量子計算のための Hoare 論理

角谷良彦
東京大学情報理工学系研究科コンピュータ科学専攻
kakutani@is.s.u-tokyo.ac.jp

概要

量子計算のための Hoare 論理

- 量子プログラムの形式的検証が可能である。
- 確率的 Hoare 論理 [den Hartog 1999] の拡張になっている。
- 量子状態の確率的な性質を扱うことができる。
- 密度行列に基づく意味論に対して健全である。

関連研究

- Baltag and Smets (2006)
- Chadha et al. (2006)
- Ying (2009)

量子プログラム

対象とする量子プログラム [Selinger 2004] は以下で定義される。

$$
\begin{aligned}
P ::= \ & \texttt{skip} \mid P \ ; \ P \\
& \mid \texttt{bit } b \mid \texttt{qbit } q \mid \texttt{discard } b \mid \texttt{discard } q \\
& \mid b := 0 \mid b := 1 \mid q, \ldots, q \mathrel{*}= U \\
& \mid \texttt{if } b \texttt{ then } P \texttt{ else } P \mid \texttt{while } b \texttt{ do } P \\
& \mid \texttt{measure } q \texttt{ then } P \texttt{ else } P
\end{aligned}
$$

プログラムの意味は、密度行列上の正値エルミート変換で与えられる。

確率的 Hoare 論理

Hoare 論理では、プログラム P と論理式 Φ、Ψ の組

$$\{\Phi\}\ P\ \{\Psi\}$$

を導出する。

これは、通常の Hoare 論理では、「Φ が成り立つ状態で P を実行すると、その実行が停止した後、Ψ が成り立つ」ということを意味する。

それに対して、確率的 Hoare 論理 [den Hartog 1999] では、「Φ が成り立つ状態で P を実行すると、（P が停止するしないに係らず、）実行後に Ψ が成り立つ」を意味する。

量子的 Hoare 論理は、確率的 Hoare 論理の拡張として定義される。

確率に関する論理式

確率的 Hoare 論理の論理式は以下の通り。

$$
\begin{aligned}
\boldsymbol{c} &::= r \mid \boldsymbol{\alpha} \mid \boldsymbol{f}(\boldsymbol{c}, \ldots, \boldsymbol{c}) \\
\boldsymbol{t} &::= \boldsymbol{c} \mid \mathrm{pr}\,(\boldsymbol{\rho}) \mid \boldsymbol{f}(\boldsymbol{t}, \ldots, \boldsymbol{t}) \\
\boldsymbol{\Phi} &::= \boldsymbol{t} \leq \boldsymbol{t} \mid \mathrm{int}\,(\boldsymbol{t}) \mid \boldsymbol{t}\boldsymbol{\Phi} \mid {}^{\boldsymbol{x},\ldots,\boldsymbol{x}}\boldsymbol{M}\boldsymbol{\Phi} \mid \boldsymbol{\Phi} \oplus \boldsymbol{\Phi} \\
&\quad \mid \neg\boldsymbol{\Phi} \mid \boldsymbol{\Phi} \wedge \boldsymbol{\Phi} \mid \forall \boldsymbol{\alpha}.\ \boldsymbol{\Phi}
\end{aligned}
$$

ここで、r は実数、ρ はプログラム変数に対する命題、M は行列。

量子的 Hoare 論理の論理式も定義は同じ。

ただし、pr (ρ) は、「観測した場合に ρ が成り立つ確率」を意味する。

推論規則

量子的 Hoare 論理の推論規則の例。

$$\frac{\{\,{}^{b}\!\begin{pmatrix}1&0\\0&0\end{pmatrix}\!\Phi\,\}\ P_0\ \{\,\Psi_0\,\} \qquad \{\,{}^{b}\!\begin{pmatrix}0&0\\0&1\end{pmatrix}\!\Phi\,\}\ P_1\ \{\,\Psi_1\,\}}{\{\,\Phi\,\}\ \texttt{if}\ b\ \texttt{then}\ P_1\ \texttt{else}\ P_0\ \{\,\Psi_0 \oplus \Psi_1\,\}}$$

