

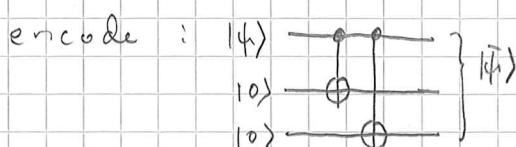
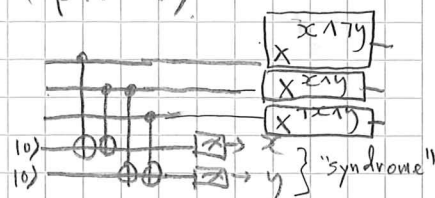
Quantum error correction, cont'd (§ 27.2)

Recap: protection against "bit flip"

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle \rightsquigarrow \alpha|1\rangle + \beta|0\rangle = |\psi_1\rangle$$

is given by 3-bit repetition for each qubit

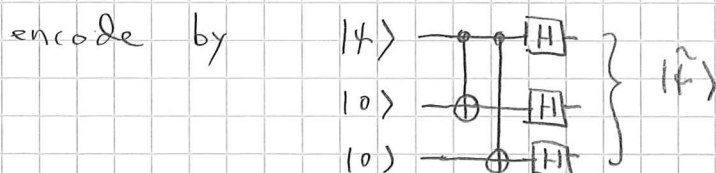
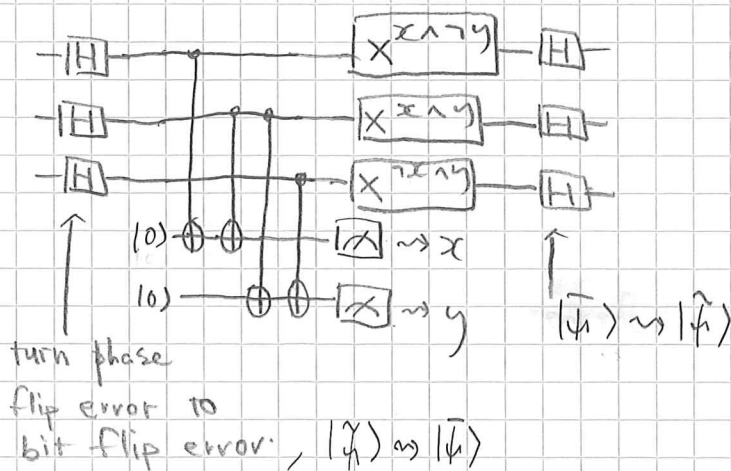
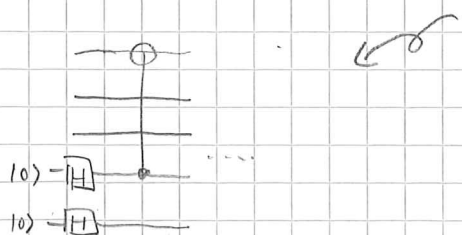
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightsquigarrow |\tilde{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle$$

error
detection
correctionTo protect against "phase flip" $\alpha|0\rangle + \beta|1\rangle \rightsquigarrow \alpha|0\rangle - \beta|1\rangle$

Note: the Hadamard gate interchanges bit flips to phase flips:

$$\text{bit flip of } |+\rangle, |-\rangle = |+\rangle, -|-\rangle$$

$$\text{phase flip of } |+\rangle, |-\rangle = |-\rangle, |+\rangle$$

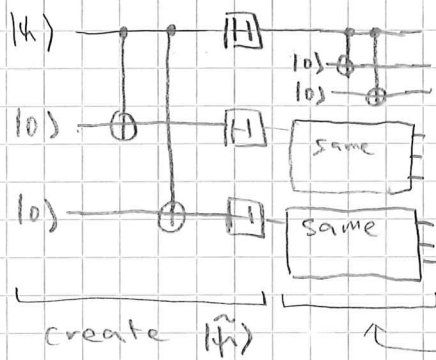
We can use $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightsquigarrow |\tilde{\psi}\rangle = \alpha|++\rangle + \beta|--\rangle$ error detection
correction by

Again this will not care about bit flip error.

