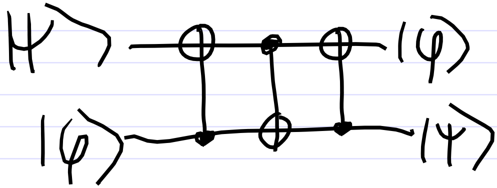
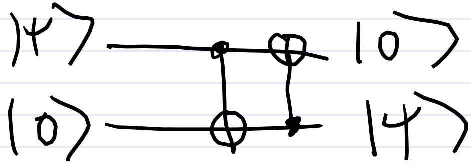
Lecture 23, 3 Dec 2020

Re last time, see arXiv:1202.5707 for factoring 15 (in 2012) using order 2 element "(pre-compiled)", $4^2 = 1 \bmod 15$

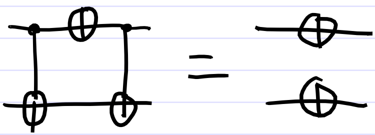
For teleportation, we'll need

General swap circuit reduces for $|\varphi\rangle = |0\rangle$ to:

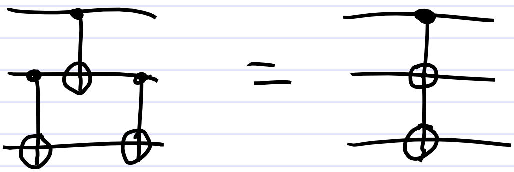




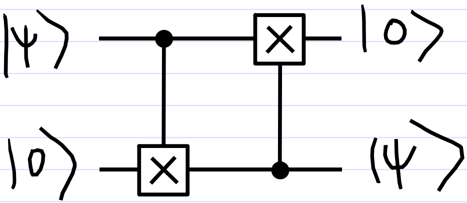
Also recall:



implies the controlled circuit identity

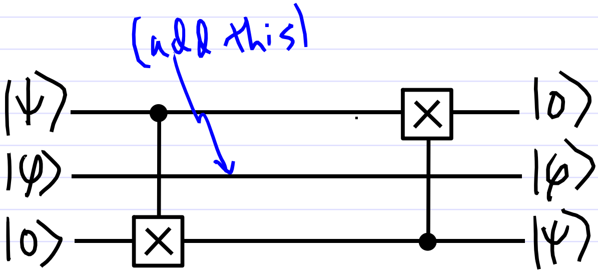


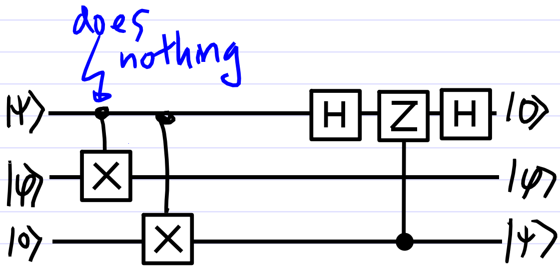
Start with

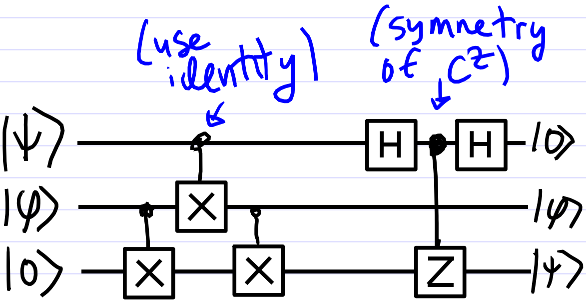


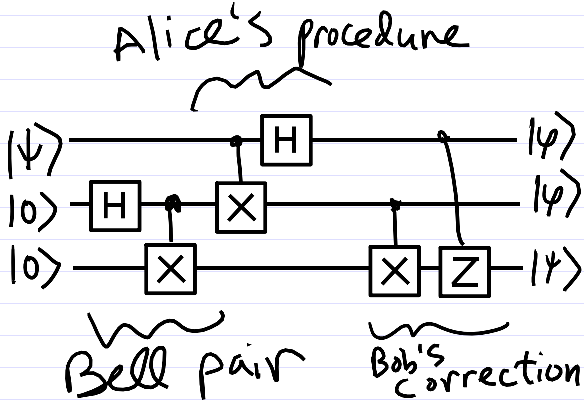
$$|\varphi\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