$$\frac{\{\,{}^{q}\!\begin{pmatrix}1&0\\0&0\end{pmatrix}\!\Phi\,\}\ P_0\ \{\,\Psi_0\,\} \qquad \{\,{}^{q}\!\begin{pmatrix}0&0\\0&1\end{pmatrix}\!\Phi\,\}\ P_1\ \{\,\Psi_1\,\}}{\{\,\Phi\,\}\ \texttt{measure}\ q\ \texttt{then}\ P_1\ \texttt{else}\ P_0\ \{\,\Psi_0 \oplus \Psi_1\,\}}$$

$$\frac{\{\,{}^{b}\!\begin{pmatrix}0&0\\0&1\end{pmatrix}\!\Phi_n\,\}\ P\ \{\,\Phi_{n+1}\,\} \qquad \{\,{}^{b}\!\begin{pmatrix}1&0\\0&0\end{pmatrix}\!\Phi_n \mid n \in \mathbb{N}\,\} \models \Psi}{\{\,\Phi_o\,\}\ \texttt{while}\ b\ \texttt{do}\ P\ \{\,\Psi\,\}}$$

$$\frac{}{\{\,\Phi\,\}\ \overrightarrow{q}\ \texttt{*=}\ U\ \{\,{}^{\overrightarrow{q}}U\Phi\,\}}$$

`while` に関する規則

以下の条件が満たされるとき、

1. $p\Phi \oplus (1-p)\Phi \models \Phi$ holds for any $p \in \mathbb{R}$.
2. ${}^{b}\mathsf{E}_{i}\Phi \models \frac{\mathsf{pr}\,(\bar{b}=i)}{\mathsf{pr}\,()}\Phi$ holds.
3. $[\![\texttt{while}\ b\ \texttt{do}\ P]\!]$ preserves traces.

次のような導出が可能である。

$$\frac{\{\,(\mathsf{pr}\,(\bar{b}=1)=1)\wedge\Phi\,\}\ P\ \{\,\Phi\,\}}{\{\,(\mathsf{pr}\,()=1)\wedge\Phi\,\}\ \texttt{while}\ b\ \texttt{do}\ P\ \{\,(\mathsf{pr}\,(\bar{b}=0)=1)\wedge\Phi\,\}}$$

糖衣構文

$$x[] \equiv x[1], \ldots, x[n]$$

$$\texttt{bit}\ b[m\text{-}n] \equiv \texttt{bit}\ b[m], \ldots, b[n]$$

$$\texttt{qbit}\ q[m\text{-}n] \equiv \texttt{qbit}\ q[m], \ldots, q[n]$$

$$\texttt{bit}\ b_1, \ldots, b_n \equiv \texttt{bit}\ b_1\ ;\ \cdots\ ;\ \texttt{bit}\ b_n$$

$$\texttt{qbit}\ q_1, \ldots, q_n \equiv \texttt{qbit}\ q_1\ ;\ \cdots\ ;\ \texttt{qbit}\ q_n$$

$$\texttt{discard}\ x_1, \ldots, x_n \equiv \texttt{discard}\ x_1\ ;\ \cdots\ ;\ \texttt{discard}\ x_n$$

$$b_1, \ldots, b_n := i \equiv b_1 := i[1]\ ;\ \cdots\ ;\ b_n := i[n]$$

$$b := \texttt{measure}\ q \equiv \texttt{measure}\ q\ \texttt{then}\ (b := 1)\ \texttt{else}\ (b := 0)$$

$$b_1, \ldots, b_n := \texttt{measure}\ q_1, \ldots, q_n$$

$$\equiv b_1 := \texttt{measure}\ q_1\ ;\ \cdots\ ;\ b_n := \texttt{measure}\ q_n$$

