Exercise 1) Quantum Circuits

In the standard basis the matrix of the controlled-NOT gate is given by

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} .$$

It is unitary since $U_{CNOT}^\dagger U_{CNOT} = \mathbb{1}_4$.

The matrix of a controlled-U gate is given by

$$U_{C-U} = \begin{pmatrix} \mathbb{1}_{(2^{n+1}-2)} & 0 \\ 0 & U \end{pmatrix} .$$

It is unitary since $U_{C-U}^\dagger U_{C-U} = \mathbb{1}_{2^{n+1}}$.

Lemma 1 can be proven as follows. A straightforward calculation gives us

$$\begin{aligned} &\exp(i\alpha)U(\vec{e}_z,\beta)U(\vec{e}_y,\gamma)U(\vec{e}_z,\delta) && (1)\\ &= \begin{pmatrix} \exp(i(\alpha-\beta/2-\delta/2))\cos(\frac{\gamma}{2}) & -\exp(i(\alpha-\beta/2+\delta/2))\sin(\frac{\gamma}{2}) \\ \exp(i(\alpha+\beta/2-\delta/2))\sin(\frac{\gamma}{2}) & \exp(i(\alpha+\beta/2+\delta/2))\cos(\frac{\gamma}{2}) \end{pmatrix} && (2) \end{aligned}$$

Since V is unitary, the rows and columns of V have to be orthonormal. From this it follows that there exist $\alpha,\beta,\gamma,\delta \in \mathbb{R}$ such that V can be written as in (2).

Lemma 2 can be proven as follows. Define

$$A = U(\vec{e}_z,\beta)U(\vec{e}_y,\frac{\gamma}{2})$$

$$B = U(\vec{e}_y,-\gamma/2)U(\vec{e}_z,-\frac{\delta+\beta}{2}))$$

$$C = U(\vec{e}_z,\frac{\delta-\beta}{2}) .$$

Then

$$ABC = U(\vec{e}_z,\beta)U(\vec{e}_y,\frac{\gamma}{2})U(\vec{e}_y,-\frac{\gamma}{2})U(\vec{e}_z,-\frac{\delta+\beta}{2}))U(\vec{e}_z,\frac{\delta-\beta}{2}) = \mathbb{1} .$$

Since $\sigma_X^2 = \mathbb{1}$ and $\sigma_X U(\vec{e}_y,\theta)\sigma_X = U(\vec{e}_y,-\theta)$ as well as $\sigma_X U(\vec{e}_z,\theta)\sigma_X = U(\vec{e}_z,-\theta)$ for all $\theta \in \mathbb{R}$, we have

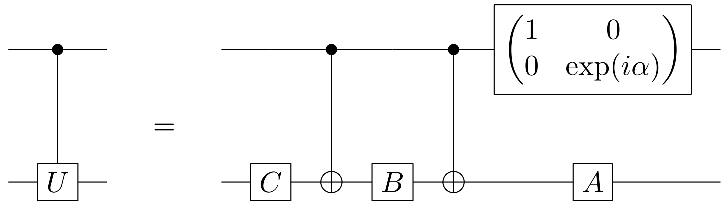
$$\sigma_X B \sigma_X = \sigma_X U(\vec{e}_y,-\frac{\gamma}{2})\sigma_X\sigma_X U(\vec{e}_z,-\frac{\delta+\beta}{2})\sigma_X = U(\vec{e}_y,\frac{\gamma}{2})U(\vec{e}_z,\frac{\delta+\beta}{2}) .$$

Hence

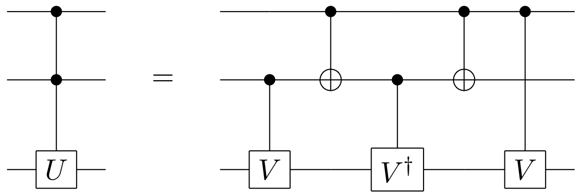
$$A\sigma_X B\sigma_X C = U(\vec{e}_z,\beta)U(\vec{e}_y,\frac{\gamma}{2})U(\vec{e}_y,\frac{\gamma}{2})U(\vec{e}_z,\frac{\delta+\beta}{2})U(\vec{e}_z,\frac{\delta-\beta}{2}) = U(\vec{e}_z,\beta)U(\vec{e}_y,\gamma)U(\vec{e}_z,\delta) .$$

By Lemma 1 this concludes the proof.

By Lemma 2 a controlled-U gate can now be implemented as follows:

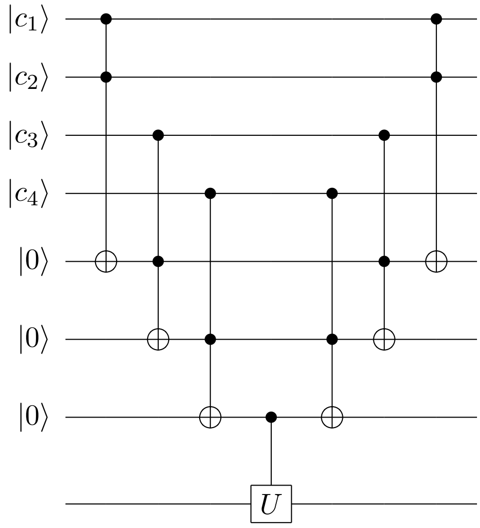


For any $V \in U(2)$ with $V^2 = U$, the circuit



does the job.[1]

A controlled-U gate with 4 control qubits, can now be implemented as follows:



The generalization to a controlled-U gate with n control qubits is then straightforward.

