Kit nr 4: Shor's algorithm

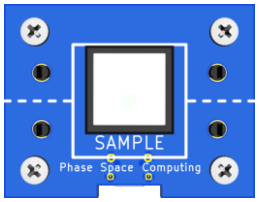
Student Manual

2021-04-26

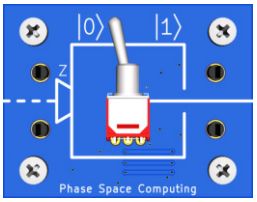
This lab kit contains material to demonstrate the Deutsch-Jozsa quantum algorithm up to three qubit inputs.

You should read through the manual before starting the laboratory work.

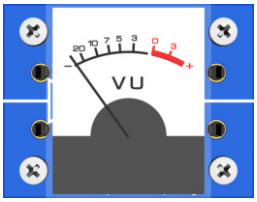
1 Content of the kit



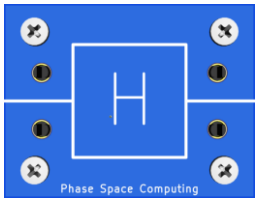
Sample button $\times 1$**:** Resamples the random numbers used in the simulation.



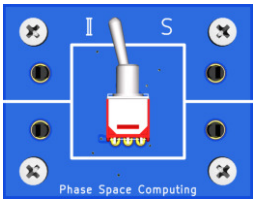
Source $\times 6$**:** component that sends a qubit in one of the computational states $|0\rangle$ or $|1\rangle$ depending on the setting of the switch.



Measurement device $\times 2$**:** Measures the quantum state and displays the result. The reading is $|0\rangle$ if the meter points to the left, and $|1\rangle$ if the meter points to the right (into the red area).

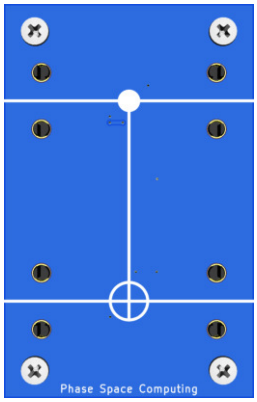


Hadamard gate $\times 4$**:** Transforms states in the $|0\rangle/|1\rangle$ basis to the $|+\rangle/|-\rangle$ basis and vice versa.

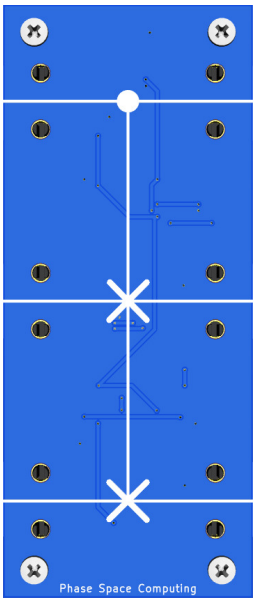


Classically controlled S gate $\times 1$**:** Rotates the state 90° around the computational basis, $|+\rangle \to |+i\rangle \to |-\rangle \to |-i\rangle \to |+\rangle$.

Power cord $\times 1$
Patch cable (7 cm) $\times 10$
Patch cable (30 cm) $\times 5$
Patch cable (150 cm) $\times 2$



CNOT gate (or Controlled NOT gate) $\times 4$**:** the gate operates on two qubits. The second qubit (that goes in the lower part of the component) is called target qubit and is flipped by the gate if and only if the first qubit (the control qubit) is $|1\rangle$.



Fredkin $\times 5$**:** the gate operates on three qubits. The second and third qubits (that goes in the lower part of the component) are called target qubits and are swapped by the gate if and only if the first qubit (the control qubit) is $|1\rangle$.

2 Required reading on Shor's Quantum Algorithm

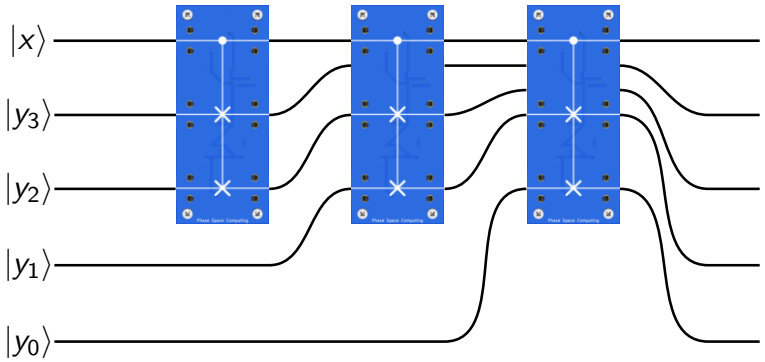
Read Sections 5.1–5.3 of M. A. Nielsen and I. L. Chuang (2010). *Quantum Computation and Quantum Information*. Vol. 10th Anniversary Edition. Cambridge University Press. ISBN: 978-1-107-00217-3.