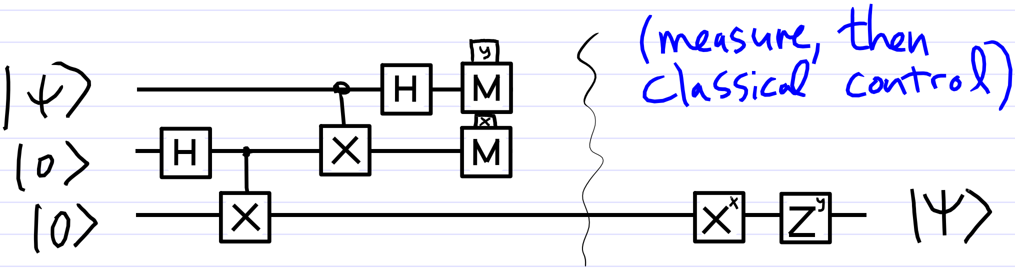
$$X|\varphi\rangle = |\varphi\rangle$$



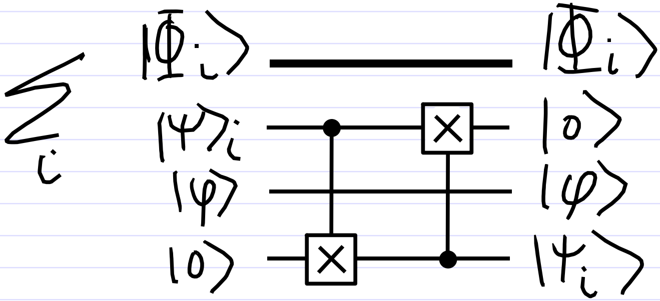


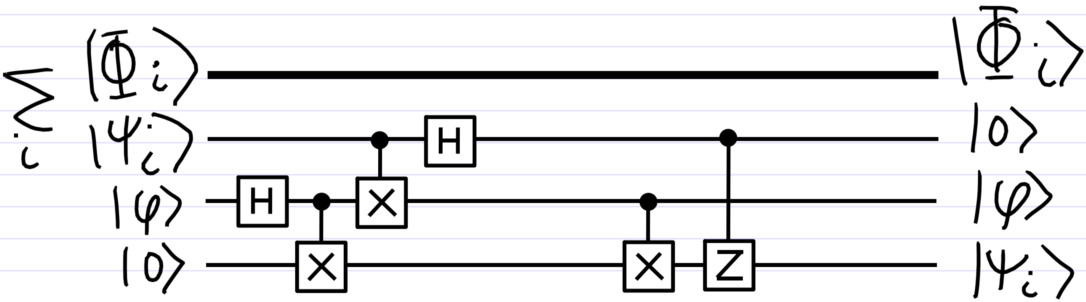




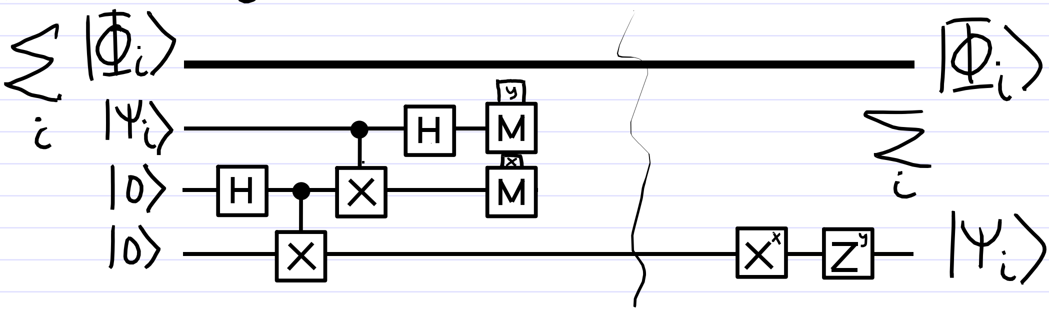


Now consider Alice's qubit is in some entangled state $\sum_i |\Psi_i\rangle_a |\Phi_i\rangle_{n-1}$:





