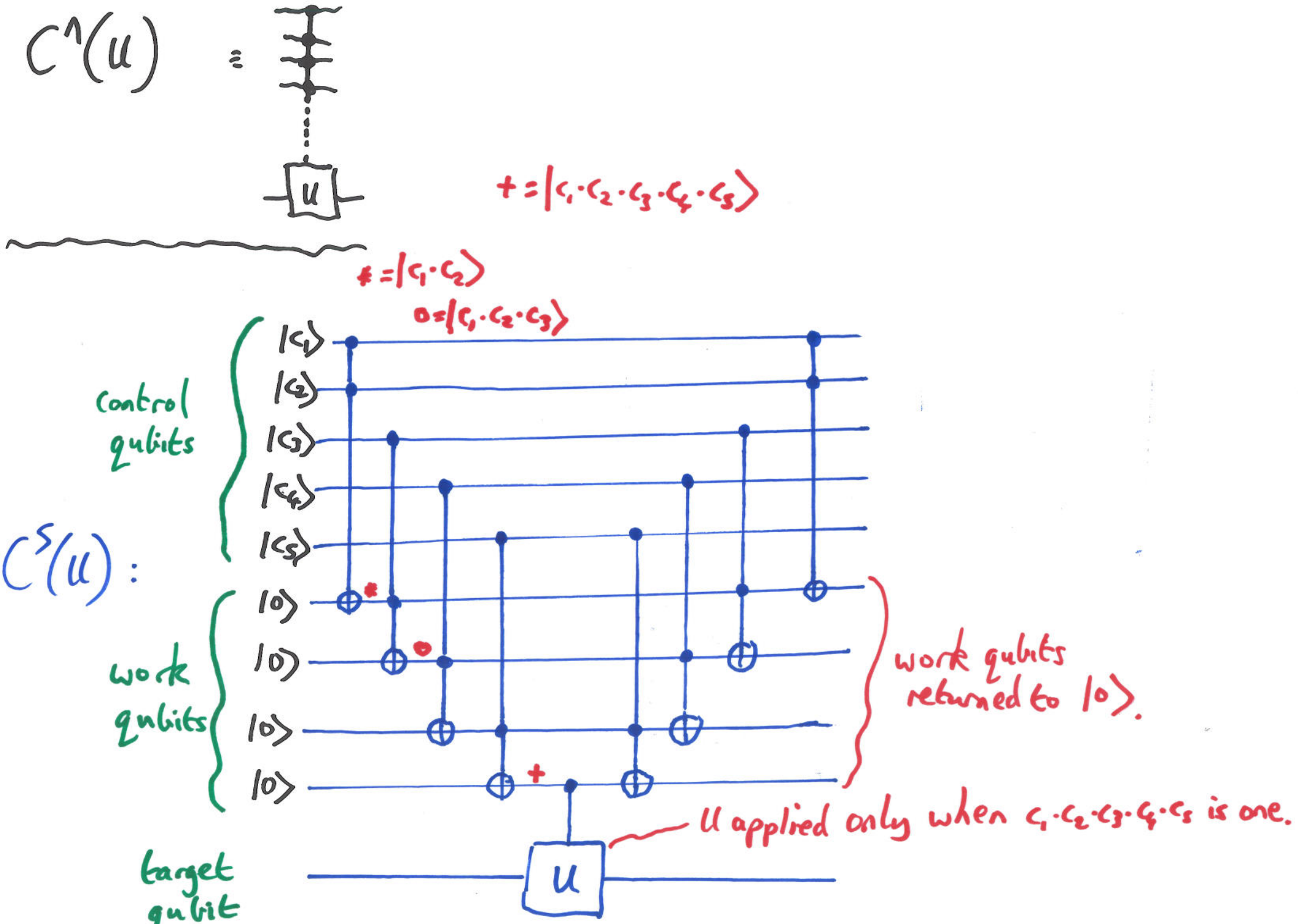
Elemental Cyclic Permutation

Construct

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Using just CNOTs and Toffoli gates?


