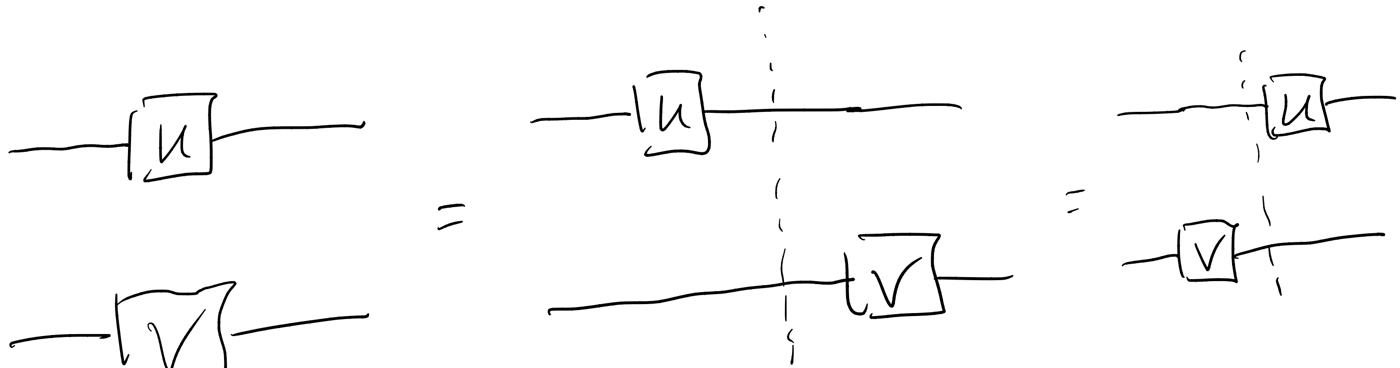
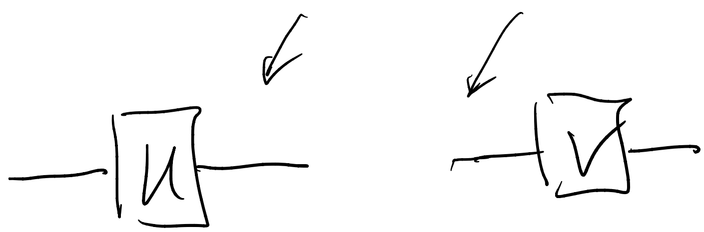
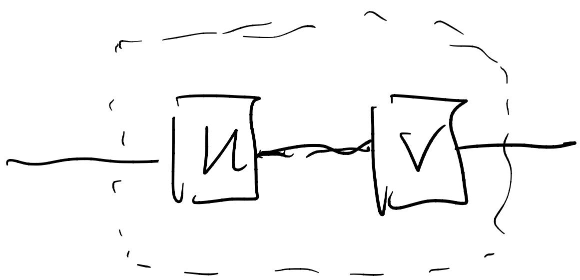
1/21/2025



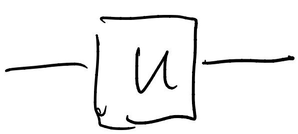
$$U \otimes V = (Id \otimes V) \circ (U \otimes Id) = (U \otimes Id) \circ (Id \otimes V)$$

