar; regular language

摘 要: 澄清了各类量子自动机之间的相互关系,并给出了量子自动机的各种等价刻画定理.引入 G-量子自动机、g-量子自动机、(广义)量子自动机及 G-量子文法和 g-量子文法,并阐明了它们与其他量子自动机之间的等价关系.在一定条件下讨论了 G(g)-量子自动机与 G(g)-量子文法的等价性,从而解决了关于量子文法产生量子正规语言的问题.讨论了量子语言与正规语言的关系,特别是回答了 Gudder 提出的两个公开问题.最后,给出了一种减少状态空间维数的方法.

---

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.G1998030509 (国家重点基础研究发展规划(973)); the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No.69725004 (国家杰出青年科学基金); the Natural Science Foundation of Guangdong Province of China under Grant No.020146 (广东省自然科学基金); the Young Foundation of Zhongshan University of China under Grant No.35100-1131127 (中山大学青年基金)

第一作者简介: **邱道文**(1967－),男,江西石城人,博士,副教授,主要研究领域为模糊自动机理论,量子计算.

关键词: Hilbert 空间;量子计算;自动机;文法;正规语言
中图法分类号: TP301 **文献标识码**: A

量子计算机的研究已有近 20 年的历史.早在 20 世纪 80 年代初,Benioff[1]和 Feyman[2]就提出了量子计算机的思想.其后,Deutsch[3]将他们的思想形式化,并引入了量子 Turing 机的概念.特别是 Shor[4]在 1994 年给出了大数分解的多项式时间算法,Grover[5]1996 年为模式识别和数据挖掘发展了更快速的量子算法之后,量子计算的研究日益活跃[6].然而,过去人们关注较多的是量子算法、量子逻辑门和量子复杂性理论(见文献[6,7]),而对最基本的量子自动机理论的研究相对较少.最近,Moore 等人[8]、Gudder[9]、Kondacs 和 Watrous[10]从不同的角度对此作了初步的研究(关于文献[8,10]中量子自动机的关系可参见文献[11]).我们知道,经典的有穷自动机一般由状态集、输入字母表和一个转移关系构成,当输入一个字符之后,由转移关系决定状态的转移.量子有穷自动机的状态集一般由有穷个状态的任意次叠加构成,而每次状态的转移有一个转移幅度(amplitude).其实,转移关系可由算子或矩阵表示[8].由于量子逻辑门与酉算子或酉矩阵有紧密联系[6](事实上,量子力学中的一个基本假设是状态的演化由酉变换来描述[12]),所以通常要求状态转移由酉算子或酉矩阵决定.若不要求转移有酉性,则称其为广义的.实际上,存在经典的有穷自动机的转移关系不能由酉矩阵表示[8].

形式上,一个量子有穷自动机一般是五元组 (H,s_0,Σ,U,F),其中 H 是有限维复 Hilbert 空间; s_0 是初始状态(通常是单位向量); Σ 是有穷输入字母表,且对任意 $x\in\Sigma,U(x)$ 是 H 上的酉算子或酉矩阵;F 是 H 的子空间(终结状态).若不要求 $U(x)$ 是酉的,则称其为广义量子有穷自动机.由(广义)量子有穷自动机识别的语言为(广义)量子正规语言(它们是 Σ^* 到[0,1]和[0, ∞]的函数).粗略地说,文献[8]主要研究了(广义)量子正规语言的基本性质以及与正规语言的关系,并用正规量子文法刻画了广义量子正规语言(参见文献[8]中的 Theorem 20),但是如何用量子文法刻画更为重要的量子正规语言仍未解决.Gudder[9]主要研究这类语言的截断函数的性质,但只讨论了 $U(x)$ 为酉算子的情形.本文第 1 节主要介绍文献[8,9]关于量子有限自动机的主要工作.为了便于讨论,第 2 节用算子代替矩阵引入 G(g)-量子自动机,特别是提出了仅有有限个状态的(广义)量子自动机,并在一定条件下($s_0\in F\cup F^{\perp}$)分别证明了 G-量子自动机与广义量子自动机以及 g-量子自动机与量子自动机等价,从而给出了文献[8,9]中的量子自动机的一个刻画.第 3 节引入 G(g)-量子文法,并在 $s_0\in F\cup F^{\perp}$ 的条件下证明它们与 G(g)-量子自动机识别的语言等价.这不仅解决了用量子文法刻画量子正规语言的问题[8],而且给出了文献[8]中的正规量子文法的一个等价刻画.最后一节讨论了各种量子语言与正规语言的关系,特别是命题 4.2 解决了 Gudder 在文献[9]中提出的两个公开问题(参见文献[9]中的 Problem 15 和 Problem 16),即是否存在非正规的量子语言或 η-量子语言及是否存在正规语言但非量子语言,并得到了 G(g)-量子自动机的转移算子族的一个刻画,给出了减少 G(g)-量子自动机状态空间的维数的方法(见定理 4.4).另外,我们假定读者熟悉 Hilbert 空间的基本理论.

