Gottesman Types for Quantum Programs

Quantum Physics and Logic, 2020

Robert Rand, Aarthi Sundaram, Kartik Singhal and Brad Lackey

Types for Quantum Programs

Types for Quantum Programs

- Linear Types
  - Prevent cloning of qubits [Quantum λ-calculus, ProtoQuipper, QWIRE]

Types for Quantum Programs

- Linear Types
  - Prevent cloning of qubits [Quantum λ-calculus, ProtoQuipper, QWIRE]
- Quantum Data Structures
  - Pairs, Lists and Trees of qubits [Quantum IO Monad, Quipper]

Types for Quantum Programs

- Linear Types
  - Prevent cloning of qubits [Quantum λ-calculus, ProtoQuipper, QWIRE]
- Quantum Data Structures
  - Pairs, Lists and Trees of qubits [Quantum IO Monad, Quipper]
- Dependent Types
  - Allow precise description of circuit datatypes [ProtoQuipper, QWIRE]

Quantum Base Types

- Qubit
- Bit
- Unit

Bits

`Bit <: Qubit`

$|0\rangle$ `: Bit`

$|1\rangle$ `: Bit`

Bits!

Bits!

- Make convenient ancillae

Bits!

- Make convenient ancillae
- Are invariant under measurement

Bits!

- Make convenient ancillae
- Are invariant under measurement
- Can be converted to Boolean values

Bits!

- Make convenient ancillae
- Are invariant under measurement
- Can be converted to Boolean values
- Can be duplicated

XBits

```
X <: Qubit

|+⟩ : X

|−⟩ : X
```

XBits

```
X <: Qubit

|+⟩ : X

|-⟩ : X
```

Also duplicable!

XBits

```
X <: Qubit

|+⟩ : X

|−⟩ : X
```

Also duplicable!

Useful for creating entangled pairs!

Ebits

Ebits

- Units of quantum entanglement

Ebits

- Units of quantum entanglement
- For our purposes: Qubits in Bell pairs

Ebits

- Units of quantum entanglement
- For our purposes: Qubits in Bell pairs
- Valuable for quantum communication

How Do We Get There?

How Do We Get There?

- Track bits, xbits and bell pairs?
  - Most quantum states are none-of-the-above

How Do We Get There?

- Track bits, xbits and bell pairs?
  - Most quantum states are none-of-the-above
- Infer types by doing the computation?
  - No

How Do We Get There?

- Track bits, xbits and bell pairs?
  - Most quantum states are none-of-the-above
- Infer types by doing the computation?
  - No
- Start with Clifford circuits and work from there?

Heisenberg

- Don't think of functions on qubits, think of operators as operators on operators.
- For instance, $HX = ZH$ and $HZ = XH$
- So H is a function from X to Z (and back)!

Gottesman

$$H : X \to Z \qquad CNOT : X \otimes I \to X \otimes X$$
$$H : Z \to X \qquad CNOT : I \otimes X \to I \otimes X$$
$$S : X \to Y \qquad CNOT : Z \otimes I \to Z \otimes I$$
$$S : Z \to Z \qquad CNOT : I \otimes Z \to Z \otimes Z$$

[Daniel Gottesman, 1998]

Gottesman

$$\begin{array}{ll} H : X \to Z & CNOT : X \otimes I \to X \otimes X \\ H : Z \to X & CNOT : I \otimes X \to I \otimes X \\ S : X \to Y & CNOT : Z \otimes I \to Z \otimes I \\ S : Z \to Z & CNOT : I \otimes Z \to Z \otimes Z \end{array}$$

$$H : (X \to Z) \cap (Z \to X)$$

[Daniel Gottesman, 1998]

Gottesman Types

Gottesman Types

Gottesman Types

Gottesman Types

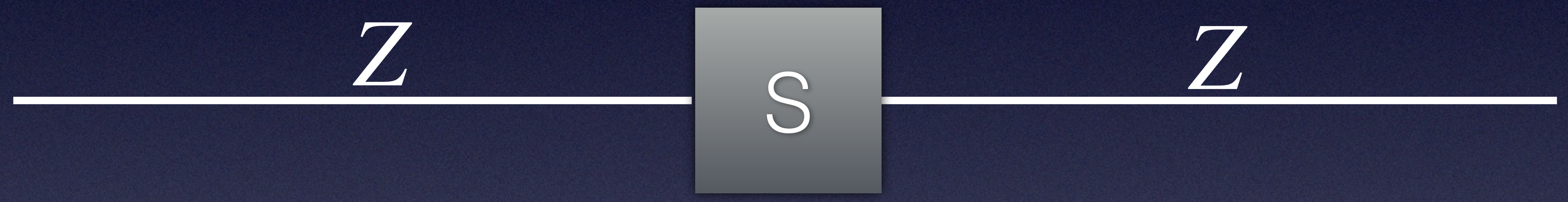
$$H: \quad Z \quad \rightarrow \quad X$$

