[P9] (Approximating circuits). The definition of the quantum Fourier transform involves the gates

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi \mathrm{i} 2^{-k}} \end{bmatrix}$$

which differ from the trivial time evolution (given by the identity matrix) only by an *exponentially small* quantity $1-e^{2\pi \mathrm{i} 2^{-k}}$. This might be a source of concern: does a quantum algorithm require exponentially precise control? Here, we will show that this is not the case: small errors in the gates will lead only to small differences in the success probability of the algorithm. (And hence *leaving out* the R_k's for large k does not significantly alter the QFT circuit).

(1) Recall the *operator norm* of a matrix A is

$$\|A\|_\infty = \max_\phi \|A|\phi\rangle\| = \max_{\phi,\psi} \langle\psi|A|\phi\rangle,$$

where the respective maximizations are over *normalized* vectors $\|\phi\| = \|\psi\| = 1$. Show that the operator norm satisfies the *triangle inequlaity* $\|A+B\|_\infty \leq \|A\|_\infty + \|B\|_\infty$. Show that the operator norm is *unitarily invariant*: if U is a unitary, then $\|AU\|_\infty = \|UA\|_\infty = \|A\|_\infty$.

(2) Let U_1, U_2 be two ideal quantum gates. Suppose we manage to engineer V_1, V_2, which are close to the U's in the sense that $\|U_i - V_i\|_\infty \leq \epsilon$. Using the two properties established above, show that

$$\|U_2 U_1 - V_2 V_1\|_\infty \leq 2\epsilon.$$

(Of course, by induction, this implies that if a circuit consists of n gates U_i realized to within precision ϵ each, then the total error of the circuit will not exceed $n\epsilon$.)

(3) Lastly, let A be the observable used to read out the result of the computation. We assume that $\|A\|_\infty = 1$ (optional problem: convince yourself that that's true for all examples we have looked at so far). If $|\psi\rangle$ is the initial state of the computation, U the ideal unitary of the circuit, V our approximation to it, then the read-out error is

$$\left| \mathrm{tr} AU|\psi\rangle\langle\psi|U^\dagger - \mathrm{tr} AV|\psi\rangle\langle\psi|V^\dagger \right|.$$

Prove that this error is no larger than $2\|U - V\|_\infty$. (5 P.)

[P10] In order to understand the quantum factoring algorithm and the RSA public key cryptosystem (the one supposedly making the Internet secure), we'll need to look at some basic number theory. All variables used in this exercise $(a, b, x, N, r, \ldots)$ will be assumed to be integers. Let N be positive. Then it's easy to see that every x is uniquely of the form

$$x = kN + r,$$

where $r \in [0, N-1]$ is the *remainder* obtained when dividing x by N. In the situation above, we say that "x is congruent to r modulo N", or "$x = r \pmod N$".

In the lecture, we'll treat *Euclid's algorithm*. Among other things, it achieves the following: given a, b, Euclid's algorithm can efficiently compute x, y such that

$$ax + by = \gcd(a, b),$$

where $\gcd(a, b)$ is the greatest common divisor of a and b. Two integers a, b are *co-prime* if $\gcd(a, b) = 1$.

(1) Use the above presentation of $\gcd(a, b)$ to show that if a and b are co-prime, then there is an integer a^{-1} such that $aa^{-1} = 1 \pmod{b}$. (This number is called the *multiplicative inverse* of a modulo b). Show that $\gcd(a, b) = 1$ is also necessary for a multiplicative inverse of a modulo b to exist.

(2) Let p be a prime number. Show that, for all $k \in [1, p-1]$, it holds that

$$\binom{p}{k} = 0 \pmod{p}.$$

(3) (Fermat's Little Theorem). Let p be prime and a be any integer. Show that

$$a^p = a \pmod{p}.$$

(Hint: Prove the claim by induction. For the induction step $a \to (a+1)$, use the previous result). Use (1) to show that if, moreover, a is not divisible by p, then $a^{p-1} = 1 \pmod{p}$.

(5 P.)