1 量子有穷状态自动机和 q-自动机

Moore 与 Crutchfield 在文献[8]中提出了量子有穷状态自动机和广义量子有穷状态自动机.

定义 1.1[8]. 量子有穷状态自动机 Q 由以下 5 部分组成:

(a) 复有限维 Hilbert 空间;

(b) 一个初始状态向量 $s_0\in H$ 且 $\|s_0\|^2=1$;

(c) H 的一个子空间 F (终结状态);

(d) 有穷输入字母表 Σ;

(e) 任意 $x\in\Sigma$,存在一个酉的转移矩阵 U_x.称被 Q 识别的语言 $f_Q:\Sigma^*\to[0,1]$为量子正规语言,定义为:任意 $\omega=x_1x_2...x_n\in\Sigma^*$, $f_Q(\omega)=\left\|P(F)U_{x_n}...U_{x_1}s_0\right\|^2$,其中当$\omega=\varepsilon$($\varepsilon$表示空串)时,令 $U_\varepsilon=E$(单位矩阵).

值得指出的是,上面的运算应理解为在 H 的某一给定正交规范基下进行,如 s_0 为在该基下的坐标.若上述定义中矩阵 U_x 未必是酉的,则称 Q 是广义量子有穷状态自动机,相应地,称 f_Q 为广义量子正规语言.文献[8]证明了

存在正规语言不是量子正规语言,但所有正规语言都是广义量子正规语言.当每个矩阵 U_x 的每行元素非负且其和为 1 时,得到一个随机自动机[10],但这时它未必是量子有穷状态自动机.文献[8]讨论了正规量子文法与广义量子正规语言的等价关系,但仍不知如何建立量子文法与量子正规语言等价.

Gudder 在文献[9]中提出了所谓的 q-自动机和广义 q-自动机.实际上,其“广义”仅指初始状态与终结状态的关系,即 $s_0 \in F \cup F^{\perp}$.

定义 1.2[9]. q-自动机是指五元组 $A=(H,s_0,\Sigma,U,F)$,其中 H,s_0,Σ,F 的定义见定义 1.1,任意 $x\in\Sigma$,$U(x)$ 是 H 上的酉算子,且 $s_0 \in F\cup F^{\perp}$,否则称 A 是广义 q-自动机.

Gudder[9]主要研究了 η-量子语言 $\{\omega\in\Sigma^*:\|P(F)U(\omega)s_0\|^2<\eta\}$ 和量子语言 $\{\omega\in\Sigma^*:U(\omega)s_0\in F\}$ 的性质,并证明存在正规语言但不是 η-量子语言,其中 $0\le\eta<1$, $U(\omega)=U(\omega_1)...U(\omega_{|\omega|})$,$|\omega|$ 表示 ω 的长度,$|\omega_i|=1$, $i=1,2,...,|\omega|$.

注:由 Hilbert 空间的基本理论可知,任意 n 维复 Hilbert 空间 H 及其一个给定的正交规范基 $\{e_1,...,e_n\}$,H 上的任意酉算子 A,存在惟一酉矩阵 A',使得任意 $x=\sum_{i=1}^{n}x_ie_i\in H$, $Ax=A'(x_1...x_n)^T$,这时 Ax 应理解为在基 $\{e_1,...,e_n\}$ 下的坐标;反之,若 A' 是 n 阶酉矩阵,且定义 $Ax=A'(x_1...x_n)^T$,则 A 是 H 上的酉算子.因此,广义 q-自动机与量子有穷状态自动机是等同的.

