软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(5):933−941 [doi: 10.3724/SP.J.1001.2013.04354]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

量子最弱自由前置条件的交换性及其性质*

雷红轩[1,2], 席政军[1], 李永明[1]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](内江师范学院 数学与信息科学学院,四川 内江 641112)

通讯作者: 雷红轩, E-mail: leihx2004@yahoo.com.cn

摘 要: 首先给出了量子最弱自由前置条件(weakest liberal precondition,简称 wlp)wlp (*A*,*B*,*C*)-可交换的定义,研究了 wlp (*A*,*B*,*C*)-可交换的充分必要条件;其次,得到了 wlp 不是良好的谓词转换,验证了 wlp 是比量子最弱前置条件(weakest precondition,简称 wp)更弱的谓词转换,揭示了 wlp 和 wp 的本质区别;最后证明了 wlp 的序列合成、并行合成和块结构等性质.

关键词: 量子谓词;超算子;量子最弱自由前置条件;交换

中图法分类号: TP301 **文献标识码**: A

中文引用格式: 雷红轩,席政军,李永明.量子最弱自由前置条件的交换性及其性质.软件学报,2013,24(5):933−941. http://www.jos.org.cn/1000-9825/4354.htm

英文引用格式: Lei HX, Xi ZJ, Li YM. Commutativity of quantum weakest liberal precondition and its properties. Ruan Jian Xue Bao/Journal of Software, 2013,24(5):933−941 (in Chinese). http://www.jos.org.cn/1000-9825/4354.htm

Commutativity of Quantum Weakest Liberal Precondition and Its Properties

LEI Hong-Xuan[1,2], XI Zheng-Jun[1], LI Yong-Ming[1]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](School of Mathematics and Information Science, Neijiang Normal University, Neijiang 641112, China)

Corresponding author: LEI Hong-Xuan, E-mail: leihx2004@yahoo.com.cn

Abstract: First, the definition of quantum weakest liberal precondition (termed wlp) wlp (*A*,*B*,*C*)-commutativity is proposed, some necessary, and sufficient conditions of wlp (*A*,*B*,*C*)-commutativity are presented. Secondly, it has been shown that wlp is not a healthy predicate transformer: it is verified that wlp is a weaker predicate transformer than the quantum weakest precondition (termed wp). The essential differences of wlp and wp are disclosed. Finally, the properties for sequential composition, parallel composition and block structure of wlp are investigated.

Key words: quantum predicate; super-operator; quantum weakest liberal precondition; commutate

从 20 世纪 80 年代早期以来,各种量子程序协议先后被提出,量子密码系统已经广泛应用于 Quantique、MagiQ 技术、SmartQuantum 和 NEC 中[1].1994 年,Shor[2]提出了著名的量子因子分解算法,1996 年,Grover[3]给出了进行数据搜索的量子搜索算法.这些算法表明,量子计算在某些计算领域比经典计算更有效.但是目前,量子算法还处在较低水平的量子线路阶段.近年来,一些学者[4−14]开始研究量子程序语言的设计和语义.Knill[5]提出了量子伪编码的理论.Ömer[6,7]首次提出了量子程序语言的概念.Sander[8],Zuliani[8,9],Selinger[10]等人提出了各种具有不同特征的量子程序语言.李阳阳和焦李成[11]研究了量子克隆多播路由算法.刘玲和徐家福[12]系统地介绍了量子程序设计语言 NDQJava-2.特别地,D'Hondt 和 Panangaden[13]介绍了量子最弱前置条件语义(简称 wp-

* 基金项目: 国家自然科学基金(11271237, 61228305)
收稿时间: 2012-04-24; 修改时间: 2012-09-29; 定稿时间: 2012-12-03

语义),建立了量子程序的谓词转换语义.

量子程序可以由超算子表示[10,13].按照 D'Hondt 和 Panangaden 的思想,量子谓词被定义成一个可观测算子,也即一个 Hilbert 空间上的 Hermite 算子.量子谓词转换语义不是经典和概率程序的简单推广,它回答了经典和概率程序中不曾出现的很多重要问题,这些问题之一就是量子最弱前置条件(wp)的可交换性.为了推理用量子语言所写的量子程序的部分正确性和总体正确性,冯元等人[15]扩展了最弱自由前置语义(简称 wlp)的概念,研究了 wp 和 wlp 的关系,给出了量子程序正确性的证明规则.应明生教授等人[16]在一个复合量子系统中给出了量子程序最弱前置条件 wp 的本质刻画,研究了 wp 可交换的一些充分条件.由于 Hoare 逻辑是经典程序公理化语义的基础,它为推理经典程序的正确性提供了有效的证明技术.为了对量子程序验证提供类似的技术,并且对量子计算机建立程序方法的逻辑基础,应明生教授[17]建立起了关于量子程序部分和总体正确性的 Floyd-Hoare 逻辑,利用 wp 和 wlp 的功能证明了这种逻辑的完备性.由于 wlp 在证明量子程序部分正确性中有很重要的作用和地位,我们有必要详细地研究 wlp 的性质.为此,我们在上述文献的基础上提出了 wlp (A,B,C)-可换的定义,研究了 wlp (A,B,C)-可换的充分必要条件.进而,讨论了 wlp 不满足良好谓词转换的条件,验证了 wlp 是比 wp 更弱的谓词转换,揭示了 wlp 和 wp 的本质区别.最后讨论了 wlp 的序列、并行合成和块结构等性质.我们的讨论为设计量子程序语言时考虑量子程序的部分正确性和为研究 Hoare 逻辑的完备性提供了理论基础.

