

スケジューラを用いた 量子プロセス間の観測同値

○安田和矢 久保田貴大 角谷良彦
(東京大学)

2014/3/19

量子暗号とプロセス計算

様々な量子暗号プロトコル

量子鍵配送：BB84, B92, ...

量子ビットコミットメント

量子紛失通信

プロセス計算を用いて形式的検証

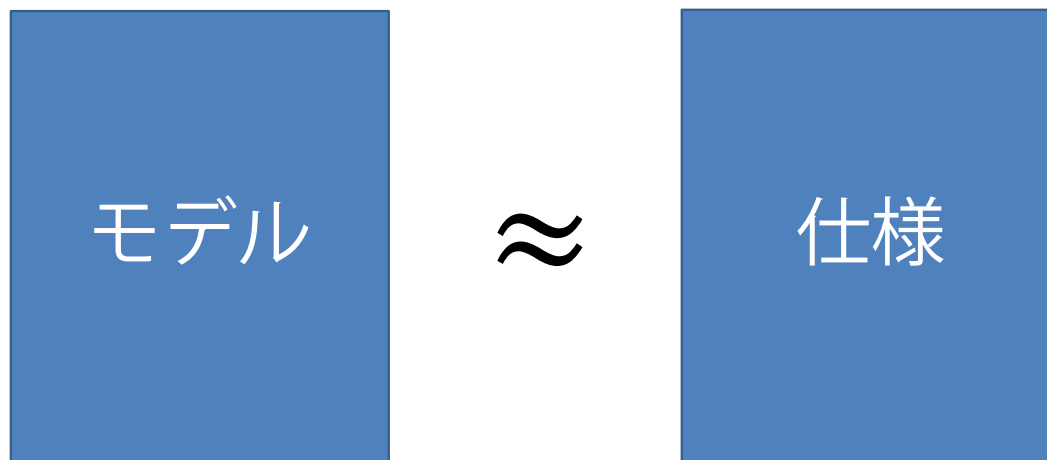
量子プロセス計算にもいくつかの計算体系

プロセス間の等価関係

ふたつのプロセスの「等しさ」

Bisimulation (双模倣関係)

Barbed congruence (bisimulation と一致)



等価にならない量子プロセス

Bisimilar ではないが、
直感的には等価な量子プロセスの存在

例：

量子状態 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ に対して
計算基底で測定を行うプロセスと、

$$|+\rangle\langle+| \mapsto \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

なるオペレータを作用させるプロセス

研究の目標

直感と一致するような等価関係を定義

既存の等価関係と比較

プロセス計算体系 qCCS [FDY'11] に定義

既存の等価関係：

(Weak) Bisimulation [FDY'11]

(Weak) Open bisimulation [DF'12]

Reduction barbed congruence [DF'12]

qCCS (syntax)

P, Q	$::=$	nil	
		$c?x.P$	古典受信
		$c!x.P$	古典送信
		$P + Q$	非決定的選択
		$P \parallel Q$	並列実行
		if b then P	条件実行
		\vdots	

qCCS (syntax)

	$c?q.P$	量子受信
	$c!q.P$	量子送信
	$\mathcal{E}[\tilde{q}].P$	オペレータ適用
	$M[\tilde{q}; x].P$	量子測定
⋮		

qCCS (semantics)