2 G(g)-量子自动机和(广义)量子自动机

为了简便起见,用算子代替(广义)量子有穷状态自动机中的矩阵,其等价性是显而易见的.特别是,基于文献[9]的思想,我们引入另一类状态有限的(广义)量子自动机.

定义 2.1. 称五元组 $M=(H,s_0,\Sigma,U,F)$ 是 G-量子自动机,其中 H 是有限维复 Hilbert 空间;$s_0\in H$ 是初始单位向量;F 是 H 的子空间(终结状态);任意 $x\in\Sigma$,$U(x)$ 是 H 上的线性有界算子.

称 M 识别的语言 f_M 为 G-量子语言,定义为:任意 $\omega=x_1...x_m\in\Sigma^*$, $f_M(\omega)=\|P(F)U(x_m)...U(x_1)s_0\|^2$,当 $\omega=\varepsilon$ 时,定义 $U(\varepsilon)=I$ (恒等算子).若任意 $x\in\Sigma$,$U(x)$ 是 H 上的酉算子,则称 M 为 g-量子自动机;相应地,称 f_M 为 g-量子语言.

定义 2.2. 若任意 $\omega\in\Sigma^*$, $f_1(\omega)=f_2(\omega)$,则称 Σ 上的两个语言 f_1 和 f_2 等价;若两个(量子)自动机识别的语言等价,则称它们等价.

引理 2.3. G-量子自动机和 g-量子自动机分别与广义量子有穷状态自动机和量子有穷状态自动机等价.

证明:略. □

定义 2.4. 一个广义量子自动机是五元组 $A=(S,s_0,\Sigma,\delta,S_f)$,其中 S 是有限个状态集,$s_0\in S$ 是初始状态,Σ 是有限输入字母表,$S_f\subseteq S$ 为终结状态,转移函数 $\delta:S\times\Sigma\times S\to C$ (C 表示复数)满足:

$$\delta(s,\varepsilon,t)=\begin{cases}1, & s=t,\\ 0, & s\neq t.\end{cases}$$

若定义 2.4 中的 δ 满足:任意 $x\in\Sigma$ 和 $s,s'\in S$,

$$\sum_{t\in S}\delta(s,x,t)\delta(s',x,t)^*=\delta_{s,s'}, \tag{1}$$

则称 A 是量子自动机,其中 $\delta_{s,s'}$ 是 Kronecker 记号(当 $s=s'$ 时,$\delta_{s,s'}=1$;否则为 0). $\delta(s,x,t)$ 表示,若当前状态为 s,则输入 x 后,状态转移至 t 的幅度;$\delta(s',x,t)^*$ ($\delta(s',x,t)$ 的共轭复数)表示自动机在逆向运行时,输入 x 后,状态回到 s' 的幅度.因此,$\delta(s,x,t)\delta(s',x,t)^*$ 表示输入 x 后,状态 s 转移至 t,当输入 x 时回到状态 s' 的幅度.所有这些幅度之和,即 $\sum_{t\in S}\delta(s,x,t)\delta(s',x,t)$ 表示输入 x 后,自动机从状态 s 向前运行一次,当再次输入 x 时,自动机逆向运行到 s' 的幅度.条件(1)说明自动机具有可逆性.显然,有限自动机及概率自动机[13]都未必满足条件(1),所以我们引入了广义量子自动机.

设 $A=(S,s_0,\Sigma,\delta,S_f)$ 是(广义)量子自动机,则定义 A 识别的语言 $f_A:\Sigma^*\to[0,\infty)$ 如下:任意 $\omega=$

$x_1x_2...x_m\in\Sigma^*$,

$$f_A(\omega)=\sum_{s\in S_f}\left|\sum_{s^{(1)},...,s^{(m-1)}\in S}\delta(s_0,x_1,s^{(1)})\delta(s^{(1)},x_2,s^{(2)})...\delta(s^{(m-1)},x_m,s)\right|^2. \qquad (2)$$

显然, $f(\varepsilon)=\begin{cases}1, & s_0\in S_f\\ 0, & s_0\notin S_f\end{cases}$.

引理 2.5. 若 $A=(S,s_0,\Sigma,\delta,S_f)$ 是量子自动机,则 $f_A:\Sigma^*\to[0,1]$.

