Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 6 (2017)

Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710

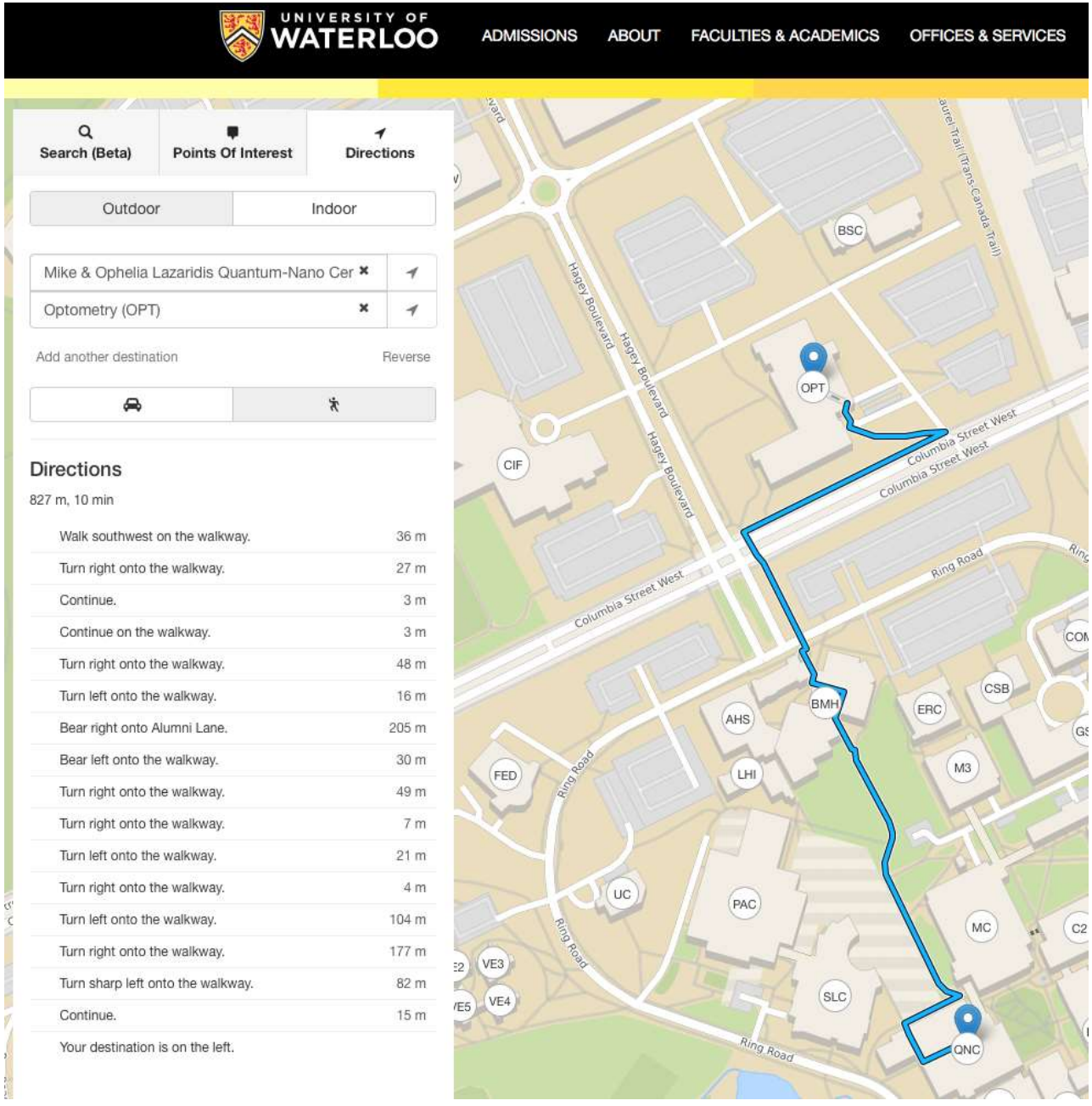
Homework on Crowdmark

- We will be using Crowdmard to grade homeworks.
- Upload .pdf once then drag each problem solution to the box for that problem.
- New page per solution (but okay this time if not, just scan relevant pages twice).
- Will accept paper for this assignment, but understand that we will need to scan it in.
- For this reason, okay to turn in on **Friday**.

