Symbolic Verification of Quantum Protocols via Quantum Distributions – Early Ideas

Gabriele Tedeschi
IRIF, CNRS - Université Paris Cité, France

Lorenzo Ceragioli
IMT Lucca, Italy

Giseppe Lomurno
University of Pisa, Italy

Fabio Gadducci
University of Pisa, Italy

Abstract

The development of quantum communication protocols sparked the interest in quantum extensions of process calculi. The prominent approaches, however, are still based on probabilistic models, which are inadequate for the quantum case, as they do not capture the observational limitations of quantum theory. In Physics, probabilistic quantum systems are not represented with probabilities, but with density operators. By lifting this concept to the Computer Science setting, we introduce Operator Distributions: they employ density operators as weights, just like probability distributions use real numbers. We give semantics to quantum protocols in a natural way, as an LTS of operator distributions, guaranteeing that only physically accessible information about the systems are represented. Moreover, these "quantum" distributions pave the way for symbolic verification of protocols whose behaviour depends on an unknown initial state: instead of considering infinitely-many LTSs, one for each possible initialization, we can build a single symbolic LTS and prove properties on it.

2012 ACM Subject Classification Hardware → Quantum communication and cryptography; Theory of computation → Process calculi; Software and its engineering → Formal software verification

Keywords and phrases Quantum Process Calculi, Symbolic Bisimilarity

Recent years have seen a flourishing development of *quantum computation* and *quantum communication* technologies [22]. We focus on the latter, which provides solutions for key distribution [23], electronic voting [2], *Quantum Internet* [3, 26], and many other applications [1]. Therefore, the need emerged for modelling and verification techniques applicable to quantum protocols. We will show why the current proposals are not fully satisfactory, and then present two novel semantic models based on *Quantum Distributions*, which abides the rules of quantum theory and supports algorithmic equivalence checking. This is useful to prove correctness of protocol implementations, or to investigate non-interference and resistance to cryptographic attackers.

Numerous works in the field [21, 17, 15, 7, 6] rely on *quantum process calculi*, where we describe a set of interacting agents, each of them manipulating and sending some qubits. The typical semantics for these quantum calculi is based on *configurations* $\langle |\psi\rangle , P\rangle$, consisting of a syntactic *process* P (the code that the agent is executing) and a quantum state $|\psi\rangle$ (the data which the process manipulates). An example would be the configuration $C = \langle |0\rangle , \underline{H(q).M_{01}(q \rhd x).c!q}\rangle$, where the data is a single qubit q in state $|0\rangle$, and the process i) updates q with an H gate, bringing its state to $|+\rangle$; ii) measures such qubit and stores the outcome in the variable x, causing q do *decay* in either $|0\rangle$ or $|1\rangle$; iii) sends q over the channel c. In literature, it is common to build a Labelled Transition System (LTS) whose states are *distributions* of such configurations. The LTS of the distribution $1{\cdot}C$ would be

$$1{\cdot}C \xrightarrow{\tau} 1{\cdot}\langle |+\rangle, \underline{M_{01}(q \rhd x).c!q}\rangle \xrightarrow{\tau} \tfrac{1}{2}{\cdot}\langle |0\rangle, \underline{c!q}\rangle \oplus \tfrac{1}{2}{\cdot}\langle |1\rangle , \underline{c!q}\rangle \xrightarrow{c!q} \tfrac{1}{2}{\cdot}\langle |0\rangle, \underline{\mathbf{0}}\rangle \oplus \tfrac{1}{2}{\cdot}\langle |1\rangle , \underline{\mathbf{0}}\rangle \quad (1)$$

where $1{\cdot}C$ is the point distribution in C, and $\frac{1}{2}{\cdot}C \oplus \frac{1}{2}{\cdot}C'$ is the uniform distribution of C, C'. Notice how configurations in quantum process calculi are akin to "quantum closures" in the operational semantics of quantum languages [25]. The approach of modelling probabilistic systems with a transition systems of distributions has already appeared for both concurrent systems [19, 11] and quantum lambda calculi [8, 12, 13].