(Same argument teleports entanglement)



arXiv:
1208.0928

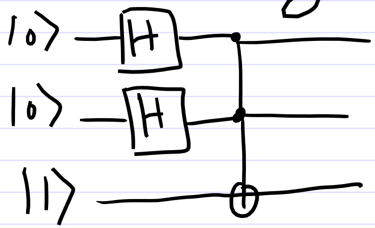
Number of computational logical qubits	Sequential Toffoli gates	Total Toffoli gates	References
$2N$	$40N^3$	$40N^3$	[35–37]
$5N$	$600N^2$	$\mathcal{O}(N^3 \log N)$	[38]
$2N^2$	$15N \log^2 N$	$\mathcal{O}(N^3 \log^2 N)$	[39]
$\mathcal{O}(N^3)$	$\mathcal{O}(\log^3 N)$	$\mathcal{O}(N^3 \log^3 N)$	[40]

TABLE I. Trade-off between number of computational logical qubits and number of sequential and total Toffoli gate operations for factoring an N-bit number into its primes using Shor's algorithm. Each line in the table corresponds to a different quantum circuit implementing the algorithm. The physical size of a circuit scales with the ratio of the total number of Toffoli gates to the number of sequential Toffoli gates.

We can make a rough estimate of the time and circuit size needed to factor a number with $N = 2,000$ bits (600 decimal digits), using a circuit size scaling as in the first line of Table I, and making assumptions about the physical qubit error rates and gate times; more details on this estimate are provided in Appendix M.[3] This Shor's algorithm implementation is constructed from ideas in Ref. [35–37], and involves a resource-intensive modular exponentiation that requires approximately $40N^3 \approx 3 \times 10^{11}$ sequential Toffoli gates. The modular exponentiation thus determines the total execution time for the factoring algorithm. A highly optimized version of this circuit [41] can complete each Toffoli gate in approximately three physical qubit measurement cycles. If we assume a physical qubit measurement time of 100 ns, it will take about 26.7 hours to complete the exponentiation.

In ps6 #6, saw that the state $|0\rangle - \boxed{H} - \boxed{T} - = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$ can be "teleported" to create a gate $T(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta e^{i\pi/4}|1\rangle$.

Similarly a state (possible to construct robustly)