Tuesday class in **OPT 309**

Sept. 19	QNC 1501	Sept. 21	MC 4058
Sept. 26	QNC 1501	Sept. 28	QNC 0101
Oct. 3	**OPT 309**	Oct. 5	QNC 1501
Oct. 10	QNC 0101	Oct. 12	QNC 0101
Oct. 17	QNC 0101	Oct. 19	QNC 0101
Oct. 24	QNC 0101	Oct. 26	QNC 1501
Oct. 31	QNC 0101	Nov. 2	QNC 0101
Nov. 7	QNC 0101	Nov. 9	QNC 0101
Nov. 14	QNC 0101	Nov. 16	QNC 0101
Nov. 21	QNC 0101	Nov. 23	QNC 0101
Nov. 28	QNC 0101	Nov. 30	QNC 0101

OPT 309


UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT
FACULTIES & ACADEMICS
OFFICES & SERVICES
Search (Beta)
Points Of Interest
Directions
Outdoor
Indoor
Mike & Ophelia Lazaridis Quantum-Nano Cer
Optometry (OPT)
Add another destination
Reverse
Directions
827 m, 10 min
Walk southwest on the walkway. 36 m
Turn right onto the walkway. 27 m
Continue. 3 m
Continue on the walkway. 3 m
Turn right onto the walkway. 48 m
Turn left onto the walkway. 16 m
Bear right onto Alumni Lane. 205 m
Bear left onto the walkway. 30 m
Turn right onto the walkway. 49 m
Turn right onto the walkway. 7 m
Turn left onto the walkway. 21 m
Turn right onto the walkway. 4 m
Turn left onto the walkway. 104 m
Turn right onto the walkway. 177 m
Turn sharp left onto the walkway. 82 m
Continue. 15 m
Your destination is on the left.
Hagey Boulevard
Columbia Street West
Ring Road
BSC
OPT
CIF
BMH
ERC
CSB
AHS
LHI
FED
M3
UC
PAC
MC
SLC
VE3
VE4
QNC

Discrete log problem

Discrete logarithm problem (DLP)

Input: p (prime), g (generator of $\mathbb{Z}_p^\times$), $a \in \mathbb{Z}_p^\times$
Output: $r \in \mathbb{Z}_{p-1}$ such that $g^r \equiv a \bmod p$

Example: $p = 7$, $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\} = \{3^0, 3^2, 3^1, 3^4, 3^5, 3^3\}$ (hence 3 is a generator of $\mathbb{Z}_7^\times$)

For $a = 6$, since $3^3 = 6$, the output should be $r = 3$

Note: No efficient classical algorithm for ***DLP*** is known, and cryptosystems exist (El Gamal encryption, Diffie-Hellman key exchange, Digital Signature Algorithm) whose security is based on the computational difficulty of DLP.

Efficient quantum algorithm for DLP?
(**Hint:** it can be made to look like Simon's problem!)

DLP similar to Simon's problem

Clever idea (of Shor): define $f: \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^\times$ as $f(x_1, x_2) = g^{x_1} a^{-x_2} \bmod p$. Can be efficiently computed *classically* (e.g. in $O(n^3)$-time by repeated squaring).

When is $f(x_1, x_2) = f(y_1, y_2)$?

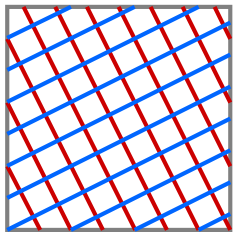
We know $a = g^r$ for ***some*** r, so $f(x_1, x_2) = g^{x_1 - r x_2} \bmod p$

Thus, $f(x_1, x_2) = f(y_1, y_2)$ iff $x_1 - r x_2 \equiv y_1 - r y_2 \bmod p - 1$

iff $(x_1, x_2) \cdot (1, -r) \equiv (y_1, y_2) \cdot (1, -r) \bmod p - 1$

iff $((x_1, x_2) - (y_1, y_2)) \cdot (1, -r) \equiv 0 \bmod p - 1$

iff $(x_1, x_2) - (y_1, y_2) \equiv k(r, 1) \bmod p - 1$



cf. Simon's property: $f(x) = f(y)$ iff $x - y \equiv r \bmod 2$.