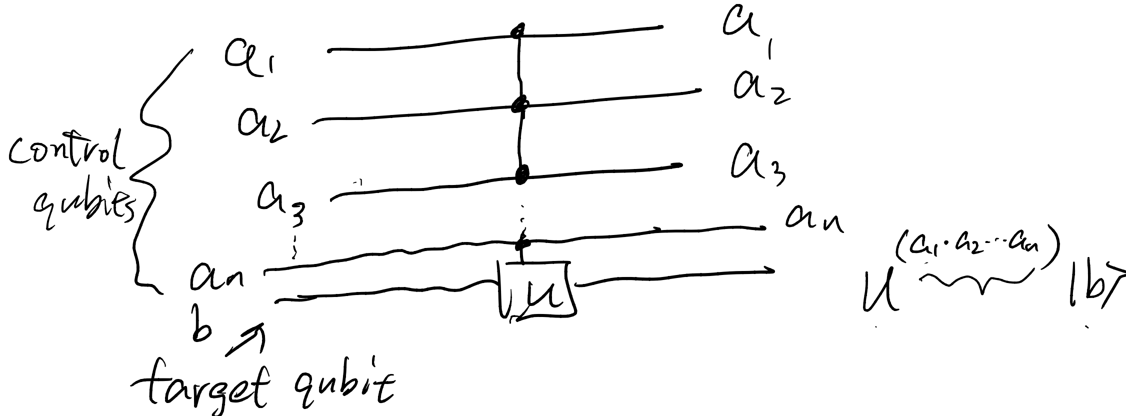




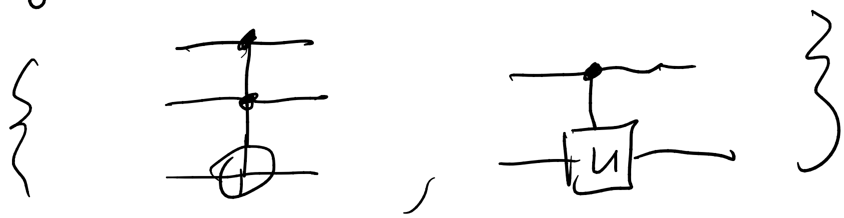
$V \circ U$

* Multi-Control U gate.