C^(u) ≡
u
+ = |c1·c2·c3·c4·c5⟩
* = |c1·c2⟩
o = |c1·c2·c3⟩
control qubits
|c1⟩
|c2⟩
|c3⟩
|c4⟩
|c5⟩
C^5(u):
work qubits
|0⟩
|0⟩
|0⟩
|0⟩
work qubits returned to |0⟩.
u applied only when c1·c2·c3·c4·c5 is one.
target qubit
u

Exercises:

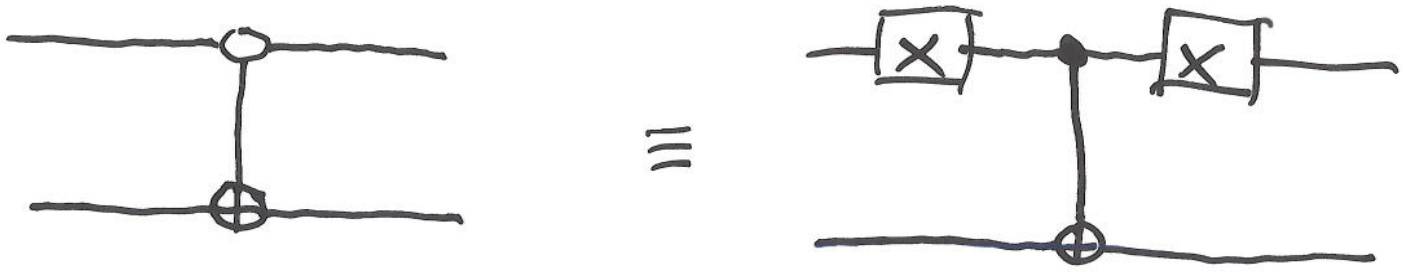
1. Let $U = V^2$, find $C^5(U)$ circuit using no work qubits, but using controlled-V and controlled-$V^\dagger$ gates.

2. Implement a $C^n(X)$, $(n>3)$, gate, using $O(n^2)$ Toffoli, CNOT, and single qubit gates, using no work qubits.

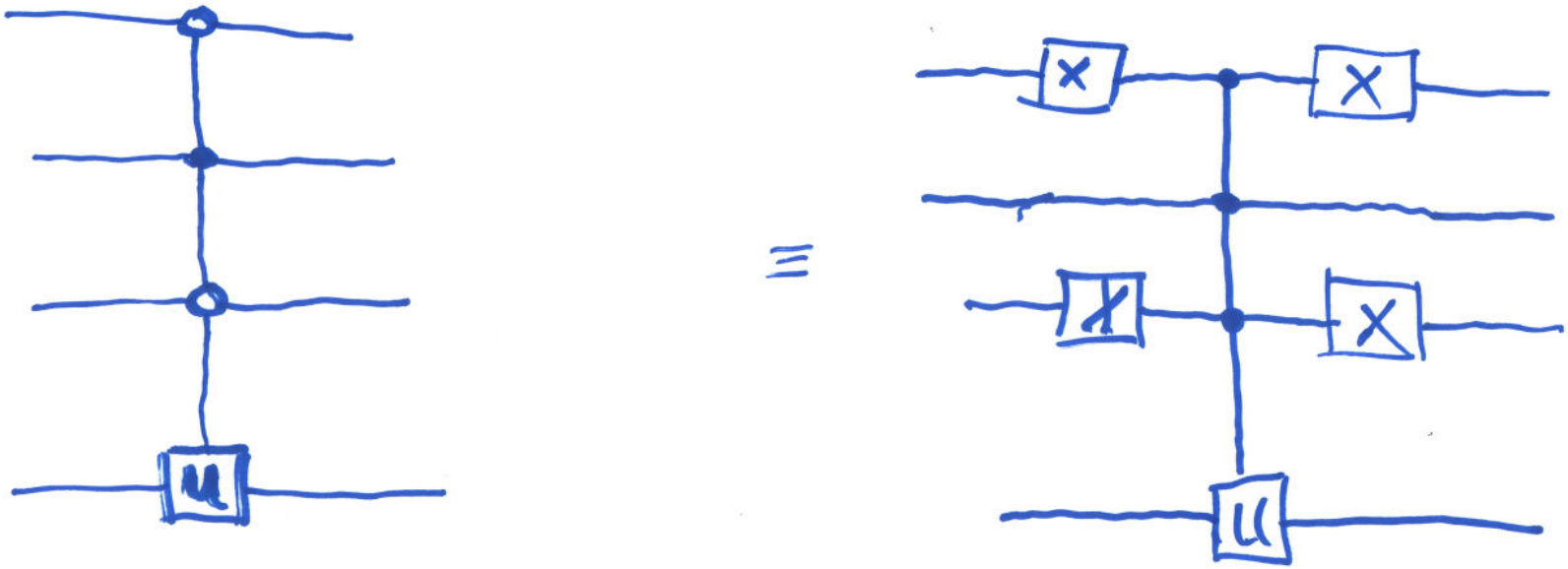
3. Implement $C^n(U)$, $(n>3)$, for U a single qubit unitary using $O(n^2)$ Toffoli, CNOT, and single qubit gates, using no work qubits.