we can combine two schemes (Shor's 9-qubit code)

$$|\hat{0}\rangle = \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}} \right)^{\otimes 3}, \quad |\hat{1}\rangle = \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}} \right)^{\otimes 3}$$

encoding circuit



$|\hat{0}\rangle = |+++ \rangle$ becomes

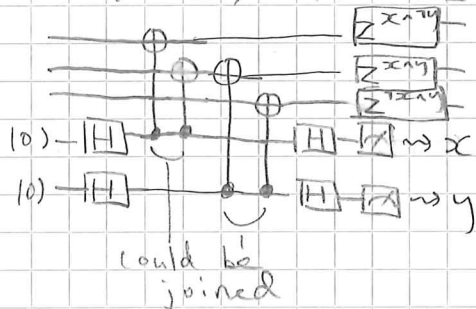
$$\frac{1}{\sqrt{2}}(|++\rangle \otimes |++\rangle \otimes |++\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes 3$$

$|\hat{1}\rangle = |--\rangle$ becomes

$$\frac{1}{\sqrt{2}}(|--\rangle \otimes |--\rangle \otimes |--\rangle) = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \otimes 3$$

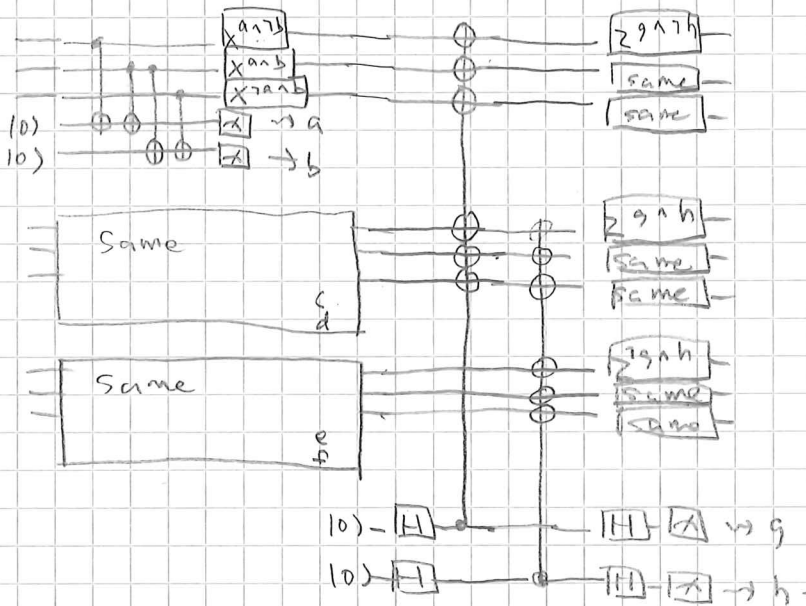
phase flip det/cor

$$H X H = Z, \quad H^2 = I_2$$



"syndrome"

error detection/correction for Shor's code



Quantum fault tolerance (§ 27.2.2)

Suppose we have a family of problems, with "size" given by N . (eg. "factor N ") and a quantum algorithm that solves this by $p(N)$ gates, $p(x)$: polynomial

Threshold theorem (quantum fault tolerance th'm)

Suppose each gate introduces "bad error" with probability δ .

If $\delta \ll 1$, we can find a arbitrary "better" circuit with $k \sim O(\text{poly}(\log(p(n)) \cdot p(n)))$ many gates.

Idea: replace each gate (error prob. δ) by composite of gates that work on encoded qubits. $\Rightarrow$ error prob. $\leq c\delta^2$ for some c .

(c depends on the coding scheme)
number of gates: d

"nesting" this: work with $\delta' = c\delta^2$ so

overall error prob. will be $c\delta'^2 = c^3\delta^4$

$\Rightarrow k$ -level nesting has $\begin{cases} c^{2^k-1} \delta^{2^k} \\ d^k \end{cases}$ error prob. gates.

there are $p(n)$ such big composite gates.

$\Rightarrow$ want $p(n) (c\delta)^{2^k} c^{-1} < \epsilon$ for desired error prob. ϵ

If $c\delta < 1$ this is possible.

$$d^k = \left(\frac{\log(p(n)/c\epsilon)}{\log(1/c\delta)} \right) \log d \sim O(\text{poly}(\log(p(n)/\epsilon)))$$