1 基本概念

本文用到的有关量子计算的基本概念见文献[1].用 $D(H)$表示 Hilbert 空间 H 上所有密度算子之集,用 $L(H)$表示 H 上所有线性算子之集.如果对任意的$|x\rangle\in H$,$\langle x|A|x\rangle\geqslant 0$,$A\in L(H)$,则称 A 为正算子.算子的 Löwner 序定义为 $A\sqsubseteq B$ 当且仅当 $B-A$ 是一个正算子.设 M 是一个算子,如果 $M^\dagger = M$, 则称 M 为 Hermite 算子,其中, $M^\dagger$ 表示 M 的共轭转置.量子谓词是一个 Hermite 算子,即一个最大特征值的界为 1 的正算子[13,15,17].用 $P(H)$表示 H 上的量子谓词之集,也即 $P(H):=\{M\in L(H)|0\sqsubseteq M\sqsubseteq I\}$.

定义 1.1[1]. 设ε为 $L(H)$上的线性算子,如果ε满足下列两个条件,则称ε为 H 上的超算子:

(1) $tr\varepsilon(\rho)\leqslant tr(\rho)$,对任意的$\rho\in D(H)$;

(2) 完全正性:设 H_R 是一个辅助 Hilbert 空间,如果 A 是 $H_R\otimes H$ 上的正算子,则$(I_R\otimes\varepsilon)(A)$也是正的,其中,$I_R$ 是 H_R 的单位算子.

如果对任意的$\rho\in D(H)$,$tr\varepsilon(\rho)=tr(\rho)$,则称$\varepsilon$是保迹的.

用 $CP(H)$表示 H 上的所有超算子之集.下面给出超算子的 Kraus 算子和表示[13].

ε是 H 上的超算子当且仅当存在一组运算元$\{E_i\}$满足下列条件:

(1) $\varepsilon(\rho)=\sum_i E_i\rho E_i^\dagger$, 对任意的$\rho\in D(H)$;

(2) $\sum_i E_i^\dagger E_i\sqsubseteq I$, 当$\varepsilon$是保迹的超算子时取等号,其中 I 是 H 的单位算子.

定义 1.2[13]. 设 $M,N\in P(H)$,$\varepsilon\in CP(H)$,如果对任意的$\rho\in D(H)$,$tr(M\rho)\leqslant tr(N\varepsilon(\rho))$,则称 M 为 N 的关于量子程序ε的前置条件,记为 $M\{\varepsilon\}N$.

定义 1.3[13]. 设 $M\in P(H)$,$\varepsilon\in CP(H)$,M 关于ε的最弱前置条件是一个量子谓词,记为 $wp(\varepsilon)(M)$,并且满足如下条件:

(1) $wp(\varepsilon)(M)\{\varepsilon\}M$;

(2) 对任意的 $N\in P(H)$,如果 $N\{\varepsilon\}M$,则有 $N\sqsubseteq wp(\varepsilon)(M)$.

设 A,B 是 H 上的两个算子,如果 $AB=BA$,则称 A 和 B 可换[1].

在下文中,$\overline{q}$ 表示 $q_1,\ldots,q_n$ 的简写,$U_{\overline{q}}$ 表示酉算子 U 作用在由 $\overline{q}$ 张成的 Hilbert 空间上,$|x\rangle_q\langle y|$是一个算子,它表示$|x\rangle\langle y|$作用在量子比特 q 上,其他量子比特不改变,也就是说,

$$|x\rangle_q\langle y|:=I_{H_1}\otimes|x\rangle\langle y|\otimes I_{H_2},$$

其中,H_1,H_2 是 Hilbert 空间.

量子最弱前置条件 wp 在量子程序的总体正确性研究中是很有用的.也就是说,当程序终止时,我们不但要考虑终态的正确性,而且要考虑程序终止的条件,有关 wp 的性质可参见文献[10,13,15−18].但是,在量子程序验证的理论研究中,不但要研究程序的总体正确性,而且要研究不要求程序终止,即程序的部分正确性问题.而量子程序的部分正确性由 wlp 来描述,为此,下面先介绍最弱自由前置条件 wlp 的概念如下:

定义 1.4[15]. 设 S 是一个量子程序,S 的 wlp-语义是 $P(H)$上的一个映射 $wlp(S)$,对任意的 $M\in P(H)$,其递归定义如下:

(1) $wlp(\textbf{abort})(M)=I$;

