RapunSL

Untangling Quantum Computing with Separation, Linear Combination and Mixing

Yusuke Matsushita*, Kengo Hirata*, Ryo Wakizaka, Emanuele D’Osualdo

This paper RapunSL

Separation Logic

capable of handling

Quantum Entanglement and Measurement

Question.

Why Quantum Separation Logic?

Answer.

Modular reasoning for scalability!!

Quick overview: RapunSL

Existing Quantum Separating Logics
$\Rightarrow$ Local reasoning for each
disentangled component.

FRAME

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

Quick overview: RapunSL

Existing Quantum Separating Logics
$\Rightarrow$ Local reasoning for each <u>disentangled component.</u>

FRAME

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

RapunSL

+ reasoning about **<u>superposition</u>** state

Hoare-SUM

$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 + P_2\}\ C\ \{Q_1 + Q_2\}}$$

Quick overview: RapunSL

Existing Quantum Separating Logics
$\Rightarrow$ Local reasoning for each disentangled component.

FRAME
$$\frac{\{\ P\ \}\ C\ \{\ Q\ \}}{\{\ P * R\ \}\ C\ \{\ Q * R\ \}}$$

RapunSL

+ reasoning about **superposition** state

Hoare-SUM
$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 + P_2\}\ C\ \{Q_1 + Q_2\}}$$

+ compatible with **measurements**

Hoare-MIX
$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 \oplus^{\iota} P_2\}\ C\ \{Q_1 \oplus^{\iota} Q_2\}}$$

Previous Work: Quantum $\times$ Separation Logic

Proposition = Quantum State

$x \mapsto |1\rangle$ *means* qubit x has state $|1\rangle$

$(x, y) \mapsto |10\rangle$ *means* qubits x, y have state $|10\rangle$

Previous Work: Quantum $\times$ Separation Logic

Proposition = Quantum State

$x \mapsto |1\rangle$ *means* qubit x has state $|1\rangle$

$(x, y) \mapsto |10\rangle$ *means* qubits x, y have state $|10\rangle$

Hoare triple

$$\{\ x \mapsto |0\rangle\ \}\ \text{NOT}\,[x]\ \{\ x \mapsto |1\rangle\ \}$$

Previous Work: Quantum × Separation Logic

Proposition = Quantum State

$x \mapsto |1\rangle$ *means* qubit x has state $|1\rangle$

$(x, y) \mapsto |10\rangle$ *means* qubits x, y have state $|10\rangle$

Hoare triple

$$\{\ x \mapsto |0\rangle\ \}\ \text{NOT}\,[x]\ \{\ x \mapsto |1\rangle\ \}$$

Under the pre-condition $x \mapsto |0\rangle$

Previous Work: Quantum $\times$ Separation Logic

Proposition = Quantum State

$x \mapsto |1\rangle$ *means* qubit x has state $|1\rangle$

$(x, y) \mapsto |10\rangle$ *means* qubits x, y have state $|10\rangle$

Hoare triple

$$\{\ x \mapsto |0\rangle\ \}\ \text{NOT}\,[x]\ \{\ x \mapsto |1\rangle\ \}$$

Under the pre-condition $x \mapsto |0\rangle$

If we execute NOT gate

Previous Work: Quantum × Separation Logic

Proposition = Quantum State

$x \mapsto |1\rangle$ *means* qubit x has state $|1\rangle$

$(x, y) \mapsto |10\rangle$ *means* qubits x, y have state $|10\rangle$

Hoare triple

$$\{\ x \mapsto |0\rangle\ \}\ \text{NOT}\,[x]\ \{\ x \mapsto |1\rangle\ \}$$

Under the pre-condition $x \mapsto |0\rangle$

If we execute NOT gate

We get the post-condition $x \mapsto |1\rangle$

Previous Work: Quantum $\times$ Separation Logic

Observation

For a quantum circuit C,

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

then

$$\{\ (x, y) \mapsto |0\rangle \otimes |1\rangle\ \}\ C\ \{\ (x, y) \mapsto |1\rangle \otimes |1\rangle\ \}.$$

Previous Work: Quantum $\times$ Separation Logic

Observation

For a quantum circuit C,

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

then

$$\{\ (x, y) \mapsto |0\rangle \otimes |1\rangle\ \}\ C\ \{\ (x, y) \mapsto |1\rangle \otimes |1\rangle\ \}.$$

To formalize this in a logic,

Separating Conjunction

$P * Q$

meaning

Separable state

$P \otimes Q$

Previous Work: Quantum × Separation Logic

Observation

For a quantum circuit C,

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

then

$$\{\ (x, y) \mapsto |0\rangle \otimes |1\rangle\ \}\ C\ \{\ (x, y) \mapsto |1\rangle \otimes |1\rangle\ \}.$$

To formalize this in a logic,

Separating Conjunction

$$P * Q$$

meaning

Separable state

$$P \otimes Q$$

For example,

$$\bar{\mathrm{x}} \mapsto |\psi\rangle \ * \ \bar{\mathrm{y}} \mapsto |\varphi\rangle \iff \underbrace{(\bar{\mathrm{x}}, \bar{\mathrm{y}}) \mapsto |\psi\rangle \otimes |\varphi\rangle}_{\text{disentangled state}}$$

Previous Work: Quantum × Separation Logic

Frame

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

For example,

$$\frac{\{\ x \mapsto |0\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ \}}{\{\ x \mapsto |0\rangle\ *\ y \mapsto |1\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ *\ y \mapsto |1\rangle\ \}}$$

Previous Work: Quantum × Separation Logic

`Frame`

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

Meaning…

Focus on

local entangled component P

Prove above, then add

disentangled resource R

For example,

$$\frac{\{\ x \mapsto |0\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ \}}{\{\ x \mapsto |0\rangle\ *\ y \mapsto |1\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ *\ y \mapsto |1\rangle\ \}}$$

Previous Work: Quantum × Separation Logic

Frame

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

Meaning…

Focus on

<u>*local entangled component*</u> P

Prove above, then add

<u>*disentangled resource*</u> R

For example,

$$\frac{\{\ x \mapsto |0\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ \}}{\{\ x \mapsto |0\rangle\ *\ y \mapsto |1\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ *\ y \mapsto |1\rangle\ \}}$$

Entanglement-Local reasoning

Previous Work: Quantum $\times$ Separation Logic

`Frame`

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

Meaning…

Focus on

local entangled component P

Prove above, then add

disentangled resource R

For example,

$$\frac{\{\ x \mapsto |0\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ \}}{\{\ x \mapsto |0\rangle\ *\ y \mapsto |1\rangle\ \}\ C\ \{\ x \mapsto |1\rangle\ *\ y \mapsto |1\rangle\ \}}$$

Entanglement-Local reasoning

Question: Is this enough to achieve "***Modular reasoning***"?

