

Concurrent Quantum Separation Logic for Fine-Grained Parallelism

Yusuke Matsushita (Kyoto University)

Kengo Hirata (The University of Edinburgh)

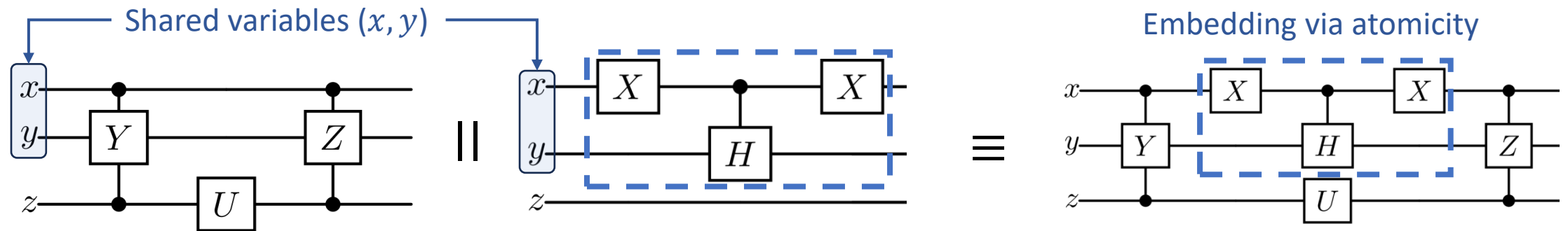
ORyo Wakizaka (Kyoto University)

