Concurrent Quantum Separation Logic for Fine-Grained Parallelism

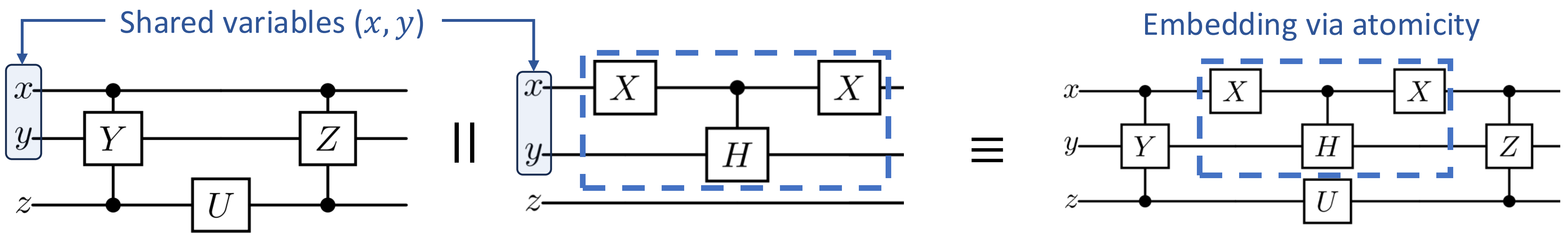
Yusuke Matsushita (Kyoto University)
w/ Kengo Hirata and Ryo Wakizaka

21th January, 2025 @ TPSA 2025

Overview of Our Work

We propose **concurrent quantum separation logic** for **modularly** verifying quantum programs with fine-grained parallelism

- Compared to existing quantum SLs [Zhou+ LICS'21] [Le+ POPL'22], our logic is the first to support concurrency and the sharing of quantum resources, and can verify non-trivial programs



Outline

- **Preliminaries on Quantum Computing**
- Motivation: Parallelizing Quantum Programs
- Our Work: Concurrent QSL for Fine-Grained Parallelism
- Extension to Probabilistic Reasoning & Conclusion

Basics of Quantum Computing

- State for a ***qubit (quantum bit)*** = *2D vector* $|\psi\rangle \in \mathbb{C}^2$

  Superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$

- State for ***n*** qubits = Vector of *tensor product* space $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$
  - Composite of $|\psi\rangle$ and $|\phi\rangle$ = *Tensor product* $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle$

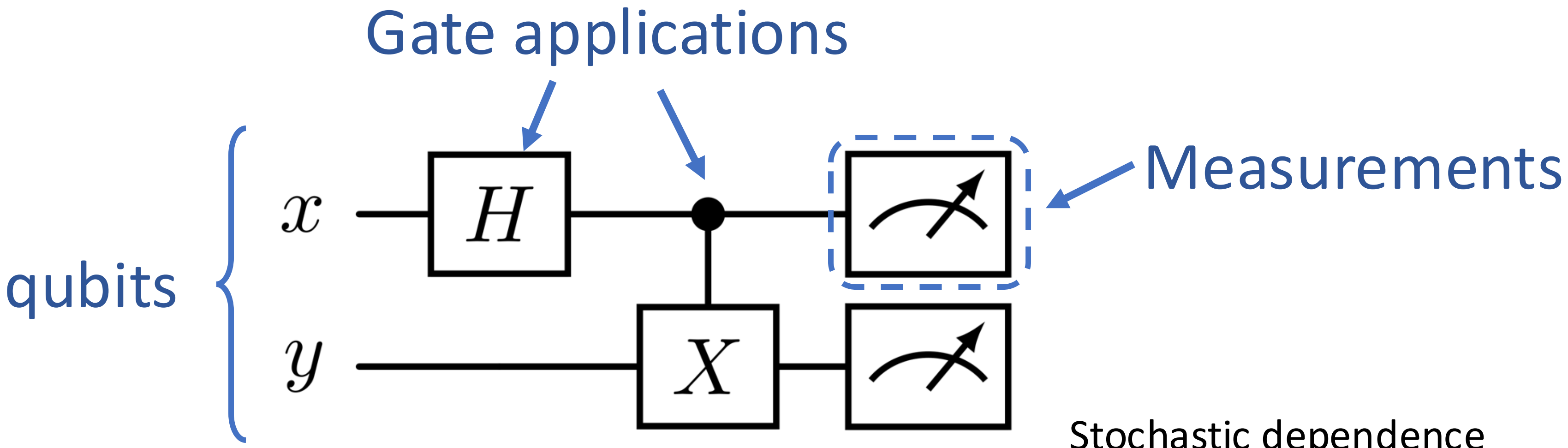
- ***Quantum gate*** = *Unitary matrix* $U : \mathcal{H} \to \mathcal{H}$

