Introduction to Quantum Information Science
Homework 9

Due Wednesday, November 12 at 11:59 PM

Note: You should explain your reasoning, i.e. show your work, for all problems. You do not need to show us every step of each calculation, but every answer should include an explanation *written with words* of what you did.

1. Toffoli-based Addition [6 Points] Work out an explicit circuit of Toffoli gates for adding two 2-bit integers to get a 3-bit integer — assume the integers are unsigned, encoded in binary in the usual, simplest way. You can use arbitrary ancilla bits initialized to 0 or 1. Be sure to designate your input, output, and garbage registers.
Show the garbage bits that are generated by your circuit when 11 is added to 10.

2. The Quantum Fourier Transform [9 points] The Quantum Fourier Transform QFT_d is a quantum gate acting on *qudits*, i.e. quantum systems with d levels. It is defined below for $x, y \in \{0, 1, ..., d-1\}$.

$$QFT_d |x\rangle = \frac{1}{\sqrt{d}} \sum_{y=0}^{d-1} \omega^{xy} |y\rangle$$

where $\omega = e^{2\pi i/d}$ is a primitive dth root of unity.

To be clear, a qudit is just like a qubit but it's a vector of d amplitudes instead of just 2 amplitudes. Then, a unitary acting on a qudit has dimension $d \times d$.

a) [3 Points] Calculate QFT_2, QFT_3, and QFT_4 explicitly (either by writing down the corresponding matrix or equivalently by specifying the action on each of the standard basis states). By what other name is QFT_2 known?

b) [3 Points] Prove that QFT_d is unitary for all d.

c) [3 Points] For which values of d is QFT_d its own inverse?

d) [Extra Credit, 3 Points] In Recitation 4, we saw that the qudit clock and shift matrices are respectively defined as $X_d |x\rangle = |x + 1 \bmod d\rangle$ and $Z_d |x\rangle = \omega^x |x\rangle$ for $x \in 0, 1, \ldots, d-1$. Show that

$$QFT_d^\dagger X_d QFT_d = Z_d^\dagger.$$

3. RSA [5 points] Two spies of an enemy nation are known to use the RSA crypto-system with public keys

$$N = 4668619 \quad \text{and} \quad e = 3.$$

And intelligence has revealed that

$$\varphi(N) = 4664296.$$

Now we've intercepted a message sent between the two spies showing that they intend to meet at a certain time:

$$m = 1202997$$

Let's arrange for them (our enemies) to miss each other by an hour.

[Note that decrypted messages are encoded in ASCII with two ***decimal*** *digits per character, as described on* `www.asciitable.com`*. You're of course free to use computer help.* `www.dcode.fr/modular-exponentiation` *and* `www.dcode.fr/ascii-code` *may prove useful. But please don't forget to show intermediate steps in the solutions.]*

a) [2 Points] Confirm that our intelligence is correct by using N and $\varphi(N)$ to determine the two factors p and q of N and checking that indeed $pq = N$. (Note that part (a) is not required in the parts that follow.)

b) [1 Point] Meanwhile an analyst has gone ahead and done the work of determining

$$d = 3109531$$

to be the inverse of e in the multiplicative group $\mathbb{Z}^{\times}_{\varphi(N)}$. Verify that this is correct.

c) [1 Point] Decrypt the given message.

d) [1 Point] Encrypt a new message in the same format instructing to meet an hour later; we will send this to the second spy instead of the original message.

4. Factoring [5 points] Let $N = pq$ be a product of two large primes. Show that given the order $(p-1)(q-1)$ of the multiplicative group $\pmod N$, one can efficiently recover the prime factors of N.