25th January, 2025 @ PAnQC2025

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

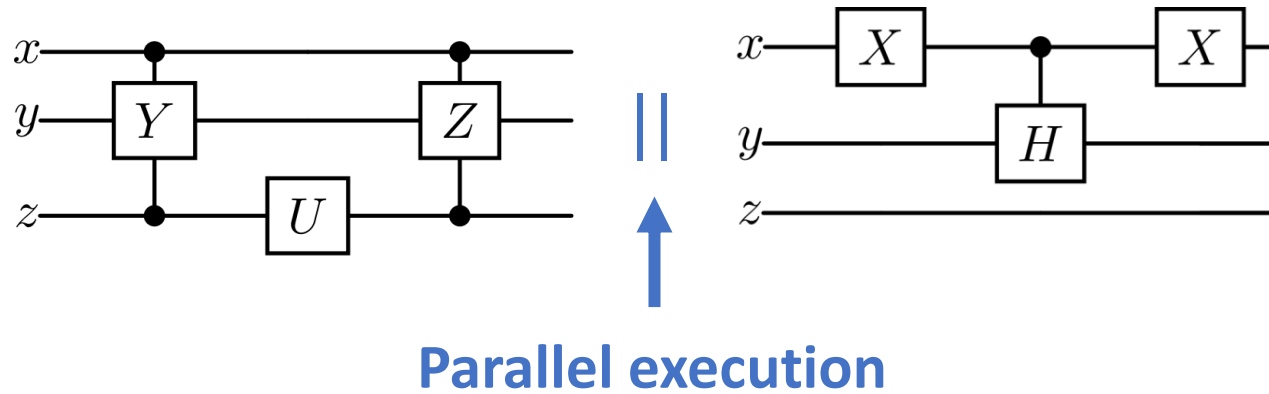


Outline

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

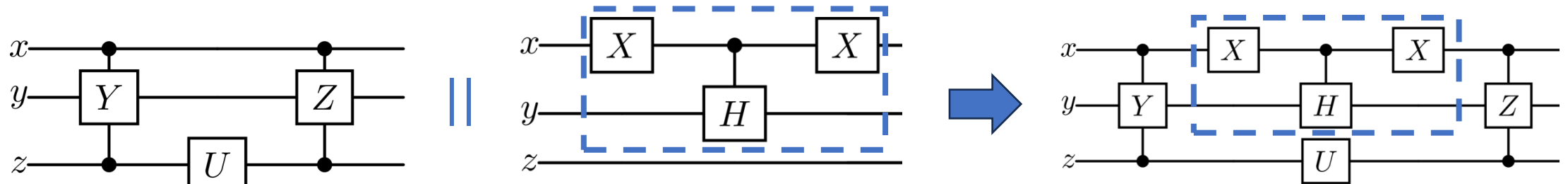
Parallelizing Quantum Programs

- **Parallelizing** quantum programs can reduce execution costs



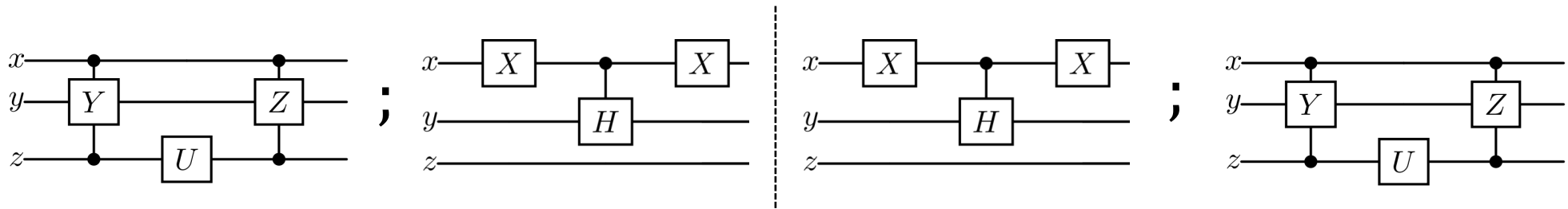
Parallelizing Quantum Programs

- **Parallelizing** quantum programs can reduce execution costs



Clover scheduling

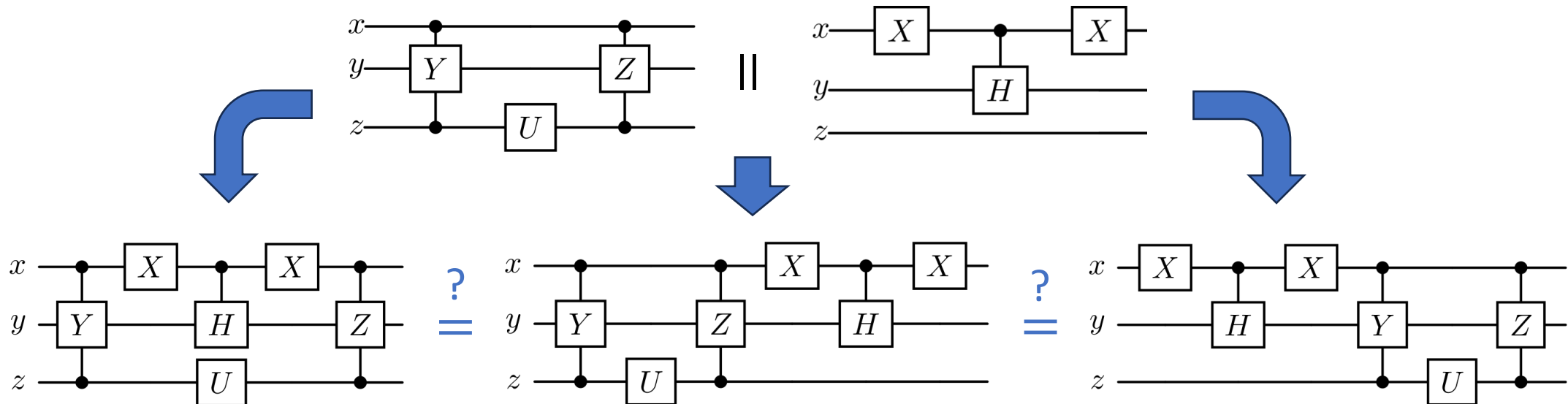
Patterns of parallelization results = Possible execution traces



