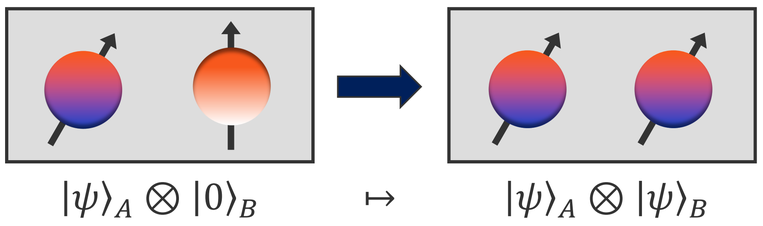
アフィン量子ラムダ計算と双模倣について

柏木力哉　五十嵐淳　（京都大学）

量子情報の保存と線形論理

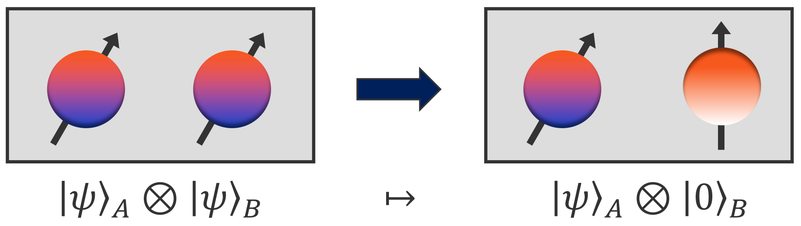
縮約と弱化を禁止

任意の量子情報の複製不可
縮約の禁止



$|\psi\rangle_A \otimes |0\rangle_B \quad \mapsto \quad |\psi\rangle_A \otimes |\psi\rangle_B$

任意の量子情報の削除不可
弱化の禁止

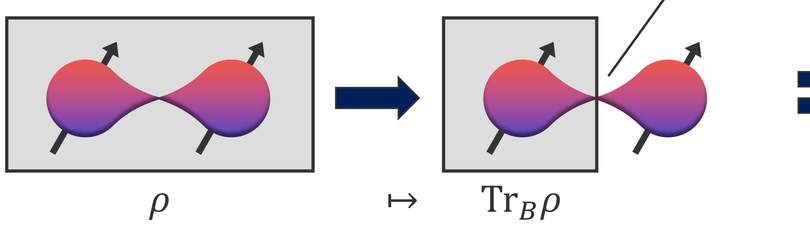


$|\psi\rangle_A \otimes |\psi\rangle_B \quad \mapsto \quad |\psi\rangle_A \otimes |0\rangle_B$