证明:由式(1)和式(2)可以得到,在此略. □

设 $M=(H,s_0,\Sigma,U,F)$ 是 G(g)-量子自动机,记 $L(M)=\{\omega\in\Sigma^*:U(\omega^c)s_0\in F\}$,其中 ω^c 是 ω 的倒写,即 $\omega^c=x_{|\omega|}...x_1$, $|\omega|$ 表示 ω 的长度.这时显然有

引理 2.6. 设 $M=(H,s_0,\Sigma,U,F)$ 是 g-量子自动机,则以下 3 条等价:

(a) $\omega\in L(M)$;

(b) $f_M(\omega)=1$;

(c) $P(F)U(\omega^c)s_0=U(\omega^c)s_0$.

定理 2.7. 设 Σ 是一个有限输入字母表,函数 $f:\Sigma^*\to[0,\infty]$满足 $f(\varepsilon)\in\{0,1\}$,则

(a) f 是量子正规语言,当且仅当存在量子自动机 $A=(S,s_0,\Sigma,\delta,S_f)$ 使得任意 $\omega\in\Sigma^*$, $f(\omega)=f_A(\omega)$.

(b) f 是广义量子正规语言,当且仅当存在广义量子自动机 $A=(S,s_0,\Sigma,\delta,S_f)$ 使得任意 $\omega\in\Sigma^*$, $f(\omega)=f_A(\omega)$.

证明:(a) 设 $M=(H,s_0,\Sigma,U,F)$ 是 G-量子自动机,且任意 $\omega\in\Sigma^*$, $f(\omega)=f_M(\omega)$.由于 $f(\varepsilon)\in\{0,1\}$,所以由引理 2.3 可知 $s_0\in F\cup F^\perp$.因此,存在 $S=\{s_0,s_1,...,s_{n-1}\}$ 为 H 的一个正交规范基,且其中 $S_f=\{s_{i_1},...,s_{i_k}\}$ 是 F 的基.定义 $\delta:S\times\Sigma\times S\to C$ 如下: $\delta(s_i,x,s_j)=\langle U(x)s_i,s_j\rangle$,则 $A=(S,s_0,\Sigma,\delta,S_f)$ 是量子自动机,其中 $\langle\cdot,\cdot\rangle$ 为 H 中的内积.这只需验证满足条件(1)即可.由于 $U(x)$是 H 上的酉算子,所以 $\sum_{t\in S}\delta(s_i,x,t)\delta(s'_i,x,t)^*=\sum_{j=0}^{n-1}\langle U(x)s_i,s_j\rangle(\langle U(x)s'_i,s_j\rangle)^*=\left\langle\sum_{j=0}^{n-1}\langle U(x)s_i,s_j\rangle s_j,\sum_{j=0}^{n-1}\langle U(x)s'_i,s_j\rangle s_j\right\rangle=\langle U(x)s_i,U(x)s'_i\rangle=\langle s_i,s'_i\rangle=\delta_{s_i,s'_i}$,故满足条件(1).下面证明任意 $\omega\in\Sigma^*$, $f(\omega)=f_A(\omega)$.当 $\omega=\varepsilon$ 时,

$$f_A(\varepsilon)=\sum_{s_j\in S_f}\left|\delta(s_0,\varepsilon,s_j)\right|^2=\begin{cases}1, & s_0\in S_f\\ 0, & s_0\notin S_f\end{cases},\quad f_M(\varepsilon)=\|P(F)s_0\|^2=\begin{cases}1, & s_0\in S_f\\ 0, & s_0\notin S_f\end{cases},$$

