Concurrent Quantum Separation Logic for Fine-Grained Parallelism

YUSUKE MATSUSHITA, Kyoto University, Japan
KENGO HIRATA, University of Edinburgh, United Kingdom and Kyoto University, Japan
RYO WAKIZAKA, Kyoto University, Japan

A promising approach to efficient quantum computation is to execute subroutines in *parallel* at a fine-grained level. While such parallelism is subject to tricky bugs, there was no quantum program logic that could modularly verify the correctness of such parallelism.

To overcome this situation, we propose novel concurrent quantum separation logic that can modularly reason about quantum programs under fine-grained parallelism. Our logic enables flexible reasoning about *quantum superposition* via new proof rules for *linearly combining* Hoare triples. Also, our logic introduces fractional tokens for *sharing* the same qubits between parallel subroutines, introducing new reasoning rules for *promoting* partial ownership into full ownership by *atomicity*. We demonstrate the effectiveness of our logic by verifying a non-trivial parallelized quantum program.

1 Introduction

Today, quantum computers are steadily becoming larger, and interest in realizing efficient quantum computation has grown. A promising approach to that is to execute subroutines in *parallel* at a fine-grained level [Gidney and Ekerå 2021; Häner et al. 2022]. One practical goal would be the automated parallelization of quantum programs, statically by the compiler or dynamically by the runtime. While such parallelism is subject to tricky bugs, there was no quantum program logic that could modularly verify the correctness of such parallelism. To tackle state mutation under concurrency, *concurrent separation logic* [O'Hearn 2004; Brookes 2004; Brookes and O'Hearn 2016] should be a great fit, but existing quantum separation logic [Zhou et al. 2021; Le et al. 2022; Su et al. 2024] unfortunately supported neither concurrency nor sharing of qubits, which is crucial for fine-grained parallelism.

To overcome this situation, we propose novel concurrent quantum separation logic that can modularly reason about quantum programs under fine-grained parallelism. Our logic is particularly new in the following two points. First, unlike the classical setting and existing quantum separation logic, our logic enables flexible reasoning about *quantum superposition* via new proof rules for *linearly combining* Hoare triples. Second, our logic features a *fractional* quantum points-to token $\bar{q} \overset{r}{\mapsto} |\psi\rangle$, which can be *shared* between parallel subroutines, introducing new reasoning rules for *promoting* partial ownership into full ownership by *atomicity*. We demonstrate the effectiveness of our logic by verifying a non-trivial parallelized quantum program.

Authors' Contact Information: Yusuke Matsushita, Kyoto University, Kyoto, Japan, ymat@fos.kuis.kyoto-u.ac.jp; Kengo Hirata, University of Edinburgh, Edinburgh, United Kingdom and Kyoto University, Kyoto, Japan, k.hirata@sms.ed.ac.uk; Ryo Wakizaka, Kyoto University, Kyoto, Japan, wakizaka@fos.kuis.kyoto-u.ac.jp.

2 Target Quantum Language

Our target quantum language has the following syntax:

$$\begin{aligned} \mathit{Exp} \ni e \ ::= \ & q \mid \ell \mid n \mid () \mid \mathit{op}(\bar{e}) \mid x \mid \texttt{let}\, x = e_1 \,\texttt{in}\, e_2 \\ & \mid \texttt{if}\, e_1 \,\{e_2\}\, \texttt{else}\, \{e_3\} \mid \texttt{while}\, e_1 \,\{e_2\} \mid e_1 \parallel e_2 \mid \texttt{atomic}\,\{e\} \\ & \mid \texttt{qalloc} \mid \texttt{qfree}\, e \mid U[\bar{e}] \mid \texttt{mkref}\, e \mid \texttt{!}e \mid e_1 \leftarrow e_2 \\ \mathit{Val} \ni v \ ::= \ & q \mid \ell \mid n \mid () \mid (v, v') \qquad e_1; e_2 \triangleq \texttt{let}\ \_ = e_1 \,\texttt{in}\, e_2 \end{aligned}$$

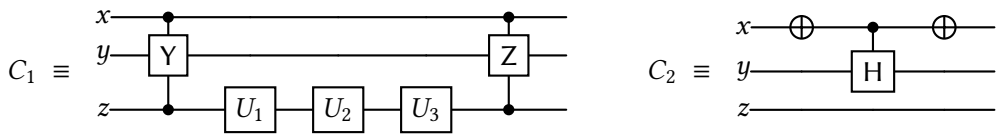
We write $q \in \mathit{Qname}$ for a qubit (name), $\ell \in \mathit{Loc}$ for a heap location, $n \in \mathbb{Z}$ for an integer, op for pure operators such as +. For concurrency, aside from the standard *parallel execution* $e_1 \parallel e_2$, we introduce *atomic execution* $\texttt{atomic}\,\{e\}$, which excludes interruption from other processes while executing e. Qubit and heap operations are pretty standard. Quantum measurements are not yet part of our language, and handling their stochastic behavior remains future work (see § 6). Please refer to Appendix A for the operational semantics.

3 Motivating Example

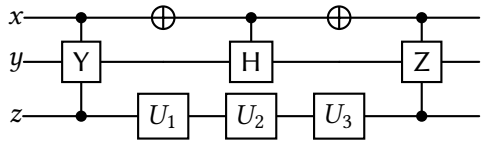
As a running example, we consider the following parallelized quantum program:

$$\begin{array}{ll} \text{Process 1} & \mathsf{CCY}[x,z,y];\ U_1[z];\ U_2[z];\ U_3[z];\ \mathsf{CCZ}[x,z,y] \\ \text{Process 2} & \parallel\ \texttt{atomic}\,\{\,\mathsf{X}[x];\ \mathsf{CH}[x,y];\ \mathsf{X}[x]\,\} \end{array} \tag{*}$$

It executes in parallel two processes, which can be illustrated as the following circuits:



The two processes may be executed sequentially (i.e., $C_1; C_2$ or $C_2; C_1$), or process 2 may be executed during the execution of process 1, as illustrated in the following circuit:



It is easy to see that the results are the same across these execution patterns.

Our goal is to prove the correctness of such a parallelized quantum program: regardless of the execution order, the program should consistently reach the same final state. This enables a compiler to safely reorder the execution sequence of concurrent circuits, provided it adheres to the program's semantics. However, modularly proving the correctness of a parallelized quantum program like (*) presents the following two challenges:

Challenge 1 Multiple processes may write to the same qubit. In the program (*), both processes write to the shared qubit y in parallel. This is naively a race condition but actually safe thanks to the commutativity of the gates.

Challenge 2 Atomic execution should be treated specially. In the program (*), Process 2 writes to x but then reverts its value within an atomic execution, and thus does not interfere with Process 1.

4 Our Quantum Separation Logic

Now we present our core contribution, the concurrent quantum separation logic for fine-grained parallelism. Please refer to Appendix B for a complete list of proof rules and Appendix C for the semantic model.

Propositions. Propositions for our separation logic are as follows:

$$\begin{aligned} \mathit{SLProp} \ni P, Q, R \ ::= \ & p \mid P \wedge Q \mid P \vee Q \mid P \to Q \mid \forall x.\, P_x \mid \exists x.\, P_x \\ & \mid \mathsf{emp} \mid P * Q \mid P \mathrel{-\!\!*} Q \mid \bar{q} \overset{r}{\mapsto} |\psi\rangle \mid [q]_r \mid \ell \overset{r}{\mapsto} v \end{aligned}$$

$$\bar{q} \mapsto |\psi\rangle \triangleq \bar{q} \overset{1}{\mapsto} |\psi\rangle \qquad \ell \mapsto v \triangleq \ell \overset{1}{\mapsto} v$$

We have the standard connectives from separation logic, including the separating conjunction $P * Q$ for combining ownership. Any pure proposition $p \in \mathit{Prop}$ can be embedded.

