Addition by QFT.

$*$. QFT.

$$|a\rangle \overset{QFT_n}{\longmapsto} \frac{1}{\sqrt{2}^{\,n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{a\cdot k}{2^n}} |k\rangle .$$

$$a = a_n \cdot 2^{n-1} + a_{n-1} 2^{n-2} + \cdots + a_1 2^0 .$$

Remarks: 1. QFT_n is unitary (linear & reversible).

2. $QFT_n(a) = \phi_n(a) \otimes \phi_{n-1}(a) \cdots \otimes \phi_1(a)$

where $\cancel{\phi}$ $\cancel{=(\phi_n(a))}$ $\phi_k(a) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \frac{a}{2^k}} |1\rangle\right).$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + \exp(0.a_k \cdots a_1)\, |1\rangle\right)$$

Note that we write $\exp(x) = e^{2\pi i x}$ and.

$\frac{a}{2^k} = a_n a_{n-1} \cdots a_{k+1} \bullet a_k \cdot a_{k-1} \cdots a_1.$, and.

$$\exp(a_n a_{n-1} \cdots a_{k+1} \bullet a_k a_{k-1} \cdots a_1) = \exp(0.a_k \cdots a_1)$$

because $\exp(l) = 1$ if l is a integer.
$= e^{(2\pi i) l}$

So if we can construct a circuit for ϕ_k, then we have a circuit for QFT_n.

* $H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$

$= \frac{1}{\sqrt{2}}(|0\rangle + \exp(\frac{x}{2})|1\rangle)$

$= \frac{1}{\sqrt{2}}(|0\rangle + \exp(0.x)|1\rangle)$.

* ~~R_k~~ let us define $R_k(|x\rangle) = e^{2\pi i \frac{x}{2^k}}|x\rangle$.

$= \exp(\underbrace{0.0\cdots x}_{k})|x\rangle$.

So R_k

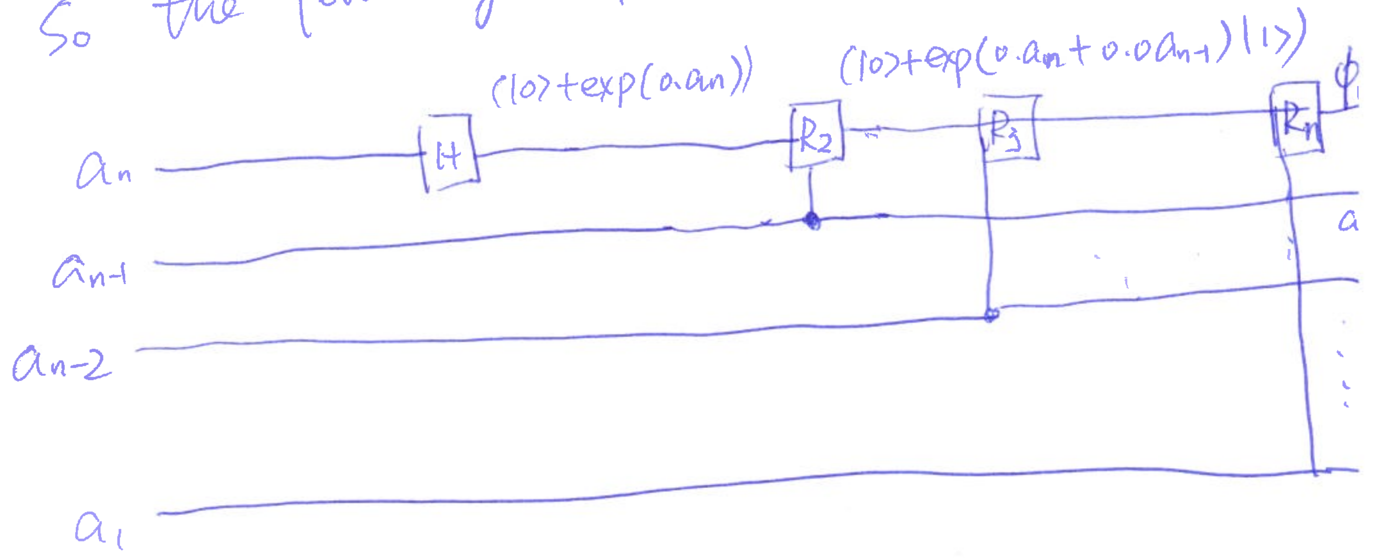
And controlled-R_k

$CR_k|ab\rangle = \exp(\frac{ab}{2^k})|ab\rangle$.

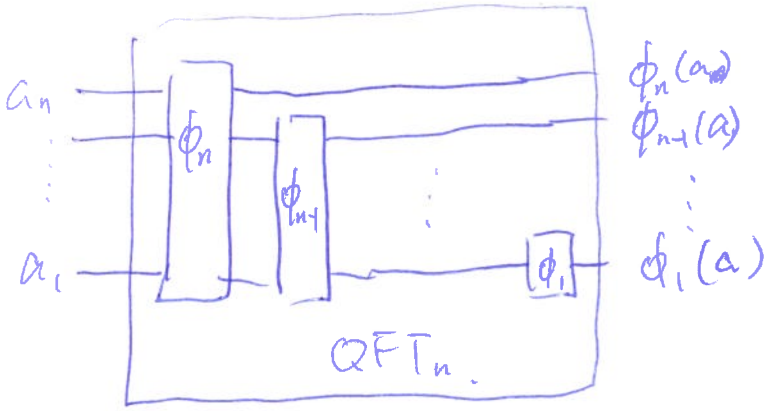
* ~~So~~ Let's consider $\phi_n(a) = \frac{1}{\sqrt{2}}(|0\rangle + \exp(0.a_n \cdots a_1)|1\rangle)$