Problem 1: Frame is not enough

Observation 2

For some *unitary* map C,

$$\{\,(\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle\,\}\; C \;\{\,(\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle\,\}$$

$$\{\,(\mathtt{x}_0, \mathtt{x}_1) \mapsto |11\rangle\,\}\; C \;\{\,(\mathtt{x}_0, \mathtt{x}_1) \mapsto |11\rangle\,\}$$

Problem 1: Frame is not enough

Observation 2

For some *unitary* map C,

$$\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}\; C \;\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}$$

$$\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |11\rangle \,\}\; C \;\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |11\rangle \,\}$$

then what if the input is entangled?

$$(\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto \alpha\,|000\rangle + \beta\,|111\rangle$$

Problem 1: Frame is not enough

Observation 2

For some *unitary* map C,

$$\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}\ C\ \{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}$$

$$\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |11\rangle \,\}\ C\ \{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |11\rangle \,\}$$

then what if the input is entangled?

$$(\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto \alpha\, |000\rangle + \beta\, |111\rangle$$

that means…

$$\neq\ (x_0, x_1) \mapsto |\psi\rangle \ \otimes\ y \mapsto |\varphi\rangle$$

Problem 1: Frame is not enough

Observation 2

For some *unitary* map C,

$$\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|00\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|00\rangle\,\}$$

$$\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|11\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|11\rangle\,\}$$

then what if the input is entangled?

$$(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle+\beta\,|111\rangle$$

Because… **Linearity of C**

$$\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle+\beta\,|111\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle+\beta\,|111\rangle\,\}$$

However…

Frame rule is only for disentangled $y\mapsto|\psi\rangle$

RapunSL: Linear combination

RapunSL: Linear combination

Our logic: **RapunSL** $\quad P \coloneqq \cdots \mid \alpha P \mid P + Q \mid \cdots$

$$\alpha\left(\bar{\mathsf{x}} \mapsto |\psi\rangle\right) \iff \bar{\mathsf{x}} \mapsto \alpha|\psi\rangle$$

$$\bar{\mathsf{x}} \mapsto |\psi\rangle \; + \; \bar{\mathsf{x}} \mapsto |\varphi\rangle \iff \bar{\mathsf{x}} \mapsto (|\psi\rangle + |\varphi\rangle)$$

RapunSL: Linear combination

Our logic: **RapunSL** $P \coloneqq \cdots \mid \alpha P \mid P + Q \mid \cdots$

$$\alpha\left(\bar{\mathsf{x}} \mapsto |\psi\rangle\right) \iff \bar{\mathsf{x}} \mapsto \alpha|\psi\rangle$$

$$\bar{\mathsf{x}} \mapsto |\psi\rangle \;+\; \bar{\mathsf{x}} \mapsto |\varphi\rangle \iff \bar{\mathsf{x}} \mapsto (|\psi\rangle + |\varphi\rangle)$$

$$\frac{\{\,P\,\}\; C\; \{\,Q\,\}}{\{\,\alpha P\,\}\; C\; \{\,\alpha Q\,\}}\ \text{Hoare-SCALAR}$$

$$\frac{\{\,P_1\,\}\; C\; \{\,Q_1\,\} \qquad \{\,P_2\,\}\; C\; \{\,Q_2\,\}}{\{\,P_1 + P_2\,\}\; C\; \{\,Q_1 + Q_2\,\}}\ \text{Hoare-SUM}$$

RapunSL: Linear combination

$$\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle \,\}$$

RapunSL: Linear combination

$$\frac{\{\,(\mathtt{x}_0,\mathtt{x}_1)\mapsto|00\rangle\,\}\ C\ \{\,(\mathtt{x}_0,\mathtt{x}_1)\mapsto|00\rangle\,\}}{\{\,(\mathtt{x}_0,\mathtt{x}_1,\mathtt{y})\mapsto|000\rangle\,\}\ C\ \{\,(\mathtt{x}_0,\mathtt{x}_1,\mathtt{y})\mapsto|000\rangle\,\}}\ \mathtt{FRAME}$$

RapunSL: Linear combination

$$
\dfrac{\dfrac{\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}\; C \;\{\, (\mathrm{x}_0, \mathrm{x}_1) \mapsto |00\rangle \,\}}{\{\, (\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto |000\rangle \,\}\; C \;\{\, (\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto |000\rangle \,\}}}{\{\, (\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto \alpha\, |000\rangle \,\}\; C \;\{\, (\mathrm{x}_0, \mathrm{x}_1, \mathrm{y}) \mapsto \alpha\, |000\rangle \,\}} \;\text{Hoare-SCALAR}
$$

RapunSL: Linear combination

$$\dfrac{\dfrac{\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |00\rangle \,\}}{\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto |000\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto |000\rangle \,\}}}{\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto \alpha\,|000\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto \alpha\,|000\rangle \,\}}$$

$$\dfrac{\dfrac{\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |11\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1) \mapsto |11\rangle \,\}}{\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto |111\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto |111\rangle \,\}}}{\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto \beta\,|111\rangle \,\}\; C \;\{\, (\mathtt{x}_0, \mathtt{x}_1, \mathtt{y}) \mapsto \beta\,|111\rangle \,\}}$$

RapunSL: Linear combination

$$\dfrac{\dfrac{\dfrac{\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|00\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|00\rangle\,\}}{\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto|000\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto|000\rangle\,\}}}{\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle\,\}} \qquad \dfrac{\dfrac{\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|11\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1)\mapsto|11\rangle\,\}}{\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto|111\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto|111\rangle\,\}}}{\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\beta\,|111\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\beta\,|111\rangle\,\}}}{\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle+\beta\,|111\rangle\,\}\;C\;\{\,(\mathrm{x}_0,\mathrm{x}_1,\mathrm{y})\mapsto\alpha\,|000\rangle+\beta\,|111\rangle\,\}}\;\text{Hoare-SUM}$$

Another perspective: intuitive → formal proof

Claim: Scalar and Sum bridge intuitive and formal proofs.

Another perspective: intuitive → formal proof

Claim: Scalar and Sum bridge intuitive and formal proofs.

Question: Does program C implement U ?

Intuitive Proof: It suffices to check for the computational basis

$$\forall \bar{b} \in \{0,1\}^n. \quad \bar{x} \mapsto |\bar{b}\rangle \quad \Rightarrow^C \quad \bar{x} \mapsto U|\bar{b}\rangle.$$

Another perspective: intuitive → formal proof

Claim: Scalar and Sum bridge intuitive and formal proofs.

Question: Does program C implement U ?

Intuitive Proof: It suffices to check for the computational basis

$$\forall \bar{b} \in \{0,1\}^n. \quad \bar{x} \mapsto |\bar{b}\rangle \quad \Rightarrow^{C} \quad \bar{x} \mapsto U|\bar{b}\rangle.$$

RapunSL Proof: We prove

$$\forall \bar{b} \in \{0,1\}^n. \left\{ \bar{\mathrm{x}} \mapsto \left|\bar{b}\right\rangle \right\} C \left\{ \bar{\mathrm{x}} \mapsto U \left|\bar{b}\right\rangle \right\}.$$

Another perspective: intuitive → formal proof

Claim: Scalar and Sum bridge intuitive and formal proofs.

