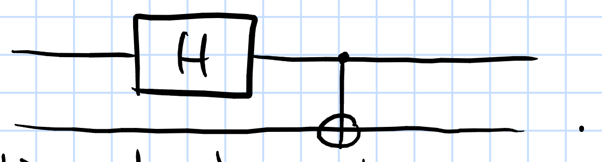
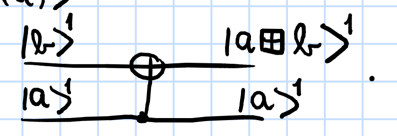
Exc.: consider the circuit $U=\Lambda^1(X)H\otimes 1\!\!1$:



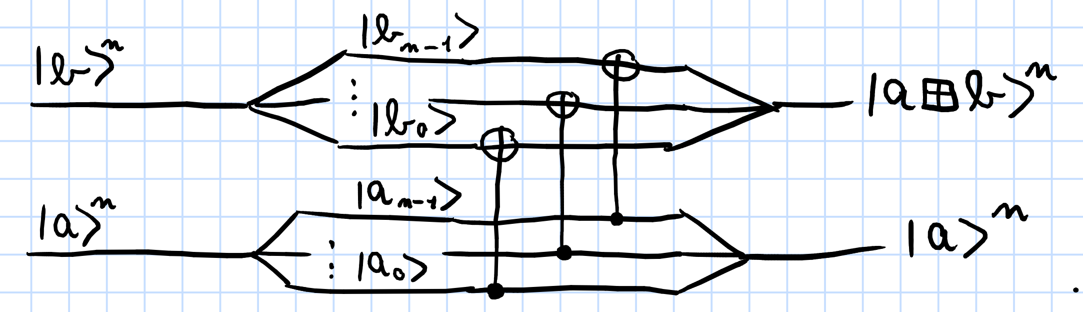
$U|00\rangle = |\Phi^+\rangle$, do the other cases.

2) $U_f : \mathbb{H}^n\otimes\mathbb{H}^n \to \mathbb{H}^n\otimes\mathbb{H}^n$, $|a\rangle\otimes|b\rangle \mapsto |a\rangle\otimes|b \boxplus f(a)\rangle$, $f:\mathbb{N}\to\mathbb{N}$.

Ex.: $U_{id} = U_{\boxplus}$. $n=1$:



$n>1$:



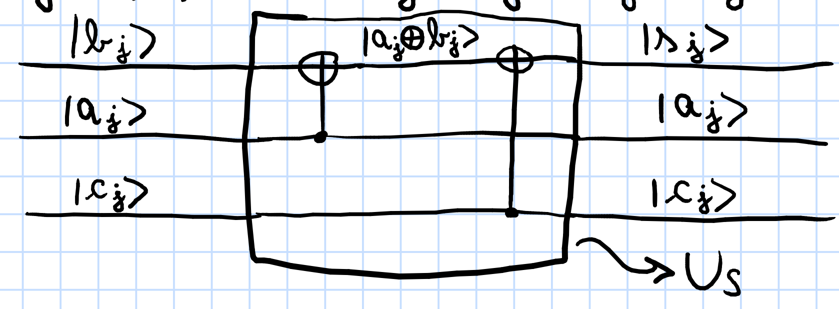
Ex.: $U_+ : \mathbb{H}^n\otimes\mathbb{H}^{n+1} \to \mathbb{H}^n\otimes\mathbb{H}^{n+1}$, $|a\rangle^n\otimes|b\rangle^{n+1}\mapsto |a\rangle^n\otimes|a+b\rangle^{n+1}$ $\forall a,b\in\{0,1,\dots,2^n-1\}$