3 Preparatory excercises

1. Let $f(y) = 2y \bmod 3$. Write down the explicit input-output map for f in a table. Verify (theoretically) that a SWAP gate gives f. Hint: $0 \equiv 3 \bmod 3$.

2. Verify (theoretically) that the Fredkin gate corresponds to a controlled-f (with f as in Exercise 1), usually written $f_x(y) = 2^x y \bmod 3$, when using the first qubit as control bit x and the last two qubits as a two-bit target register y.

3. What controlled function $f_x(y)$ does the below gate array correspond to (y_i are the bits of y in binary, x is a bit)? Hint: write down the input-output map and try to find the pattern, considering that $f_x(0) = 0$ and $f_x(15) = 15$.



4. Construct a gate array for the function $f_x(y) = 4^x y \bmod 15$, for a single control bit x. Use as few Fredkin gates as possible.

5. Construct a gate array for the function $f_x(y) = 8^x y \bmod 15$, for a single control bit x. Hint: $2 \times 8 = 16 \equiv 1 \bmod 15$.

6. Construct a gate array for the function $f_x(y) = (-1)^x y \bmod 15$. Hint: $0 \equiv 15 \bmod 15$.

7. Use the above answers to construct a gate array for the function $f_x(y) = 2^x y \bmod 15$, for a two-bit control register x. Hint: $2^x = 4^{x_1} 2^{x_0}$.

8. There exists an x so that $ax = 1 \bmod N$ if and only if $\gcd(a,N) = 1$, so that multiplication is invertible (see Nielsen and Chuang, Appendix 4.2, Corollary A4.4 for details). Then the gate array for the function $f_x(y) = a^x y \bmod N$ can be constructed. What happens if $\gcd(a,N) > 1$, and why cannot the gate array be constructed in that case?

9. What values of a are possible for $N = 15$ according to Exercise 8? Use the answers to the previous exercises to construct the corresponding gate arrays, for a general x. How many bits are needed in x?

10. Imagine you have run the Shor quantum subroutine for a setup with two controlling qubits, and found the output $x = 3$ after the semiclassical Fast Fourier Transform. What value for r does this correspond to? Does this change if you find the value $x = 2$ at the output? What happens if the output reads $x = 0$?

11. Imagine you have run the Shor quantum subroutine and found the period $r = 4$ for the function $2^x \bmod 15$. Use this knowledge (and not the multiplication table for either 3 or 5) to factor 15. Hint: The period being 4 (=even) means that $2^4 - 1 \equiv 0 \bmod 15$. Now use the conjugate rule.

*12. Determine the needed number of bits in x for general a and N.

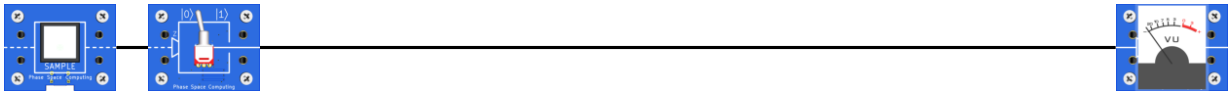
‡13. Perform the construction mentioned in Exercise 8. Note: this can be time-consuming.

4 Laboration tasks

From here, the laboratory work begins. A standard session should include running quantum Shor's algorithm for at least one controlled exponentiation.

Task 1 (Quantum bits): Verify that source and measurement works

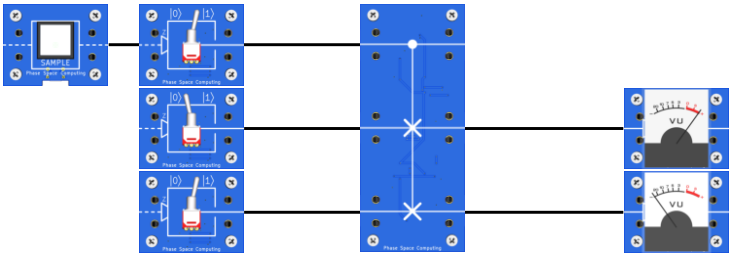
Materials: Power unit, sample button, one source, one detector, one short and one long cable