Our main focus in characterizing when two protocols are *behaviourally equivalent*, meaning that they exhibit the same interactive observable behaviour, in term of communication actions and qubit values. Different notions of behavioural equivalence have been considered [9, 16, 10, 5], all based on the distribution-of-configurations approach described above. However argue that it is the semantic model itself to be inadequate, for two reasons: it does not respect the indistinguishability results of quantum theory, and it hampers algorithmic equivalence checking.

For the first problem, consider these two sources of random qubits:

$$\Delta = \frac{1}{2}{\cdot}\left\langle |0\rangle, \underline{c!q}\right\rangle \oplus \frac{1}{2}{\cdot}\left\langle |1\rangle, \underline{c!q}\right\rangle \qquad \Theta = \frac{1}{2}{\cdot}\left\langle |+\rangle, \underline{c!q}\right\rangle \oplus \frac{1}{2}{\cdot}\left\langle |-\rangle, \underline{c!q}\right\rangle. \tag{2}$$

The Δ distribution sends a random value between $|0\rangle$ or $|1\rangle$, while Θ sends either $|+\rangle$ or $|-\rangle$. According to quantum mechanics, no realizable procedure can tell apart one source from the other [22]. Nonetheless, several existing proposals fail to make Δ and Θ equivalent [20, 15, 11], while others have to fine tune their notion of equivalence to solve this issue [10, 5, 6]. The second problem, instead, involves protocols featuring quantum inputs (e.g. Teleportation): to check their correctness we should build an infinite number of LTSs, one for each input.

We address both concerns by introducing two novel semantic models, inspired by quantum theory. In Physics, when dealing with random qubits, we do not use probability distributions of quantum values, but we employ the *Density Operator Formalism*. Qubits states are represented as matrices, called *Density Operators*, and transformations on qubits are represented as maps between matrices, called *Superoperators*. The density operators on d-dimensional Hilbert Space $\mathcal{H}$ are denoted as $DO_{\mathcal{H}} = \left\{\rho \in \mathbb{C}^{d\times d} \mid \rho \text{ is positive and } tr(\rho) \leq 1\right\}$, while superoperators are defined as $Sop_{\mathcal{H}} = \{\mathcal{E} \colon DO_{\mathcal{H}} \to DO_{\mathcal{H}} \mid \mathcal{E} \text{ is completely positive and } tr(\mathcal{E}(\rho)) \leq tr(\rho)\}$.

There is a non-injective map from probability distributions of quantum values to density operators. Distributions that are impossible to tell apart are mapped in the same matrix. For example, the two distribution $\frac{1}{2}{\cdot}|0\rangle \oplus \frac{1}{2}{\cdot}|1\rangle$ and $\frac{1}{2}{\cdot}|+\rangle \oplus \frac{1}{2}{\cdot}|-\rangle$ are both represented as

$$\frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1| \;=\; \mathbb{I}/2 \;=\; \frac{1}{2}\,|+\rangle\langle +| + \frac{1}{2}\,|-\rangle\langle -| \tag{3}$$

Density operators enjoy a *Partial Commutative Monoid* (PCM) structure: they can be summed with matrix addition, but only if the result is still in $DO_{\mathcal{H}}$. This generalizes the case of probabilities, i.e. the PCM of real numbers with sum in the interval $[0, 1]$. Following this similarity, we can define a new kind of *quantum distributions*.

▶ **Definition 1.** *Given a Hilbert Space $\mathcal{H}$, the set of* Operator (Sub)-Distributions *over X is*

$$\mathcal{Q}(X) = \left\{\, \mathfrak{D} \in (DO_{\mathcal{H}})^X \;\middle|\; \mathrm{supp}(\mathfrak{D}) \text{ is finite and } \textstyle\sum_{x\in X} \mathfrak{D}(x) \in DO_{\mathcal{H}} \right\}$$

where $\mathrm{supp}(\mathfrak{D})$ *is the support of $\mathfrak{D}$, i.e. the set* $\{\, x \in X \mid \mathfrak{D}(x) \neq \mathbf{0} \,\}$.

