The Need for Feasible Non-determinism in Modelling Quantum Protocols

Lorenzo Ceragioli*, Fabio Gadducci†, Giuseppe Lomurno† and Gabriele Tedeschi†
* *IMT School for Advanced Studies Lucca, Italy*
Email: lorenzo.ceragioli@imtlucca.it
† *Department of Computer Science, University of Pisa, Italy*
Emails: fabio.gadducci@unipi.it, giuseppe.lomurno@phd.unipi.it and gabriele.tedeschi@phd.unipi.it

***Abstract*—The development of distributed quantum architectures and protocols calls for adequate specification and verification techniques, which require abstracting and focusing on the basic features of quantum concurrent systems. Process calculi have been one of the successful formalisms for modelling quantum protocols, exploiting non-determinism to represent incomplete knowledge about the specification, unpredictable user behaviour and unknown attacks from malicious protocol participants. However, the way non-determinism is handled in probabilistic systems causes illegal behaviour in quantum systems, since it does not correspond to physically realizable evolutions. More in detail, some steps of a process may implicitly reveal the state of a qubit without performing a measurement, violating a defining constraint of quantum theory. As a result, most of the proposed equivalences among processes fail to adhere to the prescriptions of quantum theory. Recent literature has shown that this problem affects bisimilarities, as well as testing and trace equivalences, and that constraining non-determinism is required for obtaining semantics that are faithful to the physical reality.**

***Index Terms*—quantum systems, behavioural equivalences, feasible choices, physical faithfulness, process calculi.**

I. Specifying and Verifying Quantum Protocols

The recent flourishing development of *quantum computation* and *quantum communication* technologies calls for adequate modelling and verification techniques. While the specification and verification of quantum circuits have been investigated in depth, the solutions put forward for distributed quantum algorithms and protocols received less attention. To exploit the computational power of quantum computers, memories need to be larger than the ones currently available. A promising solution is based on the idea of linking multiple computers via the *Quantum Internet* [1], [2], thus providing quantum algorithms with large enough memories for practical applications. Quantum protocols aim at security and reliability properties of communication, featuring solutions for Quantum Key Distribution (QKD) [3], cryptographic coin tossing [4], secure communication [5], and private information retrieval [6]. These scenarios pose unique challenges, as they require specification and verification techniques handling concurrent execution and non-determinism, which are the focus of our investigation.

This study was carried out within the National Centre on HPC, Big Data and Quantum Computing - SPOKE 10 (Quantum Computing) and received funding from the European Union Next-GenerationEU - National Recovery and Resilience Plan (NRRP) MISSION 4 COMPONENT 2, INVESTMENT N. 1.4 – CUP N. I53C22000690001 and from the European Union through the MSCA SE project QCOMICAL (Grant Agreement ID: 101182520).

A. Specifying Quantum Protocols

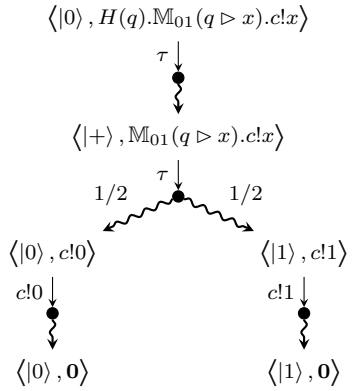
Process calculi have been successfully applied to model classical protocols and concurrent systems, also featuring probabilistic behaviour [7]. Numerous proposals of such calculi have been put forward for modelling quantum protocols and systems (see [8] and the references therein). Their features are comparable: a process P may send over a channel c a classical value v or a qubit name q, with $c!v$ and $c!q$ respectively; it may receive a value and bind it to the variable x with $c?x$; it may perform a unitary transformation U with $U(q)$, or a measurement in a given basis $\mathbb{B}$ with $\mathbb{M}_{\mathbb{B}}(q \triangleright y)$, binding the outcome to the variable y. Processes are then composed sequentially , non-deterministically, or in parallel.

Example 1: The process $P = H(q).\mathbb{M}_{01}(q \triangleright x).c!x$ represents a sequential composition of operations: it first updates a qubit q with the Hadamard unitary, then measures it in the standard bases and finally sends the boolean result over the channel c.

