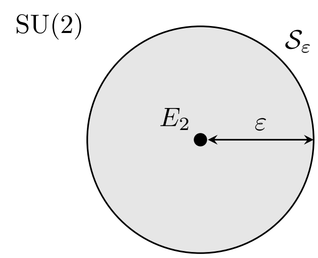
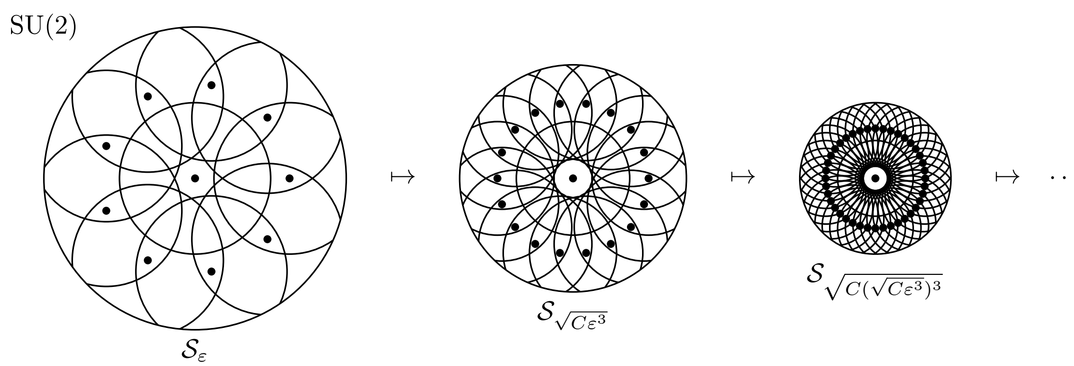
Consider the following question: Given a finite set of 1-qubit-gates, how fast can we approximate an arbitrary 1-qubit-gate? A fundamental result is that a fast approximation is generally possible, as is established by the Solovay-Kitaev Theorem. In this note, we study a part of the proof following the version from Nielsen and Chuang and make some of the arguments more precise.

The first reduction to make is to only consider SU(2). Due to the decomposition theorem of operators in U(2) into products of operators from SU(2) [1, p. 176], this suffices. We shall recall that approximating general quantum gates is a hard problem [1, pp. 198-200], as it can be shown that there are multi-qubit-gates, for which the complexity of approximation is exponentially lower bounded by the number of qubits. Since we are restricting ourselves to one qubit only however, this fact does not pose an issue.

Let $\mathcal{G} \subseteq \mathrm{SU}(2)$ be a finite set, closed wrt. inverses meaning adjoints, s.t. $\langle \mathcal{G} \rangle$ is dense in SU(2) wrt. the trace distance $d_{\mathrm{tr}}(A, B) = \mathrm{tr}(|A - B|) = \mathrm{tr}(\sqrt{(A-B)^\dagger (A-B)})$. Generally we may include E_2 into $\mathcal{G}$ to have a subgroup, but it suffices to leave it. Using the trace distance suffices as all norms in finite-dimensional spaces are equivalent. Let $\mathcal{S}_\varepsilon := d_{\mathrm{tr}}(\cdot, E_2)^{-1}([0, \varepsilon])$.



Lemma 1 ([1, pp. 619-623]). There exists a universal constant $\varepsilon_0 \in \mathbb{R}_{>0}$, independent of $\mathcal{G}$, s.t. for any $\varepsilon \in \mathbb{R}$, $\varepsilon \leq \varepsilon_0$, if $\mathcal{G}^{\cdot \ell}$ with $\ell \in \mathbb{N}$ is an ε^2-net for $\mathcal{S}_\varepsilon \subseteq \mathrm{SU}(2)$, then $\mathcal{G}^{\cdot (5\ell)}$ is a $C\varepsilon^3$-net for $\mathcal{S}_{\sqrt{C\varepsilon^3}}$, where $C \in \mathbb{R}_{>1}$, $C \in \mathcal{O}(1)$.