プロセス全体の状態：コンフィグレーション

プロセス文 P と量子状態 ρ の組 $\langle P, \rho \rangle$

プロセスの実行：

コンフィグレーション間のラベル付き状態遷移

例：

$$\langle c!0.P, \rho \rangle \xrightarrow{c!0} \langle P, \rho \rangle$$

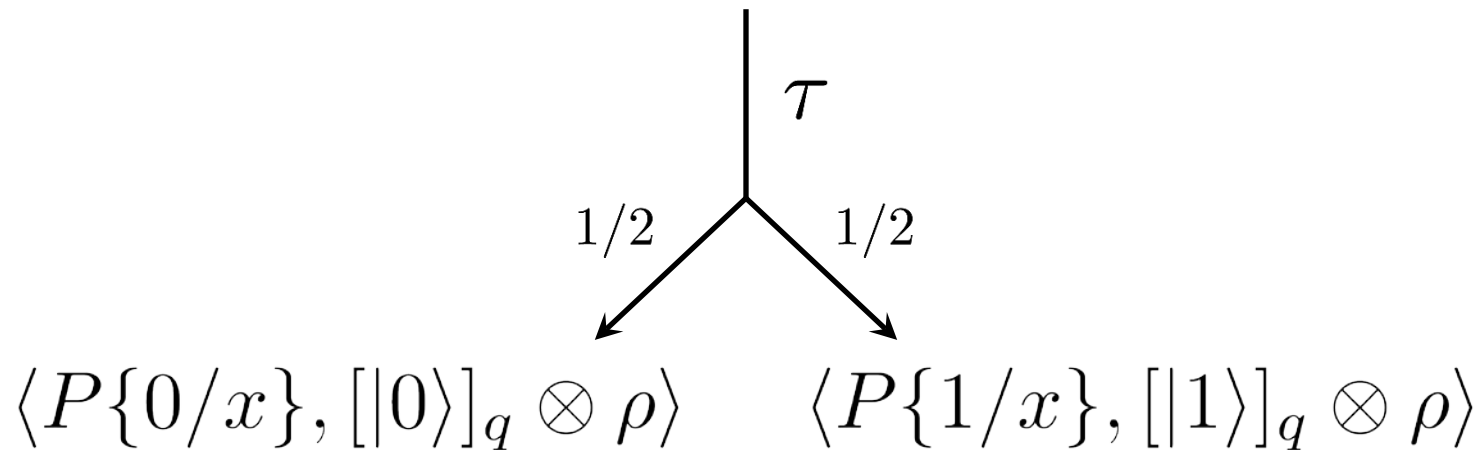
$$\langle X[q].P, [|0\rangle]_q \otimes \rho \rangle \xrightarrow{\tau} \langle P, [|1\rangle]_q \otimes \rho \rangle$$

qCCS (semantics)