(2) $wlp(\textbf{skip})(M)=M$;

(3) $wlp(q:=0)(M)=|0\rangle_q\langle 0|M|0\rangle_q\langle 0|+|1\rangle_q\langle 0|M|0\rangle_q\langle 1|$;

(4) $wlp(\overline{q}*=U)(M)=U_{\overline{q}}^{\dagger}MU_{\overline{q}}$, 其中, $\overline{q}*=U$ 表示酉算子 U 作用在由 $\overline{q}$ 张成的 Hilbert 空间上;

(5) $wlp(S_1;S_2)(M)=wlp(S_1)(wlp(S_2)(M))$;

(6) $wlp(\textbf{measure}\ q\ \textbf{then}\ S_1\ \textbf{else}\ S_0)(M)=\sum_{i=0}^{1}|i\rangle_q\langle i|wlp(S_i)(M)|i\rangle_q\langle i|$;

(7) $wlp(\textbf{while}\ q\ \textbf{do}\ S)(M)=\nu X.(|1\rangle_q\langle 1|wlp(S)(X)|1\rangle_q\langle 1|+|0\rangle_q\langle 0|M|0\rangle_q\langle 0|$,其中,$\nu X.F(X)$表示 $F(X)$的最大不动点.

2 最弱自由前置条件的交换性

设$\varepsilon\in CP(H)$,则存在一组运算元$\{E_i\}$,使得对任意的 $\rho\in D(H)$,$\varepsilon(\rho)=\sum_i E_i\rho E_i^{\dagger}$, 则对任意的 $M\in P(H)$,有 $wp(\varepsilon)(M)=\sum_i E_i^{\dagger}ME_i$ [15].这样,当 $M,N\in P(H)$,在讨论 $wp(\varepsilon)(M)$,$wp(\varepsilon)(N)$的交换性时,可以用它们的算子和形式.然而,由于 $wlp(\varepsilon)(M)$不能表示成算子和的形式,因此,$wlp(\varepsilon)(M)$和 $wlp(\varepsilon)(N)$交换性的讨论比较复杂.首先给出如下的定义:

定义 2.1[16]. 设 $M,N,A,B,C\in L(H)$,如果 $AMBNC=ANBMC$,则称 M 和 N (A,B,C)-可换.特别地,当 M 和 N (A,A,A)-可换时,简称 M 和 N 是 A-可换.

定义 2.2. 设 $A,B,C\in L(H)$,$\varepsilon\in CP(H)$.当 M 和 N (A,B,C)-可换时,都有 $wlp(\varepsilon)(M)$和 $wlp(\varepsilon)(N)$ (A,B,C)-可换,则称 ε反射(A,B,C)-可换.特别地,如果ε反射(A,A,A)-可换,则称ε反射 A-可换.同时,如果ε反射 I_H-可换,则称ε反射可换,这里,I_H 是 H 上的恒等算子.

根据以上的定义,下面给出 wlp 可交换的结论如下:

定理 2.1. 设 $S,S_0,S_1,S_2\in CP(H)$,对任意的 $M,N\in P(H)$,则有:

(1) $wlp(\textbf{abort})(M)$和 $wlp(\textbf{abort})(N)$可换;

(2) $wlp(\textbf{skip})(M)$和 $wlp(\textbf{skip})(N)$可换当且仅当 M 和 N 可换;

(3) $wlp(q:=0)(M)$和 $wlp(q:=0)(N)$可换当且仅当 M 和 N $|0\rangle_q\langle 0|$-可换和$(|1\rangle_q\langle 0|,|0\rangle_q\langle 0|,|0\rangle_q\langle 1|)$可换;

(4) $wlp(\overline{q}*=U)(M)$ 和 $wlp(\overline{q}*=U)(N)$ 可换当且仅当 M 和 N 可换;

(5) 如果 S_1 和 S_2 反射可换,则 $S_1;S_2$ 也反射可换;

(6) $wlp(\textbf{measure}\ q\ \textbf{then}\ S_1\ \textbf{else}\ S_0)(M)$和 $wlp(\textbf{measure}\ q\ \textbf{then}\ S_1\ \textbf{else}\ S_0)(N)$可换当且仅当 $wlp(S_i)(M)$和 $wlp(S_i)(N)$ $|i\rangle_q\langle i|$可换,$i=0,1$;

(7) 如果 M 和 N $|0\rangle_q\langle 0|$-可换,S 反射$|1\rangle_q\langle 1|$可换,则 $wlp(\textbf{while}\ q\ \textbf{do}\ S)(M)$和 $wlp(\textbf{while}\ q\ \textbf{do}\ S)(N)$可换;反之,如果 $wlp(\textbf{while}\ q\ \textbf{do}\ S)(M)$和 $wlp(\textbf{while}\ q\ \textbf{do}\ S)(N)$可换,则 M 和 N $|0\rangle_q\langle 0|$-可换.

证明:

(1)、(2)可以从定义 1.4 直接得到.