More General Conditions

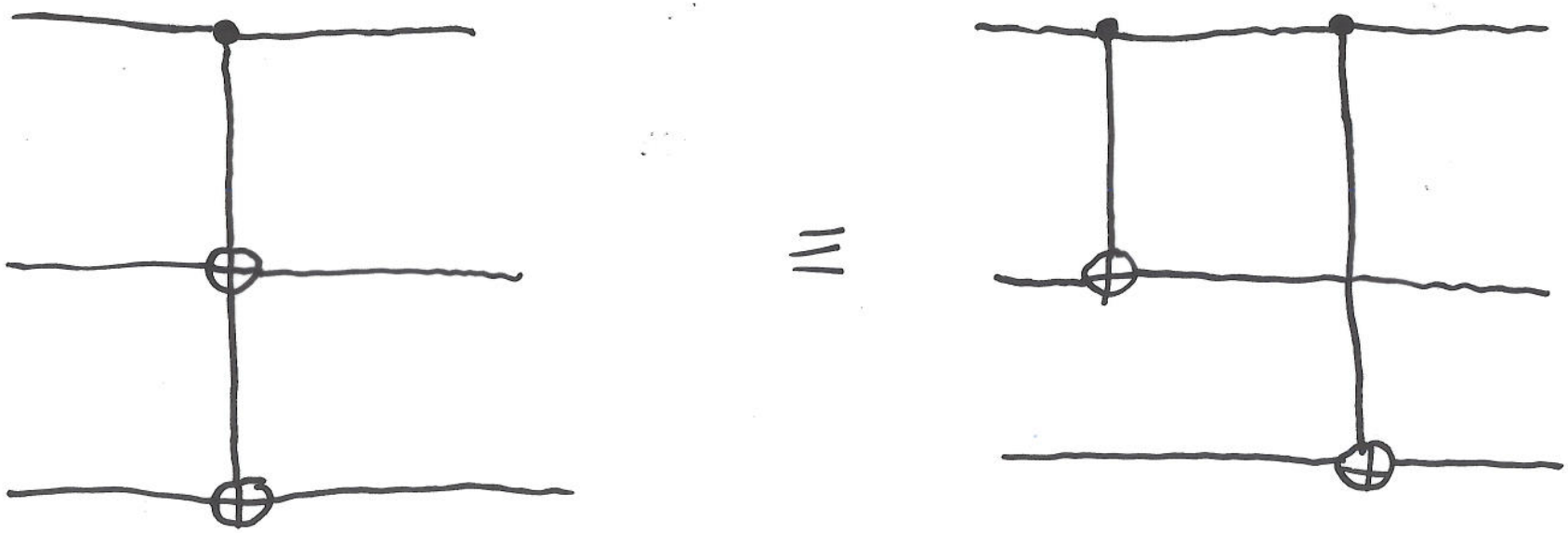
e.g. flip target qubit if control qubit is set to zero:



A More General Example



Multiple Targets



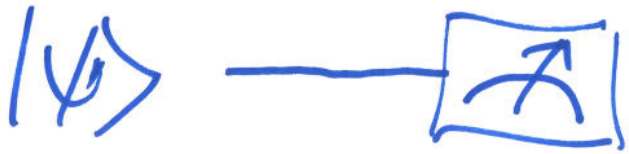
More Circuit Identities

Let C be a CNOT with qubit 1 control, and qubit 2 target. Then,

$$CX_1C = X_1X_2$$
$$CY_1C = Y_1X_2$$
$$CZ_1C = Z_1$$
$$CX_2C = X_2$$
$$CY_2C = Z_1Y_2$$
$$CZ_2C = Z_1Z_2$$
$$R_{z,1}(\theta)C = CR_{z,1}(\theta)$$
$$R_{x,2}(\theta)C = CR_{x,2}(\theta)$$