Verifying the Correctness of Parallelization

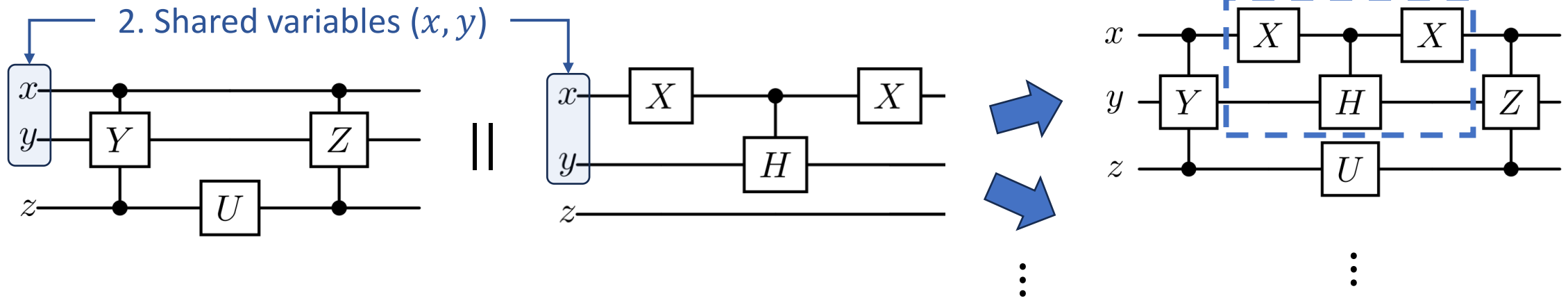
Parallelization is correct? = Concurrent program is correct?

Correctness of a parallel program $\approx$ **Uniqueness of the output**



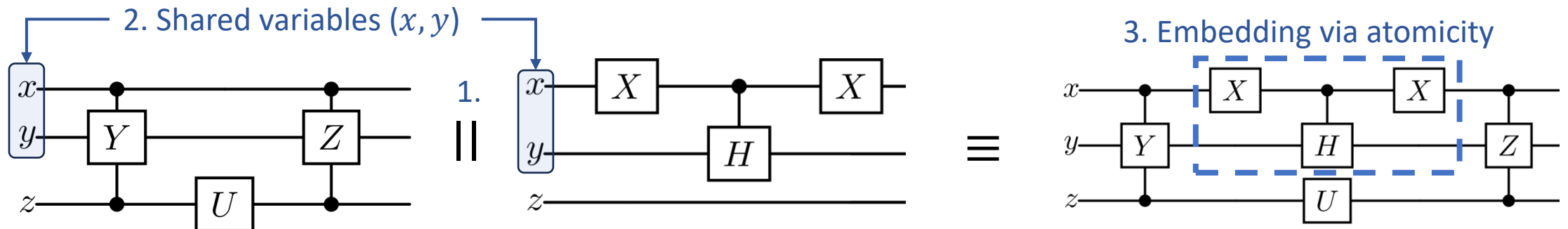
What is Challenge?

1. Parallelization allows exponentially many execution traces!
⇒ Need a **modular** method for parallel quantum programs
2. Concurrent programs may share qubits in non-trivial way
3. Support circuit embedding in non-interfered way