(3):由定义 1.4 有:

$$wlp(q:=0)(M)wlp(q:=0)(N)=|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|+|1\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 1|,$$

$$wlp(q:=0)(N)wlp(q:=0)(M)=|0\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 0|+|1\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 1|.$$

如果 M 和 N $|0\rangle_q\langle 0|$-可换和$(|1\rangle_q\langle 0|,|0\rangle_q\langle 0|,|0\rangle_q\langle 1|)$-可换,则有:

$$wlp(q:=0)(M)wlp(q:=0)(N)=wlp(q:=0)(N)wlp(q:=0)(M);$$

反之,如果 $wlp(q:=0)(M)$和 $wlp(q:=0)(N)$可换,则

$$\begin{aligned}|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|&=|0\rangle_q\langle 0|wlp(q:=0)(M)wlp(q:=0)(N)\\&=|0\rangle_q\langle 0|wlp(q:=0)(N)wlp(q:=0)(M)\\&=|0\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 0|.\end{aligned}$$

类似地,有

$$|1\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 1|=|1\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 1|.$$

(4):由定义 1.4 有:

$$wlp(\overline{q}*=U)(M)wlp(\overline{q}*=U)(N)=U_{\overline{q}}^{\dagger}MNU_{\overline{q}},$$

$$wlp(\overline{q}*=U)(N)wlp(\overline{q}*=U)(M)=U_{\overline{q}}^{\dagger}NMU_{\overline{q}}.$$

如果 M 和 N 可换,则有:

$$wlp(\overline{q}*=U)(M)wlp(\overline{q}*=U)(N)=wlp(\overline{q}*=U)(N)wlp(\overline{q}*=U)(M);$$

反之,如果 $wlp(\overline{q}*=U)(M)$和$wlp(\overline{q}*=U)(N)$ 可换,则

$$U_{\overline{q}}^{\dagger}MNU_{\overline{q}}=U_{\overline{q}}^{\dagger}NMU_{\overline{q}}.$$

故 M 和 N 可换.

(5):设 $A,B,C\in L(H)$,由 S_1 反射(A,B,C)-可换得

$$\begin{aligned}A\ wlp(S_1;S_2)(M)\ B\ wlp(S_1;S_2)(N)\ C&=A\ wlp(S_1)(wlp(S_2)(M))\ B\ wlp(S_1)(wlp(S_2)(N))\ C\\&=A\ wlp(S_1)(wlp(S_2)(N))\ B\ wlp(S_1)(wlp(S_2)(M))\ C\\&=A\ wlp(S_1;S_2)(N)\ B\ wlp(S_1;S_2)(M)\ C.\end{aligned}$$

所以,$S_1;S_2$ 也反射(A,B,C)-可换.

(6):记 S=**measure** q **then** S_1 **else** S_0,由定义 1.4 得:

$$\begin{aligned}wlp(S)(M)wlp(S)(N)=&|0\rangle_q\langle 0|wlp(S_0)(M)|0\rangle_q\langle 0|wlp(S_0)(N)|0\rangle_q\langle 0|+\\&|1\rangle_q\langle 1|wlp(S_1)(M)|1\rangle_q\langle 1|wlp(S_1)(N)|1\rangle_q\langle 1|,\\wlp(S)(N)wlp(S)(M)=&|0\rangle_q\langle 0|wlp(S_0)(N)|0\rangle_q\langle 0|wlp(S_0)(M)|0\rangle_q\langle 0|+\\&|1\rangle_q\langle 1|wlp(S_1)(N)|1\rangle_q\langle 1|wlp(S_1)(M)|1\rangle_q\langle 1|.\end{aligned}$$

如果 $wlp(S_i)(M)$和 $wlp(S_i)(N)$ $|i\rangle_q\langle i|$可换,i=0,1,则

$$wlp(S)(M)wlp(S)(N)=wlp(S)(N)wlp(S)(M);$$

反之,如果 $wlp(S)(M)$和 $wlp(S)(N)$可换,则

$$\begin{aligned}|0\rangle_q\langle 0|wlp(S_0)(M)|0\rangle_q\langle 0|wlp(S_0)(N)|0\rangle_q\langle 0|&=|0\rangle_q\langle 0|wlp(S)(M)wlp(S)(N)\\&=|0\rangle_q\langle 0|wlp(S)(N)wlp(S)(M)\\&=|0\rangle_q\langle 0|wlp(S_0)(N)|0\rangle_q\langle 0|wlp(S_0)(M)|0\rangle_q\langle 0|.\end{aligned}$$

类似地,有

$$|1\rangle_q\langle 1|wlp(S_1)(M)|1\rangle_q\langle 1|wlp(S_1)(N)|1\rangle_q\langle 1|=|1\rangle_q\langle 1|wlp(S_1)(N)|1\rangle_q\langle 1|wlp(S_1)(M)|1\rangle_q\langle 1|.$$