Measurement

Projective measurement in computational basis:

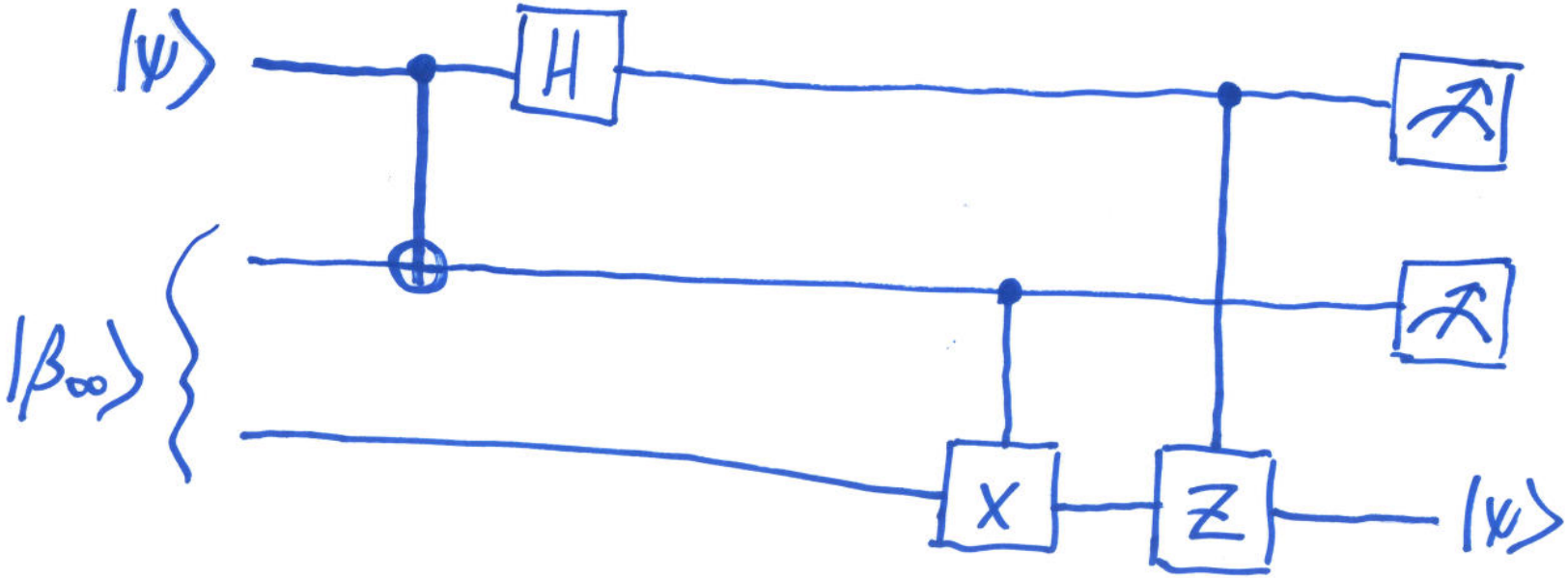


It is conventional to not use any special symbols to denote more general measurements, as they can always be represented by unitary transforms with ancilla qubits, then projective measurement