Notably, we introduce the *fractional quantum points-to token* $\bar{q} \overset{r}{\mapsto} |\psi\rangle$, a novel proposition that asserts with a fraction $r \in (0, 1]$ that the current pure state of the qubits $\bar{q} = q_1, \ldots, q_n$ is $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. It is a quantum analog of the classical points-to token $\ell \overset{r}{\mapsto} v$ [Bornat et al. 2005]. Under full ownership $r = 1$, it allows any operation to be performed over the qubits, while only a read operation is allowed under partial ownership $r < 1$. The model for this machinery is non-trivial and trickier than the classical setting, since each token may span over multiple qubits due to superposition; please see Appendix C for the details.

We also introduce the *qubit token* $[q]_r$, which asserts with a fraction r that the qubit q is allocated and not freed. It is useful for sharing *dirty qubits*, qubits without state information, between parallel subroutines. We use the shorthand $[\bar{q}]_r \triangleq \mathop{*}_i [q_i]_r$ for $\bar{q} = q_1, \ldots, q_n$.

We have the following proof rules for quantum ownership, as naturally expected:

$$(\bar{q}, \bar{q}') \mapsto |\psi\rangle |\psi'\rangle \dashv\vdash \bar{q} \mapsto |\psi\rangle * \bar{q}' \mapsto |\psi'\rangle$$

$$\bar{q} \overset{r+r'}{\mapsto} |\psi\rangle \dashv\vdash \bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q} \overset{r'}{\mapsto} |\psi\rangle \qquad [q]_{r+r'} \dashv\vdash [q]_r * [q]_{r'}$$

$$\{\mathsf{emp}\}\ \mathtt{qalloc}\ \{q.\, q \mapsto |0\rangle * [q]_1\} \qquad \{q \mapsto |0\rangle * [q]_1\}\ \mathtt{qfree}\ q\ \{\mathsf{emp}\}$$

$$\{(\bar{q}, \bar{q}') \mapsto |\psi\rangle\}\ U[\bar{q}]\ \{(\bar{q}, \bar{q}') \mapsto (U \otimes \mathrm{I})|\psi\rangle\}$$

Quantum superposition. One peculiar phenomenon in quantum computation is *quantum superposition*. While we can easily reason about classical conditional branching by case analysis between 1 and 0 on a classical bit, reasoning about controlled gates such as CX is much trickier because a qubit can be an arbitrary quantum superposition $\alpha|1\rangle + \beta|0\rangle$. To address this, we newly introduce the following proof rule for *linearly combining* Hoare triples, unlike existing quantum separation logic:

$$\frac{\{\bar{q} \mapsto |\psi\rangle * P\}\ e\ \{\bar{q} \mapsto |\varphi\rangle * Q\} \qquad \{\bar{q} \mapsto |\psi'\rangle * P\}\ e\ \{\bar{q} \mapsto |\varphi'\rangle * Q\} \qquad P, Q : \text{exact}}{\{\bar{q} \mapsto (\alpha|\psi\rangle + \beta|\psi'\rangle) * P\}\ e\ \{\bar{q} \mapsto (\alpha|\varphi\rangle + \beta|\varphi'\rangle) * Q\}}\ \textsc{qptto-lincomb}$$

The exactness judgment $P\colon \mathsf{exact}$ means that the SL proposition P is satisfied by a unique (or no) resource (for example, $[x]_1\colon \mathsf{exact}$ and $\bot\colon \mathsf{exact}$ hold but $(\exists q.\, [x]_q)\colon \mathsf{exact}$ does not hold). At a high level, this performs a 'case analysis' over the bases $|\psi\rangle$ and $|\psi'\rangle$ of the input pure state $\alpha\,|\psi\rangle + \beta\,|\psi'\rangle$. This actually solves Challenge 1 in § 3, because the 'case analysis' over x eliminates the spurious race condition. See the discussion in § 5 for details.

Concurrency. We have the following proof rules for concurrency:

$$\frac{\{P\}\ e\ \{v.\, Q_v\} \qquad \{P'\}\ e'\ \{v'.\, Q'_{v'}\}}{\{P * P'\}\ e \parallel e'\ \{(v,v').\, Q_v * Q'_{v'}\}}\ \textsc{parallel} \qquad \frac{\{P\}\ e\ \{v.\, Q_v\}}{\{P\}\ \mathtt{atomic}\ \{e\}\ \{v.\, Q_v\}}\ \textsc{atomic}$$

Parallel execution $e \parallel e'$ admits the standard proof rule with the separating conjunction. For atomic execution $\mathtt{atomic}\,\{e\}$, we simply verify the Hoare triple over e, with the help of *promotion by atomicity* explained below.

Promotion by atomicity. We say an expression e is atomic if e can take only one step. In particular, atomic execution $\mathtt{atomic}\,\{e\}$ and matrix application $U[\bar{q}]$ are atomic.

For atomic expressions, we can use the following rules for *promotion by atomicity*:

$$\frac{e \text{ is atomic} \quad P\colon \mathsf{out}\ \bar{q} \quad \{\bar{q} \mapsto |\psi\rangle * [\bar{q}]_1 * P\}\ e\ \{v.\, \bar{q} \mapsto |\psi\rangle * [\bar{q}]_1 * Q_v\}}{\{\bar{q} \overset{r}{\mapsto} |\psi\rangle * P\}\ e\ \{v.\, \bar{q} \overset{r}{\mapsto} |\psi\rangle * Q_v\}}\ \textsc{qptto-promote}$$

$$\frac{e \text{ is atomic} \quad P\colon \mathsf{out}\ q \quad \forall\, |\psi\rangle.\, \{q \mapsto |\psi\rangle * [q]_1 * P\}\ e\ \{v.\, q \mapsto |\psi\rangle * [q]_1 * Q_v\}}{\{[q]_r * P\}\ e\ \{v.\, [q]_r * Q_v\}}\ \textsc{qtok-promote}$$

By exploiting atomicity, partial ownership of a fractional points-to $\bar{q} \overset{r}{\mapsto} |\psi\rangle$ (QPTTO-PROMOTE) or qubit $[q]_r$ (QTOK-PROMOTE) token can be promoted into the full points-to and qubit tokens. Here, the judgment $P\colon \mathsf{out}\ \bar{q}$ means that the proposition P does not own any ownership over the qubits $\bar{q}$. For example, $q' \mapsto |\psi\rangle\colon \mathsf{out}\ \bar{q}$ holds if $q' \notin \{\bar{q}\}$. Promotion solves Challenge 2 in § 3, enabling temporary writes in an atomic execution.

5 Verification of the Motivating Example

Now we demonstrate how our concurrent quantum separation logic can verify the concurrent quantum program (*) presented in § 3.