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

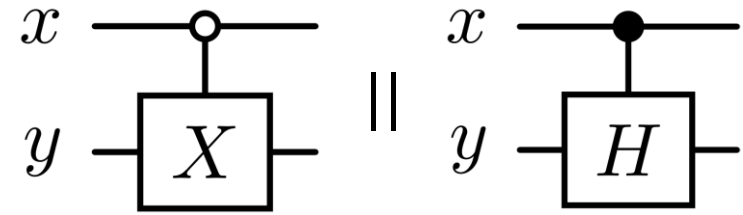


Outline

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

A Simple Example

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



Our Goal: Prove this

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

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

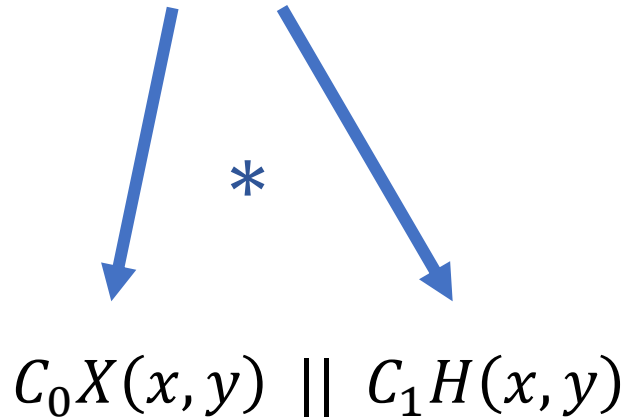
Postcondition $\{ (x, y) \mapsto (\alpha|0\rangle \otimes X|\phi_0\rangle + \beta|1\rangle \otimes H|\phi_1\rangle) * [y] \}$

- **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

Proof for $C_0X(x, y) \parallel C_1H(x, y)$

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



Quantum resources (propositions) can be distributed to processes by separation $*$
 $\Rightarrow$ How?

Remark:

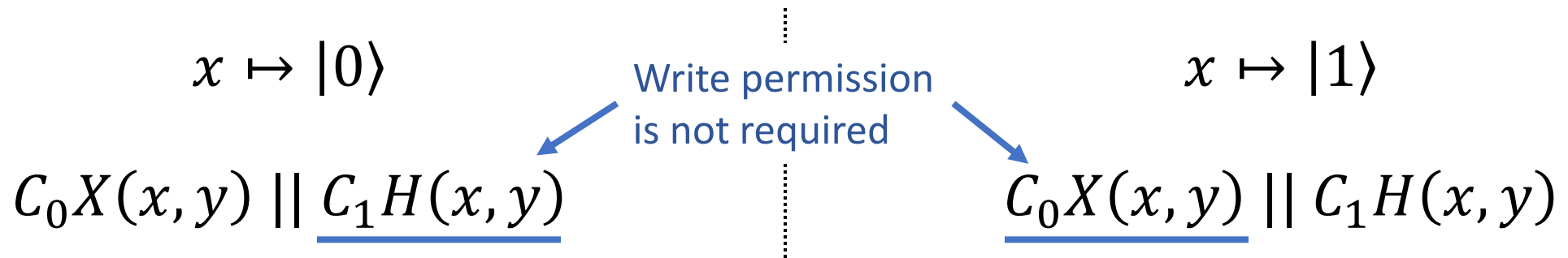
- $y \mapsto |\psi\rangle * y \mapsto |\psi\rangle$ is not allowed
- x and y may not be separable

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

Our Key Observation

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

- 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



- 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**

$$\frac{\begin{array}{l} \{ \bar{x} \mapsto |\psi\rangle * P \} e \{ \bar{x} \mapsto |\phi\rangle * Q \} \\ \{ \bar{x} \mapsto |\psi'\rangle * P \} e \{ \bar{x} \mapsto |\phi'\rangle * Q \} \end{array}}{\{ \bar{x} \mapsto (\alpha|\psi\rangle + \beta|\psi'\rangle) * P \} e \{ \bar{x} \mapsto (\alpha|\phi\rangle + \beta|\phi'\rangle) * Q \}}$$

Now Our Subgoals:

$$\begin{array}{l} \{ (x, y) \mapsto |0\rangle|\phi_0\rangle * [y] \} C_0 X(x, y) \parallel C_1 H(x, y) \{ (x, y) \mapsto |0\rangle \otimes X|\phi_0\rangle * [y] \} \\ \{ (x, y) \mapsto |1\rangle|\phi_1\rangle * [y] \} C_0 X(x, y) \parallel C_1 H(x, y) \{ (x, y) \mapsto |1\rangle \otimes H|\phi_1\rangle * [y] \} \end{array}$$

Proof for $C_0X(x, y) \parallel C_1H(x, y)$

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

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

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

$$y \mapsto |\phi_0\rangle \quad * \quad [y]$$

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

- Give $y \mapsto |\phi_i\rangle$ to i -th process
- x is required by both processes as “read-only” qubits