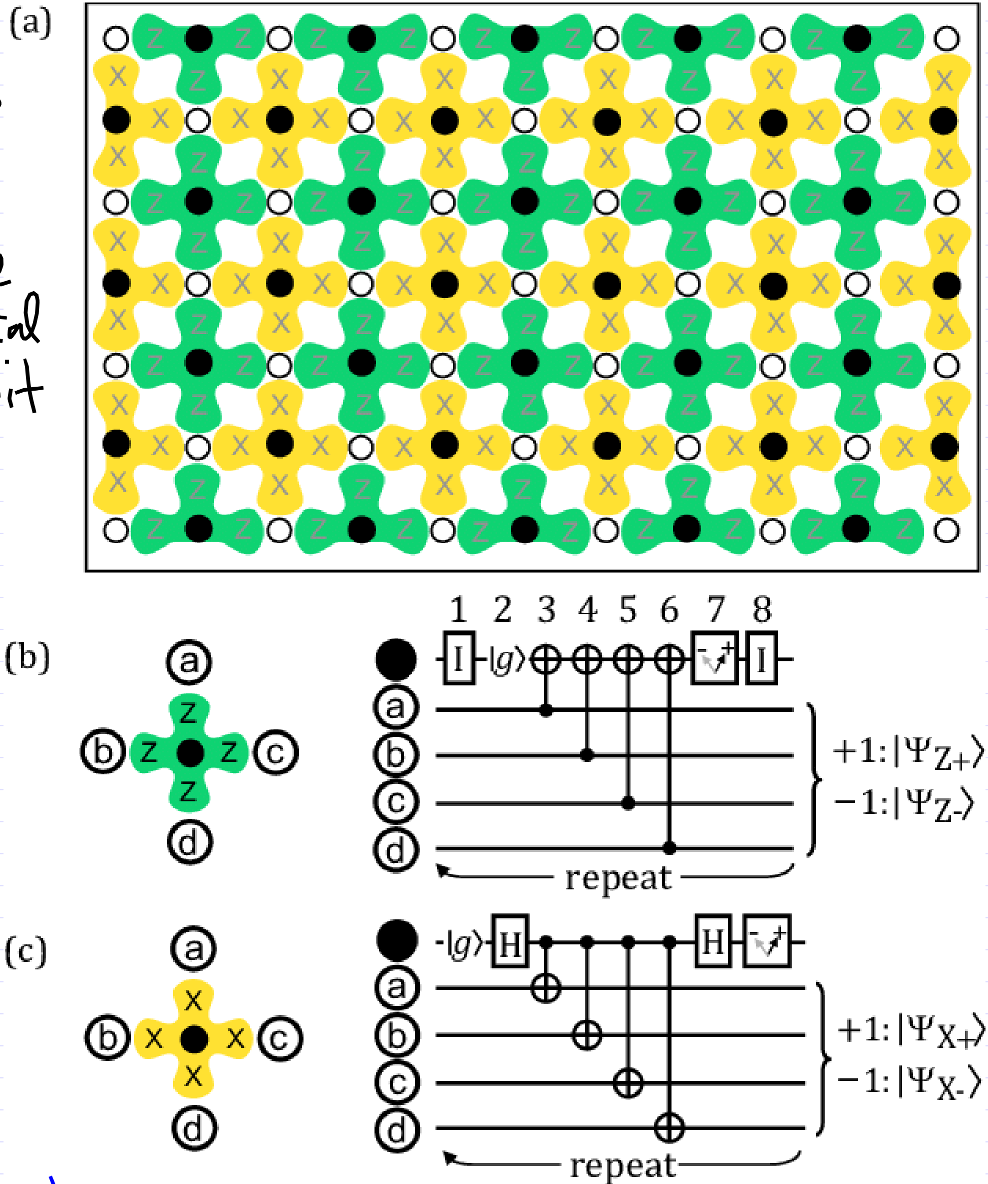


$$= \frac{1}{2}\left(|000\rangle + |010\rangle + |100\rangle + |111\rangle\right)$$

can be "teleported" to a state $|\psi\rangle_3$ (exchanging its $|110\rangle$ and $|111\rangle$ amplitudes) to create a general Toffoli gate. This turns out to be a fault-tolerant way to construct these gates.

This will all be one logical qubit

(a)



