Effect Semantics for Quantum Process Calculi — Summary

Lorenzo Ceragioli
IMT School for Advanced Studies, Lucca, Italy
lorenzo.ceragioli@imtlucca.it

Fabio Gadducci
University of Pisa, Pisa, Italy
fabio.gadducci@unipi.it

Giuseppe Lomurno
University of Pisa, Pisa, Italy
giuseppe.lomurno@phd.unipi.it

Gabriele Tedeschi
University of Pisa, Pisa, Italy
gabriele.tedeschi@phd.unipi.it

Recent years have seen a flourishing development of quantum technologies for computer science, in the form of *quantum computation* and *quantum communication*. Both of them exploit quantum phenomena like superposition and entanglement: the former is interested in harvesting the (supposedly) higher computational power of quantum computers, while the latter strives to achieve secure and reliable communication, featuring solutions for key distribution [22], cryptographic coin tossing [1], direct communication [20], and private information retrieval [10]. Protocols like BB84 QKD [1] are *unconditionally secure* [21], meaning that they are protected against all physically possible attackers. Quantum communication also promises to allow linking multiple computers via the *Quantum Internet* [2, 26], therefore providing quantum algorithms with large enough memories for practical applications.

Despite the rich theory and the potential applications, there is no accepted standard to model and verify quantum concurrent systems and protocols. Numerous works [18, 11, 8, 25, 3] rely on *quantum process calculi*, an algebraic formalism that has been successfully applied to classical protocols and concurrent systems. Their semantics is given by means of a *labelled transition system* (LTS) $(S, Act, \rightarrow)$: the relation $\rightarrow \subseteq S \times Act \times S$ specifies how a classical state $s \in S$ (representing a process) may evolve performing an action $\alpha \in Act$. The standard equivalence for such LTSs is *bisimilarity*: we say that two states are bisimilar when they express the same visible attributes, and after one step they evolve in bisimilar states. Crucially, bisimilarity allows us to abstract away from the implementation details of two systems, and focus only on the observable, interactive behaviour they offer to an external environment.

There have been several attempts [17, 4, 6, 5, 3] to adapt existing techniques to the quantum setting, mainly in terms of *probabilistic* LTSs (pLTSs) $(Conf, Act, \rightarrow)$: $Conf = S \times \mathscr{H}$ is a set of *configurations* composed by a classical state $s \in S$ and a quantum state $|\psi\rangle \in \mathscr{H}$, and $\rightarrow \subseteq Conf \times Act \times \mathscr{D}(Conf)$ with $\mathscr{D}(Conf)$ probability distributions of configurations. This approach led to a plethora of different bisimilarities, yet most of them are unsatisfactory since they spuriously distinguish processes that are deemed indistinguishable by the prescriptions of quantum theory [4, 16, 9]. Moreover, assessing bisimilarity of processes requires comparing infinitely many LTSs (one for each possible quantum state). Indeed, algorithmic verification is still missing. In [3], the root of these problems is identified in the peculiarities of the semantic model described above, a non-deterministic pLTS made of quantum states and processes.

We introduce a novel semantic model for non-deterministic quantum protocols, exploiting effect distributions and effect transition systems. Effects are the simplest kind of measurements, i.e. yes-no tests over quantum systems defined as $\mathscr{E}\!f_d = \{ E \in \mathbb{C}^{d\times d} \mid 0_d \sqsubseteq E \sqsubseteq \mathbb{I}_d \}$, where d is the dimension of $\mathscr{H}$, $\mathbb{I}_d$ is the identity matrix and $\sqsubseteq$ is the *Löwner order* ($A \sqsubseteq B$ whenever $B - A$ is positive). We introduce effect distributions, i.e. functions associating each element of a given set X with some d-dimensional effect.

Definition 1. *Given a set X, the set of d*-dimensional finite effect (sub)distributions *over X is*

$$\mathscr{Q}_d X = \{ \mathfrak{D} \in \mathscr{E}\!f_d{}^X \mid \operatorname{supp}(\mathfrak{D}) \textit{ is finite, } \textstyle\sum_{x \in \operatorname{supp}(\mathfrak{D})} \mathfrak{D}(x) \sqsubseteq I_d \}$$

Submitted to:
QPL 2024

where $supp(\mathfrak{D})$ *is the set* $\{x \in X \mid \mathfrak{D}(x) \neq 0_d\}$.