Simon's problem modulo m

The function arising in DLP can be abstracted to the following:

Given: $f: \mathbb{Z}_m \times \mathbb{Z}_m \to T$ with the property that

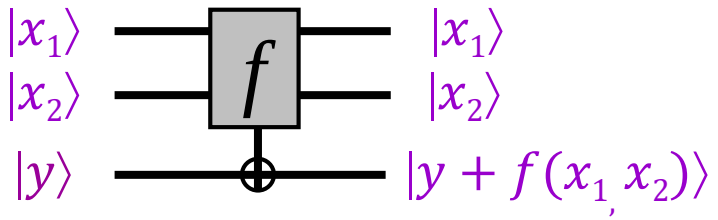
$f(x_1, x_2) = f(y_1, y_2)$ iff $(x_1, x_2) - (y_1, y_2) \equiv k(r_1, r_2) \bmod m$,

where (r_1, r_2) is the hidden data.

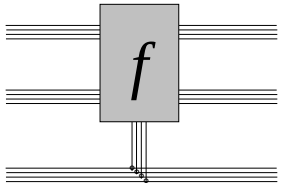
Goal: determine (r_1, r_2)

Note: in DLP case, $(r_1, r_2) = (r, 1)$

The reversible query box for f is



where each "wire" denotes many qubit wires, to represent elements of $\mathbb{Z}_m$ like:



Not a "black" box, because we can simulate it by 1-qubit and 2-qubit gates (and this can be done efficiently)…

Digression:
on simulating black boxes

How *not* to simulate a black box

Given an efficiently (classically) computable function, over some finite domain, such as $f(x) = g^{x_1} a^{-x_2} \bmod p$, need to simulate f-queries over that domain.

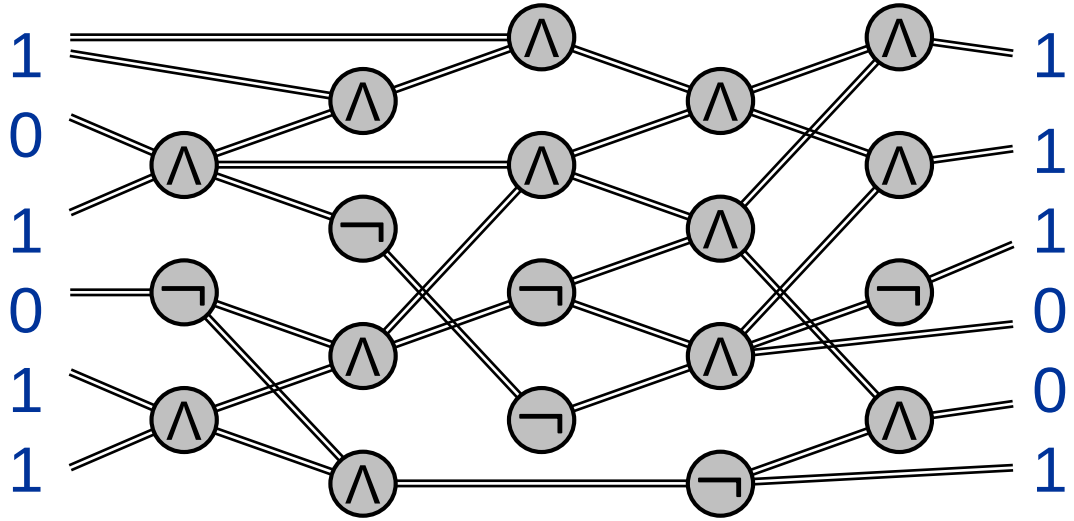
Easy to compute mapping $|x\rangle|y\rangle|0\cdots 0\rangle \mapsto |x\rangle|y + f(x)\rangle|g(x)\rangle$, where the third register is "work space" with accumulated "garbage" (e.g., two such bits arise when a Toffoli gate is used to simulate an AND gate inside a classical circuit).