故 $f_A(\varepsilon)=f_M(\varepsilon)$;当 $\omega=x_1...x_m$ 时,由于任意 $t\in S$,

$$\begin{aligned}\langle U(\omega^c)s_0,t\rangle&=\langle U(x_m)...U(x_1)s_0,t\rangle\\&=\left\langle U(x_m)...U(x_2)\sum_{s^{(1)}\in S}\langle U(x_1)s_0,s^{(1)}\rangle s^{(1)},t\right\rangle\\&=\sum_{s^{(1)}\in S}\langle U(x_1)s_0,s^{(1)}\rangle\langle U(x_m)...U(x_2)s^{(1)},t\rangle\\&=\sum_{s^{(1)}\in S}\langle U(x_1)s_0,s^{(1)}\rangle\left\langle U(x_m)...U(x_s)\sum_{s^{(2)}\in S}\langle U(x_2)s^{(1)},s^{(2)}\rangle s^{(2)},t\right\rangle\\&=\sum_{s^{(1)},s^{(2)}\in S}\langle U(x_1)s_0,s^{(1)}\rangle\langle U(x_2)s^{(1)},s^{(2)}\rangle\langle U(x_m)...U(x_3)s^{(2)},t\rangle\\&=\sum_{s^{(1)},...,s^{(m-1)}\in S}\langle U(x_1)s_0,s^{(1)}\rangle\langle U(x_2)s^{(1)},s^{(2)}\rangle...\langle U(x_m)s^{(m-1)},t\rangle\\&=\sum_{s^{(1)},...,s^{(m-1)}\in S}\delta(s_0,x_1,s^{(1)})\delta(s^{(1)},x_2,s^{(2)})...\delta(s^{(m-1)},x_m,t),\end{aligned}$$

因此 $$f(\omega)=f_M(\omega)=\left\|P(F)U(\omega^c)s_0\right\|^2=\sum_{j=1}^{k}\left|\left\langle U(\omega^c)s_0,s_{i_j}\right\rangle\right|^2=f_A(\omega).$$

另一方面,设有量子自动机 $A=(S,s_0,\Sigma,\delta,S_f)$ 使得任意 $\omega\in\Sigma^*$, $f(\omega)=f_A(\omega)$.设 $S=\{s_0,s_1,...,s_{n-1}\}$ 及 $S_f=\{s_{i_1},...,s_{i_k}\}$,则将 S 看作 n 维复 Hilbert 空间 H 的一个正交规范基, S_f 是 H 的子空间 F 的基.任意 $x\in\Sigma$,定义 H 上的算子 $U(x)$ 为 $U(x)s_i=\sum_{t\in S}\delta(s_i,x,t)\,t$,并线性延拓到 H 上.这时 $U(x)$ 是 H 上的酉算子.事实上,任意 $s_i,s_j\in S$,由条件(1)有

$$\left\langle U(x)s_i,U(x)s_j\right\rangle=\left\langle\sum_{k=0}^{n-1}\delta(s_i,x,s_k)s_k,\sum_{k=0}^{n-1}\delta(s_j,x,s_k)s_k\right\rangle=\sum_{k=0}^{n-1}\delta(s_i,x,s_k)\delta(s_j,x,s_k)^*=\delta_{s_i,s_j},$$

因此, $U(x)$ 是 H 上的酉算子.任意 $\omega\in\Sigma^*$,类似于前面的证明可以得到 $f(\omega)=f_A(\omega)=f_M(\omega)$.最后,由引理 2.2 即完成了(a)的证明.

(b) 用类似的方法可以证明. □

推论 2.8. (a) 设 $M=(H,s_0,\Sigma,U,F)$ 是 g-量子自动机,则 $s_0\in F\cup F^\perp$ 的充要条件是 M 等价于量子自动机.

(b) 设 $M=(H,s_0,\Sigma,U,F)$ 是 G-量子自动机,则 $s_0\in F\cup F^\perp$ 的充要条件是 M 等价于广义量子自动机.

3 G-量子文法与 g-量子文法

为了便于比较,我们先简要给出文献[8]中正规量子文法的定义.

定义 3.1[8]. 一个正规的量子文法由以下 4 部分构成:

(a) 有限变元集合 V;

(b) 有限终端集合 T;

(c) 初始变元 $I\in V$;

(d) 生成式集合 $P\subseteq\{\alpha\to\beta:\alpha\in V^*,\beta\in(V\cup T)^*\}$, 且任意 $\alpha\to\beta\in P$,有 n 个生成幅度(amplitude) $c_k(\alpha\to\beta)\in C$, $1\le k\le n$,而且仅有形如 $v_1\to\omega v_2$ 及 $v_1\to\omega$ 的生成式有非零生成幅度,其中 $v_1,v_2\in V,\omega\in T^*$, n 为该文法的维数.