Question: Does program C implement U ?

Intuitive Proof: It suffices to check for the computational basis

$$\forall \bar{b} \in \{0,1\}^n. \quad \bar{x} \mapsto |\bar{b}\rangle \quad \Rightarrow^C \quad \bar{x} \mapsto U|\bar{b}\rangle.$$

RapunSL Proof: We prove

$$\forall \bar{b} \in \{0,1\}^n. \left\{ \bar{\mathrm{x}} \mapsto \left|\bar{b}\right\rangle \right\} C \left\{ \bar{\mathrm{x}} \mapsto U \left|\bar{b}\right\rangle \right\}.$$

From $\texttt{Hoare-SCALAR}$ and $\texttt{Hoare-SUM}$,

$$\forall \left|\psi\right\rangle. \left\{ \bar{\mathrm{x}} \mapsto \left|\psi\right\rangle \right\} C \left\{ \bar{\mathrm{x}} \mapsto U \left|\psi\right\rangle \right\}.$$

Another perspective: intuitive → formal proof

Claim: Scalar and Sum bridge intuitive and formal proofs.

Question: Does program C implement U ?

Intuitive Proof: It suffices to check for the computational basis

$$\forall \bar{b} \in \{0,1\}^n. \quad \bar{x} \mapsto |\bar{b}\rangle \quad \Rightarrow^C \quad \bar{x} \mapsto U|\bar{b}\rangle.$$

RapunSL Proof: We prove

$$\forall \bar{b} \in \{0,1\}^n. \left\{ \bar{\mathrm{x}} \mapsto \left|\bar{b}\right\rangle \right\} C \left\{ \bar{\mathrm{x}} \mapsto U \left|\bar{b}\right\rangle \right\}.$$

From $\texttt{Hoare-SCALAR}$ and $\texttt{Hoare-SUM}$,

$$\forall \left|\psi\right\rangle. \left\{ \bar{\mathrm{x}} \mapsto \left|\psi\right\rangle \right\} C \left\{ \bar{\mathrm{x}} \mapsto U \left|\psi\right\rangle \right\}.$$

basis-locality

Hmm…, how can such a simple thing be new?

Problem 2: Measurement

C = meas x

$$\{\, \mathtt{x} \mapsto |0\rangle \,\}\ C\ \{\, \mathtt{x} \mapsto |0\rangle \,\} \qquad\qquad \{\, \mathtt{x} \mapsto |1\rangle \,\}\ C\ \{\, \mathtt{x} \mapsto |1\rangle \,\}$$

Problem 2: Measurement

C = meas x

$$\frac{\{\,\mathtt{x} \mapsto |0\rangle\,\}\; C\; \{\,\mathtt{x} \mapsto |0\rangle\,\} \qquad \{\,\mathtt{x} \mapsto |1\rangle\,\}\; C\; \{\,\mathtt{x} \mapsto |1\rangle\,\}}{\{\,\mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\,\}\; C\; \{\,\mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\,\}}\ \text{Hoare-SCALAR, Hoare-SUM}$$

Problem 2: Measurement

C = meas x

$$\frac{\{\,\mathrm{x} \mapsto |0\rangle\,\}\; C\; \{\,\mathrm{x} \mapsto |0\rangle\,\} \qquad \{\,\mathrm{x} \mapsto |1\rangle\,\}\; C\; \{\,\mathrm{x} \mapsto |1\rangle\,\}}{\{\,\mathrm{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\,\}\; C\; \{\,\mathrm{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\,\}}\ \text{Hoare-SCALAR, Hoare-SUM}$$

$\Longrightarrow$ C $\cong$ noop

Problem 2: Measurement

C = meas x

$$\frac{\{\, \mathtt{x} \mapsto |0\rangle \,\}\ C\ \{\, \mathtt{x} \mapsto |0\rangle \,\} \qquad \{\, \mathtt{x} \mapsto |1\rangle \,\}\ C\ \{\, \mathtt{x} \mapsto |1\rangle \,\}}{\{\, \mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle \,\}\ C\ \{\, \mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle \,\}}\ \text{Hoare-SCALAR, Hoare-SUM}$$

$\Longrightarrow$ $\cancel{C \cong \text{noop}}$

Measurement is not linear!

Idea: Branching as Measurement Outcomes

Idea: Add more detail to the post-condition

Idea: Branching as Measurement Outcomes

Idea: Add more detail to the post-condition

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

meas[x]

$$\{ \qquad ? \qquad \}$$

Idea: Branching as Measurement Outcomes

Idea: Add more detail to the post-condition

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

meas[x]

{ "Some branching has happened.

If it branched to "0", the state is $\alpha|0\rangle$.

If it branched to "1", the state is $\beta|1\rangle$." }

Idea: Branching as Measurement Outcomes

$$\left\{ \begin{array}{l} \quad x \mapsto \alpha|0\rangle + \beta|1\rangle \\ + \; x \mapsto \alpha'|0\rangle + \beta'|1\rangle \end{array} \right\}$$

meas[x]

{ "Some branching has happened.

If it branched to "0", the state is $\alpha|0\rangle$.

If it branched to "1", the state is $\beta|1\rangle$." }

Idea: Branching as Measurement Outcomes

$$\left\{ \begin{array}{l} \quad x \mapsto \alpha\,|\,0\rangle + \beta\,|\,1\rangle \\ + \; x \mapsto \alpha'\,|\,0\rangle + \beta'\,|\,1\rangle \end{array} \right\}$$

meas[x]

$\{$ “Some branching has happened.

If it branched to “0”, the state is $(\alpha + \alpha')\,|\,0\rangle$.

If it branched to “1”, the state is $(\beta + \beta')\,|\,1\rangle$.” $\}$

Measurement is linear for each branch

Solution: Mixing operator

ι: branching ID

RapunSL $P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$

Solution: Mixing operator

ι: branching ID

RapunSL $\quad P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$

C = meas$^{\iota}$ x

$$\{\, \mathtt{x} \mapsto |0\rangle \,\}\; C \;\{\; \mathtt{x} \mapsto |0\rangle \;\oplus^{\iota}\; \underline{\mathtt{x} \mapsto 0} \;\}$$

State of probability 0

Solution: Mixing operator

ι: branching ID

RapunSL $\quad P ::= \cdots \mid P \oplus^{\iota} Q \mid \cdots$

C = meas$^{\iota}$ x

$$\{\, \mathrm{x} \mapsto |0\rangle \,\}\; C \;\{\; \mathrm{x} \mapsto |0\rangle \;\oplus^{\iota}\; \underline{\mathrm{x} \mapsto 0} \;\}$$