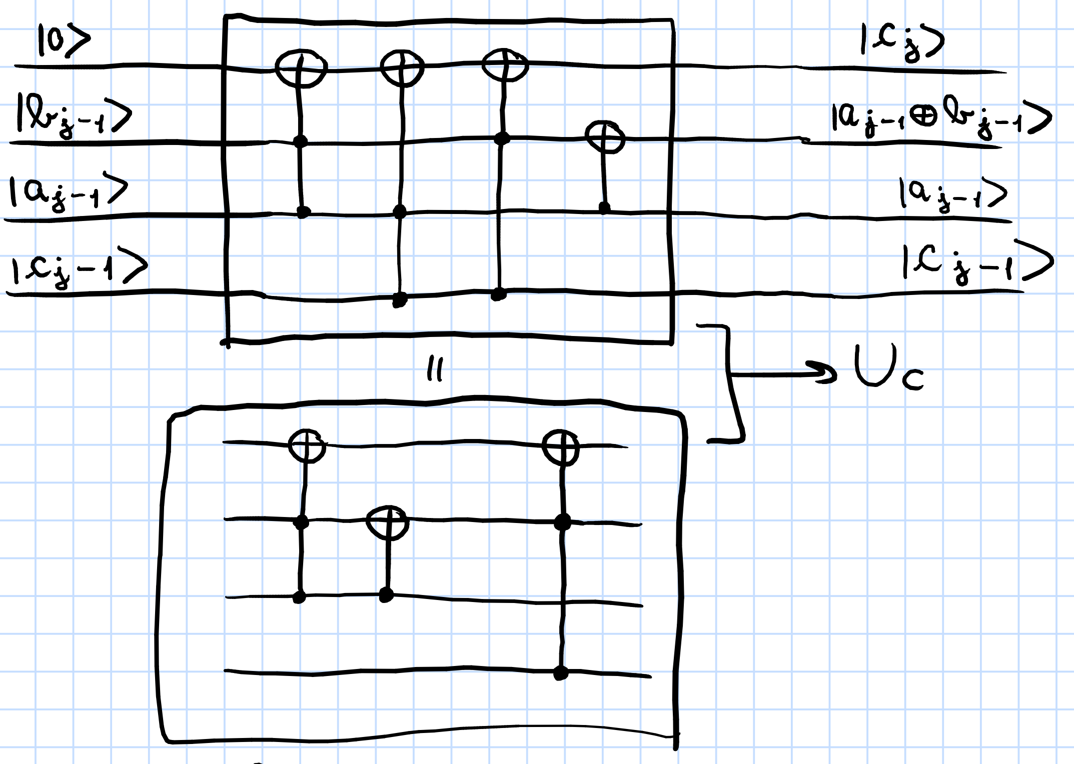
$a=\sum_{j=0}^{n-1}2^j a_j$, $b=\sum_{j=0}^{n-1}2^j b_j$, $a_j,b_j\in\{0,1\}$.

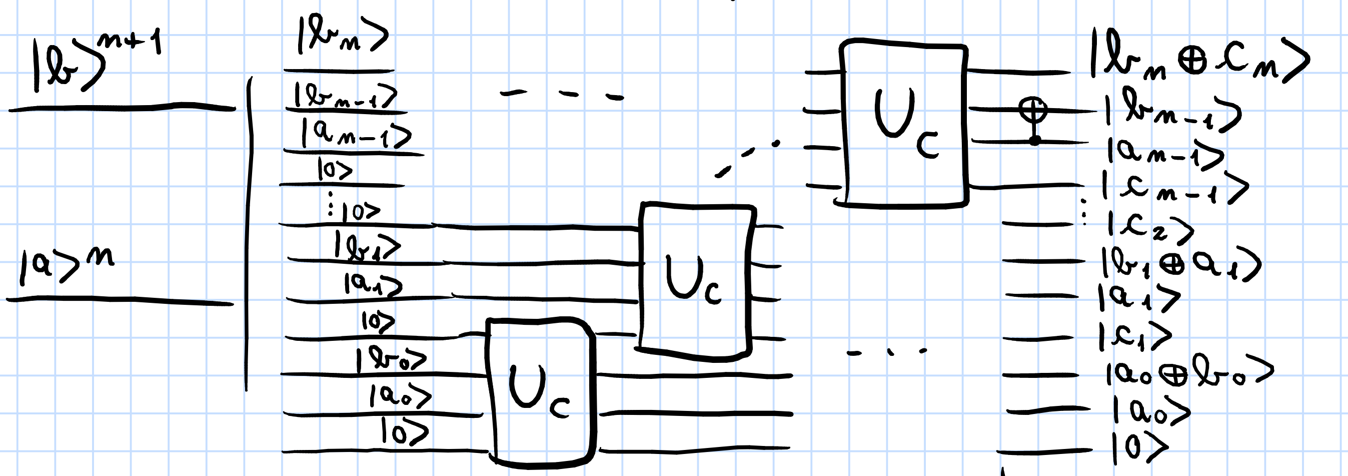
$a+b=\sum_{j=0}^{n-1}2^j s_j + 2^n c_n$ where we define

