Analysis of Quantum Entanglement in Quantum Programs using Stabilizer Formalism

The University of Tokyo
Kentaro Honda

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$|0001\rangle$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{2}}(|0000\rangle - |0001\rangle)$$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{2}(\,|0000\rangle - |0001\rangle + |0010\rangle - |0011\rangle)$$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{2}(\,|0000\rangle - |0001\rangle + |0011\rangle - |0010\rangle)$$

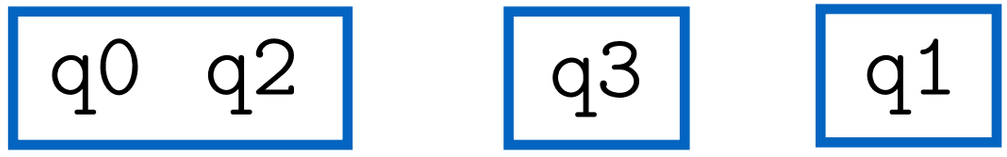
q0 q2	q3	q1

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{8}}(\,|0000\rangle + |0100\rangle - |0001\rangle - |0101\rangle + |0011\rangle + |0111\rangle - |0010\rangle - |0110\rangle)$$

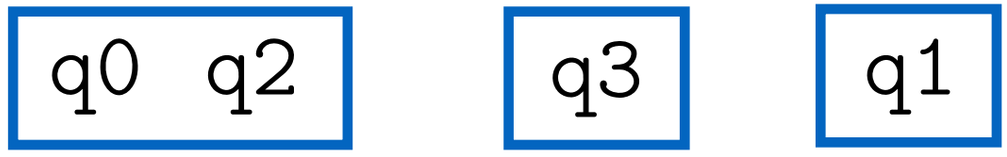


Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{8}}(\,|0000\rangle + |0101\rangle - |0001\rangle - |0100\rangle + |0011\rangle + |0110\rangle - |0010\rangle - |0111\rangle)$$



Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{4}(\,|0000\rangle + |1000\rangle + |0101\rangle + |1101\rangle - |0001\rangle - |1001\rangle - |0100\rangle - |1100\rangle + |0011\rangle + |1011\rangle + |0110\rangle + |1110\rangle - |0010\rangle - |1010\rangle - |0111\rangle - |1111\rangle)$$

q0 q2	q3	q1

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{4}(\,|0000\rangle + |1000\rangle + |0101\rangle + |1101\rangle - |0001\rangle - |1001\rangle - |0100\rangle - |1100\rangle + |0011\rangle + |1010\rangle + |0110\rangle + |1111\rangle - |0010\rangle - |1011\rangle - |0111\rangle - |1110\rangle)$$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{2}}(|0---\rangle + |1-+-\rangle)$$

Purpose

Analyse how separated the output of a program are.

approximation of

```
q0
q1 :=  |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{2}}(|0---\rangle + |1-+-\rangle)$$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

approximation of

$$\frac{1}{\sqrt{2}}(|0---\rangle + |1-+-\rangle)$$

Purpose

Analyse how separated the output of a program are.

```
q0 := |0⟩;
q1 := |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

approximation of

$$\frac{1}{\sqrt{2}}(|0---\rangle + |1-+-\rangle)$$

may be entangled

q0 q2 q3	q1

Purpose

Analyse how separated the output of a program are.

approximation of

```
q0
q1 :=  |0⟩;
q2 := |0⟩;
q3 := |1⟩;
H q3;
H q2;
CX q2, q3;
H q1;
CX q1, q3;
H q0;
CCX q0, q2, q3;
```

$$\frac{1}{\sqrt{2}}(|0---\rangle + |1-+-\rangle)$$

```
q0  q2        q3        q1
```

Previous work

- Measured qubit is separated from the others [Perdrix07]

Previous work

- Measured qubit is separated from the others [Perdrix07]

```
meas q0;
```

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]

```
U q0 q1;
```

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
- Restriction to CX gate [Perdrix08][Prost&Zerrari09]
  - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
  - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, [Perdrix07] Abstract interpretation [Perdrix08], Hoare-like logic [Prost&Zerrari09]

Abstract Interpretation

```
x := 312;
y := -251;
z := y * 31;
x := x + y * z;
if x > 0 then
    y := -y;
else
    y := x + y;
fi
z := z * y;
```

Concrete domain

$\mathbb{Z}^3$

x	312
y	-251
z	-7781

Abstract Interpretation

```
x := 312;
y := -251;
z := y * 31;
x := x + y * z;
if x > 0 then
    y := -y;
else
    y := x + y;
fi
z := z * y;
```

Concrete domain

$\mathbb{Z}^3$

x	1953343
y	251
z	1953031

Abstract Interpretation

```
x := 312;
y := -251;
z := y * 31;
x := x + y * z;
if x > 0 then
    y := -y;
else
    y := x + y;
fi
z := z * y;
```

Concrete domain

$\mathbb{Z}^3$

x	1953343
y	251
z	1953031

$z > 0?$

Abstract Interpretation

```
x := 312;
y := -251;
z := y * 31;
x := x + y * z;
if x > 0 then
    y := -y;
else
    y := x + y;
fi
z := z * y;
```

Concrete domain

$\mathbb{Z}^3$

x	1953343
y	251
z	1953031

Abstract domain

$\{+, -, \pm\}^3$

x	$+$
y	$-$
z	$-$

Abstract Interpretation

```
x := 312;
y := -251;
z := y * 31;
x := x + y * z;
if x > 0 then
    y := -y;
else
    y := x + y;
fi
z := z * y;
```

Concrete domain

$\mathbb{Z}^3$

x	1953343
y	251
z	1953031

Abstract domain

$\{+, -, \pm\}^3$

x	$+$
y	$+$
z	$+$

Quantum Imperative Language

$$
\begin{aligned}
C, C' ::= \ & \texttt{skip} \\
& \mid C ; C' \\
& \mid \texttt{X}(q_i) \mid \texttt{Y}(q_i) \mid \texttt{Z}(q_i) \\
& \mid \texttt{H}(q_i) \mid \texttt{S}(q_i) \mid \texttt{T}(q_i) \\
& \mid \texttt{CX}(q_i, q_j) \\
& \mid \texttt{if } q_i \texttt{ then } C \texttt{ else } C' \texttt{ fi} \\
& \mid \texttt{while } q_i \texttt{ do } C \texttt{ od}
\end{aligned}
$$

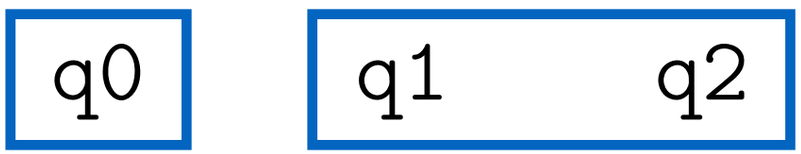
$$[\![C]\!] : \{\text{partial density matrix}\} \to \{\text{partial density matrix}\}$$

Abstract Domain $A^{\mathbf{Q}}$

[Perdrix08]

$$(\pi, b) \in A^{\mathbf{Q}}$$

π: partition



b: $\{\text{variables}\} \to \{\mathrm{I}, \mathrm{X}, \mathrm{Z}, \top\}$

q0	Z
q1	$\top$
q2	$\top$

Abstract Domain $A^{\mathbf{Q}}$

[Perdrix08]

$$(\pi, b) \in A^{\mathbf{Q}}$$

π: partition

b: $\{\text{variables}\} \to \{\mathrm{I}, \mathrm{X}, \mathrm{Z}, \top\}$

q0	q1 q2

q0	Z
q1	$\top$
q2	$\top$

$$\rho = p_0 |0\rangle\langle 0|_{\mathtt{q0}} \otimes \sigma^0_{\mathtt{q1,q2}} + p_1 \, |1\rangle\langle 1|_{\mathtt{q0}} \otimes \sigma^1_{\mathtt{q1,q2}}$$

Abstract Domain $A^{\mathbf{Q}}$

[Perdrix08]

$$(\pi, b) \in A^{\mathbf{Q}}$$

π: partition

b: $\{\text{variables}\} \to \{\mathrm{I}, \mathrm{X}, \mathrm{Z}, \top\}$

q0	q1 q2

q0	Z
q1	$\top$
q2	$\top$

$$\rho = p_0 |0\rangle\langle 0|_{\mathtt{q0}} \otimes \sigma^0_{\mathtt{q1},\mathtt{q2}} + p_1 \, |1\rangle\langle 1|_{\mathtt{q0}} \otimes \sigma^1_{\mathtt{q1},\mathtt{q2}}$$

$$[\![C]\!]^\natural : A^{\mathbf{Q}} \to A^{\mathbf{Q}}$$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