State of probability 0

$$\{\, \mathrm{x} \mapsto |1\rangle \,\}\; C \;\{\; \underline{\mathrm{x} \mapsto 0} \;\oplus^{\iota}\; \mathrm{x} \mapsto |1\rangle \;\}$$

Solution: Mixing operator

RapunSL $P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$

C = meas$^{\iota}$ x

$\{ \mathtt{x} \mapsto |0\rangle \}\ C\ \{ \mathtt{x} \mapsto |0\rangle \oplus^{\iota} \mathtt{x} \mapsto 0 \}$ $\{ \mathtt{x} \mapsto |1\rangle \}\ C\ \{ \mathtt{x} \mapsto 0 \oplus^{\iota} \mathtt{x} \mapsto |1\rangle \}$

Solution: Mixing operator

RapunSL $P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$

C = meas$^{\iota}$ x

$$\frac{\{\mathtt{x} \mapsto |0\rangle\}\, C\, \{\, \mathtt{x} \mapsto |0\rangle \;\oplus^{\iota}\; \mathtt{x} \mapsto 0 \,\} \qquad \{\mathtt{x} \mapsto |1\rangle\}\, C\, \{\, \mathtt{x} \mapsto 0 \oplus^{\iota} \mathtt{x} \mapsto |1\rangle \,\}}{\{\, \mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle \,\}\, C\, \{\; \alpha(\, \mathtt{x} \mapsto |0\rangle \;\oplus^{\iota}\; \mathtt{x} \mapsto 0 \,) + \beta(\, \mathtt{x} \mapsto 0 \;\oplus^{\iota}\; \mathtt{x} \mapsto |1\rangle \,) \;\}}$$

Solution: Mixing operator

RapunSL $P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$

C = meas$^{\iota}$ x

$$\frac{\{\mathtt{x} \mapsto |0\rangle\}\ C\ \{\ \mathtt{x} \mapsto |0\rangle\ \oplus^{\iota}\ \mathtt{x} \mapsto 0\ \} \qquad \{\mathtt{x} \mapsto |1\rangle\}\ C\ \{\ \mathtt{x} \mapsto 0 \oplus^{\iota}\ \mathtt{x} \mapsto |1\rangle\ \}}{\begin{aligned}\{\ \mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\ \}\ C\ \{\ &(\ \mathtt{x} \mapsto \alpha\,|0\rangle\ \oplus^{\iota}\ \mathtt{x} \mapsto 0\ ) \\ &+ (\ \mathtt{x} \mapsto 0\ \oplus^{\iota}\ \mathtt{x} \mapsto \beta\,|1\rangle\ )\ \}\end{aligned}}$$

Solution: Mixing operator

RapunSL

$$P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$$

C = meas$^{\iota}$ x

$$\frac{\{\mathtt{x} \mapsto |0\rangle\}\; C \;\{\ \mathtt{x} \mapsto |0\rangle \ \oplus^{\iota}\ \mathtt{x} \mapsto 0\ \} \qquad \{\mathtt{x} \mapsto |1\rangle\}\; C \;\{\ \mathtt{x} \mapsto 0 \oplus^{\iota}\ \mathtt{x} \mapsto |1\rangle\ \}}{\{\mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle\}\; C \;\{\ \mathtt{x} \mapsto \alpha\,|0\rangle \ \oplus^{\iota}\ \mathtt{x} \mapsto \beta\,|1\rangle\ \}}$$

Solution: Mixing operator

RapunSL

$$P \coloneqq \cdots \mid P \oplus^{\iota} Q \mid \cdots$$

C = meas$^{\iota}$ x

$$\frac{\{\, \mathtt{x} \mapsto |0\rangle \,\}\ C\ \{\ \mathtt{x} \mapsto |0\rangle\ \oplus^{\iota}\ \mathtt{x} \mapsto 0\ \} \qquad \{\, \mathtt{x} \mapsto |1\rangle \,\}\ C\ \{\ \mathtt{x} \mapsto 0\ \oplus^{\iota}\ \mathtt{x} \mapsto |1\rangle\ \}}{\{\, \mathtt{x} \mapsto \alpha\,|0\rangle + \beta\,|1\rangle \,\}\ C\ \{\ \mathtt{x} \mapsto \alpha\,|0\rangle\ \oplus^{\iota}\ \mathtt{x} \mapsto \beta\,|1\rangle\ \}}$$

outcome-locality

$$\frac{\{\, P_1 \,\}\ C\ \{\, Q_1 \,\} \qquad \{\, P_2 \,\}\ C\ \{\, Q_2 \,\}}{\{\, P_1 \oplus^{\iota} P_2 \,\}\ C\ \{\, Q_1 \oplus^{\iota} Q_2 \,\}}\ \textsc{Hoare-MIX}$$

RapunSL: Three Localities

entanglement-locality

$$\frac{\{\ P\ \}\ C\ \{\ Q\ \}}{\{\ P * R\ \}\ C\ \{\ Q * R\ \}}\ \text{FRAME}$$

basis-locality

$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 + P_2\}\ C\ \{Q_1 + Q_2\}}\ \text{Hoare-SUM}$$

outcome-locality

$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 \oplus^{\iota} P_2\}\ C\ \{Q_1 \oplus^{\iota} Q_2\}}\ \text{Hoare-MIX}$$

And… Many Rules!

$$(P + Q) * R \vdash (P * R) + (Q * R)$$

$$(P \oplus^{\iota} Q) * R \vdash (P * R) \oplus^{\iota} (Q * R)$$

$$(P_1 \oplus^{\iota} P_2) + (Q_1 \oplus^{\iota} Q_2) \dashv\vdash (P_1 + Q_1) \oplus^{\iota} (P_2 + Q_2)$$

Please see the paper for details!

And… Many Rules!

$$(P + Q) * R \dashv\vdash (P * R) + (Q * R)$$

$$(P \oplus^{\iota} Q) * R \dashv\vdash (P * R) \oplus^{\iota} (Q * R)$$

$$(P_1 \oplus^{\iota} P_2) + (Q_1 \oplus^{\iota} Q_2) \dashv\vdash (P_1 + Q_1) \oplus^{\iota} (P_2 + Q_2)$$

$\dashv$: Require side-condition

P, Q, R : Frameable = class of "nice" propositions

"Propositions without $P \vee Q$, $\neg P$"

And… Many Rules!

$$(P + Q) * R \dashv\vdash (P * R) + (Q * R)$$

$$(P \oplus^{\iota} Q) * R \dashv\vdash (P * R) \oplus^{\iota} (Q * R)$$

$$(P_1 \oplus^{\iota} P_2) + (Q_1 \oplus^{\iota} Q_2) \dashv\vdash (P_1 + Q_1) \oplus^{\iota} (P_2 + Q_2)$$

$\dashv$: Require side-condition

P, Q, R : Frameable = class of "nice" propositions

"Propositions without $P \vee Q$, $\neg P$"

