Reversibility in Process Calculi with Nondeterminism and Probabilities

Marco Bernardo and Claudio Antares Mezzina

University of Urbino, Italy

ICTAC2024@Bangkok

Why Reversibility?

Historical Reasons

Landaurer Principle (IBM) 1961

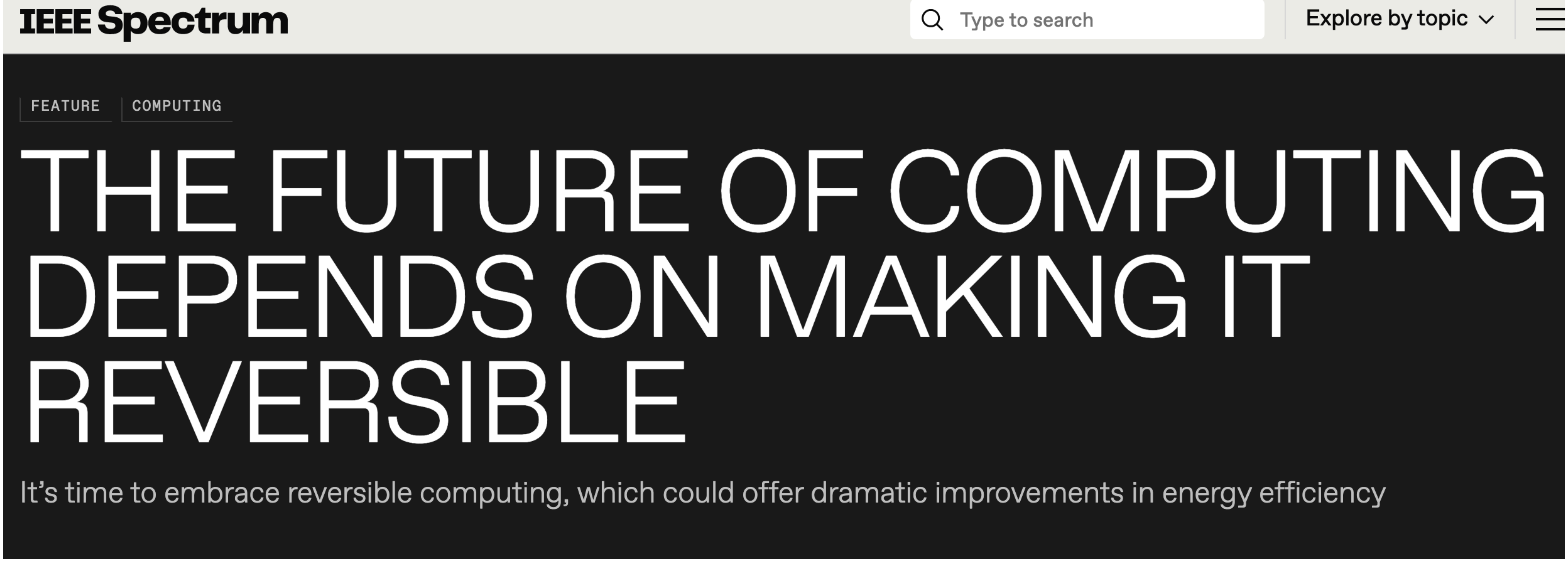
“any logically irreversible manipulation of information, such as the erasure of a bit or the merging of two computation paths, must be accompanied by a corresponding entropy increase in non-information-bearing degrees of freedom of the information-processing apparatus or its environment”

- A so-called logically reversible computation, in which no information is erased, may in principle be carried out without releasing any heat.

- This has led to considerable interest in the study of reversible computing.