Remark:

- $x \mapsto |\psi\rangle * x \mapsto |\psi\rangle$ is not allowed

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

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

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

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

Resource Sharing via Invariants

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

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

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

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

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

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

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

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

$$\frac{\{ P \} e \{ Q \}^{I*J}}{\{ P * I \} e \{ Q * I \}^J}$$

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

Anti-Frame Rule by Atomicity

$$\{x \mapsto |0\rangle * [y]\} \ C_1 X(x, y) \ \{x \mapsto |0\rangle * [y]\}$$

$$\frac{\begin{array}{c} e \text{ is atomic} \quad P: \text{out } x \quad Q: \text{precise} \\ \forall |\psi\rangle. \{x \mapsto |\psi\rangle * [x] * P\} \ e \ \{x \mapsto |\psi\rangle * [x] * Q\} \end{array}}{\{[x] * P\} \ e \ \{[x] * Q\}}$$

Cf. Frame rule

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

- Qubit token $[x]$ allows atomic temporary writes to x
 - e.g., $I(x)$, $\text{atomic} \{ X(x); (\dots x \text{ is unchanged } \dots); X(x) \}$
- 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 $C_0X(x, y) \parallel C_1H(x, y)$

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

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

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

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

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

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

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

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

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

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

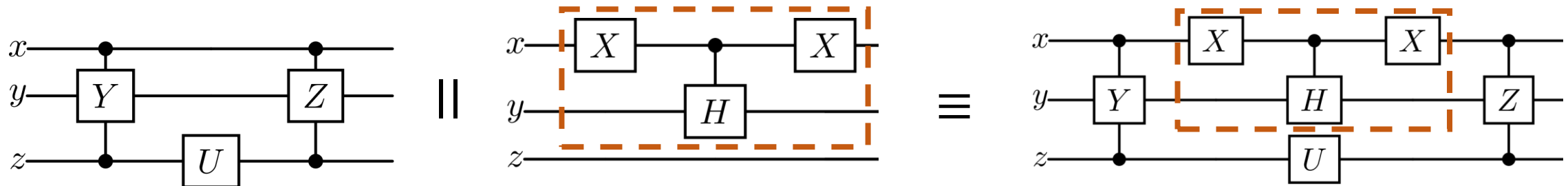
$$\{ (x, y) \mapsto (\alpha|0\rangle \otimes X|\phi_0\rangle + \beta|1\rangle \otimes H|\phi_1\rangle) * [y] \}$$

$$\begin{aligned} & \{ y \mapsto |\phi_0\rangle \}^{x \mapsto |0\rangle} \{ [y] \}^{x \mapsto |1\rangle} \\ & \{ y \mapsto |\phi_0\rangle * x \mapsto |0\rangle \} \{ [y] * x \mapsto |1\rangle \} \\ & C_0X(x, y) \\ & \{ y \mapsto X|\phi_0\rangle * x \mapsto |0\rangle \} \{ [y] * x \mapsto |1\rangle \} \\ & \{ y \mapsto X|\phi_0\rangle \}^{x \mapsto |0\rangle} \{ [y] \}^{x \mapsto |1\rangle} \end{aligned}$$

$$\begin{aligned} & \{ [y] \}^{x \mapsto |0\rangle} \{ y \mapsto |\phi_1\rangle \}^{x \mapsto |1\rangle} \\ & \{ [y] \} \{ y \mapsto |\phi_1\rangle * x \mapsto |1\rangle \} \\ & C_1H(x, y) \\ & \{ [y] * x \mapsto |0\rangle \} \{ y \mapsto H|\phi_1\rangle * x \mapsto |1\rangle \} \\ & \{ [y] \}^{x \mapsto |0\rangle} \{ y \mapsto H|\phi_1\rangle \}^{x \mapsto |1\rangle} \end{aligned}$$

$$\begin{aligned} & \{P_1\} \{P_2\} e \{Q_1\} \{Q_2\} \stackrel{\text{def}}{=} \\ & \{P_1\} e \{Q_1\} \wedge \{P_2\} e \{Q_2\} \end{aligned}$$

