# CS 593/MA 592 - Intro to Quantum Computation
# Homework 7

Due Friday, April 5 at 8pm (upload to Brightspace)

1. In this problem, you'll prove the two mathematical facts we needed to know in order for Simon's algorithm to work.

   (a) Let $A$ be a finite abelian group. Prove that if $g_1, \dots, g_l$ are $l$ independently and uniformly randomly chosen elements of $A$, then the probability that $\langle g_1, g_2, \dots, g_l \rangle = A$ is at least $1 - \frac{|A|}{2^l}$. [Hint: as an intermediate step, you might use Lagrange's theorem to argue that the probability that $g_{i+1} \notin \langle g_1, \dots, g_i \rangle$ is at least $1/2$ whenever $\langle g_1, \dots, g_i \rangle \neq A$.]

   (b) Let $A = (\mathbb{Z}/2\mathbb{Z})^n$ be an $n$ dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$. Let $s \in A$ be a non-zero element and suppose $g_1, \dots, g_l \in A$ generate what I called $\langle s \rangle^\perp$, which is defined as

   $$\langle s \rangle^\perp = \{a \in A \mid a \cdot s = 0 \mod 2\},$$

   where $a \cdot s$ is the mod 2 dot product of $a = (a_1, \dots, a_n)$ and $s = (s_1, \dots, s_n)$. Prove that $s$ is the unique non-zero solution to the system of equations

   $$\begin{aligned} g_1 \cdot x &= 0 \mod 2 \\ g_2 \cdot x &= 0 \mod 2 \\ &\vdots \\ g_l \cdot x &= 0 \mod 2 \end{aligned}$$

2. List all of the numbers $1 \leq x \leq 100$ such that Shor's factoring algorithm actually needs to use a quantum computer in order to find a factor.

3. Do Exercise A4.17 in Nielsen and Chuang.

4. Do Exercise 5.13 in Nielsen and Chuang.

5. Do Exercise 5.16 in Nielsen and Chuang.

6. Do Exercise 5.17 in Nielsen and Chuang.