Effect distributions are finite non-normalized POVMs [12] and they generalize probability distributions: $\mathscr{Q}_1 X$ coincides with the usual set of (sub-)probability distributions $\mathscr{D}X$.

In general, effects can be regarded as functions from density operators to probabilities, thus an effect distribution $\mathfrak{D} \in \mathscr{Q}_d X$ denotes a function $\mathfrak{D}{\downarrow_{\_}} \in (\mathscr{D}X)^{DM_d}$ associating any $\rho \in DM_d$ with the probability distribution $\mathfrak{D}{\downarrow_\rho}$ such that $\mathfrak{D}{\downarrow_\rho}(x) = tr(\mathfrak{D}(x) \cdot \rho)$ for any $x \in X$.

Theorem 1. *Effect distributions correspond to all and only the parameterized sub-probability distributions that are convex and have an "overall" finite support.*

$$\mathscr{Q}_d \cong \left\{ \mathfrak{D}{\downarrow_{\_}} \in (\mathscr{D}(X))^{DM_d} \,\middle|\, \mathfrak{D}{\downarrow_{\rho\,{}_p\!\oplus\sigma}} = (\mathfrak{D}{\downarrow_\rho})\,{}_p\!\oplus(\mathfrak{D}{\downarrow_\sigma}),\ \textit{and}\ \bigcup_{\rho \in DM_d} \mathrm{supp}(\mathfrak{D}{\downarrow_\rho})\ \textit{is finite} \right\}$$

As for probability distributions, we compose multiple effect distributions in an effect-weighted sum, writing $\sum_{i \in I} E_i \otimes \mathfrak{D}_i$ for a distribution such that $(\sum_{i \in I} E_i \otimes \mathfrak{D}_i)(x) = \sum_{i \in I} E_i \otimes \mathfrak{D}_i(x)$, when $\sum_i E_i \sqsubseteq \mathbb{I}$. Intuitively, $\mathfrak{D}$ measures a portion of the quantum state to choose between the distributions $\mathfrak{D}_i$, which in turn behave accordingly to the remaining quantum state.

One could be tempted to use the binary composition $\Delta\,{}_E\!\oplus \Theta$, defined as $E \otimes \Delta + (\mathbb{I} - E) \otimes \Theta$, as it is common in the probabilistic case. We show that this is not a safe simplification for finite effect distributions, as some (finite support) effect distributions cannot be defined using the binary operator only. Roughly, the proof is based on the fact that some effects cannot be decomposed as the tensor product of smaller effects, like for $\mathfrak{D}$ such that $\mathfrak{D}(x_1) = |\Phi^+\rangle\langle\Phi^+|$, $\mathfrak{D}(x_2) = |\Phi^-\rangle\langle\Phi^-|$, $\mathfrak{D}(x_3) = |\Psi^+\rangle\langle\Psi^+|$, $\mathfrak{D}(x_4) = |\Psi^-\rangle\langle\Psi^-|$.

To model quantum systems and protocols we introduce effect labelled transition systems (eLTSs).

Definition 2. *An eLTS of dimension d is a triple $(S, Act, \rightarrow)$ where S is a set of states, Act is a set of labels, and $\rightarrow \subseteq S \times Act \times \mathscr{Q}_d S$ is the transition relation. As usual, we write $s \xrightarrow{\mu} \mathfrak{D}$ for $(s, \mu, \mathfrak{D}) \in \rightarrow$.*

We instantiate two distinct definitions of semantic equivalence on quantum systems: *Aczel-Mendler* and *Larsen-Skou* bisimilarities [24]. Roughly, the first requires bisimilar distributions to assign the same weight to bisimilar states, while the latter compares the combined weights of equivalence classes of bisimilar states. They are known to coincide on classical probabilistic processes [14]. Notably, they do not in the quantum case.

Definition 3. AM-bisimilarity $\sim_{am}$ *is the largest symmetric relation $\mathscr{R} \subseteq S \times S$ such that for any $s \mathscr{R} t$*

$$\textit{if } s \xrightarrow{\mu} \mathfrak{D} \textit{ then } t \xrightarrow{\mu} \mathfrak{T} \textit{ for some } \mathfrak{T} \textit{ such that } \mathfrak{D} \overset{\square}{\mathscr{R}} \mathfrak{T}$$

where $\overset{\square}{\mathscr{R}}$ is the smallest relation between effect distributions such that $s \mathscr{R} t$ implies $\{(s,1)\} \overset{\square}{\mathscr{R}} \{(t,1)\}$, and $\mathfrak{D}_i \overset{\square}{\mathscr{R}} \mathfrak{T}_i$ implies $(\sum_{i \in I} E_i \otimes \mathfrak{D}_i) \overset{\square}{\mathscr{R}} (\sum_{i \in I} E_i \otimes \mathfrak{T}_i)$.