Reversible Computation on the hype

https://spectrum.ieee.org/the-future-of-computing-depends-on-making-it-reversible



THE FUTURE OF COMPUTING DEPENDS ON MAKING IT REVERSIBLE

It’s time to embrace reversible computing, which could offer dramatic improvements in energy efficiency

Aside Circuits

Reversibility or reversible behaviour can be found in other fields

- System biology (many biological reactions are reversible)
- Transaction / Checkpoint Rollback Schema / Failure handling primitives
- Reversible Debugging (gdb, undoDB, Mozilla RR)
- Record/Replay (reproducibility of system behaviour)
- Quantum computing

Reversible systems

- In a reversible system one can observe two flows of computation
  - Normal one: computing in a forward way
  - Backward one: undoing the effect of the forward one

Causal Consistent reversibility

- How you can undo a computation?
- In a sequential setting this is straightforward: you start undoing for the last action
- In a concurrent/distributed setting there is no clear definition of last action
  - We can consider as last action any action which has no consequences (e.g., it has not caused anything)
  - Hence an action can be undone provided that its consequences are undone beforehand
  - Essentially any reached state is a state that can be reached just with forward moves
  - This idea is used in transactions/rollback schemas where the system has to get back to a consistent state

Reversibility in Concurrent System

Calculi

Reversible Communicating System (RCCS) Danos&Krivine

- Use of explicit memories to keep track of past events
- Suitable for complex languages (e.g., scales with pi-calculus, Erlang)
- Give the first notion of causally consistent reversibility
- **Won CONCUR23 test of time award**

CCS with communication keys (CCSK) Phillips&Ulidowski

- History information directly recorderded into the term
- Use of keys to keep track of synchronisations
- Suitable for CCS-like languages with LTSs

Example

$$a.P + b.Q \xrightarrow{a} P$$

After the computation, we loose information about

- The performed action a
- The other branch b.Q

CCSK

$$\underbrace{a.P + b.Q}_{\text{No need of extra memories}} \xrightarrow{a[i]} \boxed{a[i]}.P + \boxed{b.Q} \xrightarrow{\underline{a[i]}} a.P + b.Q$$

History information directly in the term

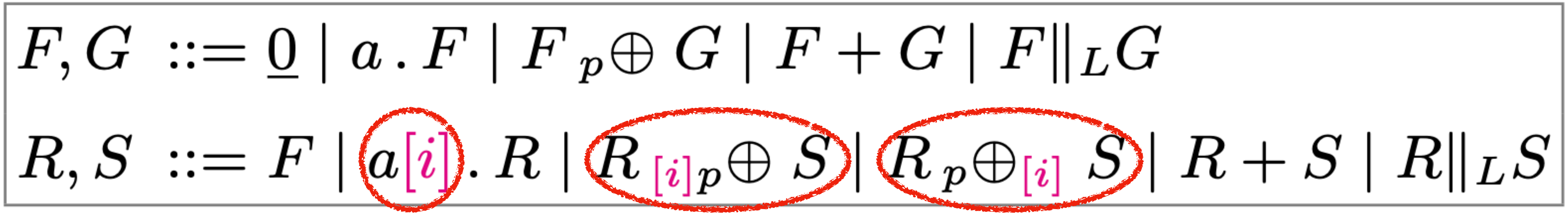
The two reversible CCSs have been shown to be equivalent LMM2021

Problem statement

- How do we adapt reversible process calculi to cope with
  - Nondeterministic choices
  - Probabilistic transitions
- Ensuring causal consistent reversibility

RPPC: reversible probabilistic process calculus

- A simple extension of CCS with probabilistic choice $F\ {}_p\!\oplus\ G$
- Synchronisation à la CSP
- Reversing à la CCSK



$$F, G \ ::= \underline{0} \mid a\,.\,F \mid F\ {}_p\!\oplus\ G \mid F + G \mid F \|_L G$$

$$R, S \ ::= F \mid a[i]\,.\,R \mid R\ {}_{[i]p}\!\oplus\ S \mid R\ {}_p\!\oplus_{[i]}\ S \mid R + S \mid R \|_L S$$

past action prefix

past left/right choice

RPPC - action semantics

$$(\textsc{Act}1)\ \frac{\mathtt{std}(R)}{a\,.\,R \xrightarrow{a[i]}_{\mathtt{a}} a[i]\,.\,R}$$

$$(\textsc{Act}2)\ \frac{R \xrightarrow{b[j]}_{\mathtt{a}} R' \quad j \neq i}{a[i]\,.\,R \xrightarrow{b[j]}_{\mathtt{a}} a[i]\,.\,R'}$$

$$(\textsc{Act}3)\ \frac{R \xrightarrow{b[j]}_{\mathtt{a}} R'}{R\ {}_{[i]p}\!\oplus S \xrightarrow{b[j]}_{\mathtt{a}} R'\ {}_{[i]p}\!\oplus S}$$

