Universal construction of unitaries

We're now ready to tackle the generic problem of given an n-qubit unitary $U: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$, implement it over a fixed (but infinite, for now) set of unitary gates on 1 or 2 qubits. We will progress down through progressively smaller gate sets as below, showing that each can be constructed over the simpler set.

n-qubit unitaries

↓

two-level unitaries

↓

single-qubit + permutation gates

↓

single qubit + MCT gates

↓ DONE!

single qubit + CNot gates

⇓ — squiggly line...

$\{H, CNOT, T\}$

This made QC possible!!!

Construction by two-level unitaries

A two-level unitary is a unitary matrix that acts non-trivially on only two rows and columns

E.g. $H_{1,3} = \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \end{bmatrix}$ is a two-level H gate on rows/colums 1 & 3

Thm.

Any $d \times d$ unitary matrix U can be factorised as a product of $O(d^2)$ two-level unitaries

$$U = U_1 \cdots U_k, \quad U_i \text{ is two-level}$$

To prove the above theorem, it will help to give a column lemma.

Lemma. (column lemma)

Let $v \in \mathbb{C}^d$ be a unit vector. There exists a series of (at most d) two-level $d \times d$ unitary matrices $U_1, \ldots, U_k$ such that

$$U_k^\dagger \cdots U_1^\dagger v = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

PF.

By induction on the non-zero entries of v.

If v has 1 non-zero entry, then

$$\begin{bmatrix} 0 & \cdots & a^* & \cdots & 0 \\ \vdots & \ddots & & & \vdots \\ a & & 0 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ a \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

(Pf. cont.)

If v has ≥ 2 non-zero entries, then

$$\frac{1}{\alpha}\begin{bmatrix} a & \cdots & & 0 \\ \vdots & \ddots & & \\ & a^* & b^* & \\ & \vdots & \vdots & \\ & b & -a & \\ 0 & & & \alpha \end{bmatrix}\begin{bmatrix} \vdots \\ a \\ \vdots \\ b \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \alpha \\ \vdots \\ 0 \\ \vdots \end{bmatrix}$$

where $\alpha = \sqrt{|a|^2+|b|^2}$. Since the matrix on the left acts trivially on every other row of v, we've reduced the number of non-zero rows, so we're done □

(Note: d rows so $\leq d$ operators)

Now we can prove the theorem, namely that every unitary can be factorized as a product of two-level operators.

Pf.

By induction on d (recall U is a $d \times d$ unitary)

If $d = 2$, then U is two-level by definition.

If $d > 2$, then let v be the first column of U.

By the column lemma, there exists a two-level unitary U_1 s.t.

$$U_1^\dagger v = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \text{ so } U_1^\dagger U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ 0 & & U' & \\ \vdots & & & \\ 0 & & & \end{bmatrix}$$

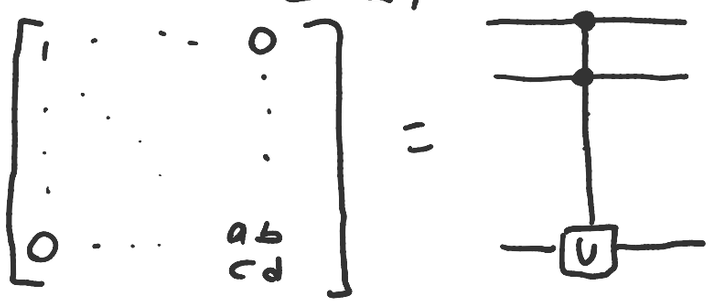
where U' is a $d-1 \times d-1$ unitary. We can use the ind. hyp. to write U' as a product $U_2 \cdots U_k$ of two-level matrices

hence $U_1^\dagger U = U_2 \cdots U_k \Rightarrow U = U_1 U_2 \cdots U_k$ ← $O(d^2)$

Decomposing two-level unitaries

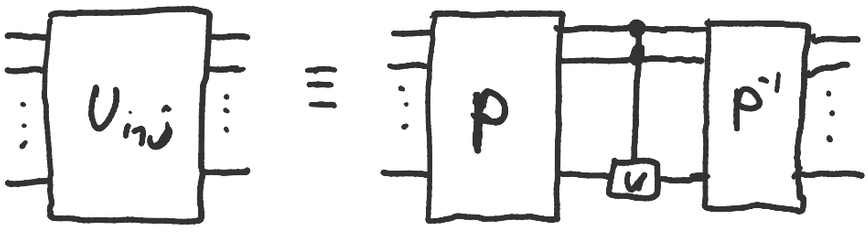
Next we need to show how two-level unitaries may be implemented. We do this in stages.