Gottesman Types

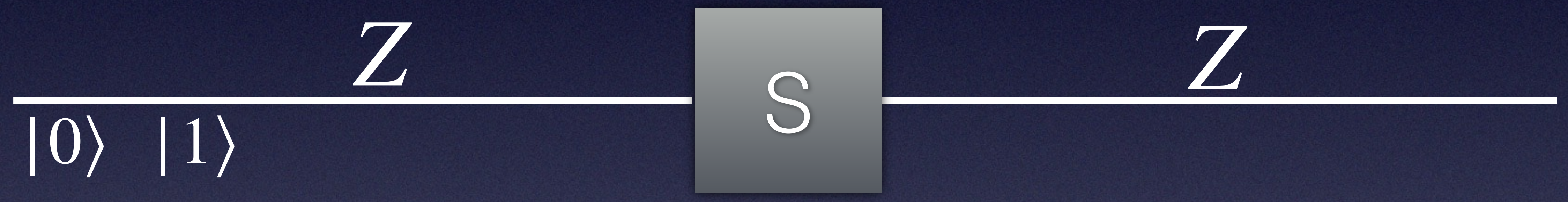
$$H : \quad Z \quad \to \quad X$$

$$H : \{\,|0\rangle, |1\rangle\} \to \{\,|+\rangle, |-\rangle\}$$

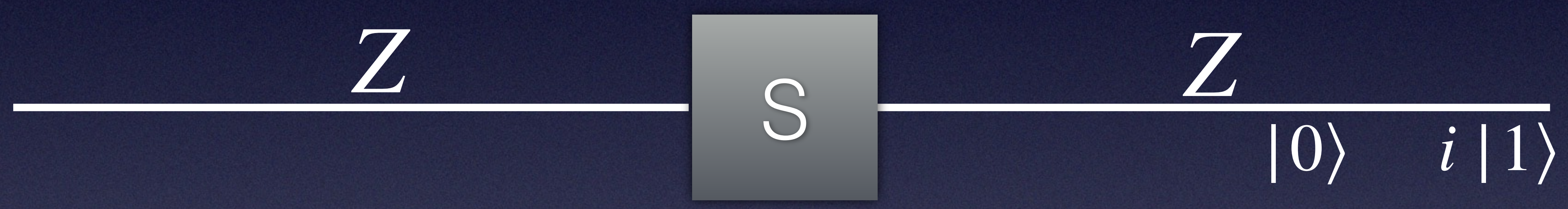
Gottesman Types



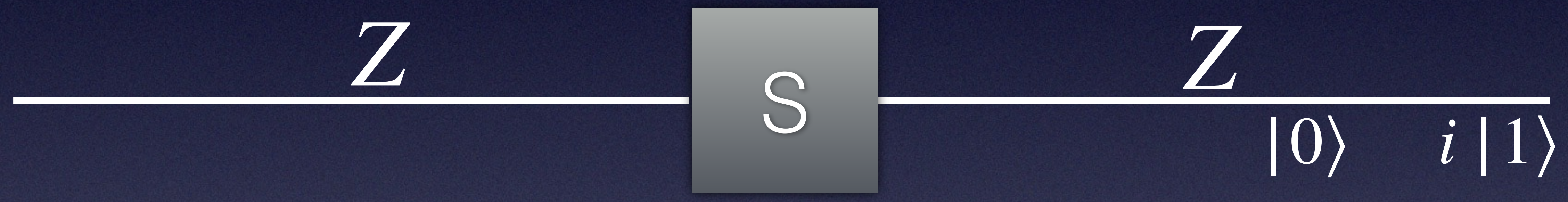
Gottesman Types



Gottesman Types

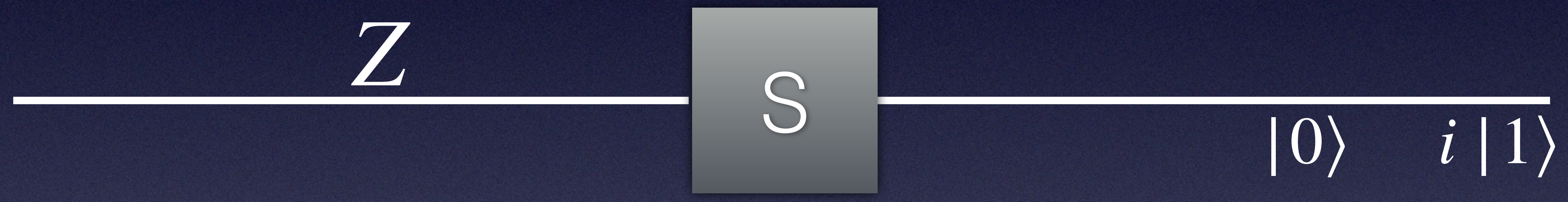


Gottesman Types



$$S : \quad Z \quad \rightarrow \quad Z$$

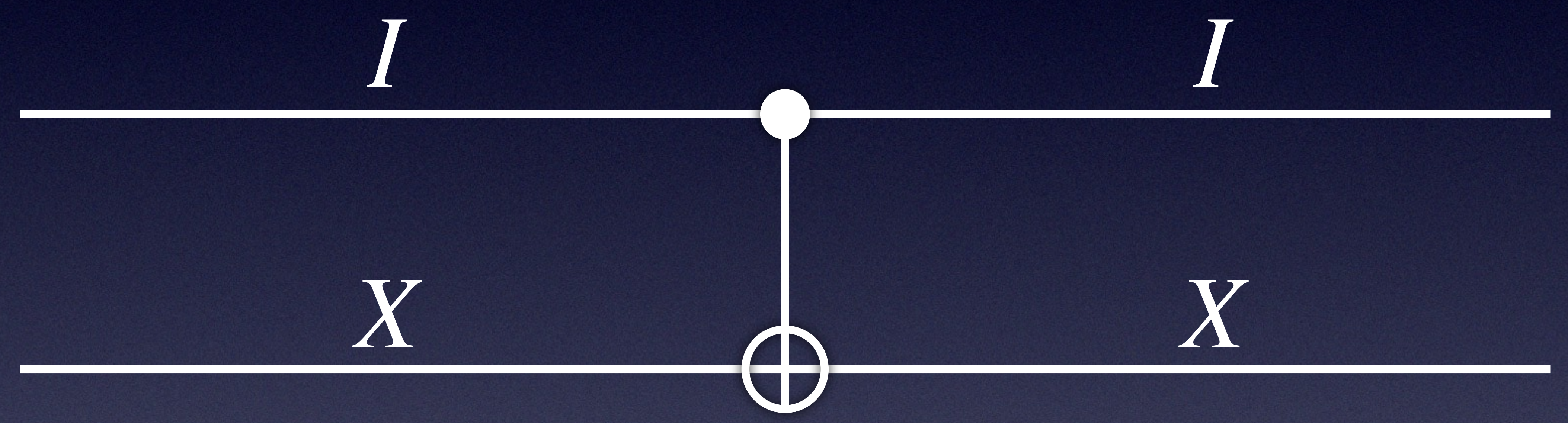
Gottesman Types



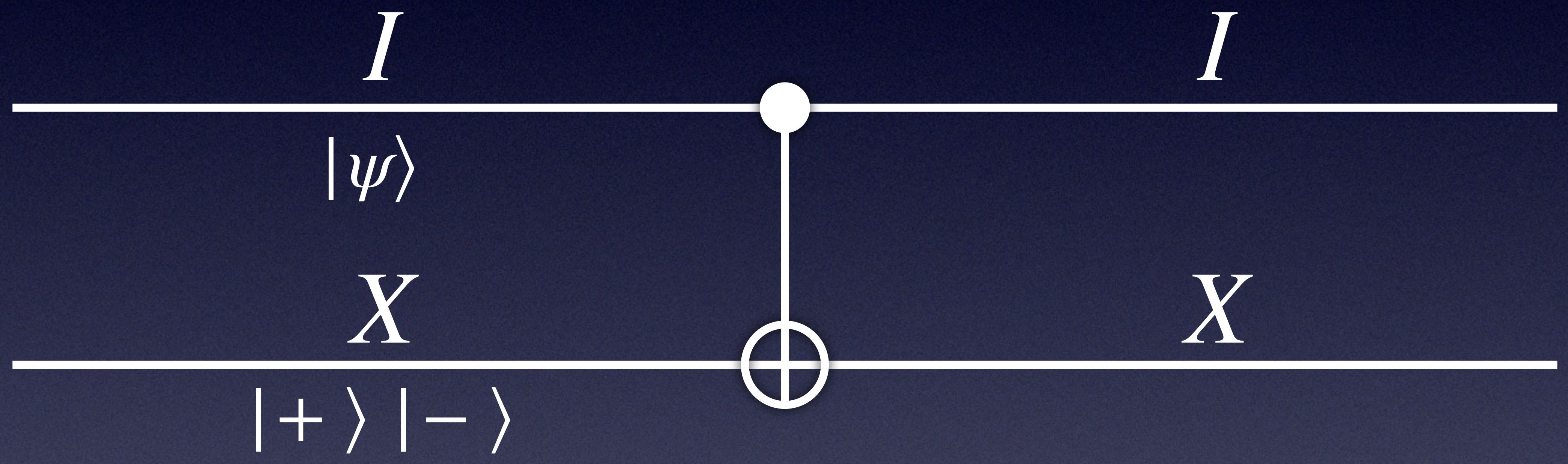
$$S: \quad Z \quad \to \quad Z$$

$$S : e^{i\pi\theta}\{\,|\,0\rangle, |\,1\rangle\} \to e^{i\pi\theta}\{\,|\,0\rangle, |\,1\rangle\}$$