$$(\textsc{Cho})\ \frac{R \xrightarrow{a[i]}_{\mathtt{a}} R' \quad \mathtt{npa}(S) \quad S \not\rightarrow_{\mathtt{p}}}{R + S \xrightarrow{a[i]}_{\mathtt{a}} R' + S}$$

no past action

$$(\textsc{Par})\ \frac{R \xrightarrow{a[i]}_{\mathtt{a}} R' \quad a \notin L \quad i \notin \mathtt{key}_{\mathtt{a}}(S) \quad S \not\rightarrow_{\mathtt{p}}}{R \|_L S \xrightarrow{a[i]}_{\mathtt{a}} R' \|_L S}$$

$$(\textsc{Coo})\ \frac{R \xrightarrow{a[i]}_{\mathtt{a}} R' \quad S \xrightarrow{a[i]}_{\mathtt{a}} S' \quad a \in L}{R \|_L S \xrightarrow{a[i]}_{\mathtt{a}} R' \|_L S'}$$

$$(\textsc{Act}1^{\bullet})\ \frac{\mathtt{std}(R)}{a[i]\,.\,R \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} a\,.\,R}$$

$$(\textsc{Act}2^{\bullet})\ \frac{R \overset{b[j]}{\dashrightarrow}_{\mathtt{a}} R' \quad j \neq i}{a[i]\,.\,R \overset{b[j]}{\dashrightarrow}_{\mathtt{a}} a[i]\,.\,R'}$$

$$(\textsc{Act}3^{\bullet})\ \frac{R \overset{b[j]}{\dashrightarrow}_{\mathtt{a}} R'}{R\ {}_{[i]p}\!\oplus S \overset{b[j]}{\dashrightarrow}_{\mathtt{a}} R'\ {}_{[i]p}\!\oplus S}$$

$$(\textsc{Cho}^{\bullet})\ \frac{R \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' \quad \mathtt{npa}(S) \quad S \not\rightarrow_{\mathtt{p}}}{R + S \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' + S}$$

$$(\textsc{Par}^{\bullet})\ \frac{R \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' \quad a \notin L \quad i \notin \mathtt{key}_{\mathtt{a}}(S) \quad S \not\rightarrow_{\mathtt{p}}}{R \|_L S \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' \|_L S}$$

$$(\textsc{Coo}^{\bullet})\ \frac{R \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' \quad S \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} S' \quad a \in L}{R \|_L S \overset{a[i]}{\dashrightarrow}_{\mathtt{a}} R' \|_L S'}$$

RPPC - probabilistic transitions

- We do not impose a strict alternation between nondetermistic processes and probabilistic choices
- Probabilistic choices have to be resolved before nondeterministic one while going forward
- A probabilistic choice cannot
  - resolve a nondeterministic choice or
  - decide who advances in a parallel composition
  - Similar to time determinism in timed-semantics settings

RPPC - probabilistic transitions Snippet

$$(\textsc{PSel1})\ \frac{\mathtt{std}(R) \quad \mathtt{std}(S) \quad R \not\rightarrow_{\mathrm{p}}}{R \,{}_{p}\!\oplus S \xrightarrow{(p)^{[i]}}_{\mathrm{p}} R \,{}_{[i]p}\!\oplus S}$$

$$(\textsc{PSel2})\ \frac{R \xrightarrow{(q)^{[j]}}_{\mathrm{p}} R' \quad \mathtt{std}(R) \qquad \mathtt{std}(S) \quad i \notin \mathtt{key}_{\mathrm{p}}(R')}{R \,{}_{p}\!\oplus S \xrightarrow{(p\cdot q)^{[i]}}_{\mathrm{p}} R' \,{}_{[i]p}\!\oplus S}$$

$$(\textsc{PSel3})\ \frac{R \xrightarrow{(q)^{[j]}}_{\mathrm{p}} R' \quad \neg\mathtt{std}(R) \quad j \neq i}{R \,{}_{[i]p}\!\oplus S \xrightarrow{(q)^{[j]}}_{\mathrm{p}} R' \,{}_{[i]p}\!\oplus S}$$

