Lecture 9.

There is a small issue with the proof of the lemma from last lecture.

What if $u_{11}=0$?

<u>Rmk</u> ① There is at least one element in the first column of $U\in U_m(\mathbb{C})$, s.t. $u_{i1}\neq 0$ (otherwise $\det U=0$, while we know $|\det U|=1$).

② Let i be an index ($1\leq i\leq n$) with $u_{i1}\neq 0$, then

$$\begin{array}{cc} & \begin{array}{ccccccc} & & & i & & & \end{array} \\ i & \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & & & & & & 0 \\ \vdots & & \ddots & & & & & \vdots \\ 1 & & & 0 & & & & \vdots \\ 0 & & & & 1 & & & \vdots \\ \vdots & & & & & \ddots & & \vdots \\ 0 & 0 & \cdots & & & & & 1 \end{pmatrix} \end{array} \cdot U = \begin{pmatrix} u_{i1} & u_{i2} & \cdots & u_{im} \\ \vdots & & & \vdots \\ u_{11} & u_{12} & \cdots & u_{1m} \\ \vdots & & & \vdots \\ u_{m1} & \cdots & \cdots & u_{mm} \end{pmatrix}.$$

The 11-entry is nonzero now and we can proceed as last time.

<u>Observation</u>. The total number of operations will not exceed $1+2+\ldots+m-1=\frac{1+(m-1)}{2}(m-1)=\frac{m(m-1)}{2}$ as one of the entries in the first column is 0, hence, no 'action' on this entry is required.

The theorem looks cool, but how practical is it? There are way too many one-qubit operators (all matrices in $U_2(\mathbb{C})$) and we also want all two-qubit operators...

This is impractical, so let's try to use approximations instead.

Def-n. Let $A: \mathbb{C}^n \circlearrowleft$ be an operator. The norm of A is $\|A\| := \sup\limits_{|v\rangle \in \mathbb{C}^n} \frac{||A|v\rangle|}{||v\rangle|}$.

Example. Let $U \in U_n(\mathbb{C})$ be a unitary operator. Then $\forall |v\rangle \in \mathbb{C}^n$, we have

$$|U|v\rangle|^2 = \langle Uv|Uv\rangle = \langle v|v\rangle = ||v\rangle|^2.$$

Thus $\|U\| = 1$.

Properties of the norm.

1. $\|AB\| \leq \|A\| \|B\|$;
2. $\|A^\dagger\| = \|A\|$;
3. $\|A \otimes B\| = \|A\| \cdot \|B\|$;
4. $\|A+B\| \leq \|A\| + \|B\|$.

Q: what does it mean that $\tilde{U}$ approximates U with precision $\varepsilon > 0$?

Answer: $\|U - \tilde{U}\| \leq \varepsilon$, in other words, if we evaluate $\tilde{U}|v\rangle$ instead of $U|v\rangle$ the magnitude of the 'error vector' does not exceed ε (for any $|v\rangle$).

Rmk. The difference of two unitary operators $U, \tilde{U} \in U_n(\mathbb{C})$ is usually not a unitary operator.

Observation/lemma. $\|U-\tilde{U}\| \leq \varepsilon \Rightarrow \|U^{-1}-\tilde{U}^{-1}\| \leq \varepsilon$.

Indeed, $\underbrace{\|\tilde{U}^{-1}(U-\tilde{U})U^{-1}\|}_{\|\tilde{U}^{-1}-U^{-1}\|} \leq \underbrace{\|\tilde{U}^{-1}\|}_{1} \cdot \|U-\tilde{U}\| \cdot \underbrace{\|U^{-1}\|}_{1} \leq \varepsilon$.

Def-n. We say that a unitary operator $U : (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ is approximated by $\tilde{U}$ with precision ε using ancillas (auxiliary qubits) if for arbitrary $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$:

$$\|\tilde{U}(|\psi\rangle \otimes |0^k\rangle) - U(|\psi\rangle) \otimes |0^k\rangle\| \leq \varepsilon \cdot \||\psi\rangle\|.$$

Thm. For any $\varepsilon > 0$ the basis $A = \{H, T, T^{-1}, NOT, CCNOT\}$ allows to realize any unitary operator on a fixed number of qubits with precision ε by a poly$(\log(1/\varepsilon))$-size circuit using ancillas.

$H \in U_2(\mathbb{C})$, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ the Hadamard operator

$T \in U_2(\mathbb{C})$, $T = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.