  e.g., $\underbrace{H|b\rangle}_{\text{Hadamard}} = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b|1\rangle\right) \quad \underbrace{CX|b\rangle|c\rangle}_{\text{Controlled X}} = |b\rangle|b \text{ xor } c\rangle \quad b, c \in \{0,1\}$

- ***Measurement*** = *Probabilistic branching & convergence*

$$\alpha|0\rangle + \beta|1\rangle \to \begin{cases} |0\rangle & (w.p. \ \ |\alpha|^2) \\ |1\rangle & (w.p. \ \ |\beta|^2) \end{cases}$$

Quantum Program (Circuit)



Stochastic dependence

$$x, y \mapsto |00\rangle \to |+\rangle|0\rangle \to \underline{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)} \to \begin{cases} |00\rangle & (w.p.\ 1/2) \\ |11\rangle & (w.p.\ 1/2) \end{cases}$$

$$|\pm\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

Entangled state

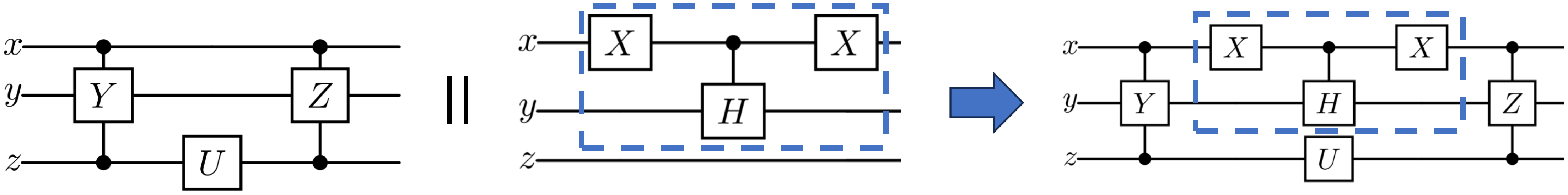
x and y are entangled $\Leftrightarrow$ $x, y \mapsto |\psi\rangle$ such that $\forall |\phi\rangle, |\phi'\rangle.\ |\psi\rangle \neq |\phi\rangle \otimes |\phi'\rangle$

Outline

- Preliminaries on Quantum Computing
- **Motivation: Parallelizing Quantum Programs**
- Our Work: Concurrent QSL for Fine-Grained Parallelism
- Extension to Probabilistic Reasoning & Conclusion