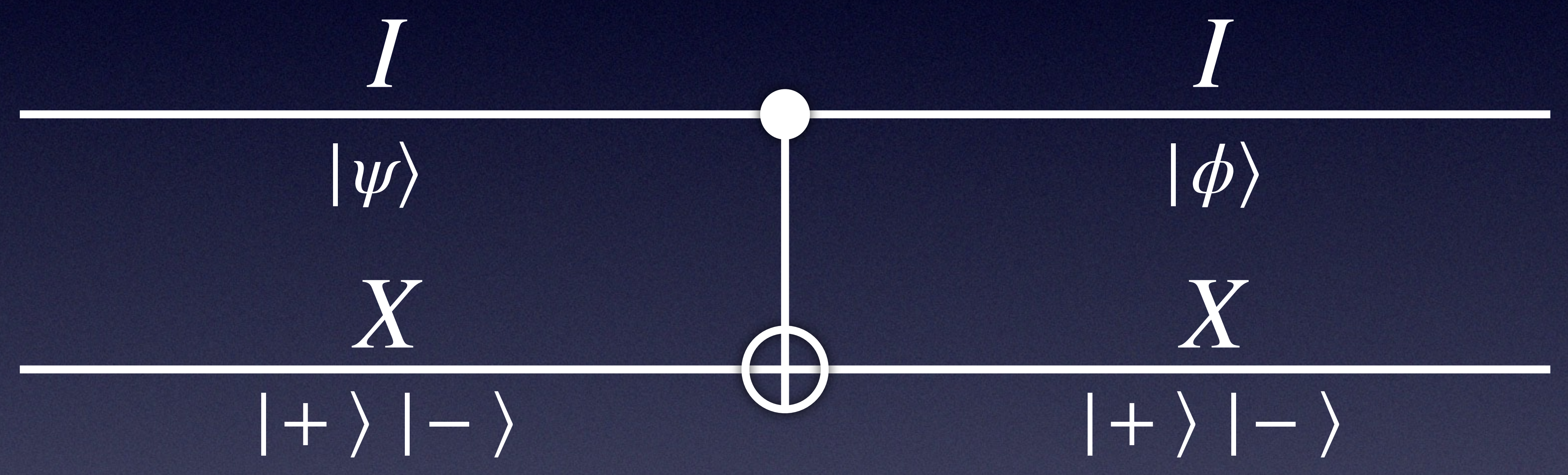
Gottesman Types



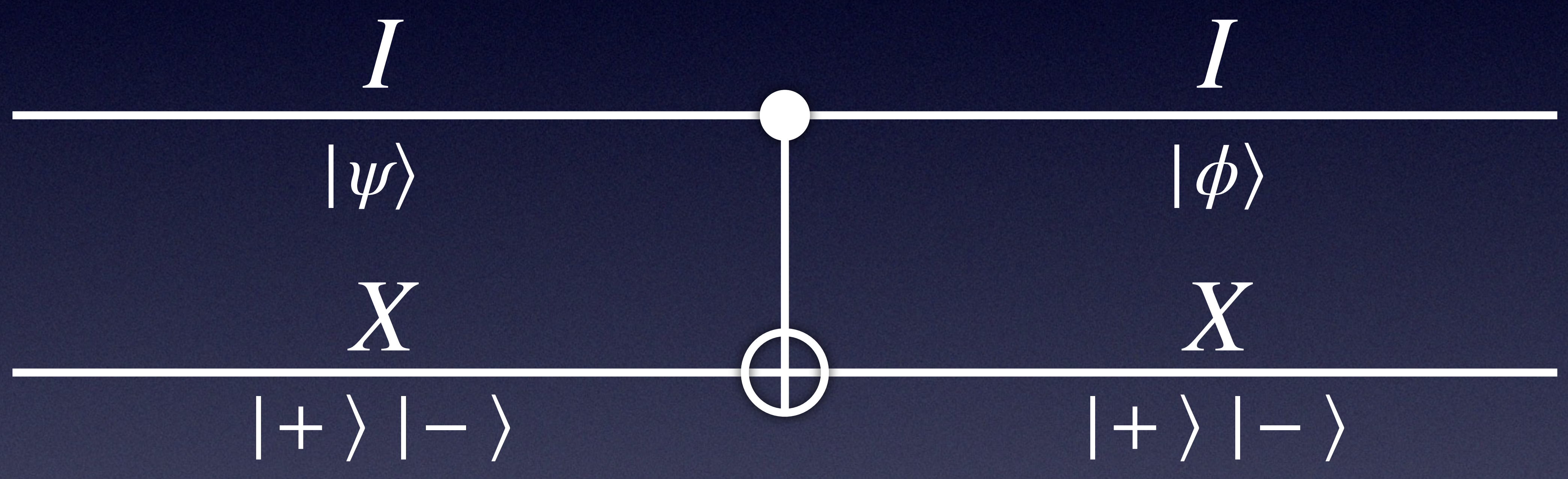
Gottesman Types



Gottesman Types

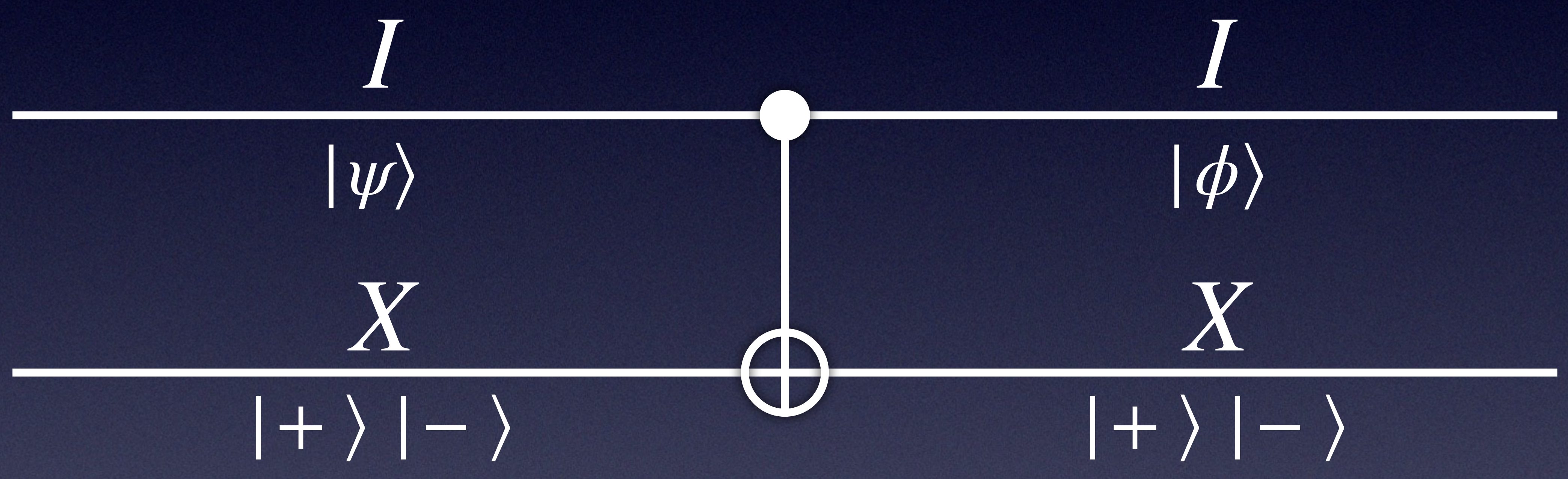


Gottesman Types



$$CNOT: \qquad I \otimes X \qquad \rightarrow \qquad I \otimes X$$

