Quantum Computing & Cryptography Week 8

Special gates for quantum algorithms
- Grover's search algorithm Mermin 4
- Toffoli gates Mermin 2.6

Steve Vickers

Building quantum gates
1 Qbit gates: normally not too hard
2 Qbit gates: harder - must make Qbits interact temporarily
   Use cNOT as standard 2 Qbit gate
   How to make cNOT? Mermin Appendix H
   Actually easier to make controlled Z

What can be built using cNOTs + 1 Qbit unitaries?

Toffoli gates T

\begin{align*}
\text{Doubly controlled NOT gate} \\
|1\rangle & \rightarrow |1\rangle \\
|0\rangle & \rightarrow |0\rangle \\
|1\rangle & \rightarrow |1\oplus xy\rangle
\end{align*}

Classically:
To build arbitrary reversible computations
- must have at least one 3 Qbit gate
  e.g. Toffoli

Toffoli = reversible form of AND gate

Logically: NOT, AND enough to build all other logic gates
Quantum:
Can build Toffoli out of:
<NOTs + 1-qubit unitaries
Good! - because difficult to control quantum interaction of 3 qbits together
Look at construction later

Grover’s search algorithm
- will need Toffoli gates

The problem
- You have a black box routine that tests n-bit integers
- You know exactly one of those integers, a, passes the test
- How do you find it?

f - n-bit argument
- 1-bit result

\[ f(x) = \begin{cases} 
1 & \text{if } x = a \\
0 & \text{if } x \neq a 
\end{cases} \]

Classical random testing
- avoid repetitions
- Test random numbers until you find the one that passes
Probability of finding it in M tests = \( \frac{M}{N} \)
Expected number of tests = \( \frac{N}{2} \)
Quantum: reduce this to \( \frac{\pi}{4} \sqrt{N} \)
Unitary operator $U_f$

As usual $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$.

Trick for Bernstein-Vazirani: use $H|1\rangle$ for output - 1 output of $f$ shown by sign change

$U_f(|x\rangle \otimes H|1\rangle) = \frac{1}{2} (|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1\rangle)$

where $V|x\rangle = (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{N}} |x\rangle$ if $x \neq a$

$\frac{1}{\sqrt{N}} |a\rangle$ if $x = a$

From now on: can ignore output line

In general -

$V|x\rangle = \frac{1}{\sqrt{N}} \begin{pmatrix} x_1 & \cdots & x_N \end{pmatrix} |x\rangle$

$V|a\rangle = \frac{1}{\sqrt{N}} \begin{pmatrix} x_1 & \cdots & x_N \end{pmatrix} |a\rangle = \frac{1}{\sqrt{N}} |a\rangle - 2 \langle a | |a\rangle |a\rangle$

Write as $|a\rangle - 2 \langle a | |a\rangle |a\rangle$

Think of $V$ as $1 - 2 \langle a | |a\rangle$

Note: matrix for $|a\rangle \langle a|$ is correct - matrix multiply column vector $|a\rangle \times$ row vector $\langle a|$.

Reflections

For any $|\psi\rangle$ with $\langle \psi | \psi \rangle$

$V_\psi = 1 - 2 |\psi\rangle \langle \psi |$

$V_\psi |\psi\rangle = -|\psi\rangle$

$V_\psi |\phi\rangle = |\phi\rangle$ if $\langle \psi | \phi \rangle = 0$

$V_\psi$ reflects in space of vectors $|\psi\rangle$ orthogonal to $|\psi\rangle$

If $W_\psi = -V_\psi$

$W_\psi |\psi\rangle = -|\psi\rangle$

$W_\psi |\phi\rangle = -|\phi\rangle$ if $\langle \psi | \phi \rangle = 0$

$W_\psi$ reflects in ray $|\psi\rangle$

Properties

$V_\psi$ is a unitary.

- $V_\psi$ has same properties

1. $V_\psi$ is self-adjoint

$V_\psi^+ = 1 + 2 (\langle \psi | \psi \rangle)^+ = 1 - 2 |\psi\rangle \langle \psi | = V_\psi$

2. $V_\psi^2 = 1$

$V_\psi^2 = (1 - 2 |\psi\rangle \langle \psi |) (1 - 2 |\psi\rangle \langle \psi |) = 1 - 4 |\psi\rangle \langle \psi | + 4 |\psi\rangle \langle \psi | = 1$

So $V_\psi$ is unitary. $V_\psi V_\psi^+ = 1$. Using $\langle \psi | \psi \rangle = 1$. 