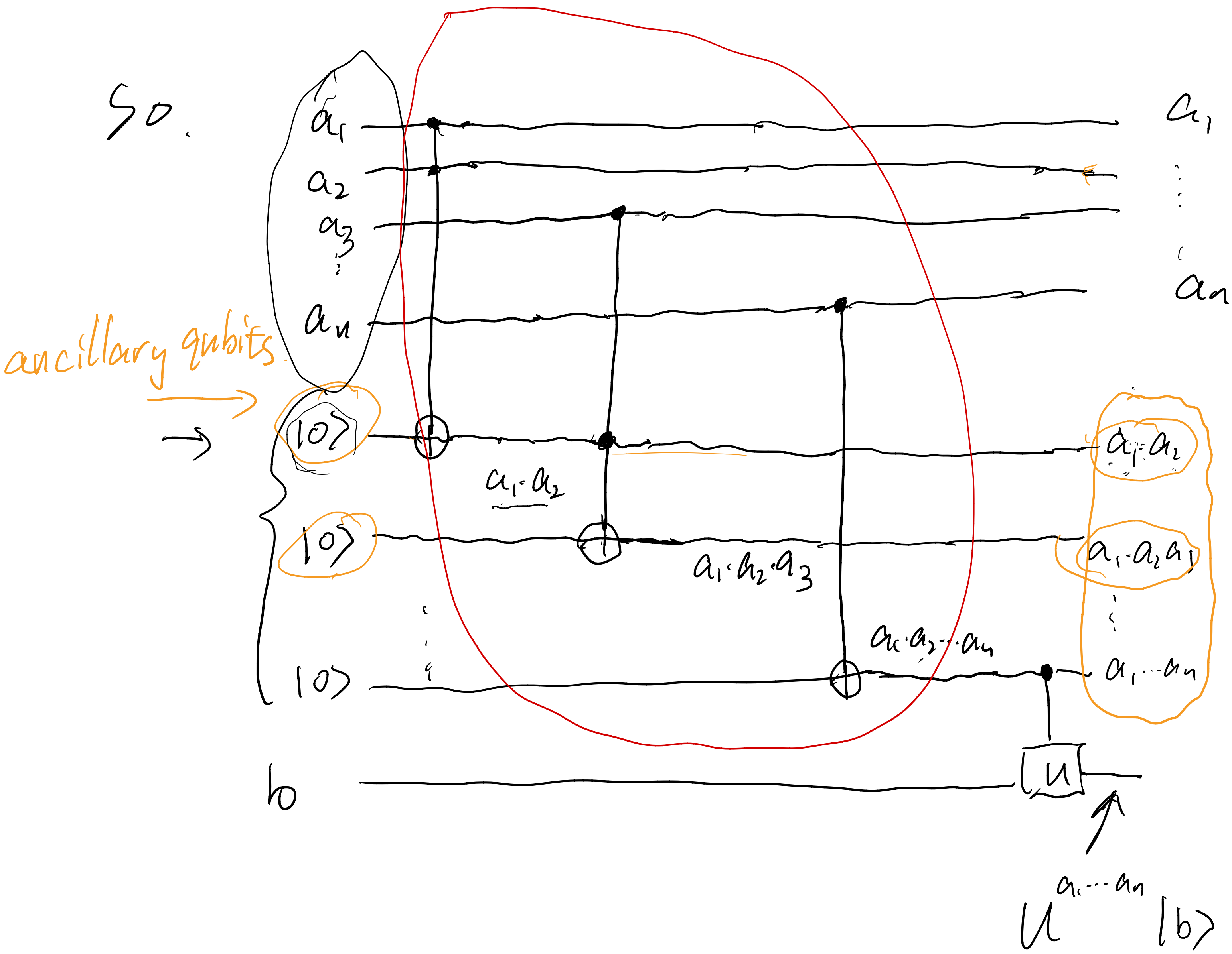


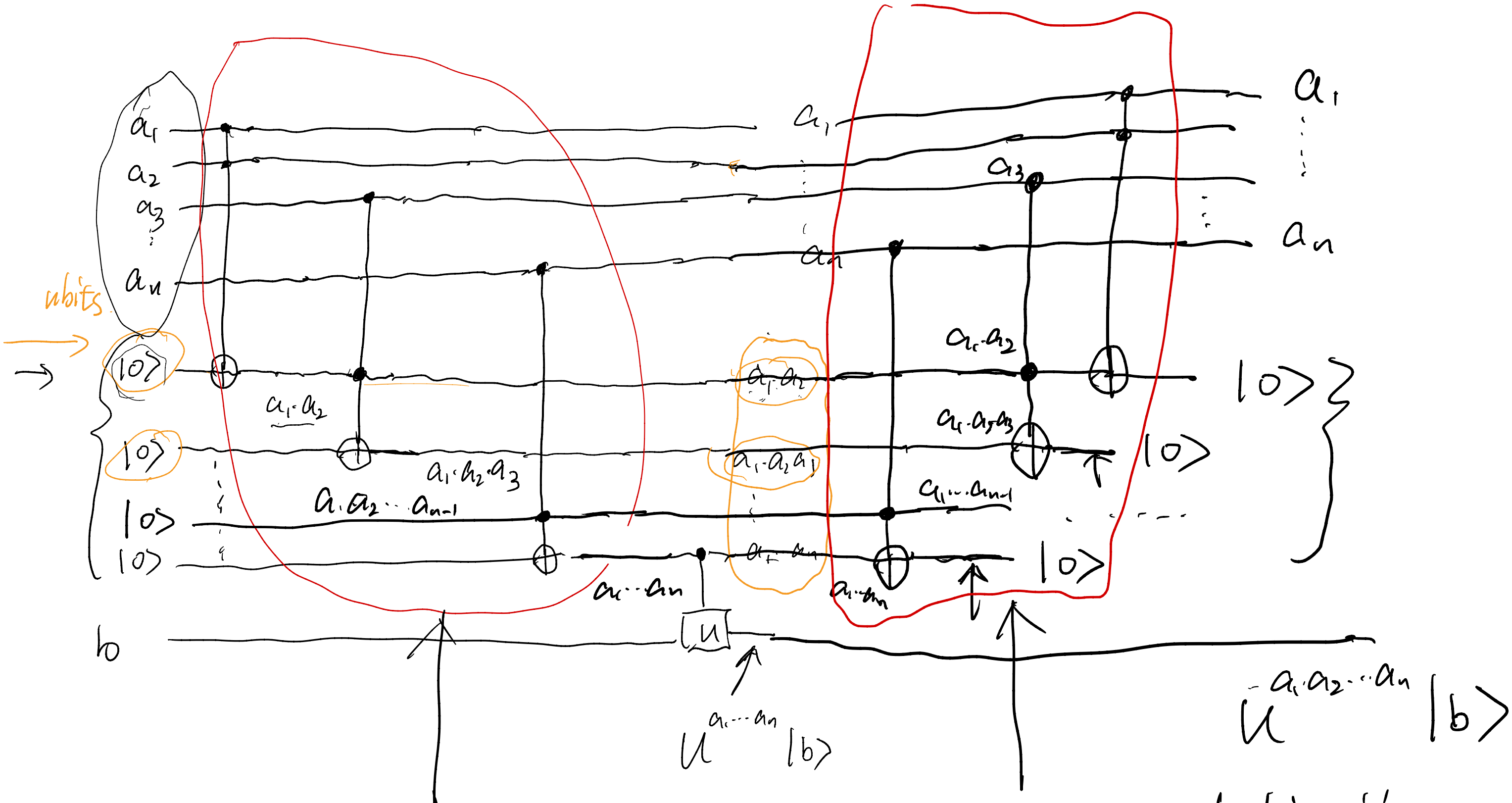


We can implement n-fold controlled U gate via Toffoli gate and a single controlled U gate.



So.