To give semantics to these processes, a quantum memory is needed to specify the current value of the used qubits. For example, the behaviour of P depends on the value $|\psi\rangle$ of the qubit q. The semantics of P with $|\psi\rangle$, that we write $\langle |\psi\rangle , R\rangle$, is a probabilistic Labelled Transition System (pLTS) describing the possible probabilistic evolutions of each state, all represented as pairs $\langle |\phi\rangle , R'\rangle$ composed by a quantum state $|\phi\rangle$ and a process R' representing the classical control. Namely, unitary applications cause silent transitions, called τ, as in $\langle |0\rangle , H(q).P\rangle \xrightarrow{\tau} \langle |+\rangle , P\rangle$, and so do measurements, yielding probability distributions of states according to the Born rule, as in $\langle |0\rangle , \mathbb{M}_{\pm}(q \triangleright x).c!x\rangle \xrightarrow{\tau} \langle |+\rangle , c!0\rangle \ {}_{1/2}\!\oplus \langle |-\rangle , c!1\rangle$. Visible (non-$\tau$) labels are used to encode communications with whom the process evolves: a sending process evolves as in $\langle |\psi\rangle , c!v.P\rangle \xrightarrow{c!v} \langle |\psi\rangle , P\rangle$ and a receiving process as in $\langle |\psi\rangle , c?x.Q\rangle \xrightarrow{c?v} \langle |\psi\rangle , Q[{}^{v}/_{x}]\rangle$ where $Q[{}^{q'}/_{v}]$ is the process obtained by substituting in Q all the occurrences of x with v. When two processes are composed in parallel, they can synchronize yielding a τ-labelled transition, as in $\langle |\psi\rangle , c!v \parallel c?x.a!x\rangle \xrightarrow{\tau} \langle |\psi\rangle , a!v\rangle$. Non-determinism is modelled by allowing $\langle |\psi\rangle , P + Q\rangle$ to replicate the moves of both $\langle |\psi\rangle , P\rangle$ and $\langle |\psi\rangle , Q\rangle$.

Example 2: The semantics of $\langle |0\rangle , P\rangle$ is given by the following pLTS, where the straight arrows model labelled

actions and the squiggly ones represent the elements of a distribution, labelled by their probability (we omit 1).



B. Verification Objectives and Techniques

Quantum process calculi are in fact a powerful and expressive specification formalism, and once the implementation of a quantum protocol is modelled as a pLTS, different verification techniques can be employed. We consider the simple case of checking equivalences between different implementations (or possibly an implementation and a more abstract specification encoding the desired behaviour), such as:

- *bisimilarity*, which requires both the branching structure and the labels of two systems to coincide;
- *trace equivalence*, which ignores the branching structure and checks that the labelled traces of the system at hand are included in a set of desired behaviours;
- *testing equivalence*, which focuses on τ-transitions and requires that the two systems are indistinguishable for any external observer that runs tests on them.

For checking security properties, the behaviour of the system is often investigated when combined with an attacker capable of interacting with the protocols according to some predefined attacker model, like the one proposed by Dolev and Yao [9].

II. The Need for Non-determinism

In protocol verification, one has to deal with probabilistic or non-deterministic behaviours, where the next state of the system is not uniquely determined and the computation branches into alternative paths. If a *deterministic* system is in state x at time t_0, then at time t_1 it will be in a unique state y. A *probabilistic* system, instead, at time t_1 could be in a unique probability distribution Δ of states. Finally, *non-deterministic probabilistic* systems, may evolve into multiple possible distributions of states $\{\Delta, \Theta, \Gamma, \ldots\}$.