We write $\rho_0{\cdot}x_0 \oplus \rho_1{\cdot}x_1$ for the distribution where x_i has weight ρ_i for $i \in \{0, 1\}$, and all other $x_i \in X$ have weight $\mathbf{0}$, the all-zero matrix. Categorically, operator distributions form a functor on **Set**, and indeed we can build similar "distribution functors" for any PCM.

We can give semantics to quantum protocols using *operator distribution of processes*. Each process is weighted with an operator, encoding both the quantum data and the probability of having reached that process. The LTS in Equation 1 would become

$$|0\rangle\langle 0|\cdot\underline{H(q).M_{01}(q \rhd x).c!q} \xrightarrow{\tau} |+\rangle\langle +|\cdot\underline{M_{01}(q \rhd x).c!q} \xrightarrow{\tau} \mathbb{I}/2\cdot\underline{c!q} \xrightarrow{c!q} \mathbb{I}/2\cdot\underline{\mathbf{0}}. \tag{4}$$

Indeed, after measuring q, the system evolves in the distribution $\frac{1}{2}|0\rangle\langle 0|\cdot\underline{c!q} \oplus \frac{1}{2}|1\rangle\langle 1|\cdot\underline{c!q}$. But $\frac{1}{2}|0\rangle\langle 0|\cdot\underline{c!q} \oplus \frac{1}{2}|1\rangle\langle 1|\cdot\underline{c!q}$ is just another way to write $\mathbb{I}/2\cdot\underline{c!q}$, thanks to Equation 3. This solves the problem in Equation 2: equivalent sources are modelled as the same operator distribution. Notice how this would not happen for the process $\underline{H(q).M_{01}(q \rhd x).c!x}$, which measures the qubit and sends the classical outcome. It evolves in $\frac{1}{2}|0\rangle\langle 0|\cdot\underline{c!0} \oplus \frac{1}{2}|1\rangle\langle 1|\cdot\underline{c!1}$, where the processes are *classically* distinguished, and thus the quantum states are not combined.

However, the process $\underline{P} = \underline{H(q).M_{01}(q).c!q}$ in Equation 4 has still a different transition system for all its inputs, like $|0\rangle\langle 0|\cdot\underline{P}, |+\rangle\langle +|\cdot\underline{P}$ or $\mathbb{I}/2\cdot\underline{P}$. We thus introduce a second kind of quantum distributions, based on superoperators, inspired by the denotational semantics of quantum programming languages [24, 18]. Similarly to $DO_{\mathcal{H}}$ and to $[0, 1]$, also superoperators on $\mathcal{H}$ enjoy a PCM structure, such that we can define *Superoperator Distributions* as follows.

▶ **Definition 2.** *Given a Hilbert Space $\mathcal{H}$, we define* Superoperator Distributions *over X as*

$$\mathcal{S}(X) = \left\{ \mathfrak{D} \in (Sop_{\mathcal{H}})^X \;\middle|\; \mathrm{supp}(\mathfrak{D}) \text{ is finite and } \textstyle\sum_{x\in X} \mathfrak{D}(x) \in Sop_{\mathcal{H}} \right\}$$

where $\mathrm{supp}(\mathfrak{D}) = \{ x \in X \mid \mathfrak{D}(x) \neq \mathcal{Z} \}$, *$\mathcal{Z}$ is the constant $\mathbf{0}$ map, and superoperators are summed in a point-wise manner.*

