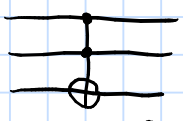
The set $\{M(\alpha), D_{\hat{y}}(\beta), D_{\hat{z}}(\gamma), \Lambda^1(X)\}_{\alpha,\beta,\gamma\in\mathbb{R}}$ is universal. How?

Ex.: i) $U\in\mathcal{U}(\mathbb{C}^2)$, $\Lambda^1(U)=?$

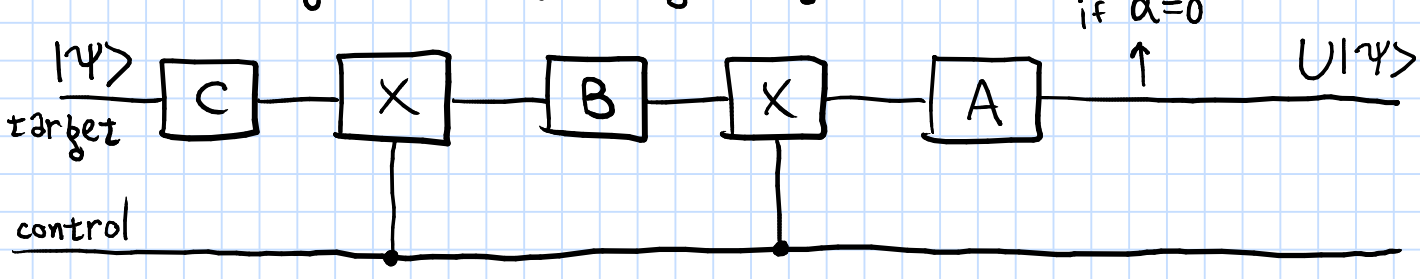
ii) Q-TOFFOLI:  ?

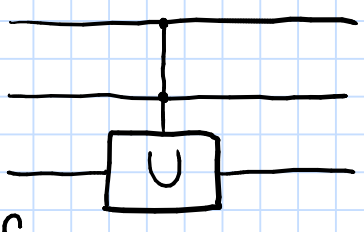
i) Recall that any $U\in\mathcal{U}(\mathbb{C}^2)$ can be decomposed as

$U=e^{i\alpha}A\sigma_x B\sigma_x C$ where $A=D_{\hat{z}}(\beta)D_{\hat{y}}(\gamma/2)$,

$B=D_{\hat{y}}(-\gamma/2)D_{\hat{z}}(-\frac{\delta+\beta}{2})$, $C=D_{\hat{z}}(\frac{\delta-\beta}{2})$, $\alpha,\beta,\gamma\in\mathbb{R}$ $(ABC=\mathbb{1})$.

$\sigma_x=X=-i\sigma_y\sigma_z\in F(\{M, D_{\hat{y}}, D_{\hat{z}}\})$





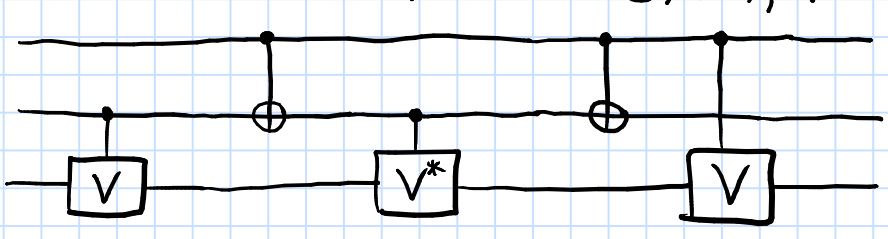
? Strategy 1: generalize the decomposition.

$U=EXDXCXBXA$,

$EDXCBXA=EXDCXBA=EDCBA=Id$.

Strategy 2: $V\in\mathcal{U}(\mathbb{C}^2)$ s.t. $V^2=U$, $VV^*=\mathbb{1}$.

Ex.: $\sigma_x=X=D_{\hat{x}}(\pi)$, $V=D_{\hat{x}}(\pi/2)$.