More Complex Example



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

Invariant

$$x \mapsto |0\rangle * [y] * [z]$$

||

Invariant

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

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

x is updated only **temporarily**

$$\{(x, y, z) \mapsto (\alpha|0\rangle \otimes H_y U_z |\psi_{yz}\rangle + \beta|1\rangle \otimes CY_{zy} U_z CZ_{zy} |\phi_{yz}\rangle) * \dots\}$$

Another Fun Thing: Commuting Matrices

We can verify parallelization of arbitrary commuting matrices

- Since commutative matrices are simultaneously diagonalizable

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

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

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

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

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

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

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

$R_{\theta_1}(x)$ 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

- 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

Two-Layer Logic

Layer1: Vector-based Quantum Separation Logic (I talked today)

- Quantum points-to token (as vector) $\bar{x} \mapsto |\psi\rangle$ and qubit token $[x]$
- Sensitive to global phase because of linear combination of Hoare triples

“densify”

Layer2: Probabilistic Quantum Separation Logic (New)

- Quantum points-to token (as *density operator*) $\bar{x} \mapsto \rho$
- Probabilistic combination $P +_p Q$
- Support quantum measurements
- Insensitive global phase

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

Our Target Language

$e ::= x \mid l \mid n \mid () \mid op(\bar{e})$
| qalloc (qubit allocation)
| qfree e (qubit deallocation) **Quantum**
| $U(\bar{e})$ (quantum gate)
| meas(e) (qubit measurement)
| $e \parallel e'$ (parallel execution) **Concurrency**
| atomic { e } (atomic block)
| ! e | $e \leftarrow e'$ | $\dots$ (heap)
| if e { e' } else { e'' } | while e { e' } | $\dots$

Overview of Our Logic

$$\begin{array}{ll}
 \text{Invariant} & P ::= \top \mid \perp \mid \neg P \mid P \wedge Q \mid P \vee Q \\
 \{P\} e \{v. Q_v\}^I & \mid P \rightarrow Q \mid \forall a. P_a \mid \exists a. P_a \\
 \{P\} e \{v. Q_v\} \triangleq \{P\} e \{v. Q_v\}^{\text{emp}} & \mid \text{emp} \mid P * Q \mid P - * Q \quad (\text{SL connectives}) \\
 & \mid l \mapsto v \mid \bar{x} \mapsto |\psi\rangle \mid [x]
 \end{array}$$

$$\begin{array}{l}
 \{ \text{emp} \} \text{qalloc } \{ x. x \mapsto |0\rangle * [x] \} \quad \{ x \mapsto |0\rangle * [x] \} \text{qfree } x \{ \text{emp} \} \\
 \{ \bar{x} \mapsto |\psi\rangle \} U(\bar{x}) \{ \bar{x} \mapsto U|\psi\rangle \} \quad \dots \text{ and more interesting rules!}
 \end{array}$$

- **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

Linear Combination Rule

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

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

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

Now Our Subgoals:

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

Teaser of Our Probabilistic Quantum SL

- On probabilistic combinations

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

$$P \vdash P +_p P \quad P: \text{convex} \stackrel{\text{def}}{=} \forall p. P +_p P \equiv P$$

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

$$P \vdash \Delta P \quad \Delta \Delta P \equiv \Delta P \quad \Delta P: \text{convex} \quad \Delta (P +_p Q) \equiv \Delta P +_p \Delta Q$$

$$(P +_p Q) * R \equiv P * R +_p Q * R \quad \text{if } R: \text{precise}$$

$$\{ \text{emp} \} v \oplus_p v' \{ \langle v \rangle +_p \langle v' \rangle \} \quad \{ \text{emp} \} \text{ndint} \{ \Delta (\exists n. \langle n \rangle) \}$$