(7):记 $qloop$=**while** q **do** S,对任意的 $M\in P(H)$,由定义 1.4 知

$$wlp(qloop)(M)=\bigcap_{n=0}^{\infty}F^{(n)}(M),$$

其中,$F^{(0)}(M)=I$,并且

$$F^{(n+1)}(M)=|1\rangle_q\langle 1|wlp(qloop)(F^{(n)}(M))|1\rangle_q\langle 1|+|0\rangle_q\langle 0|M|0\rangle_q\langle 0|,n\geqslant 0.$$

由于$|1\rangle_q\langle 1|F^{(0)}(M)|1\rangle_q\langle 1|F^{(0)}(N)|1\rangle_q\langle 1|=|1\rangle_q\langle 1|F^{(0)}(N)|1\rangle_q\langle 1|F^{(0)}(M)|1\rangle_q\langle 1|=|1\rangle_q\langle 1|$,下证 $F^{(n)}(M)F^{(n)}(N)=F^{(n)}(N)F^{(n)}(M)$:

① 当 n=0 时,结论成立;

② 假设 $n=k$ 时结论成立,即

$$F^{(k)}(M)F^{(k)}(N)=F^{(k)}(N)F^{(k)}(M),$$

那么,当 $n=k+1$ 时,

$$F^{(k+1)}(M)F^{(k+1)}(N)=|1\rangle_q\langle 1|wlp(qloop)(F^{(k)}(M))|1\rangle_q\langle 1|wlp(qloop)(F^{(k)}(N))|1\rangle_q\langle 1|+|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|,$$

由于 S 反射$|1\rangle_q\langle 1|$-可换,M 和 N $|0\rangle_q\langle 0|$-可换,则上式变为

$$|1\rangle_q\langle 1|wlp(qloop)(F^{(k)}(N))|1\rangle_q\langle 1|wlp(qloop)(F^{(k)}(M))|1\rangle_q\langle 1|+|0\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 0|=F^{(k+1)}(N)F^{(k+1)}(M).$$

由数学归纳法可知,

$$F^{(n)}(M)F^{(n)}(N)=F^{(n)}(N)F^{(n)}(M),n\geqslant 0.$$

于是有:

$$\begin{aligned} wlp(qloop)(M)wlp(qloop)(N) &= \bigcap_{n=0}^{\infty}F^{(n)}(M)\bigcap_{n=0}^{\infty}F^{(n)}(N)\\ &= \bigcap_{n=0}^{\infty}F^{(n)}(N)\bigcap_{n=0}^{\infty}F^{(n)}(M)\\ &= wlp(qloop)(N)wlp(qloop)(M); \end{aligned}$$

反之,因为

$$|0\rangle_q\langle 0|F^{(n)}(M)F^{(n)}(N)=|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|,$$

而且

$$\begin{aligned} |0\rangle_q\langle 0|wlp(qloop)(M)wlp(qloop)(N) &= \bigcap_{n=0}^{\infty}|0\rangle_q\langle 0|F^{(n)}(M)F^{(n)}(N)\\ &=|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|, \end{aligned}$$

由 $wlp(qloop)(M)$和 $wlp(qloop)(N)$可换,则有:

$$\begin{aligned} |0\rangle_q\langle 0|wlp(qloop)(M)wlp(qloop)(N)&=|0\rangle_q\langle 0|wlp(qloop)(N)wlp(qloop)(M)\\ &=|0\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 0|. \end{aligned}$$

故 M 和 N $|0\rangle_q\langle 0|$-可换. □

3 最弱自由前置条件的若干性质

文献[13]提出最弱前置条件谓词转换 wp 是良好谓词转换,即满足条件:① 线性性;② 单调性;③ 连续性;④ 独异性.文献[15]中讨论了 wlp 的很多性质,并就其与 wp 的关系做了较为详尽的讨论.因此,本节我们针对最弱自由前置条件谓词转换 wlp 的部分性质讨论如下,并验证 wlp 不是良好谓词转换:

设 $S\in CP(H),M\in P(H),\rho\in D(H)$,则

$$tr(wp(S)(M)\rho)=trMS(\rho) \tag{1}$$

$$tr(wlp(S)(M)\rho)=trMS(\rho)+tr\rho-trS(\rho) \tag{2}$$

同时,对任意的 $M\in P(H)$,有 $wp(S)(M)\sqsubseteq wlp(S)(M)$,$wp(S)(M)+wlp(S)(M)=I$[15].

从 Hoare 逻辑的角度分析,等式(1)说明了输入ρ满足量子谓词 $wp(S)(M)$的概率等于量子程序 S 在ρ终止且输出为 $S(\rho)$满足 M 的概率.在等式(2)中,$tr\rho-trS(\rho)$表示量子程序 S 从输入ρ发散的概率.等式(2)表明,输入ρ满足 $wlp(S)(M)$的概率等于 $S(\rho)$满足 M 的概率与 S 从ρ发散的概率之和.