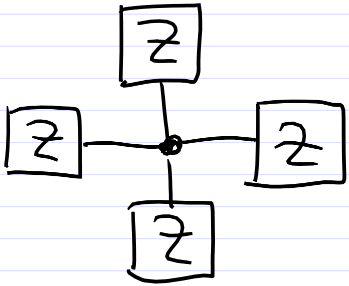
arXiv: 1208.0928

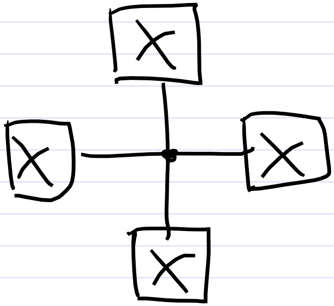
$2^{39}/2^{38} = 2$ φ

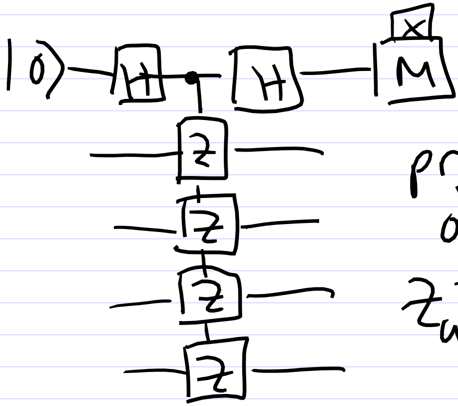
○ = "data" qubits

● = measurement qubits

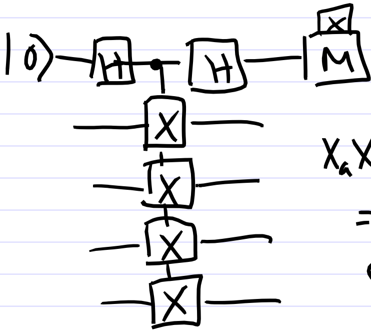
either measure $Z_a Z_b Z_c Z_d$ or $X_a X_b X_c X_d$ on neighboring qubits







projects onto $Z_a Z_b Z_c Z_d = (-1)^x$ eigenstate



$X_a X_b X_c X_d = (-1)^x$ eigenstate

each measurement reduces the dimension of the Hilbert space by a factor of 2.

Start with $4 \cdot 6 + 3 \cdot 5 = 39$ data qubits so 2^{39} dim space.

But $4 \cdot 5 + 3 \cdot 6 = 38$ measurement qubits so $2^{39} / 2^{38} = 2$

$\Rightarrow$ 1 logical qubit

For example, 2 qubits

$|00\rangle \; |01\rangle \; |10\rangle \; |11\rangle$

measure $Z_0 Z_1 = +1 \Rightarrow |00\rangle, |11\rangle$

$= -1 \Rightarrow |01\rangle, |10\rangle$

Joint eigenstates of
$Z_0 Z_1$ $X_0 X_1$ (they commute)

$Z_0 Z_1$	$X_0 X_1$	
1	1	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	-1	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
-1	1	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$
-1	-1	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

"Bell Basis"

For 4 qubits, there are eight $Z_a Z_b Z_c Z_d = +1$ eigenstates:

$|0000\rangle, |0011\rangle, \ldots, |1100\rangle, |1111\rangle$

(all with even # of 1's)

Similarly, eight $Z_a Z_b Z_c Z_d = -1$ eigenstates:

$|0001\rangle, |0010\rangle, \ldots, |1101\rangle, |1110\rangle$

(all with odd # of 1's)

Same for $X_a X_b X_c X_d$ in terms of $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

$+1$ $|++++\rangle, |++--\rangle, \ldots, |--++\rangle, |----\rangle$

-1 $|+++-\rangle, |--+-\rangle, \ldots, |--+-\rangle, |---+\rangle$

Now consider error syndromes

$$Z_a Z_b Z_c Z_d \; X_a |\psi\rangle$$

error
on qubit a

$$= -X_a Z_a Z_b Z_c Z_d |\psi\rangle = -X_a |\psi\rangle$$

(if started in +1 eigenstate)