ρ

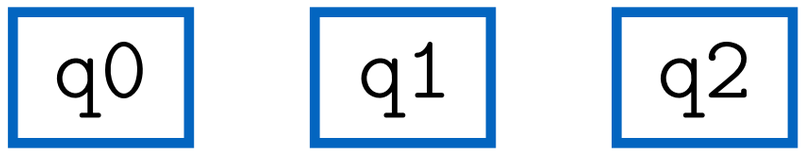
q0 q1 q2

q0	—
q1	—
q2	—

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$|100\rangle$

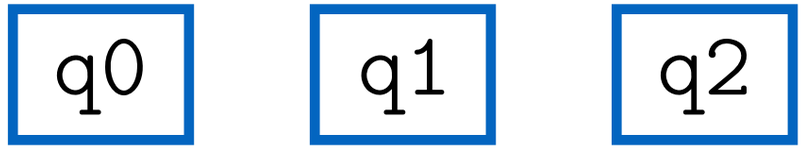


q0	Z
q1	Z
q2	Z

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$|10+\rangle$



q0	Z
q1	Z
q2	X

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$|10+\rangle$

q0 q1 q2

q0	Z
q1	Z
q2	X

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$|-0+\rangle$

q0 q1 q2

q0	X
q1	Z
q2	X

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$$\frac{1}{\sqrt{2}} |-0\rangle (|0\rangle + e^{i\frac{\pi}{4}} |1\rangle)$$

q0 q1 q2

q0	X
q1	Z
q2	⊤

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$$\frac{1}{\sqrt{2}} |{-0}\rangle \left(|0\rangle + e^{i\frac{\pi}{4}} |1\rangle\right)$$

q0 q1 q2

q0	X
q1	Z
q2	⊤

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$$\frac{1}{\sqrt{2}} |{-0}\rangle \left(|0\rangle - e^{i\frac{\pi}{4}} |1\rangle\right)$$

q0 q1 q2

q0	X
q1	Z
q2	⊤

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$$\frac{1}{2}(|00\rangle - |11\rangle)(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle)$$

q0 q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Soundness

[Perdrix08]

$\forall \rho$: quantum state

$\forall (\pi, b) \in A^{\mathbf{Q}}$

$\forall C$: program

$$(\pi, b) \vDash \rho \Rightarrow [\![C]\!]^{\natural}(\pi, b) \vDash [\![C]\!](\rho)$$

Soundness

[Perdrix08]

$\forall \rho$: quantum state

$\forall (\pi, b) \in A^{\mathbf{Q}}$

$\forall C$: program

$$(\pi, b) \vDash \rho \Rightarrow [\![C]\!]^{\natural}(\pi, b) \vDash [\![C]\!](\rho)$$

valid approximation

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
```

$$\frac{1}{2}(|00\rangle - |11\rangle)(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle)$$

q0 q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

$$\frac{1}{2}(|00\rangle - |11\rangle)(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle)$$

q0 q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

$$\frac{1}{2}(|00\rangle - |11\rangle)(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle)$$

q0 q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

$$\frac{1}{\sqrt{2}} |0-\rangle (|0\rangle - e^{i\frac{\pi}{4}} |1\rangle)$$

q0 q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

$$\frac{1}{2}\,|0\rangle\,(\,|00\rangle - e^{i\frac{\pi}{4}}\,|01\rangle + e^{i\frac{\pi}{4}}\,|10\rangle - |11\rangle)$$

q0	q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX [Prost&Zerrari09]
  - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
  - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

disentangle

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
```

ρ

q0 q1 q2

q0	—
q1	—
q2	—

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
```

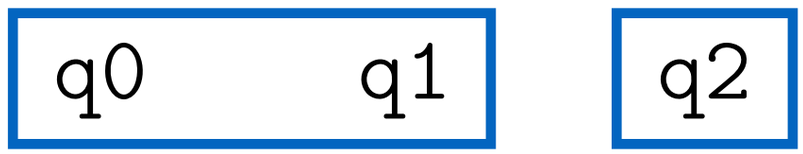
$|+00\rangle$

q0	X
q1	Z
q2	Z

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
```