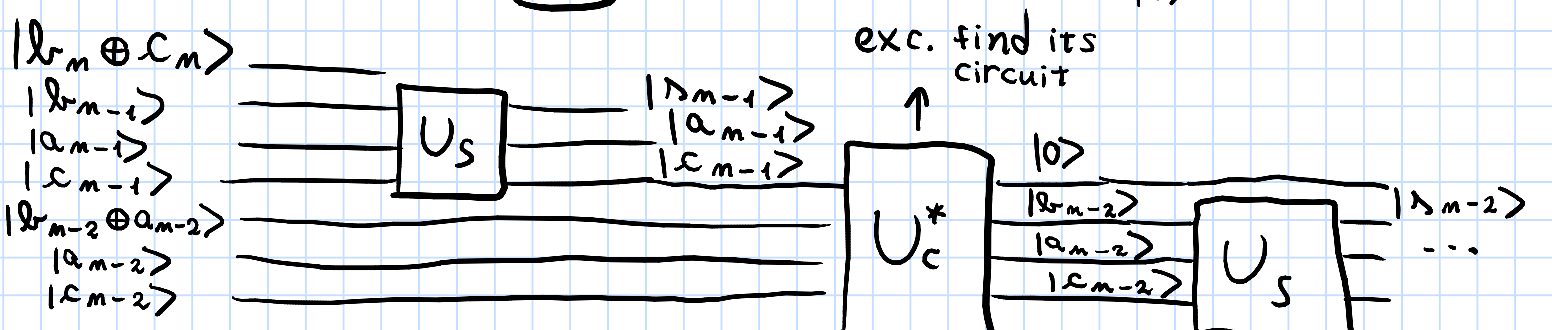
$\forall j=0,1,\dots,n$ $\quad c_j := \begin{cases}0 & j=0\\ (a_{j-1}b_{j-1})\oplus(a_{j-1}c_{j-1})\oplus(b_{j-1}c_{j-1}) & j=1,\dots,n,\end{cases}$

$\forall j=0,1,\dots,n-1$ $\quad s_j = a_j\oplus b_j\oplus c_j$.

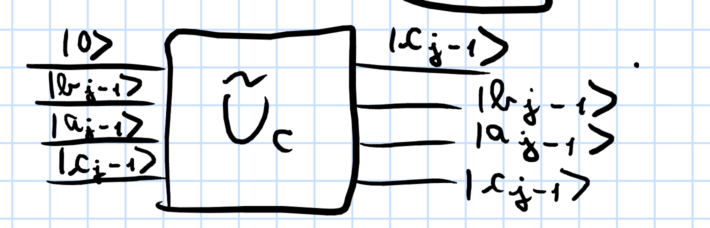








Exc.: try with



The construction requires $O(n)$ "elementary gates".

Extensions: $U_{+\bmod N} : \mathbb{H}^n\otimes\mathbb{H}^n\to\mathbb{H}^n\otimes\mathbb{H}^n$, $|a\rangle^n\otimes|b\rangle^n\mapsto|a\rangle^n\otimes|a+b \bmod N\rangle^n$

$\forall a,b\in\{0,1,\dots,N-1\}$ provided that $2^n\geq N$.

Define $\mathbb{H}^{<N}\subseteq\mathbb{H}^{\otimes n}$ as $\operatorname{span}\{|a\rangle^n \mid a\in\{0,1,\dots,N-1\}\}$;

then $U_{+\bmod N} : \mathbb{H}^{<N}\otimes\mathbb{H}^{<N}\to\mathbb{H}^{<N}\otimes\mathbb{H}^{<N}$.