量子状態の隠蔽とアフィン論理

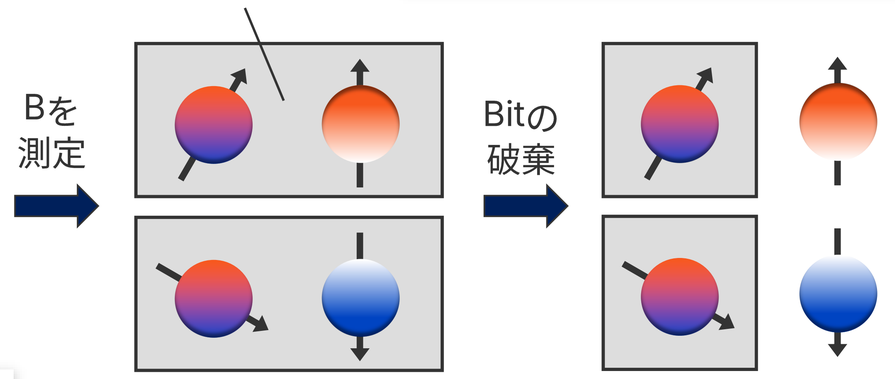
縮約のみ禁止

状態の隠蔽
観測する世界を制限



$\rho \quad \mapsto \quad \mathrm{Tr}_B\rho \quad = \quad \rho$

干渉が壊れる



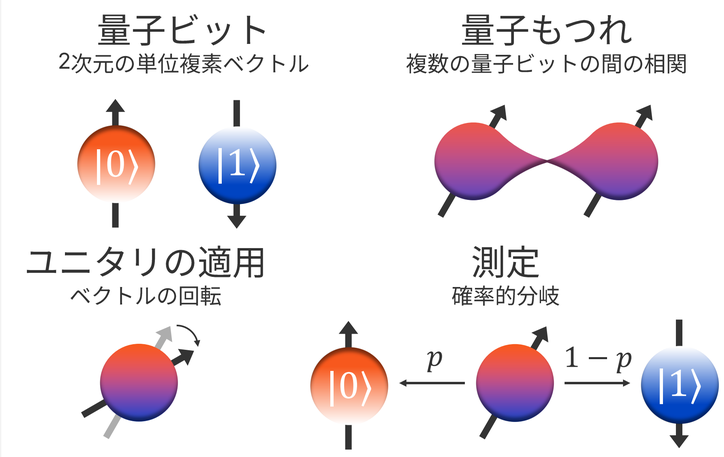
$\Sigma_{i\in\{0,1\}} P_{i,B}\rho P_{i,B} \qquad \mathrm{Tr}_B\left[\Sigma_{i\in\{0,1\}} P_{i,B}\rho P_{i,B}\right]$

※ $\mathrm{Tr}_B\rho = \mathrm{Tr}_B\left[\Sigma_{i\in\{0,1\}} P_{i,B}\rho P_{i,B}\right]$

内部状態を区別しないで観測する世界に注目するなら弱化は可能！

$\mathrm{drop}\ x\ \mathrm{in}\ M \coloneqq \mathrm{let}\,!\,x = \mathrm{meas}\ x\ \mathrm{in}\ M \approx M$

量子計算の構成要素



目的：高階量子プログラムのより一般の等価性の分析

線形論理×量子計算
観測する世界を固定し、行列の等価性で区別

→ アフィン論理×量子計算
観測によって区別できない内部状態の差を無視

アフィン
初期の定義では実はアフィン性ベース
[Selinger & Valiron,TLCA'05,CUP'09]

量子ラムダ計算：高階関数＋線形性＋量子計算効果

$$M,N,L ::= x \mid \lambda x.M \mid M\ N \mid (M,N) \mid \mathrm{let}\,(x,y) = M\ \mathrm{in}\ N \mid 0 \mid 1 \mid \mathrm{if}\ M\ \mathrm{then}\ N\ \mathrm{else}\ L$$
$$\mid !\,M \mid \mathrm{let}\,!\,x = M\ \mathrm{in}\ N \mid \mathrm{new} \mid \mathrm{gate}_U \mid \mathrm{meas}$$

$$\frac{!\,\Gamma \vdash M}{!\,\Gamma \vdash !\,M} \qquad \frac{\Gamma \vdash M \quad \Delta, !\,x \vdash N}{\Gamma,\Delta \vdash \mathrm{let}\,!\,x = M\ \mathrm{in}\ N}$$

線形ラムダ計算[Maraist et al.,ENTCS'95]

$\mathrm{new} : \mathrm{Bit} \multimap \mathrm{Qubit}$ 量子状態準備
$\mathrm{gate}_U : \mathrm{Qubit}^{\otimes n} \multimap \mathrm{Qubit}^{\otimes n}$ ゲートU適用
$\mathrm{meas} : \mathrm{Qubit} \multimap !\,\mathrm{Bit}$ 測定

	縮約	弱化
M	~~$\dfrac{\Gamma, y, z \vdash M}{\Gamma, x \vdash M[x/y, x/z]}$~~	$\dfrac{\Gamma \vdash M}{\Gamma, x \vdash M}$
$!\,M$	$\dfrac{\Gamma, !\,y, !\,z \vdash M}{\Gamma, !\,x \vdash M[x/y, x/z]}$	$\dfrac{\Gamma \vdash M}{\Gamma, !\,x \vdash M}$