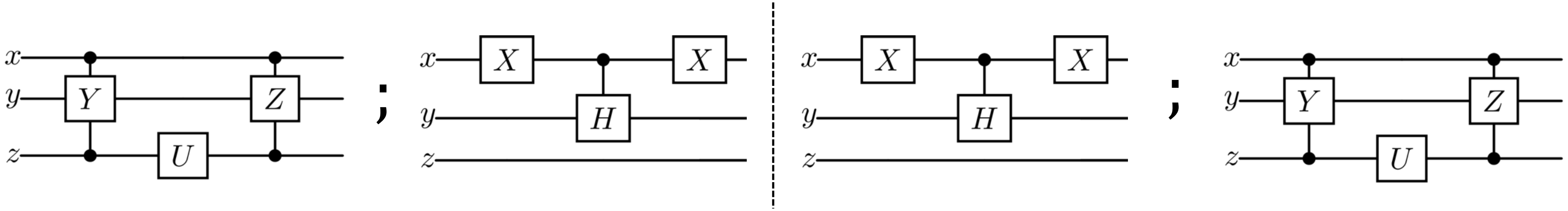
Parallelizing Quantum Programs

- Parallelizing quantum programs can reduce execution costs



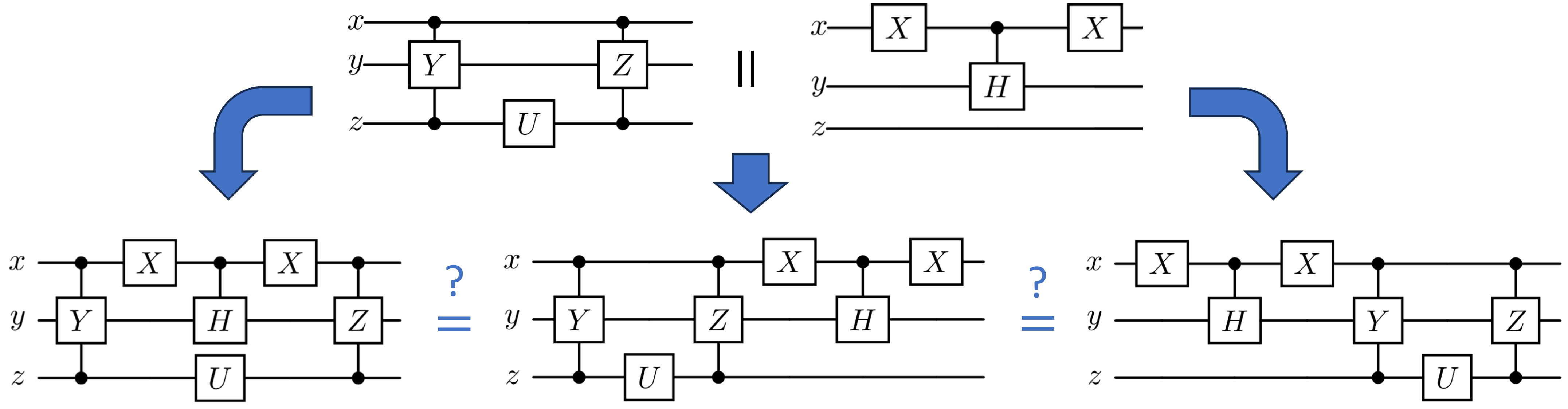
Clever scheduling

- Other candidates



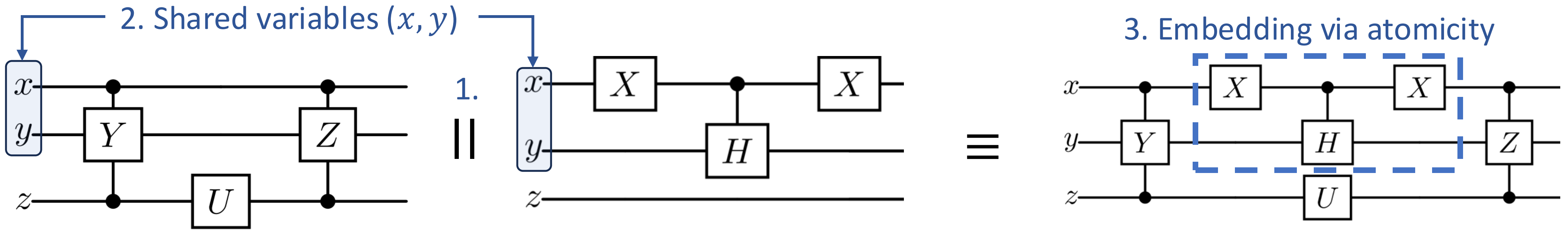
Correctness of Parallelization

- Parallelization allows exponentially many execution traces!
- Need a **modular** program logic for parallel quantum programs
  - Correctness of a parallel program ≈ **Uniqueness of the output**