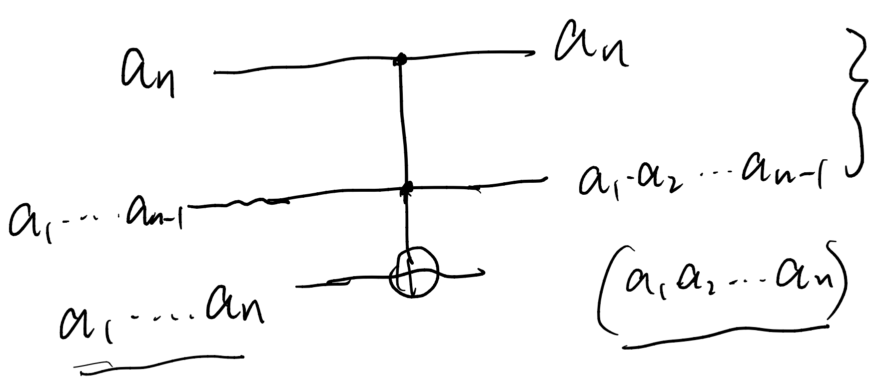




G.

"uncomputation"

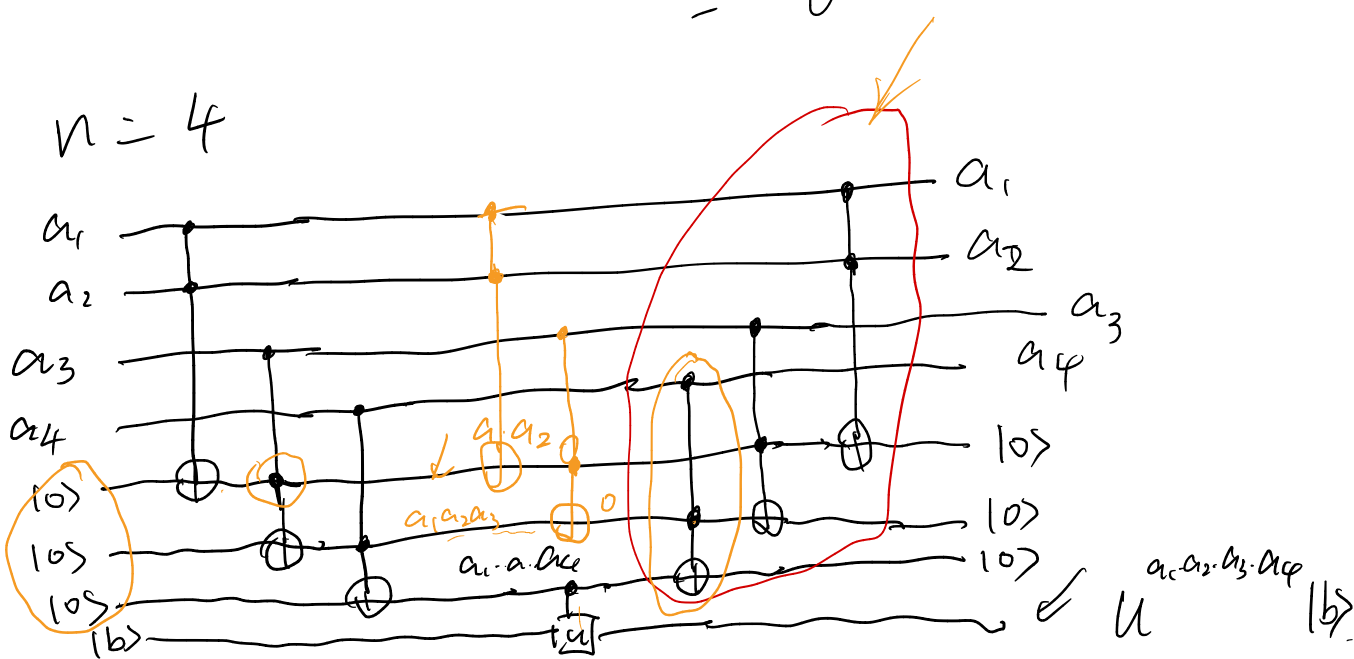
$G^\dagger$



$$(a_1 a_2 \cdots a_n) \oplus (a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n)$$

$$= 0$$

$n = 4$



* Non-unitary gates.

① Initialization gates (Linear function)

$|0\rangle$ ——— $=$ $0 \vdash$——

init0 : Unit $\to$ Qubit

init0 $= |0\rangle$

$1 \vdash$——

init1 : Unit $\to$ Qubit

init1 $= |1\rangle$

② Termination gates.