$$(\textsc{PSel4})\ \frac{R \xrightarrow{(q)^{[j]}}_{\mathrm{p}} R'}{a[i]\,.\,R \xrightarrow{(q)^{[j]}}_{\mathrm{p}} a[i]\,.\,R'}$$

$$(\textsc{PCho1})\ \frac{R \xrightarrow{(p)^{[i]}}_{\mathrm{p}} R' \quad i \notin \mathtt{key}_{\mathrm{p}}(S) \qquad \mathtt{npa}(S) \quad S \not\rightarrow_{\mathrm{p}}}{R + S \xrightarrow{(p)^{[i]}}_{\mathrm{p}} R' + S}$$

$$(\textsc{PCho2})\ \frac{R \xrightarrow{(p)^{[i]}}_{\mathrm{p}} R' \quad S \xrightarrow{(q)^{[i]}}_{\mathrm{p}} S'}{R + S \xrightarrow{(p\cdot q)^{[i]}}_{\mathrm{p}} R' + S'}$$

Prob choice are resolved at once

Probability does not resolve choices

$$(\textsc{PSel1}^{\bullet})\ \frac{\mathtt{std}(R) \quad \mathtt{std}(S) \quad R \not\rightarrow_{\mathrm{p}}}{R \,{}_{[i]p}\!\oplus S \overset{(p)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R \,{}_{p}\!\oplus S}$$

$$(\textsc{PSel2}^{\bullet})\ \frac{R \overset{(q)^{[j]}}{\dashrightarrow}_{\mathrm{p}} R' \quad \mathtt{std}(R') \qquad \mathtt{std}(S) \quad i \notin \mathtt{key}_{\mathrm{p}}(R)}{R \,{}_{[i]p}\!\oplus S \overset{(p\cdot q)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R' \,{}_{p}\!\oplus S}$$

$$(\textsc{PSel3}^{\bullet})\ \frac{R \overset{(q)^{[j]}}{\dashrightarrow}_{\mathrm{p}} R' \quad \neg\mathtt{std}(R') \quad j \neq i}{R \,{}_{[i]p}\!\oplus S \overset{(q)^{[j]}}{\dashrightarrow}_{\mathrm{p}} R' \,{}_{[i]p}\!\oplus S}$$

$$(\textsc{PSel4}^{\bullet})\ \frac{R \overset{(q)^{[j]}}{\dashrightarrow}_{\mathrm{p}} R'}{a[i]\,.\,R \overset{(q)^{[j]}}{\dashrightarrow}_{\mathrm{p}} a[i]\,.\,R'}$$

$$(\textsc{PCho1}^{\bullet})\ \frac{R \overset{(p)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R' \quad i \notin \mathtt{key}_{\mathrm{p}}(S) \qquad \mathtt{npa}(S) \quad S \not\rightarrow_{\mathrm{p}}}{R + S \overset{(p)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R' + S}$$

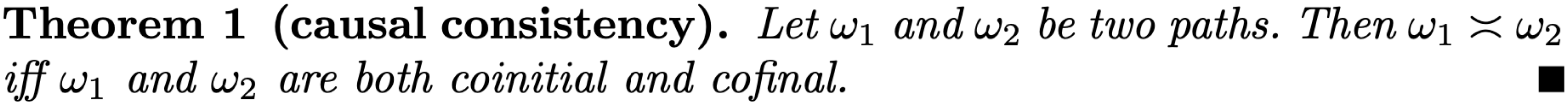
$$(\textsc{PCho2}^{\bullet})\ \frac{R \overset{(p)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R' \quad S \overset{(q)^{[i]}}{\dashrightarrow}_{\mathrm{p}} S'}{R + S \overset{(p\cdot q)^{[i]}}{\dashrightarrow}_{\mathrm{p}} R' + S'}$$

RPPC properties

- Loop lemma: any transition can be undone
- Square property: two independent action can be always swapped
- BTI: backward transitions are independent

Classical proofs

- Challenges into defining causal equivalence $\asymp$
  - probabilistic choices take precedence over nondeterministic ones in the forward direction
  - a swap between two concurrency action transitions is not always possible (unless probabilistic choices have been resolved)
  - Cannot use the axiomatization of Lanese, Phillips & Ulidowski to prove cc



Theorem 1 (causal consistency). *Let ω_1 and ω_2 be two paths. Then $\omega_1 \asymp \omega_2$ iff ω_1 and ω_2 are both coinitial and cofinal.* ■

Application

- We have a language with reversibility and probabilistic choice
- What kind of computing paradigm has these two distinguished characteristics?