The semantics of a protocol can then be given as a single LTS made of superoperator distributions, similar to [14, 4]. The LTS in Equation 1 becomes

$$\mathcal{I}d\cdot\underline{H(q).M_{01}(q \rhd x).\mathbf{0}} \xrightarrow{\tau} \mathcal{H}ad\cdot\underline{M_{01}(q \rhd x).c!q} \xrightarrow{\tau} \mathcal{S}et_{\mathbb{I}/2}\cdot\underline{c!q} \xrightarrow{c!q} \mathcal{S}et_{\mathbb{I}/2}\cdot\underline{\mathbf{0}}. \tag{5}$$

where $\mathcal{H}ad$ is the Hadamard gate, and $\mathcal{S}et_{\mathbb{I}/2}$ is the map which prepares the state $\mathbb{I}/2$. In these distributions, each process has a superoperator as weight, representing the sequence of transformation that have been applied on the quantum input to arrive at that process.

Noticeably, this LTS is independent on the state of the input qubit. We can check our behavioural equivalence of choice, e.g. bisimilarity, between these *symbolic*, superoperator-based transition systems, instead of comparing an infinite number of *ground*, operator-based ones. Once we know the input quantum state, each symbolic LTS can be instantiated to a ground LTS, just by updating the weights in the distributions. In the case of Equation 5, if the input state is $|0\rangle\langle 0|$ we get the LTS in Equation 4.

Categorically, each input state ρ defines a natural transformation between superoperator distributions and operator distributions, and these transformations commute with the semantics of processes. From this, it is possible to prove full abstraction: two symbolic LTSs are bisimilar if and only if all their ground instantiations are.

More in detail, we can lift some useful properties from our weights ($DO_{\mathcal{H}}$ and $Sop_{\mathcal{H}}$) to our distributions ($\mathcal{Q}(X)$ and $\mathcal{S}(X)$). We can show that $Sop_{\mathcal{H}}$ forms an appropriate kind of *partial semiring*, with partial addition and total multiplication, while both $DO_{\mathcal{H}}$ and $Sop_{\mathcal{H}}$ form a *partial Sop-semimodule*, as they can be summed and can be "updated" by a superoperator. Then, given a quantum input ρ, instantiating a superoperator $\mathcal{E} \in Sop_{\mathcal{H}}$ to get a quantum output $\mathcal{E}(\rho) \in DO_{\mathcal{H}}$ is a *homomorphism of Sop-semimodules*: updating our symbolic weight $\mathcal{E}$ with another superoperator $\mathcal{F}$ commutes with instantiating it to a

ground weight $\mathcal{E}(\rho)$. Lifting these properties from weights to distributions and LTSs, get a fully abstract translation between our symbolic $Sop_{\mathcal{H}}$-weighted semantics and our ground $DO_{\mathcal{H}}$-weighted one.

To sum up, we propose two quantum generalization of probability distributions, suitable to model and verify quantum communication protocols. Our ground semantics is defined in terms of $DO_{\mathcal{H}}$-weighted distributions of processes, where density operators represent both quantum data and probabilities, and they naturally abide to the observational limitations of quantum theory. Then, to check equivalence between quantum protocols in a symbolic fashion, we can define $Sop_{\mathcal{H}}$-weighted distributions, employing superoperators to represent the sequence of transformations applied on an unknown quantum state. Thanks to full abstraction, we can check equivalence between symbolic systems, and know that they will be equivalent under any possible quantum input.

References

1 Quantum Protocol Zoo. https://wiki.veriqloud.fr/index.php?title=Protocol_Library.

2 Myrto Arapinis, Nikolaos Lamprou, Elham Kashefi, and Anna Pappa. Definitions and Security of Quantum Electronic Voting. *ACM Transactions on Quantum Computing*, 2(1):4:1–4:33, April 2021. doi:10.1145/3450144.

3 Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. Quantum internet: From communication to distributed computing! In *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*, pages 1–4, Reykjavik Iceland, September 2018. ACM. doi:10.1145/3233188.3233224.

4 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Effect Semantics for Quantum Process Calculi. In Rupak Majumdar and Alexandra Silva, editors, *35th International Conference on Concurrency Theory (CONCUR 2024)*, volume 311 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:22, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CONCUR.2024.16.