——$\dashv 0$ "Terminate a qubit in the zero state".

term0 $= \langle 0|$: Qubit $\to$ $\underline{\text{Unit}} \cong \mathbb{C}$

"bra"

ket

$\langle 0|(|0\rangle) = \langle 0|0\rangle = 1$

$\langle 0|(|1\rangle) = \langle 0|1\rangle = 0$

——$\dashv 1$ "Terminate a qubit in the one state

term1 $= \langle 1|$: Qubit $\to$ Unit.

$\langle 1 | (|0\rangle) = \langle 1 | 0 \rangle = 0$

$\langle 1 | (|1\rangle) = \langle 1 | 1 \rangle = 1$

ex. side note.

$$\begin{array}{ccc} \text{Qubit} & \rightarrow & \text{Unit} \\ \cong & & \cong \\ \mathbb{C}^2 & & \mathbb{C} \end{array} \qquad \dim(\mathbb{C}) = 0$$

"vector space" of dimension 2.

basis $\left| \{ |0\rangle , |1\rangle \} \right| = 2$

$\varphi \in \mathbb{C}^2$, $a|0\rangle + b|1\rangle$
$a, b \in \mathbb{C}$

Why init and termination gates are not unitary?

if U is unitary, $\begin{cases} ① \text{ linear} \\ ② \ U^\dagger \circ U = U \circ U^\dagger = I \end{cases}$

init0 : Unit → Qubit

term0 : Qubit → Unit.

term0 ∘ init0 : Unit → Unit. id.

$\langle 0 | \circ | 0 \rangle (a \cdot 1) = a (\langle 0 | \circ | 0 \rangle 1) = a = a \cdot 1$

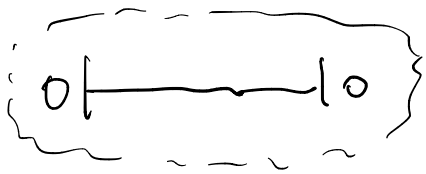
$init0 \circ term0 : Qubit \to Qubit.$

$$\begin{cases} |0\rangle\circ\langle 0|\,(|0\rangle) = |0\rangle\,(\langle 0|\circ|0\rangle) = |0\rangle \\ |0\rangle\circ\langle 0|\,(|1\rangle) = |0\rangle\,(\underbrace{\langle 0|\circ|1\rangle}_{0}) = 0 \end{cases}$$

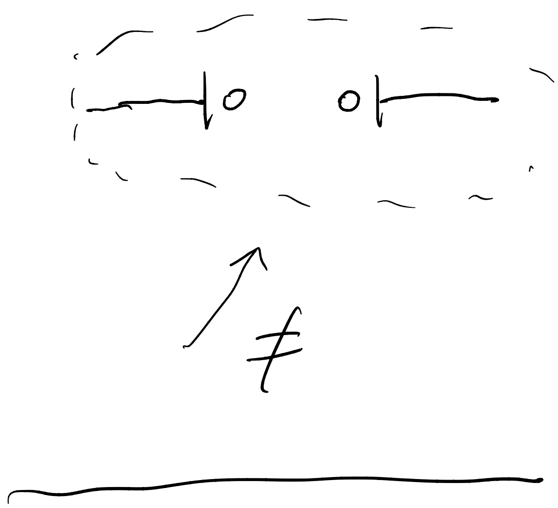
$$|0\rangle\langle 0| \neq Id.$$

That's why initialization and termination gates are not unitary

* in the circuit notation.

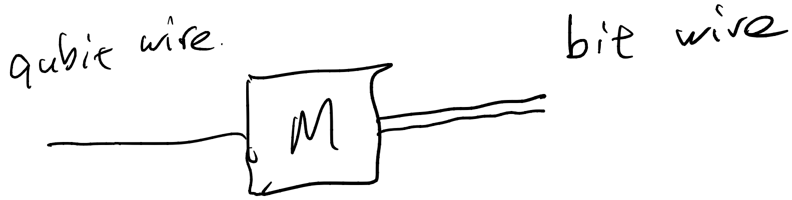


represent a "scalar"/a complex number.



represents a "projector", i.e. it maps a qubit to $|0\rangle$ if the qubit is $|0\rangle$, otherwise undefined (0).

* Measurement gate.



M : Qubit $\to$ Bit.

$M(a|0\rangle + b|1\rangle) = |0\rangle$ with $|a|^2$ probability

$M(a|0\rangle + b|1\rangle) = |1\rangle$ with $|b|^2$ probalitity