- Quantum

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

$$\{ x \mapsto \rho \} \text{meas}(x) \left\{ \langle 0 \rangle * x \mapsto \frac{1}{p} P r_0 \rho P r_0 +_p \langle 1 \rangle * x \mapsto \frac{1}{1-p} P r_1 \rho P r_1 \right\}$$

where $p = \text{tr}(P r_0 \rho)$

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 $\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$

- Composite of $|\psi\rangle$ and $|\phi\rangle = \textit{Tensor product } |\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle$

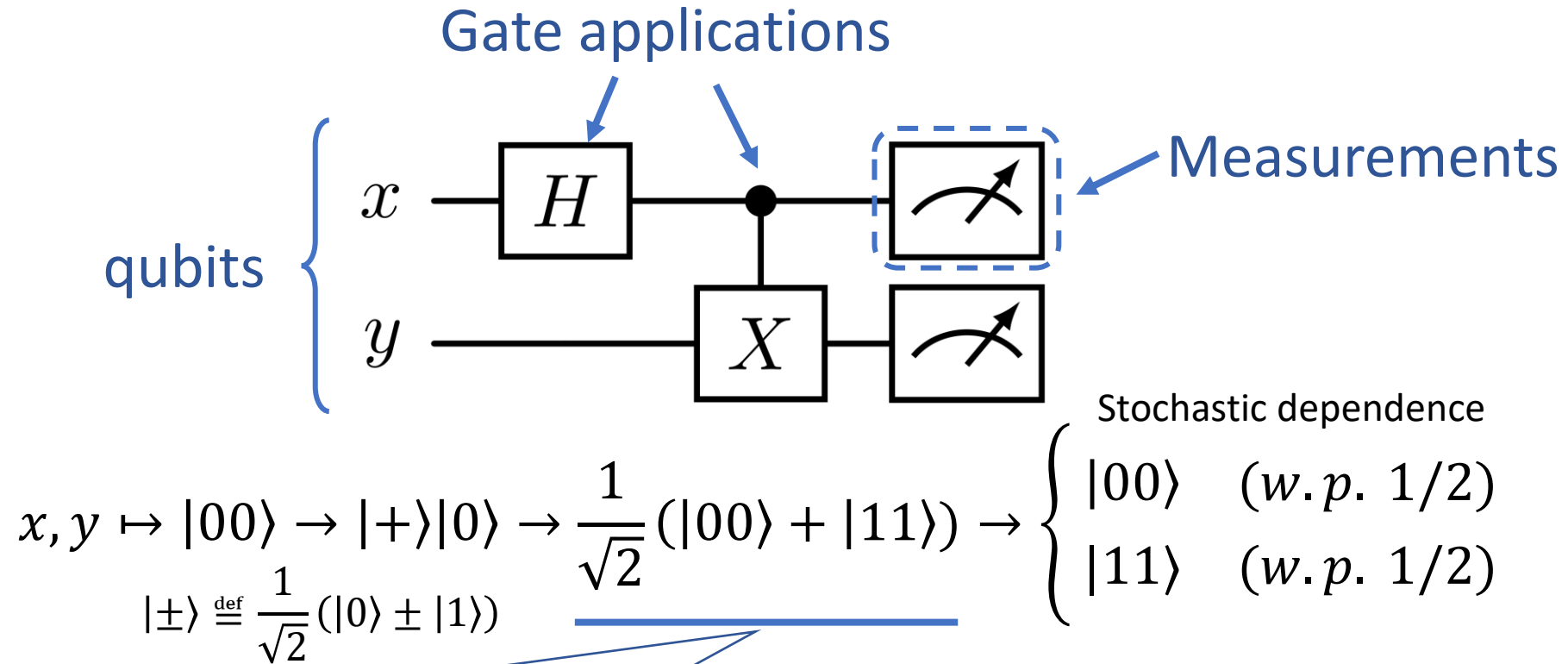
- **Quantum gate** = Unitary matrix $U : \mathcal{H} \rightarrow \mathcal{H}$

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

- **Measurement** = Probabilistic branching & convergence

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

Quantum Program (Circuit)



Entangled state

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