进一步,定义派生 $\alpha\xrightarrow{*}\beta$ 的某个第 k 派生幅度为该链中每个生成幅度 c_k 的乘积,并记 $c_k(\alpha\xrightarrow{*}\beta)$ 为 $\alpha\xrightarrow{*}\beta$ 的所有第 k 派生幅度之和,从而定义该文法产生的语言 $f:T^*\to[0,1]$为 $f(\omega)=\sum_{k=1}^{n}\left|c_k(I\xrightarrow{*}\omega)\right|^2$. 下面给出简单一些的定义.

定义 3.2. 称四元组 $G=(V,T,v_0,P)$ 为 G-量子文法,其中 V 与 T 分别为有限变元集合与有限终端集合, $v_0\in V$ 表示初始变元, P 是有限生成式之集.任意 $\alpha\to\beta\in P$ 有一个生成幅度(amplitude) $c(\alpha\to\beta)\in C$,其中 $c(v\to\varepsilon)\in\{0,1\}$,且仅有形如 $v\to xv'$ 或 $v\to\varepsilon$ 的生成式的幅度可能非零.若 G-量子文法的生成式满足:

$$\sum_{u\in V}c(v\to xu)c(v'\to xu)^*=\delta_{v,v'},\tag{3}$$

则称其为 g-量子文法.

设 $G=(V,T,v_0,P)$ 为 G(g)-量子文法,其中 $V=\{v_0,v_1,...,v_{n-1}\},\omega\in T^*$,则称序列 v_0,ε (当 $\omega=\varepsilon$)或 $v_0,\omega_1v,\omega_1\omega_2v',...,\omega v_k,\omega$ 为 ω 的一个派生.序列中最后一步利用生成式 $v_k\to\varepsilon$,所以称其为 ω 的 v_k 型派生,并定义其派生幅度为 $c(v_0\to\omega_1v)c(v\to\omega_2v')...c(v_k\to\varepsilon)$.记 ω 的所有 v_k 型派生幅度之和为 $c_{v_k}(\omega)$,即

$$c_{v_k}(\omega)=\sum_{v^{(1)},...,v^{(m-1)}\in V}c\left(v_0\to\omega_1v^{(1)}\right)c\left(v^{(1)}\to\omega_2v^{(2)}\right)...c\left(v^{(m-1)}\to\omega_mv^{(k)}\right)c(v_k\to\varepsilon),\tag{4}$$

其中 $\omega=\omega_1\omega_2...\omega_m$.设 $X\subset V$,则由 G 产生的 (G,X) 语言 $f_{G,X}:T^*\to[0,+\infty)$ 定义为

$$f_{G,X}(\omega)=\sum_{v\in X}\left|c_v(\omega)\right|^2.\tag{5}$$

引理 3.3. 若 G 是 g-量子文法,则其产生的语言 $f_{G,X}$ 的取值范围为[0,1].

证明:类似于引理 2.5. □

定理 3.4. (a) 语言 f 被量子自动机识别,当且仅当 f 是 g-量子文法 G 产生的一个 (G,X) 语言;

(b) 语言 f 被广义量子自动机识别,当且仅当 f 是 G-量子文法 G 产生的一个 (G,X) 语言.

证明:略. □

由定理 2.7、定理 3.4 和引理 2.3 容易得到下面两个推论:

推论 3.5. (a) f 是 g-量子语言且 $f(\varepsilon)\in\{0,1\}$ 的充要条件是 f 是 g-量子文法 G 产生的 (G,X) 语言;

(b) f 是 G-量子语言且 $f(\varepsilon)\in\{0,1\}$ 的充要条件是 f 是 G-量子文法 G 产生的 (G,X) 语言.

推论 3.6. (a) f 是被量子有限状态自动机识别的语言且 $f(\varepsilon)\in\{0,1\}$ 的充要条件是 f 是 g-量子文法 G 产生的 (G,X) 语言;

(b) f 是被广义量子有限状态自动机识别的语言且 $f(\varepsilon)\in\{0,1\}$ 的充要条件是 f 是 G-量子文法 G 产生的 (G,X) 语言.

定义 3.7. 称两个量子文法等价,如果它们识别的语言等价.