First, we apply QPTTO-LINCOMB to decompose the superposition of the pure state $|\chi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$ of the qubit x by the basis $|1\rangle, |0\rangle$:

$$\{(x,y,z) \mapsto |\chi\rangle\,|\psi\rangle\,|\varphi\rangle\ *\ [y]_1\}$$

$$\{(x,y,z) \mapsto |1\rangle\,|\psi\rangle\,|\varphi\rangle\ *\ [y]_1\}\ \{(x,y,z) \mapsto |0\rangle\,|\psi\rangle\,|\varphi\rangle\ *\ [y]_1\}$$

$$\{\left(x \overset{1/2}{\mapsto} |1\rangle\ *\ (y,z) \mapsto |\psi\rangle\,|\varphi\rangle\right)\ *\ \left(x \overset{1/2}{\mapsto} |1\rangle\ *\ [y]_1\right)\}$$

$$\{\left(x \overset{1/2}{\mapsto} |0\rangle\ *\ [y]_1\ *\ z \mapsto |\varphi\rangle\right)\ *\ \left(x \overset{1/2}{\mapsto} |0\rangle\ *\ y \mapsto |\psi\rangle\right)\}$$

$$\mathsf{CCY}[x,z,y];\ U_1[z];\ U_2[z];\ U_3[z];\ \mathsf{CCZ}[x,z,y] \ \parallel\ \mathtt{atomic}\,\{\mathsf{X}[x];\ \mathsf{CH}[x,y];\ \mathsf{X}[x]\}$$

$$\{\left(x \overset{1/2}{\mapsto} |1\rangle\ *\ (y,z) \mapsto \mathsf{CZ}_{zy}\,(\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy}\,(|\psi\rangle\,|\varphi\rangle)\right)\ *\ \left(x \overset{1/2}{\mapsto} |1\rangle\ *\ [y]_1\right)\}$$

$$\left\{\left(x \overset{1/2}{\mapsto} |0\rangle \ast [y]_1 \ast z \mapsto U_+ |\varphi\rangle\right) \ast \left(x \overset{1/2}{\mapsto} |0\rangle \ast y \mapsto \mathsf{H}|\psi\rangle\right)\right\}$$
$$\left\{x \mapsto |1\rangle \ast (y,z) \mapsto \mathsf{CZ}_{zy}\,(\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy}\,(|\psi\rangle|\varphi\rangle)[y]_1\right\}$$
$$\left\{x \mapsto |0\rangle \ast y \mapsto \mathsf{H}|\psi\rangle \ast z \mapsto U_+|\varphi\rangle \ast [y]_1\right\}$$
$$\left\{(x,y,z) \mapsto \mathsf{If}\left(\mathsf{CZ}_{zy}\,(\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy},\ \mathsf{H}\otimes U_+\right)(|\chi\rangle|\psi\rangle|\varphi\rangle) \ast [y]_1\right\}$$

We use the shorthand $U_+ \triangleq U_3U_2U_1$ and define the linear map $\mathsf{If}\,(U_1,U_0)$ by $\mathsf{If}\,(U_1,U_0)\,(|b\rangle|\omega\rangle) \triangleq |b\rangle \cdot U_b|\omega\rangle$ for $b \in \{1,0\}$. The final postcondition says that, regardless of execution scheduling, the final state of the qubits x, y, z is always set to $\mathsf{If}\left(\mathsf{CZ}_{zy}\,(\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy},\ \mathsf{H}\otimes U_+\right)(|\chi\rangle|\psi\rangle|\varphi\rangle)$. By QPTTO-LINCOMB, the verification boils down to the two cases where the qubit x stores $|1\rangle$ (marked green) and $|0\rangle$ (marked blue). Here, $\{P_1\}\{P_2\}\ e\ \{Q_1\}\{Q_2\}$ indicates that both $\{P_1\}\ e\ \{Q_1\}$ and $\{P_2\}\ e\ \{Q_2\}$ hold. Notably, how to split the ownership between two processes in PARALLEL can depend on whether x stores $|1\rangle$ or $|0\rangle$. More concretely, here the full points-to token $y \mapsto |\psi\rangle$ over the qubit y is given to Process 1 if x stores $|1\rangle$ and to Process 2 if x stores $|0\rangle$. This solves Challenge 1. Also, we split the points-to token over the qubit x using fractions.

We can verify Process 1 as follows:

$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast (y,z) \mapsto |\psi\rangle|\varphi\rangle\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast [y]_1 \ast z \mapsto |\varphi\rangle\right\}\ \mathsf{CCY}[x,z,y]$$
$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast (y,z) \mapsto \mathsf{CY}_{zy}\,(|\psi\rangle|\varphi\rangle)\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast [y]_1 \ast z \mapsto |\varphi\rangle\right\}\ U_1[z];U_2[z];U_3[z];$$
$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast (y,z) \mapsto (\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy}\,(|\psi\rangle|\varphi\rangle)\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast [y]_1 \ast z \mapsto U_+|\varphi\rangle\right\}\ \mathsf{CCZ}[x,z,y]$$
$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast (y,z) \mapsto \mathsf{CZ}_{zy}\,(\mathsf{I}\otimes U_+)\,\mathsf{CY}_{zy}\,(|\psi\rangle|\varphi\rangle)\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast [y]_1 \ast z \mapsto U_+|\varphi\rangle\right\}$$

Notably, the qubit token $[y]_1$ suffices for performing $\mathsf{CCX}[x,y,z]$ and $\mathsf{CCY}[x,z,y]$ in the case where x stores $|0\rangle$, as the value of y remains unchanged.

We can verify Process 2 as follows:

$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast [y]_1\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast y \mapsto |\psi\rangle\right\}$$
$$\texttt{atomic}\ \{\ \left\{x \mapsto |1\rangle \ast [y]_1\right\}\left\{x \mapsto |0\rangle \ast y \mapsto |\psi\rangle\right\}\ \mathsf{X}[x];$$
$$\left\{x \mapsto |0\rangle \ast [y]_1\right\}\left\{x \mapsto |1\rangle \ast y \mapsto |\psi\rangle\right\}\ \mathsf{CH}[x,y];$$
$$\left\{x \mapsto |0\rangle \ast [y]_1\right\}\left\{x \mapsto |1\rangle \ast y \mapsto \mathsf{H}|\psi\rangle\right\}\ \mathsf{X}[x];$$
$$\left\{x \mapsto |1\rangle \ast [y]_1\right\}\left\{x \mapsto |0\rangle \ast y \mapsto \mathsf{H}|\psi\rangle\right\}\ \}$$
$$\left\{x \overset{1/2}{\mapsto} |1\rangle \ast [y]_1\right\}\left\{x \overset{1/2}{\mapsto} |0\rangle \ast y \mapsto \mathsf{H}|\psi\rangle\right\}$$

Remarkably, we can *promote* the partial points-to token $x \overset{1/2}{\mapsto} |\chi\rangle$ into the full points-to token $x \mapsto |\chi\rangle$ by exploiting the *atomicity* of `atomic`, because the value of x is restored after applying $\mathsf{X}[x]$ twice. This solves Challenge 2.

6 Future Work

We plan to apply our separation logic to verify more practical quantum programs. We are particularly interested in verifying optimization techniques that involve advanced concurrency, entangled copying, or uncomputation [Bichsel et al. 2020]. Furthermore, we

aim to develop new methods for automatically parallelizing quantum programs via ownership analysis based on our separation logic. Also, future work remains in extending our concurrent quantum separation logic to support measurement. A fundamental challenge is how to extend proof rules like QPTTO-LINCOMB for superposition to that setting. For precise analysis of probabilistic distribution, an approach like outcome separation logic [Zilberstein et al. 2024] may be a good fit.