行列の略記

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

量子テレポーテーション

$\{\ {}^{\mathtt{qa}}U(\mathsf{pr}\,(\overline{\mathtt{qa}} = 0) = 1)\ \}$

$\mathtt{qbit\ q, qb}$

$\{\ {}^{\mathtt{qa}}U(\mathsf{pr}\,(\overline{\mathtt{qa}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\mathtt{q}} = 0) = 1)\ \}$

$\mathtt{q, qb} \mathrel{*}= \begin{pmatrix} \mathsf{N} & \mathsf{N} \\ -\mathsf{I} & \mathsf{I} \end{pmatrix}\ ;\ \mathtt{qa, q} \mathrel{*}= \begin{pmatrix} \mathsf{N} & \mathsf{N} \\ -\mathsf{I} & \mathsf{I} \end{pmatrix}^{\dagger}$

$\{\ {}^{\mathtt{qa,q}}\begin{pmatrix} \mathsf{N} & \mathsf{N} \\ -\mathsf{I} & \mathsf{I} \end{pmatrix}^{\dagger} {}^{\mathtt{q,qb}}\begin{pmatrix} \mathsf{N} & \mathsf{N} \\ -\mathsf{I} & \mathsf{I} \end{pmatrix} {}^{\mathtt{qa}}U(\cdots)\ \}$

$\mathtt{measure\ q}$

$\quad \mathtt{then}\ (\mathtt{measure\ qa\ then}\ (\mathtt{qb} \mathrel{*}= \mathsf{N}\mathsf{V}^{\mathbf{2}}\mathsf{N})\ \mathtt{else}\ (\mathtt{qb} \mathrel{*}= \mathsf{V}^{\mathbf{2}}))$

$\quad \mathtt{else}\ (\mathtt{measure\ qa\ then}\ (\mathtt{qb} \mathrel{*}= \mathsf{N})\ \mathtt{else\ skip})$

$\{\ {}^{\mathtt{qb}}U(\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1)\ \}$

量子テレポーテーション

$$\{\ {}^{\mathtt{qa}}\mathsf{E}_0\,{}^{\mathtt{q}}\mathsf{E}_0\,\boldsymbol{\Phi}\ \}\ \ \mathtt{skip}\ \ \{\ r_{00}\,{}^{\mathtt{qb}}\boldsymbol{U}(\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1)\ \}$$

$$\{\ {}^{\mathtt{qa}}\mathsf{E}_0\,{}^{\mathtt{q}}\mathsf{E}_1\,\boldsymbol{\Phi}\ \}\ \ \mathtt{qb} \mathrel{*}= \mathsf{V}^2\ \ \{\ r_{01}\,{}^{\mathtt{qb}}\boldsymbol{U}(\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1)\ \}$$

$$\{\ {}^{\mathtt{qa}}\mathsf{E}_1\,{}^{\mathtt{q}}\mathsf{E}_0\,\boldsymbol{\Phi}\ \}\ \ \mathtt{qb} \mathrel{*}= \mathsf{N}\ \ \{\ r_{10}\,{}^{\mathtt{qb}}\boldsymbol{U}(\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1)\ \}$$

$$\{\ {}^{\mathtt{qa}}\mathsf{E}_1\,{}^{\mathtt{q}}\mathsf{E}_1\,\boldsymbol{\Phi}\ \}\ \ \mathtt{qb} \mathrel{*}= \mathsf{N}\,\mathsf{V}^2\,\mathsf{N}\ \ \{\ r_{11}\,{}^{\mathtt{qb}}\boldsymbol{U}(\mathsf{pr}\,(\overline{\mathtt{qb}} = 0) = 1)\ \}$$

ただし、r_{ij} は $\mathsf{pr}\,((\overline{\mathtt{qa}} = i) \wedge (\overline{\mathtt{q}} = j))$。

