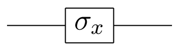
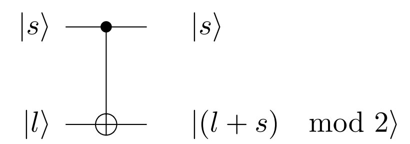
Exercise 1) Quantum Circuits

Any (unitary) transformation of a quantum system can be represented as a quantum circuit. An easy example is the Pauli-X transformation applied to a qubit:



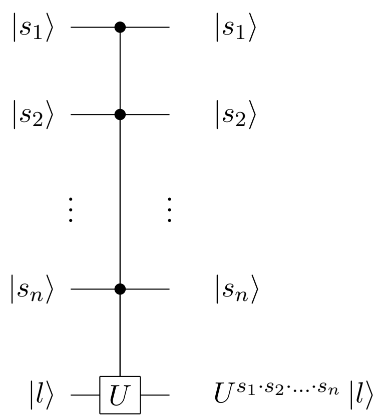
The circuit is to be read from left-to-right. From now on we restrict ourselves to qubits, but the generalization to higher dimensional systems is straightforward.

An important transformation is the controlled-NOT gate. It is defined as:



Write down the matrix of the controlled-NOT gate and check that it is unitary.

Other transformations are so called controlled-U gates, where U is some unitary transformation:



Write down the matrix of the controlled-U gate and check that it is unitary.

The goal of this exercise is to show that general controlled-U gates can be decomposed into single qubit unitary operations and controlled-NOT gates. For this we need the following Lemmata.

Lemma 1. Let $V \in U(2)$, where $U(2) = \{M \in M_2(\mathbb{C}) | MM^\dagger = \mathbb{1}_2\}$. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$V = \exp(i\alpha) U(\vec{e}_z, \beta) U(\vec{e}_y, \gamma) U(\vec{e}_z, \delta) \ ,$$

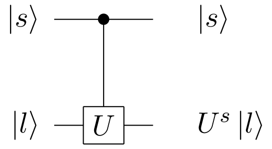
where $U(\vec{e}, \epsilon) = \exp(-i\frac{\epsilon}{2}\vec{e} \cdot \vec{\sigma})$, $\vec{e}_z = (0,0,1)^T$ and $\vec{e}_y = (0,1,0)^T$.

Prove Lemma 1.

Lemma 2. Let $V \in U(2)$. Then there exist $\alpha \in \mathbb{R}$ and $A, B, C \in U(2)$ such that $ABC = \mathbb{1}$ and

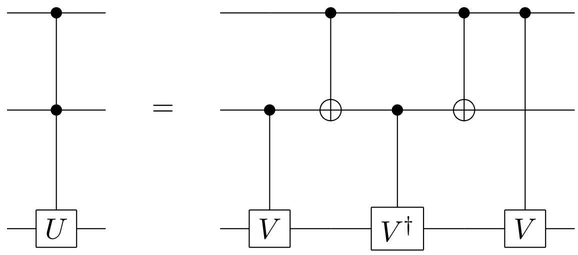
$$V = \exp(i\alpha) A \sigma_x B \sigma_x C \ .$$

Use Lemma 1 to prove Lemma 2 (a bit tricky!) and then use Lemma 2 to decompose



into single qubit unitary operations and controlled-NOT gates.

Thereafter show that there exist a $V \in U(2)$ for every $U \in U(2)$ such that



Finally put everything together and describe how you can decompose general controlled-U gates into single qubit unitary operations and controlled-NOT gates.

Exercise 2) Representations of SU(2)

The goal of this exercise is to show explicitly that there is a one-to-one relation between representations of the Lie group $SU(2)$ and representations of the corresponding Lie algebra $su(2)$.

For every $a \in su(2)$ the exponential map is defined by

$$\begin{aligned} &\exp : su(2) \to SU(2) \\ &a \mapsto \exp(ia) \ , \end{aligned}$$

where $\exp(X) := \sum_{k=0}^{\infty} \frac{X^k}{k!}$.

Let v_k be the irreducible representations of $su(2)$ as defined in the lecture. Show that

$$V_k(\exp(ia)) := \exp(iv_k(a))$$

defines representations of $SU(2)$.

And vice versa, let V_k be the representations of $SU(2)$ as found above. Show that

$$v_k(a) := -i\frac{d}{dt}V_k(\exp(iat))|_{t=0}$$

defines representations of $su(2)$.

Hint: Use the Baker-Campbell-Hausdorff formula.