Example 1. *Consider an eLTSs having the following transitions (only):*

$$s_1 \xrightarrow{\alpha} \{(s_4, |0\rangle\langle 0|), (s_5, |1\rangle\langle 1|)\} \qquad s_2 \xrightarrow{\alpha} \{(s_4, \mathbb{I})\} \qquad s_3 \xrightarrow{\alpha} \{(s_4, |+\rangle\langle +|), (s_5, |-\rangle\langle -|)\}$$

We have that $s_1 \sim_{am} s_2$ and $s_2 \sim_{am} s_3$. Indeed, $|0\rangle\langle 0| + |1\rangle\langle 1| = I = |+\rangle\langle +| + |-\rangle\langle -|$. Nonetheless, $s_1 \nsim_{am} s_3$.

This example, inspired by [23], proves that $\sim_{am}$ is not transitive. We thus generalize *Larsen-Skou bisimilarity* [19] to the quantum case (named kernel bisimilarity in [24]).

$$\frac{s_1 \xrightarrow{\mu} \mathfrak{D}}{s_1 + s_2 \xrightarrow{\mu} \mathfrak{D}}\ \textsc{ExtL} \qquad \frac{s_1 \xrightarrow{\mu} \mathfrak{D}}{s_1 \parallel s_2 \xrightarrow{\mu} \mathfrak{D} \parallel \{s_2 \rhd \mathbb{I}_{d'}\}}\ \textsc{ParL} \qquad \frac{s_1 \xrightarrow{\mu} \mathfrak{D} \quad s_2 \xrightarrow{\overline{\mu}} \mathfrak{T}}{s_1 \parallel s_2 \xrightarrow{\tau} \mathfrak{D} \parallel \mathfrak{T}}\ \textsc{Synch} \qquad \frac{s \xrightarrow{\mu} \mathfrak{D}}{s|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho}\ \textsc{QInst}$$

Figure 1: Operators on eLTSs (right rules omitted).

Definition 4. *Let* LS-bisimilarity $\sim_{ls}$ *be the largest equivalence relation $\mathscr{R} \subseteq S \times S$ such that for any $s\mathscr{R}t$*

$$\textit{if } s \xrightarrow{\mu} \mathfrak{D} \textit{ then } t \xrightarrow{\mu} \mathfrak{T} \textit{ for some } \mathfrak{T} \textit{ such that } \ \forall C \in S/_{\mathscr{R}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$$

with $S/_{\mathscr{R}}$ the equivalence classes of S.

We show that $\sim_{ls}$ correctly equates s_1, s_3 of Example 1, as both $\mathfrak{D}$ and $\mathfrak{T}$ associate the equivalence class $\{s_4, s_5\}$ with the effect $\mathbb{I}$. Moreover, LS-bisimilarity is coarser than AM-bisimilarity.

Note that we can instantiate any effect distribution with a density operator ρ obtaining a probability distribution. Therefore, we can compute the pLTS characterizing the probabilistic behaviour of an eLTS in a given state ρ. We write $s \sim_\rho t$ if s and t are *probabilistic* bisimilar in the pLTS obtained with ρ. Since probabilistic behaviour is the only observable property of quantum systems, we consider *probabilistic behavioural equivalence* ($\simeq_{pbe} = \bigcap_\rho \sim_\rho$) as the ground truth our bisimilarity must comply with.