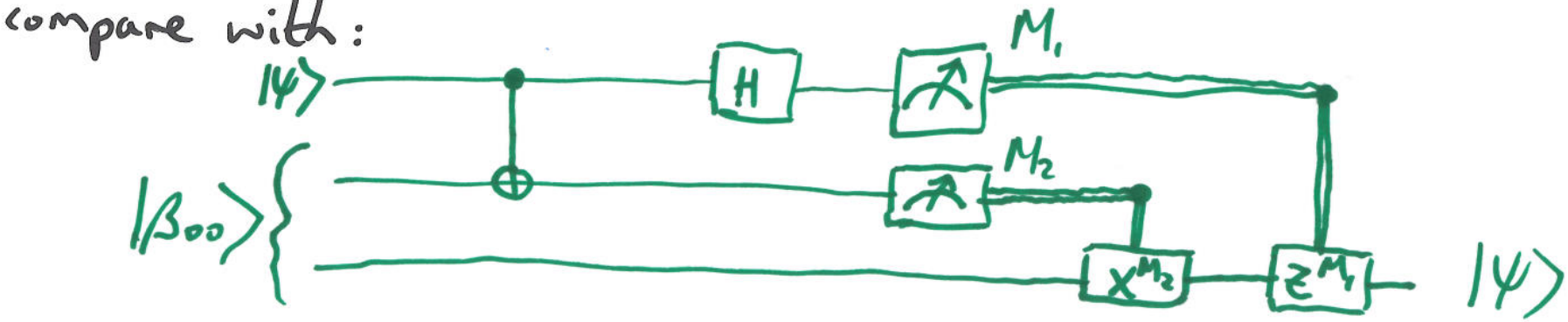
Principle of Deferred Measurement

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

"Teleportation" where classical conditional operations replaced by quantum conditional operations



compare with:



Principle of Implicit Measurement

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.

Measure then forget

Let ρ be the density matrix for a two qubit system.

Perform a projective measurement in the computational basis of the second qubit, where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ are projectors for the second qubit.

Then density matrix, ρ', after measurement, assuming the observer does not learn the measurement result, is

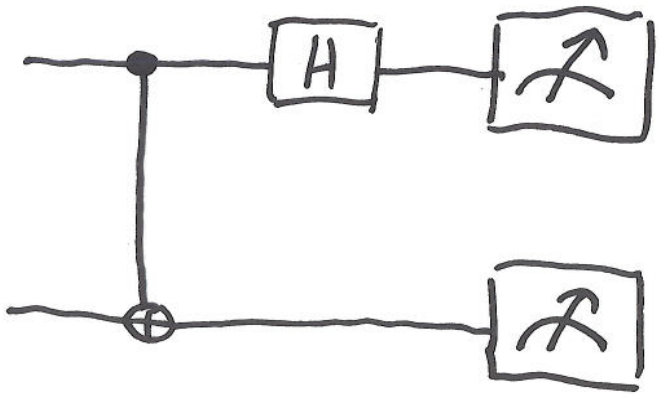
$$\rho' = P_0 \rho P_0 + P_1 \rho P_1.$$

In such a case, the reduced density matrix of the first qubit is not affected by the measurement. i.e., $tr_2(\rho) = tr_2(\rho')$.

Measurement in the Bell basis

We often want to perform a measurement in some orthonormal basis other than the computational basis.

e.g. w.r.t. the Bell basis:

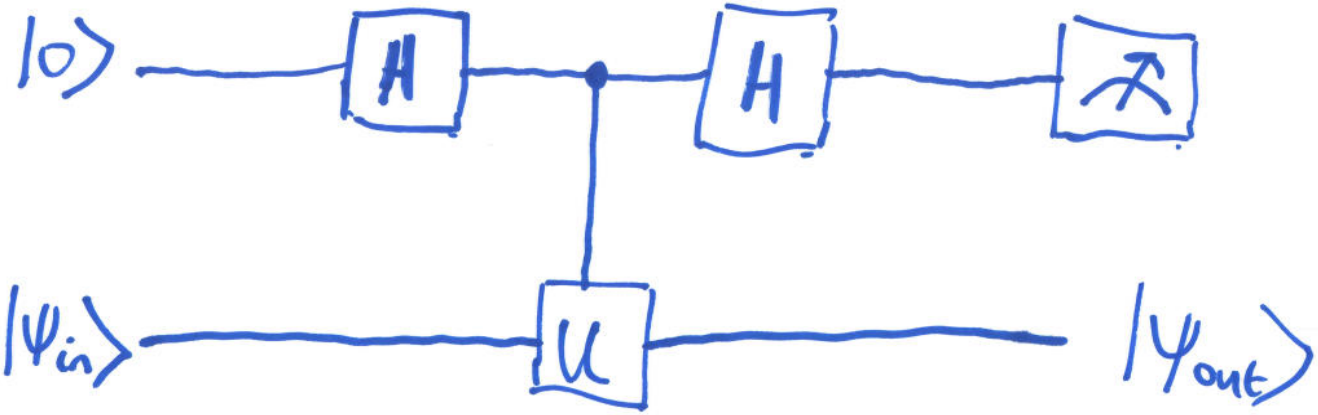


Measuring an Operator

Let U be a single qubit operator with eigenvalues ± 1, so that U is both Hermitian and unitary.

