Lecture 8.

Let $V = \mathbb{C}^n$ be a vector space with a hermitian inner product. Given a vector $v \in V$ we can produce a map $f_v : V \to \mathbb{C}$ via $f_v(w) := \langle v | w \rangle$. It is straightforward to check that the map f_v is linear:

(1) $f_v(w_1 + w_2) = f_v(w_1) + f_v(w_2) \quad \forall w_1, w_2 \in V$.

(2) $f_v(\lambda w) = \lambda f_v(w) \quad \forall w \in V, \lambda \in \mathbb{C}$.

<u>Def-n.</u> The <u>dual space</u> V^* is the space of linear functions on V with values in $\mathbb{C}$: $V^* := \left\{ \ell : V \to \mathbb{C} \;\middle|\; \ell \text{ satisfies the (1),(2) above} \right\}$

The vector spaces V and V^* are isomorphic via $v \mapsto f_v$.

Dirac's notation.

Let $v, w \in V$

$\langle v | w \rangle$ - bracket

$\langle v |$ $= f_v \in V^*$ bra-vector (written as a row vector)

$| w \rangle \in V$ ket-vector (written as a column vector)

Rmk. Let $U : V \circlearrowleft$ be a unitary operator. We use the notation $\langle v | U | w \rangle$ for $f_v(U|w\rangle)$.

The following result shows that one-qubit and two-qubit gates (unitary operators) suffice to realize any n-qubit gate (operator in $U_{2^n}(\mathbb{C})$).

Thm. The basis consisting of all one-qubit and two-qubit unitary operators allows realization of an arbitrary unitary operator $(\mathbb{C}^2)^{\otimes n} \circlearrowleft$.

Strategy of proof.

Step 1. Realize CCNOT.

Step 2. Let $U \in U_2(\mathbb{C})$ be a unitary operator. Realize the operator $\underbrace{C \ldots C}_{k} U$ with $2 \leq k \leq n-1$. This is the operator acting as U on the indicated qubit provided all control qubits are in state $|1\rangle$.

Step 3. Let $U \in U_2(\mathbb{C})$ with $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{B}^n$ (basic states). Realize $\tilde{U} : (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ given by

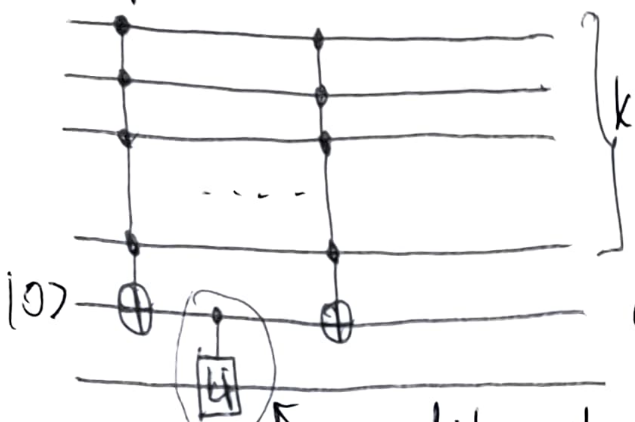
$$\tilde{U}(|\psi\rangle) := \begin{cases} |\psi\rangle, & \psi \neq x, y \text{ is a basic vector } (\psi \in \mathbb{B}^n) \\ U|\psi\rangle, & |\psi\rangle \in \operatorname{span}_{\mathbb{C}}(|x\rangle, |y\rangle). \end{cases}$$

Step 4. Show that any $U \in U_{2^n}(\mathbb{C})$ can be written as a composition (product) of operators from step 3.

The actual proof:

Step 1 is an exercise (see HW2)

Step 2 is realized via the circuit:



<u>Rmk.</u> We can use the classical circuit for $\underbrace{C\ldots C}NOT$ that we had before (comprised of CCNOT and NOT^k operators). $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in U_2(\mathbb{C})$ is a one-qubit operator and CCNOT is at our disposal

Algorithm and circuit for step 3:

① Single out $|x\rangle$ and $|y\rangle$

via $|x\rangle \mapsto |11\ldots 10\rangle$

$|y\rangle \mapsto |11\ldots 11\rangle$.

② Apply $\underbrace{C\ldots C}_{k}U$.

③ Undo ① by repeating it.