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,|0\rangle$$



q0	⊤
q1	⊤
q2	Z

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
```

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

q0	q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

q0	q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

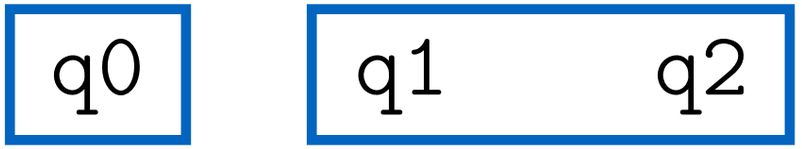
q0	q1	q2

q0	$\top$
q1	$\top$
q2	$\top$

Abstract Semantics $[\![\cdot]\!]^\natural$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$



q0	Z
q1	⊤
q2	⊤

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Multi-qubit gate may entangle qubits [Perdrix07]
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Previous work

- Measured qubit is separated from the others [Perdrix07]
- Measurement may affect unmeasured qubits
  - Restriction to CX gate [Perdrix08][Prost&Zerrari09]
    - C-qubit $|0\rangle/|1\rangle$ preserves separability [Perdrix08][Prost&Zerrari09]
    - T-qubit $|\pm\rangle$ preserves separability [Perdrix08]
- Type system, Abstract interpretation, Hoare-like logic
  [Perdrix07] [Perdrix08] [Prost&Zerrari09]

Observation

- Multi-qubit gate may undo entangled qubits
- Measurement may destroy multipartite entanglement

Observation

- Multi-qubit gate may undo entangled qubits
- Measurement may destroy multipartite entanglement
- Information about entangled qubits is needed
- Semantics should be easily computable

Observation

- Multi-qubit gate may undo entangled qubits
- Measurement may destroy multipartite entanglement
- Information about entangled qubits is needed
- Semantics should be easily computable

Stabilizer Formalism

Stabilizer Formalism

standard

$$|\psi\rangle = \alpha_{0\ldots00}\,|0\cdots00\rangle + \cdots + \alpha_{1\ldots11}\,|1\cdots11\rangle$$

e.g.

$$\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$$

stabilizer

$$\{P \,|P\text{: Pauli matrix s.t. } P\,|\psi\rangle = |\psi\rangle\}$$

$$\{\mathrm{III}, \mathrm{XXX}, -\mathrm{ZZI}, -\mathrm{IZZ}, \mathrm{ZIZ}, \mathrm{YYX}, -\mathrm{YXY}, \mathrm{XYY}\}$$

Stabilizer Formalism

standard

$$|\psi\rangle = \alpha_{0\ldots00}\,|0\cdots00\rangle + \cdots + \alpha_{1\ldots11}\,|1\cdots11\rangle$$

e.g.

$$\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$$

stabilizer