Similarly, $U_{-\bmod N} = U^*_{+\bmod N}$, $U_{\cdot c \bmod N} : |a\rangle\otimes|b\rangle\mapsto|a\rangle\otimes|b+a c \bmod N\rangle$,

$U_{b^{\cdot} \bmod N} : \mathbb{H}^{<N}\to\mathbb{H}^{<N}$, $|a\rangle\mapsto|b^a \bmod N\rangle$, $a,b\in\{0,1,\dots,N-1\}$.

Quantum Fourier Transform

Recall: finite F.T.: $F: \underset{\mathbb{C}^N}{(c_x)_{x=0}^{N-1}} \mapsto (c_\xi)_{\xi=0}^{N-1} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{2\pi i\xi x/N} c_x$.

Fix $N=2^n$, $F:\mathbb{C}^{2^n}=\mathbb{H}^{\otimes n}\to\mathbb{H}^{\otimes n}$ unitary s.t.

$F|x\rangle^n = \frac{1}{\sqrt{2^n}}\sum_{\xi=0}^{2^n-1} e^{2\pi i x\xi/2^n}|\xi\rangle^n$, $F=(F_{\xi x})_{\xi,x=0,1,\dots,2^n-1}$, $F_{\xi x}=\frac{e^{2\pi i\xi x/2^n}}{\sqrt{2^n}}$.

$c_y = \begin{cases}1 & x=y\\ 0 & x\neq y\end{cases}$ How to implement F?

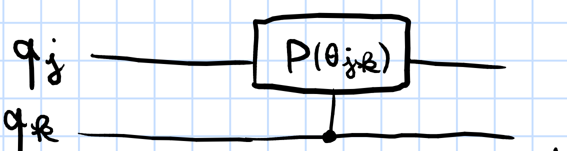
Lemma: we have for $|x\rangle^n\in\mathbb{H}^n$, $x=\sum_{j=0}^{n-1}x_j 2^j$,

$F|x\rangle^n = \frac{1}{2^{n/2}}\bigotimes_{j=0}^{n-1}\left(|0\rangle + e^{2\pi i(0,x_j x_{j-1}\dots x_0)}|1\rangle\right)$ where

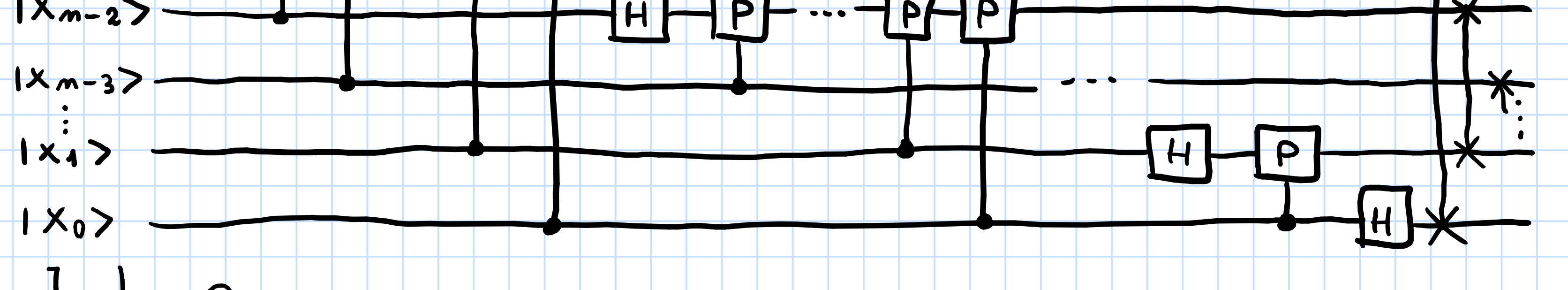
$0,x_j x_{j-1}\dots x_0 = \frac{x_j}{2}+\frac{x_{j-1}}{2^2}+\dots+\frac{x_0}{2^{j+1}}$.

Proof: do the calculations. □

Define P_{jk} "controlled phase shift by $\theta_{jk}=\frac{\pi}{2^{j-k}}$ with control at cubit k, actin on target qubit j", $j>k$.



Then one has $F = \underset{\text{swap}}{S^{(n)}}\prod_{j=0}^{n-1}\left(\prod_{k=0}^{j-1}P_{jk}\right)H_j$.



It has $O(n^2)$ gates.