量子 Deutsch 問題の解法

$f(0) = f(1) = 1$ の場合。

$\{\, \mathsf{pr}\,() = 1 \,\}$

`bit b ; qbit q1,q2`

$\{\, (\mathsf{pr}\,(\overline{\mathtt{q1}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\mathtt{q2}} = 0) = 1) \,\}$

`q2 *= HN ; q1 *= H ; q1,q2 *=` U_f `; q1 *= H`

$\{\, {}^{\mathtt{q1},\mathtt{q2}}(\mathsf{H} \otimes \mathsf{I}) U_f (\mathsf{H} \otimes \mathsf{HN})(\cdots) \,\}$

$\{\, \mathsf{pr}\,(\overline{\mathtt{q1}} = 0) = 1 \,\}$

`b := measure q1`

$\{\, \mathsf{pr}\,(\overline{\mathtt{b}} = 0) = 1 \,\}$

Shor の素因数分解アルゴリズム

n、m、x は、$x^2 < n^2 \leq 2^m < 2n^2$ を満たす自然数。また、r は、$\mathbb{N}/{=_n}$ における x の位数。

$\{ \mathsf{pr}\,() = 1 \}$

$\texttt{bit c[1-}m\texttt{] ; bit r[1-}\lfloor m/2 \rfloor\texttt{]}$

$\texttt{qbit q1[1-}m\texttt{] ; qbit q2[1-}m\texttt{]}$

$\{ (\mathsf{pr}\,(\overline{\texttt{q1}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\texttt{q2}} = 0) = 1) \}$

$\texttt{q1[] *= H}_m$

$\{ {}^{\texttt{q1}}\mathsf{H}_m(\mathsf{pr}\,(\overline{\texttt{q1}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\texttt{q2}} = 0) = 1) \}$

$\mathsf{Exp}\,(\texttt{q1[]}, \texttt{q2[]})$

Shor の素因数分解アルゴリズム

$$\{\ {}^{\mathtt{q1}}\mathsf{H}_m\,(\mathsf{pr}\,(\overline{\mathtt{q1}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\mathtt{q2}} =_n x^{\overline{\mathtt{q1}}}) = 1)\ \}$$

$$\mathtt{q1[]}\ \mathtt{*=}\ \mathsf{F}_m$$

$$\{\ {}^{\mathtt{q1}}\mathsf{F}_m\,({}^{\mathtt{q1}}\mathsf{H}_m\,(\mathsf{pr}\,(\overline{\mathtt{q1}} = 0) = 1) \wedge (\mathsf{pr}\,(\overline{\mathtt{q2}} =_n x^{\overline{\mathtt{q1}}}) = 1))\ \}$$

$$\mathtt{c[]}\ \mathtt{:=}\ \mathtt{measure}\ \mathtt{q1[]}$$

$$\{\ \forall \alpha.\ \mathsf{int}\,(\alpha) \supset (\mathsf{pr}\,(\overline{\mathtt{c}} = \alpha) = f(\alpha))\ \}$$

$$\{\ \mathsf{pr}\,(\exists k \in \mathbb{N}.\ (r\overline{\mathtt{c}} =_{2^m} k) \wedge (-r/2 \leq k \leq r/2)) > 1/3\ \}$$

$$\{\ \mathsf{pr}\,(\exists d \in \mathbb{N}.\ |(\overline{\mathtt{c}}/2^m) - (d/r)| \leq 1/2^{m+1}) > 1/3\ \}$$

$$\mathsf{Frac}\,(\mathtt{c[]}, \mathtt{r[]})$$

$$\{\ \exists \delta.\ \mathsf{pr}\,(\overline{\mathtt{r}} = r) > \delta/(\log\log r)\ \}$$

今後の課題

- 完全性の考察
- より複雑なプログラムの検証
- 検証の自動化
  - 推論規則の改良
  - 他のプログラミング言語への対応