References

Benjamin Bichsel, Maximilian Baader, Timon Gehr, and Martin T. Vechev. 2020. Silq: a high-level quantum language with safe uncomputation and intuitive semantics. In *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*, Alastair F. Donaldson and Emina Torlak (Eds.). ACM, 286–300. https://doi.org/10.1145/3385412.3386007

Richard Bornat, Cristiano Calcagno, Peter W. O'Hearn, and Matthew J. Parkinson. 2005. Permission accounting in separation logic. In *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2005, Long Beach, California, USA, January 12-14, 2005*, Jens Palsberg and Martín Abadi (Eds.). ACM, 259–270. https://doi.org/10.1145/1040305.1040327

Stephen Brookes and Peter W. O'Hearn. 2016. Concurrent separation logic. *ACM SIGLOG News* 3, 3 (2016), 47–65. https://doi.org/10.1145/2984450.2984457

Stephen D. Brookes. 2004. A Semantics for Concurrent Separation Logic. In *CONCUR 2004 - Concurrency Theory, 15th International Conference, London, UK, August 31 - September 3, 2004, Proceedings (Lecture Notes in Computer Science, Vol. 3170)*, Philippa Gardner and Nobuko Yoshida (Eds.). Springer, 16–34. https://doi.org/10.1007/978-3-540-28644-8_2

Craig Gidney and Martin Ekerå. 2021. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 5 (2021), 433. https://doi.org/10.22331/Q-2021-04-15-433

Thomas Häner, Vadym Kliuchnikov, Martin Roetteler, Mathias Soeken, and Alexander Vaschillo. 2022. QParallel: Explicit Parallelism for Programming Quantum Computers. *CoRR* abs/2210.03680 (2022). https://doi.org/10.48550/ARXIV.2210.03680 arXiv:2210.03680

Xuan-Bach Le, Shang-Wei Lin, Jun Sun, and David Sanán. 2022. A quantum interpretation of separating conjunction for local reasoning of quantum programs based on separation logic. *Proc. ACM Program. Lang.* 6, POPL (2022), 1–27. https://doi.org/10.1145/3498697

Peter W. O'Hearn. 2004. Resources, Concurrency and Local Reasoning. In *CONCUR 2004 - Concurrency Theory, 15th International Conference, London, UK, August 31 - September 3, 2004, Proceedings (Lecture Notes in Computer Science, Vol. 3170)*, Philippa Gardner and Nobuko Yoshida (Eds.). Springer, 49–67. https://doi.org/10.1007/978-3-540-28644-8_4

Bonan Su, Li Zhou, Yuan Feng, and Mingsheng Ying. 2024. BI-based Reasoning about Quantum Programs with Heap Manipulations. arXiv:2409.10153 [quant-ph] https://arxiv.org/abs/2409.10153

Li Zhou, Gilles Barthe, Justin Hsu, Mingsheng Ying, and Nengkun Yu. 2021. A Quantum Interpretation of Bunched Logic & Quantum Separation Logic. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*. IEEE, 1–14. https://doi.org/10.1109/LICS52264.2021.9470673

Noam Zilberstein, Angelina Saliling, and Alexandra Silva. 2024. Outcome Separation Logic: Local Reasoning for Correctness and Incorrectness with Computational Effects. *Proc. ACM Program. Lang.* 8, OOPSLA1 (2024), 276–304. https://doi.org/10.1145/3649821

A Operational Semantics of the Target Quantum Language

Here we present the operational semantics of the target quantum language of § 2.

Transition label. We use the following transition labels in our operational semantics:

$$\mathit{Label} \ni L ::= \texttt{qalloc} = q \mid \texttt{qfree}\, q \mid U[\bar{q}] \mid \texttt{mkref}\, v = \ell \mid !\ell = v \mid \ell \leftarrow v$$

Labeled transition over expressions. Evaluation contexts have the following form:

$$K ::= \cdot \mid op(\bar{v}, K, \bar{e}) \mid \texttt{let}\, x = K\, \texttt{in}\, e \mid \texttt{if}\, K\, \{e_1\}\, \texttt{else}\, \{e_2\} \mid K \parallel e \mid e \parallel K \mid \texttt{qfree}\, K \mid U[\bar{v}, K, \bar{e}] \mid \texttt{mkref}\, K \mid !K \mid K \leftarrow e \mid v \leftarrow K$$

The labeled transition $e \xrightarrow{\bar{L}} e'$ (where $\bar{L} \in \mathit{Label}^*$ is a finite sequence of transition labels) is inductively defined by the following rules:

$$\frac{e \xrightarrow{\bar{L}} e'}{K[e] \xrightarrow{\bar{L}} K[e']} \qquad \frac{op(\bar{v}) = v'}{op(\bar{v}) \to v'} \qquad \texttt{let}\, x = v\, \texttt{in}\, e \to e[v/x]$$

$$\texttt{if}\, b\, \{e_1\}\, \texttt{else}\, \{e_0\} \to e_b \qquad \texttt{while}\, e_1\, \{e_2\} \to \texttt{if}\, e_1\, \{e_2; \texttt{while}\, e_1\, \{e_2\}\}$$

$$v_1 \parallel v_2 \to (v_1, v_2) \qquad \frac{e_1 \xrightarrow{\overline{L_1}} e_2 \xrightarrow{\overline{L_2}} \cdots \xrightarrow{\overline{L_n}} v}{\texttt{atomic}\, \{e_1\} \xrightarrow{\overline{L_1}, \overline{L_2}, \ldots, \overline{L_n}} v}$$

$$\texttt{qalloc} \xrightarrow{\texttt{qalloc} = q} q \qquad \texttt{qfree}\, q \xrightarrow{\texttt{qfree}\, q} () \qquad U[\bar{q}] \xrightarrow{U[\bar{q}]} ()$$

$$\texttt{mkref}\, v \xrightarrow{\texttt{mkref}\, v = \ell} \ell \qquad !\ell \xrightarrow{!\ell = v} v \qquad \ell \leftarrow v \xrightarrow{\ell \leftarrow v} ()$$

Here we use the shorthand $\texttt{if}\, e_1\, \{e_2\} \triangleq \texttt{if}\, e_1\, \{e_2\}\, \texttt{else}\, \{()\}$.

The labeled infinite transition $e \xrightarrow{\vec{L}} \infty$ (where $\vec{L} \in \mathit{Label}^* \cup \mathit{Label}^\omega$ is a *possibly infinite* sequence of transition labels) is defined by the following rules:

$$\frac{e_1 \xrightarrow{\overline{L_1}} e_2 \xrightarrow{\overline{L_2}} \cdots \xrightarrow{\overline{L_{k-1}}} e_k \xrightarrow{\overline{L_k}} \cdots}{K[\texttt{atomic}\, \{e_1\}] \xrightarrow{\overline{L_1}, \overline{L_2}, \ldots, \overline{L_{k-1}}, \overline{L_k}, \ldots} \infty} \qquad \frac{e_1 \xrightarrow{\overline{L_1}} e_2 \xrightarrow{\overline{L_2}} \cdots \xrightarrow{\overline{L_n}} e_{n+1} \xrightarrow{\vec{L'}} \infty}{K[\texttt{atomic}\, \{e_1\}] \xrightarrow{\overline{L_1}, \overline{L_2}, \ldots, \overline{L_n}, \vec{L'}} \infty}$$

Atomicity. We say an expression e is atomic if $e \xrightarrow{\bar{L}} e'$ entails $e' \in \mathit{Val}$ for any expression e' and labels $\bar{L}$. The following rules hold:

$$\texttt{atomic}\, \{e\} \text{ is atomic}$$

$$\texttt{qalloc} \text{ is atomic} \qquad \texttt{qfree}\, v \text{ is atomic} \qquad U[\bar{v}] \text{ is atomic}$$

$$\texttt{mkref}\, v \text{ is atomic} \qquad !v \text{ is atomic} \qquad v \leftarrow v' \text{ is atomic}$$