P, Q $\triangleq$ a $\mapsto$ v | x $\mapsto |\psi\rangle$

| P $\wedge$ Q | P $*$ Q | P + Q | P $\oplus^{\iota}$ Q | …

$\subseteq$ Frameable

Trade-off regarding measurements & Scalability in practice

Treatment of global phase

Global phase = Complex coefficient (of size 1) of a vector

Treatment of global phase

Global phase = Complex coefficient (of size 1) of a vector

Fact. Global phase is not observable

$$|1\rangle \quad \underset{\text{observably equivalent}}{\equiv} \quad -|1\rangle \quad \equiv \quad i|1\rangle$$

Treatment of global phase

Global phase = Complex coefficient (of size 1) of a vector

Fact. Global phase is not observable

$$|1\rangle \equiv -|1\rangle \equiv i|1\rangle$$

However…

In RapunSL, global phase CANNOT be ignored

Treatment of global phase

Global phase = Complex coefficient (of size 1) of a vector

Fact. Global phase is not observable

$$|1\rangle \equiv -|1\rangle \equiv i|1\rangle$$

However…

In RapunSL, global phase CANNOT be ignored

If we ignore it,

$$\mathrm{X} \mapsto |1\rangle \iff \mathrm{X} \mapsto -|1\rangle$$

Treatment of global phase

Global phase = Complex coefficient (of size 1) of a vector

Fact. Global phase is not observable

$$|1\rangle \equiv -|1\rangle \equiv i|1\rangle$$

However…

In RapunSL, global phase CANNOT be ignored

If we ignore it,

$$\dfrac{\mathtt{x} \mapsto |1\rangle \iff \mathtt{x} \mapsto -|1\rangle}{\mathtt{x} \mapsto |\psi\rangle + |1\rangle \iff \mathtt{x} \mapsto |\psi\rangle - |1\rangle}\ \text{SUM}$$

✗

Model: Vector state

Model of RapunSL is based on

✓ Vector states rather than ✗ Density matrices

Have been preferred as a model

Model: Vector state

Model of RapunSL is based on

✓ Vector states rather than ✗ Density matrices

Have been preferred as a model

There is a **trade-off**

	Vector	**Density Matrix**
Global Phase	✓	✗

Basis-locality

Model: Vector state

Model of RapunSL is based on

✓ Vector states rather than ✗ Density matrices

Have been preferred as a model

There is a **trade-off**

	Vector	**Density Matrix**	
Global Phase	✓	✗	Basis-locality
Measurement	**Can blow up Exponentially**	✓	Outcome-locality

Handling Exponential Blow-Up

2^n branches

After n *measurements,* $\bigoplus^{\iota_1 = i_1} \bigoplus^{\iota_2 = i_2} \ldots \bigoplus^{\iota_n = i_n} P_{i_1, i_2, \ldots, i_n}$

(Notation $\bigoplus^{\iota = i} P_i \quad := \quad P_0 \oplus^{\iota} P_1$)

Handling Exponential Blow-Up

2^n branches

After n *measurements,* $\bigoplus^{\iota_1 = i_1} \bigoplus^{\iota_2 = i_2} \ldots \bigoplus^{\iota_n = i_n} P_{i_1, i_2, \ldots, i_n}$

(Notation $\bigoplus^{\iota = i} P_i \;:=\; P_0 \oplus^{\iota} P_1$)

Indeed, blow-up is sometimes unavoidable…

Basis-locality *v.s.* Size

Handling Exponential Blow-Up

2^n branches

After n *measurements,* $\bigoplus^{\iota_1 = i_1} \bigoplus^{\iota_2 = i_2} \ldots \bigoplus^{\iota_n = i_n} P_{i_1, i_2, \ldots, i_n}$

(Notation $\bigoplus^{\iota = i} P_i \; := \; P_0 \oplus^{\iota} P_1$)

Indeed, blow-up is sometimes unavoidable…

Basis-locality *v.s.* Size

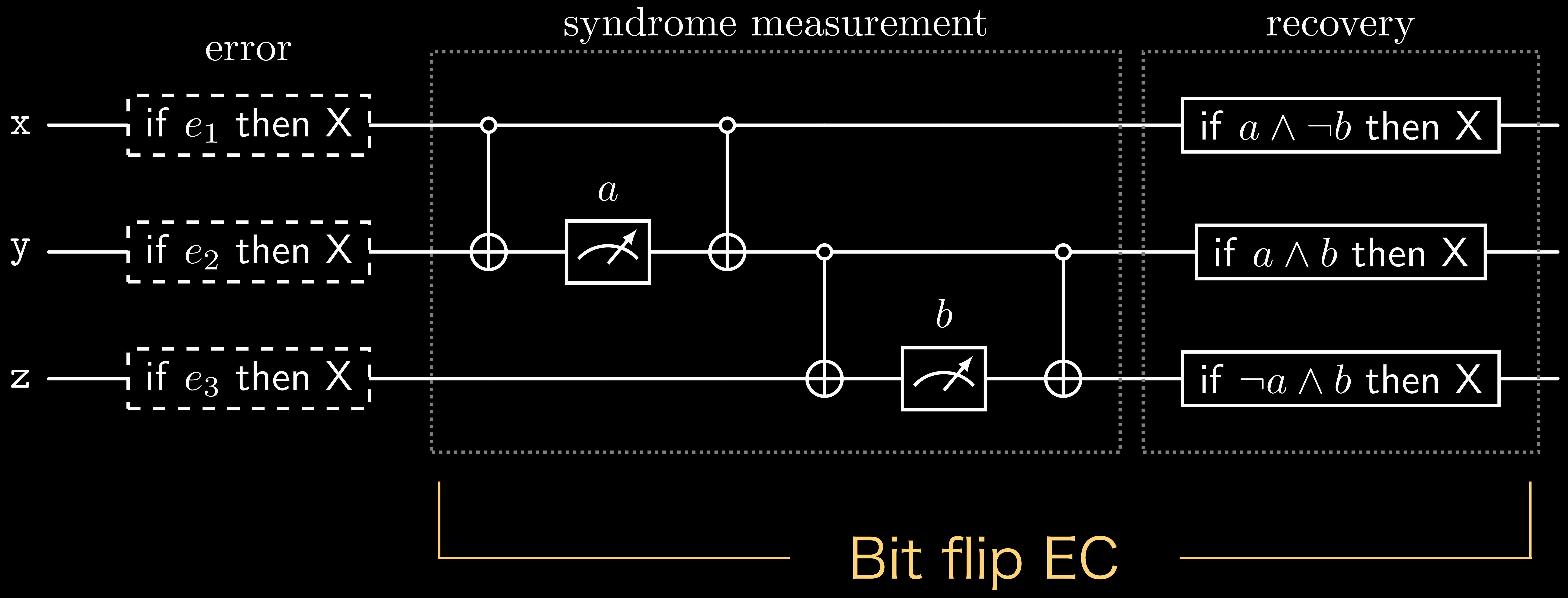
But in many practical cases, you can actually avoid it!