Our Work: Concurrent Quantum Separation Logic for Fine-Grained Parallelism

1. **Support parallel execution of quantum processes**
2. **Support shared quantum variables**
   - Even when there are apparent write-write races
3. **Support atomic expressions**
   - For non-interfered embedding of quantum circuits



Outline

- Preliminaries on Quantum Computing
- Motivation: Parallelizing Quantum Programs
- **Our Work: Concurrent QSL for Fine-Grained Parallelism**
- Extension to Probabilistic Reasoning & Conclusion

Our Target Language

$e ::= x \mid l \mid n \mid (\,) \mid op(\bar{e})$

| qalloc (qubit allocation)

| qfree e (qubit deallocation)

| $U(\bar{e})$ (quantum gate)

| meas(e) (qubit measurement)

Quantum

| $e \mid\mid e'$ (parallel execution)

| atomic { e } (atomic block)

Concurrency

| $!e \mid e \leftarrow e' \mid \cdots$ (heap)

| if e { e'} else { e''} | while e { e'} $\mid \cdots$

Overview of Our Logic

Invariant

$$\{P\}\, e\, \{v.\, Q\}^{I}$$

$$\{P\}\, e\, \{v.\, Q\} \triangleq \{P\}\, e\, \{v.\, Q\}^{\mathrm{emp}}$$

$$\begin{aligned} P ::= {} & \top \mid \bot \mid \neg P \mid P \wedge Q \mid P \vee Q \\ & \mid P \to Q \mid \forall a.\, P_a \mid \exists a.\, P_a \\ & \mid \mathrm{emp} \mid P * Q \mid P -\!\!* \; Q \\ & \mid l \mapsto v \mid \bar{x} \mapsto |\psi\rangle \mid [x] \end{aligned}$$

(SL connectives)

$$\{\, \mathrm{emp} \,\}\ \mathrm{qalloc}\ \{\, x.\ x \mapsto |0\rangle * [x] \,\} \qquad \{\, x \mapsto |0\rangle * [x] \,\}\ \mathrm{qfree}\, x\ \{\, \mathrm{emp} \,\}$$

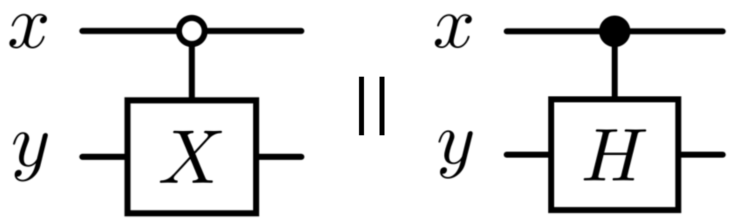
$$\{\, \bar{x} \mapsto |\psi\rangle \,\}\ U(\bar{x})\ \{\, \bar{x} \mapsto U|\psi\rangle \,\}$$

… and more interesting rules!

- ***Quantum points-to token*** $\bar{x} \mapsto |\psi\rangle$: the state vector of $\bar{x}$ is $|\psi\rangle$
- Separation $*$ means disentangled qubit states:
$$\bar{x} \mapsto |\psi\rangle \ * \ \bar{y} \mapsto |\phi\rangle \ \equiv \ (\bar{x}, \bar{y}) \mapsto |\psi\rangle \otimes |\phi\rangle$$
- ***Qubit token*** $[x]$ (new!): Qubit x is alive, but its state is unknown

A Simple Example

$$C_0X(x, y) \;\; || \;\; C_1H(x, y)$$



- Apparent write-write race: X and H gates don't commute ($XH \neq HX$)
- Still, no real race condition: C_0X and C_1H do commute, thanks to the controls by the "cases" where x is $|0\rangle$ or $|1\rangle$ resp.