量子測定の例

→ コンフィグレーション上の確率分布が得られる

$$\langle M[q; x].P, [|+\rangle]_q \otimes \rho \rangle$$



定義したい等価関係

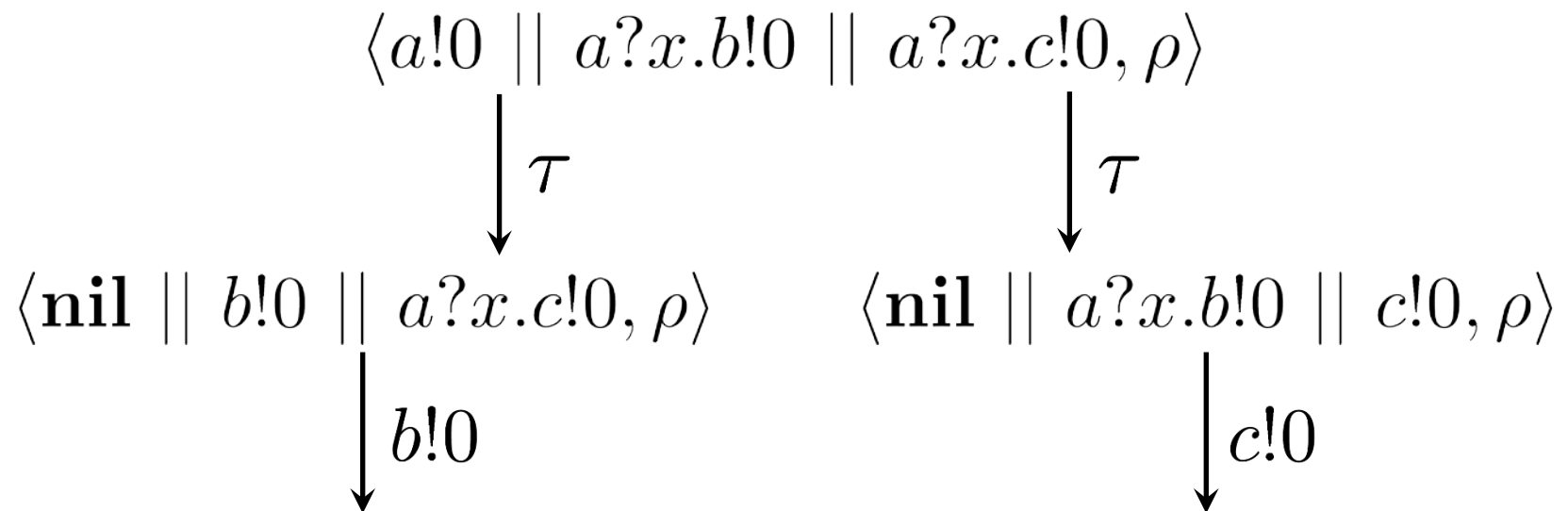
ふたつのプロセスが「等価」とは？

→ プロセスの外（攻撃者）から見て
同じ振る舞いをする事

→ どのような外部者（攻撃者）が存在しても
各チャンネルを等確率で使用する事

非決定的選択と確率

qCCS のプロセスは非決定的選択を伴う

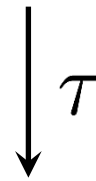


→ チャンネルを使用する確率を
どのように定義すればよいか？

スケジューラ (scheduler)