Theorem 2 (Solovay-Kitaev Theorem [1, pp. 618-620])**.** For any $\varepsilon \in \mathbb{R}_{>0}$, there exists an $\ell \in \mathbb{N}$, $\ell \in \mathcal{O}(\log_2^c(1/(C^2\varepsilon)))$ with $c \in \mathbb{R}_{>0}$, $c \in \mathcal{O}(1)$ a universal constant, s.t. $\mathcal{G}^{\cdot \ell}$ is an ε-net of SU(2).

Proof. The first step is to prove that we can take an initial net and make it successively smaller with exponential speed. Take an arbitrary $\varepsilon'_0 \in (0, 1)$ with just $\varepsilon'_0 \leq \varepsilon_0$ for now. $\langle \mathcal{G} \rangle$ is dense in SU(2), so there is an ε'^2_0-net of $S_{\varepsilon'_0}$ by the following topological argument.

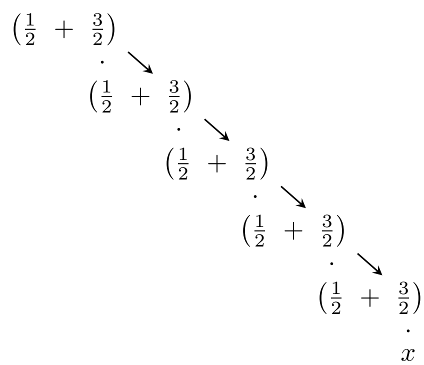
Since the determinant map $\det\colon \mathbb{C}^{2\times 2} \to \mathbb{C}$ is continuous as a polynomial and $\mathrm{SU}(2) = \det^{-1}(\{1\})$, SU(2) is closed in $\mathbb{C}^{2\times 2}$. The matrices being unitary gives the boundedness of $\mathrm{SU}(2) \subseteq \mathbb{C}^{2\times 2} \cong \mathbb{R}^8$. Applying the Heine-Borel theorem gives the compactness of SU(2). To obtain an $\varepsilon_0'^2$-net for SU(2) and thus $\mathcal{S}_{\varepsilon_0'}$, choose for any $U \in \mathrm{SU}(2)$ a $V_U^{\ell_U} \in \mathcal{G}^{\cdot \ell_U} \subseteq \langle \mathcal{G} \rangle$ with $\ell_U \in \mathbb{N}$, s.t. $\|U - V_U^{\ell_U}\| < \varepsilon_0'^2$. Then $\{V_U^{\ell_U}\}_{U\in \mathrm{SU}(2)}$ is an open cover, so choose a finite cover $\{V_1^{\ell_1}, ..., V_n^{\ell_n}\}$ with $n \in \mathbb{N}_{\geq 1}$ and select $\ell_0 := \max\{\ell_1, ..., \ell_n\}$. We can do this analogously for $\mathbb{S}_{\varepsilon_0'}$ to obtain a different ℓ_0 value and take the maximum.

Apply the theorem on $\mathcal{G}^{\cdot \ell_0}$ to obtain a $C\varepsilon_0'^3$-net of $S_{\sqrt{C\varepsilon_0'^3}}$. Iterating k-times, $k \in \mathbb{N}_{\geq 1}$, we obtain some ε_k, which corresponds to applying the map $\varepsilon \mapsto C^{1/2}\varepsilon^{3/2}$ exactly k times on ε_0'. Looking at the exponents and considering $\varepsilon_0' = C^0 \varepsilon_0'^1$, we can alternatively consider the exponents as pairs and look at k applications of the map $(x, y) \mapsto (1/2 + (3/2)x, (3/2)y)$ with initial values $(x, y) = (0, 1)$. For the first component we thus have the geometric sum

$$\frac{1}{2} + \frac{3}{2}\left(\frac{1}{2} + \frac{3}{2}\left(... \left(\frac{1}{2} + \frac{3}{2}x\right) ...\right)\right) = \frac{1}{2} + \frac{3}{4} + \frac{9}{8} + \frac{27}{16} + \frac{81}{32} + ... + \frac{3^{k-1}}{2^k} + \frac{3^k}{2^k}x \tag{1}$$

$$= \frac{1}{3}\sum_{k'=0}^{k}\left(\frac{3}{2}\right)^{k'} - \frac{1}{3} + \left(\frac{3}{2}\right)^{k} x = \left(\frac{3}{2}\right)^{k}(x+1) - 1 \tag{2}$$

for which the derivation may be visualized the following way. In other words, $\varepsilon_k = (C\varepsilon_0')^{((3/2)^k)}/C$ and