Case Study: Handling Blow-Up

Case Study Error Correction: Bit Flip Code

Case Study: Handling Blow-Up

Case Study Error Correction: Bit Flip Code



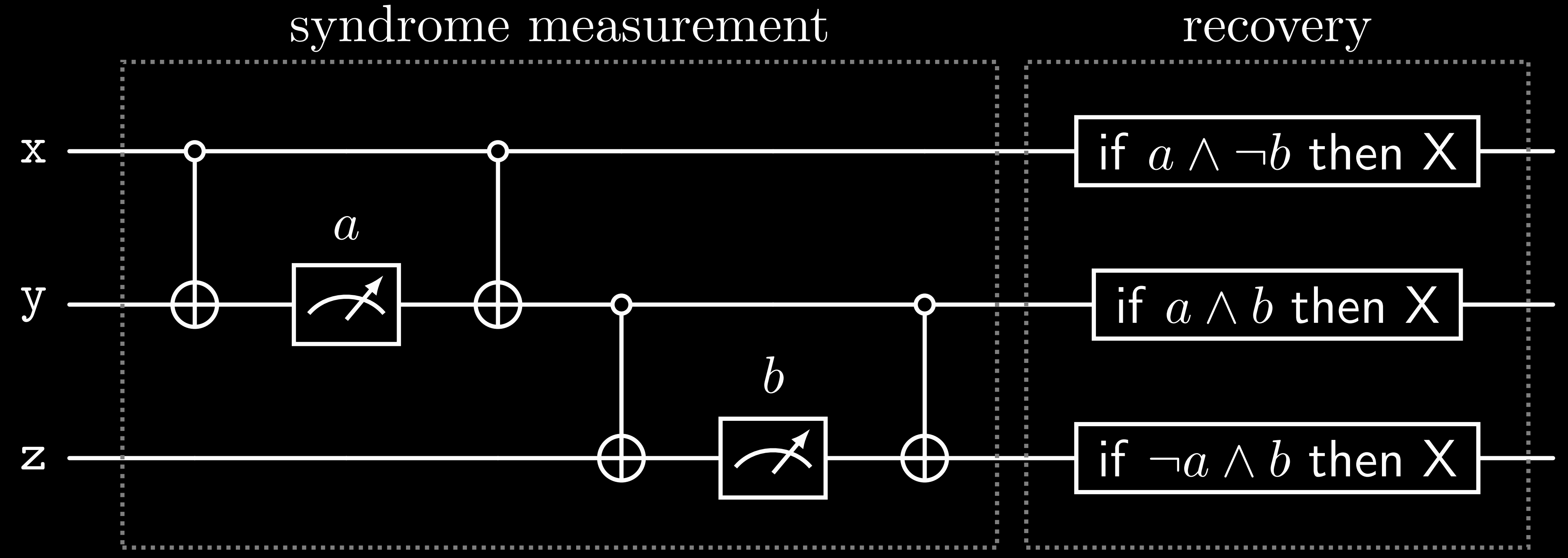
Case Study: Handling Blow-Up

First step: Reduce it to classical case

Case Study: Handling Blow-Up

First step: Reduce it to classical case

$$\left\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\,|iii\rangle\ \right\}$$

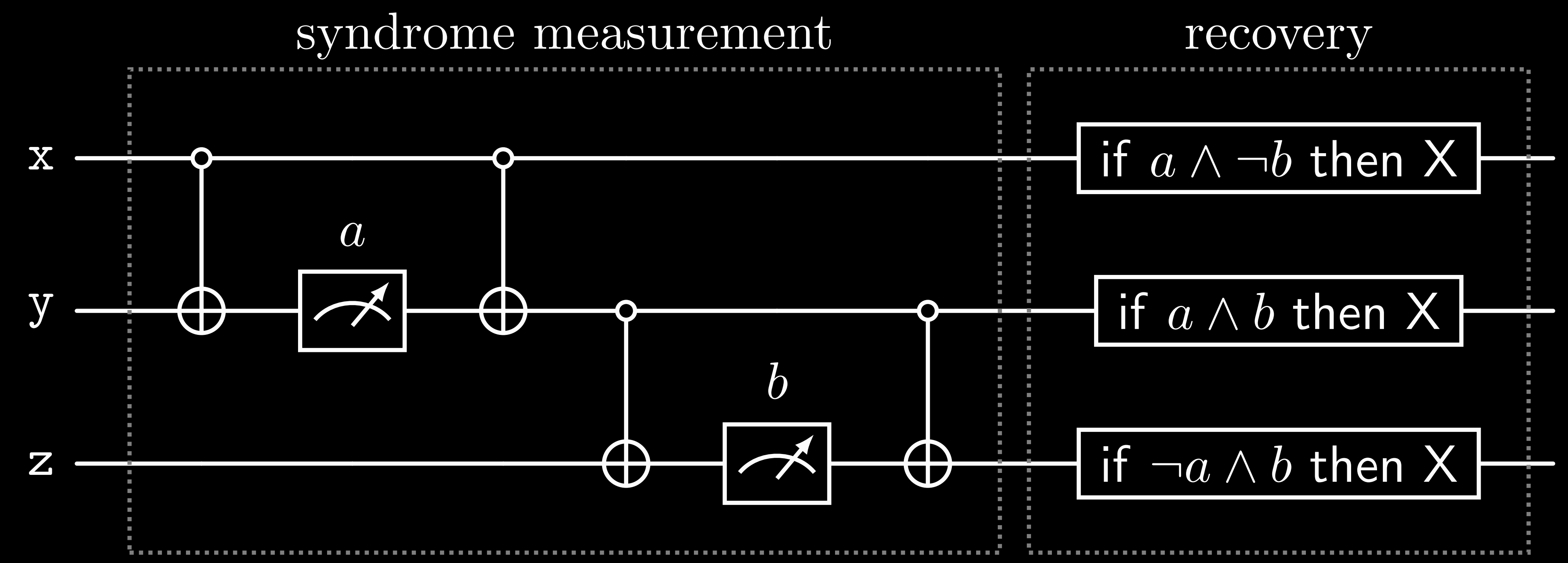


$$\left\{\ \bigoplus^{a=0,1} \delta_{a,e_1+e_2} \cdot \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \cdot (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto |iii\rangle\ \right\}$$

Case Study: Handling Blow-Up

First step: Reduce it to classical case

$$\left\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\,|iii\rangle\ \right\}$$