$$\{P \,|P\text{: Pauli matrix s.t. } P\,|\psi\rangle = |\psi\rangle\}$$

$$\{\mathrm{III}, \mathrm{XXX}, -\mathrm{ZZI}, -\mathrm{IZZ}, \mathrm{ZIZ}, \mathrm{YYX}, -\mathrm{YXY}, \mathrm{XYY}\}$$

$$\begin{bmatrix} \mathrm{X} & \mathrm{X} & \mathrm{X} & + \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} & - \\ \mathrm{Z} & \mathrm{I} & \mathrm{Z} & + \end{bmatrix}$$

Stabilizer Formalism

standard

$$|\psi\rangle = \alpha_{0\ldots00}\,|0\cdots00\rangle + \cdots + \alpha_{1\ldots11}\,|1\cdots11\rangle$$

e.g.

$$\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$$

stabilizer

$$\{P \,|P\text{: Pauli matrix s.t. } P\,|\psi\rangle = |\psi\rangle\}$$

$$\{\mathrm{III}, \mathrm{XXX}, -\mathrm{ZZI}, -\mathrm{IZZ}, \mathrm{ZIZ}, \mathrm{YYX}, -\mathrm{YXY}, \mathrm{XYY}\}$$

$$\begin{bmatrix} \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{Z} & \mathrm{I} & \mathrm{Z} \end{bmatrix}$$

Stabilizer Formalism

standard

$$|\psi\rangle = \alpha_{0\ldots00}\,|0\cdots00\rangle + \cdots + \alpha_{1\ldots11}\,|1\cdots11\rangle$$

e.g.

$$\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$$

$$\rho = \sum_a |\psi_a\rangle\langle\psi_a| \otimes \rho_a$$

stabilizer

$$\{P \,|P\text{: Pauli matrix s.t. } P\,|\psi\rangle = |\psi\rangle\}$$

$$\{\mathrm{III}, \mathrm{XXX}, -\mathrm{ZZI}, -\mathrm{IZZ}, \mathrm{ZIZ}, \mathrm{YYX}, -\mathrm{YXY}, \mathrm{XYY}\}$$

$$\begin{bmatrix} \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{Z} & \mathrm{I} & \mathrm{Z} \end{bmatrix}$$

Stabilizer Formalism

standard

$$|\psi\rangle = \alpha_{0\ldots00}\,|0\cdots00\rangle + \cdots + \alpha_{1\ldots11}\,|1\cdots11\rangle$$

e.g.

$$\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$$

$$\rho = p_0\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|\,\sigma^0 + p_1(\mathrm{IIX})\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|\,(\mathrm{IIX})\sigma^1 + \cdots$$

stabilizer

$$\{P\,|P\text{: Pauli matrix s.t. } P\,|\psi\rangle = |\psi\rangle\}$$

$$\{\mathrm{III}, \mathrm{XXX}, -\mathrm{ZZI}, -\mathrm{IZZ}, \mathrm{ZIZ}, \mathrm{YYX}, -\mathrm{YXY}, \mathrm{XYY}\}$$

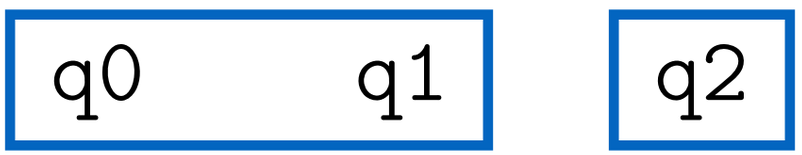
$$\begin{bmatrix} \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{Z} & \mathrm{I} & \mathrm{Z} \end{bmatrix}$$

Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers

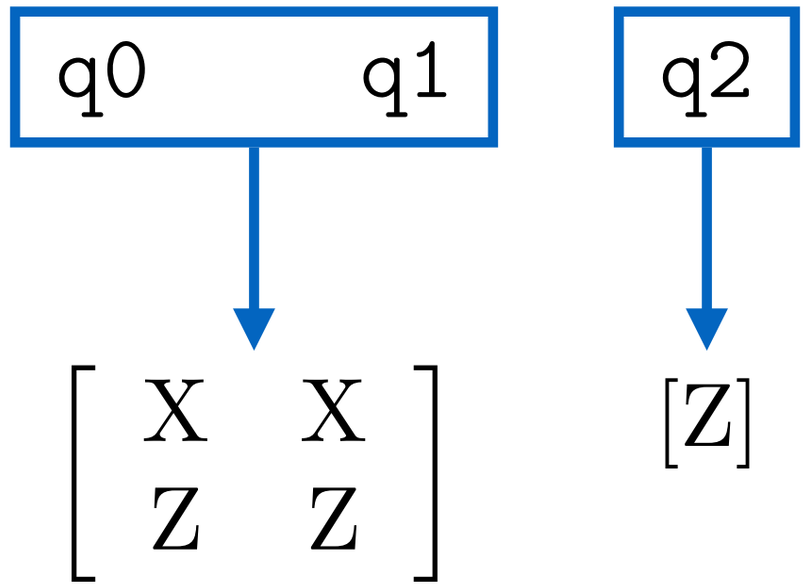
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



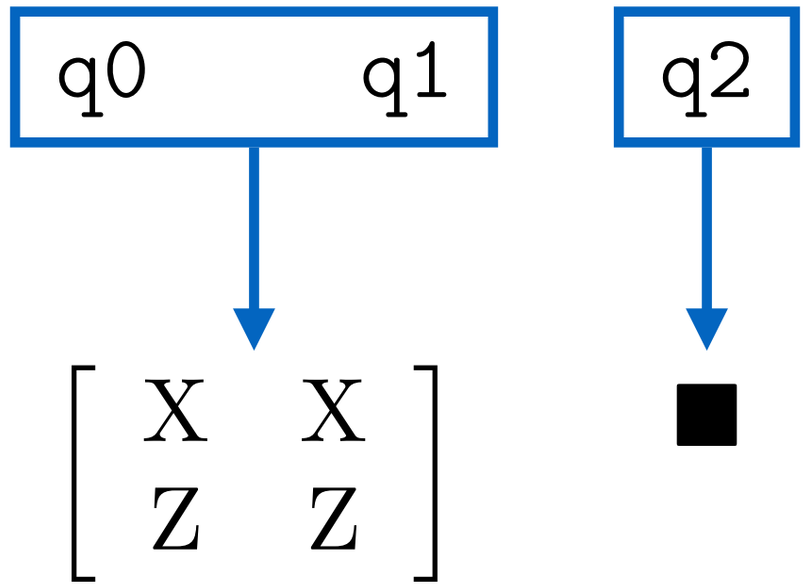
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



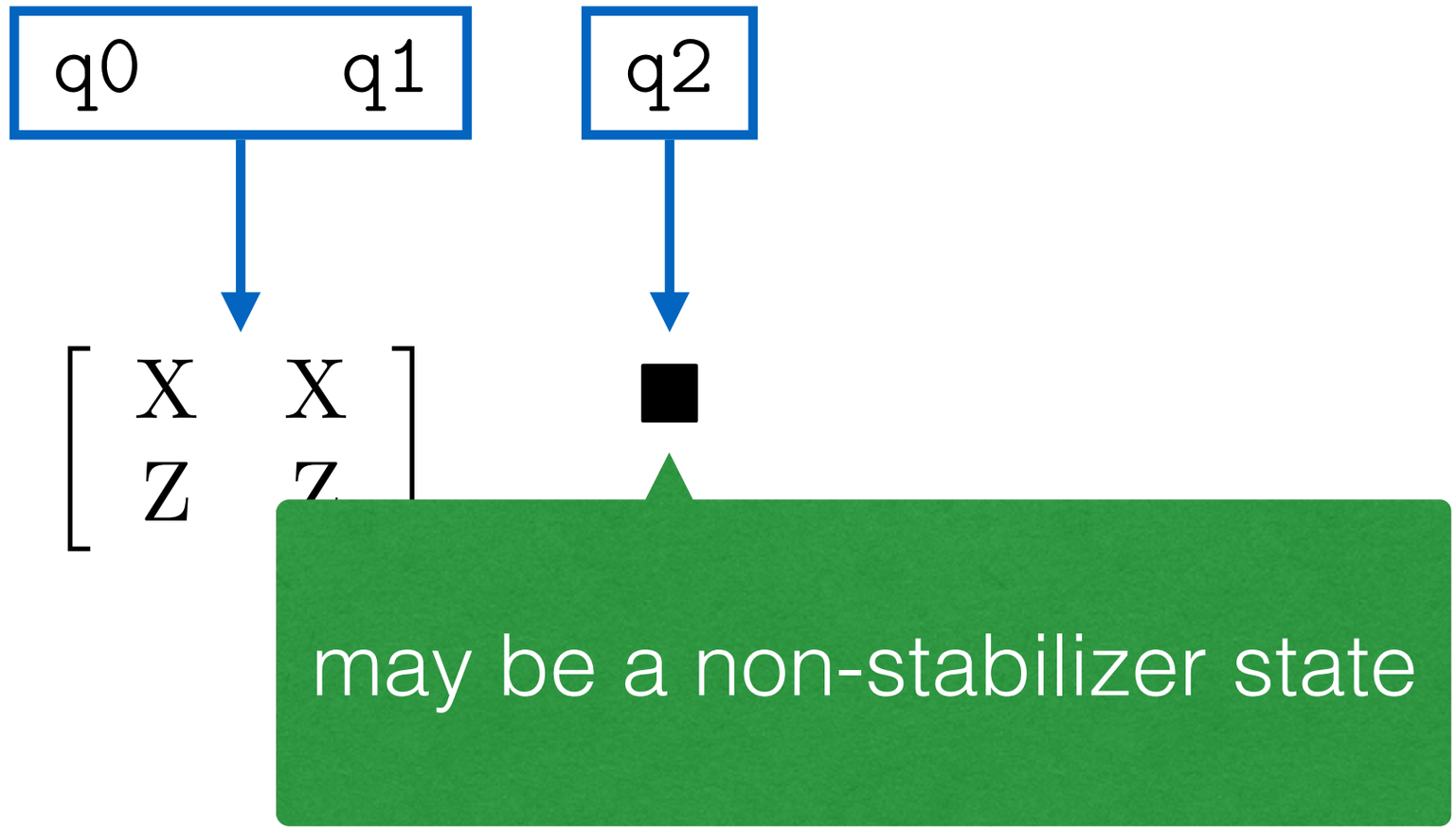
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



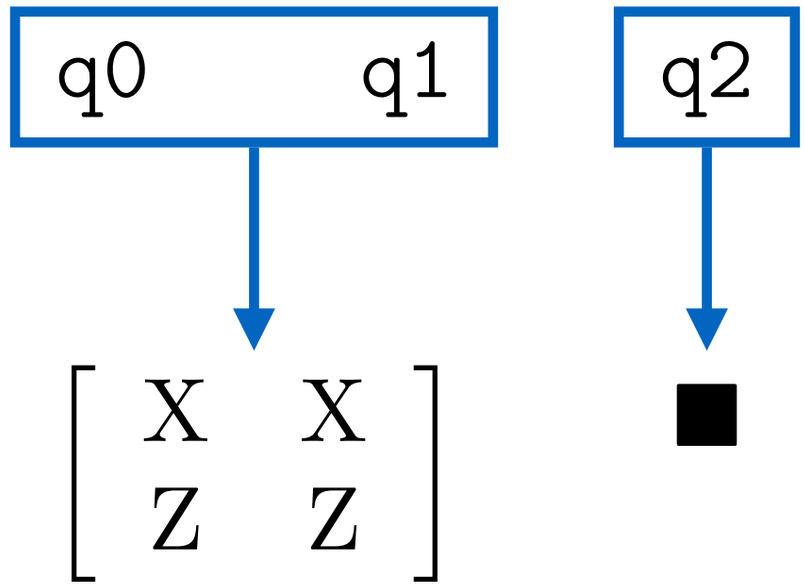
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



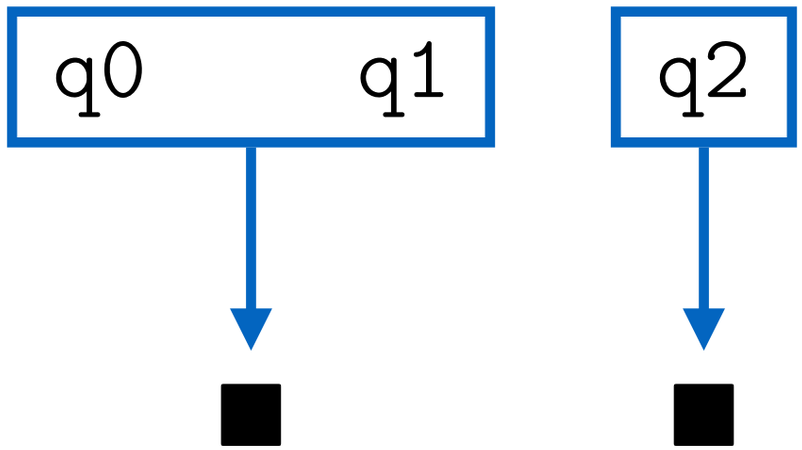
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



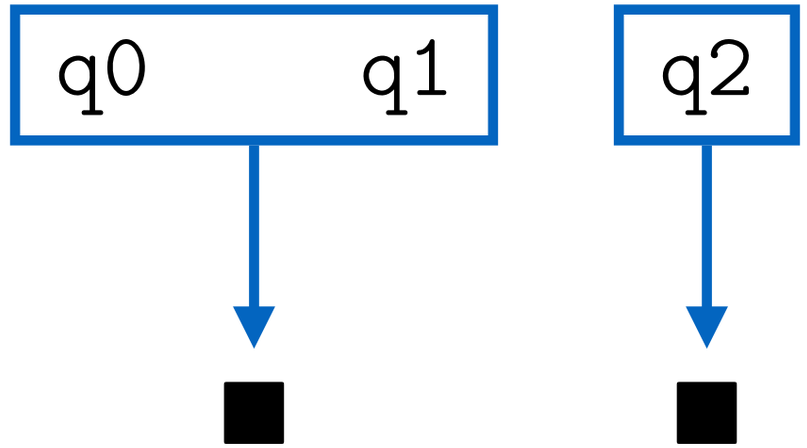
Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers



Our Abstract Domain $C^{\mathbf{Q}}$

Partition with stabilizers

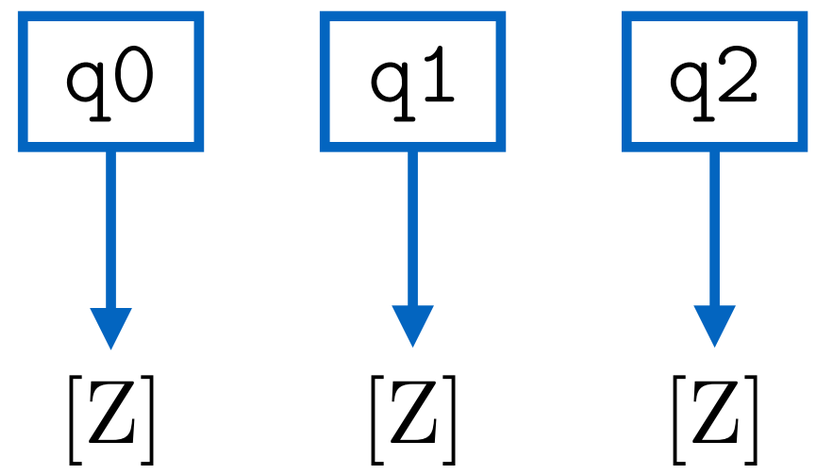


$$[\![C]\!]_{\mathrm{C}} : C^{\mathbf{Q}} \to C^{\mathbf{Q}}$$

Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

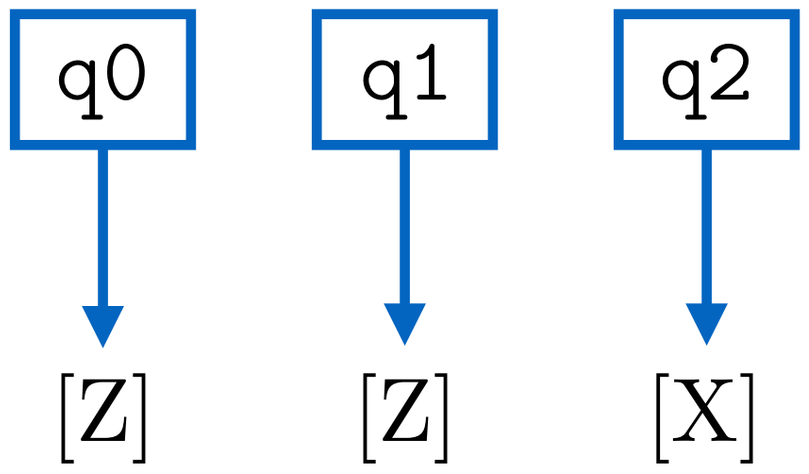
$|100\rangle$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

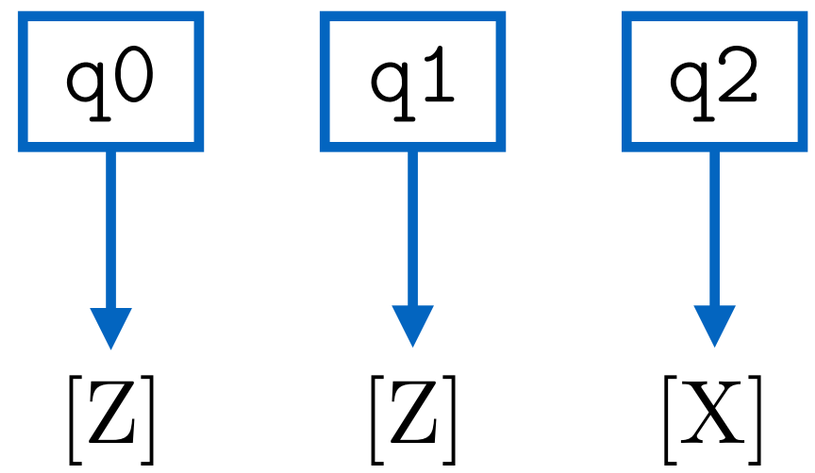
$|10+\rangle$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

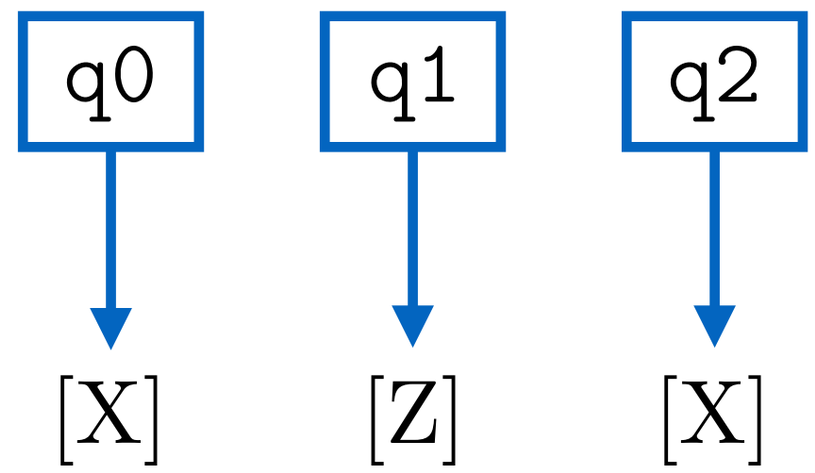
$|10+\rangle$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

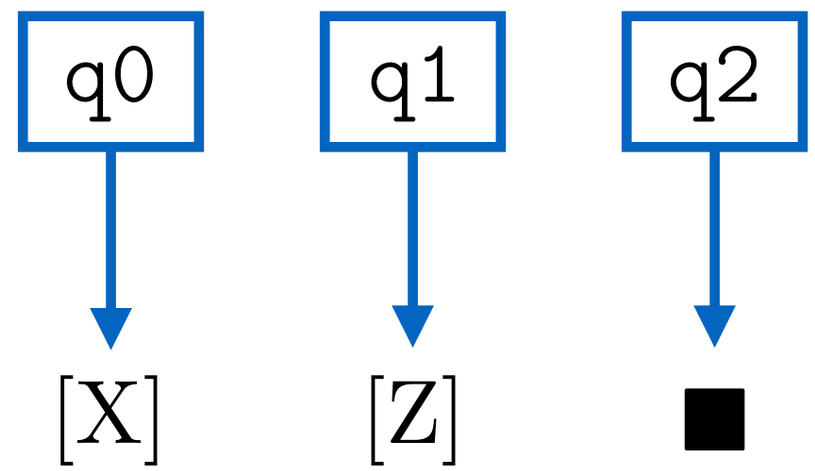
$|-0+\rangle$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

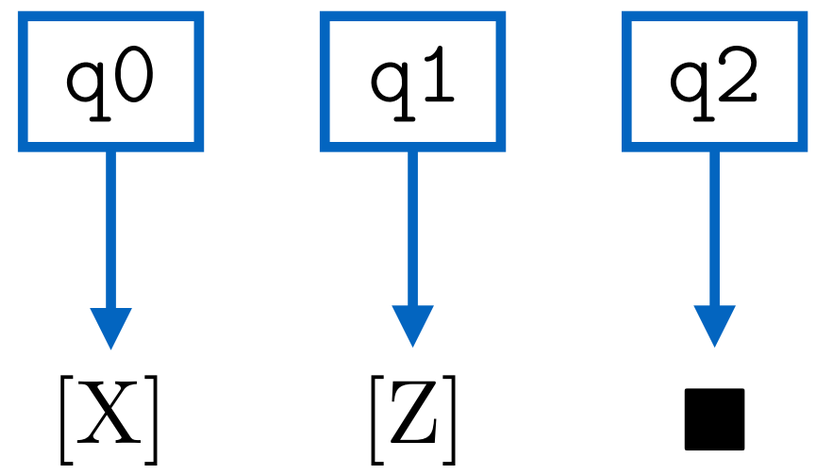
$$\frac{1}{\sqrt{2}} |-0\rangle (|0\rangle + e^{i\frac{\pi}{4}} |1\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

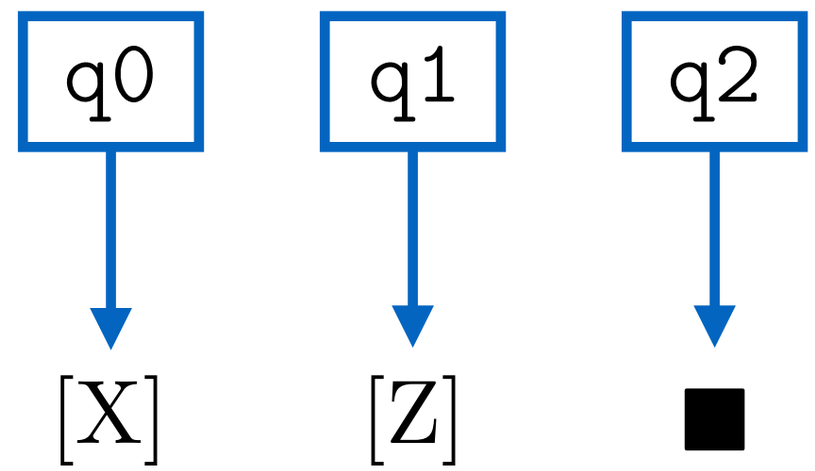
$$\frac{1}{\sqrt{2}} |-0\rangle (|0\rangle + e^{i\frac{\pi}{4}} |1\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

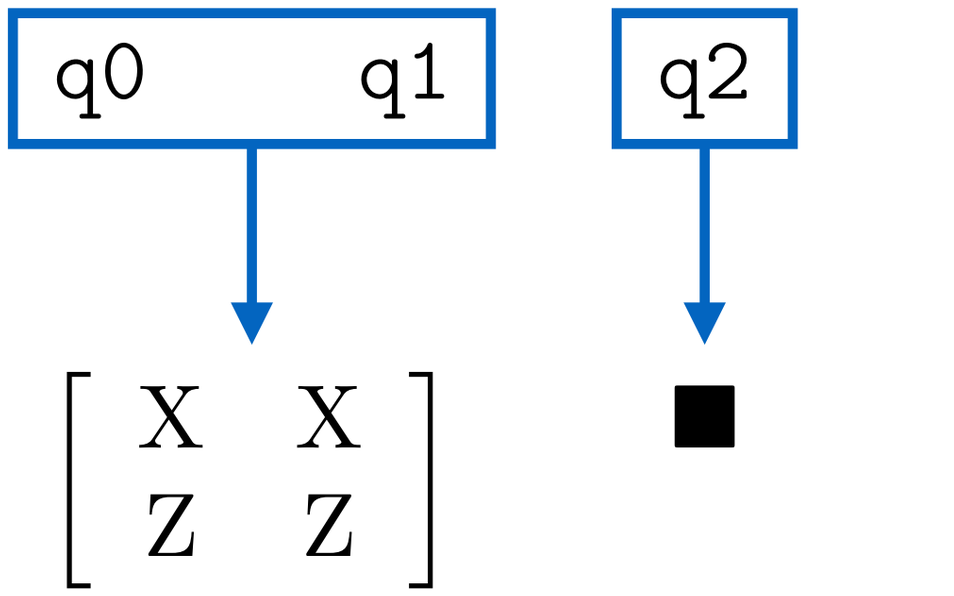
$$\frac{1}{\sqrt{2}} |-0\rangle \left(|0\rangle - e^{i\frac{\pi}{4}} |1\rangle\right)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

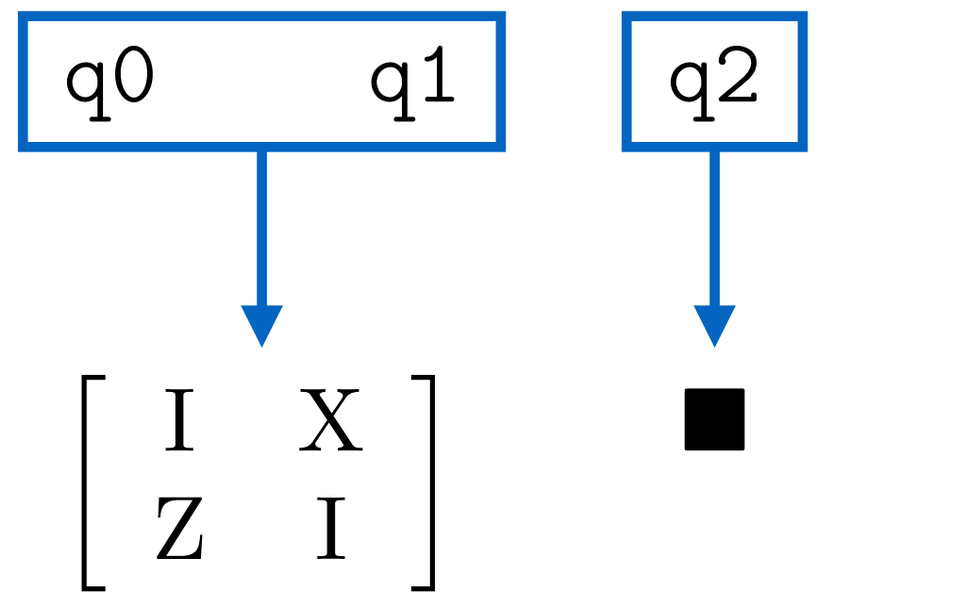
$$\frac{1}{2}(|00\rangle - |11\rangle)(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

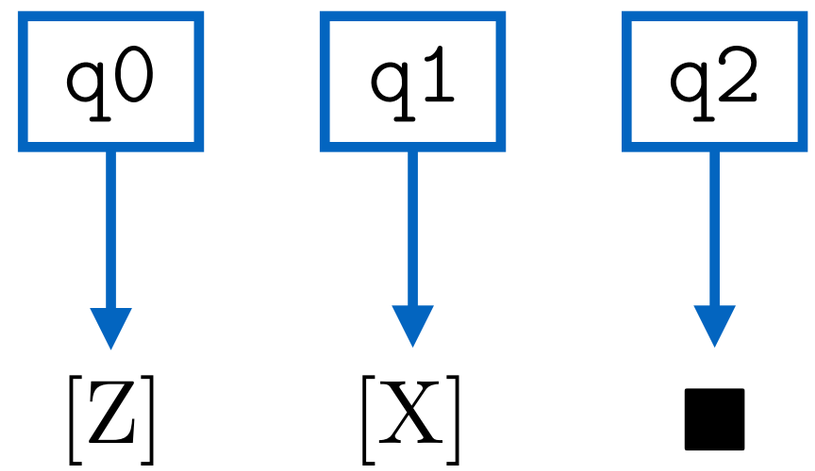
$$\frac{1}{\sqrt{2}} |0-\rangle (|0\rangle - e^{i\frac{\pi}{4}} |1\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

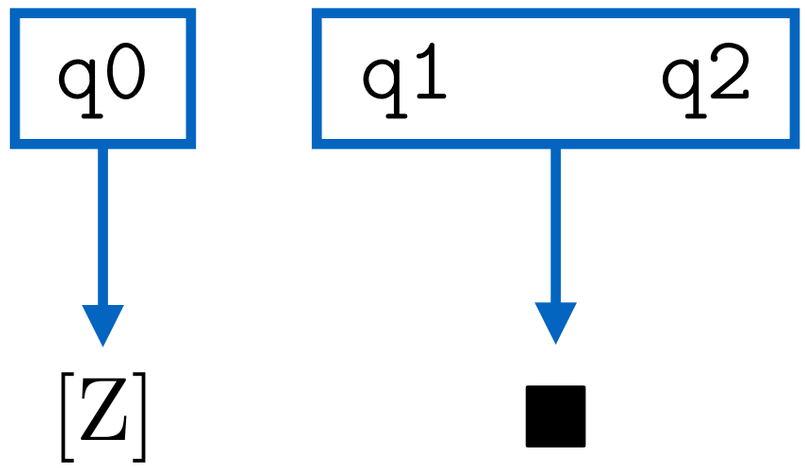
$$\frac{1}{\sqrt{2}} |0-\rangle \left(|0\rangle - e^{i\frac{\pi}{4}} |1\rangle\right)$$



Abstract Semantics $[\![\cdot]\!]_{\mathrm{C}}$