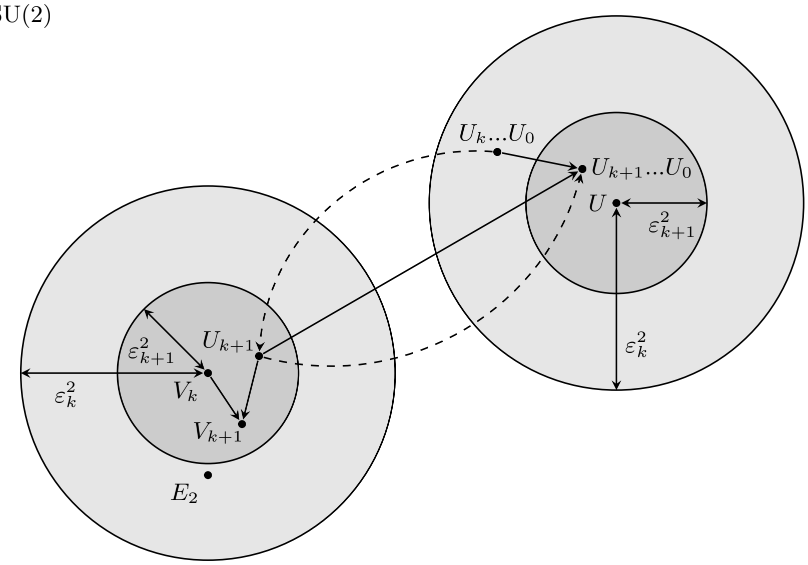
$\mathcal{G}^{\cdot 2^k \ell_0}$ is a ε_k^2-net of $\mathcal{S}_{\varepsilon_k}$. Now assume $C\varepsilon_0' \in (0, 1)$ to make the nets smaller with each increase of k. Thus $\varepsilon_k \to_{k\to\infty} 0$ under exponential decline. For the following, we want $\varepsilon_k^2 < \varepsilon_{k+1}$ and the direct computation gives $\varepsilon_0' \in (0, C)$ as a sufficient condition, so wlog. assume that.

We now find an ℓ as claimed by using the construction of nets from above. Let $U \in \mathrm{SU}(2)$ be arbitrary, but fixed and take a $\varepsilon_0'^2$-approximation of U, denoted $U_0 \in \mathcal{G}^{\cdot \ell_0}$. Set $V_0 := UU_0^\dagger$. Then

$$d_{\mathrm{tr}}(V_0, E_2) = \mathrm{tr}\,|(U - U_0)U_0^\dagger| = \mathrm{tr}\,|U_0(U - U_0)U_0^\dagger| = \mathrm{tr}\,|U - U_0| = d_{\mathrm{tr}}(U, U_0) \leq \varepsilon_0^2 < \varepsilon_1 \tag{3}$$

Establishing $V_0 \in \mathcal{S}_{\varepsilon_1}$. By construction, $\mathcal{G}^{\cdot(5\ell_0)}$ is a ε_1^2-net of $\mathcal{S}_{\varepsilon_1}$, so take an ε_1^2-approximation $U_1 \in \mathcal{G}^{\cdot(5\ell_0)}$ of V_0 and set $V_1 := V_0 U_1^\dagger$. The same argument as before gives $d_{\mathrm{tr}}(V_1, E_2) = d_{\mathrm{tr}}(U, U_1 U_0) \leq \varepsilon_1^2 < \varepsilon_2$. We iterate this procedure to obtain for any $k \in \mathbb{N}_{\geq 1}$ a unitary $U_k U_{k-1} ... U_0$ with $U_i \in \mathcal{G}^{\cdot(5^i \ell_0)}$ for every $i \in [0, k]_{\mathbb{N}}$, which is a ε_k^2-approximation of U.