非決定性を解決し、プロセスの確率分布を与える
コンフィギュレーションを受け取り、次の遷移を返す

$$\langle a!0 \parallel a?x.b!0 \parallel a?x.c!0, \rho \rangle$$



$$\langle \mathbf{nil} \parallel b!0 \parallel a?x.c!0, \rho \rangle$$

$$\langle \mathbf{nil} \parallel a?x.b!0 \parallel c!0, \rho \rangle$$

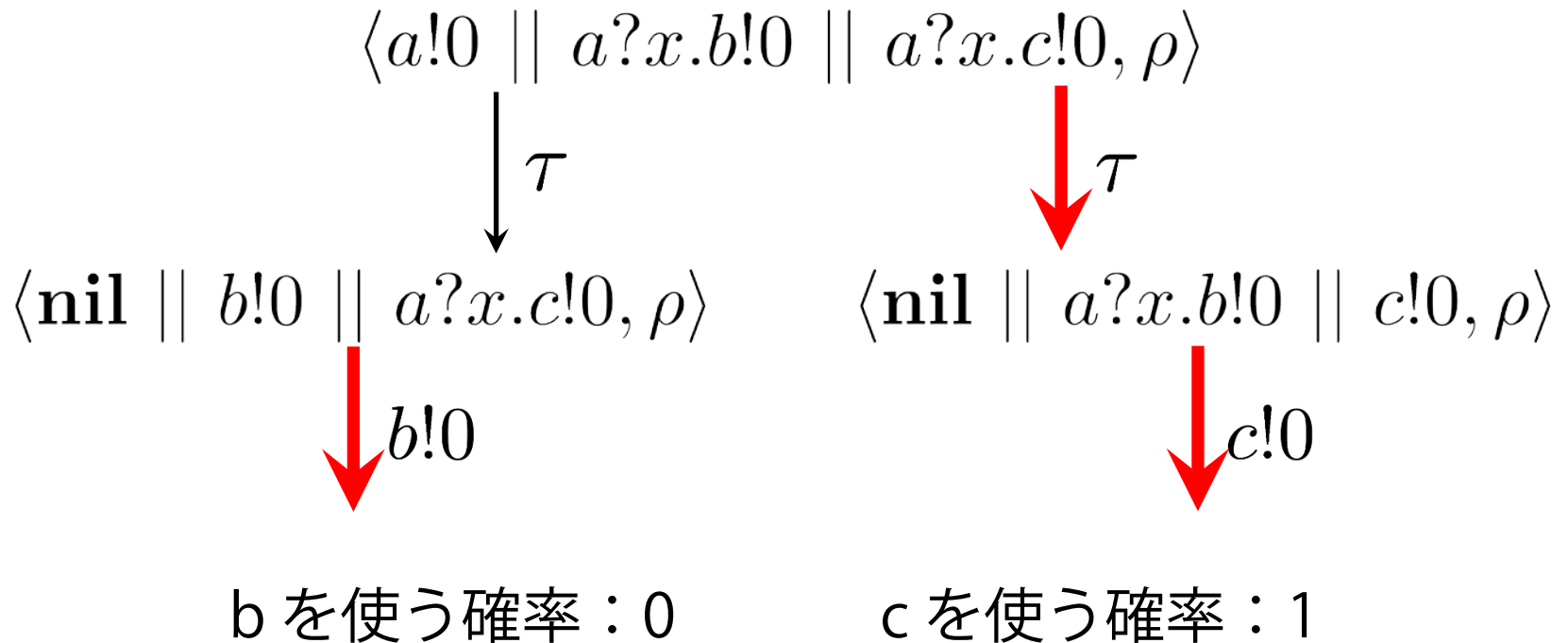


b を使う確率 : 1

c を使う確率 : 0

スケジューラ (scheduler)

非決定性を解決し、プロセスの確率分布を与える
コンフィギュレーションを受け取り、次の遷移を返す



観測同値 (observational equivalence)

$\langle P, \rho \rangle, \langle Q, \sigma \rangle$ が観測同値 ($\langle P, \rho \rangle \approx_{oe} \langle Q, \sigma \rangle$)

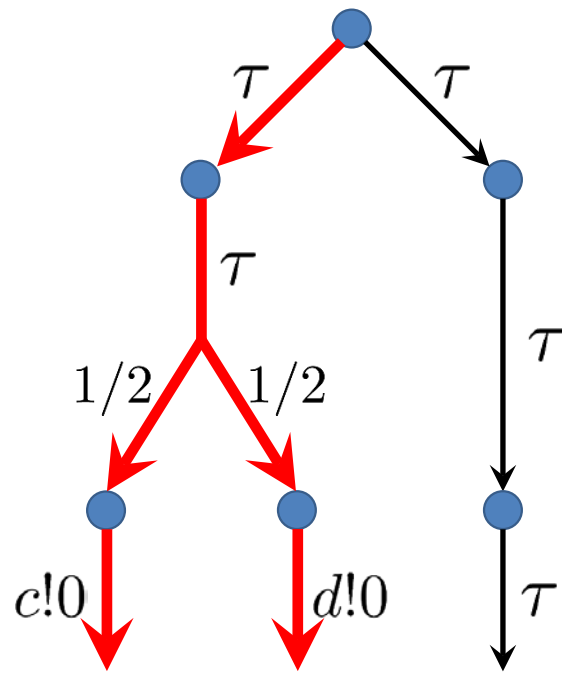
- ⇔ 1. P と Q の外から見える量子状態が等しい
2. 任意のプロセス R , 任意のチャンネル c ,
任意のスケジューラ F について $\langle P || R, \rho \rangle$ が
 F に従い確率 p で c から送信するならば、
あるスケジューラ F' が存在して $\langle Q || R, \sigma \rangle$ も
 F' に従い確率 p で c から送信する
3. (2. の $\langle P, \rho \rangle$ と $\langle Q, \sigma \rangle$ を逆にしたもの)

観測同値 (observational equivalence)