由推论 3.6(b)可知,当正规的量子文法(见定义 3.1)满足 $\sum_{k=1}^{n}\left|c_k(I\to\varepsilon)\right|^2\in\{0,1\}$ 时,它与 G-量子文法等价.

4 G(或 g)-量子语言与正规语言

本节简要讨论 G(或 g)-量子语言的几个比较重要的性质.其余的基本性质参见文献[8,9].

定义 4.1. 设 $M=(H,s_0,\Sigma,U,F)$ 是 G(或 g)-量子自动机,则称 $f_{M,\eta}=\{\omega\in\Sigma^*: f_M(\omega)>\eta\}$ 为 η-G(或 g)-量子语言,其中 $0\le\eta<1$;若 $\eta=1$,则定义 1-G(或 g)-量子语言为 $f_{M,1}=\{\omega\in\Sigma^*: f_M(\omega)=1\}$.

由引理 2.6 可知,对任意 G(或 g)-量子自动机, $L(M)=f_{M,1}$.

命题 4.2. (1) 存在正规语言但不是 g-量子语言;

(2) 正规语言和 g-量子语言都是 G-量子语言的真子集;

(3) 存在正规语言但不是 η-g-量子语言;

(4) 正规语言都是 η-G-量子语言;

(5) 存在非正规的 1-g-量子语言和 0-g-量子语言.

证明:(1)与(2)由引理 2.3 及文献[8]中的 Theorem 7 和 Lemma 8 可以得到证明;(3)由文献[9]中的 Corollary 5.5 可以得到证明;由(2)可以直接推出(4).下面给出(5)的证明.设 $\Sigma=\{a,b\}$ 和语言 $L\subset\{a,b\}^*$,其中字 $\omega\in L$ 当且仅当 ω 所含 a 和 b 的个数相同.我们知道 L 不是正规语言.然而,L 是 1-g-量子语言,即存在 g-量子自动机 M 使得 $L=f_{M,1}$.事实上,设 $M=(H,s_0,\Sigma,U,F)$,其中,$H=C^2,\Sigma=\{a,b\},s_0=\left(\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right)^T$,对任意 $e\in H$,$U(a)e=\begin{pmatrix}e^{-it}&0\\0&e^{it}\end{pmatrix}e$ 和 $U(b)e=\begin{pmatrix}e^{it}&0\\0&e^{-it}\end{pmatrix}e$,其中 t 是 π 与无理数的乘积,$F=\{(c,c)^T:c\in C\}$.若用 $\omega(m,n)$ 表示含 m 个 a 和 n 个 b 的字,则容易验证 $f_M(\omega(m,n))=\left|\cos(m-n)t\right|^2$. 所以 $f_M(\omega(m,n))=1$ 当且仅当 $m=n$,即 $\omega(m,n)\in L$.因此,$L=f_{M,1}$ 成立.关于构造非正规的 0-g-量子语言可参见文献[14]中的 Theorem 4.事实上,只要在上述 g-量子自动机 M 中取 $q_0=(1,0)$, $F=span\{(0,1)\}$, 对任意 $e\in H$, $U(a)e=\begin{pmatrix}\cos\pi t&-\sin\pi t\\\sin\pi t&\cos\pi t\end{pmatrix}e$ 和 $U(b)e=\begin{pmatrix}\cos\pi t&\sin\pi t\\-\sin\pi t&\cos\pi t\end{pmatrix}e$,其中 $t=\frac{\sqrt{5}-1}{2}$. □

由于文献[9]中的量子语言就是本文的 1-g-量子语言,所以如引言所述,命题 4.2 中的(4)和(5)回答了文献[9]中的问题 15 和问题 16.算子族 U 在 G(或 g)-量子自动机中起着关键作用,下面给出其刻画.

定理 4.3. 设 Σ 是有限字母表,H 是有限维复 Hilbert 空间.函数 $A:\Sigma^*\to H$ 满足 $A(\varepsilon)$ 是单位向量,则以下 3 条等价:

(a) 存在 G-量子自动机 $M=(H,s_0,\Sigma,U,F)$ 使得任意 $\omega\in\Sigma^*$, $A(\omega)=U(\omega^c)s_0$.