Quantum computing

Due to the unitarity of quantum mechanics, quantum circuits are reversible, as long as they do not "collapse" the quantum states on which they operate.

A qubit can be expressed as a superposition of two states

$$\alpha|0\rangle + \beta|1\rangle$$

Indicating that with probability α the qubit is in state 0 and with probability β it is in state 1

Qubit in RPPC

In RPPC we can model a qubit as follows:

$$Q \;=\; m\,.\,(z\,{}_{p}\!\oplus\, o)$$

Where

- m stands for measurement
- p is the probability of being in state 0 (z for 0) and 1-p is the probability of being in state 1 (o for 1)

Qubits

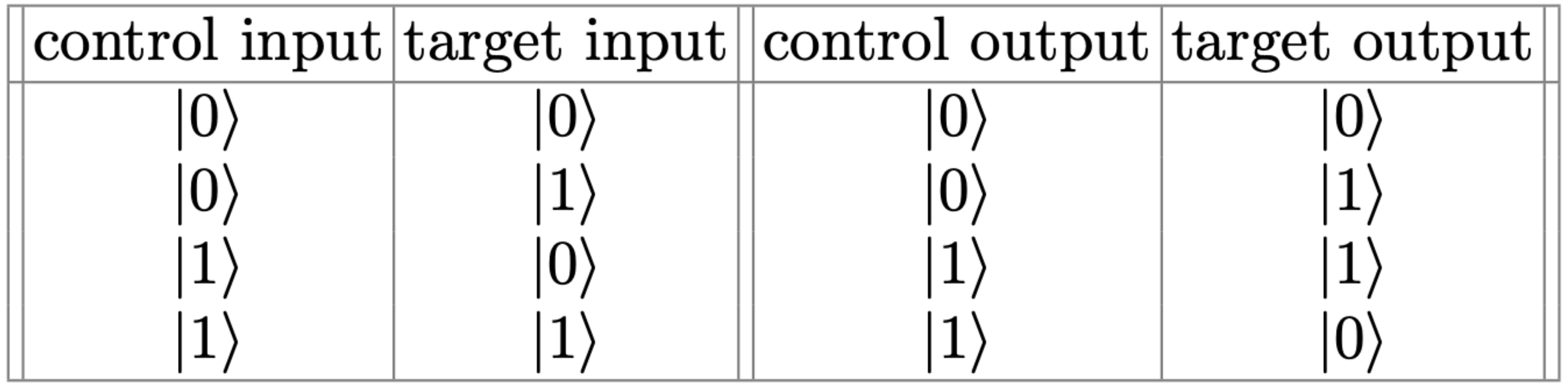
Qubit basis states can also be combined to form product basis states. A set of qubits taken together is called a quantum register.

In RPPC a 2qubit register can be rendered as follows

$$QQ \;=\; m\,.\,(z\,.\,(z\;{}_{q_1}\!\oplus\; o)\;{}_{p}\!\oplus\; o\,.\,(z\;{}_{q_2}\!\oplus\; o))$$

where $p \cdot q_1 = |\alpha|^2$, $p \cdot (1 - q_1) = |\beta|^2$, $(1 - p) \cdot q_2 = |\gamma|^2$, $(1 - p) \cdot (1 - q_2) = |\delta|^2$.

Modelling up a CNOT



control input	target input	control output	target output
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

$$CNOT = m\,.\,(z\,.\,z\,.\,z'.\,z' + z\,.\,o\,.\,z'.\,o' + \mathrm{o}\,.\,z\,.\,o'.\,o' + o\,.\,o\,.\,o'.\,z')$$

$$QQ\|_L CNOT$$

Conclusions

- We have studied causal reversibility of a nondeterministic and probabilistic calculus
- Showed how we can model (and simulate) quantum computing
- We plan to study behavioural equivalences for RPPC
- We plan to study the relation with (Markovian) time-reversibility
- Investigate more relations with quantum
- Model some smart contract scenario with lottery vulnerabilities