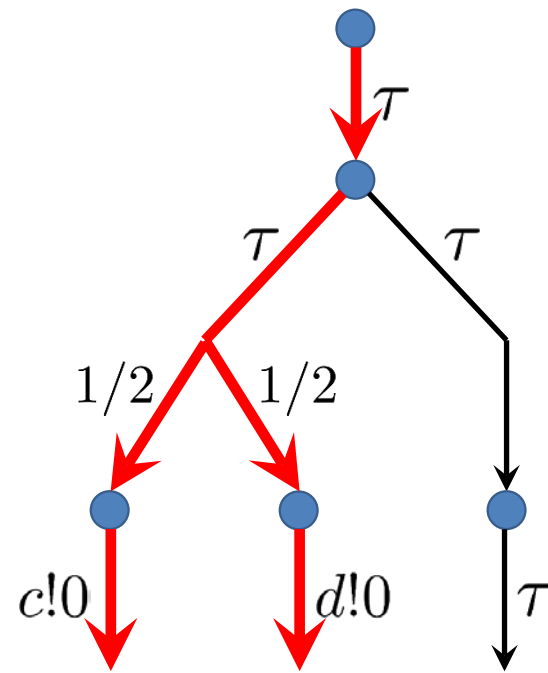
$\langle P, \rho \rangle, \langle Q, \sigma \rangle$ が観測同値 ($\langle P, \rho \rangle \approx_{oe} \langle Q, \sigma \rangle$)

- ⇔ 1. P と Q の外か外部者 (攻撃者) が等しい
2. 任意のプロセス R , 任意のチャンネル c ,
任意のスケジューラ F について $\langle P || R, \rho \rangle$ が
 F に従い確率 p で c から送信するならば、
あるスケジューラ F' が存在して $\langle Q || R, \sigma \rangle$ も
 F' に従い確率 p で c から送信する
3. (2. の $\langle P, \rho \rangle$ と $\langle Q, \sigma \rangle$ を逆にしたもの)

観測同値 (observational equivalence)

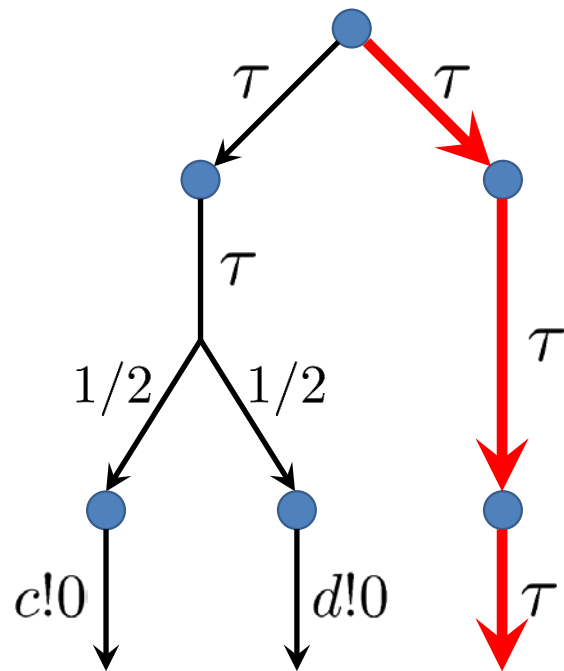


cを使う確率：1/2
dを使う確率：1/2

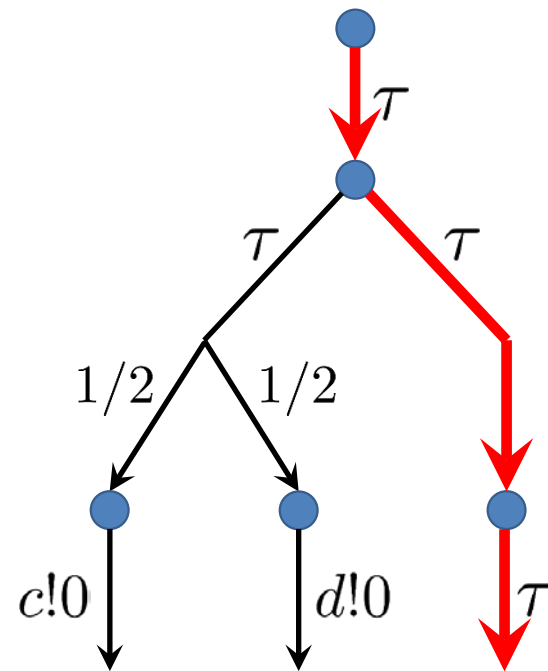


任意のプロセス R をつけて可能 \rightarrow 観測同値

観測同値 (observational equivalence)