Finally, step 4 follows from the following general result:

<u>Lemma.</u> Let $U : \mathbb{C}^m \circlearrowleft$ be a unitary operator. Then U can be written as a composition of operators (product of the corresponding matrices) of the form

$$\begin{array}{cc} & \begin{matrix} \quad & i & \quad & j & \quad \end{matrix} \\ U_{ij} := \begin{matrix} \\ i \\ \\ j \\ \\ \end{matrix} & \left(\begin{array}{c|c|c|c|c} \begin{smallmatrix}1 & & \\ & \ddots & \\ & & 1\end{smallmatrix} & & 0 & & 0 \\ \hline & a & & b & \\ \hline 0 & & \begin{smallmatrix}1 & & \\ & \ddots & \\ & & 1\end{smallmatrix} & & 0 \\ \hline & c & & d & \\ \hline 0 & & 0 & & \begin{smallmatrix}1 & & \\ & \ddots & \\ & & 1\end{smallmatrix} \end{array}\right) \end{array} \quad \text{with } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_2(\mathbb{C}).$$

<u>Proof.</u> By induction on m with base $m=2$. Let

$$U = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ u_{21} & u_{22} & & \vdots \\ \vdots & & \ddots & \\ u_{m1} & \cdots & & u_{mm} \end{pmatrix} \in U_m(\mathbb{C}) \text{ and}$$

$$U_{12} := \left(\begin{array}{c|c} A & 0 \\ \hline 0 & \begin{smallmatrix}1 & & \\ & \ddots & \\ & & 1\end{smallmatrix} \end{array}\right) \quad \text{with } A = \begin{pmatrix} * & * \\ -\frac{u_{21}}{u_{11}} & 1 \end{pmatrix} \text{ a } 2\times 2 \text{ matrix.}$$

Notice that $U_{12}U$ is of the form $\left(\begin{array}{c|c} * & * \cdots * \\ \hline 0 & \\ * & * \\ \vdots & \\ * & \end{array}\right)$.

Similarly we can choose $U_{13} \in U_{13}$ to get

$U_{13}U_{12}U = \left(\begin{array}{c|c} * & * \cdots * \\ \hline 0 & \\ 0 & \\ * & * \\ \vdots & \\ * & \end{array}\right)$ and similarly $U_{1m}U_{1m-1}\cdots U_{13}U_{12}$ with

$$\tilde{U} := U_{1m}\cdots U_{12}U = \left(\begin{array}{c|c} \lambda & \tilde{u}_{12} \cdots \tilde{u}_{1m} \\ \hline 0 & \\ \vdots & * \\ 0 & \end{array}\right).$$

Here is an important observation / exercise:
as $\tilde{U} \in U_m(\mathbb{C})$ is unitary, $U^\dagger U = UU^\dagger = I$, hence $UU^\dagger_{11} = U^\dagger U_{11} = 1$. Show that the latter implies $\tilde{U}_{12} = \tilde{U}_{13} = \dots \tilde{U}_{1m} = 0$, hence $\tilde{U} = \begin{pmatrix} \lambda & 0 \dots 0 \\ 0 & \\ \vdots & U' \\ 0 & \end{pmatrix}$ (with $|\lambda| = 1$). Multiplying $\tilde{U}$ by $\begin{pmatrix} \bar{\lambda} & 0 \\ 0 & \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} \end{pmatrix}$, we can assume that $\lambda = 1$. The statement follows by inductive assumption.

<u>Rmk.</u> ① We need A_{ij} to be unitary. Not a big deal:
$A = \begin{pmatrix} a & b \\ -\frac{u_{j1}}{u_{11}} & 1 \end{pmatrix}$. Pick $(a\ b)$, so that $\langle (a, b) | (-\frac{u_{j1}}{u_{11}}, 1) \rangle = 0$ and normalize the vectors (a, b) and $(-\frac{u_{j1}}{u_{11}}, 1)$, so they become of norm 1 (this is done by rescaling).

② As $|\bar{\lambda}| = |\lambda| = 1$, we can use $U_{1m} = \begin{pmatrix} \bar{\lambda} a & b \\ c & d \end{pmatrix}$ (the 2×2 part of the matrix) in order to get $U_{1m} \dots U_{12} U = \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & U_{new} \\ 0 & \end{pmatrix}$ with $U_{new} \in U_{m-1}(\mathbb{C})$.

③ In the end we arrive with the expression

$$[U_{m-1m} U_{m-2m} U_{m-2m-1} \cdots U_{1m} \cdots U_{12}] U = Id \text{ or } U = A^{-1} =$$

$$\underbrace{\phantom{U_{m-1m} U_{m-2m}}}_{= A}$$

$$= A^{\dagger} = U_{12}^{\dagger} \cdots U_{1m}^{\dagger} \cdots U_{m-1m}^{\dagger}.$$

<u>Observation.</u> The classical reversible operators $\mathbb{B}^n \circlearrowleft$ are permutations. Each permutation $\sigma \in S_n$ is a unitary operator. As $\langle e_{\sigma(i)} | e_{\sigma(j)} \rangle = \delta_{\sigma(i)\sigma(j)} = \delta_{ij}$ (since σ is one to one), σ preserves the inner product.