Connect the source to the detector using the long connector cable, connect the sample button, connect power, and test the circuit by flipping the switch and pressing the send button. When sending a 0, the measurement device should show a low value (the meter should point to the left), and when sending a 1, the measurement device should show a high value (the meter should point to the right, into the red area)

Task 2 Build and test a controlled multiplication with 2 mod 3

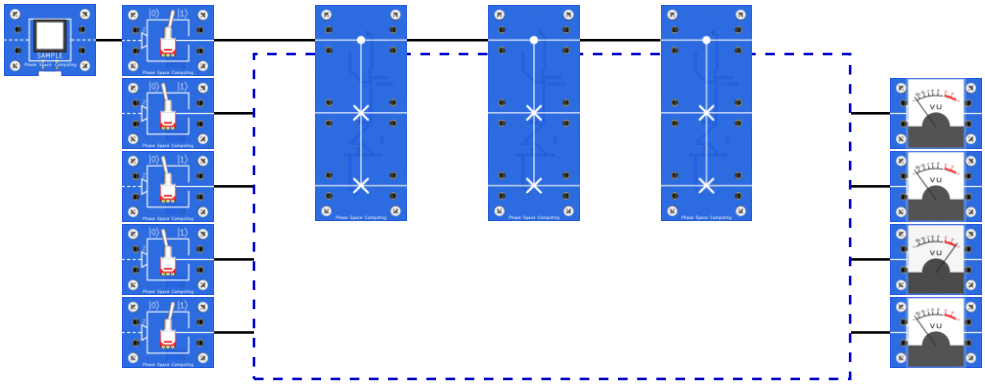
Materials: Power unit, sample button, three sources, two detectors, one Fredkin gate, cables



Connect as in the above picture, and verify that this really gives a controlled multiplication with 2 mod 3, see Excercise 2.

Task 3 Build and test a controlled multiplication with 2 mod 15

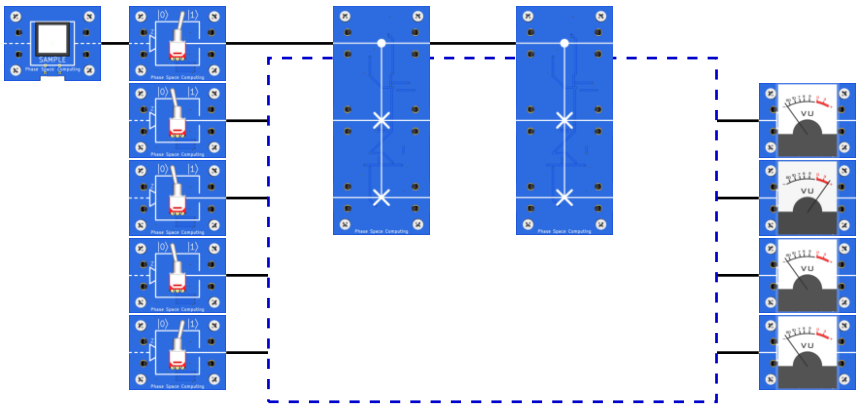
Materials: Power unit, sample button, five sources, four detectors, three Fredkin gates, cables



The preparatory exercises should have told you what gate array gives a controlled multiplication with 2 mod 15. Connect that gate array, using your prepared gate array drawing, and verify that this really gives a controlled multiplication with 2 mod 15.

Task 4 Build and test a controlled multiplication with 4 mod 15

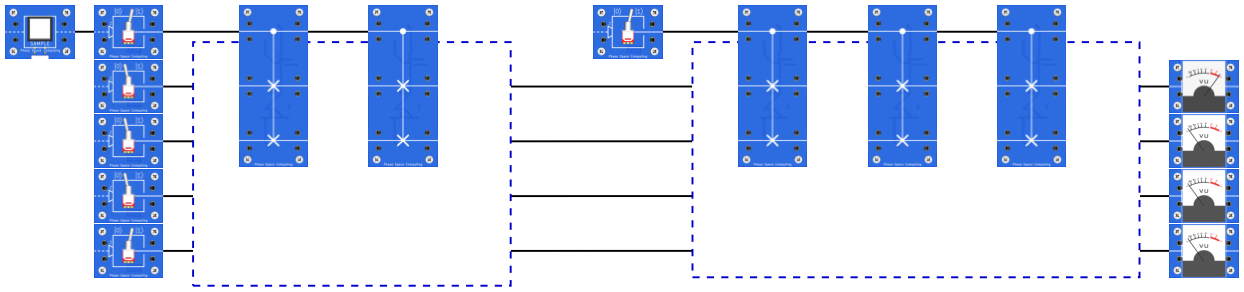
Materials: Power unit, sample button, five sources, four detectors, two Fredkin gates, cables



You designed a gate array for a controlled multiplication with 4 mod 15 in Exercise 4. Connect that gate array, using your prepared gate array drawing, and verify that this really gives a controlled multiplication with 4 mod 15. (Keep the Fredkin gate array from Task 3, you will need it later.)