5 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-deterministic Observers. *Proceedings of the ACM on Programming Languages*, 8(POPL):43:1269–43:1297, January 2024. doi:10.1145/3632885.

6 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Quantum Bisimilarity Is a Congruence Under Physically Admissible Schedulers. In Oleg Kiselyov, editor, *Programming Languages and Systems*, pages 176–195, Singapore, 2025. Springer Nature. doi:10.1007/978-981-97-8943-6_9.

7 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Testing Quantum Processes. In Tiziana Margaria and Bernhard Steffen, editors, *Leveraging Applications of Formal Methods, Verification and Validation. REoCAS Colloquium in Honor of Rocco De Nicola*, pages 132–151, Cham, 2025. Springer Nature Switzerland. doi:10.1007/978-3-031-73709-1_9.

8 Ugo Dal Lago, Andrea Masini, and Margherita Zorzi. Confluence results for a quantum lambda calculus with measurements. *Electronic Notes in Theoretical Computer Science*, 270(2):251–261, 2011. Proceedings of the 6th International Workshop on Quantum Physics and Logic (QPL 2009). URL: https://www.sciencedirect.com/science/article/pii/S1571066111000363, doi:10.1016/j.entcs.2011.01.035.

9 Timothy AS Davidson. *Formal Verification Techniques Using Quantum Process Calculus*. PhD thesis, University of Warwick, 2012.

10 Yuxin Deng. Bisimulations for Probabilistic and Quantum Processes (Invited Paper). In Sven Schewe and Lijun Zhang, editors, *29th International Conference on Concurrency Theory (CONCUR 2018)*, volume 118 of *Leibniz International Proceedings in Informatics (LIPIcs)*,

pages 2:1–2:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CONCUR.2018.2.

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

12 Yuxin Deng, Yuan Feng, and Ugo Dal Lago. On coinduction and quantum lambda calculi. *Leibniz International Proceedings in Informatics, LIPIcs*, 2015.

13 Claudia Faggian, Gaetan Lopez, and Benoît Valiron. A rewriting theory for quantum lambda-calculus. In *CSL 2025-33rd EACSL Annual Conference on Computer Science Logic*, volume 326, pages 47–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2025.

14 Yuan Feng, Yuxin Deng, and Mingsheng Ying. Symbolic Bisimulation for Quantum Processes. *ACM Transactions on Computational Logic*, 15(2):14:1–14:32, May 2014. doi:10.1145/2579818.

15 Yuan Feng, Runyao Duan, and Mingsheng Ying. Bisimulation for Quantum Processes. *ACM Transactions on Programming Languages and Systems*, 34(4):17:1–17:43, December 2012. doi:10.1145/2400676.2400680.

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

17 Simon J. Gay and Rajagopal Nagarajan. Communicating quantum processes. In *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '05, pages 145–157, New York, NY, USA, January 2005. Association for Computing Machinery. doi:10.1145/1040305.1040318.

18 Ichiro Hasuo and Naohiko Hoshino. Semantics of Higher-Order Quantum Computation via Geometry of Interaction. In *2011 IEEE 26th Annual Symposium on Logic in Computer Science*, pages 237–246, June 2011. doi:10.1109/LICS.2011.26.

19 Matthew Hennessy. Exploring probabilistic bisimulations, part I. *Formal Aspects of Computing*, 24(4-6):749–768, July 2012. doi:10.1007/s00165-012-0242-7.

20 Marie Lalire. Relations among quantum processes: Bisimilarity and congruence, March 2006. arXiv:quant-ph/0603274.

21 Marie Lalire and Philippe Jorrand. A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics, July 2004. arXiv:quant-ph/0407005.

22 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge ; New York, 10th anniversary ed edition, 2010.

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

24 PETER SELINGER. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004. doi:10.1017/S0960129504004256.

25 PETER SELINGER and BENOIT VALIRON. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006. doi:10.1017/S0960129506005238.

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