This behaviour arises from unknown information at modelling time, such as:

- *User Input:* When modelling a protocol, no assumption can be made on the user behaviour. Whenever the execution depends on user inputs, we shall consider all the possible branches. A simple example is the Superdense Coding Protocol [10], where the user can freely decide which pair of bits to send to the receiver by encoding it into a qubit value. Similar user choices also appear in several quantum protocols, like quantum secure communication [5] and blind computation [11].
- *Incomplete Specification:* A good specification shall abstract away from implementation details. Consider for example a set of quantum computers serving requests for quantum computations received over the Internet: the process managing such requests may decide which computer to use for each computation according to different policies (round-robin, fair probability distributions etc), but the specification can abstract away from such implementation details by just assuming that it chooses according to an unknown strategy, i.e. non-deterministically.
- *Concurrency:* The behaviour of parallel threads in a computer or of agents in a protocol is often difficult to predict due to race conditions. Race conditions are even more critical in the quantum setting: due to entanglement, the action of an agent can influence the behaviour of others even without an explicit interaction. Parallel execution of agents is interpreted as a non-deterministic choice between all their possible interleaving, since we have no way to predict in which order agents will act.
- *Cryptographic Attackers:* Most quantum communication protocols are cryptographic in nature, and verifying their correctness means accounting for the multiple strategies of an attacker. For example, non-determinism allows considering all the possible moves of the eavesdropper Eve when modelling the BB84 QKD protocol.

Non-deterministic behaviour ultimately arises from a lack of knowledge about the system details (intentionally abstracted away) or from unpredictable human behaviour. To a Physics-minded person, it may seem legit to model it as a probability distribution on the possible choices of our system, thus reducing non-determinism to probabilistic branching and obtaining a deterministic stochastic system. Roughly, this requires assuming a probability for every non-deterministic move. While tempting, this is incorrect in a Computer Science setting, where we want instead to quantify all possible choices.

To prove the point, we devise an example inspired by [12]. Consider an architecture where a hash map is used for deciding which server to forward a request received over the Internet. If the hash is computed over some value of the received queries, an attacker can forge requests so that all of them arrive at the same server, causing congestion and thus a possible denial-of-service. Assuming that the received queries follow a given probability distribution is not sound for assessing the security of the implementation, since the attacker can choose the most effective strategy no matter how improbable it is.

In general, probabilistic branching characterizes the probable and improbable computations: while in some cases it could suffice to verify that the probable executions are secure, sometimes this is not enough, and we need non-deterministic branching in order to consider all the possible computations, including those in which non-determinism favours the attacker.

III. Unfeasible Non-deterministic Behaviour

The model of choice for quantum protocols are pLTSs, which encode both non-deterministic branching (as discussed above) and probabilistic branching (due to quantum measurements). The standard way of modelling the interplay of these different kinds of branching is to assume they are independent. However, recent works have shown that this causes a mismatch with respect to physical reality in modelling quantum systems [8]. In order to note this mismatch, it suffices to consider the specification of simple physical processes.

A. A Simple Example of Unfeasible Move

For example, consider the following processes S_{01} and $S_{\pm}$ encoding sources sending fair distributions of qubits in $|0\rangle$ or $|1\rangle$, and in $|+\rangle$ or $|-\rangle$, respectively.

$$S_{01} = \left\langle |+\rangle, \mathbb{M}_{01}(q \rhd x).c!q \right\rangle,\ S_{\pm} = \left\langle |0\rangle, \mathbb{M}_{\pm}(q \rhd x).c!q \right\rangle$$

Note that, after their measurements, the systems evolve with equal probability in processes sending a qubit in state $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Assume that these sources run in parallel with some observer process O that receives the qubit and chooses non-deterministically which measurement to perform between $\mathbb{M}_{01}$ and $\mathbb{M}_{\pm i}$: The former tells apart $|0\rangle$ from $|1\rangle$ and equates $|+\rangle$ and $|-\rangle$, the latter equates all of them.

$$O = c?x.(O_{01} + O_{\pm i})$$
$$O_{01} = \mathbb{M}_{01}(x \rhd y).d!y \qquad O_{\pm i} = \mathbb{M}_{\pm i}(x \rhd y).d!y$$

Figure 1 presents the evolution of the two sources and of the observer. The presence of non-determinism implies that we are abstracting away from an unknown scheduler, which has the job of deciding which measurement the observer will perform, i.e., which straight arrow to choose, either the red or blue ones. The former corresponds to performing $\mathbb{M}_{01}$ and the latter $\mathbb{M}_{\pm i}$.