推论 3.1. 如果 S 是保迹的,则

$$tr(wlp(S)(M)\rho)=tr(MS(\rho)).$$

推论 3.2. 如果 S 是保迹的,对任意的$\lambda,\mu\in R,M,N\in P(H)$,假如$\lambda M+\mu N\in P(H)$,则

$$wlp(S)(\lambda M+\mu N)=\lambda wlp(S)(M)+\mu wlp(S)(N).$$

下面验证 $wlp(\cdot)$不是良好谓词转换:

(1) $wlp(\cdot)$不满足线性性质

设 $S,F\in CP(H),\alpha,\beta\in C,M\in P(H)$,因为

$$tr(wlp(\alpha S+\beta F)(M)\rho)=tr(M(\alpha S+\beta F)\rho)+tr\rho-tr(\alpha S+\beta F)\rho$$

$$=\alpha trMS(\rho)+\beta trMF(\rho)+tr\rho-\alpha trS(\rho)-\beta trF(\rho)$$
$$=tr(\alpha wlp(S)+\beta wlp(F))(M)\rho+tr\rho-\alpha tr\rho-\beta tr\rho,$$

所以,$wlp(\alpha S+\beta F)\neq\alpha wlp(S)+\beta wlp(F)$.然而当 $\alpha=\beta=\frac{1}{2}$ 时,有 $wlp\left(\frac{1}{2}S+\frac{1}{2}F\right)=\frac{1}{2}wlp(S)+\frac{1}{2}wlp(F)$.

(2) $wlp(\cdot)$满足单调性

$wlp(S)$的单调性是说,如果 $M\sqsubseteq N$,则 $wlp(S)(M)\sqsubseteq wlp(S)(N)$[15].

我们给出另一种证法:

因为

$$tr(wlp(S)(M)\rho)=trMS(\rho)+tr\rho-trS(\rho),$$
$$tr(wlp(S)(N)\rho)=trNS(\rho)+tr\rho-trS(\rho),$$

所以, $$tr(wlp(S)(N)\rho)-tr(wlp(S)(M)\rho)=trNS(\rho)-trMS(\rho)\sqsupseteq 0,$$

即 $$wlp(S)(M)\sqsubseteq wlp(S)(N).$$

(3) $wlp(\cdot)$满足连续性

设谓词序列 $M_1\sqsubseteq M_2\sqsubseteq\ldots\sqsubseteq M_i\sqsubseteq\ldots$有上确界 $\bigcup_i M_i$,则对任意的$\rho\in D(H)$,有

$$tr\left(wlp(S)\left(\bigcup_i M_i\right)\rho\right)=tr\left(\bigcup_i M_i\right)S(\rho)+tr\rho-trS(\rho)$$
$$=\bigcup_i trM_iS(\rho)+tr\rho-trS(\rho)$$
$$=\bigcup_i[trM_iS(\rho)+tr\rho-trS(\rho)]$$
$$=\bigcup_i tr(wlp(S)(M_i)\rho)$$
$$=tr\left(\bigcup_i wlp(S)(M_i)\rho\right),$$

所以, $wlp(S)\left(\bigcup_i M_i\right)=\bigcup_i wlp(S)(M_i)$.

(4) $wlp(\cdot)$不满足独异性

$wlp(\cdot)$单调性不成立,即 $S_1\sqsubseteq S_2$ 不能推出 $wlp(S_1)\sqsubseteq wlp(S_2)$.但是,

$$tr\left(wlp\left(\bigcup_i S_i\right)(M)\rho\right)=trM\bigcup_i S_i(\rho)+tr\rho-tr\bigcup_i S_i(\rho)$$
$$=\bigcup_i trMS_i(\rho)+tr\rho-\bigcup_i trS_i(\rho)$$
$$=\bigcup_i[trMS_i(\rho)+tr\rho+trS_i(\rho)]$$
$$=\bigcup_i tr(wlp(S_i)(M)\rho)$$
$$=tr\left(\bigcup_i wlp(S_i)(M)\rho\right),$$

所以, $wlp\left(\bigcup_i S_i\right)=\bigcup_i wlp(S_i)$. □

以上我们从 Hoare 逻辑满足关系的角度和 wlp 不满足良好谓词转换的 4 个条件的分析可知,wlp 不是良好谓词转换,而是比 wp 更弱(即更大)的一类量子谓词转换,这与结论 $wp(S)(M)\sqsubseteq wlp(S)(M)$[15]是一致的.在经典程序中,总体正确性考虑的是程序 S 的每条计算,部分正确性考虑的是程序 S 的每条终止计算,程序的发散计算是不考虑的.在量子情况下,量子最弱前置条件 wp 和量子最弱自由前置条件 wlp 在研究量子程序的总体正确性和部分正确性中起了很关键的作用[10,13,15,17,18].Hoare 逻辑的公理化系统有两个证明系统:一个是总体正确性,另一个是部分正确性.正如文献[17]所述,通过研究量子程序的 wp 和 wlp,进而证明量子程序 Hoare 逻辑的完备性,这为量子程序语言的设计提供了逻辑基础.

根据上述分析,下面讨论 wlp 的序列合成、并行合成、块结构等性质.