チャンネルを使わない



任意のプロセス R をつけて可能 \rightarrow 観測同値

観測同値にならない例

直感的に等価なコンフィギュレーション

$$\langle M[q; x].(c!0 + d!0), [|+\rangle]_q \otimes \rho \rangle$$

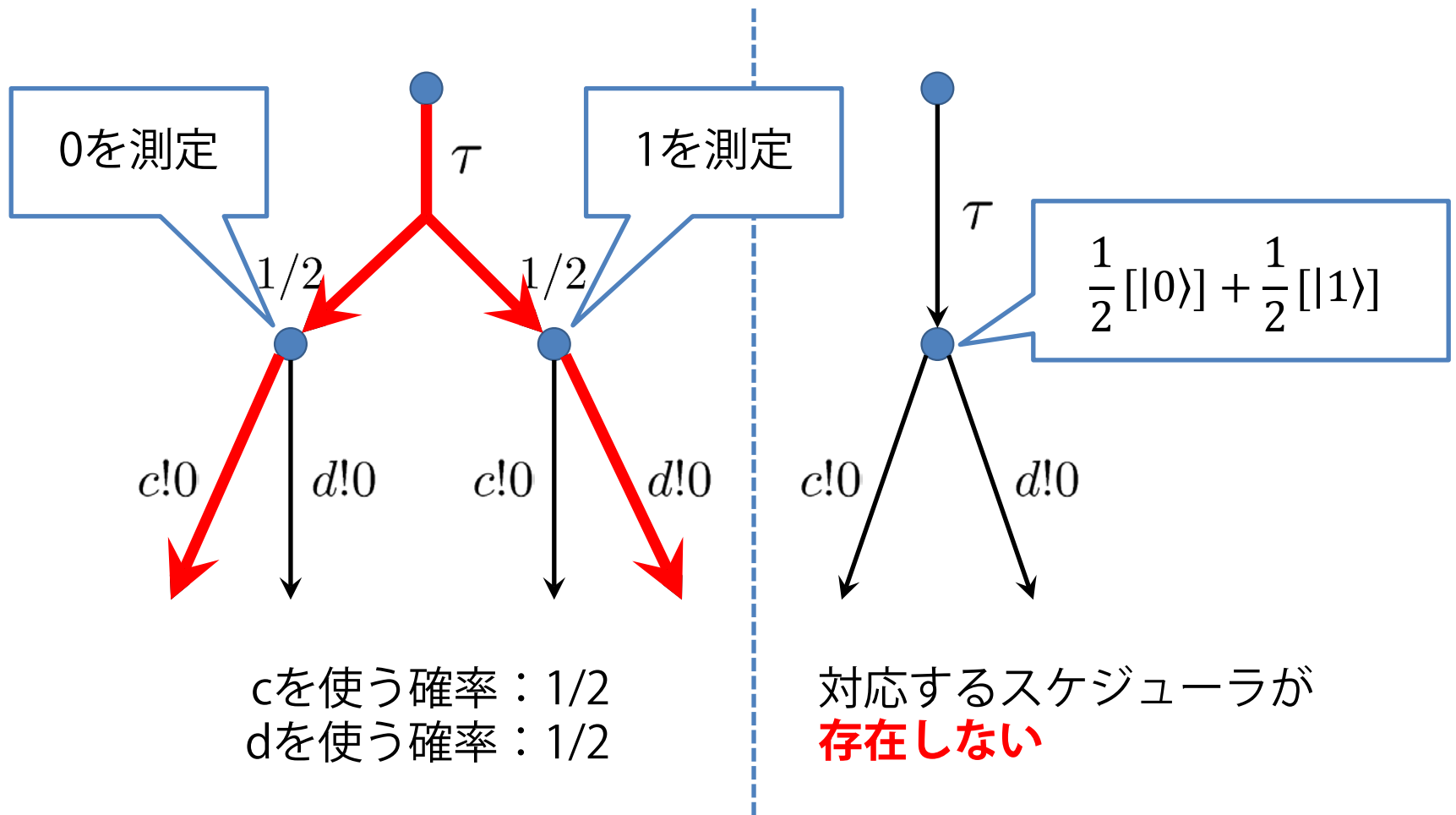
$$\langle \mathcal{E}[q].(c!0 + d!0), [|+\rangle]_q \otimes \rho \rangle$$