Take the system on the left. If the measurement is chosen according to the value of the received qubit, the observer can perform $\mathbb{M}_{01}$ when receiving $|0\rangle$ and $\mathbb{M}_{\pm i}$ otherwise, thus reaching the state $d!0$ with probability $3/4$. This move is based on the state of the received qubit, yet without performing a measurement. Thus, unconstrained non-deterministic choices contradict a defining feature of quantum theory: the state of a quantum system cannot be observed without altering it.

The physical constraints of quantum theory limit the capability of discerning the behaviour of quantum systems. Indeed, the two sources S_{01} and $S_{\pm}$ are deemed indistinguishable, as the qubits states are represented by the same density operator

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\mathbb{I} = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|.$$

On the contrary, the two sources are distinguished by the observer O. The process on the right cannot match the behaviour of the left one, because it cannot reach $d!1$ with probability $3/4$. However, this distinction is spurious: the non-deterministic choice performed by O in the left process depends on some knowledge that the scheduler cannot have, and it implicitly reveals the state vector of the received qubit. This counterexample proves that the standard approach for pLTSs cannot be used to faithfully model quantum protocols.

B. The Impact on Quantum Protocols Verification

The example above shows that unconstrained non-determinism allows for physically unrealizable moves that violate the prescriptions of quantum theory. The same approach can be used to show that non-determinism allows two actors, named Alice and Bob, to communicate a classical bit at a superluminal speed by exploiting quantum entanglement. Assume that Alice and Bob have each a qubit of an entangled pair in state $|\Phi^+\rangle$, and that they move apart agreeing that at some fixed time, Alice will perform a measurement on one of two possible bases and Bob will try to guess the basis. If there is a strategy for correctly guessing the basis, the classical bit of information would be instantly communicated, regardless of distance, thus modelling a physically impossible superluminal communication. Since the guess is arbitrary, it is reasonable to model it as a non-deterministic choice. The procedure is as follows: Alice chooses either $\mathbb{B}_{01}$ or $\mathbb{B}_{\pm}$, i.e. she realizes either the process $A_0 = \mathbb{M}_{01}(q_A \rhd x)$ or $A_1 = \mathbb{M}_{\pm}(q_A \rhd x)$. The system is thus modelled as $\left\langle |\Phi^+\rangle, A \parallel B \right\rangle$ where $A \in \{A_0, A_1\}$ and B is the process of Bob. By allowing Bob to choose between two measurements to perform on his qubit (e.g. in $\mathbb{B}_{01}$ or $\mathbb{B}_{\pm i}$), and by assuming unconstrained non-determinism, we recover a result similar to the one of Figure 1. Bob can discriminate between the two versions of Alice, thus decoding the classical bit without any real communication.

As shown in [8], the same kind of problems occurs when verifying real-world protocols, like BB84 QKD, quantum coin tossing protocol, quantum teleportation, and superdense coding. The impact on the analysis of the quantum coin tossing protocol is particularly interesting. According to unconstrained non-determinism, the user who does not start the communication (say Bob) can trick the other one (say Alice) and always win the toss. This is because Bob can exploit non-determinism to reveal the state of the qubits sent by Alice, with a technique similar to the one of Figure 1. A closer inspection based on constrained non-determinism reveals that in reality it is Alice, who starts the protocol, who can actually cheat by using entangled qubits. Therefore, the result of the analysis performed with the standard probabilistic approach is diametrically opposed to that of one considering physically feasible moves only (and it is opposed to reality too).

Non-determinism is essential for modelling protocols and their implementations, thus we cannot ignore it. In a nutshell, we need to constrain non-determinism for recovering the desired indistinguishability prescribed by quantum theory.

