Outline of the algorithm

Matthew Gregoire

June 2020

1 Overview

1.1 Inputs

1. A modulus N
2. An integer $a \mod N$
3. A power b, where $b = a^m \mod N$

1.2 Outputs

The half-bit of b, with greater than 50% probability.

2 First phase of the algorithm

Let n be the number of bits needed to store any value from 0 to $N-1$. So $n = \lceil N-1 \rceil$. This is what we need to do on the quantum computer:

1. Initialize two quantum registers, each of size n, to the state $|0\rangle |1\rangle$.
2. Apply an n-bit Hadamard to the first register.
3. Apply the operator U_{a^x} to the second register, so that each term in the superposition is of the form $|x\rangle |a^x\rangle$. (We need to figure out how to implement this operator.)
4. Apply the quantum Fourier transform to the first register.
5. Measure the first register to leave it in a particular state $|y\rangle$.

Now calculate the value k by rounding $yr/2^n$, where r is the value such that $a^r = 1 \mod N$. The second register is left in an approximation of the superposition $|\Psi_k\rangle$, needed for the second phase.

3 Second phase of the algorithm

Calculate k^{-1} in $\mod r$ using the extended Euclidean algorithm. We need k to be invertible for the rest to work. Now we'll operate on the number $b' = b^{k^{-1}} \mod N$. On the quantum computer:

1. Initialize a one-qubit register to $|0\rangle$, so that we have the overall state $|\Psi_k\rangle |0\rangle$.
2. Apply a Hadamard to the one-qubit register.
3. Apply a controlled $U_{b'}$ operation to the first register, using the second register as the control bit. (We need to implement this operator as well, by modifying the quantum circuit semi-classically.)
4. Apply a controlled phase shift of $-i$ to the second register, again using the second register as the control.
5. Apply a Hadamard to the second register again.
6. Measure the second register.

The result of this measurement is the output of the "magic box" for the half-bit. Also, we don't disturb the state $|\Psi_k\rangle$ during the second phase, so we can re-use this state later on.

Once we have the half-bit, I'm not sure how we solve the discrete logarithm problem. Blum and Micali's paper will probably go into detail on that, but we can worry about it later because this algorithm is self-contained.