M は計算基底での測定

\mathcal{E} は $|+\rangle\langle+| \mapsto \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ なるオペレータ

$$(\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|)$$

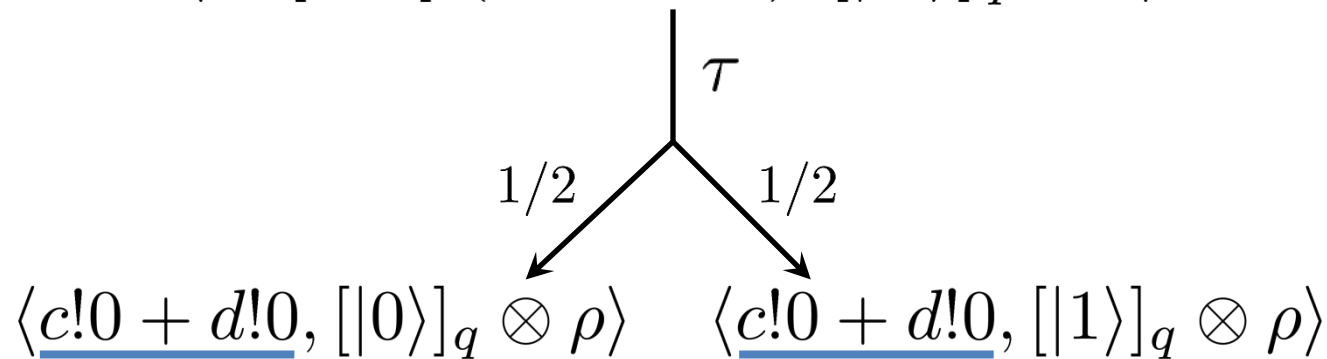
観測同値にならない例



観測同値にならない理由

0を測定した後と1を測定した後で
スケジューラは異なる遷移を選択できてしまう

$$\langle M[q; x].(c!0 + d!0), [|+\rangle]_q \otimes \rho \rangle$$



プロセスは等しいのだから

どちらでも同じ遷移を選ぶべきではないか？

戦略 (strategy)

スケジューラに

「プロセスが等しければ同じ遷移を選ぶ」
という制限を加えたもの

戦略を用いた観測同値

スケジューラの時と同様に観測同値を定義

($\langle P, \rho \rangle \approx_{oe}^{st} \langle Q, \sigma \rangle$ と表記)