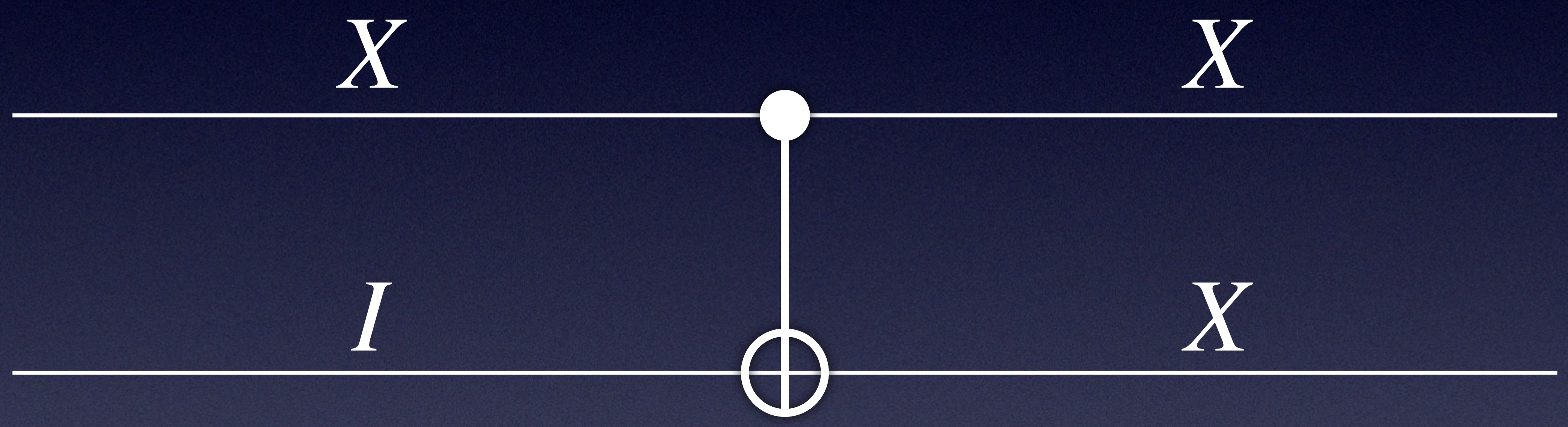
Gottesman Types



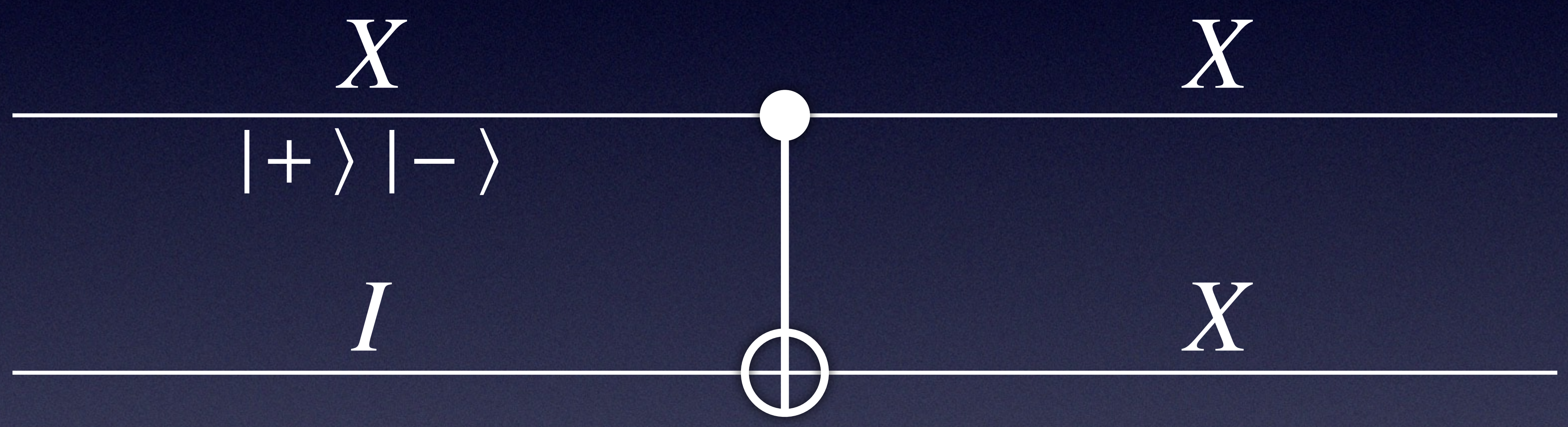
$$CNOT : \quad I \otimes X \quad \rightarrow \quad I \otimes X$$

$$CNOT := (q, \{\, |+\rangle, |-\rangle \}) \quad \rightarrow \quad (q', \{\, |+\rangle, |-\rangle \})$$

