Quantum Computation

Lectures 22-24

Classical linear codes and CSS quantum codes

Bit strings $X = x_1 \ldots x_n$ are vectors in a vector space over Z_2 (bitwise mod-2 addition and scalar multiplication).

M ← matrix of 0's and 1's

Mx

↑ ↑ ← column, not row vectors

classical bit transformations (gates)

Reversible gates are invertible; they permute the bit strings.

QM

$|x\rangle$ — basis vectors in a complex vector space

$A_M |x\rangle = |Mx\rangle$

$\langle y | A_M | x \rangle = \delta_{y, Mx}$

M reversible ⟺ A_M a permutation unitary

Code C is a map from k bits to n bits

$C(x) = y$ ← codeword

$[n, k]$ code

↑ k-bit column vector

↑ n-bit column vector

Linear code: $C(x) = Gx = y$

↑ $n \times k$ generator matrix

$G = (y_1 \cdots y_k)$

0 string is always encoded as 0 codeword

"basis codewords" for "basis strings," i.e., strings with a single 1

$y = Gx = \sum_j x_j y_j$ ← to get distinct codewords, these must be l.i. They span a k-dimensional subspace, which has 2^k codewords.

Examples:

① 3-bit repetition code: $G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ [3,1]

② 7-bit Hamming code: $G = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ [7,4]

The basis codewords span a k-dimensional subspace C; the codewords are the 2^k vectors in this subspace. A [n,k] linear code is a k-dimensional subspace in an n-dimensional binary vector space.

Swapping columns of G:
Replacing column w/ sum of two columns
} Leaves C same
Permutes codewords

Swapping rows of G: Changes C
Permutes codeword bits

Dual definition:

C is the null subspace of <u>parity-check matrix</u> H.

$$y \in C \iff y = Gx \iff \underbrace{Hy = 0}_{k \text{ linearly independent constraints}} \quad \forall y$$

on each row of H; H is a $(n-k) \times n$ matrix with l.i. rows

Swapping rows of H:
Replacing row w/ sum of two rows
} Leaves C same

Swapping columns of H: Changes C, permutes codeword bits

$$HGx=0 \ \forall x \iff HG=0 \iff G^T H^T = 0$$

$$H=\begin{pmatrix} z_1^T \\ \vdots \\ z_{n-k}^T \end{pmatrix} \qquad G=(y_1 \cdots y_k) \qquad HG=\begin{pmatrix} z_1^T y_1 & z_1^T y_2 & \cdots & z_1^T y_k \\ z_2^T y_1 & z_2^T y_2 & \cdots & z_2^T y_k \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-k}^T y_1 & z_{n-k}^T y_2 & \cdots & z_{n-k}^T y_k \end{pmatrix} = 0$$

$$(-1)^{z^T y} = (-1)^{z \cdot y} = \begin{pmatrix} \text{parity of bits } y_j \text{ for which } z_j = 1 \end{pmatrix} = \begin{pmatrix} \text{parity of } y \text{ relative to } z \end{pmatrix}$$

$$z^T y = z \cdot y = 0 \iff z \perp y$$

even relative parity

strings with an even # of 1s are self-orthogonal

$H \longrightarrow G$: pick $y_1, \ldots, y_k$ l.i. in kernel of H, i.e., pick $y_1, \ldots, y_k \perp$ to $z_1, \ldots, z_{n-k}$.

$G \longrightarrow H$: pick $z_1, \ldots, z_{n-k} \perp$ to $y_1, \ldots, y_k$, i.e., pick $z_1, \ldots, z_{n-k}$ l.i. in kernel of G^T.

Examples:

① 3-bit repetition code: $G=\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad H=\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

② 7-bit Hamming code:

$$G=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} & & & 1 \\ & & & \\ & & & \\ & & & \\ & H^T & & \\ & & & \\ & & & \\ & & & 1 \end{pmatrix} \qquad H=\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

How does it work? An error e is a vector with 1s in the position of bit flips:

$$y = Gx \xrightarrow[\text{error } e]{} y' = y \oplus e$$

Syndrome is constant on cosets of C considered as an additive group. $|C| = 2^k$, (# of cosets) $= 2^{n-k}$

$$Hy' = Hy \oplus He = He \leftarrow \text{Syndrome for error } e, \text{ indep. of codeword } y$$

($Hy = 0$)

If can diagnose error, easy to correct, $y' \oplus e = y$.