Hadamard's
As usual: apply Hadamard's to input, use
\[ |\psi\rangle = H^\otimes n |0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n \]
Now define
\[ W = 2 |\psi\rangle \langle \psi | - I \]
W also self-adjoint & unitary
\[ W \text{ does not depend on } f \]

Calculate
\[ V |\psi\rangle = - |\psi\rangle \]
\[ V |\phi\rangle = |\phi\rangle - 2 \langle \phi | a |\psi\rangle |\psi\rangle \]
\[ = |\phi\rangle - \frac{1}{\sqrt{2^{n-1}}} |a\rangle \]
\[ W |\psi\rangle = 2 \langle \phi | a |\psi\rangle - |\psi\rangle = \frac{1}{\sqrt{2^{n-1}}} |\phi\rangle - |\psi\rangle \]
\[ W |\phi\rangle = 2 \langle \phi | a |\phi\rangle - |\phi\rangle = |\phi\rangle \]

In every case - a real linear combination of \(|\psi\rangle\) and \(|a\rangle\)
\[ \therefore V, W \text{ transform real } 2\text{-dim. space on basis } |\psi\rangle, |a\rangle \]

Orthonormal basis
\[ \langle a | \phi \rangle = \frac{1}{2^{n/2}} \approx 0 \text{ if } n \text{ large} \]
|\psi\rangle, |\phi\rangle \text{ almost orthogonal}
Find \(|a_\perp\rangle - \text{ real linear combination of } |\psi\rangle, |\phi\rangle\)
\[ - |\psi\rangle, |a_\perp\rangle \text{ orthonormal} \]
If \[ |a_\perp\rangle = \langle a | + \phi | a \rangle \]
\[ \langle a_\perp | a \rangle = 2 + \frac{\phi}{2^{n/2}} = 0 \]
\[ \therefore |a_\perp\rangle \text{ normalized multiple of } -\frac{\phi}{2^{n/2}} |\psi\rangle + |\phi\rangle = W|\psi\rangle, \text{ say} \]
\[ \langle a_\perp | a \rangle = \frac{1}{2^{n/2}} |\psi\rangle - \frac{\phi}{2^{n/2}} \langle a \rangle + \langle a_\perp | a \rangle = 1 - \frac{2^2}{2^{n/2}} \]
\[ |a_\perp\rangle = \frac{1}{1 - \frac{2^2}{2^{n/2}}} (-\frac{2^{n/2}}{2^{n/2}} |\psi\rangle + |\phi\rangle) \]

Real 2-dim. space on \(|a\rangle, |\phi\rangle\)
\[ V = 1 - 2 |a\rangle \langle a | \]
\[ W = 2 |\psi\rangle \langle \psi | - I \]

\[ V \text{ reflects in } |a\rangle \text{ axis} \]
\[ W \text{ reflects in } |\phi\rangle \text{ ray} \]
\[ WV \text{ must be rotation} \]
What angle? 28
\[ V |a_\perp\rangle = |a_\perp\rangle \]
\[ \therefore WV |a_\perp\rangle = W |a_\perp\rangle \]
\[ |a_\perp\rangle \text{ reflected in } |a\rangle \]

\[ \sin \theta = \cos \left(\frac{\pi}{2} - \phi \right) \]
\[ \phi = \langle a | a \rangle = \frac{1}{2^{n/2}} \]
Rotating $|\phi\rangle$ to $|a\rangle$

- NV acts as rotation $2\theta$ on real linear combinations of $|a\rangle = |\phi\rangle$
  - If $k$ an integer, $k = \frac{\pi}{4\theta}$, then $(NV)^k$ is rotation $= \frac{\pi}{2}$
  - $|\phi\rangle$, $|a\rangle$ approximately orthogonal
  - $(NV)^k |\phi\rangle \approx |a\rangle$

Strategy: apply $NV$ to $|\phi\rangle$ $k$ times, then measure

Probably get result $a$ - test by applying $f$

If fails test $\oplus$ start again.

Gate for $W$

Want $W$ built from $1$-$\&2$-qubit gates

Just as good to do $-W$

$-H^{\otimes n} WH^{\otimes n} = H^{\otimes n} (1 \& -2|\phi\rangle\langle\phi|) H^{\otimes n}$

$= 1 - 2 H^{\otimes n} |\phi\rangle \langle\phi| H^{\otimes n}$

$= 1 - 2 |0\rangle \langle 0| H^{\otimes n}$

$-H^{\otimes n} WH^{\otimes n} |x\rangle = \begin{cases} |1x\rangle & \text{if $x \neq 0$} \\ -1|x\rangle & \text{if $x = 0$} \end{cases}$

Task: implement $c^{\otimes n} Z$ using $1$-$\&2$-qubit gates

Like multiply-controlled $Z$

- $-H^{\otimes n} WH^{\otimes n} |x\rangle = \begin{cases} |1x\rangle & \text{if $x \neq 0$} \\ -1|x\rangle & \text{if $x = 0$} \end{cases}$