Theorem 2. *In any eLTS, $\sim_{ls} \subseteq \simeq_{pbe}$. Moreover, if the eLTS is finite, then $\simeq_{pbe} \subseteq \sim_{ls}$.*

We lift the operators commonly considered for probabilistic systems to the case of eLTSs, namely non-deterministic sum and parallel composition, and we propose a new operator tailored for the quantum case, the *quantum partial instantiation*. We let $E|_\rho = tr_A(E(\rho \otimes \mathbb{I}_B))$ with ρ in $\mathscr{H}_A$ and E in $\mathscr{H}_A \otimes \mathscr{H}_B$: roughly, $E|_\rho$ is obtained by partially evaluating E over the input provided by ρ. In Figure 1, we define such operators, where we write $(\mathfrak{D} \parallel \mathfrak{T})$ and $\mathfrak{D}|_\rho$ for the distributions associating $s_1 \parallel s_2$ with $\mathfrak{D}(s_1) \otimes \mathfrak{T}(s_2)$, and $s'|_\rho$ with $\mathfrak{D}(s')|_\rho$ respectively. We prove that $\sim_{ls}$ is closed under all the operations above.

We then explore operations over effect distributions and present a pair of no-go theorems distinguishing the quantum case from the probabilistic one. First, we notice that the lack of expressivity of $\oplus$ is not only syntactical: it is possible with n-ary composition to define eLTSs for which no bisimilar state can be defined using the binary operator $\oplus$ only. Then, we consider non-deterministic composition of effect distributions. An effect distribution $\mathfrak{D} + \mathfrak{T}$ such that $(\mathfrak{D} + \mathfrak{T}){\downarrow_\rho}\ (s_1 + s_2) = \mathfrak{D}{\downarrow_\rho}\ (s_1) \cdot \mathfrak{T}{\downarrow_\rho}\ (s_2)$ does not always exist, preventing us from lifting the usual notion of non-deterministic sum of probability distributions [14] to effect distributions. In particular, $\mathfrak{D} + \mathfrak{T}$ never exists if the dimension of the Hilbert space is two or greater and $\mathfrak{D}(s) = |\psi\rangle\langle\psi|$ and $\mathfrak{T}(t) = |\phi\rangle\langle\phi|$ for some states $s, t \in S$ and quantum states $|\psi\rangle$ and $|\phi\rangle$.

To assess our proposal, we define a *minimal quantum process algebra* (mQPA) featuring actions, synchronization, non-determinism, parallel composition, destructive measurements and unitary transformations, and we enrich it with two different semantics: a stateful Schrödinger-style semantics that given a quantum state as input returns a pLTS representing the observable behaviour of the system; and a Heisenberg-style semantics in the form of an eLTS that is independent of the actual quantum input, in the style of [13, 7]. We prove that the Heisenberg-style eLTS is indeed the “symbolic” version of the Schrödinger-style pLTSs of the same system. In a nutshell, this means that we can prove bisimilarity just once on the Heisenberg semantics, and have it automatically verified for all the possible “ground” systems obtained by instantiating the quantum input. Notably, our notion of bisimilarity can be efficiently verified with standard techniques [15].

References

[1] Charles H. Bennett & Gilles Brassard (2014): *Quantum Cryptography: Public Key Distribution and Coin Tossing*. Theoretical Computer Science 560, pp. 7–11, doi:10.1016/j.tcs.2014.05.025.

[2] Marcello Caleffi, Angela Sara Cacciapuoti & Giuseppe Bianchi (2018): *Quantum Internet: From Communication to Distributed Computing!* In: Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication, ACM, Reykjavik Iceland, pp. 1–4, doi:10.1145/3233188.3233224.

[3] Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno & Gabriele Tedeschi (2024): *Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-deterministic Observers*. Proc. ACM Program. Lang. 8(POPL), pp. 43:1269–43:1297, doi:10.1145/3632885.

[4] Timothy AS Davidson (2012): *Formal Verification Techniques Using Quantum Process Calculus*. Ph.D. thesis, University of Warwick.

[5] Yuxin Deng (2018): *Bisimulations for Probabilistic and Quantum Processes (Invited Paper)*. In Sven Schewe & Lijun Zhang, editors: 29th International Conference on Concurrency Theory (CONCUR 2018), Leibniz International Proceedings in Informatics (LIPIcs) 118, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, pp. 2:1–2:14, doi:10.4230/LIPIcs.CONCUR.2018.2.

[6] Yuxin Deng & Yuan Feng (2012): *Open Bisimulation for Quantum Processes*. In Jos C. M. Baeten, Tom Ball & Frank S. de Boer, editors: Theoretical Computer Science, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 119–133, doi:10.1007/978-3-642-33475-7_9.

[7] Yuan Feng, Yuxin Deng & Mingsheng Ying (2014): *Symbolic Bisimulation for Quantum Processes*. ACM Trans. Comput. Logic 15(2), pp. 14:1–14:32, doi:10.1145/2579818.