SU(2)



We used the following properties of the trace from [1, p. 75] here: Consider that the trace tr is *additive* and *cyclic*, in the sense that

$$\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B) \text{ and } \operatorname{tr}(AB) = \operatorname{tr}(BA) \tag{4}$$

for any $A, B \in \mathbb{C}^{n\times n}$, $n \in \mathbb{N}_{\geq 1}$. Thus the trace is perserved under unitary transformations, meaning that for any $U \in U(n)$,

$$\operatorname{tr}\big(UAU^\dagger\big) = \operatorname{tr}\big(U^\dagger UA\big) = \operatorname{tr}(A) \tag{5}$$

is fulfilled.

We require a total of $\sum_{i=0}^{k} 5^i \ell_0 = \frac{5^{k+1}-1}{4}\ell_0 < 5/4 \cdot 5^k \ell_0$ gates. To approximate with a precision of ε, we use the Ansatz $\varepsilon_k^2 < \varepsilon$ and conclude

$$\left(\frac{3}{2}\right)^k > \frac{1}{2}\frac{\log_2(C^2\varepsilon)}{\log_2(C\varepsilon_0')} \tag{6}$$

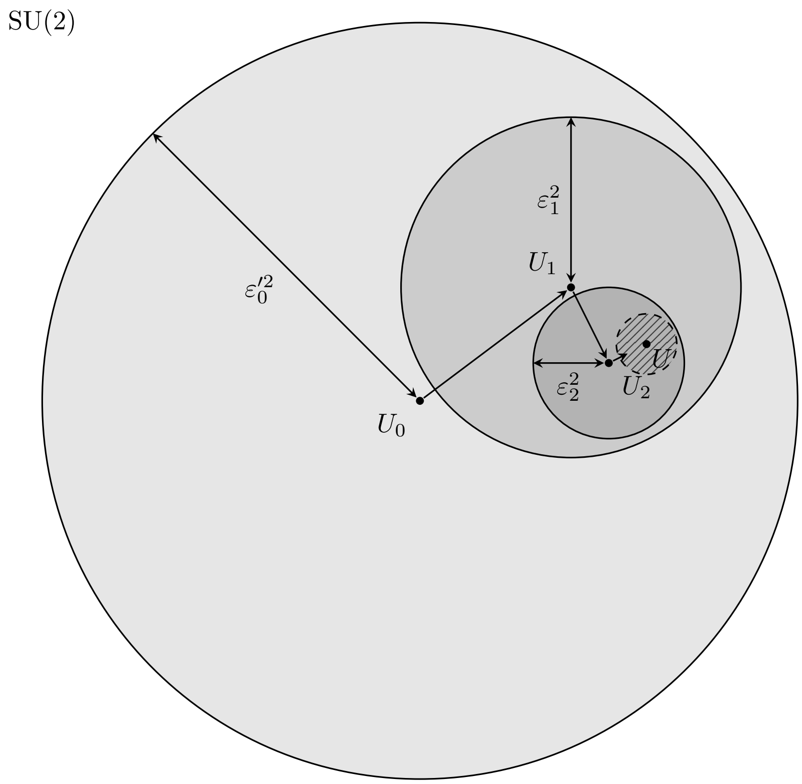
where we wlog. assume $C^2\varepsilon \in (0,1)$. Set $c \coloneqq \log_{3/2}(5) = \log_2(5)/\log_2(3/2)$ and obtain a gate count of

$$\frac{5}{4}5^k\ell_0 = \frac{5}{4}\left(\frac{3}{2}\right)^{ck}\ell_0 \leq \frac{5}{4}\frac{1}{2^c}\frac{\log_2^c(C^2\varepsilon)}{\log_2^c(C\varepsilon_0')}\ell_0 \in \Theta(\log_2^c(1/(C^2\varepsilon))) \tag{7}$$

where we omit any rounding to a next number k sufficing the construction, proving the Solovay-Kitaev Theorem. ■

References

[1] A. N. Michael and L. C. Isaac, *Quantum Computation and Quantum Information*, ISBN: 9781107002173.


SU(2)
$\varepsilon_0'^2$
ε_1^2
U_1
U_0
ε_2^2
U_2
U