2/4/2025

methods for circuit verification.

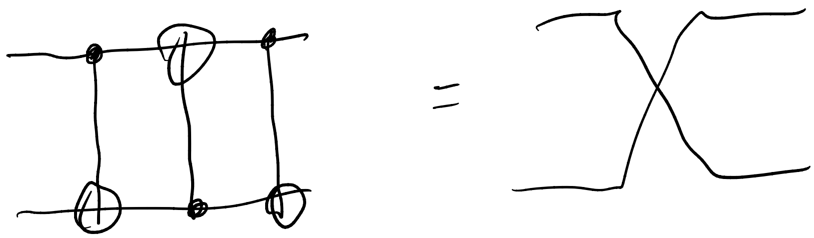
① Check if the circuits give the same result for all possible basis states.

Pro: Simple calculation.

Cons: There are too many basisstates to check.

② Symbolic check.

e.g.



$\forall a, b \in \{0,1\}$

$$\boxed{CX|a,b\rangle = |a, a\oplus b\rangle}$$

$$|a,b\rangle \xmapsto{CX_{1\to2}} |a, a\oplus b\rangle \xmapsto{CX_{2\to1}} |a\oplus a\oplus b, a\oplus b\rangle$$

$$= |b, a\oplus b\rangle$$

$$\xmapsto{CX_{1\to2}} |b, a\oplus b\oplus b\rangle = |b, a\rangle$$

Pro: when it works, it is straight forward.

Cons: when we work with gates like H, it can gen complicated.

$$T|a\rangle = e^{i\frac{\pi}{4}a}|a\rangle.$$

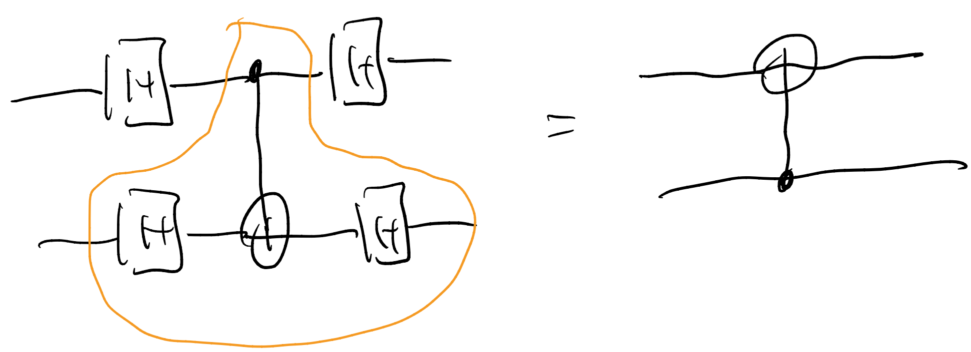
$$H|a\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} e^{i\pi a\cdot k}|k\rangle$$

$$a=0,\ \frac{1}{\sqrt{2}}\left(|0\rangle + \overbrace{e^{i\pi 0}}^{=1}|1\rangle\right) = |+\rangle$$

$$a=1,\ \frac{1}{\sqrt{2}}\left(|0\rangle + \underbrace{e^{i\pi}}_{=-1}|1\rangle\right) = |-\rangle.$$

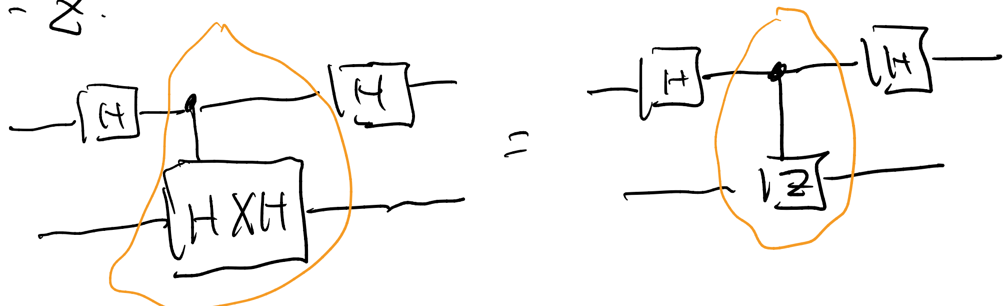
③ Circuit equational reasoning.

e.g.