设 $S\in CP(H),M\in P(H),\rho\in D(H),S_i\in CP(H_i),M_i\in P(H_i),\rho_i\in D(H_i),i=1,2$.

(1) 序列合成

因为

$$\begin{aligned}tr(wlp(S_1;S_2)(M)\rho)&=trM(S_1;S_2)\rho+tr\rho-tr(S_1;S_2)\rho\\&=trMS_2(S_1(\rho))+tr\rho-trS_2(S_1(\rho))\\&=tr[wlp(S_2)(M)S_1(\rho)]+tr\rho-trS_1(\rho)\\&=tr[wlp(S_1)(wlp(S_2)(M))\rho]\\&=tr[(wlp(S_2);wlp(S_1))(M)\rho],\end{aligned}$$

所以,$wlp(S_1;S_2)=wlp(S_2);wlp(S_1)$.

(2) 并行合成

因为

$$\begin{aligned}tr(wlp(S_1\oplus S_2)(M_1\oplus M_2)(\rho_1\oplus\rho_2))&=tr(M_1\oplus M_2)(S_1\oplus S_2)(\rho_1\oplus\rho_2)+tr(\rho_1\oplus\rho_2)-tr(S_1\oplus S_2)(\rho_1\oplus\rho_2)\\&=trM_1S_1(\rho_1)+trM_2S_2(\rho_2)+tr\rho_1+tr\rho_2-trS_1(\rho_1)-trS_2(\rho_2)\\&=tr(wlp(S_1)(M_1)\rho_1)+tr(wlp(S_2)(M_2)\rho_2)\\&=tr(wlp(S_1)\oplus wlp(S_2))(M_1\oplus M_2)(\rho_1\oplus\rho_2),\end{aligned}$$

所以,$wlp(S_1\oplus S_2)=wlp(S_1)\oplus wlp(S_2)$.

(3) 块结构

因为

$$\begin{aligned}tr(wlp(S_1\otimes I_2)(M_1\otimes I_2)(\rho_1\otimes\rho_2))&=tr(M_1\otimes I_2)(S_1\otimes I_2)(\rho_1\otimes\rho_2)+tr(\rho_1\otimes\rho_2)-tr(S_1\otimes I_2)(\rho_1\otimes\rho_2)\\&=trM_1S_1(\rho_1)tr\rho_2+tr\rho_1tr\rho_2-trS_1(\rho_1)tr\rho_2\\&=[trM_1S_1(\rho_1)+tr\rho_1-trS_1(\rho_1)]tr\rho_2\\&=tr(wlp(S_1)(M_1)\rho_1)tr\rho_2\\&=tr[(wlp(S_1)(M_1)\rho_1)\otimes\rho_2]\\&=tr[(wlp(S_1)(M_1)\otimes I_2)(\rho_1\otimes\rho_2)]\\&=tr(wlp(S_1)\otimes I_2)(M_1\otimes I_2)(\rho_1\otimes\rho_2),\end{aligned}$$

所以,$wlp(S_1\otimes I_2)=wlp(S_1)\otimes I_2$.

量子流程图语言,如大家熟知的量子程序语言 QPL,是量子计算中按照量子数据经典控制思想设计的一种程序语言,它形式化地被定义为范畴的语境,并且有一个指称语义.在语法构成上,QPL 中的程序可以用流程图来表示,也可以用 QPL 术语来描述[10,13,14,18].本节我们针对量子流程图语言的序列合成、并行合成、块结构等讨论了 wlp 语义,这些结构同 wp 语义是一致的.

4 结 论

本文主要研究了最弱自由前置条件 wlp 的交换性及其部分性质.由于 wlp 不能表示成算子和的形式,wlp 的可换性的讨论就比较复杂.因此,我们先给出了量子谓词 M 和 $N(A,B,C)$-可换和超算子 ε 反射 (A,B,C)-可换的定义,研究了 wlp 的可换性问题.同时,讨论了 wlp 不是良好谓词转换的问题,验证了 wlp 是比 wp 更弱的谓词转换,揭示了 wlp 和 wp 的本质区别.最后,从量子流程图语言的角度研究了 wlp 的序列合成、并行合成和块结构等性质,发现 wlp 和 wp 在上述 3 个方面的性质都是保持的.另外,在经典概率程序中,不变量在推理 Loop 程序时起到了关键的作用,同样的结论在量子系统情况下也是正确的.为了推理量子程序部分正确性的完备性,文献[15]引入了 wlp 不变量来推理量子 Loop 程序,这些结果为我们设计量子程序语言时考虑量子程序的部分正确性提供了理论保证.