Our Goal: Prove this

$$\{ \, (x, y) \mapsto (\alpha|0\rangle|\phi_0\rangle + \beta|1\rangle|\phi_1\rangle) \; * [y] \, \}$$
$$C_0X(x, y) \;\; || \;\; C_1H(x, y)$$
$$\{ \, (x, y) \mapsto (\alpha|0\rangle \otimes X|\phi_0\rangle + \beta|1\rangle \otimes H|\phi_1\rangle) * [y] \, \}$$

Our Key Observation

$C_0X(x,y) \mid\mid C_1H(x,y)$

- Both processes can write to y simultaneously due to superposition
  - If $x \mapsto \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \neq 0$, then both C_0X and C_1H update y
- How to distribute “write permission” on y to both processes?
- **Our idea: Quantum case analysis over the bases** of a qubit x

$x \mapsto |0\rangle$

$C_0X(x,y) \mid\mid \underline{C_1H(x,y)}$

Write permission is not required

$x \mapsto |1\rangle$

$\underline{C_0X(x,y)} \mid\mid C_1H(x,y)$

- After the case analysis, only one process writes to the qubit
  $\Rightarrow$ The apparent write-write race is eliminated!

Linear Combination Rule

- This idea can be formalized as **linear combination of Hoare triples**

$$\frac{\{\,\bar{x} \mapsto |\psi\rangle * P\,\}\ e\ \{\,\bar{x} \mapsto |\phi\rangle * Q\,\}^I \quad \{\,\bar{x} \mapsto |\psi'\rangle * P\,\}\ e\ \{\,\bar{x} \mapsto |\phi'\rangle * Q\,\}^I}{\{\,\bar{x} \mapsto (\alpha|\psi\rangle + \beta|\psi'\rangle)\ * P\,\}\ e\ \{\,\bar{x} \mapsto (\alpha|\phi\rangle + \beta|\phi'\rangle)\ * Q\,\}^I}$$

  - With the side condition Q, I: precise
    - Precise assertions represent a unique (or no) resource
      - e.g., $\mathrm{emp}, \perp, l \mapsto v, x \mapsto |\psi\rangle, l \mapsto v * x \mapsto |\psi\rangle, \ldots$
    - If not I: precise, the angelic branching on I makes the rule unsound

Now Our Subgoals:

$$\{\,(x,y) \mapsto |0\rangle|\phi_0\rangle * [y]\,\}\ C_0X(x,y)\ ||\ C_1H(x,y)\ \{\,(x,y) \mapsto |0\rangle \otimes X|\phi_0\rangle * [y]\,\}$$
$$\{\,(x,y) \mapsto |1\rangle|\phi_1\rangle * [y]\,\}\ C_0X(x,y)\ ||\ C_1H(x,y)\ \{\,(x,y) \mapsto |1\rangle \otimes H|\phi_1\rangle * [y]\,\}$$

Resource Sharing via Invariants

$\{ (x,y) \mapsto |0\rangle|\phi_0\rangle * [y] \}\ C_0X(x,y) \,||\, C_1H(x,y)\ \{ (x,y) \mapsto |0\rangle \otimes X|\phi_0\rangle * [y] \}$

$\{ y \mapsto |\phi_0\rangle * [y] \}\ C_0X(x,y) \,||\, C_1H(x,y)\ \{ y \mapsto X|\phi_0\rangle * [y] \}^{x\mapsto|0\rangle}$

Share $x \mapsto |0\rangle$ via the **invariant**

$\{ y \mapsto |\phi_0\rangle \}\ C_0X(x,y)\ \{ y \mapsto X|\phi_0\rangle \}^{x\mapsto|0\rangle}$