Similarly

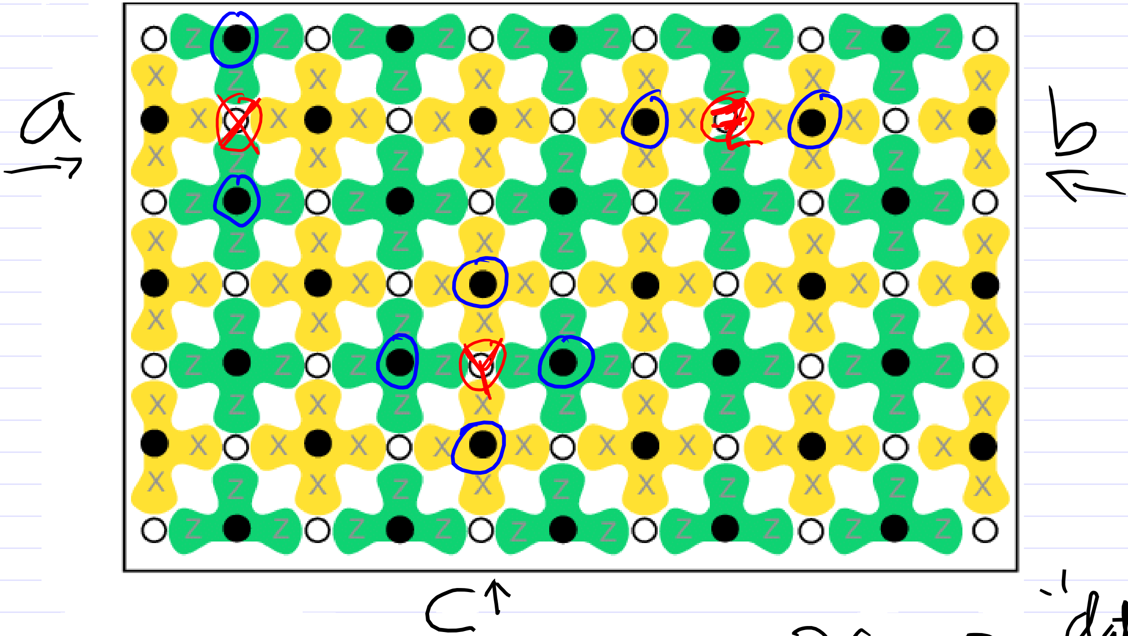
error on qubit b

$$X_a X_b X_c X_d \; Z_b |\psi\rangle$$

$$= -Z_b X_a X_b X_c X_d |\psi\rangle = -Z_b |\psi\rangle$$

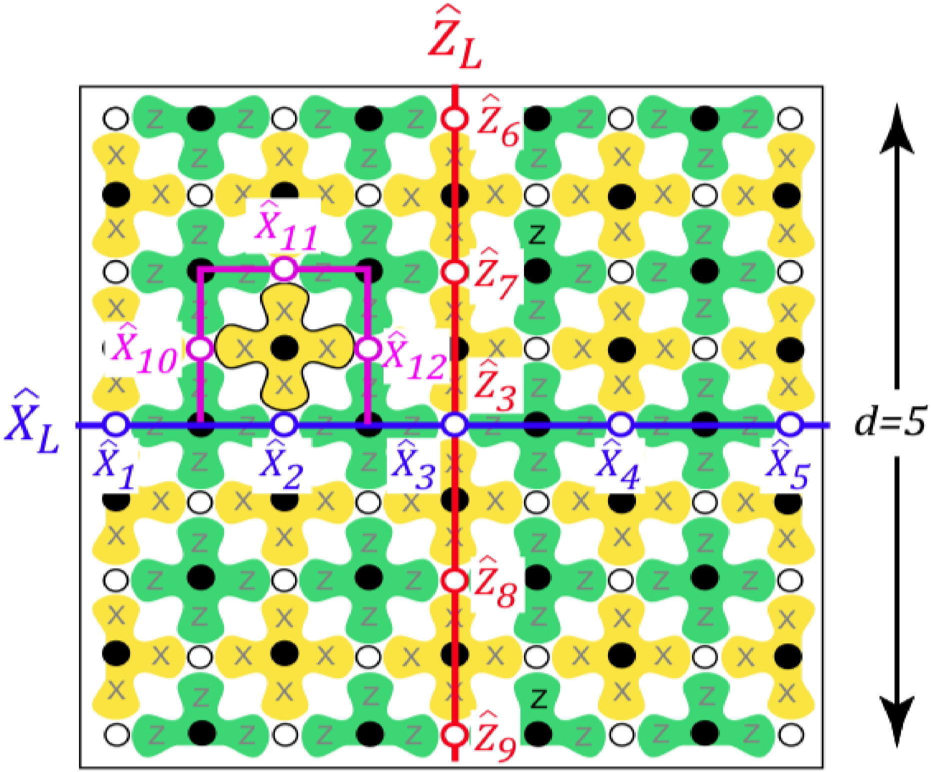
○ = flipped measurement value

○ = error on data qubit



a = X error
b = Z error
c = Y error

39 ○ "data"
38 ● "meas"
2 or 1 qubit



Still need logical operators

$\bar{X}_L$, $\bar{Z}_L$ satisfying

$\bar{X}_L^2 = \bar{Z}_L^2 = 1$, $\quad \bar{X}_L \bar{Z}_L = -\bar{Z}_L \bar{X}_L$