Circuits

i) plain circuit $H^{\otimes n}=\mathbb{H}^{I/O}$

ii) circuit with ancillas $\mathbb{H}^{I/O}\otimes(\mathbb{H}^{\otimes m})$ → ancillas

iii) general circuits with partial measurements and classical operations

Def.: a plain circuit is a composition of L "elementary" gates (↓ depth or length)

$U_1,U_2,\dots,U_L\in\mathcal{U}(\mathbb{H}^{I/O})$, $U=U_L\dots U_2U_1$.

If the system is initially in state $\rho\in\mathcal{D}(\mathbb{H}^{I/O})$, then after applying U we get the state $\rho\mapsto U\rho U^*$ $(|\psi\rangle\mapsto U|\psi\rangle)$.

Theorem: let $\mathbb{H}^{I/O}$, $\mathbb{H}^W$ be Hilbert spaces, let $|w_i\rangle$, $|w_f\rangle$ be states in $\mathbb{H}^W$ and let $\hat{U}\in\mathcal{U}(\mathbb{H}^{I/O}\otimes\mathbb{H}^W)$ s.t. $\hat{U}(|\psi\rangle\otimes|w_i\rangle)=(U|\psi\rangle)\otimes|w_f\rangle$ $\forall|\psi\rangle\in\mathbb{H}^{I/O}$. Then $|\psi\rangle\mapsto U|\psi\rangle$ is unitary on $\mathbb{H}^{I/O}$, and if $\rho\in\mathcal{D}(\mathbb{H}^{I/O})$ we have $U\rho U^*=Tr^W(\hat{U}(\rho\otimes|w_i\rangle\langle w_i|)\hat{U}^*)$.

Exc.: $M_A\otimes M_B\in\mathcal{D}(\mathbb{H}^A\otimes\mathbb{H}^B)$ if $M_A\in\mathcal{D}(\mathbb{H}^A)$, $M_B\in\mathcal{D}(\mathbb{H}^B)$.

Proof: it is easy to check linearity and the fact that is unitary.

$\rho=\sum_j p_j|\psi_j\rangle\langle\psi_j|$, $p_j\geq0$, $\sum_j p_j=1$, $|\psi_j\rangle$ ONB.

$Tr^W(\hat{U}(\rho\otimes|w_i\rangle\langle w_i|)\hat{U}^*)=\sum_j p_j\,Tr^W(\hat{U}|\psi_j\rangle\langle\psi_j|\otimes|w_i\rangle\langle w_i|\hat{U}^*)$.

We want $Tr^W(\hat{U}\underbrace{|\psi_j\rangle\langle\psi_j|\otimes|w_i\rangle\langle w_i|}_{=}\hat{U}^*)=U|\psi_j\rangle\langle\psi_j|U^*$.

$(|\psi_j\rangle\otimes|w_i\rangle)(\langle\psi_j|\otimes\langle w_i|)$

$\hat{U}|\psi_j\rangle\otimes|w_i\rangle=(U|\psi_j\rangle)\otimes|w_f\rangle\Rightarrow$

$\Rightarrow\hat{U}(|\psi_j\rangle\otimes|w_i\rangle)(\langle\psi_j|\otimes\langle w_i|)\hat{U}^*=$

$=(U|\psi_j\rangle)\otimes|w_f\rangle((\langle\psi_j|U^*)\otimes\langle w_f|)=(U|\psi_j\rangle\langle\psi_j|U^*)\otimes|w_f\rangle\langle w_f|$,

$Tr^W((U|\psi_j\rangle\langle\psi_j|U^*)\otimes|w_f\rangle\langle w_f|)=U|\psi_j\rangle\langle\psi_j|U^*$. ☐

Exc.: $Tr^B(\rho_A\otimes\rho_B)=\rho_A$

Def.: a unitary $U\in\mathcal{U}(\mathbb{H}^{I/O})$ is implemented by a q-circuit with ancilla system $\mathbb{H}^W$ and states $|w_i\rangle,|w_f\rangle\in\mathbb{H}^W$ if $\exists\hat{U}$ plain quantum circuit on $\mathbb{H}^{I/O}\otimes\mathbb{H}^W$ s.t. $\hat{U}(|\psi\rangle\otimes|w_i\rangle)=(U|\psi\rangle)\otimes|w_f\rangle$ $\forall|\psi\rangle\in\mathbb{H}^{I/O}$ (or equivalently $U\rho U^*=Tr^W(\hat{U}\rho\otimes|w_i\rangle\langle w_i|\hat{U}^*)$).