(b) 存在映射 $M:\Sigma \to B(H)$ 使得任意 $\omega \in \Sigma^*$ 和 $x \in \Sigma$, $A(\omega x) = M(x)A(\omega)$,其中 $B(H)$ 表示 H 上的所有线性有界算子.

(c) 对 H 中的任意正交规范基 $\{e_1,...,e_n\}$ 和任意 $x \in \Sigma$,存在 H 中的向量 $e_1(x),...,e_n(x)$ 满足:任意 $\omega \in \Sigma^*$, $\langle A(\omega x), e_i\rangle = \langle A(\omega), e_i(x)\rangle$.

证明:类似于文献[9]中的 Theorem 3.1 关于 q-自动机的讨论. □

那么,是否可以减少 G(或 g)-量子自动机的状态空间的维数而不改变其识别的语言呢?

定理 4.4. 设 $M=(H,s_0,\Sigma,U,F)$ 是 G-量子自动机.若令 $H_0 = span\{U(\omega)s_0 : \omega \in \Sigma^*\}$ 及 $U_0(x) = U(x)|_{H_0}$,则 $M_0 = (H_0, s_0, \Sigma, U_0, F \cap H_0)$ 是 G-量子自动机,且满足:

(a) $L(M) = L(M_0)$;

(b) 若 $P(H_0)P(F) = P(F)P(H_0)$,则 $f_M = f_{M_0}$.

证明:由于任意 $x \in \Sigma^*$, $U_0(x) \subseteq H_0$,所以 M_0 是 G-量子自动机.

(a) 任意 $\omega \in \Sigma^*$,由于 $U(\omega^c)s_0 = U_0(\omega^c)s_0 \in H_0$,所以 $U_0(\omega^c)s_0 \in F \cap H_0$ 当且仅当 $U(\omega^c)s_0 \in F$.

(b) 由于 $P(H_0)P(F) = P(F)P(H_0)$,所以 $P(F)P(H_0)$ 是投影算子且 $P(F \cap H_0) = P(F)P(H_0)$.因此

$$f_{M_0}(\omega) = \left\|P(F \cap H_0)U_0(\omega^c)s_0\right\|^2 = \left\|P(F)P(H_0)U_0(\omega^c)s_0\right\|^2 = \left\|P(F)U(\omega^c)s_0\right\|^2 = f_M(\omega). \quad \square$$

注:若 $H_0 \neq H$,则 H_0 比 H 的维数至少少一维.当 M 是 g-量子自动机时,定理 4.3 也成立.但是此时令 $H_0 = span\{U(\omega)s_0, U(\omega)^* s_0 : \omega \in \Sigma^*\}$.

致谢 本文的工作是我们在清华大学做博士后期间完成的.我们衷心感谢应明生教授的帮助和鼓励,并对审稿人提出的宝贵建议深表谢意!

References:

[1] Benioff P. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics, 1980,22:563~591.

[2] Feynman RP. Simulting physics with computers. Journal of Statistical Physics, 1982,21(6-7):467~488.

[3] Deutsh D. Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London A, 1985,400(1818):97~117.

[4] Shor PW. Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997,26(5):1484~1509.

[5] Grover L. Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters, 1997,79(2):326~328.

[6] Berman GP, Doolen GD, Mainieri R, Tsifrinovich VI. Introduction to Quantum Computers. Singapore: World Scientific Publishing, 1998. 1~68.

[7] Williams CP, Clearwater SH. Explorations in Quantum Computing. New York: Springer-Verlag, 1998.

[8] Moore C, Crutchfield JP. Quantum automata and quantum grammars. Theoretical Computer Science, 2000,237(1~2):275~306.

[9] Gudder S. Basic properties of quantum automata. International Journal of Theoretical Physics, 1999,38(9):2261~2282.

[10] Kondacs A, Watrous J. On the power of finite state automata. In: Proceedings of the 38th Symposium on Foundations of Computer Science. IEEE Computer Society Press, 1997. 66~75.

[11] Gruska J. Quantum Computing. London: McGraw-Hill, 1999. 151~192.

[12] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 60~119.

[13] Rabin MO. Probabilistic automata. Information and Control, 1963,6(3):230~245.

[14] Bertoni A, Carpentieri M. Analogies and differences between quantum and stochastic automata. Theoretical Computer Science, 2001,262(1):69~81.