Labeled transition over global states. The global state we consider is as follows:

$$\textbf{Quantum memory} \quad M = (qs, |\psi\rangle) \in \mathit{Qmem} \triangleq \coprod_{qs \in \mathrm{Pow}_{\mathrm{fin}}\, \mathit{Qname}} \left(\mathbb{C}^2\right)^{\otimes qs}$$

$$\textbf{Heap memory} \quad H \in \mathit{Heap} \triangleq \mathit{Loc} \xrightarrow{\mathrm{fin}} \mathit{Val}$$

$$\textbf{Global state} \quad G = (M, H) \in \mathit{Glob} \triangleq \mathit{Qmem} \times \mathit{Heap}$$

The labeled global state transition $G \xrightarrow{L} G'$ is defined by the following rules:

$$\frac{q \notin qs}{\big((qs, |\psi\rangle), H\big) \xrightarrow{\texttt{qalloc} = q} \big((qs \cup \{q\}, |\psi\rangle_{qs} \otimes |0\rangle_q), H\big)}$$

$$\frac{q \notin qs}{\big((qs \cup \{q\}, |\psi\rangle_{qs} \otimes |0\rangle_q), H\big) \xrightarrow{\texttt{qfree}\, q} \big((qs, |\psi\rangle), H\big)}$$

$$\frac{\bar{q} \text{ are pairwise distinct} \qquad \{\bar{q}\} \cap qs \neq \emptyset}{\big((\{\bar{q}\} \cup qs, |\psi\rangle), H\big) \xrightarrow{U[\bar{q}]} \big((\{\bar{q}\} \cup qs, U_{\bar{q}}\,|\psi\rangle), H\big)}$$

$$\frac{\ell \notin \operatorname{dom} H}{(M, H) \xrightarrow{\texttt{mkref}\, v = \ell} (M, H\{\ell \coloneqq v\})}$$

$$\frac{\ell \in \operatorname{dom} H \qquad v = H[\ell]}{(M, H) \xrightarrow{!\ell = v} (M, H)} \qquad \frac{\ell \in \operatorname{dom} H}{(M, H) \xrightarrow{\ell \leftarrow v} (M, H\{\ell \coloneqq v\})}$$

Expression-state transition. The expression-state transition $(e, G) \to (e', G')$ is defined by the following rule:

$$\frac{e \xrightarrow{L_1, L_2, \cdots, L_n} e' \qquad G_1 \xrightarrow{L_1} G_2 \xrightarrow{L_2} \cdots \xrightarrow{L_n} G_{n+1}}{(e, G_1) \to (e', G_{n+1})}$$

The expression-state infinite transition $(e, G) \to \infty$ is defined by the following rule:

$$\frac{e \xrightarrow{L_1, L_2, \ldots, L_{k-1}, L_k, \ldots} \infty \qquad G_1 \xrightarrow{L_1} G_2 \xrightarrow{L_2} \cdots \xrightarrow{L_{k-1}} G_k \xrightarrow{L_k} \cdots}{(e, G_1) \to \infty}$$

The reducibility $\mathsf{red}(e, G)$ is defined by the following rule:

$$\frac{(e, G) \to (e', G')}{\mathsf{red}(e, G)} \qquad \frac{(e, G) \to \infty}{\mathsf{red}(e, G)}$$

B Proof Rules of Our Separation Logic

Judgments. We use the following judgments:

$$P \vdash Q \qquad \{P\}\ e\ \{v.\ Q_v\} \qquad P : \text{out}\ a$$

As usual, we introduce the entailment judgment $P \vdash Q$ and the (partial) Hoare triple $\{P\}\ e\ \{v.\ Q_v\}$ (where v is the return value of the execution). We also introduce the ownership exclusion judgment $P : \text{out}\ a$, meaning that a proposition $P \in \mathit{SLProp}$ does not own a qubit or location $a \in \mathit{Qname} \cup \mathit{Loc}$.

We use the following syntax sugar:

$$P \dashv\vdash Q \triangleq (P \vdash Q) \wedge (Q \vdash P) \qquad \{P\}\ e\ \{Q\} \triangleq \{P\}\ e\ \{\_.\ Q\}$$

$$P : \text{out}\ \bar{a} \triangleq \forall i.\ (P : \text{out}\ a_i)$$

General proof rules.

$$P \vdash P \qquad \frac{P \vdash Q \quad Q \vdash R}{P \vdash R} \qquad \frac{p \text{ holds}}{P \vdash p} \qquad \frac{P \vdash p \quad p \text{ implies } P \vdash Q}{P \vdash Q}$$

$$P_1 \wedge P_2 \vdash P_i \qquad \frac{R \vdash P \quad R \vdash Q}{R \vdash P \wedge Q} \qquad P_i \vdash P_1 \vee P_2 \qquad \frac{P \vdash R \quad Q \vdash R}{P \vee Q \vdash R}$$

$$(P \to Q) \wedge P \vdash Q \qquad \frac{P \wedge Q \vdash R}{P \vdash Q \to R}$$

$$(\forall x.\, P_x) \vdash P_a \qquad \frac{\forall x.\, (Q \vdash P_x)}{Q \vdash \forall x.\, P_x} \qquad P_a \vdash (\exists x.\, P_x) \qquad \frac{\forall x.\, (P_x \vdash Q)}{(\exists x.\, P_x) \vdash Q}$$

$$\frac{P \vdash Q}{P * R \vdash Q * R} \qquad P * \mathsf{emp} \dashv\vdash P \qquad P * Q \dashv\vdash Q * P \qquad (P * Q) * R \dashv\vdash P * (Q * R)$$

$$(P \mathrel{-\!\!*} Q) * P \vdash Q \qquad \frac{P * Q \vdash R}{P \vdash Q \mathrel{-\!\!*} R}$$

Basic Hoare-triple proof rules.

$$\frac{P' \vdash P \quad \{P\}\ e\ \{v.\, Q_v\} \quad \forall v.\ (Q_v \vdash Q'_v)}{\{P'\}\ e\ \{v.\, Q'_v\}} \qquad \frac{\{P\}\ e\ \{v.\, Q_v\}}{\{P * R\}\ e\ \{v.\, Q_v * R\}}$$

$$\{\bot\}\ e\ \{v.\, Q_v\} \qquad \frac{\forall x.\ \{P_x\}\ e\ \{v.\, Q_v\}}{\{\exists x.\, P_x\}\ e\ \{v.\, Q_v\}}$$

$$\frac{\{P\}\ e\ \{v.\, Q_v\} \quad \forall v.\ \{Q_v\}\ K[v]\ \{v'.\, R_{v'}\}}{\{P\}\ K[e]\ \{v'.\, R_{v'}\}} \qquad \frac{\{P\}\ e[v/x]\ \{v'.\, Q_{v'}\}}{\{P\}\ \mathtt{let}\ x = v\ \mathtt{in}\ e\ \{v'.\, Q_{v'}\}}$$

$$\frac{\{P\}\ e_b\ \{v.\, Q_v\}}{\{P\}\ \mathtt{if}\ b\ \{e_1\}\ \mathtt{else}\ \{e_0\}\ \{v.\, Q_v\}} \qquad \frac{\{P\}\ e_1\ \{b.\, Q_b\} \quad \{Q_1\}\ e_2\ \{P\}}{\{P\}\ \mathtt{while}\ e_1\ \{e_2\}\ \{v.\, Q_0\}}$$

Basic proof rules for concurrency.

$$\frac{\{P\}\ e\ \{v.\, Q_v\} \quad \{P'\}\ e'\ \{v'.\, Q'_{v'}\}}{\{P * P'\}\ e \parallel e'\ \{(v, v').\, Q_v * Q'_{v'}\}}\ \textsc{parallel} \qquad \frac{\{P\}\ e\ \{v.\, Q_v\}}{\{P\}\ \mathtt{atomic}\ \{e\}\ \{v.\, Q_v\}}\ \textsc{atomic}$$