Def.: given $f:\mathbb{N}\to\mathbb{N}$ we write (for $n\geq1$) $U_f:\mathbb{H}^n\otimes\mathbb{H}^n\to\mathbb{H}^n\otimes\mathbb{H}^n$ where $\boxplus$ denotes bitwise addition mod 2: $|x\rangle^n\otimes|y\rangle^n\mapsto|x\rangle^n\otimes|y\boxplus f(x)\rangle^n$

$y\rightsquigarrow s(y)\in\{0,1\}^n=(\mathbb{Z}_2)^n$

$f(x)\rightsquigarrow s(f(x)\bmod 2^n)\in\{0,1\}^n=(\mathbb{Z}_2)^n$,

$a,b\in\{0,1\}^n$, $a\boxplus b:=(a_i\oplus b_i)_{i=1}^n$.

Ex.: $f(x)=x$. Then $U_f=U_\boxplus:|x\rangle^n\otimes|y\rangle^n\mapsto|x\rangle^n\otimes|x\boxplus y\rangle^n$.

A general structure of q-algorithms

1) Prepare the input state $|\psi\rangle\in\mathbb{H}^{I/O}$;

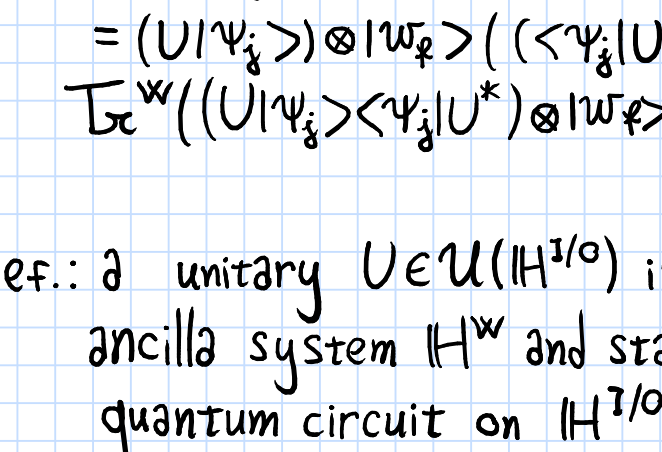
2) implementation of U_f for some (problem dependent) $f:\mathbb{N}\to\mathbb{N}$;

3) further "clever" transformations;

4) measure/observe the output.

1) Input state $|0\dots0\rangle=|0\rangle^n$, ancilla state $|w_i\rangle=|0\dots0\rangle=|0\rangle^m$.

Separable state $|\psi_0\rangle=\frac{1}{2^{m/2}}\sum_{x=0}^{2^n-1}|x\rangle^n$.



$|\psi_0\rangle=\underbrace{H\otimes\dots\otimes H}_{n}|0\dots0\rangle$.

If U_f implements $f:\mathbb{N}\to\mathbb{N}$, then $U_f(|\psi_0\rangle^n\otimes|y\rangle^m)=\frac{1}{2^{m/2}}\sum_{x=0}^{2^n-1}|x\rangle^n\otimes|y\boxplus f(x)\rangle^m$;

if $y=|0\rangle^m$, $\frac{1}{2^{m/2}}\sum_{x=0}^{2^n-1}|x\rangle^n\otimes|f(x)\rangle^m$.

4) Output measurement on $\mathbb{H}^{\otimes n}$.

$\Sigma_z^j=\mathbb{1}\otimes\dots\otimes\mathbb{1}\otimes\underset{\uparrow\ j\text{-th}}{\sigma_z}\otimes\mathbb{1}\otimes\dots\otimes\mathbb{1}$. $j\neq j'$, $[\Sigma_z^j,\Sigma_z^{j'}]=0$.

We can measure (or read out) on a state $\rho\in\mathcal{D}(\mathbb{H}^m)$ all the $(\Sigma_z^j)_{j=0}^{n-1}$ in any order and obtain a binary string $s\in\{-1,1\}^n\rightsquigarrow$

$\rightsquigarrow$ $x\in\{0,1,\dots,2^n-1\}$: after the measurement the system is in the pure state $|x\rangle^n$.