Task 5 Build and test a controlled multiplication with 2^x mod 15

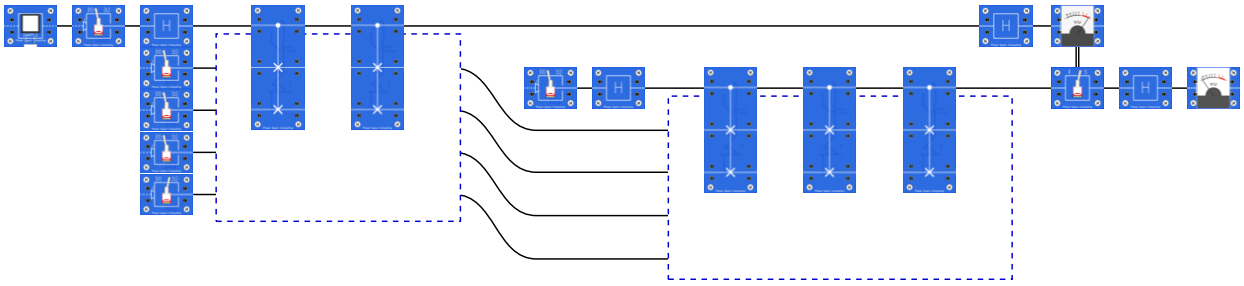
Materials: Power unit, sample button, six sources, four detectors, five Fredkin gates, cables



Use the Fredkin gate arrays from Task 3 and Task 4, and connect as in the above picture. Verify that this really gives a controlled multiplication with 2^x mod 15.

Task 6 Run the Shor quantum algorithm for $N = 15$ for the basis $a = 2$

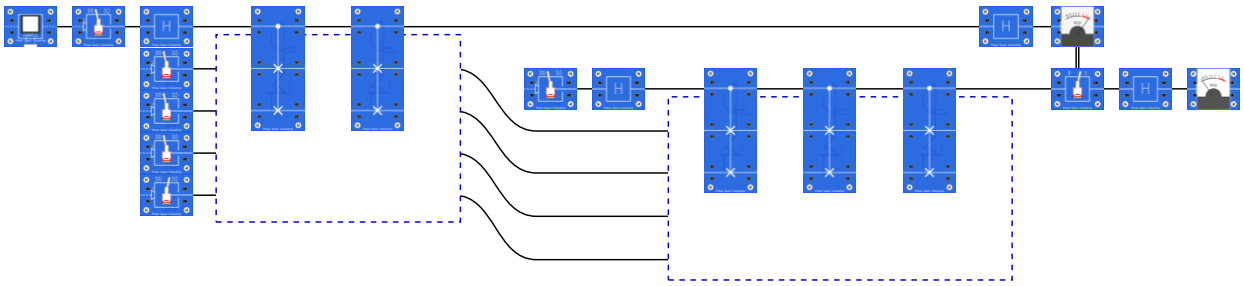
Materials: Power unit, sample button, six sources, two detectors, four Hadamards, one classically-controlled S, five Fredkin gates, cables



Use the gate array from Task 5, but reconnect to add the semiclassical Fast Fourier Transform, on the controls before and after the multiplications, as above. You will need to do the classical control by hand. Read off the output, and if possible, use your output to factor 15. If the experimental run is unsuccessful, try again by pressing the sample button.

Task *7 Run the Shor quantum algorithm for $N = 15$ for a random basis a

Materials: Power unit, sample button, six sources, two detectors, four Hadamards, one classically-controlled S, five Fredkin gates, four CNOTs, cables



Generate a random number a between 2 and 13. Check that $\gcd(a, 15) = 1$ (if not, recall your answer to Exercise 8). Construct the gate array you designed in Exercise 9 (you may need to add CNOTs not shown above), and add the semiclassical Fast Fourier Transform as above. You will need to do the classical control by hand. Factor 15 using the Shor algorithm.