$!\,M$の用途
- 古典データの複製
- 量子回路の複製≠量子状態の複製

$(\lambda x.\mathrm{let}\,!\,y = x\ \mathrm{in}\ \langle x,x\rangle)\,!\,(H\ 0) \to^* \langle H\ 0, H\ 0\rangle$

量子ラムダ計算の文脈等価性・双模倣性

双模倣性 ($\sim$)
Compatibleであれば文脈等価に対して健全

⟷

文脈等価性 ($\approx$)
任意の文脈の下で観測可能な振る舞いが等価

双模倣による局所的な書き換えがプログラム全体の振る舞いを損なわないことを保証

Compatible関係

$$M\ \mathcal{R}\ N \implies \forall C.\ C[M]\ \mathcal{R}\ C[N]$$

アフィン文脈
- 一つだけ穴を持つ項
- アフィン性を保つ：$\Gamma \vdash M \implies \Delta \vdash C[M]$

線形量子ラムダ計算の双模倣の先行研究[Dal Lago+,FSE'15][Deng+,CONCUR'15]

定義(Big step意味論)
$[\![[\rho, M]]\!] = \Sigma_i p_i[\rho_i, V_i]$

量子状態と項の組に対して定義
✗ 変数の破棄が外部的な効果

定理(健全性)
$(\forall \rho.\,[\rho, M] \sim [\rho, N]) \implies M \approx N$

任意の量子状態ρについてテスト
✗ 双模倣の強みである局所性がない

提案：プロセスベースの操作的意味論

項を量子プロセスとして解釈することで内部状態を隠蔽

kステップのBig step意味論（抜粋）

入力に量子状態が現れない & リソース主導
入力の量子状態
量子ビット数 $n = |\Gamma|$
出力の量子状態と結果の値

$$[\![\Gamma \vdash M]\!]_k : \mathbf{CPTP}(\mathcal{D}(n), \oplus_{m\in\mathbb{N}} \mathcal{D}(m) \times \mathcal{V}(m))$$
$$[\![\Gamma \vdash M]\!]_0 = \bot$$
$$[\![\Gamma \vdash E[\mathrm{new}\ b]]\!]_{k+1} = \underline{new_b}([\![\Gamma, q_{n+1} \vdash E[q_{n+1}]]\!]_k)$$
$$[\![\Gamma \vdash E[\mathrm{gate}_U\ q_{\vec{i}}]]\!]_{k+1} = \underline{gate_{U,\vec{i}}}([\![\Gamma \vdash E[q_{\vec{i}}]]\!]_k)$$
$$[\![\Gamma \vdash E[\mathrm{meas}\ q_i]]\!]_{k+1} = \underline{meas_i}([\![\Gamma \vdash E[!\,0]]\!]_k, [\![\Gamma \vdash E[!\,1]]\!]_k)$$

文脈等価性

$$M \approx N \overset{\mathrm{def}}{\Leftrightarrow} \forall C.\vdash C : \Gamma \rightrightarrows \emptyset \implies \mathrm{obs}([\![\vdash C[M]]\!]) = \mathrm{obs}([\![\vdash C[N]]\!])$$

双模倣性

既存	提案
$\forall \rho.\,[\rho, M] \sim [\rho, N]$	$M \sim N$
変数の破棄には外部的な遷移が必要 $[\rho, M] \to [\mathrm{Tr}_q\ \rho, M]$	破棄を内部的な効果として吸収 $(I_\Gamma \otimes \mathrm{Tr}_q) \circ [\![\Gamma, q \vdash M]\!]$ $= [\![\Gamma \vdash M]\!] \circ (I_\Gamma \otimes \mathrm{Tr}_q)$

仮説
- 提案する双模倣が健全性・完全抽象性を満たすか
- $(T\mathcal{V})(n) = \mathbf{CPTP}(\mathcal{D}(n), \oplus_{m\in\mathbb{N}} \mathcal{D}(m) \times \mathcal{V}(m))$はモナドか
- $\underline{new_b}, \underline{gate_{U,\vec{j}}}, \underline{meas_j}$は$T\mathcal{V}$で解釈される代数的効果か