C. Constraining Non-determinism

Characterizing feasible choices is a general problem arising in modelling protocols. A common solution relies on schedulers for explicitly representing choices and restricting them to a desired "admissible" set of legal moves [13], [14]. For example, in security applications, partial information schedulers are used to model secrecy in protocols dependent on private information, like a password, by requiring that two instances of the same protocol differing only for the

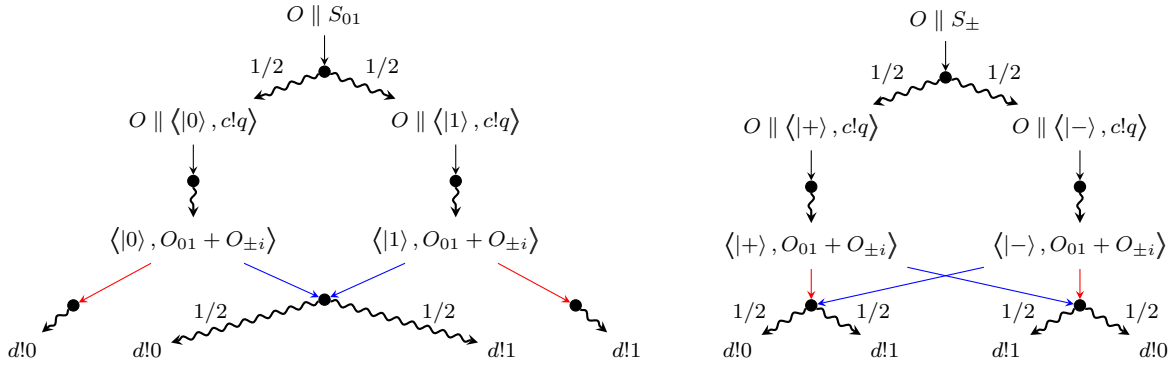


Fig. 1: Observer in parallel with indistinguishable qubit sources, with all transitions implicitly labelled by τ.

private information should behave the same. As argued in the previous section, preventing visibility is even more critical when modelling quantum systems, as the physical laws forbid some specific moves. For quantum protocols, the quantum state is inherently private until a measurement is performed and hence a classical outcome is obtained. More precisely, an admissible scheduler must perform choices that do not depend on quantum values. Consider the processes in Figure 1. As argued before, an arbitrary scheduler can choose between the measurements $\mathbb{M}_{01}$ or $\mathbb{M}_{\pm}$ according to the unknown value of the received qubit. However, since no measurement has been performed, there is no classical value to base the scheduling upon, and such schedulers should be considered inadmissible.

Simple constrained schedulers that resolve non-determinism according to classical values only are proposed in [15], which match the indistinguishability results of quantum theory. This solution rules out all the problematic moves presented above, since they cannot be replicated by admissible schedulers. In essence, the approach proposed in [15] requires tagging the possible non-deterministic choices, and avoiding schedulers which mix-and-match them. Looking back at Figure 1, the observer O can perform a non-deterministic choice, and we keep track of the selection they made. Either O performs the measurement $\mathbb{M}_{01}$, visually represented by the two outermost red transitions; or they perform the measurement $\mathbb{M}_{\pm}$, visually represented by the two innermost blue transitions. In both cases, the probability of reaching $d!0$ is $1/2$, and the same for $d!1$. If we restrict ourselves to these cases , the system on the right can replicate the same behaviour of the one on the left, thus the two processes are correctly equated, as prescribed by quantum theory.

IV. Conclusions

Quantum protocols are characterized by the interplay of parallelism, non-determinism and probabilities, and thus they require ad hoc modelling and verification techniques different from the ones used for quantum circuits. Process calculi are a promising approach that succeeds in specifying quantum-capable agents and their composition, and offers a suitable semantic model via pLTSs.

Non-determinism is required for modelling concurrency, user input, abstract specifications and unknown malicious attackers. However, the standard approach of combining non-determinism with the probabilities arising from quantum measurements turns out to be problematic, allowing for moves that are not physically reasonable. Unconstrained non-determinism allows processes to act based on unknown quantum values, implicitly revealing them. This causes the standard equivalence relations over pLTSs to fail in adhering to the prescriptions of quantum theory. In particular, they are shown to discriminate indistinguishable states like the random sources in Figure 1. We argue that, under very natural and mild assumptions, any sensible specification and verification framework for quantum protocols will encounter this problematic interplay between quantum values, probabilities and non-determinism. A solution [15] involves characterizing the admissible schedulers, i.e. those that act based on classical information only.