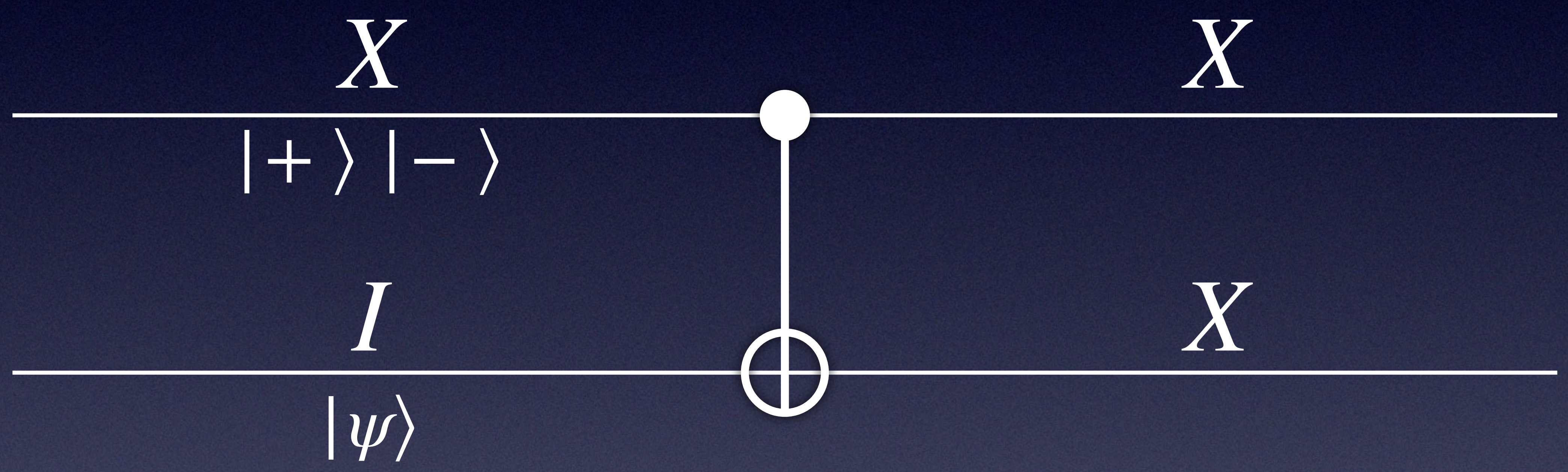
Gottesman Types



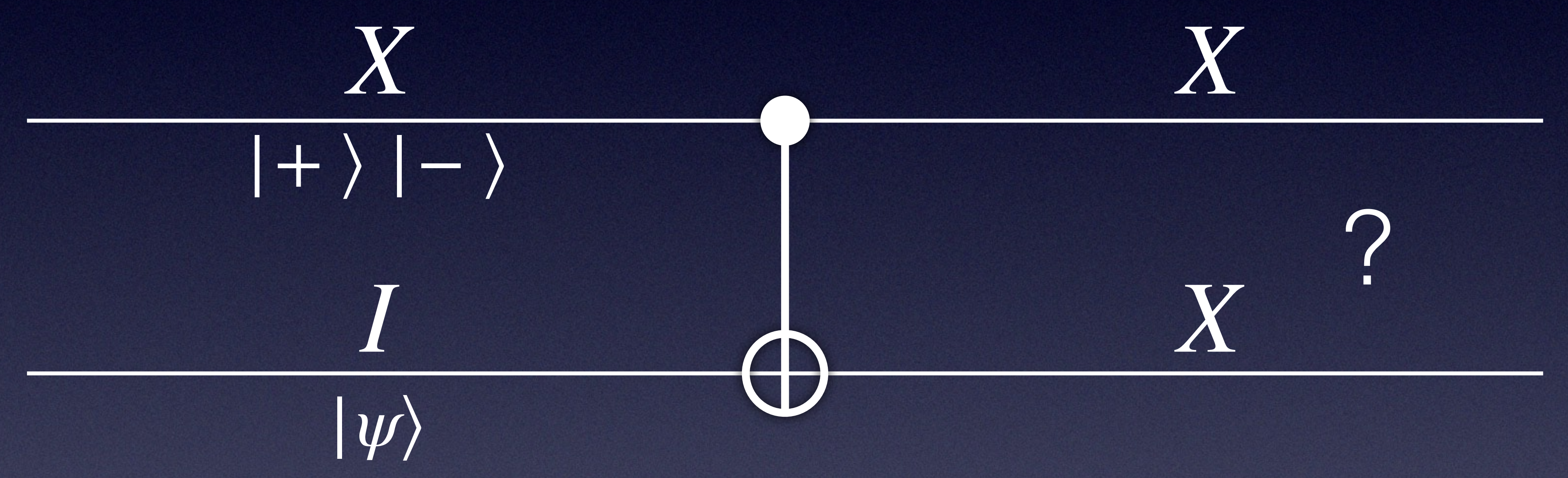
Gottesman Types



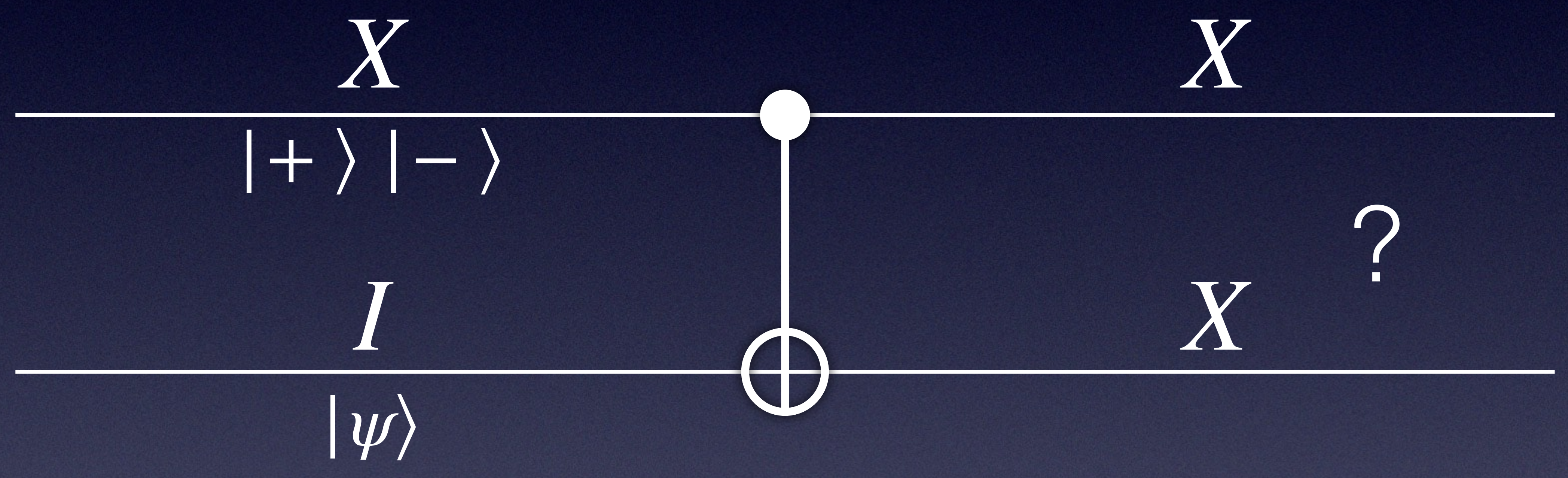
Gottesman Types



Gottesman Types

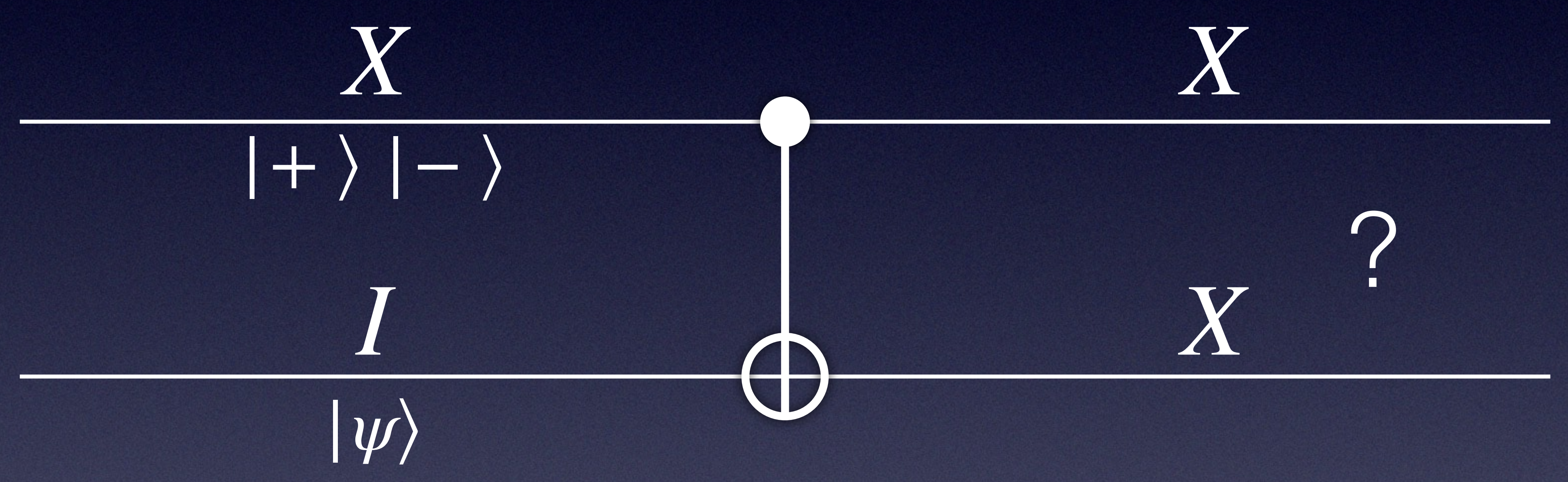


Gottesman Types



$$CNOT: \qquad X \otimes I \qquad \rightarrow \qquad X \otimes X$$

Gottesman Types



$$CNOT: \quad X \otimes I \quad \rightarrow \quad X \otimes X$$

$$CNOT: \quad (\{\,|+\rangle, |-\rangle\}, q) \quad \rightarrow \quad \{v : (X \otimes X)v = kv\}$$