[8] Yuan Feng, Runyao Duan & Mingsheng Ying (2012): *Bisimulation for Quantum Processes*. ACM Trans. Program. Lang. Syst. 34(4), pp. 17:1–17:43, doi:10.1145/2400676.2400680.

[9] Yuan Feng & Mingsheng Ying (2015): *Toward Automatic Verification of Quantum Cryptographic Protocols*. In Luca Aceto & David de Frutos Escrig, editors: 26th International Conference on Concurrency Theory (CONCUR 2015), Leibniz International Proceedings in Informatics (LIPIcs) 42, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, pp. 441–455, doi:10.4230/LIPIcs.CONCUR.2015.441.

[10] Fei Gao, SuJuan Qin, Wei Huang & QiaoYan Wen (2019): *Quantum Private Query: A New Kind of Practical Quantum Cryptographic Protocol*. Sci. China Phys. Mech. Astron. 62(7), p. 70301, doi:10.1007/s11433-018-9324-6.

[11] Simon J. Gay & Rajagopal Nagarajan (2005): *Communicating Quantum Processes*. In: Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '05, Association for Computing Machinery, New York, NY, USA, pp. 145–157, doi:10.1145/1040305.1040318.

[12] Teiko Heinosaari & Mário Ziman (2011): *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*. Cambridge University Press.

[13] M Hennessy & H Lin (1995): *Symbolic Bisimulations*. Theoretical Computer Science 138(2), pp. 353–389, doi:10.1016/0304-3975(94)00172-F.

[14] Matthew Hennessy (2012): *Exploring Probabilistic Bisimulations, Part I*. Form. Asp. Comput. 24(4-6), pp. 749–768, doi:10.1007/s00165-012-0242-7.

[15] Jules Jacobs & Thorsten Wißmann (2023): *Fast Coalgebraic Bisimilarity Minimization*. Proc. ACM Program. Lang. 7(POPL), pp. 52:1514–52:1541, doi:10.1145/3571245.

[16] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano & Hideki Sakurada (2012): *Application of a Process Calculus to Security Proofs of Quantum Protocols*. In: Proceedings of the International Conference on Foundations of Computer Science (FCS), The Steering Committee of The World Congress in Computer Science, Computer ..., p. 1.

[17] Marie Lalire (2006): *Relations among Quantum Processes: Bisimilarity and Congruence*. arXiv:quant-ph/0603274.

[18] Marie Lalire & Philippe Jorrand (2004): *A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics*. arXiv:quant-ph/0407005.

[19] Kim G. Larsen & Arne Skou (1991): *Bisimulation through Probabilistic Testing*. Information and Computation 94(1), pp. 1–28, doi:10.1016/0890-5401(91)90030-6.

[20] Gui-lu Long, Fu-guo Deng, Chuan Wang, Xi-han Li, Kai Wen & Wan-ying Wang (2007): *Quantum Secure Direct Communication and Deterministic Secure Quantum Communication*. Front. Phys. China 2(3), pp. 251–272, doi:10.1007/s11467-007-0050-3.

[21] Dominic Mayers (2001): *Unconditional Security in Quantum Cryptography*. J. ACM 48(3), pp. 351–406, doi:10.1145/382780.382781.

[22] Ali Ibnun Nurhadi & Nana Rachmana Syambas (2018): *Quantum Key Distribution (QKD) Protocols: A Survey*. In: 2018 4th International Conference on Wireless and Telematics (ICWT), pp. 1–5, doi:10.1109/ICWT.2018.8527822.

[23] Hiroshi Ogawa (2014): *Coalgebraic Approach to Equivalences of Quantum Systems*. Master's thesis, University of Tokyo.

[24] Sam Staton (2011): *Relating Coalgebraic Notions of Bisimulation*. Logical Methods in Computer Science 7.

[25] Yong Wang (2019): *Probabilistic Process Algebra to Unifying Quantum and Classical Computing in Closed Systems*. Int J Theor Phys 58(10), pp. 3436–3509, doi:10.1007/s10773-019-04216-2.

[26] Peiying Zhang, Ning Chen, Shigen Shen, Shui Yu, Sheng Wu & Neeraj Kumar (2022): *Future Quantum Communications and Networking: A Review and Vision*. IEEE Wireless Commun., pp. 1–8, doi:10.1109/MWC.012.2200295.