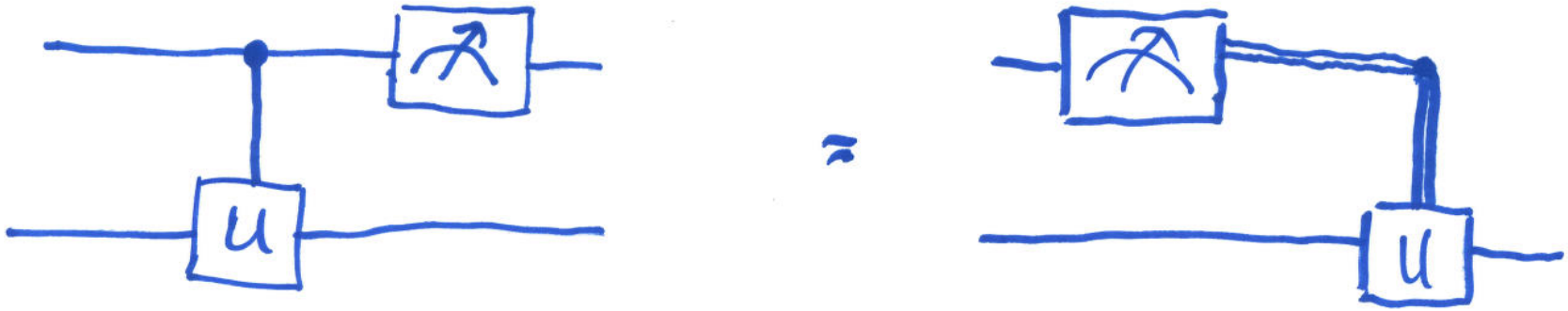
Therefore U can be regarded as both an observable and a quantum gate.

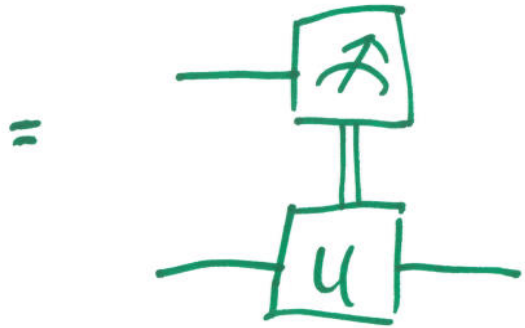
The following circuit measures the observable, U:



Measurement Commutes with Controls

... by the principle of defered measurement...





Universal Quantum Gates

A small set of gates (e.g. AND, OR, NOT) can be used to compute an arbitrary classical function.

.. such a set is **universal** for classical computation.

.... similarly ... a set of gates is **universal** for quantum computation if any unitary operation may be approximated **to arbitrary accuracy** by a circuit involving only those gates.

Universality

Any unitary operation can be approximated to arbitrary accuracy using Hadamard, CNOT, and T gates,

... where $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ ($\pi/8$ gate)

(phase gate, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, sometimes unnecessarily added to the above list.)

..... but how efficient are these implementations?

.... i.e. how many gates are required?

a polynomial number? an exponential number?

$\exists$ unitary transforms which require exponentially many gates to approximate.

Two-Level Unitary Gates are Universal

Let U be a unitary matrix acting on a d-dimensional Hilbert space.

Then U may be decomposed into a product of two-level unitary matrices

....i.e. matrices acting non-trivially on two-or-fewer vector components.

$U = 3 \times 3$

Let $U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$.

Find two-level unitaries, U_1, U_2, U_3, such that

$$U_3 U_2 U_1 U = I.$$

Then,

$$U = U_1^\dagger U_2^\dagger U_3^\dagger.$$

Procedure (a bit like Gaussian elimination)

1. Find U_1 such that

$$U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}$$

$$U_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{or} = \begin{bmatrix} \frac{a'}{\sqrt{|a'|^2+|c'|^2}} & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2. Find U_2 such that

$$U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & f'' \\ 0 & h'' & j'' \end{bmatrix}$$

$$U_2 = \begin{bmatrix} a''^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{or} = \begin{bmatrix} \text{something} \\ \text{messy} \end{bmatrix}$$

3. Find U_3 such that

$$U_3 U_2 U_1 U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{bmatrix}$$

More Generally...