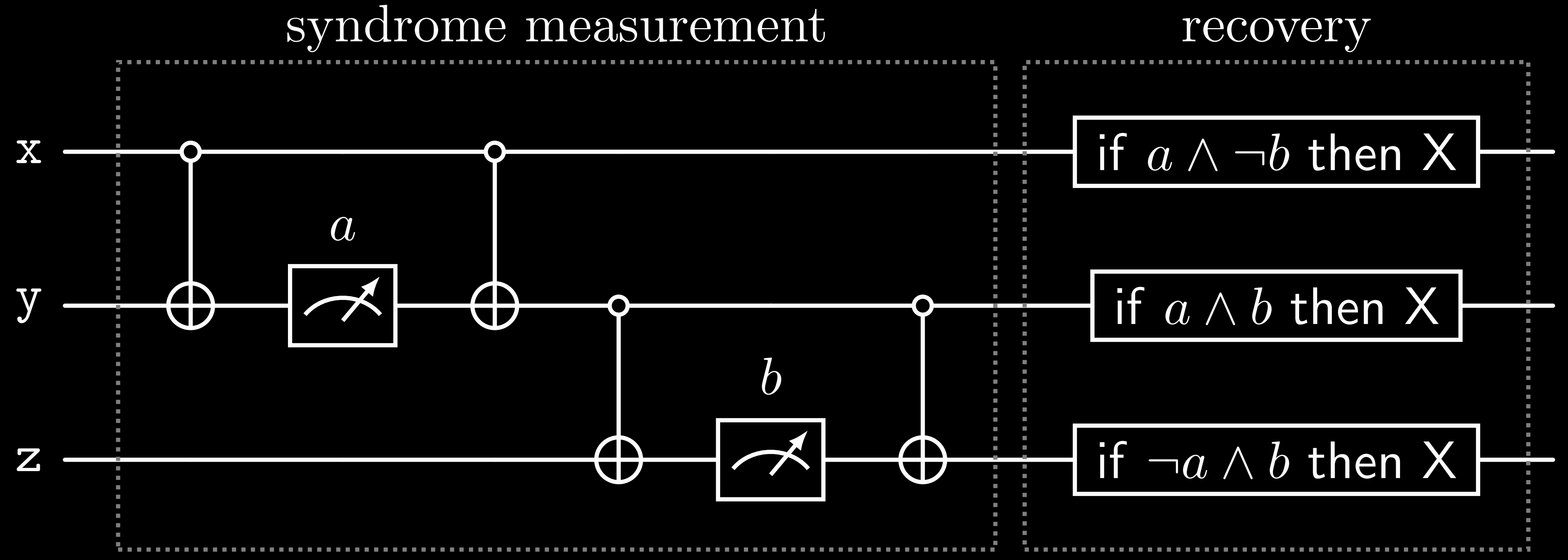
$$\left\{ \bigoplus^{a=0,1} \delta_{a,e_1+e_2} \cdot \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \cdot \underline{(\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto |iii\rangle} \right\}$$

not depend on a or b

Case Study: Handling Blow-Up

First step: Reduce it to classical case

$$\{\ (\mathtt{x}, \mathtt{y}, \mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\,|iii\rangle\ \}$$



$$\left\{ \bigoplus^{a=0,1} \delta_{a,e_1+e_2} \cdot \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \cdot \underline{(\mathtt{x}, \mathtt{y}, \mathtt{z}) \mapsto |iii\rangle} \right\}$$

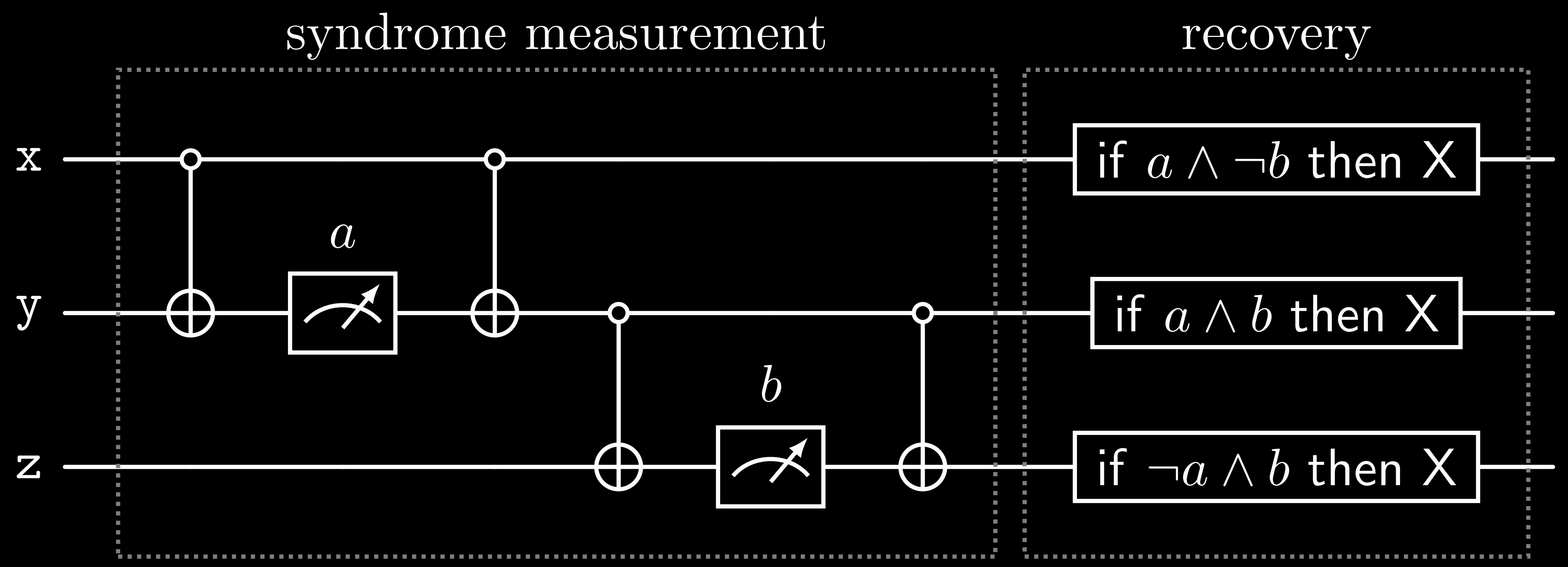
not depend on a or b

distributivity

Case Study: Handling Blow-Up

First step: Reduce it to classical case

$$\{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\,|iii\rangle\ \}$$



$$\left\{ \bigoplus^{a=0,1} \delta_{a,e_1+e_2} \cdot \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \cdot \underline{(\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto |iii\rangle} \right\}$$