Rules for exactness.

$$\mathsf{emp} : \mathsf{exact} \qquad \frac{P, Q : \mathsf{exact}}{P * Q : \mathsf{exact}} \qquad \frac{P : \mathsf{exact} \quad Q \vdash P}{Q : \mathsf{exact}}$$

$$\bar{q} \overset{r}{\mapsto} |\psi\rangle : \mathsf{exact} \qquad [q]_r : \mathsf{exact} \qquad \ell \overset{r}{\mapsto} v : \mathsf{exact}$$

Rules for quantum and heap ownership exclusion.

$$\mathsf{emp} : \mathsf{out}\ a \qquad \frac{P, Q : \mathsf{out}\ a}{P \vee Q, P * Q : \mathsf{out}\ a} \qquad \frac{\forall x.\ (P_x : \mathsf{out}\ a)}{(\exists x.\, P_x) : \mathsf{out}\ a} \qquad \frac{P : \mathsf{out}\ a \quad Q \vdash P}{Q : \mathsf{out}\ a}$$

$$\bar{q} \overset{r}{\mapsto} |\psi\rangle, [q]_r : \mathsf{out}\ \ell \qquad \frac{q \notin \{\bar{q}'\}}{\bar{q}' \overset{r}{\mapsto} |\psi\rangle : \mathsf{out}\ q} \qquad \frac{q \neq q'}{[q']_r : \mathsf{out}\ q}$$

$$\ell \overset{r}{\mapsto} v : \mathsf{out}\ q \qquad \frac{\ell \neq \ell'}{\ell' \overset{r}{\mapsto} v : \mathsf{out}\ \ell}$$

Basic proof rules for quantum ownership.

$$(\bar{q}, \bar{q}') \mapsto |\psi\rangle\,|\psi'\rangle \dashv\vdash \bar{q} \mapsto |\psi\rangle * \bar{q}' \mapsto |\psi'\rangle \quad \textsc{qptto-tensor}$$

$$\bar{q} \overset{r+r'}{\mapsto} |\psi\rangle \dashv\vdash \bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q} \overset{r'}{\mapsto} |\psi\rangle$$

$$\bar{q} \overset{r}{\mapsto} |\psi\rangle \vdash (\bar{q} \text{ are pairwise distinct}) \wedge r \leq 1$$

$$\frac{\{\bar{q}\} \cap \{\bar{q}'\} \neq \varnothing}{\bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q}' \overset{r'}{\mapsto} |\psi'\rangle \vdash \bar{q} = \bar{q}' \wedge |\psi\rangle = |\psi'\rangle} \quad \textsc{qptto-agree}$$

$$(q_{\sigma(1)}, q_{\sigma(2)}, \ldots, q_{\sigma(n)}) \overset{r}{\mapsto} \ulcorner\sigma\urcorner\,|\psi\rangle \dashv\vdash (q_1, q_2, \ldots, q_n) \overset{r}{\mapsto} |\psi\rangle \quad \textsc{qptto-permute}$$

$$[q]_{r+r'} \dashv\vdash [q]_r * [q]_{r'} \qquad [q]_r \vdash r \leq 1$$

$$\{\mathsf{emp}\}\ \mathtt{qalloc}\ \{q.\ q \mapsto |0\rangle * [q]_1\} \qquad \{q \mapsto |0\rangle * [q]_1\}\ \mathtt{qfree}\ q\ \{\mathsf{emp}\}$$

$$\{(\bar{q}, \bar{q}') \mapsto |\psi\rangle\}\ U[\bar{q}]\ \{(\bar{q}, \bar{q}') \mapsto (U_{\bar{q}} \otimes \mathsf{I}_{\bar{q}'})\,|\psi\rangle\}$$

The rule QPTTO-TENSOR cannot be applied to fractional points-to tokens, because that would violate the agreement rule QPTTO-AGREE, due to tensor decomposition $|\varphi\rangle = |\psi\rangle\,|\psi'\rangle$ of a vector $|\varphi\rangle$ not being unique. In the rule QPTTO-PERMUTE, σ is a permutation (bijective map) over $\{1, 2, \ldots, n\}$ and $\ulcorner\sigma\urcorner$ denotes the permutation matrix over $(\mathbb{C}^2)^{\otimes n}$ mapping $|b_1 b_2 \cdots b_n\rangle$ to $\left|b_{\sigma(1)} b_{\sigma(2)} \cdots b_{\sigma(n)}\right\rangle$ (where $b_i \in \{0, 1\}$).

Proof rules for heap ownership.

$$\ell \overset{r+r'}{\mapsto} v \dashv\vdash \ell \overset{r}{\mapsto} v * \ell \overset{r'}{\mapsto} v \qquad \ell \overset{r}{\mapsto} v \vdash r \leq 1$$

$$\{\mathsf{emp}\}\ \mathtt{mkref}\ v\ \{\ell.\ \ell \mapsto v\}$$

$$\{\ell \overset{r}{\mapsto} v\}\ !\ell\ \{v'.\ v = v' \wedge \ell \overset{r}{\mapsto} v\} \qquad \{\ell \mapsto v\}\ \ell \leftarrow v'\ \{\ell \mapsto v'\}$$

Proof rules for quantum superposition.

$$\frac{\{\bar{q} \mapsto |\psi\rangle * P\}\ e\ \{\bar{q} \mapsto |\varphi\rangle * Q\} \quad \{\bar{q} \mapsto |\psi'\rangle * P\}\ e\ \{\bar{q} \mapsto |\varphi'\rangle * Q\} \quad P, Q : \mathsf{exact}}{\{\bar{q} \mapsto (\alpha\,|\psi\rangle + \beta\,|\psi'\rangle) * P\}\ e\ \{\bar{q} \mapsto (\alpha\,|\varphi\rangle + \beta\,|\varphi'\rangle) * Q\} \quad P, Q : \mathsf{exact}}$$

QPTTO-LINCOMB

$$\frac{\begin{array}{c} P : \mathsf{out}\ \bar{q} \qquad P, Q : \mathsf{exact} \\ \{\bar{q} \overset{r}{\mapsto} |\psi\rangle * P\}\ e\ \{\bar{q} \overset{r}{\mapsto} |\psi\rangle * Q\} \quad \{\bar{q} \overset{r}{\mapsto} |\psi'\rangle * P\}\ e\ \{\bar{q} \overset{r}{\mapsto} |\psi'\rangle * Q\} \end{array}}{\{\bar{q} \overset{r}{\mapsto} (\alpha\,|\psi\rangle + \beta\,|\psi'\rangle) * P\}\ e\ \{\bar{q} \overset{r}{\mapsto} (\alpha\,|\psi\rangle + \beta\,|\psi'\rangle) * Q\}}$$

FRQPTTO-LINCOMB

Proof rules for modifying fractional quantum points-to tokens.