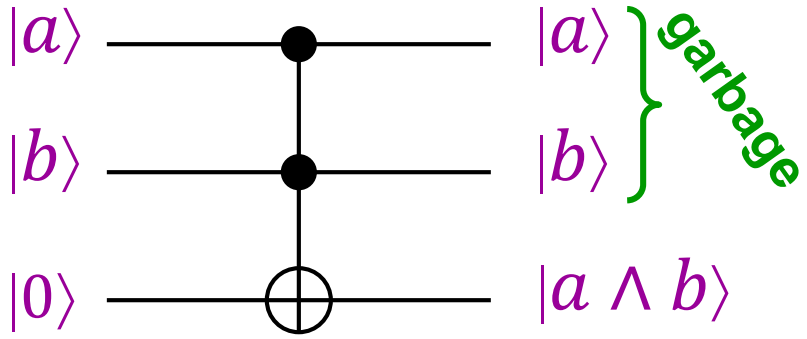
This works fine ***as long as f is not queried in superposition***

If f is queried in superposition then the resulting state can be $\sum_x \alpha_x |x\rangle|y + f(x)\rangle|g(x)\rangle$.
Can't we just discard the third register?

No ... there could be entanglement ...

Intermediate AND gates





How *to* simulate a black box

Simulate the mapping $|x\rangle|y\rangle|0\cdots 0\rangle \mapsto |x\rangle|y+f(x)\rangle|0\cdots 0\rangle$,
(i.e., clean up the "garbage")

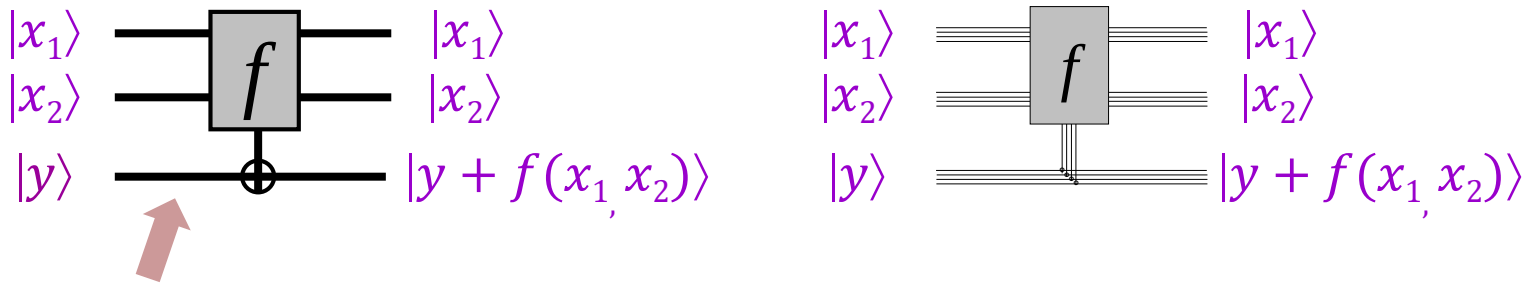
To do this, use an additional register, and:

1. compute $|x\rangle|y\rangle|0\cdots 0\rangle|0\cdots 0\rangle \mapsto |x\rangle|y\rangle|f(x)\rangle|g(x)\rangle$
   (ignoring the 2nd register in this step)
2. compute $|x\rangle|y\rangle|f(x)\rangle|g(x)\rangle \mapsto |x\rangle|y+f(x)\rangle|f(x)\rangle|g(x)\rangle$
   (using CNOT gates between the 2nd and 3rd registers)
3. compute $|x\rangle|y+f(x)\rangle|f(x)\rangle|g(x)\rangle \mapsto |x\rangle|y+f(x)\rangle|0\cdots 0\rangle|0\cdots 0\rangle$
   (by reversing, i.e. "*uncomputing*", the procedure in step 1)

Total cost about twice the classical cost of computing f,
plus n auxiliary CNOT gates.

Simon's problem modulo m

So now we have an efficient way of implementing the reversible black box for f



Reminder: each "thick wire" denotes several qubits, to represent an element of $\mathbb{Z}_m$ (e.g. $\{0,1,2,3,4,5,6\} = \{000,001,010,011,100,101,110\}$)

OK, so what about a quantum algorithm for this problem?