Recall that for $U = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$,



(Decomposition into permutations & single qubit ops)

Let $U_{i,j}$ be an n-qubit unitary acting as U on rows/columns i, j (i.e. $U_{i,j}$ is a two-level U-gate). Then



for some permutation $P: |i\rangle \mapsto |2^n - 1\rangle$
$|j\rangle \mapsto |2^n\rangle$

E.g.

$$\begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix} \begin{matrix} \\ \\ i \\ \\ j \end{matrix} \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & a & b & \\ & & c & d & \\ 0 & & & & 1 \end{bmatrix} \begin{matrix} \\ \\ i \\ \\ j \end{matrix} \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & & & \\ & & & \ddots & \\ 0 & & & & \begin{matrix} a & b \\ c & d \end{matrix} \end{bmatrix}$$

Since we know the multiply-controlled U gate can be implemented with permutations (e.g. Toffoli & CNOT) and single-qubit gates, we're done!

Decomposing into MCT gates

Now that we've reduced our gate set to single qubit and permutation operators, we need to show that permutation operators can be compiled to MCT gates.

Let's do the fun algebraic version!

Fact

A $d \times d$ permutation matrix P is a linear representation of a permutation σ in S_d (Symmetric group)

E.g. Let $P = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. Then

$P|0\rangle = |1\rangle$
$P|1\rangle = |2\rangle$ → P is the permutation
$P|2\rangle = |0\rangle$

in S_3

Fact

Every permutation in S_d can be written as a product of adjacent transpositions $(i, i+1)$ ← swaps i & $i+1$

E.g. 

$= \underbrace{(0,1)(1,2)}$

evaluated right to left, i.e.

$0 \to 0 \to 1$
$1 \to 2 \to 2$
$2 \to 1 \to 0$

The Gray code

The gray code is a binary encoding of numbers such that adjacent numbers differ by a single bit

E.g. $0 \longrightarrow 00$

$1 \longrightarrow 01$

$2 \longrightarrow 11$

$3 \longrightarrow 10$

Fact.

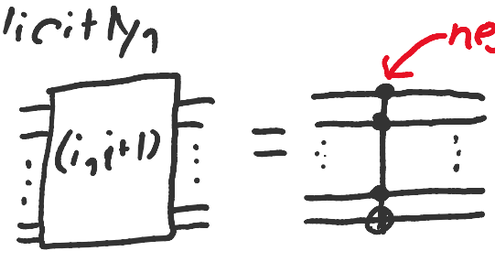
Under the gray encoding, an adjacent transposition $(i, i+1)$ can be implemented by an MCT gate with some negative controls

E.g. WLOG assume $i, i+1$ differ in their last bit, i.e.

$$i = x_1 \cdots x_k 0$$
$$i+1 = x_1 \cdots x_k 1$$

Then with a single MCT gate we can transpose $i, i+1$ by flipping the final bit if and only if each of the preceding bits are in the state $x_1 \cdots x_k$

Explicitly,



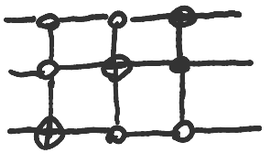
Decomposition into MCT gates

Thm.

An arbitrary permutation $P: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ can be implemented using MCT gates

Ex.

To permute $|001\rangle \to |111\rangle$ we can use the sequence $001 \to 000 \to 010 \to 110$, which corresponds to the following circuit



Note:

Generically, implementing a permutation this way would use $O(4^n)$ MCT gates for an n-qubit circuit. A tighter analysis gives $O(n)$ since we can choose **any** permutation that sends

$$|i\rangle \longmapsto |i\rangle \quad \leftarrow \text{(gray code order)}$$
$$|j\rangle \longmapsto |i+1\rangle$$

and in particular we need only flip at most $n-1$ bits. It doesn't really matter anyway because we already have $O(4^n)$ two-level operators, so this won't be efficient in practice!

A note about permutations

Recall that permutations on $\mathbb{C}^{2^n}$ are exactly the n-bit reversible functions, so it is useful to study them. A classic theorem relates the even permutations

$$A_d \triangleleft S_d$$

to the existence of ancilla-free circuits over

$$\{CNot, X, Toffoli\}$$

(Note: even permutations are ones with an even number of transpositions. As matrices, P is an even permutation if & only if $\det P = 1$)

Thm.

Let P be a $2^n \times 2^n$ permutation matrix. Then P can be implemented over $\{CNOT, X, Toffoli\}$ if and only if P is even (i.e. $\det P$ is 1) provided $n > 3$.

Pf sketch.