$$\frac{\left\{\bar{q} \overset{r}{\mapsto} |\psi\rangle * P\right\}\ e\ \left\{v.\ \bar{q} \overset{r}{\mapsto} |\psi\rangle * Q_v\right\} \qquad P : \mathrm{out}\ \bar{q} \qquad r < 1}{\left\{\bar{q} \overset{r'}{\mapsto} |\psi\rangle * P\right\}\ e\ \left\{v.\ \bar{q} \overset{r'}{\mapsto} |\psi\rangle * Q_v\right\}}$$

$$\frac{\left\{\bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q}' \overset{r}{\mapsto} |\psi'\rangle * P\right\}\ e\ \left\{v.\ \bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q}' \overset{r}{\mapsto} |\psi'\rangle * Q_v\right\} \qquad P : \mathrm{out}\ \bar{q}, \bar{q}'}{\left\{(\bar{q}, \bar{q}') \overset{r}{\mapsto} |\psi\rangle\,|\psi'\rangle * P\right\}\ e\ \left\{v.\ (\bar{q}, \bar{q}') \overset{r}{\mapsto} |\psi\rangle\,|\psi'\rangle * Q_v\right\}}$$

$$\frac{\left\{(\bar{q}, \bar{q}') \overset{r}{\mapsto} |\psi\rangle\,|\psi'\rangle * P\right\}\ e\ \left\{v.\ (\bar{q}, \bar{q}') \overset{r}{\mapsto} |\psi\rangle\,|\psi'\rangle * Q_v\right\} \qquad P : \mathrm{out}\ \bar{q}, \bar{q}'}{\left\{\bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q}' \overset{r}{\mapsto} |\psi'\rangle * P\right\}\ e\ \left\{v.\ \bar{q} \overset{r}{\mapsto} |\psi\rangle * \bar{q}' \overset{r}{\mapsto} |\psi'\rangle * Q_v\right\}}$$

Proof rules for promotion by atomicity.

$$\frac{e \text{ is atomic} \qquad P : \mathrm{out}\ \bar{q} \qquad \left\{\bar{q} \mapsto |\psi\rangle * [\bar{q}]_1 * P\right\}\ e\ \left\{v.\ \bar{q} \mapsto |\psi\rangle * [\bar{q}]_1 * Q_v\right\}}{\left\{\bar{q} \overset{r}{\mapsto} |\psi\rangle * P\right\}\ e\ \left\{v.\ \bar{q} \overset{r}{\mapsto} |\psi\rangle * Q_v\right\}}\ \textsc{qptto-promote}$$

$$\frac{e \text{ is atomic} \qquad P : \mathrm{out}\ q \qquad \forall\, |\psi\rangle.\ \left\{q \mapsto |\psi\rangle * [q]_1 * P\right\}\ e\ \left\{v.\ q \mapsto |\psi\rangle * [q]_1 * Q_v\right\}}{\left\{[q]_r * P\right\}\ e\ \left\{v.\ [q]_r * Q_v\right\}}\ \textsc{qtok-promote}$$

$$\frac{e \text{ is atomic} \qquad P : \mathrm{out}\ \ell \qquad \left\{\ell \mapsto v * P\right\}\ e\ \left\{v'.\ \ell \mapsto v * Q_{v'}\right\}}{\left\{\ell \overset{r}{\mapsto} v * P\right\}\ e\ \left\{v'.\ \ell \overset{r}{\mapsto} v * Q_{v'}\right\}}\ \textsc{hptto-promote}$$

C Semantic Model of Our Separation Logic

Here we present the semantic model of our separation logic presented in § 4.

Heap PCM. The heap PCM (partial commutative monoid) Heap is defined in a standard way:

$$|\textsc{Heap}| \triangleq \mathit{Loc} \overset{\mathsf{fin}}{\rightharpoonup} (0, 1] \times \mathit{Val} \qquad \varepsilon_{\textsc{Heap}} \triangleq \varnothing$$

$$\hat{H} \cdot_{\textsc{Heap}} \hat{H}' \triangleq \lambda\, \ell \in \mathrm{dom}\, \hat{H} \cup \mathrm{dom}\, \hat{H}'.\ \begin{cases} \hat{H}[\ell] & \ell \notin \mathrm{dom}\, \hat{H}' \\ \hat{H}'[\ell] & \ell \notin \mathrm{dom}\, \hat{H} \\ \hat{H}[\ell] \cdot \hat{H}[\ell'] & \text{otherwise} \end{cases}$$

$$\text{where} \quad (q, v) \cdot (q', v') \triangleq \begin{cases} (q + q', v) & q + q' \le 1,\ v = v' \\ \text{undefined} & \text{otherwise} \end{cases}$$

The lifting $\ulcorner H \urcorner \in |\textsc{Heap}|$ of a heap $H \in \mathit{Heap}$ into a heap PCM element is defined as follows:

$$\ulcorner H \urcorner \triangleq \lambda\, \ell \in \mathrm{dom}\, H.\ (1, H[\ell])$$

Quantum memory PCM. The qubit token PCM Qtok is defined as follows:

$$|\textsc{Qtok}| \triangleq \mathit{Qname} \overset{\mathsf{fin}}{\rightharpoonup} [0, 1] \qquad \varepsilon_{\textsc{Qtok}} \triangleq \lambda\_.\ 0$$

$$R \cdot_{\text{QTOK}} R' \triangleq \lambda q. \begin{cases} R\,q + R'\,q & R\,q + R'\,q \le 1 \\ \text{undefined} & \text{otherwise} \end{cases}$$

Here, by $\xrightarrow{\text{fin}}$, we mean a finite-support mapping. For any $R \in |\text{QTOK}|$, the support $\operatorname{supp} R \triangleq \{q \in \mathit{Qname} \mid R\,q \neq 0\}$ is a finite set.

The quantum points-to token PCM QPTTO is defined as follows:

$$|\text{QPTTO}| \triangleq \coprod_{qs \in \mathsf{Pow}_{\mathsf{fin}} \mathit{Qname}} \left(\mathbb{C}^2\right)^{\otimes qs} \times \coprod_{qss \in \mathit{QnamePart}\ qs} (0,1)^{qss} \times \prod_{qs' \in qss} \left(\mathbb{C}^2\right)^{\otimes qs'}$$

$$\text{where}\quad \mathit{QnamePart}\ qs \triangleq \left\{ \{\overline{qs}'\} \in \mathsf{Pow}_{\mathsf{fin}} \mathsf{Pow}_{\mathsf{fin}} \mathit{Qname} \;\middle|\; qs, \overline{qs}' \text{ are pairwise disjoint} \right\}$$

$$\varepsilon_{\text{QPTTO}} \triangleq (\varnothing, 1, \varnothing, \varnothing, \varnothing)$$

$$(qs, |\psi\rangle, qss, R, F) \cdot_{\text{QPTTO}} (qs', |\psi'\rangle, qss', R', F') \triangleq$$

$$\begin{cases} \mathsf{normal}_{\text{QPTTO}}\big(qs \cup qs',\ |\psi\rangle \otimes |\psi'\rangle,\ qss \cup qss',\ (\lambda qs_+.\ R\,qs_+ + R'\,qs_+),\ F \cup F'\big) & \begin{array}{l} qs, qs', (qss \cup qss')\text{'s elements} \\ \quad \text{are pairwise disjoint,} \\ F|_{qss \cap qss'} = F'|_{qss \cap qss'}, \\ \forall qs_+.\ R\,qs_+ + R'\,qs_+ \le 1 \end{array} \\ \text{undefined} & \text{otherwise} \end{cases}$$

$$\text{where}\quad \mathsf{normal}_{\text{QPTTO}}(qs, |\psi\rangle, qss, R, F) \triangleq \text{let } qss' = \{qs' \in qss \mid R\,qs' = 1\} \text{ in}$$
$$\left(qs \cup \bigcup qss',\ |\psi\rangle \otimes \bigotimes_{qs' \in qss'} F\,qs',\ qss \setminus qss',\ R|_{qss \setminus qss'},\ F|_{qss \setminus qss'}\right)$$

Here we introduce the function $\mathsf{normal}_{\text{QPTTO}}$ to normalize the state by clearing parts of the full fraction. In the definition of $\cdot_{\text{QPTTO}}$, the application $R\,qs_+$ is defined as 0 if $qs_+ \notin \operatorname{dom} R$. We write $\dot{M}$ for elements of $|\text{QPTTO}|$.