$\{ [y] \}\ C_1X(x,y)\ \{ [y] \}^{x\mapsto|0\rangle}$

$\{ x \mapsto |0\rangle * y \mapsto |\phi_0\rangle \}\ C_0X(x,y)\ \{ x \mapsto |0\rangle * y \mapsto X|\phi_0\rangle \}$

$\boxed{\{ x \mapsto |0\rangle * [y] \}\ C_1X(x,y)\ \{ x \mapsto |0\rangle * [y] \}}$

$$\frac{e \text{ is atomic} \quad \{ P * I \}\, e\, \{ Q * I \}}{\{ P \}\ e\ \{ Q \}^{I}} \qquad \frac{\{ P \}\ e\ \{ Q \}^{I*J}}{\{ P * I \}\ e\ \{ Q * I \}^{J}}$$

$$\frac{\{P\}\, e\, \{Q\}^{I} \quad \{P'\}\, e'\, \{Q'\}^{I}}{\{P * P'\}\ e \,||\, e'\ \{Q * Q'\}^{I}}$$

Anti-Frame Rule by Atomicity

$$\boxed{\{\, x \mapsto |0\rangle * [y] \,\}\ C_1X(x,y)\ \{\, x \mapsto |0\rangle * [y] \,\}}$$

$$\frac{e \text{ is atomic} \qquad P\colon \text{out } x \qquad Q\colon \text{precise} \qquad \forall |\psi\rangle.\ \{\, x \mapsto |\psi\rangle * [x] * P \,\}\ e\ \{\, x \mapsto |\psi\rangle * [x] * Q \,\}}{\{\, [x] * P \,\}\ e\ \{\, [x] * Q \,\}}$$

Cf. Frame rule

$$\frac{\{P\}\, e\, \{Q\}}{\{P * R\}\, e\, \{Q * R\}}$$

- Qubit token $[x]$ allows atomic temporary writes to x
  - e.g., $I(x)$, atomic $\{\, X(x); (\ldots\, x \text{ is unchanged} \ldots); X(x) \,\}$
- Other processes can freely access x with the points-to token $x \mapsto |\psi\rangle$
  - Technically, qubit tokens can be used for *dirty qubits*

Complete Proof for $C_0X(x,y) \mid\mid C_1H(x,y)$

$\{ (x,y) \mapsto (\alpha|0\rangle|\phi_0\rangle + \beta|1\rangle|\phi_1\rangle) * [y] \}$

$\{ x \mapsto |0\rangle * y \mapsto |\phi_0\rangle * [y] \}$

$\{ x \mapsto |1\rangle * y \mapsto |\phi_1\rangle * [y] \}$

$\{ y \mapsto |\phi_0\rangle * [y] \}^{x \mapsto |0\rangle}$

$\{ y \mapsto |\phi_1\rangle * [y] \}^{x \mapsto |1\rangle}$

$C_0X(x,y) \mid\mid C_1H(x,y)$

$\{ y \mapsto X|\phi_0\rangle * [y] \}^{x \mapsto |0\rangle}$

$\{ y \mapsto H|\phi_1\rangle * [y] \}^{x \mapsto |1\rangle}$

$\{ x \mapsto |0\rangle * y \mapsto X|\phi_0\rangle * [y] \}$

$\{ x \mapsto |1\rangle * y \mapsto H|\phi_1\rangle * [y] \}$

$\{ (x,y) \mapsto (\alpha|0\rangle \otimes X|\phi_0\rangle + \beta|1\rangle \otimes H|\phi_1\rangle) * [y] \}$

$\{ y \mapsto |\phi_0\rangle \}^{x \mapsto |0\rangle} \; \{ [y] \}^{x \mapsto |1\rangle}$

$\{ y \mapsto |\phi_0\rangle * x \mapsto |0\rangle \} \{ [y] * x \mapsto |1\rangle \}$