The backwards direction is easy given that:

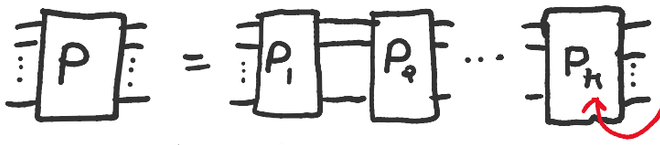
$$\det AB = \det A \cdot \det B$$

$$\det A \otimes I_2 = (\det A)^2$$

$$\det X/CNOT/Toffoli = -1$$

So any 4 or more qubit circuit over $\{CNOT, X, Toffoli\}$ has determinant 1

The other direction can be shown constructively by implementing



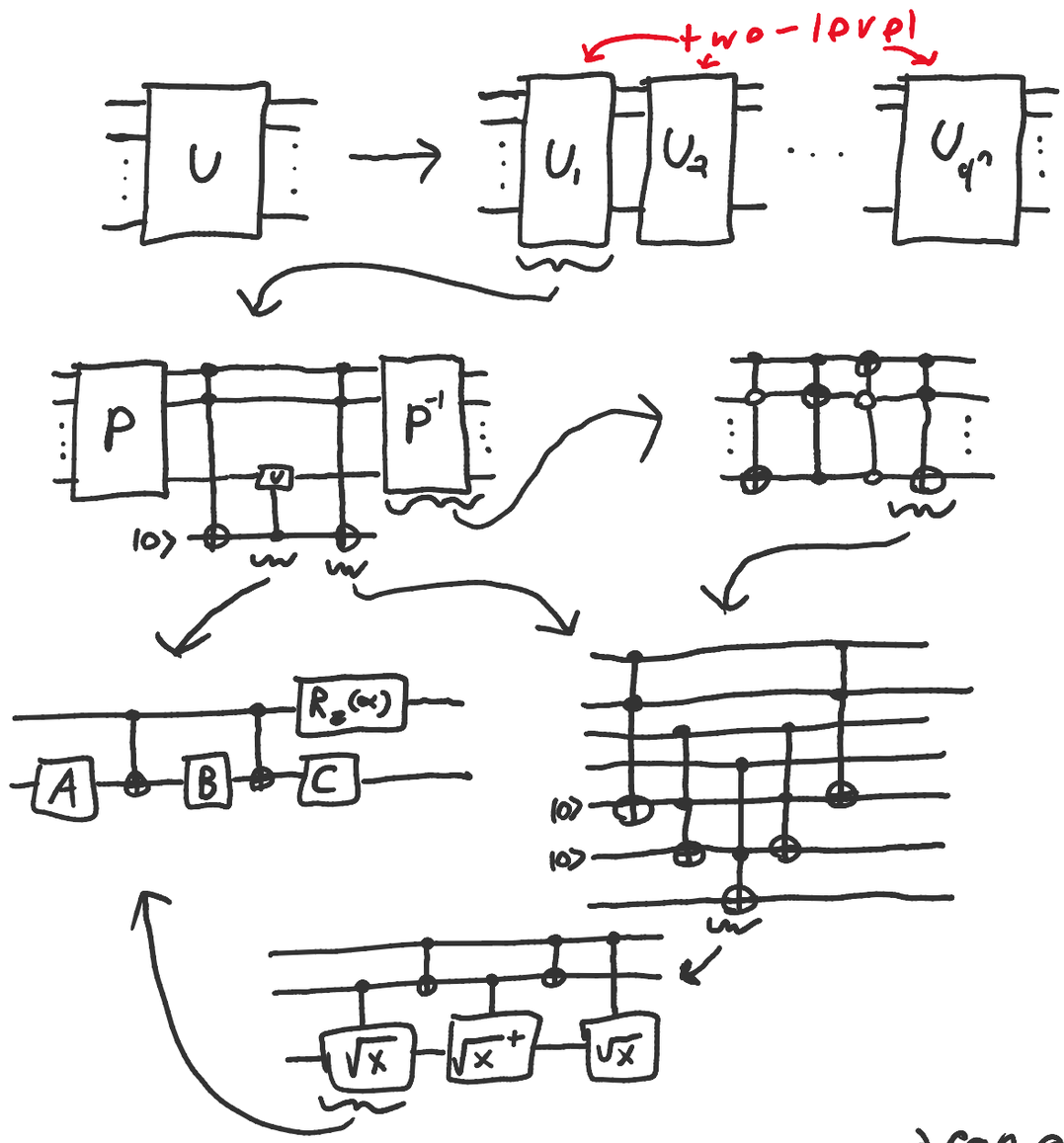
where each P_i is on only n-1 qubits

best known upper bound is 9

Open question!

Decomposition into single-qubit + CNOT gates

What we've shown



How many gates is that?

- $O((2^n)^2)$ two-level per Unitary
- $O((2^n)^2)$ MCT per permutation* → can get down to $O(n)$
- $O(n)$ single-qubit + CNOT per MCT

$\therefore O(n^2 16^n)$ (or $O(n^2 4^n)$)