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$CNOT : Z \otimes I \rightarrow Z \otimes I$

$CNOT : I \otimes Z \rightarrow Z \otimes Z$

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\frac{CNOT : Z \otimes I \rightarrow Z \otimes I}{CNOT : Z \times I \rightarrow Z \times I} \qquad \frac{CNOT : I \otimes Z \rightarrow Z \otimes Z}{CNOT : I \times Z \rightarrow Z \otimes Z}$$

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$
\dfrac{\dfrac{CNOT : Z \otimes I \to Z \otimes I}{CNOT : Z \times I \to Z \times I} \qquad \dfrac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}}{CNOT : (Z \times I \to Z \times I) \cap (I \times Z \to Z \otimes Z)}
$$

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\cfrac{\cfrac{CNOT : Z \otimes I \to Z \otimes I}{CNOT : Z \times I \to Z \times I} \qquad \cfrac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}}{\cfrac{CNOT : (Z \times I \to Z \times I) \cap (I \times Z \to Z \otimes Z)}{CNOT : (Z \times I \cap I \times Z) \to (Z \times I \cap Z \otimes Z)}}$$

Separability!

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$
\dfrac{\dfrac{\dfrac{\dfrac{CNOT : Z \otimes I \rightarrow Z \otimes I}{CNOT : Z \times I \rightarrow Z \times I} \qquad \dfrac{CNOT : I \otimes Z \rightarrow Z \otimes Z}{CNOT : I \times Z \rightarrow Z \otimes Z}}{CNOT : (Z \times I \rightarrow Z \times I) \cap (I \times Z \rightarrow Z \otimes Z)}}{CNOT : (Z \times I \cap I \times Z) \rightarrow (Z \times I \cap Z \otimes Z)}}{CNOT : (Z \times Z) \rightarrow (Z \times Z)}
$$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$CNOT : X \otimes I \to X \otimes X$

$CNOT : I \otimes Z \to Z \otimes Z$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\frac{CNOT : X \otimes I \to X \otimes X}{CNOT : X \times I \to X \otimes X}$$

$$\frac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}$$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\cfrac{\cfrac{CNOT : X \otimes I \rightarrow X \otimes X}{CNOT : X \times I \rightarrow X \otimes X} \qquad \cfrac{CNOT : I \otimes Z \rightarrow Z \otimes Z}{CNOT : I \times Z \rightarrow Z \otimes Z}}{CNOT : (X \times I \rightarrow X \otimes X) \cap (I \times Z \rightarrow Z \otimes Z)}$$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\dfrac{\dfrac{CNOT : X \otimes I \to X \otimes X}{CNOT : X \times I \to X \otimes X} \qquad \dfrac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}}{\dfrac{CNOT : (X \times I \to X \otimes X) \cap (I \times Z \to Z \otimes Z)}{CNOT : (X \times I \cap I \times Z) \to (X \otimes X \cap Z \otimes Z)}}$$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\dfrac{\dfrac{CNOT : X \otimes I \to X \otimes X}{CNOT : X \times I \to X \otimes X} \qquad \dfrac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}}{\dfrac{CNOT : (X \times I \to X \otimes X) \cap (I \times Z \to Z \otimes Z)}{\dfrac{CNOT : (X \times I \cap I \times Z) \to (X \otimes X \cap Z \otimes Z)}{CNOT : (X \times Z) \to (X \otimes X \cap Z \otimes Z)}}}$$

Entanglement

Lemma: $\forall\ U \in \{\pm X, \pm Y, \pm Z\}, U \otimes I_k$ is separable.

$$\dfrac{\dfrac{CNOT : X \otimes I \to X \otimes X}{CNOT : X \times I \to X \otimes X} \qquad \dfrac{CNOT : I \otimes Z \to Z \otimes Z}{CNOT : I \times Z \to Z \otimes Z}}{\dfrac{\dfrac{CNOT : (X \times I \to X \otimes X) \cap (I \times Z \to Z \otimes Z)}{CNOT : (X \times I \cap I \times Z) \to (X \otimes X \cap Z \otimes Z)}}{CNOT : (X \times Z) \to (X \otimes X \cap Z \otimes Z)}}$$

Bell Pair

Greenberger–Horne–Zeilinger

```
GHZ :=
INIT ;       Z ⊗ I ⊗ I
H 1;         X ⊗ I ⊗ I
CNOT 1 2;    X ⊗ X ⊗ I
CNOT 2 3;    X ⊗ X ⊗ X
```

Greenberger–Horne–Zeilinger

```
GHZ :=
INIT ;      Z ⊗ I ⊗ I
H 1;        X ⊗ I ⊗ I
CNOT 1 2;   X ⊗ X ⊗ I
CNOT 2 3;   X ⊗ X ⊗ X
```

```
GHZ :=
INIT ;      I ⊗ Z ⊗ I
H 1;        I ⊗ Z ⊗ I
CNOT 1 2;   Z ⊗ Z ⊗ I
CNOT 2 3;   Z ⊗ Z ⊗ I
```

```
GHZ :=
INIT ;      I ⊗ I ⊗ Z
H 1;        I ⊗ I ⊗ Z
CNOT 1 2;   I ⊗ I ⊗ Z
CNOT 2 3;   I ⊗ Z ⊗ Z
```

Greenberger–Horne–Zeilinger

```
GHZ :=
INIT ;       Z ⊗ I ⊗ I
H 1;         X ⊗ I ⊗ I
CNOT 1 2;    X ⊗ X ⊗ I
CNOT 2 3;    X ⊗ X ⊗ X
```

```
GHZ :=
INIT ;       I ⊗ Z ⊗ I
H 1;         I ⊗ Z ⊗ I
CNOT 1 2;    Z ⊗ Z ⊗ I
CNOT 2 3;    Z ⊗ Z ⊗ I
```

```
GHZ :=
INIT ;       I ⊗ I ⊗ Z
H 1;         I ⊗ I ⊗ Z
CNOT 1 2;    I ⊗ I ⊗ Z
CNOT 2 3;    I ⊗ Z ⊗ Z
```

$$GHZ : Z \times Z \times Z \to ((X \otimes X \otimes X) \cap (Z \otimes Z \otimes I) \cap (I \otimes Z \otimes Z))$$