To get one, we go beyond the Hadamard transform, which has been our main tool so far, to…

Quantum Fourier transform (QFT)

Quantum Fourier transform

$$F_m = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(m-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(m-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & \omega^{3(m-1)} & \cdots & \omega^{(m-1)^2} \end{pmatrix}$$

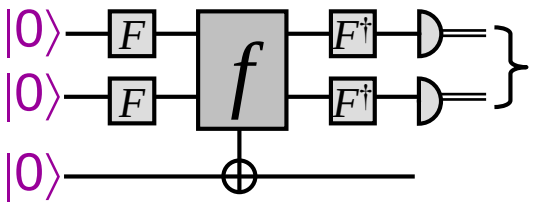
where $\omega = e^{2\pi i/m}$ (for n qubits, $m = 2^n$).

This is unitary and generalizes the Hadmard transform $F_2 = H$.

The quantum Fourier transform is an important component of several interesting quantum algorithms …

Quantum algorithm for Simon mod m

$f(x_1, x_2) = f(y_1, y_2)$ iff $(x_1, x_2) - (y_1, y_2) \equiv k(r, 1) \bmod m$



Turns out that the result is a random (s_1, s_2) such that $(s_1, s_2) \cdot (r, 1) \equiv 0 \bmod m$.
(generalizes idea from Simon's algorithm)

If $\gcd(s_1, m) = 1$, then s_1 has an inverse mod m, and r can be computed as $r \equiv -s_2/s_1 \bmod m$.
(The details of computing $s_1^{-1} \bmod m$ follow from the extended Euclidean algorithm).

Moreover, the probability that $\gcd(s_1, m) = 1$ occurs is not too small (if it fails the algorithm can be run again).

Quantum algorithm for Simon mod m

Steps that have been shown to be efficiently implementable (i.e., in terms of a number of 1- and 2-qubit/bit gates that scales polynomially with respect to the number of bits of m):

- Implementation of reversible gate for f
- The classical post-processing at the end

What's missing?

- Implementation of the QFT f modulo m ($= p - 1$ for DLP)
- Proof that outcome is random s.t. $(s_1, s_2) \cdot (r, 1) \equiv 0 \bmod m$

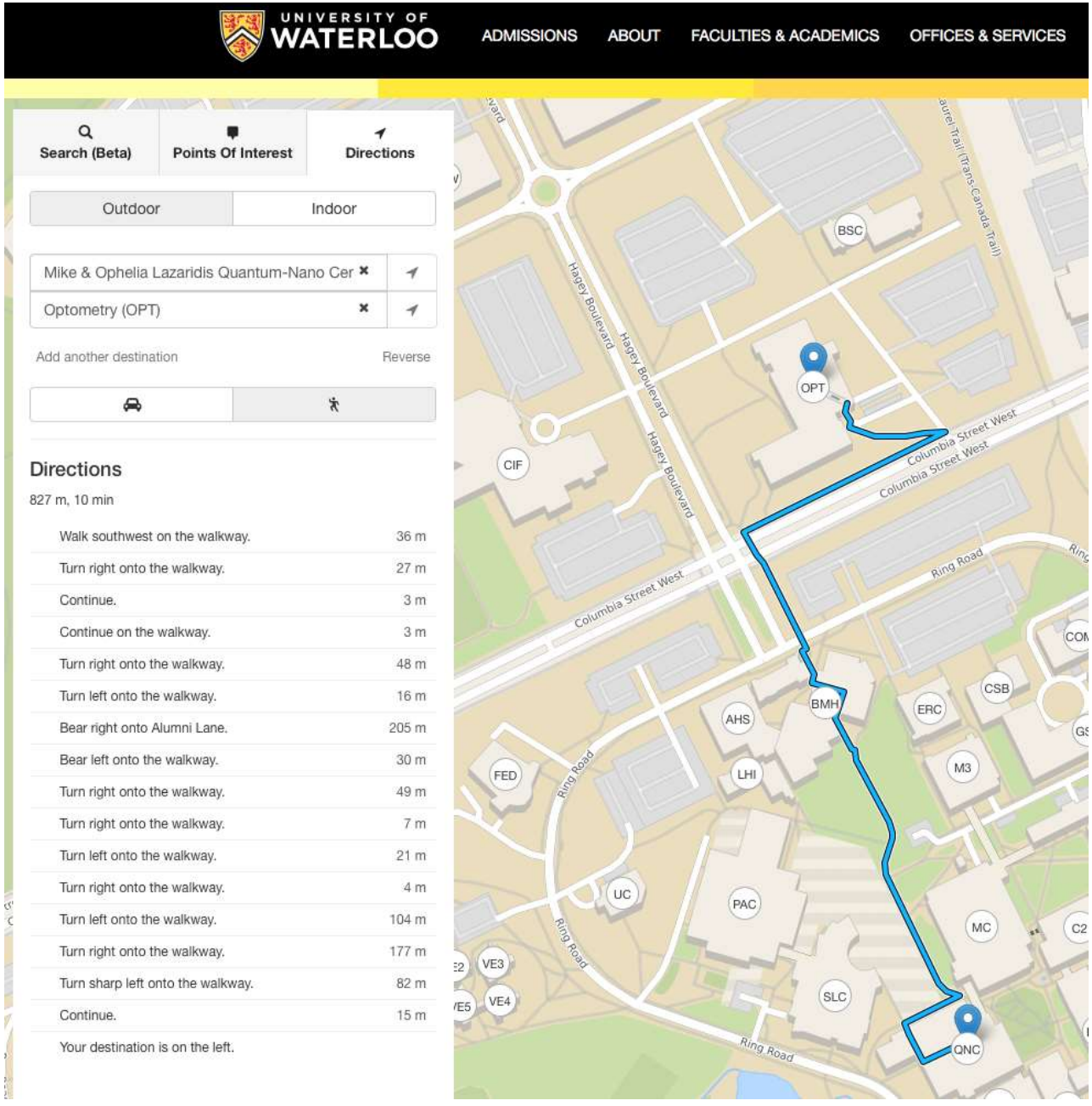
Next time, we'll show how to implement the QFT for $m = 2^n$.

