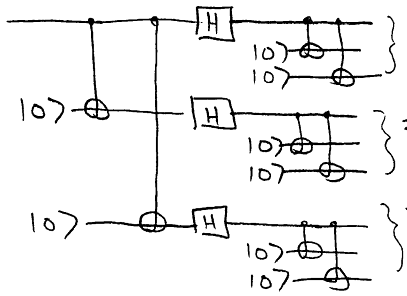
11/23/10 QIC 710 Lecture 21 CSS codes

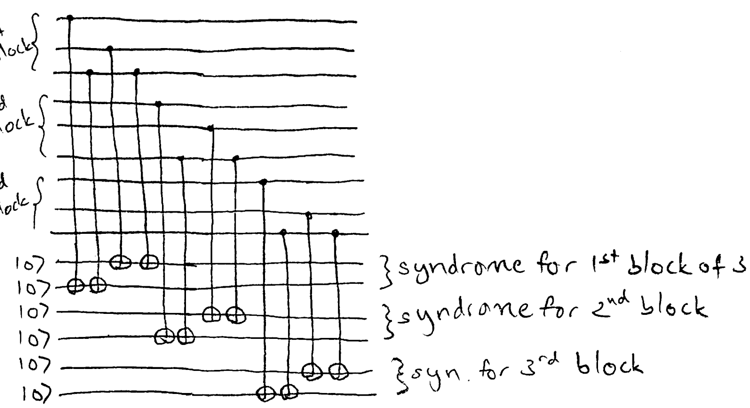
Recall: Shor's 9-qubit quantum error-correction code (QECC):

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\text{encoding}} \alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle) + \beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)$$

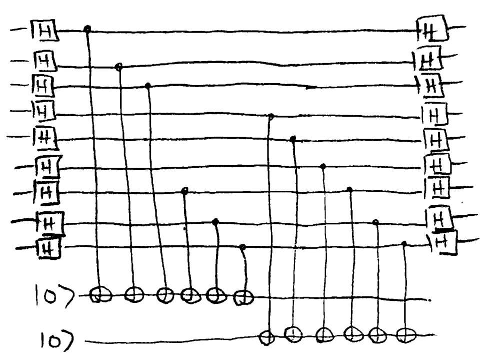
Encoding circuit:



X-error syndrome extraction:



Z-error syndrome extraction:



- X error syndrome suffices to identify (and therefore correct) up to one X error per block of 3
- Z error syndrome suffices to identify up to one Z error total

code can therefore correct an arbitrary quantum map on one qubit

CSS codes: a special case of quantum stabilizer codes (a generalization of classical linear codes) in which X and Z errors are protected against separately (as in Shor's code)

Classical linear codes

Def: An $[n,k]$ (classical) code is a subset $C \subseteq \{0,1\}^n$ of size $|C| = 2^k$. "It encodes k bits into n."

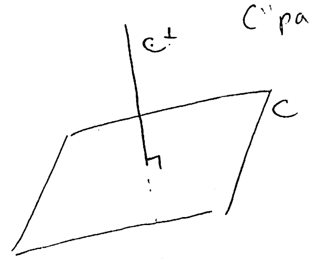
The distance of a code is the minimum Hamming distance between two distinct codewords in C, ie. the minimum number of positions in which two codewords differ.

Def.: A code is linear if it forms a linear subspace in $\{0,1\}^n = \mathbb{Z}_2^n$, ie., if it is closed under coordinate-wise addition mod 2.

Example: $C = \{000, 111\} \subset \{0,1\}^3$ is an $[n=3, k=1, d=3]$ linear code.

Observe: For a linear code C,

* $0^n \in C$ necessarily
* distance of C = minimum Hamming weight (# of 1s) of a nonzero element
* Being a linear subspace of size 2^k over $\mathbb{Z}_2$,
  - C can be specified by a basis, ie., a set of k linearly independent elements ("generators")
  - or it can equivalently be specified by a basis for $C^\perp$, ie., by a set of n-k linearly independent constraints ("parity checks") satisfied by each element of C.



Ex: The $[3,1,3]$ code is generated by $\{111\}$. Its codewords $c_1c_2c_3$ satisfy the parity checks

$$c_1 + c_3 = c_2 + c_3 = c_1 + c_2 = 0 \mod 2$$

The first two checks, $c_1 + c_3 = 0$, $c_2 + c_3 = 0$, are indep.

Write these constraints using ket notation

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sum_{c=0}^{1} (-1)^c |c\rangle\langle c| = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$Z \otimes I \otimes Z = \sum_{c_1, c_2, c_3 = 0}^{1} (-1)^{c_1 + c_3} |c_1 c_2 c_3\rangle\langle c_1 c_2 c_3|$$

$\Rightarrow$ $[3, 1, 3]$ codewords are $+1$-eigenvalue eigenstates of $Z \otimes I \otimes Z$ and $I \otimes Z \otimes Z$.