$= \frac{1}{\sqrt{2}}(|0\rangle + \exp(0.a_n + 0.0a_{n-1} + \cdots$
$0.0\cdots a_1)|1\rangle$

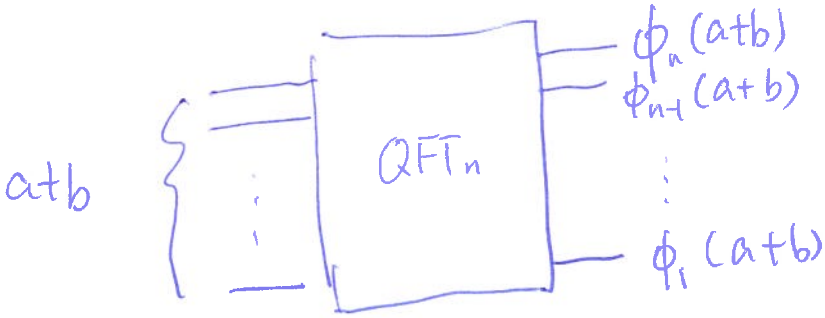
So the following implement ϕ_n.



So QFT_n ~~is a~~ can be implemented by a circuit of the following form.

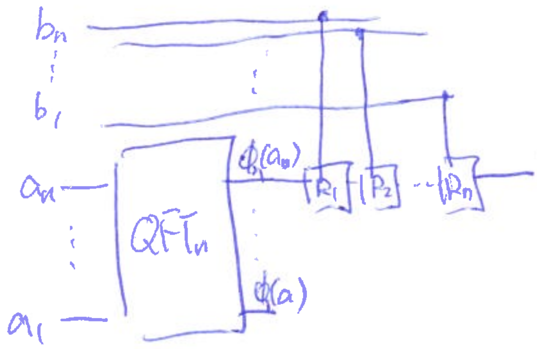


* ~~Now imagine~~ Note that we have



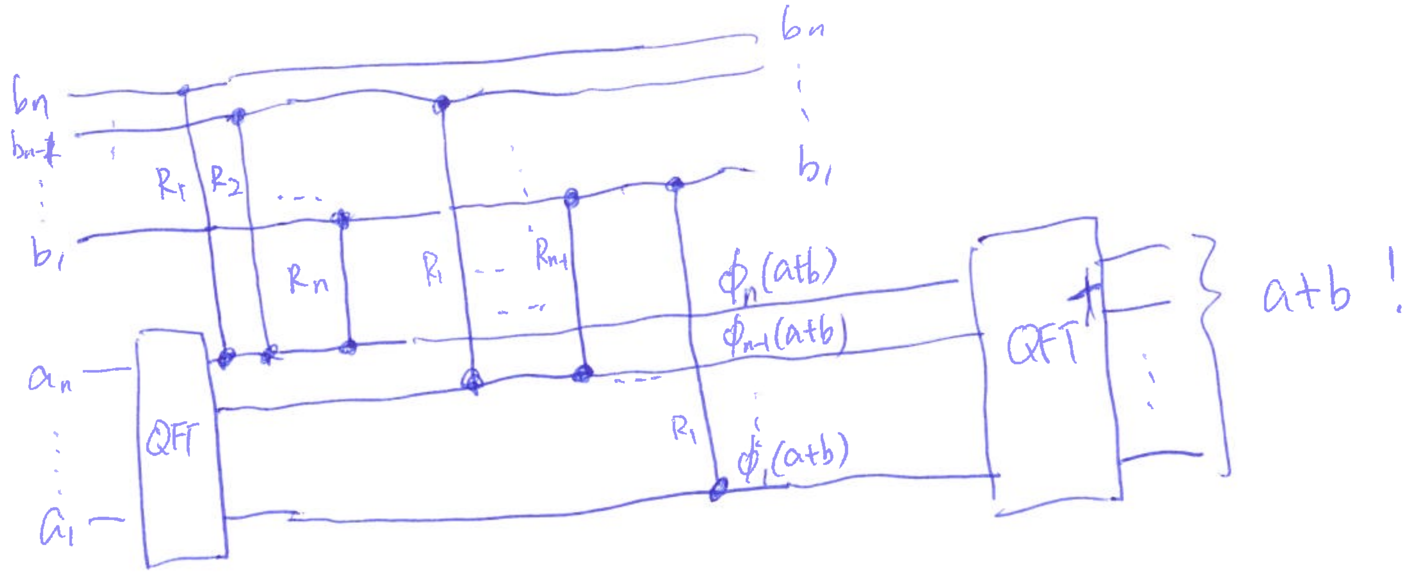
So if we can figure out how to construct $\phi_k(a+b)$, then we can apply $QFT_n^\dagger$ to obtain $a+b$.

* e.g. $\phi_n(a+b)$ can be realized by the following.



$$\phi_n(a+b) = |0\rangle + \exp\left(\frac{a+b}{2^n}\right)|1\rangle$$
$$= |0\rangle + \exp\left(\frac{a}{2^n} + \frac{b}{2^n}\right)|1\rangle$$
$$= |0\rangle + \exp(0.a_n + \cdots + 0.0\cdots 0a_1 + 0.b_n + \cdots + 0.00\cdots b_1)|1\rangle$$

* So the general scheme of doing QFT - addition is the following.



* Remark: 1. We basically shift the problem of addition to phase. and we do phase addition by using CR_n. gate. Then we use $QFT^\dagger$ to retrieve the result.

2. The QFT-addition scales nicely with multiple additions. e.g. $a+b+c$ will just be adding another layer of ~~contr~~ CRs.