$C_0X(x,y)$

$\{ y \mapsto X|\phi_0\rangle * x \mapsto |0\rangle \} \{ [y] * x \mapsto |1\rangle \}$

$\{ y \mapsto X|\phi_0\rangle \}^{x \mapsto |0\rangle} \; \{ [y] \}^{x \mapsto |1\rangle}$

$\{ [y] \}^{x \mapsto |0\rangle} \; \{ y \mapsto |\phi_1\rangle \}^{x \mapsto |1\rangle}$

$\{ [y] \} \; \{ y \mapsto |\phi_1\rangle * x \mapsto |1\rangle \}$

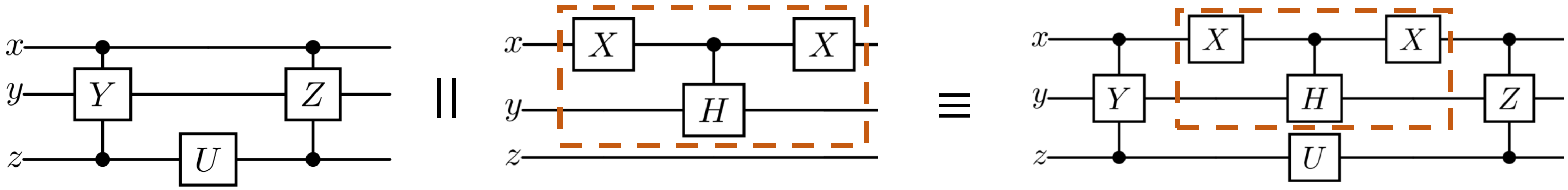
$C_1H(x,y)$

$\{ [y] * x \mapsto |0\rangle \} \; \{ y \mapsto H|\phi_1\rangle * x \mapsto |1\rangle \}$

$\{ [y] \}^{x \mapsto |0\rangle} \; \{ y \mapsto H|\phi_1\rangle \}^{x \mapsto |1\rangle}$

$$\{P_1\}\{P_2\}\, e\, \{Q_1\}\{Q_2\} \stackrel{\text{def}}{=} \{P_1\}\, e\, \{Q_1\} \wedge \{P_2\}\, e\, \{Q_2\}$$

More Complex Example



$$\{(x,y,z) \mapsto (\alpha|0\rangle|\psi_{yz}\rangle + \beta|1\rangle|\phi_{yz}\rangle) * [y] * [z] * \cdots\}$$

Invariant

$x \mapsto |0\rangle * [y] * [z]$ || Invariant $x \mapsto |0\rangle * (y,z) \mapsto |\psi_{yz}\rangle$

$CCY(x,z,y); U(z); CCZ(x,z,y)$ || atomic $\{ X(x); CH(x,y); X(x) \}$

x is updated only **temporarily**

$$\{ (x,y,z) \mapsto (\alpha|0\rangle \otimes H_y U_z |\psi_{yz}\rangle + \beta|1\rangle \otimes CCY_{xzy} U_z CCZ_{xzy} |\phi_{yz}\rangle) * \cdots \}$$

Another Fun Thing: Commuting Matrices

We can verify parallelization of arbitrary commuting matrices

- Since commutative matrices are simultaneously diagonalizable

$$\{\, x \mapsto (\alpha|0\rangle + \beta|1\rangle) \,\}$$

$$\{\, x \mapsto |0\rangle \,\}\{\, x \mapsto |1\rangle \,\}$$

$$\{\, () \mapsto 1 \,\}^{x\mapsto|0\rangle}\{\, () \mapsto 1 \,\}^{x\mapsto|1\rangle}$$

$$R_{\theta_1}(x) \mid\mid R_{\theta_2}(x)$$

$$\{\, () \mapsto 1 \,\}^{x\mapsto|0\rangle}\underline{\{\, () \mapsto e^{i(\theta_1+\theta_2)} \,\}}^{x\mapsto|1\rangle}$$

$$\{\, x \mapsto |0\rangle \,\}\{\, x \mapsto e^{i(\theta_1+\theta_2)}|1\rangle \,\}$$

$$\{\, x \mapsto (\alpha|0\rangle + \beta e^{i(\theta_1+\theta_2)}|1\rangle) \,\}$$