Exercise 2) Representations of SU(2)

We first check that the exponential map is surjective. In the Bloch sphere representation every pure state can be represented as Bloch vector on the Bloch sphere S^2. Since every $g \in SU(2)$ takes pure states to pure states, it takes Bloch vectors to Bloch vectors. Thus every $g \in SU(2)$ corresponds to a rotation on the Bloch sphere. But by exercise 1 on problem sheet 2, rotations on the Bloch sphere correspond to $U(\vec{e}, \alpha) = \exp(-i\frac{\alpha}{2}\vec{e}\cdot\vec{\sigma})$. Hence we can write every $g \in SU(2)$ as $g = \exp(ia)$ for some $a \in su(2)$.

The Baker-Campbell-Hausdorff formula together with the defining property of a Lie Algebra

[1] That such a V exists can be seen as follows. Since U is unitary, we can write $U = WDW^\dagger$ with W and $D = \mathrm{diag}(\lambda_1, \lambda_2)$ unitary, where $\lambda_1, \lambda_2 \in \mathbb{C}$. Now choose $V = W\sqrt{D}W^\dagger$.

representation give us

$$\begin{aligned}
V_k(g \cdot h) &= V_k(\exp(ia) \cdot \exp(ib)) \\
&= V_k(\exp(ia + ib + \frac{1}{2}[ia, ib] + \frac{1}{12}([ia, [ia, ib]] - [ib, [ia, ib]]) + \ldots)) \\
&= \exp(iv_k(a) + iv_k(b) - \frac{1}{2}v_k([a, b]) + \frac{i}{12}v_k([b, [a, b]] - [a, [a, b]]) + \ldots) \\
&= \exp(iv_k(a) + iv_k(b) - \frac{1}{2}[v_k(a), v_k(b)] + \ldots) \\
&= \exp(iv_k(a)) \cdot \exp(iv_k(b)) = V_k(\exp(ia)) \cdot V_k(\exp(ib)) = V_k(g) \cdot V_k(h) \ .
\end{aligned}$$

We take

$$\exp(iv_k(b)) = V_k(\exp(ib)) \tag{3}$$

as an implicit definition for $v_k(b)$ given a representation V_k of $SU(2)$. To see that the formula from the exercise sheet follows from that, we have a look at $\exp(iv_k(ta)) = V_k(\exp(ita))$ with $t \in \mathbb{R}$. We have

$$\exp(iv_k(ta)) = V_k(\exp(ita)) = (V_k(\exp(ia)))^t = (\exp(iv_k(a)))^t = \exp(itv_k(a)) \ , \tag{4}$$

and so by differentiating $\exp(itv_k(a)) = V_k(\exp(ita))$ with respect to t, multiplying it with $(-i)$ and setting $t = 0$ we get

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

Note that (4) shows $v_k(ta) = tv_k(a)$.

Using definition (3) we can also show that $v_k(a + b) = v_k(a) + v_k(b)$. For this we use the Zassenhaus formula (which is the converse of the Baker-Campbell-Hausdorff formula):

$$\exp(t(a + b)) = \exp(ta) \cdot \exp(tb) \cdot \exp(-\frac{t^2}{2}[a, b]) \cdot \exp(\frac{t^3}{6}([a, [a, b]] + 2[b, [a, b]])) \cdot \ldots \ .$$

We calculate

$$\begin{aligned}
\exp(itv_k(a + b)) &= \exp(iv_k(t(a + b))) = V_k(\exp(it(a + b))) \\
&= V_k(\exp(ita) \cdot \exp(itb) \cdot \exp(-\frac{t^2}{2}[ia, ib]) \cdot \ldots) \\
&= V_k(\exp(ita)) \cdot V_k(\exp(itb)) \cdot V_k(\exp(\frac{t^2}{2}[a, b])) \cdot \ldots \\
&= \exp(iv_k(ta)) \cdot \exp(iv_k(tb)) \cdot \exp(v_k(\frac{t^2}{2}[a, b])) \cdot \ldots \\
&= \exp(itv_k(a)) \cdot \exp(itv_k(b)) \cdot \exp(\frac{t^2}{2}v_k([a, b])) \cdot \ldots \ .
\end{aligned}$$

Taking Taylor expansions of the exponential functions gives us for the first order in t that $v_k(a + b) = v_k(a) + v_k(b)$.

Now we continue by reading off the second order in t:

$$-\frac{1}{2}v_k(a + b)v_k(a + b) = -\frac{1}{2}v_k(a)v_k(a) - \frac{1}{2}v_k(b)v_k(b) - v_k(a)v_k(b) + \frac{1}{2}v_k([a, b]) \ .$$

But this is $[v_k(a), v_k(b)] = v_k([a, b])$.