- $-H^{\otimes n} WH^{\otimes n} = X^{\otimes n} c^{\otimes n-1} Z X^{\otimes n}$

- but flips role of bits
- change sign if all bits are $0$

$\text{(n-1)-fold controlled } Z$

- enough to construct $c^{\otimes n} Z$

Strategy:

1. Reduce to Toffolis $\text{**thanks enough**}$
2. Use ancillas (ancillary qubits)
   - extra qubits used to help calculation
   - must ensure ancillas restored to start state
   - otherwise they get entangled with input
   - spoils Grover analysis
3. Develop in steps
   - start with simple solution, then improve
First solution
Illustrated for \( n = 6 \)

Use \( n-3 \) ancillas prepared as \( 10 \rangle \)

Second solution
Still \( n-3 \) ancillas – but they don’t have to be prepared as \( 10 \rangle \)

How does it work?

If line 4 or 5 is \( 10 \rangle \)

How does it work?

If line 3 is \( 10 \rangle \)
How does it work? If line 2 is 10

How does it work? If line 1 is 10

How does it work? If lines 1-5 all 1

Focus on ancillas
One of these active
:: one of these active
On ancillas these cancel the left hand ones
:: one of these active
Third solution: One ancilla only
+n input lines
Divide input lines into two parts
part A - size m
part B - size n-m
If n even: \( m = \frac{n}{2} + 1 \)
\( n-m = \frac{n}{2} - 1 = m-2 \)
If n odd: \( m = \frac{n+1}{2} \)
\( n-m = \frac{n-1}{2} = m-1 \)
Idea: \( c^m Z \) (part A + ancilla)
borrows ancillas from part B
There are enough: \( n-m \geq m+1-3 \)

Third solution: One ancilla only
+n input lines
Divide input lines into two parts
part A - size m
part B - size n-m
If n even: \( m = \frac{n}{2} + 1 \)
\( n-m = \frac{n}{2} - 1 = m-2 \)
If n odd: \( m = \frac{n+1}{2} \)
\( n-m = \frac{n-1}{2} = m-1 \)
Idea: \( c^m Z \) (part A + ancilla)
borrows ancillas from part B
There are enough: \( n-m \geq m+1-3 \)

How does it work?
If any B line is \( |0\rangle \): \( c^m Z \) is cancel
If all B lines are \( |1\rangle \): just one \( c^m Z \) can be active
**Summary of Grover**

- Prepare inputs as $|\phi\rangle = H^{\otimes n} |0\rangle_n$
- Prepare output as $|1\rangle$
- $U_f$ acts as $V$ on inputs
- Build $W = 2 \langle \phi | \psi | -1 \rangle$
- Apply $(WV)^k$ to $|\psi\rangle$
- Where $k = \frac{\pi}{4} \frac{1}{N} JN$ to nearest integer
- Measure input
- Test result to see if it is a $\bigcirc$
- If not $\bigcirc$ start again

**Toffoli Gates**

Two constructions of $T = c^2 X$

- Both rely on same basic ideas
- 6 CNOTs - these slides
- 8 CNOTs - see exercises

**Controlled unitaries**

- Given any 1-qubit unitary $U$

  \[ C_{10}^U = \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix} \]

  \[ C_{10}^U |x\rangle |y\rangle = U^x |x\rangle |y\rangle \]

  Applies $U$ to qubit 0 if $|x\rangle = 1$.

  $C_{10} = C_{10}^x$ - controlled NOT

  Start by looking at how to construct controlled unitaries.

**“Block operators”**

- Non-standard terminology

  Let $A$ be an operator for 1 qubit.
  I call it a Block operator if it is:
  - Self-adjoint
  - Unitary
  - With trace 0, $\text{Tr} (A^2) = a + d$
**Bloch operators: some facts**

- A acts on Bloch sphere by reflection in an axis.
  \[ A = a_x X + a_y Y + a_z Z \]
  with \(a_x^2 + a_y^2 + a_z^2 = 1\).

- If \(A, B\) are Bloch operators, then there is some unitary \(V\) with
  \[ A = V B V^\dagger \]
  useful for reducing to simple cases, e.g., \(X\) or \(Z\).

