# Exercise 6: Solovay-Kitaev, Deutsch-Jozsa, and RSA

1. In the lecture you proved the Solovay-Kitaev theorem up-to a claim, which we'll prove here:

   **Claim 6.1**

   *Let $A$ be a traceless $d$-dimensional Hermitian operator. Then there are $B, C$ Hermitian operators such that $[B, C] = iA$ and $\|B\|, \|C\| \leq \sqrt[4]{d}\sqrt{\frac{d-1}{2}}\sqrt{\|A\|}$.*

   We will be working in a basis which is Fourier-conjugate to to $H$'s eigenbasis: Let $W_d$ be the normalised $d$ dimensional Vandermonde matrix, i.e. $(W_d)_{j,k} = \frac{\omega^{jk}}{d}$ for $\omega = e^{i2\pi/d}$ a primitive $d$'th root of unity. In our basis, $H$ is represented by the matrix $W_d diag(\lambda_1, \ldots, \lambda_d) W_d^\dagger$ for the $d$ eigenvalues (possible with some repeated ones) $\lambda_i \in \mathbb{R}$.

   (a) Show that in our basis the diagonal entries of $H$ are all 0.

   (b) Assume the $C$ we construct is a diagonal matrix. Calculate the requirement $[B, C] = iA$ for each entry $j, k$ and use this and the previous subquestion to define $B$'s entries using $A$'s and $C$'s entries. You may assume $C$'s diagonal has no repeated values. Confirm you defined a Hermitian $B$.

   (c) Set the diagonal of $C$ to be $-\frac{d-1}{2} + i$ for $i \in \{0, \ldots, d-1\}$. Show that this implies that $|B_{j,k}| \leq |A_{j,k}|$ for all $j, k \in [d]$.

   (d) Show $\|B\|^2 \leq d\|A\|^2$.
   *hint: look at traces of squared operators and use the fact these are Hermitian.*

   (e) Rescale $B, C$ to get to the final operators that satisfy both requirements and show we're done.

2. Here we will see a similar result to the ones you saw in the lecture: Deutsch-Jozsa.

   In the oracle/black-box model we are given a function $f : \{0,1\}^n \to \{0,1\}$ that is promised to either be balanced or constant, i.e. either $\forall x, y \in \{0,1\}^n : f(x) = f(y)$ or $|f^{-1}(0)| = |f^{-1}(1)|$.

(a) Find the classical deterministic query-complexity of this problem, i.e. find a function $T(n)$ and show both a deterministic classical algorithm that uses at most $T(n)$ queries and that no deterministic classical algorithm can use less than that.

(b) Quantum advantage: Find a quantum algorithm that uses exactly one query and answers guesses correctly with certainty.

*hint: Sometimes this algorithm is taught after Deutsch's algorithm and before Bernstein-Vazirani's algorithm.*

(c) Weakness of this advantage: Argue that a probabilistic classical algorithm that is allowed to err with some constant probability (say 1/3) can also use a constant number of queries.

3. RSA: Alice generates a public key and a private key that allows Bob to send an encripted message which she can decript, while others need to factor a number to do so.

Keys: Her public key includes $N = p \cdot q$ for prime numbers $p, q$ and $e$ that is coprime to $\Phi(N)$ (she can draw a number and divide by the $GCD$ with $\Phi(N)$) and her private key is $p, q$.

Encription: When Bob wants to send the message $a \in [N-1]$, he sends $b := a^e \pmod N$.

Decription: When Alice wants to read Bob's message she calculates $b^d \equiv a \pmod N$ for $de \equiv 1 \pmod{\Phi(N)}$.

(a) What is $\Phi(N)$? How can Alice know it?

(b) Show how Euclid's algorithm allows Alice to calculate $d$ efficiently.

(c) Show that indeed $b^d = a^{de} \equiv a \pmod N$.

*hint: use lagrange's theorem or the Chinese remainder theorem together with Euler's theorem.*

(d) How could Eve, who already knows the public key $N, e$ and the encripted message $b$, learn the message itself $a$ if she could factor any number to its prime factors?