The quantum memory PCM QMEM is defined as the product of the quantum points-to token PCM and the qubit token PCM:

$$\text{QMEM} \triangleq \text{QPTTO} \times \text{QTOK}$$

We write $\hat{M}$ for elements of $|\text{QMEM}|$. The lifting $\ulcorner M \urcorner \in |\text{QMEM}|$ of a quantum memory $M \in \mathit{Qmem}$ into a quantum memory PCM element is defined as follows:

$$\ulcorner M \urcorner \triangleq \left((qs, |\psi\rangle, \varnothing, \varnothing, \varnothing),\ \lambda q.\ \text{if } q \in qs \text{ then } 1 \text{ else } 0\right)$$

Global state PCM. The global state PCM is the product of the heap PCM and quantum memory PCM:

$$\text{GLOB} \triangleq \text{QMEM} \times \text{HEAP}$$

We write $\hat{G}$ for elements of $|\text{GLOB}|$. The lifting $\ulcorner G \urcorner \in |\text{GLOB}|$ of a global state $G \in \mathit{Glob}$ into a global state PCM element is defined as follows:

$$\ulcorner (M, H) \urcorner \triangleq \left(\ulcorner M \urcorner, \ulcorner H \urcorner\right)$$

Propositions. We interpret a proposition $P \in \mathit{SLProp}$ as a predicate over the global PCM $[\![P]\!] : |\text{GLOB}| \to \mathit{Prop}$ as follows:

$$[\![p]\!]\,\_ \triangleq p \qquad [\![P \wedge Q]\!]\,\hat{G} \triangleq [\![P]\!]\,\hat{G} \wedge [\![Q]\!]\,\hat{G}$$

$$[\![P \vee Q]\!]\,\hat{G} \triangleq [\![P]\!]\,\hat{G} \vee [\![Q]\!]\,\hat{G} \qquad [\![P \to Q]\!]\,\hat{G} \triangleq [\![P]\!]\,\hat{G} \to [\![Q]\!]\,\hat{G}$$

$$[\![\forall x.\, P_x]\!]\,\hat{G} \triangleq \forall x.\, [\![P_x]\!]\,\hat{G} \qquad [\![\exists x.\, P_x]\!]\,\hat{G} \triangleq \exists x.\, [\![P_x]\!]\,\hat{G}$$

$$[\![\mathsf{emp}]\!]\,\hat{G} \triangleq \hat{G} = \varepsilon \qquad [\![P * Q]\!]\,\hat{G} \triangleq \exists \hat{G}_1, \hat{G}_2.\ \hat{G} = \hat{G}_1 \cdot \hat{G}_2 \wedge [\![P]\!]\,\hat{G}_1 \wedge [\![Q]\!]\,\hat{G}_2$$

$$[\![P \mathrel{-\!\!*} Q]\!]\,\hat{G} \triangleq \forall \hat{G}' \text{ s.t. } \hat{G} \cdot \hat{G}' \downarrow .\ [\![P]\!]\,\hat{G}' \to [\![Q]\!]\,(\hat{G} \cdot \hat{G}')$$

$$[\![\bar{q} \overset{r}{\mapsto} |\psi\rangle]\!]\,((\dot{M}, R), \hat{H}) \triangleq R = \varepsilon \wedge \hat{H} = \varepsilon \wedge (\bar{q} \text{ are pairwise distinct}) \wedge r \le 1 \wedge \dot{M} = \mathrm{qptto}^r\big(\{\bar{q}\}, \ulcorner \bar{q} \urcorner\, |\psi\rangle\big)$$

$$\text{where} \quad \mathrm{qptto}^r(qs, |\psi\rangle) \triangleq \begin{cases} (qs, |\psi\rangle, \varnothing, \varnothing, \varnothing) & r = 1 \\ \big(\varnothing, 1, \{qs\}, (\lambda\_.\, r), (\lambda\_.\, |\psi\rangle)\big) & r < 1 \end{cases}$$

$$[\![[q]_r]\!]\,((\dot{M}, R), \hat{H}) \triangleq \dot{M} = \varepsilon \wedge \hat{H} = \varepsilon \wedge R\,q = r \wedge \forall q' \neq q.\ R\,q' = 0$$

$$[\![\ell \overset{r}{\mapsto} v]\!]\,(\hat{M}, \hat{H}) \triangleq \hat{M} = \varepsilon \wedge \hat{H} = \{(\ell, (r, v))\}$$

In the semantics of $\bar{q} \overset{r}{\mapsto} |\psi\rangle$, we write $\ulcorner \bar{q} \urcorner$ for the linear map that maps $|b_1 b_2 \cdots b_n\rangle$ to $|\{q_i \mapsto b_i \mid i\}\rangle$, under the condition that $\bar{q} = q_1, q_2, \ldots, q_n$ are pairwise distinct.

Basic judgments. The entailment judgment is interpreted as follows, as usual:

$$[\![P \vdash Q]\!] \triangleq \forall \hat{G}.\ [\![P]\!]\,\hat{G} \to [\![Q]\!]\,\hat{G}$$

The exactness judgment is interpreted as follows:

$$[\![P : \mathrm{exact}]\!] \triangleq \forall \hat{G} \text{ s.t. } [\![P]\!]\,\hat{G}.\ \forall \hat{G}' \text{ s.t. } [\![P]\!]\,\hat{G}'.\ \hat{G} = \hat{G}'$$

The ownership exclusion judgment is interpreted as follows:

$$[\![P : \mathrm{out}\ q]\!] \triangleq \forall \hat{M}, \hat{H}.\ [\![P]\!]\,(\hat{M}, \hat{H}) \to q \notin \mathrm{dom}\,\hat{M}$$

$$[\![P : \mathrm{out}\ \ell]\!] \triangleq \forall \hat{M}, \hat{H}.\ [\![P]\!]\,(\hat{M}, \hat{H}) \to \ell \notin \mathrm{dom}\,\hat{H}$$

Here, we define $\mathrm{dom}\,\hat{M} \subseteq \mathit{Qname}$ as follows:

$$\mathrm{dom}\big((qs, |\psi\rangle, qss, R', F), R\big) \triangleq qs \cup \bigcup qss \cup \mathrm{supp}\,R$$

Hoare triple. The Hoare triple $\{P\}\ e\ \{v.\ Q_v\}$ is interpreted as follows:

$$[\![\{P\}\ e\ \{v.\ Q_v\}]\!] \triangleq \forall \hat{G}.\ [\![P]\!]\,\hat{G} \to \mathrm{Hoare}\big(e, \hat{G}, \lambda v.\, [\![Q_v]\!]\big)$$

Here, the predicate $\mathrm{Hoare} : \mathit{Exp} \times |\textsc{Glob}| \times (\mathit{Val} \to |\textsc{Glob}| \to \mathit{Prop}) \to \mathit{Prop}$ is coinductively defined as follows:

$$\mathrm{Hoare}(e, \hat{G}, \Phi) \triangleq_\nu \big(e \in \mathit{Val} \wedge \Phi\, e\, \hat{G}\big) \vee \forall G, \hat{G}_+ \text{ s.t. } \ulcorner G \urcorner = \hat{G} \cdot \hat{G}_+.\ \mathrm{red}(e, G) \wedge \forall (e', G') \leftarrow (e, G).\ \exists \hat{G}' \text{ s.t. } \ulcorner G' \urcorner = \hat{G}' \cdot \hat{G}_+.\ \mathrm{Hoare}(e', \hat{G}', \Phi)$$