Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 20 Jan 2021

Tutorial 9 (RSA cryptosystem[1])

Bob wants to send a message to Alice, and they want the message to remain private. One way they can achieve this is by a *public key cryptosystem*. These systems have two main components: a public key P, which Bob uses to encrypt his message, and a secret key S, which is only known by Alice and can be used to decrypt the message. One of these systems is what is known as *RSA cryptosystem*, which works according to the following procedure:

1. Choose two large prime numbers p and q and compute their product $n = pq$.
2. Select at random a small odd integer e which is co-prime to $\varphi(n)$. $\varphi(n)$ is defined to be the number of positive integers less than n which are co-prime[2] to n. In the present setting, $\varphi(n) = (p-1)(q-1)$.
3. Compute d: the multiplicative inverse of e in modular arithmetic of $\varphi(n)$, i.e., $ed = 1 \mod \varphi(n)$.
4. The keys are chosen to be $P = (e, n)$ and $S = (d, n)$.
5. Bob encrypts his message M by
$$E(M) = M^e \mod n.$$
6. Alice decrypts by performing
$$D(E(M)) = E(M)^d \mod n.$$

(a) Assuming that M and n are co-prime, prove that Alice recovers M. It will be helpful to recall Euler's generalization of Fermat's little theorem:

Theorem. *Suppose a is co-prime to n. Then $a^{\varphi(n)} = 1 \mod n$.*

(b) If M is not co-prime to n, p and/or q must be prime factors of M. Assume p is and q isn't and show that Alice again recovers M. The other cases can be treated similarly.

Exercise 9.1 (Phase estimation)

(a) Specify the quantum circuits performing the forward and inverse Fourier transform for vectors of length 2 (i.e., acting on a single qubit), and verify your circuits based on the definition of the Fourier transform.

Hint: Each of your circuits should consist of a single gate.

(b) Let U be a unitary operator with eigenvalues ± 1, which acts on a state $|\psi\rangle$. Using the phase estimation procedure, construct a quantum circuit to collapse $|\psi\rangle$ into one or the other of the two eigenspaces of U, giving also a classical indicator as to which space the final state is in. Compare your result with tutorial 3.

Exercise 9.2 (Order-finding)

Let x and N be positive integers with no common factors and $x < N$. Recall that the *order* of x modulo N is the least positive integer r such that $x^r = 1 \mod N$. We denote the number of bits required to represent N by L. The quantum algorithm for order-finding is the phase estimation algorithm applied to the unitary operator

$$U|y\rangle = \begin{cases} |x \cdot y \mod N\rangle & 0 \le y < N \\ |y\rangle & N \le y < 2^L \end{cases}$$

for $y \in \{0, 1, \dots, 2^L - 1\}$. (Only the case $y < N$ is relevant here.)

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Appendix 5

[2] Two integers a and b are said to be *co-prime* if their greatest common divisor is 1.

(a) We have discussed in the lecture that the states

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \mathrm{e}^{-2\pi i s k/r} |x^k \mod N\rangle \quad \text{for } s = 0, 1, \ldots, r-1$$

are eigenstates of U with corresponding eigenvalues $\mathrm{e}^{2\pi i s/r}$, and that

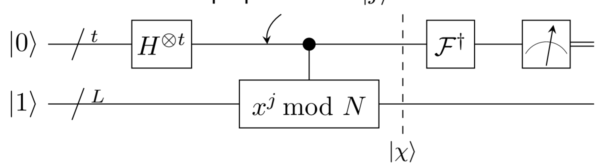
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle. \tag{1}$$

Verify the following generalization of Eq. (1):

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \mathrm{e}^{2\pi i s k/r} |u_s\rangle = |x^k \mod N\rangle \quad \text{for all } k = 0, 1, \ldots, r-1.$$

Hint: Use that $\frac{1}{r} \sum_{s=0}^{r-1} \mathrm{e}^{2\pi i s k/r} = \delta_{0,k \bmod r}$ for all integer k.

Based on Eq. (1), the quantum algorithm for order-finding uses $|1\rangle$ as input in the second register. You should convince yourself that $U^j|1\rangle = |x^j \bmod N\rangle$. This leads to the following schematic circuit:



Thus the quantum state $|\chi\rangle$ before the inverse Fourier transform is

$$|\chi\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |x^j \mod N\rangle.$$

(b) In the following, we set $N = 15$ and $x = 7$. What is the order r of x modulo N? Write down the state $|\chi\rangle$ explicitly for $t = 5$.

The *principle of implicit measurement* states that, without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

(c) Apply this principle by projecting $|\chi\rangle$ from (b) onto one of the (randomly selected) basis states appearing in the second register, say $|4\rangle$: that is, retain only basis states of the form $|j\rangle|4\rangle$ in $|\chi\rangle$, and normalize the resulting state $|\chi'\rangle$ to 1.

(d) Finally, compute the inverse Fourier transform $\mathcal{F}^\dagger|\chi'\rangle$, and plot the probability distribution of the result.

Hint: You can use the following Python code for this purpose, where you still have to insert $|\chi'\rangle$ represented as vector. Because of different conventions, we use NumPy's forward Fourier transform here.

```
import numpy as np
import matplotlib.pyplot as plt

chip = np.array([...])

Fchip = np.fft.fft(chip, norm='ortho')

plt.plot(np.abs(Fchip)**2, '.')
```

The nonzero entries of $\mathcal{F}^\dagger|\chi'\rangle$ should appear at indices ℓ with $\frac{\ell}{2^t} = \frac{s}{r}$ for some $s \in \{0, 1, \ldots, r-1\}$, in accordance with phase estimation.