Greenberger–Horne–Zeilinger

```
GHZ' :=
INIT ;      Z ⊗ I ⊗ I
H 1;        X ⊗ I ⊗ I
CNOT 1 2;   X ⊗ X ⊗ I
CNOT 2 3;   X ⊗ X ⊗ X
CNOT 2 1;   I ⊗ X ⊗ X
```

```
GHZ' :=
INIT ;     I ⊗ Z ⊗ I
H 1;       I ⊗ Z ⊗ I
CNOT 1 2;  Z ⊗ Z ⊗ I
CNOT 2 3;  Z ⊗ Z ⊗ I
CNOT 2 1;  Z ⊗ I ⊗ I
```

```
GHZ' :=
INIT ;     I ⊗ I ⊗ Z
H 1;       I ⊗ I ⊗ Z
CNOT 1 2;  I ⊗ I ⊗ Z
CNOT 2 3;  I ⊗ Z ⊗ Z
CNOT 2 1;  I ⊗ Z ⊗ Z
```

Greenberger–Horne–Zeilinger

```
GHZ' :=
INIT ;      Z ⊗ I ⊗ I
H 1;        X ⊗ I ⊗ I
CNOT 1 2;   X ⊗ X ⊗ I
CNOT 2 3;   X ⊗ X ⊗ X
CNOT 2 1;   I ⊗ X ⊗ X
```

```
GHZ' :=
INIT ;      I ⊗ Z ⊗ I
H 1;        I ⊗ Z ⊗ I
CNOT 1 2;   Z ⊗ Z ⊗ I
CNOT 2 3;   Z ⊗ Z ⊗ I
CNOT 2 1;   Z ⊗ I ⊗ I
```

```
GHZ' :=
INIT ;      I ⊗ I ⊗ Z
H 1;        I ⊗ I ⊗ Z
CNOT 1 2;   I ⊗ I ⊗ Z
CNOT 2 3;   I ⊗ Z ⊗ Z
CNOT 2 1;   I ⊗ Z ⊗ Z
```

Greenberger–Horne–Zeilinger

```
GHZ' :=
INIT ;      Z ⊗ I ⊗ I
H 1;        X ⊗ I ⊗ I
CNOT 1 2;   X ⊗ X ⊗ I
CNOT 2 3;   X ⊗ X ⊗ X
CNOT 2 1;   I ⊗ X ⊗ X
```

```
GHZ' :=
INIT ;      I ⊗ Z ⊗ I
H 1;        I ⊗ Z ⊗ I
CNOT 1 2;   Z ⊗ Z ⊗ I
CNOT 2 3;   Z ⊗ Z ⊗ I
CNOT 2 1;   Z ⊗ I ⊗ I
```

```
GHZ' :=
INIT ;      I ⊗ I ⊗ Z
H 1;        I ⊗ I ⊗ Z
CNOT 1 2;   I ⊗ I ⊗ Z
CNOT 2 3;   I ⊗ Z ⊗ Z
CNOT 2 1;   I ⊗ Z ⊗ Z
```

$$GHZ' : Z \times Z \times Z \to Z \times ((X \otimes X) \cap (Z \otimes Z))$$

Greenberger–Horne–Zeilinger

```
GHZ' :=
INIT ;        Z ⊗ I ⊗ I
H 1;          X ⊗ I ⊗ I
CNOT 1 2;     X ⊗ X ⊗ I
CNOT 2 3;     X ⊗ X ⊗ X
CNOT 2 1;     I ⊗ X ⊗ X
```

```
GHZ' :=
INIT ;        I ⊗ Z ⊗ I
H 1;          I ⊗ Z ⊗ I
CNOT 1 2;     Z ⊗ Z ⊗ I
CNOT 2 3;     Z ⊗ Z ⊗ I
CNOT 2 1;     Z ⊗ I ⊗ I
```

```
GHZ' :=
INIT ;        I ⊗ I ⊗ Z
H 1;          I ⊗ I ⊗ Z
CNOT 1 2;     I ⊗ I ⊗ Z
CNOT 2 3;     I ⊗ Z ⊗ Z
CNOT 2 1;     I ⊗ Z ⊗ Z
```

$$GHZ' : Z \times Z \times Z \to Z \times \underbrace{((X \otimes X) \cap (Z \otimes Z))}_{\text{Bell Pair}}$$

Greenberger–Horne–Zeilinger

```
GHZ'' :=
INIT ;      Z ⊗ I ⊗ I
H 1;        X ⊗ I ⊗ I
CNOT 1 2;   X ⊗ X ⊗ I
CNOT 2 3;   X ⊗ X ⊗ X
CNOT 2 1;   I ⊗ X ⊗ X
CNOT 3 2;   I ⊗ I ⊗ X
```

```
GHZ'' :=
INIT ;      I ⊗ Z ⊗ I
H 1;        I ⊗ Z ⊗ I
CNOT 1 2;   Z ⊗ Z ⊗ I
CNOT 2 3;   Z ⊗ Z ⊗ I
CNOT 2 1;   Z ⊗ I ⊗ I
CNOT 3 2;   Z ⊗ I ⊗ I
```

```
GHZ'' :=
INIT ;      I ⊗ I ⊗ Z
H 1;        I ⊗ I ⊗ Z
CNOT 1 2;   I ⊗ I ⊗ Z
CNOT 2 3;   I ⊗ Z ⊗ Z
CNOT 2 1;   I ⊗ Z ⊗ Z
CNOT 3 2;   I ⊗ Z ⊗ I
```

Greenberger–Horne–Zeilinger

```
GHZ'' :=
INIT ;       Z ⊗ I ⊗ I
H 1;         X ⊗ I ⊗ I
CNOT 1 2;    X ⊗ X ⊗ I
CNOT 2 3;    X ⊗ X ⊗ X
CNOT 2 1;    I ⊗ X ⊗ X
CNOT 3 2;    I ⊗ I ⊗ X
```

```
GHZ'' :=
INIT ;       I ⊗ Z ⊗ I
H 1;         I ⊗ Z ⊗ I
CNOT 1 2;    Z ⊗ Z ⊗ I
CNOT 2 3;    Z ⊗ Z ⊗ I
CNOT 2 1;    Z ⊗ I ⊗ I
CNOT 3 2;    Z ⊗ I ⊗ I
```

```
GHZ'' :=
INIT ;       I ⊗ I ⊗ Z
H 1;         I ⊗ I ⊗ Z
CNOT 1 2;    I ⊗ I ⊗ Z
CNOT 2 3;    I ⊗ Z ⊗ Z
CNOT 2 1;    I ⊗ Z ⊗ Z
CNOT 3 2;    I ⊗ Z ⊗ I
```

Greenberger–Horne–Zeilinger

```
GHZ'' :=
INIT ;        Z ⊗ I ⊗ I
H 1;          X ⊗ I ⊗ I
CNOT 1 2;     X ⊗ X ⊗ I
CNOT 2 3;     X ⊗ X ⊗ X
CNOT 2 1;     I ⊗ X ⊗ X
CNOT 3 2;     I ⊗ I ⊗ X
```

```
GHZ'' :=
INIT ;        I ⊗ Z ⊗ I
H 1;          I ⊗ Z ⊗ I
CNOT 1 2;     Z ⊗ Z ⊗ I
CNOT 2 3;     Z ⊗ Z ⊗ I
CNOT 2 1;     Z ⊗ I ⊗ I
CNOT 3 2;     Z ⊗ I ⊗ I
```

```
GHZ'' :=
INIT ;        I ⊗ I ⊗ Z
H 1;          I ⊗ I ⊗ Z
CNOT 1 2;     I ⊗ I ⊗ Z
CNOT 2 3;     I ⊗ Z ⊗ Z
CNOT 2 1;     I ⊗ Z ⊗ Z
CNOT 3 2;     I ⊗ Z ⊗ I
```

$$GHZ'' : Z \times Z \times Z \rightarrow Z \times Z \times X$$

Clifford+T?

$$T : Z \to Z$$
$$T : X \to \mathsf{T}$$

Clifford+T?

$$T : Z \to Z$$
$$T : X \to \text{T}$$

Those who leave the Clifford set may never return

Clifford+T?

$$T : Z \rightarrow Z$$
$$T : X \rightarrow \text{T}$$

Those who leave the Clifford set may never return

So can we do anything useful with T?