文献[15]定义了类似于概率谓词的交算子&算子,研究了 wp 在量子谓词的交算子&下的许多性质,那么&算子在 wlp 语义下是否有意义,其性质如何,是我们下一步研究的问题.另外,在确定型程序中,经典谓词的交($\wedge$)运算有很重要的性质[4],也就是说,对任意经典谓词 p 和 q,

$$wp(S)(p\wedge q)\Leftrightarrow wp(S)(p)\wedge wp(S)(q),$$

并且对概率谓词α和β,有

$$wp(S)(\alpha\&\beta)<\equiv wp(S)(\alpha)\&wp(S)(\beta).$$

然而,文献[15]中的定义 4.4 指出,两个量子谓词的交一般不是单调的,类似的性质对量子程序是不成立的.文献[15]给出了一个公开问题,即对量子谓词而言,是否存在一个交的概念使得类似的性质被保持.那么,本文的研究对上述问题的解决是否有促进作用,量子谓词交的概念是否可以推广到 wlp 语义中等等,是我们进一步研究的课题.

References:

[1] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000.

[2] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proc. of the 35th Annual Symp. on Foundations of Computer Science. Los Alamitos: IEEE Press, 1994. 124−134. [doi: 10.1109/SFCS.1994.365700]

[3] Grover L. A fast quantum mechanical algorithm for database search. In: Proc. of the 28th Annual ACM Symp. on the Theory of Computing. New York: ACM Press, 1996. 212−219. [doi: 10.1145/237814.237866]

[4] Dijlstra EW. A Discipline of Programming. Englewood Cliffs: Prentice-Hall, 1976.

[5] Knill EH. Conventions for quantum pseudocode. LANL Report, LAUR-96-2724, 1996.

[6] Ömer B. A procedural formalism for quantum computing [MS. Thesis]. Department of Theoretical Physics, Technical University of Vienna, 1998.

[7] Ömer B. Structured quantum programming [Ph.D Thesis]. Department of Theoretical Physics, Technical University of Vienna, 2003.

[8] Sanders JW, Zuliani P. Quantum programming. In: Proc. of the Mathematics of Program Construction 2000. LNCS 1837, Berlin, Heidelberg: Springer-Verlag, 2000. 80−99. [doi: 10.1007/10722010_6]

[9] Zuliani P. Compiling quantum programs. Acta Informatica, 2005,41(7-8):435−473. [doi: 10.1007/s00236-005-0165-3]

[10] Selinger P. Towards a quantum programming language. Mathematics Structures in Computer Science, 2004,14(4):527−586. [doi: 10.1017/S0960129504004256]

[11] Li YY, Jiao LC. Quantum clonal algorithm for multicast routing problem. Ruan Jian Xue Bao/Journal of Software, 2007,18(9): 2063−2069 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2063.html [doi: 10.1360/jos182063]

[12] Liu L, Xu JF. Quantum programming language NDQJava-2. Ruan Jian Xue Bao/Journal of Software, 2011,22(5):877−886 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3979.html [doi: 10.3724/SP.J.1001.2011.03979]

[13] D'Hondt E, Panangaden P. Quantum weakest preconditions. Mathematical Structures in Computer Science, 2006,16:429−451. [doi: 10.1017/S0960129506005251]

[14] Ying MS, Feng Y. A flow chart language for quantum programming. IEEE Trans. on Software Engineering, 2011,37(4):466−485. [doi: 10.1109/TSE.2010.94]

[15] Feng Y, Duan RY, Ji ZF, Ying MS. Proof rules for the correctness of quantum programs. Theoretical Computer Science, 2007,386: 151−166. [doi: 10.1016/j.tcs.2007.06.011]

[16] Ying MS, Chen JX, Feng Y, Duan RY. Commutativity of quantum weakest preconditions. Information Processing Letters, 2007, 104:152−158. [doi: 10.1016/j.ipl.2007.06.003]

[17] Ying MS. Floyd-Hoare logic for quantum programs. ACT Trans. on Programming Languages and Systems, 2011,33(6):19−49. [doi: 10.1145/2049706.2049708]

[18] Ying MS, Duan RY, Feng Y, Ji ZF. Predicate transformer semantics of quantum programs. In: Gay S, Makie I, eds. Proc. of the Semantic Techniques in Quantum Computation. Cambridge University Press, 2010. 311−360.

附中文参考文献:

[11] 李阳阳,焦李成.量子克隆多播路由算法.软件学报,2007,18(9):2063−2069. http://www.jos.org.cn/1000-9825/18/2063.html [doi: 10.1360/jos182063]

[12] 刘玲,徐家福.量子程序设计语言 NDQJava-2.软件学报,2011,22(5):877−886. http://www.jos.org.cn/1000-9825/3979.html [doi: 10.3724/SP.J.1001.2011.03979]

雷红轩(1967－),男,陕西洋县人,博士生,副教授,主要研究领域为自动机理论,量子程序验证,量子模型检测.
E-mail: leihx2004@yahoo.com.cn

席政军(1983－),男,博士,讲师,CCF 会员,主要研究领域为量子信息论,量子程序语言.
E-mail: xizhengjun@snnu.edu.cn

李永明(1966－),男,博士,教授,CCF 高级会员,主要研究领域为计算智能,模糊系统分析,量子逻辑,量子计算,模型检测.
E-mail: liyongm@snnu.edu.cn