Shor did this too, and showed that if the modulus is within a factor of 2 from $p - 1$, by using careful error-analysis, this was good enough, though the calculations and analysis become more complicated (we'll omit the details of this).

Tuesday class in **OPT 309**

Sept. 19	QNC 1501	Sept. 21	MC 4058
Sept. 26	QNC 1501	Sept. 28	QNC 0101
Oct. 3	**OPT 309**	Oct. 5	QNC 1501
Oct. 10	QNC 0101	Oct. 12	QNC 0101
Oct. 17	QNC 0101	Oct. 19	QNC 0101
Oct. 24	QNC 0101	Oct. 26	QNC 1501
Oct. 31	QNC 0101	Nov. 2	QNC 0101
Nov. 7	QNC 0101	Nov. 9	QNC 0101
Nov. 14	QNC 0101	Nov. 16	QNC 0101
Nov. 21	QNC 0101	Nov. 23	QNC 0101
Nov. 28	QNC 0101	Nov. 30	QNC 0101

OPT 309


UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT
FACULTIES & ACADEMICS
OFFICES & SERVICES
Search (Beta)
Points Of Interest
Directions
Outdoor
Indoor
Mike & Ophelia Lazaridis Quantum-Nano Cer
Optometry (OPT)
Add another destination
Reverse
Directions
827 m, 10 min
Walk southwest on the walkway. 36 m
Turn right onto the walkway. 27 m
Continue. 3 m
Continue on the walkway. 3 m
Turn right onto the walkway. 48 m
Turn left onto the walkway. 16 m
Bear right onto Alumni Lane. 205 m
Bear left onto the walkway. 30 m
Turn right onto the walkway. 49 m
Turn right onto the walkway. 7 m
Turn left onto the walkway. 21 m
Turn right onto the walkway. 4 m
Turn left onto the walkway. 104 m
Turn right onto the walkway. 177 m
Turn sharp left onto the walkway. 82 m
Continue. 15 m
Your destination is on the left.
Hagey Boulevard
Columbia Street West
Ring Road
BSC
OPT
CIF
BMH
ERC
CSB
AHS
LHI
FED
M3
UC
PAC
MC
SLC
VE3
VE4
QNC