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                     I ⊗ I ⊗ X
  ---------------------------------------------------
  H 3;                      I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;           I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;            Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;           Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;       I ⊗ I ⊗ Z
  H 3;                      I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;      I ⊗ I ⊗ X
  CNOT 1 2.                 I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                      I ⊗ I ⊗ X
  H 3;                       I ⊗ I ⊗ Z
  ------------------------------------
  CNOT 2 3; T† 3;            I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;             Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;            Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;        I ⊗ I ⊗ Z
  H 3;                       I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;       I ⊗ I ⊗ X
  CNOT 1 2.                  I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                      I ⊗ I ⊗ X
  H 3;                       I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;            I ⊗ Z ⊗ Z
------------------------------------------
  CNOT 1 3; T 3;             Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;            Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;        I ⊗ I ⊗ Z
  H 3;                       I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;       I ⊗ I ⊗ X
  CNOT 1 2.                  I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                     I ⊗ I ⊗ X
  H 3;                      I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;           I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;            Z ⊗ Z ⊗ Z
  ------------------------------------
  CNOT 2 3; T† 3;           Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;       I ⊗ I ⊗ Z
  H 3;                      I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;      I ⊗ I ⊗ X
  CNOT 1 2.                 I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                     I ⊗ I ⊗ X
  H 3;                      I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;           I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;            Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;           Z ⊗ I ⊗ Z
  --------------------------------------
  CNOT 1 3; T 2; T 3; I ⊗ I ⊗ Z
  H 3;                      I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2; I ⊗ I ⊗ X
  CNOT 1 2.                 I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                       I ⊗ I ⊗ X
  H 3;                        I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;             I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;              Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;             Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;         I ⊗ I ⊗ Z
  ------------------------------------------
  H 3;                        I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;        I ⊗ I ⊗ X
  CNOT 1 2.                   I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                     I ⊗ I ⊗ X
  H 3;                      I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;           I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;            Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;           Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;       I ⊗ I ⊗ Z
  H 3;                      I ⊗ I ⊗ X
  ---------------------------------------
  CNOT 1 2; T 1; T† 2;      I ⊗ I ⊗ X
  CNOT 1 2.                 I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                      I ⊗ I ⊗ X
  H 3;                       I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;            I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;             Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;            Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;        I ⊗ I ⊗ Z
  H 3;                       I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;       I ⊗ I ⊗ X
  ------------------------------------------
  CNOT 1 2.                  I ⊗ I ⊗ X
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                     I ⊗ I ⊗ X
  H 3;                      I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;           I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;            Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;           Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;       I ⊗ I ⊗ Z
  H 3;                      I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;      I ⊗ I ⊗ X
  CNOT 1 2.                 I ⊗ I ⊗ X
  -----------------------------------
```

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                      I ⊗ I ⊗ X
  H 3;                       I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;            I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;             Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;            Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;        I ⊗ I ⊗ Z
  H 3;                       I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;       I ⊗ I ⊗ X
  CNOT 1 2.                  I ⊗ I ⊗ X
-----------------------------------------
```

$\mathtt{TOFFOLI} : Z \otimes I \otimes I \rightarrow Z \otimes I \otimes I$

$\mathtt{TOFFOLI} : I \otimes Z \otimes I \rightarrow I \otimes Z \otimes I$

$\mathtt{TOFFOLI} : I \otimes I \otimes X \rightarrow I \otimes I \otimes X$

$\mathtt{TOFFOLI} : X \otimes I \otimes I \rightarrow \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes X \otimes I \rightarrow \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes I \otimes Z \rightarrow \top \otimes \top \otimes \top$

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                    I ⊗ I ⊗ X
  H 3;                     I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;          I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;           Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;          Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;      I ⊗ I ⊗ Z
  H 3;                     I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;     I ⊗ I ⊗ X
  CNOT 1 2.                I ⊗ I ⊗ X
```

$\mathtt{TOFFOLI} : Z \otimes I \otimes I \rightarrow Z \otimes I \otimes I$

$\mathtt{TOFFOLI} : I \otimes Z \otimes I \rightarrow I \otimes Z \otimes I$

$\mathtt{TOFFOLI} : I \otimes I \otimes X \rightarrow I \otimes I \otimes X$

$\mathtt{TOFFOLI} : X \otimes I \otimes I \rightarrow \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes X \otimes I \rightarrow \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes I \otimes Z \rightarrow \top \otimes \top \otimes \top$

Toffoli

```
TOFFOLI 1 2 3 :=
  INIT;                        I ⊗ I ⊗ X
  H 3;                         I ⊗ I ⊗ Z
  CNOT 2 3; T† 3;              I ⊗ Z ⊗ Z
  CNOT 1 3; T 3;               Z ⊗ Z ⊗ Z
  CNOT 2 3; T† 3;              Z ⊗ I ⊗ Z
  CNOT 1 3; T 2; T 3;          I ⊗ I ⊗ Z
  H 3;                         I ⊗ I ⊗ X
  CNOT 1 2; T 1; T† 2;         I ⊗ I ⊗ X
  CNOT 1 2.                    I ⊗ I ⊗ X
```

$\mathtt{TOFFOLI} : Z \otimes I \otimes I \to Z \otimes I \otimes I$

$\mathtt{TOFFOLI} : I \otimes Z \otimes I \to I \otimes Z \otimes I$

$\mathtt{TOFFOLI} : I \otimes I \otimes X \to I \otimes I \otimes X$

$\mathtt{TOFFOLI} : X \otimes I \otimes I \to \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes X \otimes I \to \top \otimes \top \otimes \top$

$\mathtt{TOFFOLI} : I \otimes I \otimes Z \to \top \otimes \top \otimes \top$

$$\frac{}{\mathtt{TOFFOLI} : Z \times Z \times X \to Z \times Z \times X}$$

What’s Next?

- Generalizing separability to multiqubit states.
- Expand more robustly beyond Clifford.
- Efficiently incorporating measurement.
- Resource tracking: E.g. use of e-bits in a circuits
- Provenance tracking: Show correctness of communication protocols
- Validating error-correction codes.

What's Next?

- Generalizing separability to multiqubit states.
- Expand more robustly beyond Clifford.
- Efficiently incorporating measurement.
- Resource tracking: E.g. use of e-bits in a circuits
- Provenance tracking: Show correctness of communication protocols
- Validating error-correction codes.

THANKS!