These considerations pertain to the semantics of quantum protocols, and thus they have consequences for a wide range of verification techniques. We have argued here and shown in a series of papers that the aforementioned issue affects various forms of *equivalence checking*: saturated [8] and labelled bisimilarity [15], testing equivalence [16], and trace equivalence [17]. They all require non-determinism to be constrained to recover physical faithfulness. This suggests that the problem spans the whole range of the linear time-branching time spectrum [18]. Moreover, since the problem is mostly caused by a modelling issue, it is reasonable to assume even more verification techniques to be affected, like testing preorder and temporal logic model checking.

References

[1] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, "Quantum Internet: From communication to distributed computing!" in *NANOCOM 2018*, J. A. Benediktsson and F. Dressler, Eds. ACM, 2018, pp. 3:1–3:4.

[2] P. Zhang, N. Chen, S. Shen, S. Wu, and N. Kumar, "Future quantum communications and networking: A review and vision," *IEEE Wireless Communications*, vol. 31, no. 1, pp. 141–148, 2024.

[3] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," in *ICWT 2018*. IEEE, 2018, pp. 1–5.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.

[5] G.-L. Long, F.-G. Deng, C. Wang, X.-H. Li, K. Wen, and W.-Y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251–272, 2007.

[6] F. Gao, S. Qin, W. Huang, and Q. Wen, "Quantum private query: A new kind of practical quantum cryptographic protocol," *Science China Physics, Mechanics & Astronomy*, vol. 62, no. 7, p. 70301, 2019.

[7] M. Hennessy, "Exploring probabilistic bisimulations, part I," *Formal Aspects of Computing*, vol. 24, no. 4-6, pp. 749–768, 2012.

[8] L. Ceragioli, F. Gadducci, G. Lomurno, and G. Tedeschi, "Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers," *Proceedings of the ACM on Programming Languages*, vol. 8, no. POPL, pp. 43:1269–43:1297, 2024.

[9] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[10] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[11] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, "Efficient universal blind quantum computation," *Physical Review Letters*, vol. 111, no. 23, p. 230501, 2013.

[12] S. A. Crosby and D. S. Wallach, "Denial of service via algorithmic complexity attacks," in *USENIX Security Symposium 2003*. USENIX Association, 2003.

[13] K. Chatzikokolakis and C. Palamidessi, "Making random choices invisible to the scheduler," in *CONCUR 2007*, ser. LNCS, L. Caires and V. T. Vasconcelos, Eds., vol. 4703. Springer, 2007, pp. 42–58.

[14] K. Chatzikokolakis, G. Norman, and D. Parker, "Bisimulation for demonic schedulers," in *FOSSACS 2009*, ser. LNCS, L. de Alfaro, Ed., vol. 5504. Springer, 2009, pp. 318–332.

[15] L. Ceragioli, F. Gadducci, G. Lomurno, and G. Tedeschi, "Quantum bisimilarity is a congruence under physically admissible schedulers," in *APLAS 2024*, ser. LNCS, O. Kiselyov, Ed., vol. 15194. Springer, 2025, pp. 176–195.

[16] ——, "Testing quantum processes," in *ISoLA 2024*, ser. LNCS, T. Margaria and B. Steffen, Eds., vol. 15219. Springer, 2024, pp. 132–151.

[17] L. Ceragioli, G. Lomurno, and G. Tedeschi, "Reconciling quantum theory and process equivalence via physically admissible schedulers," in *Recent Trends in Algebraic Development Techniques - 27th IFIP WG 1.3 International Workshop, WADT 2024, Enschede, The Netherlands, July 8, 2024, Revised Selected Papers*, ser. Lecture Notes in Computer Science, I. Tutu, Ed., vol. 15587. Springer, 2024, pp. 111–133. [Online]. Available: https://doi.org/10.1007/978-3-031-88930-1_6

[18] R. J. Van Glabbeek, "The linear time-branching time spectrum I. The semantics of concrete, sequential processes," in *Handbook of Process Algebra*, J. A. Bergstra, A. Ponse, and S. A. Smolka, Eds. Elsevier, 2001, pp. 3–99.