**Summary**

- For solution with 6 CNOTs
  
  1. Any 1-qubit unitary \(U\) can be written as \(U = e^{\theta \sigma_z} B A\) (Bloch operators)
  
  2. Any Bloch operator \(A\) is \(V X V^\dagger\) (some unitary)
  
  3. Singly controlled unitary using 2xnor & 1-qubit unitaries
  
  4. Circuit for doubly controlled phase change
  
  5. Circuit for doubly controlled \(BA\ BA\)
  
  6. Find \(JX\), i.e., solve \(U^2 = X\)

**Next**

- \(U = (e^{i\theta_1} \ 0) \begin{pmatrix} e^{\frac{i\theta_1}{2}} & i e^{\frac{i\theta_2}{2}} \\ i e^{-\frac{i\theta_2}{2}} & e^{\frac{i\theta_1}{2}} \end{pmatrix} \begin{pmatrix} e^{i\theta_2} & 0 \\ 0 & e^{-i\theta_2} \end{pmatrix}^\dagger\)
  
  - \(\theta_1, \theta_2\) - some unitary \(U\) with real trace \((e^{i\phi} + e^{-i\phi} = 2\cos\beta)\)
  
  - Want \(U\) in form \(AB\) (both Bloch)

- Fact: There is a unitary \(V\) such that \(U = V (e^{i\theta_1} \ 0) V^\dagger\), some \(\theta_1, \theta_2\).
  
  This allows us to focus on case \(U = (e^{i\theta_1} \ 0)\).
$U' = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$ is product of Bloch operators.

$= \cos \beta \ 1 + i \sin \beta \ 2$

- Acts on Bloch sphere as rotation $2\beta$ about axis through poles.
- Find $A\ B$ corresponding to axes through equator, angle $\beta$ between.

If $U = V e^{i\alpha} U' V^+ \text{ and } U' = AB$ then $U = e^{i\alpha} (VAV^+) (VBV^+)$ both Bloch.

**Looking down on N. pole**

**Reflecting in A axis then B axis**

- Fixes N & S poles.
- Rotates equator through $2\beta$.

E.g.: Rotates whole sphere $2\beta$ about axis.

\[ AB = U' \]
Any Bloch operator $A^\dagger$ is $VXV^\dagger$ for some unitary $V$

On Bloch sphere:
- Find unitary $V$ that rotates $X$ point to $A$ point ($e^V$ does reverse)
- Bloch operator $X$ reflects in $X$-axis
- $VXV^\dagger$ reflects in $A$-axis
- i.e. $VXV^\dagger = A$

Singly controlled unitary $U$
$U = EAB$
$E = e^{ix}$
$A = VXV^\dagger$ $B = WXW^\dagger$
$cU = \frac{U}{c}$

order reversed in circuit diagram (But note: phase change commutes with everything)

Controlled Bloch operator
If $A = VXV^\dagger$ then
$C_{1,0}^A = V_0 C_{1,0} V_0^\dagger$

Controlled phase change
$c e^{ix}$

Phase changes can be moved from one line to another.
\[ c e^{ix} 10|y\rangle = 10|y\rangle \]
\[ c e^{ix} |1\rangle|y\rangle = e^{ix} |1\rangle|y\rangle \]
\[ c e^{ix} (|x\rangle|y\rangle) = (e^{inx} |x\rangle)|y\rangle \]

Number operator
\[ n |x\rangle = x |x\rangle \]
\[ e^{inx} |x\rangle = e^{inx} |x\rangle \]
**Numeric functions \( f \) on diagonal matrices**

Apply \( f \) to each diagonal entry

\[ f(x) = x^2, \quad M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \]

\[ f(M) = \begin{pmatrix} 2^2 & 0 \\ 0 & 3^2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 9 \end{pmatrix} \]

- \( f(n) = e^{inx} \)

\[ f(n) = e^{inx} = (1 \ 0 \ e^{inx}) \]

Later: see with \( f(x) = \text{Re} \)

**Singly controlled unitary \( U \)**

\[ U = EAB \]

\[ e^{i \alpha} \]

\[ A = V X V^* \quad B = W X W^* \]

\[ cU = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \]

\[ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

2 cNOT gates

5 1-qbit unitaries

**Doubly controlled phase change**

\[ c e^{i \alpha} \]

\[ e^{i \alpha} \]

\[ = \]

\[ c e^{i \alpha} \]

\[ e^{i \alpha} \]

\[ = \]

\[ c e^{i \alpha} \]

\[ e^{i \alpha} \] \[ \text{top line controls controlled phase change on other two} \]

\[ c(e^{i \alpha}) \]

\[ e^{i \alpha} \]

\[ = \]

\[ e^{i \alpha} \]

\[ e^{i \alpha} \] \[ \text{can do it with 2 cNOTs since } e^{i \alpha} \text{ unitary} \]

**Doubly controlled BABA**

\[ A, B \text{ both Bloch operators} \]

\[ A^2 = B^2 = 1 \]

If either control line is 0 other two controlled gates cancel
Find \( U = J \hat{X} \)

\( J \) is easy:
\( J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \)

\( J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \)

Apply for \( J \) to diagonal matrix \( Z \).

Could also choose \( \pm \) instead.

But \( X = HZH \)

\( JX = HJZH \)

Summary: \( T \) is —

Still must convert this controlled unitary to CNOTS & Hadamard

I'm not going to calculate \( V, W, \alpha \), etc. The point is to know it's possible.