```
q0 := |1⟩;
q1 := |0⟩;
q2 := |0⟩;
H q2;
T q1;
H q0;
T q2;
CX q1, q2;
CX q2, q0;
CX q0, q1;
CX q1, q0;
CX q1, q2;
```

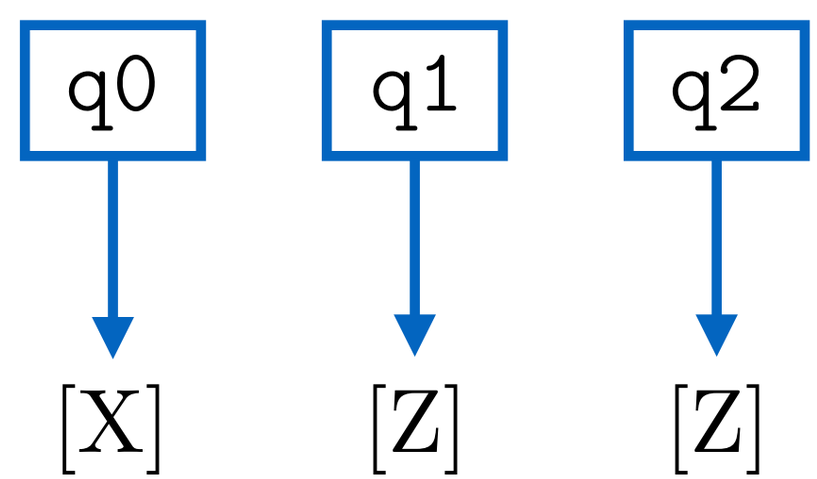
$$\frac{1}{2}\,|0\rangle\,(\,|00\rangle - e^{i\frac{\pi}{4}}\,|01\rangle + e^{i\frac{\pi}{4}}\,|10\rangle - |11\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

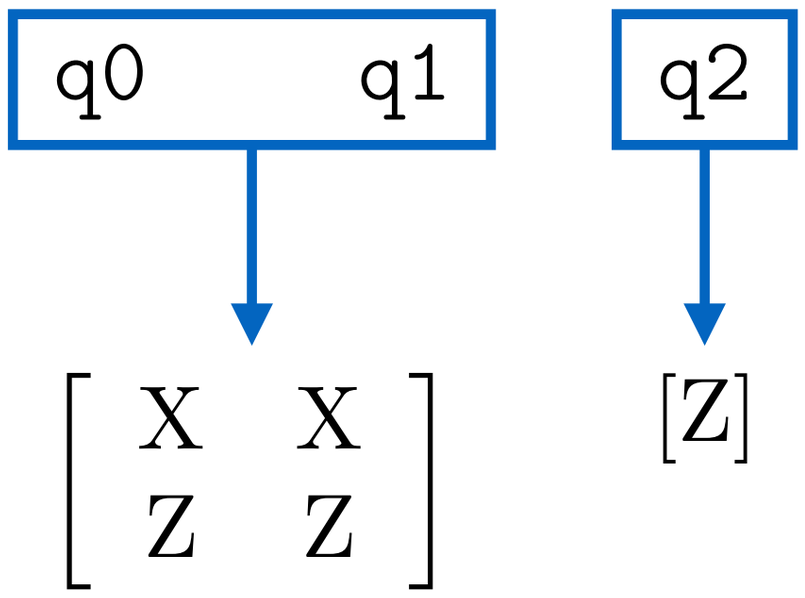
$|+00\rangle$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

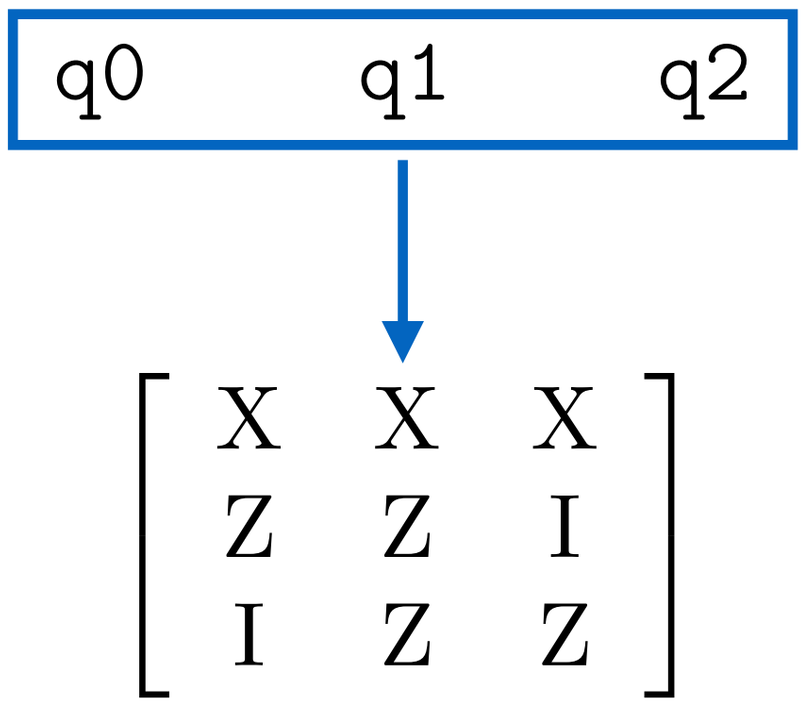
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,|0\rangle$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

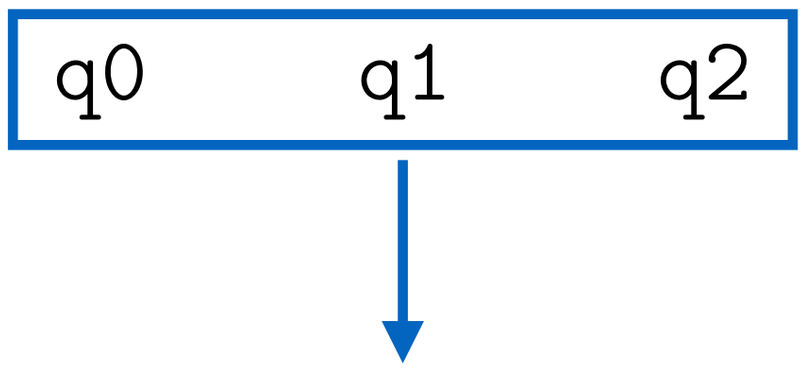
$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$



Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$

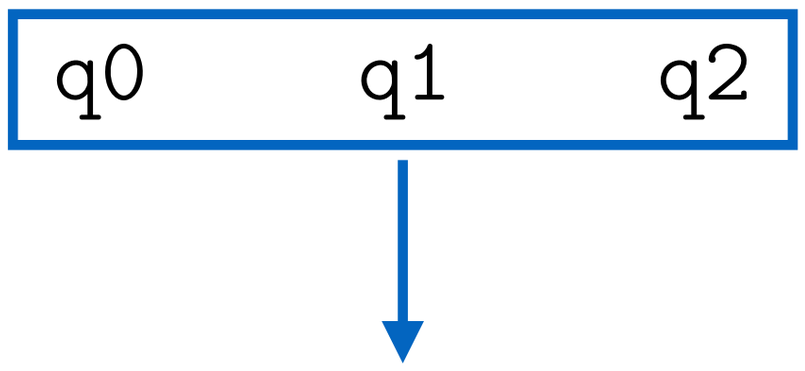


$$\begin{bmatrix} Z & I & I \\ Z & Z & I \\ I & Z & Z \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$

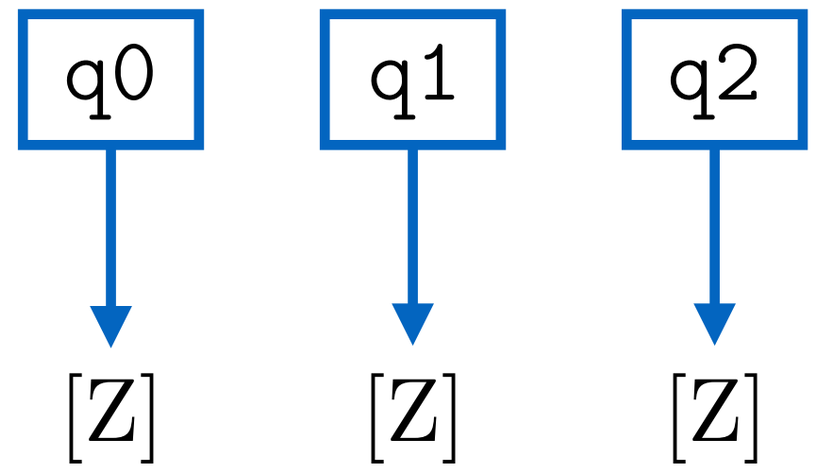


$$\begin{bmatrix} Z & I & I \\ I & Z & I \\ I & I & Z \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$



Soundness

$\forall \rho$: quantum state

$\forall \alpha \in C^{\mathbf{Q}}$

$\forall C$: program