$R_{\theta_1}(x)$ and $R_{\theta_2}(x)$ have the same eigenvectors $\{|0\rangle, |1\rangle\}$
$\Rightarrow$ Quantum case analysis by $|0\rangle, |1\rangle$

Global phases can be tracked with empty-qubit points-to tokens

Outline

- Preliminaries on Quantum Computing
- Motivation: Parallelizing Quantum Programs
- Our Work: Concurrent QSL for Fine-Grained Parallelism
- **Extension to Probabilistic Reasoning & Conclusion**

Extension to Probabilistic Reasoning

- Want to support quantum measurements!
- Challenge: Precise reasoning about **probabilistic** behavior
  - **Density matrix**, probabilistic distribution modulo equalities
    - e.g., $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \;=\; \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| \;=\; \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Our idea: Refine **Demonic Outcome Logic** [Zilberstein+ POPL'25] & its CSL variant [Zilberstein+ arXiv]
  - Key mechanism: **Probabilistic combination** $P +_p Q$
    - Solves the limitations of the existing quantum SL [Le+ POPL'22]
  - Model: **Convex PCM** (new!), a hybrid of convex space & PCM

Teaser of Our Probabilistic Quantum SL

- On probabilistic combinations

$$P +_p Q \;\equiv\; Q +_{1-p} P \qquad \big(P +_p Q\big) +_q R \;\equiv\; P +_{pq} \big(Q +_{\frac{(1-p)q}{1-pq}} R\big)$$

$$P \vdash P +_p P \qquad P\colon \mathrm{convex} \;\stackrel{\mathrm{def}}{\equiv}\; \forall p.\; P +_p P \equiv P$$

Convex hull modality $\triangle P \;\stackrel{\mathrm{def}}{\equiv}\; \exists\, \bar{p} \in (0,1)^*\ \mathrm{s.t.} \sum \bar{p} = 1. \sum_i p_i P$

$$P \vdash \triangle P \qquad \triangle\triangle P \equiv \triangle P \qquad \triangle P\colon \mathrm{convex} \qquad \triangle \big(P +_p Q\big) \equiv \triangle P +_p \triangle Q$$

$$\big(P +_p Q\big) * R \;\equiv\; P * R +_p Q * R \quad \text{if } R\colon \mathrm{precise}$$

$$\{\,\mathrm{emp}\,\}\;\; v \oplus_p v' \;\; \{\, \langle v \rangle +_p \langle v' \rangle \,\} \qquad \{\,\mathrm{emp}\,\}\;\; \mathrm{ndint} \;\; \{\, \triangle\, (\exists n.\, \langle n \rangle)\,\}$$

- Quantum

$$\bar{x} \mapsto \rho +_p \bar{x} \mapsto \rho' \;\equiv\; \bar{x} \mapsto (p\rho + (1-p)\rho')$$

$$\{\, x \mapsto \rho \,\}\;\; \mathrm{meas}(x) \;\; \left\{ \langle 0 \rangle * x \mapsto \tfrac{1}{p} Pr_0 \rho Pr_0 +_p \langle 1 \rangle * x \mapsto \tfrac{1}{1-p} Pr_1 \rho Pr_1 \right\}$$

where $p = \mathrm{tr}(Pr_0 \rho)$

Conclusion

- We proposed a concurrent quantum separation logic
  for modular verification of fine-grained parallelism
- Our logic supports shared quantum resources via invariants,
  the linear combination rule, and the anti-frame rule by atomicity
- Future work
  - More powerful concurrency reasoning
  - Automated optimization of quantum programs & its verification