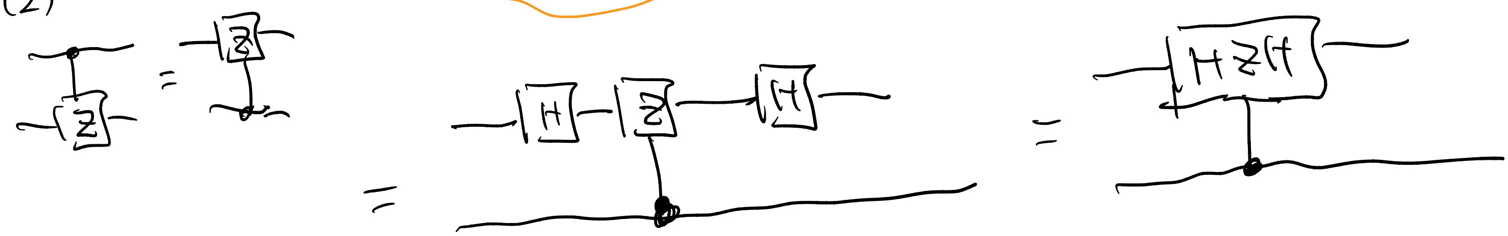


(1) $HXH = Z$.

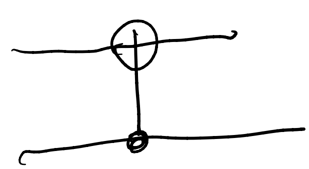
(LHS) =



(2)



(3) $HZH = X$



Pro: It is circuit rewriting.

Cons: It may be hard rewrite big circuits.

$*$ $U(|\varphi\rangle \otimes |0\rangle) = |\varphi\rangle \otimes |\varphi\rangle$. for all $|\varphi\rangle \in Q$.

So assume U exists.

let $|\varphi\rangle = a|0\rangle + b|1\rangle$,

$$LHS = U(|\varphi\rangle \otimes |0\rangle) = U((a|0\rangle + b|1\rangle) \otimes |0\rangle)$$

$$= U(a|00\rangle + b|10\rangle)$$

$$= aU|00\rangle + bU|10\rangle$$

$$= a|00\rangle + b|11\rangle$$

$$RHS = (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle)$$

$$= a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle.$$

Since LHS = RHS.

$a^2 = a$, $ab = 0$, $b^2 = b$.

$a = 0$, $b = 1$

$a = 1$, $b = 0$ $\Rightarrow$ a and b can not be arbitrary.

So no such U that works for arbitrary a, b s.t. $|a|^2 + |b|^2 = 1$.

* Type inference Problem.

e.g. $\quad \phi \vdash \lambda x. x(\lambda y. y) : \ ?$

$B = D \to C$

$$\dfrac{\dfrac{}{x:\underbrace{B}_{=D\to C} \vdash x : D \to C}\,\text{var.} \qquad \dfrac{\dfrac{(E=F)}{x:B,\ y:E \vdash y:F}\,\text{var.}}{x:B \vdash \lambda y. y : D}}{\dfrac{x:B \vdash x(\lambda y. y) : C}{\phi \vdash \lambda x. x(\lambda y. y) : B \to C}}$$

$D = E \to F$

$$\begin{cases} A = B \to C \\ B = D \to C. \\ D = E \to F \\ E = F \end{cases}$$

$$\begin{aligned} B \to C &= (D \to C) \to C \\ &= ((E \to F) \to C) \to C \\ &= ((F \to F) \to C) \to C \end{aligned}$$

Therefore

$$\lambda x. x(\lambda y. y) : ((F \to F) \to C) \to C$$

$$\overset{?}{\neq} \lambda x. \lambda y. x y.$$

* Type Inhabitation

$$\emptyset \vdash ? : A$$

$$M = x$$

eg 1.

$$\frac{x : A \vdash M : A}{\emptyset \vdash \lambda x. M : A \to A}$$

$$\lambda x. x : A \to A.$$

eg 2

$$\frac{\dfrac{\dfrac{}{x : A \times B \vdash x : A \times B}\,\text{var}}{x : A \times B \vdash M_1 = \text{snd } x : B} \qquad \dfrac{\dfrac{}{x : A \times B \vdash x : A \times B}\,\text{var}}{x : A \times B \vdash M_2 = \text{fst } x : A}}{\dfrac{x : A \times B \vdash (M_1, M_2) : B \times A}{\emptyset \vdash \lambda x. M : A \times B \to B \times A}}$$

Therefore $\lambda x. (\text{snd } x, \text{fst } x)$