$\langle M[q; x].(c!0 + d!0), [|+\rangle]_q \otimes \rho \rangle$ と

$\langle \mathcal{E}[q].(c!0 + d!0), [|+\rangle]_q \otimes \rho \rangle$ は

戦略を用いた観測同値になる

→ この例に関して

直感に近い等価関係を定義することができた

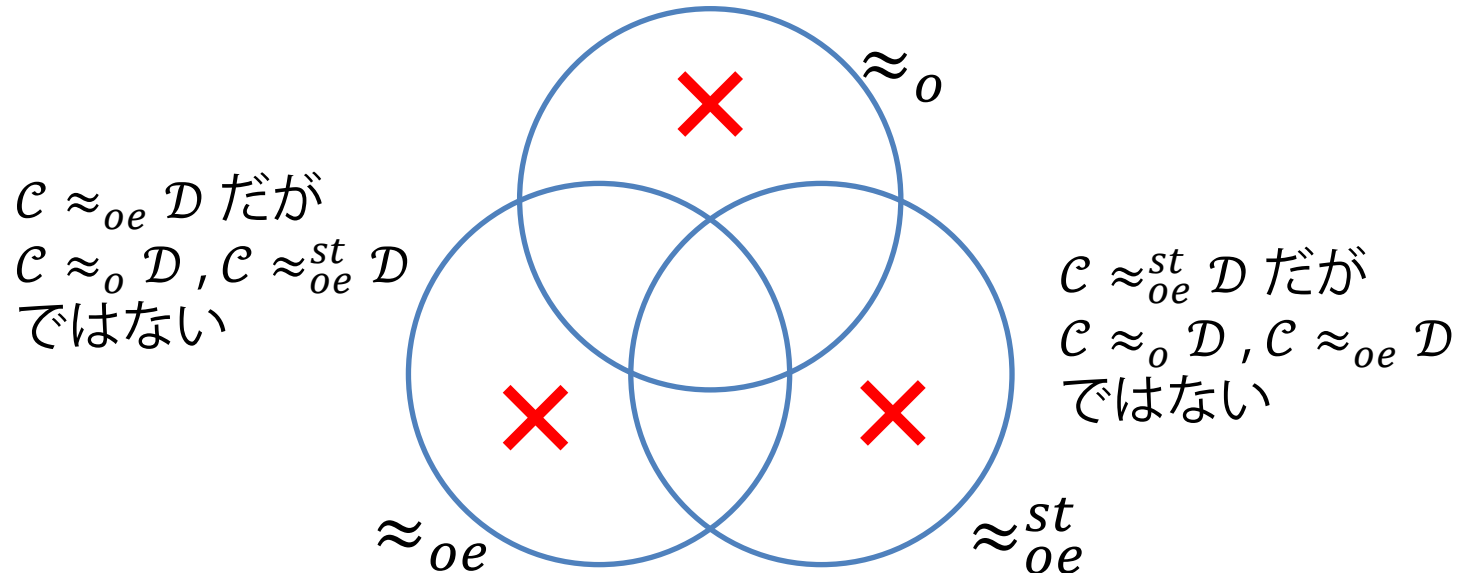
等価関係間の関係

既存の open bisimulation \approx_o と
定義した観測同値 \approx_{oe} , \approx_{oe}^{st} の間の関係は？
 \approx_o は \approx_{oe}^{st} に包含される？

等価関係間の関係

$\approx_o, \approx_{oe}, \approx_{oe}^{st}$ らは互いに包含関係に**ない**

$C \approx_o D$ だが $C \approx_{oe} D, C \approx_{oe}^{st} D$ ではない



どれが一番「直感」に近いのか？

「直感」とは？

区別できない量子状態が存在する

- 確率 $1/2$ で $|0\rangle$ 、確率 $1/2$ で $|1\rangle$
- 確率 $1/2$ で $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 、
確率 $1/2$ で $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

これらを同一視することは自然に行われている
プロセス計算の記述では表現できていない

課題

「直感」の定式化

→ 等価関係の健全性・完全性を示す

観測同値をより直感に近づけるために

「確率 p 以上で送信する」か否かで判断する？

スケジューラにかける制限を変える？

まとめ

qCCS 上に等価関係 観測同値を定義

非決定的選択を解決するためスケジューラを定義

スケジューラに制限を加え戦略とすることで
観測同値をより直感に近いものに

References

Y. Deng and Y. Feng,
“Open bisimulation for quantum processes,”
in *Lecture Notes in Computer Science*, vol. 7604,
pp. 119-133, 2012.

Y. Feng, R. Duan and M. Ying,
“Bisimulation for quantum processes,”
in *Proceedings of the 38th ACM SIGPLAN-SIGACT
Symposium on Principles of Programming Languages*,
pp. 523-534, 2011.