Let U act on a d-dimensional space.

1. Find two-level unitaries $U_1, \ldots U_{d-1}$,
   such that, $U_{d-1} U_{d-2} \ldots U_1 U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{bmatrix}$

2. Repeat for U' .... etc..

$\Rightarrow$

$U = V_1 \ldots V_k$,

where V_i are two-level

and $k \leq (d-1) + (d-2) + \ldots + 1 = \frac{d(d-1)}{2}$

Decompose

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix},$$

into a product of two-level unitaries.

.... special case of Quantum Fourier Transform.

Corollary (of main result)

An arbitrary unitary matrix on an n qubit system may be written as a product of at most $2^{n-1}(2^n-1)$ two-level unitary matrices.

.... more efficient decompositions may exist.

... but there exist matrices which cannot be decomposed as a product of fewer than $d-1$ two-level unitaries.

Single Qubit and CNOT gates are universal

Consider an n-qubit Hilbert space.

Consider the two-dimensional space spanned by the computational basis states, $|s\rangle$ and $|t\rangle$.

Let U be a two-level unitary that acts non-trivially on the space spanned by $|s\rangle$ and $|t\rangle$.

Let $\tilde{U}$ be the non-trivial 2×2 unitary submatrix of U.

First of all, we wish to implement U, using single qubit and CNOT gates:

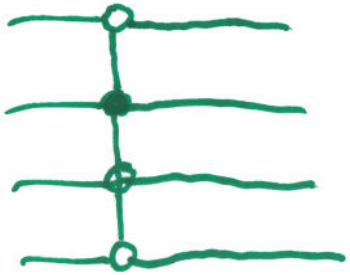
1. Effect state changes $|g_1\rangle \to |g_2\rangle \to \ldots |g_{m-1}\rangle$, where $wt(g_i \oplus g_{i+1}) = 1$.
2. Perform controlled-$\tilde{U}$. "Target" is bit-location of $g_i \oplus g_{i+1}$.
3. Effect $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \ldots |g_1\rangle$.

More Precisely

Let g_1 and g_2 differ at the ith bit.

Swap $|g_1\rangle$ and $|g_2\rangle$ by performing a controlled bit flip on the ith qubit, conditional on the values of the other qubits being identical to those in both g_1 and g_2.

e.g.



Do the same for g_i and g_{i+1}, to achieve:

$|g_1\rangle \rightarrow |g_{m-1}\rangle$

$|g_2\rangle \rightarrow |g_1\rangle$

$\vdots$

$|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle$

.... all other computational basis states are left unchanged!!

Example

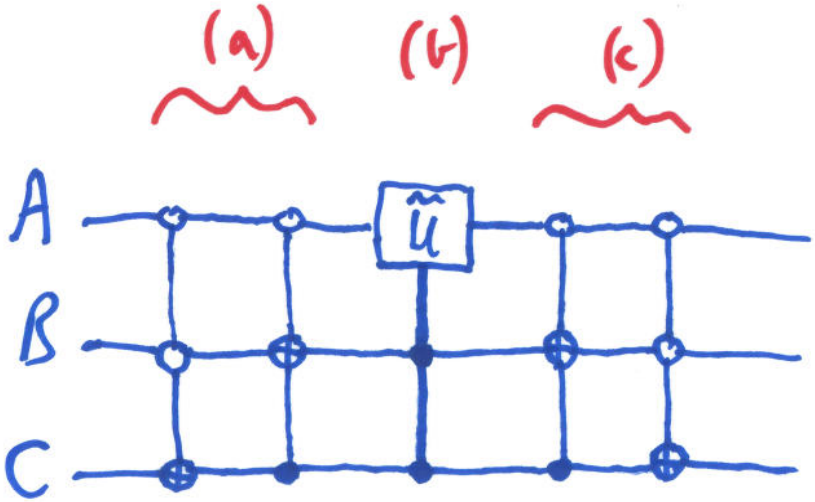
Let $U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & d & 0 \end{bmatrix}$ $\Rightarrow \tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$

U acts non-trivially on $|000\rangle$ and $|111\rangle$.