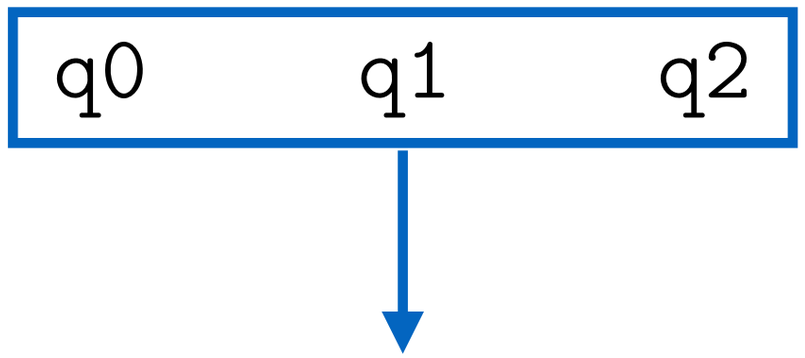
$$\alpha \vDash \rho \Rightarrow [\![C]\!]_{\mathrm{C}}(\alpha) \vDash [\![C]\!](\rho)$$

For better
approximation

Abstract Semantics $[\![\cdot]\!]_C$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

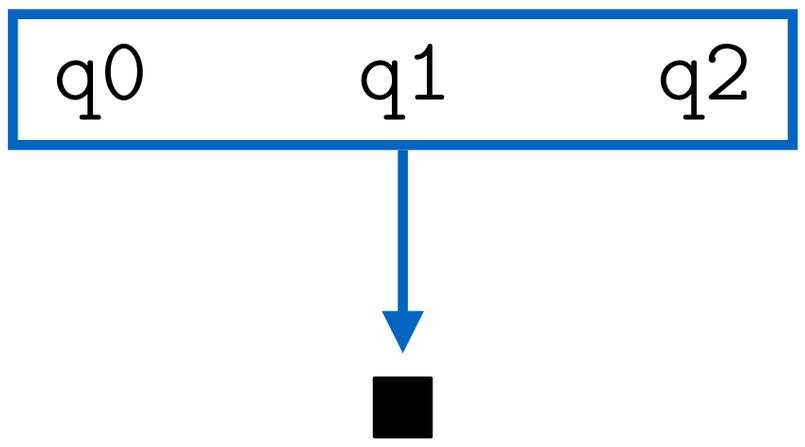


$$\begin{bmatrix} X & X & X \\ Z & Z & I \\ I & Z & Z \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

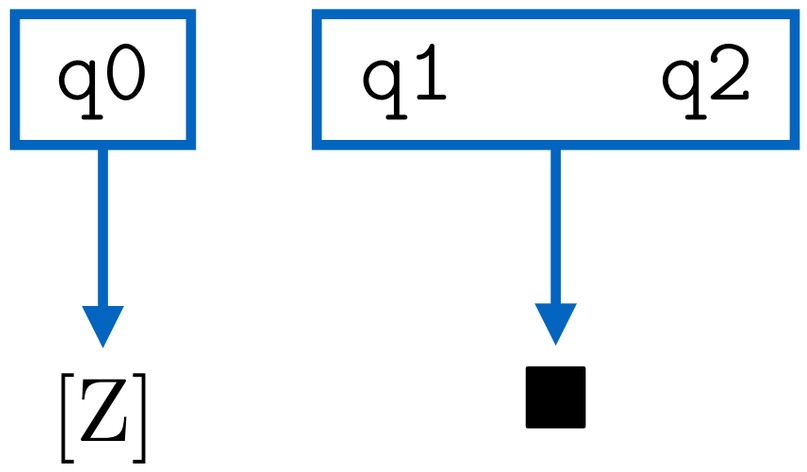
$$\frac{1}{\sqrt{2}}(|000\rangle + e^{i\frac{\pi}{4}}\,|111\rangle)$$



Abstract Semantics $[\![\cdot]\!]_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

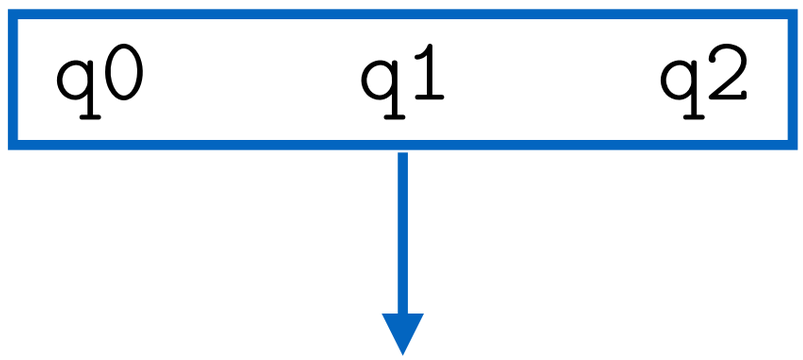
$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$



Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

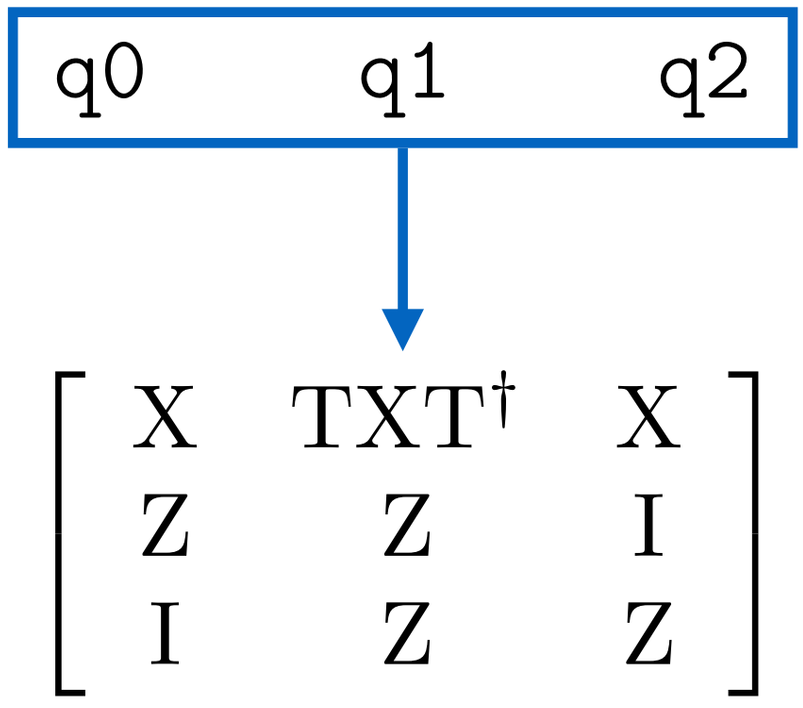


$$\begin{bmatrix} \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

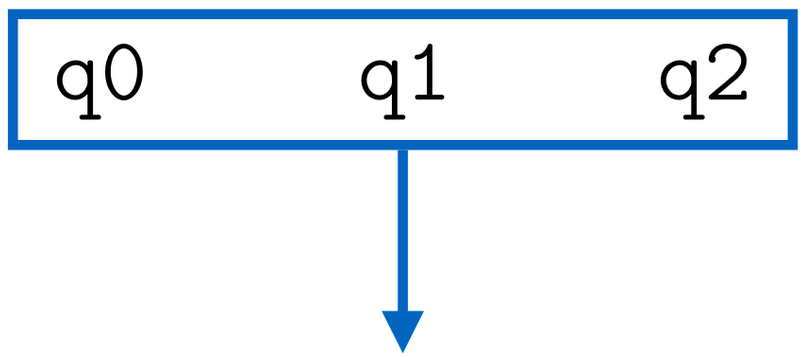
$$\frac{1}{\sqrt{2}}(|000\rangle + e^{i\frac{\pi}{4}}\,|111\rangle)$$



Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$

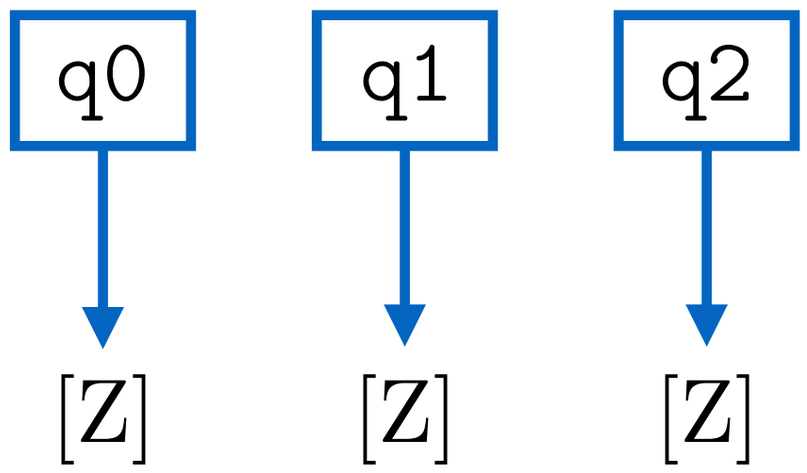


$$\begin{bmatrix} \mathrm{Z} & \mathrm{I} & \mathrm{I} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

