

ET4340 Electronics for Quantum Computing

Homework 4

Mick van Gelderen
4091566

November 2013

Problem 1: Quantum Fourier Transform

1. Write the 8×8 matrix (in the computational basis) corresponding to the quantum Fourier transform on a 3-qubit register.

The matrix $U_{QFT,8}$ is defined as:

$$U_{QFT,8} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{k=0}^{N-1} e^{\frac{i2\pi lk}{N}} |l\rangle \langle k|$$

where $N = 8$.

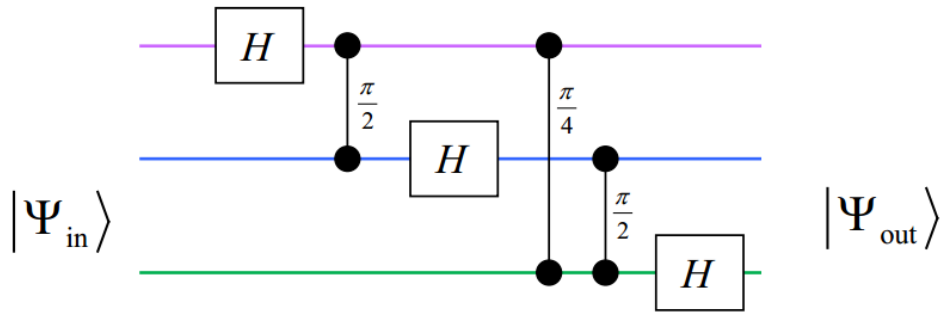
$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \sqrt{2} + \sqrt{2}i & i & -\sqrt{2} + \sqrt{2}i & -1 & -\sqrt{2} - \sqrt{2}i & -i & \sqrt{2} - \sqrt{2}i \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & -\sqrt{2} + \sqrt{2}i & -i & \sqrt{2} + \sqrt{2}i & -1 & \sqrt{2} - \sqrt{2}i & i & -\sqrt{2} - \sqrt{2}i \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\sqrt{2} - \sqrt{2}i & i & \sqrt{2} - \sqrt{2}i & -1 & \sqrt{2} + \sqrt{2}i & -i & -\sqrt{2} + \sqrt{2}i \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & \sqrt{2} - \sqrt{2}i & -i & -\sqrt{2} - \sqrt{2}i & -1 & -\sqrt{2} + \sqrt{2}i & i & \sqrt{2} + \sqrt{2}i \end{pmatrix}$$

2. Show that this matrix is unitary

Use a computer to calculate $U_{QFT}U_{QFT} = I$. You can easily see that the matrix is symmetric so this is the only thing we have to show. Matlab indeed gives I with some near zero imaginary parts.

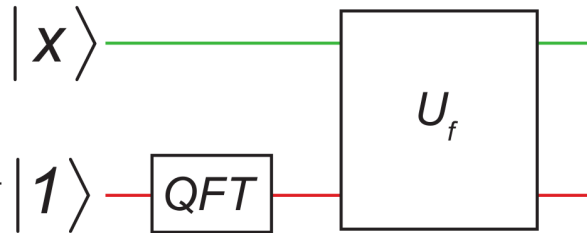
3. Draw the quantum circuit that implements this QFT

From the lecture slides where it was drawn for 4 qubits:



Problem 2: Generalized quantum kick-back

In the lectures, we have seen how the Deutsch and Bernstein-Vazirani quantum games exploit quantum kick-back to efficiently extract properties of n -to-1 bit boolean functions. In this problem, we generalize quantum kick-back to n -to- m bit boolean functions encoded in unitary functions as usual: $U_f |x\rangle |y\rangle = |x\rangle |(y + f(x)) \bmod M\rangle$ for computational states $|x\rangle$ and $|y\rangle$ in the top and bottom registers, respectively. Consider the circuit below.



1. What is the state of the bottom register after application of the m -bit QFT on the initial state $|1\rangle = |00000\dots 1\rangle$?

$$U_{QFT} |1\rangle \text{ equals the last column of } U_{QFT}. \text{ So } U_{QFT} |1\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{i2\pi(N-1)k}{N}} |k\rangle$$

2. Now apply U_f , with the top register starting in a computational state $|x\rangle$. What is the combined state of the top and bottom registers immediately after U_f ? Show that this state can be rewritten as:

$$e^{\frac{-i2\pi f(x)}{M}} |x\rangle \otimes U_{QFT} |1\rangle,$$

where $M = 2^m$. Evidently, the top and bottom registers are not entangled, and $f(x)$ is encoded in the quantum phase of the probability amplitude!

?

- Finally, consider the case that the top register is initialized in the maximal superposition state $\frac{1}{\sqrt{N}}(|0\rangle + \dots + |N-1\rangle)$. As usual, $N = 2^n$. What will be the final state after application of U_f ?

?

Problem 3: Breaking RSA In this exercise, we will break RSA by period finding. N will be small enough that we will find periods by brute force.

- List the integers $a < N$ that are co-prime with N . Let us pick one of these integers: let us agree to all ‘randomly’ pick $a = 8$.

	n	divisible by	co-primes
I guess $N = 21$.	2	2	1
	3	3	1 2
	4	2 4	1 3
	5	5	1 2 3 4
	6	2 3 6	1 5
	7	7	1 2 3 4 5 6
	8	2 4 8	1 3 5 7
	9	3 9	1 2 4 5 7 8
	10	2 5 10	1 3 7 9
	11	11	1 2 3 4 5 6 7 8 9 10
	12	2 3 4 6 12	1 5 7 11
	13	13	1 2 3 4 5 6 7 8 9 10 11 12
	14	2 7 14	1 3 5 6 9 11 13
	15	3 5 15	1 2 4 7 8 11 13 14
	16	2 4 8 16	1 3 5 7 9 11 13 15
	17	17	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
	18	2 3 6 9 18	1 5 7 11 13 17
	19	19	1 3 5 7 8 9 10 11 12 13 14 15 16 17 18 19
	20	2 4 5 10 20	1 3 7 9 11 13 17 19
	21	3 7 21	1 2 4 5 8 10 11 13 16 17 19

- Compute $8^0 \bmod 21$, $8^1 \bmod 21$, ...until you discover the period r of $f(x) = 8^x \bmod 21$.

n	$8^n \bmod 21$	
0	1	The period seems to be 2.
1	8	
2	1	

- Find the greatest common denominator (gcd) between, $8^{r/2} + 1$ and 21. Check whether the result is a prime factor of 21.

Since $r = 2$, $8^{r/2} + 1 = 9$. The gcd of 9 and 21 is 3 which is indeed a prime factor of 21.

- Similarly, find the gcd between $8^{r/2} - 1$ and 21.

The gcd of 7 and 21 is 7 which is a prime factor of 21.

- Repeat the process for $a = 10$.

	n	$10^n \bmod 21$	
	0	1	
	1	10	
Finding the period:	2	6	The period seems to be 6. The gcd's of $10^3 \pm 1$
	3	13	
	4	4	
	5	19	
	6	1	
and 21 are 3 and 7, magic!			

Problem 4: Breaking RSA with Shor's algorithm

Now we will go through the steps of Shor's algorithm in order to find the period r of $8^x \bmod 21$. For simplicity, let us use just four qubits for the top register which is enough for our choice of $a = 8$. *Note: Please use decimal bra-ket notation instead of binary.*

- Initialize each register to $|0\rangle$.