So form Gray code:

A	B	C
0	0	0
0	0	1
0	1	1
0	1	0
1	1	0
1	1	1
1	0	1
1	0	0

$\Rightarrow$



(a) Swap $|000\rangle$ with $|011\rangle$

(b) Apply $\tilde{U}$ to first qubit of $|011\rangle$ and $|111\rangle$

(c) Swap $|011\rangle$ with $|000\rangle$.

In General....

We require $2(n-1)$ controlled operations

...each requiring $O(n)$ single qubit and CNOT gates.

The controlled-$\tilde{U}$ requires $O(n)$ gates.

$\Rightarrow$ Implementing U requires $O(n^2)$ single qubit and CNOT gates

But,

An arbitrary unitary requires $O(4^n)$ two-level unitaries

$\Rightarrow$ An arbitrary unitary requires $O(n^2 4^n)$ single qubit and CNOT gates.

A Discrete Set of Universal Operations

No simple method known to implement CNOT and single qubit unitaries which are resistant to error.

..... so...

we determine a discrete set of gates

which will later be combined in an error-resistant fashion, using quantum error-correcting codes.

Approximating Unitary Operators

No discrete set of gates can exactly represent all unitaries

. . . . but . . .

a discrete set can approximate any unitary

the error when V is implemented instead of U is,

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$$

Meaning of $E(U,V)$

If M is a POVM element, and P_U (P_V) is the probability of obtaining this outcome if U (V) were performed, then,

$$|P_U - P_V| \leq 2E(U,V).$$

Approximation Errors

If $V_1, \ldots V_m$ approximate $U_1, \ldots U_m$,

then the errors add at most linearly,

$$E(U_m U_{m-1} \ldots U_1, V_m V_{m-1} \ldots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j).$$

For a circuit with m gates, then the probabilities of measurement outcomes are within tolerance $\Delta > 0$, if,

$$E(U_j, V_j) \leq \Delta / 2m.$$

Universality of Hadamard + CNOT + T gates

Consider T and HTH:

T is, (up to global phase), a rotation by $\pi/4$ radians around the $\hat{z}$ axis on the Bloch sphere.

HTH is a rotation by $\pi/4$ radians around the $\hat{x}$ axis on the Bloch sphere.

Composing gives (up to global phase),

$$e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \left[\cos\tfrac{\pi}{8}I - i\sin\tfrac{\pi}{8}Z\right]\left[\cos\tfrac{\pi}{8}I - i\sin\tfrac{\pi}{8}X\right]$$

$$= \cos^2\tfrac{\pi}{8}I - i\left[\cos\tfrac{\pi}{8}(X+Z) + \sin\tfrac{\pi}{8}Y\right]\sin\tfrac{\pi}{8}$$

$$\cos^2\frac{\pi}{8} I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8} Y\right]\sin\frac{\pi}{8}$$

= rotation on Bloch sphere along $\hat{n} = \left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$, through an angle θ, where $\cos\left(\frac{\theta}{2}\right) \equiv \cos^2\frac{\pi}{8}$.

$\Rightarrow$ Using only Hadamard and T gates we construct,

$$R_{\hat{n}}(\theta)$$

(remember:

$$R_{\hat{n}}(\theta) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\left(n_x X + n_y Y + n_z Z\right)$$

$$= e^{-i\theta \hat{n}\cdot\vec{\sigma}/2}\Big)$$

Observe: θ is an irrational multiple of 2π,

.... and so ....

Approximating $R_{\hat{n}}(\alpha)$

Repeated iteration of $R_{\hat{n}}(\theta)$ can approximate $R_{\hat{n}}(\alpha)$ to arbitrary precision.

Let $\delta > 0$, and N integer $> 2\pi/\delta$.

Let $\theta_k \in [0, 2\pi)$, and $\theta_k = (k\theta) \bmod 2\pi$.

$\exists j, k \in (1, \ldots N)$, such that,

$$|\theta_k - \theta_j| \leq 2\pi/N < \delta.$$

w.l.o.g., $k > j \Rightarrow |\theta_{k-j}| < \delta$. Since θ is irrational, $\theta_{k-j} \neq 0$.

$\Rightarrow$ the sequence $\theta_{l(k-j)}$ fills up $[0, 2\pi)$ as l varies, so that adjacent members are no more than δ apart. $\Rightarrow E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n\right) < \frac{\epsilon}{3}$