```
q0 := |+⟩;
q1 := |0⟩;
q2 := |0⟩;
CX q0, q1;
CX q1, q2;
T q1;
meas q0;
```

$$\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$



Abstract Semantics $[\![\cdot]\!]_{\mathrm{C}}^{'}$

$$\begin{bmatrix} \mathrm{X} & \mathrm{TXT}^{\dagger} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{bmatrix}$$

Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

$$\left[\begin{array}{ccc} \mathrm{X} & \mathrm{TXT}^{\dagger} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{array}\right]$$

Abstract Semantics $[\![\cdot]\!]_{\mathrm{C}}^{'}$

$$\left[\begin{array}{ccc} \boxed{\mathrm{X}} & \mathrm{TXT}^{\dagger} & \mathrm{X} \\ \boxed{\begin{array}{ccc} \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{array}} & & \end{array}\right]$$

Abstract Semantics $[\![\cdot]\!]'_{\mathrm{C}}$

$$\left[\begin{array}{ccc} \mathrm{X} & \heartsuit & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{array}\right]$$

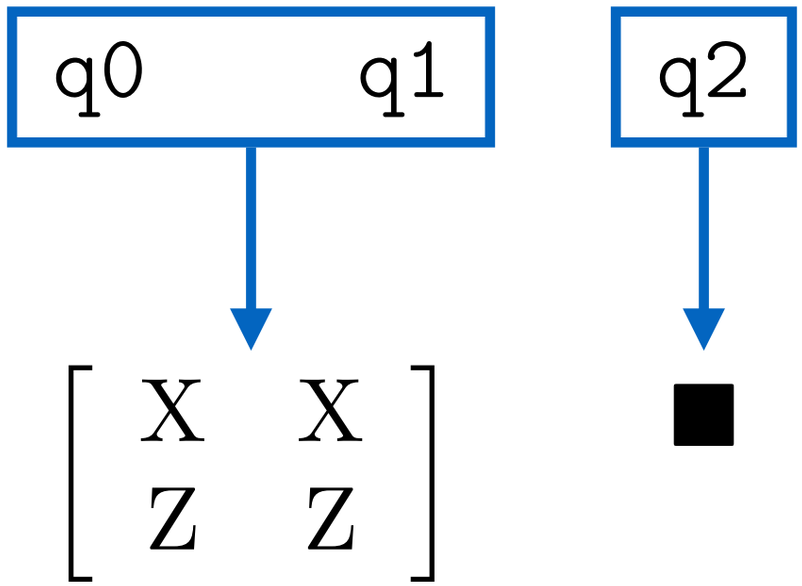
Abstract Semantics $[\![\cdot]\!]'_C$

may be a non-Pauli matrix

$$\left[\begin{array}{ccc} \boxed{\mathrm{X}} & \heartsuit & \mathrm{X} \\ \boxed{\begin{array}{ccc} \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} \end{array}} & & \end{array}\right]$$

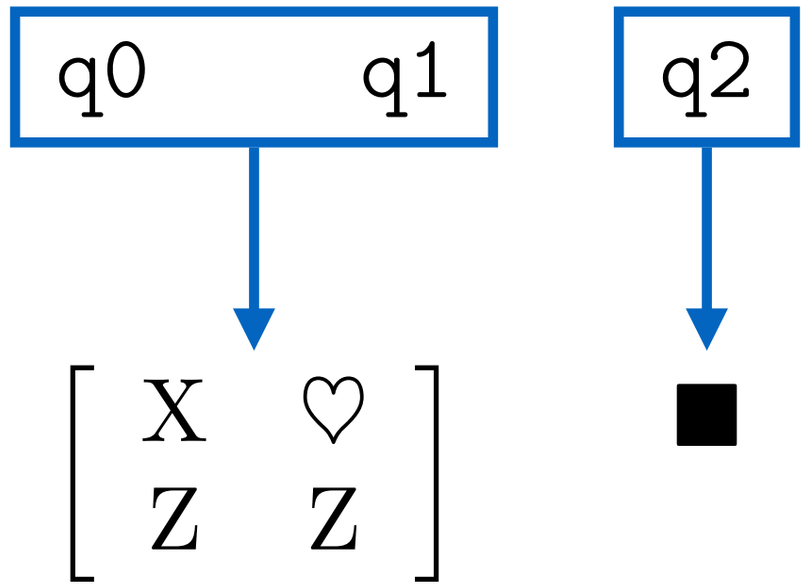
Abstract Domain $E^{\mathbf{Q}}$

Partition with stabilizers



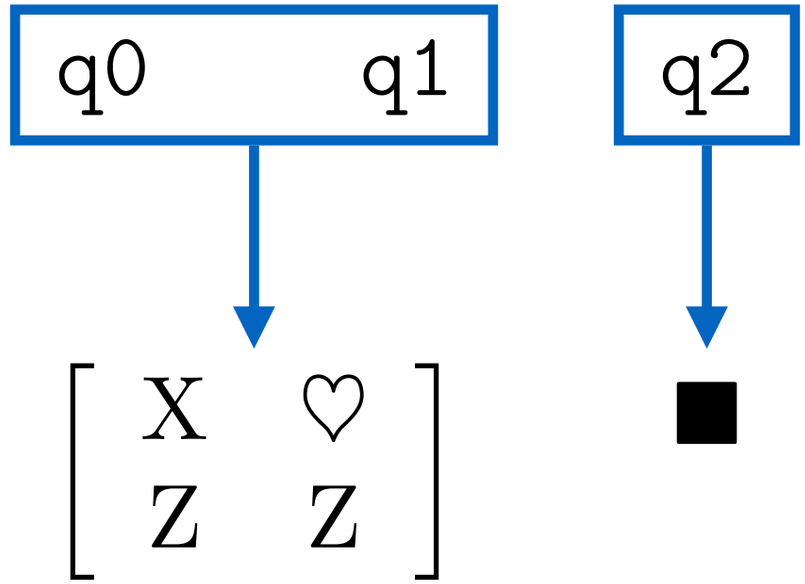
Abstract Domain $E^{\mathbf{Q}}$

Partition with stabilizers



Abstract Domain $E^{\mathbf{Q}}$

Partition with stabilizers



$$[\![C]\!]_{\mathrm{E}} \colon E^{\mathbf{Q}} \to E^{\mathbf{Q}}$$

Structure of $E^{\mathbf{Q}}$

$$\left[\begin{array}{cc} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{array}\right] \vee \left[\begin{array}{cc} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{array}\right]$$

Structure of $E^{\mathbf{Q}}$

$$\begin{bmatrix} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{bmatrix} \vee \begin{bmatrix} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{bmatrix} = \begin{bmatrix} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{bmatrix}$$

$$\begin{bmatrix} \mathrm{X} & \mathrm{I} \\ \mathrm{I} & \mathrm{X} \end{bmatrix} \vee \begin{bmatrix} \mathrm{X} & \mathrm{Z} \\ \mathrm{Z} & \mathrm{X} \end{bmatrix} \neq \begin{bmatrix} \mathrm{X} & \heartsuit \\ \heartsuit & \mathrm{X} \end{bmatrix}$$

Semantics of If

$$\left[\!\!\left[\begin{array}{lll} \texttt{if} & \texttt{qi} & \\ & \texttt{then} & C \\ & \texttt{else} & C' \\ \texttt{fi} & & \end{array} \right]\!\!\right]_{\mathrm{E}} = [\![C]\!]_{\mathrm{E}} \vee [\![C']\!]_{\mathrm{E}}$$

Semantics of If

$$\left[\!\!\left[\begin{array}{lll} \texttt{if} & \texttt{qi} & \\ & \texttt{then} & C \\ & \texttt{else} & C' \\ \texttt{fi} & & \end{array} \right]\!\!\right]_{\mathrm{E}} = [\![C]\!]_{\mathrm{E}} \uplus [\![C']\!]_{\mathrm{E}}$$

Approximate Join

$$\begin{bmatrix} \mathrm{X} & \heartsuit & \mathrm{Z} \\ \mathrm{Z} & \mathrm{I} & \heartsuit \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix} \qquad \begin{bmatrix} \heartsuit & \heartsuit & \mathrm{Z} \\ \mathrm{Z} & \mathrm{I} & \heartsuit \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix}$$

Approximate Join

$$\begin{bmatrix} X & \heartsuit & Z \\ Z & I & \heartsuit \\ Z & Z & I \end{bmatrix} \qquad \begin{bmatrix} \heartsuit & \heartsuit & Z \\ Z & I & \heartsuit \\ Z & Z & I \end{bmatrix}$$

$$\downarrow \qquad \downarrow$$

$$\begin{bmatrix} \\ \\ Z & Z & I \end{bmatrix} \qquad \begin{bmatrix} \\ \\ Z & Z & I \end{bmatrix}$$

Approximate Join

$$\begin{bmatrix} X & \heartsuit & Z \\ Z & I & \heartsuit \\ Z & Z & I \end{bmatrix} \qquad \begin{bmatrix} \heartsuit & \heartsuit & Z \\ Z & I & \heartsuit \\ Z & Z & I \end{bmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\begin{bmatrix} \\ \\ Z & Z & I \end{bmatrix} \quad \vee \quad \begin{bmatrix} \\ \\ Z & Z & I \end{bmatrix}$$

$$= \begin{bmatrix} Z & Z & I \end{bmatrix}$$

Approximate Join

$$\begin{bmatrix} \mathrm{X} & \heartsuit & \mathrm{Z} \\ \mathrm{Z} & \mathrm{I} & \heartsuit \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix} \uplus \begin{bmatrix} \heartsuit & \heartsuit & \mathrm{Z} \\ \mathrm{Z} & \mathrm{I} & \heartsuit \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix}$$

$$= \begin{bmatrix} & & \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix} \vee \begin{bmatrix} & & \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix}$$

$$= \begin{bmatrix} \mathrm{Z} & \mathrm{Z} & \mathrm{I} \end{bmatrix}$$

Soundness

$\forall \rho$: quantum state

$\forall \gamma \in E^{\mathbf{Q}}$

$\forall C$: program

$$\gamma \vDash \rho \Rightarrow [\![C]\!]_{\mathrm{E}}(\gamma) \vDash [\![C]\!](\rho)$$

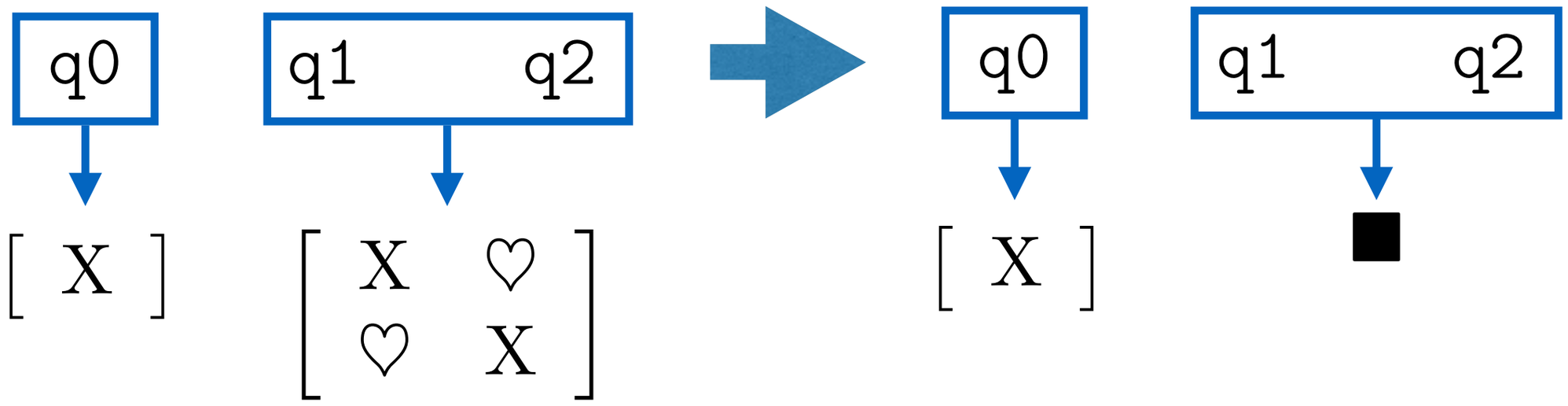
Summary

- Refined the existing abstract domain
  - Used stabilizer formalism with ■
- Improved the above abstract domain
  - Introduced the non-Pauli symbol ♡
  - Introduced the approximate join operator
- Proved soundness

Future Work

- Implementation
- Further Refinement
  - Better join

```
if q0 then skip else skip;
```



Future Work

- Implementation
- Further Refinement
- Better join

```
if q0 then skip else skip;
```