not depend on a or b

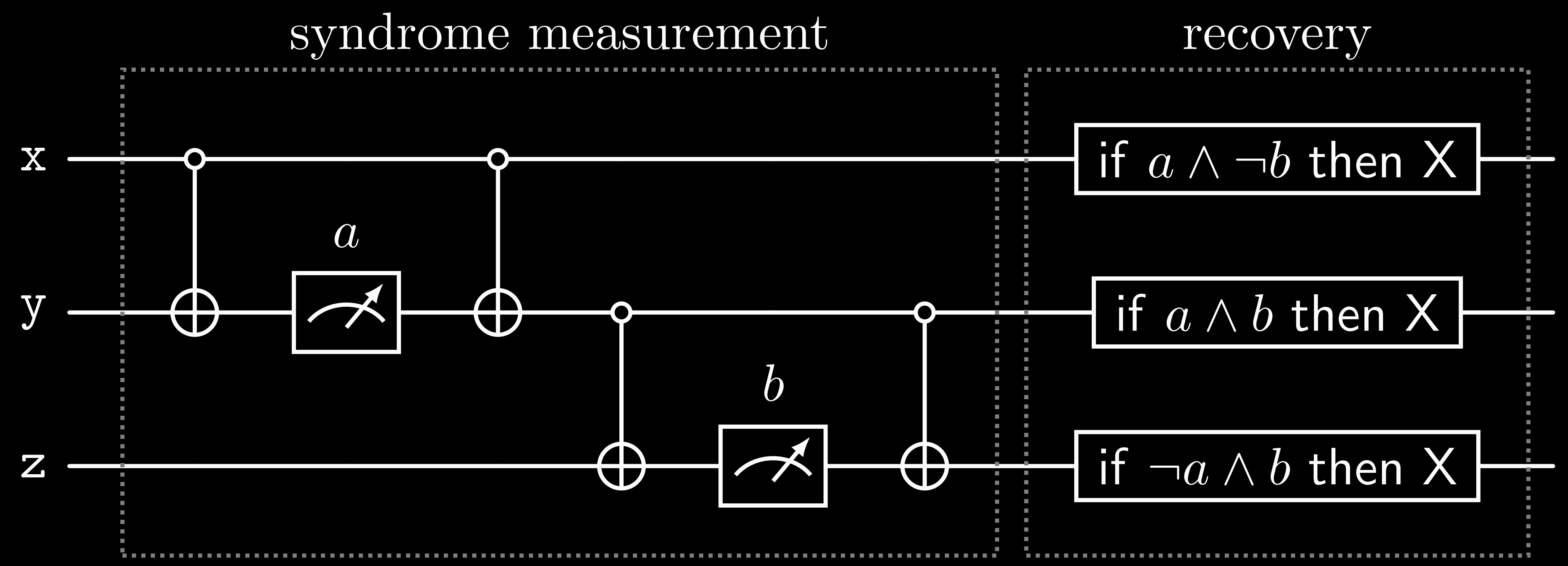
distributivity

$$\left\{ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto |iii\rangle \ * \left(\bigoplus^{a=0,1} \delta_{a,e_1+e_2} * \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \right) \right\}$$

Case Study: Handling Blow-Up

First step: Reduce it to classical case

$$\{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto \mathrm{X}^{e_1}\mathrm{X}^{e_2}\mathrm{X}^{e_3}\ |iii\rangle\ \}$$



$$\left\{\ \bigoplus^{a=0,1} \delta_{a,e_1+e_2} \cdot \bigoplus^{b=0,1} \delta_{b,e_2+e_3} \cdot \underline{(\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto |iii\rangle}\ \right\}$$

not depend on a or b

Second step: Hide $\bigoplus$

∃ P: frameable $\left\{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto |iii\rangle\ *\ \Big(\qquad P \qquad\Big)\ \right\}$

Case Study: Handling Blow Up

$$\{\ (\mathtt{x}, \mathtt{y}, \mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\ |iii\rangle\ \} \quad \mathsf{C} \quad \{\ (\mathtt{x}, \mathtt{y}, \mathtt{z}) \mapsto |iii\rangle * P\ \}$$

P : Frameable

Case Study: Handling Blow Up

$$\left\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\,|iii\rangle\ \right\} \quad \mathsf{C} \quad \left\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto |iii\rangle * P\ \right\}$$

P : Frameable

Hoare-Scalar
Hoare-SUM

Case Study: Handling Blow Up

$$\{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\ |iii\rangle\ \} \quad \mathsf{C} \quad \{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto |iii\rangle * P\ \}$$

P : Frameable

Hoare-Scalar
Hoare-SUM

$$\left\{\ (\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3} \sum_{i=0,1} \alpha_i\, |iii\rangle\ \right\} \quad \mathsf{C} \quad \left\{ \left((\mathrm{x},\mathrm{y},\mathrm{z}) \mapsto \sum_{i=0,1} \alpha_i\, |iii\rangle \right) * P \right\}$$

qed. $\square$

Case Study: Handling Blow Up

$$\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3}\ |iii\rangle\ \} \quad \mathsf{C} \quad \{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto |iii\rangle * P\ \}$$

P : Frameable

$$\{\ (\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \mathsf{X}^{e_1}\mathsf{X}^{e_2}\mathsf{X}^{e_3} \textstyle\sum_{i=0,1} \alpha_i\, |iii\rangle\ \} \quad \mathsf{C} \quad \{\ \left((\mathtt{x},\mathtt{y},\mathtt{z}) \mapsto \textstyle\sum_{i=0,1} \alpha_i\, |iii\rangle\right) * P\ \}$$

Hoare-Scalar
Hoare-SUM

qed. $\square$

P: Frameable is used implicitly

Other Case Studies

Many practical case studies

- Dirty Qubit: Implementation of CCCX by Toffoli Gates
- Quantum Teleportation
- Lattice Surgery: Implementation of CNOT with Measurements
- Error Correction 1: Bit-Flip Code
- Error Correction 2: Shor's Code

Related Work

	$\ast$-locality	$+$-locality	$\oplus$-locality	**Model**
Zhou et al. LICS '21	✓	✗	✗	Density Matrix
Le et al. POPL '22	✓	✗	✗	Vector*
Deng et al. VMCAI '24	✓	✗	✓	Density Matrix
RapunSL POPL '26	✓	✓	✓	Vector
Su et al. arXiv 24	Different $\ast$, and hard to compare			Density Matrix

Classical

Probability

Basis-locality

Conclusion

Contribution:

New logic RapunSL

$*$

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

$+$

$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 + P_2\}\ C\ \{Q_1 + Q_2\}}$$

$\oplus$

$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 \ {}_0{\oplus}_1^{\iota}\ P_2\}\ C\ \{Q_1 \ {}_0{\oplus}_1^{\iota}\ Q_2\}}$$

Future Work:

Thank you!!

Conclusion

Contribution:

New logic RapunSL

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

$+$
$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 + P_2\}\ C\ \{Q_1 + Q_2\}}$$

$\oplus$
$$\frac{\{P_1\}\ C\ \{Q_1\} \qquad \{P_2\}\ C\ \{Q_2\}}{\{P_1 \;{}_0{\oplus}_1^{\iota}\; P_2\}\ C\ \{Q_1 \;{}_0{\oplus}_1^{\iota}\; Q_2\}}$$

and many practical case studies

Future Work:

- Relational logic
- Automation
- Non-determinism / Concurrency

Thank you!!