Recall: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle +| - |-\rangle\langle -| = HZH$

<u>Def</u>. A Calderbank-Shor-Steane (CSS) quantum code is the simultaneous $+1$ eigenspace of

- a set of parity checks in the computational $(|0\rangle, |1\rangle)$ basis, ie; of tensor products of I's and Z's.
- a set of parity checks in the dual/Hadamard basis $(|+\rangle, |-\rangle)$, ie., of tensor products of I's and X's.

Ex. 9

7

commute, syndrome

generate codewords

toric

<u>Example</u>: Shor's 9-qubit code is CSS. Each block of 3 satisfies the parity checks of the $[3, 1, 3]$ repetition code, ie.,

$$Z \otimes I \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$$
$$I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$$
$$I \quad I \quad I \quad Z \quad I \quad Z \quad I \quad I \quad I$$
$$I \quad I \quad I \quad I \quad Z \quad Z \quad I \quad I \quad I$$
$$I \quad I \quad I \quad I \quad I \quad I \quad Z \quad I \quad Z$$
$$I \quad I \quad I \quad I \quad I \quad I \quad I \otimes Z \otimes Z$$

States in the codespace further satisfy the two dual parity checks

$$X \quad X \quad X \quad I \quad I \quad I \quad X \quad X \quad X$$

and

$$I \quad I \quad I \quad X \quad X \quad X \quad X \quad X \quad X.$$

(Check this!)

<u>Observe</u>: The syndrome-extraction circuits given above are designed to read out these eight parity checks.
Any single X error can be identified by its pattern of Z syndromes.
Any Z error can be determined up to equivalence by the X parity checks.

Not coincidences: * Shor's code encodes one logical qubit into 9 physical qubits, and has $8 = 9-1$ independent parity checks ("stabilizers")

* The parity checks commute with each other (so they can be diagonalized simultaneously)

(A general "stabilizer code" is determined by commuting parity checks that are tensor products of Pauli operators, not necessarily with X and Z separate.)

Example Steane's 7-qubit code

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{encoding}} \alpha|0_L\rangle + \beta|1_L\rangle$$

where logical $|0\rangle$ and $|1\rangle$ are given by

$$|0_L\rangle = \frac{1}{\sqrt{8}}\Big[|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle$$
$$+ |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle\Big]$$

$$|1_L\rangle = X^{\otimes 7}|0_L\rangle$$

The parity checks are

$$IIIZZZZ \;,\quad IZZIIZZ \;,\quad ZIZIZIZ$$
$$IIIXXXX \;,\quad IXXIIXX \;,\quad XIXIXIX$$

these & XXXXXXX → generate C

(tensor products implied). (Check this!)

It corrects an arbitrary error on any one qubit. (Check this!)

Some interesting quantum stabilizer codes

[[number of physical qubits $= n$, number of logical qubits $= k$, distance $= d$]]

$= 2t+1$, $t =$ correctable # of errors

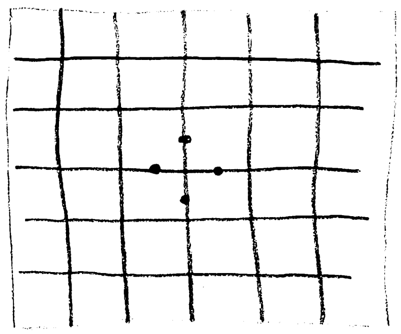
	n	k	d	
	4	2	2	[iaks-www.ira.uka.de/home/grassl/QECC/circuits]
	5	1	3	not CSS
Steane	7	1	3	
Shor	9	1	3	
Hamming	15	7	3	
Golay	23	1	7	
BCH	31	11	5	
Steane∘Steane	$49 = 7^2$	1	$9 = 3^2$	
⋮				
BCH	127	29	15	corrects up to 7 errors

Remark: While low n, high k, high d are good properties for quantum error-correcting codes, these are not necessarily the most important properties. More important is how easy the code is to work with: to prepare codewords, to extract syndromes, to compute on.

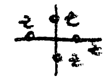
Example: A "low-density parity-check code" (LDPC code) has a low-weight set of parity checks $\Rightarrow$ syndrome extraction requires fewer CNOT gates.

For implementations, geometric locality is often key: parity checks should only involve nearby qubits.

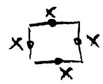
Toric code [Kitaev 9707021]: (sketch)



- one qubit per edge



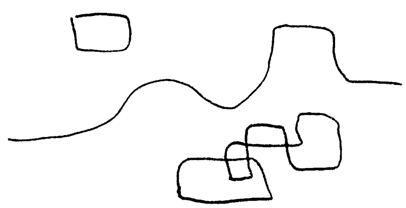
Z parity check for every vertex



X parity check for every face

- geometrically local! involving 4 qubits each

for a codeword to satisfy the Z parity checks, it must look like



i.e., a collection of cycles, where
1 = edge present
0 = absent edge
(since every vertex must have 0, 2 or 4 incident edges)

to satisfy the X parity checks, it must be an equal superposition over all such terms ...