Examples

① 3-bit repetition code: $G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

	1	0	0	1	1	0	1
e	0	1	0	1	0	1	1
	0	0	1	0	1	1	1
	1	1	0	0	1	1	0
He	0	1	1	1	1	0	0

Generally the syndromes for single-bit errors are the columns of H, and the syndrome for a multi-bit error is the sum of the columns of H corresponding to the bits in error.

The syndromes form a $(n-k)$-dimensional "syndrome vector space." Can correct 1 error for each of the 2^{n-k} syndromes. (cosets)

② General Hamming codes: The syndromes for the n single-bit errors are the binary numbers from 1 to $n = 2^r - 1$, all of which fit into $r = n - k$ bits (one syndrome for no error). Syndromes for single-bit errors fill up the syndrome space.

$r=2,\ n=3,\ k=1$: $H=\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}$ 3-bit repetition code

$r=3,\ n=7,\ k=4$: $H=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}$

Hamming distance: $d(y,z) = \begin{pmatrix}\#\text{ of differences}\\ \text{between } y \text{ and } z\end{pmatrix} = \sum_j y_j \oplus z_j$

↑ not mod-2

Triangle inequality: $d(y,z)+d(z,w) \geq d(y,w)$

$$\left(\sum_j y_j \oplus z_j\right)+\left(\sum_j z_j \oplus w_j\right) = \sum_j y_j \oplus z_j + z_j \oplus w_j$$

$$\geq \sum_j y_j \oplus z_j \oplus z_j \oplus w_j$$

$$= \sum_j y_j \oplus w_j$$

$d(y\oplus w,\ z\oplus w) = d(y,z) \rightarrow d(y,z) = d(y\oplus z, 0)$

Weight: $w(y) = d(y,0) = \sum_j y_j$

$w(e) = \begin{pmatrix}\#\text{ of flips}\end{pmatrix}$

$w(e)$ even $\Leftrightarrow e^T e = 0$

$d(y,z) = d(y\oplus z, 0) = w(y\oplus z) \leq w(y) + w(z)$

↓

$\leq d(y,0) + d(0,z) = w(y) + w(z)$

Why important? If $e \in C$, $He = 0$, and it is clear the error cannot be corrected. If we want to correct low-weight errors, it is clear we need to make the codewords have high weight. This is formalized by

Code distance $d = d(C) = \min_{\substack{y,z \in C \\ y \neq z}} d(y,z) = \min_{\substack{y \in C \\ y \neq 0}} w(y)$

$[n,k,d]$ code

If $d(C) \geq 2t+1$, C can correct all errors on t or fewer bits.

Proof:

$y' = y \oplus e$, $w(e) \leq t$

$d(y',y) = w(y' \oplus y) = w(e) \leq t$

$d(y',z) \geq \underbrace{d(y,z)}_{\geq 2t+1} - \underbrace{d(y',y)}_{\geq -t} \geq t+1$ $\quad z \in C$

So all errors of weight $\leq t$ can be corrected by restoring to the nearest codeword

Suppose $He_1 = He_2$, with $w(e_1) \leq t$, $w(e_2) \leq t$

$\Rightarrow H(e_1 \oplus e_2) = 0 \Rightarrow e_1 \oplus e_2 \in C$

$2t \geq w(e_1) + w(e_2)$

$\geq w(e_1 + e_2)$

$\geq d$

$\geq 2t+1$ Contradiction.

Dual codes:

C	$[n,k]$	$C^\perp$	$[n,n-k]$
G	$n \times k$	$n \times (n-k)$ H^T	codewords $\perp$ to C
H	$(n-k) \times n$	$k \times n$ G^T	
$HG = 0$		$G^T H^T = 0$	

$C \subseteq C^\perp$ — Weakly self-dual ← even-parity (self-orthogonal) and mutually orthogonal codewords

$C = C^\perp$ — Self-dual

choose columns of E to make l.i. columns of $\mathcal{G}$

$$\mathcal{G} = (G \quad E) \qquad \mathcal{G}^T = \begin{pmatrix} G^T \\ E^T \end{pmatrix}$$

(G: k columns, E: $n-k$ columns)

$$\mathcal{H} = \begin{pmatrix} H \\ F \end{pmatrix} = \wedge \mathcal{G}^{-1} \qquad \mathcal{H}^T = (H^T \; F^T)$$

(H: $n-k$ rows, F: k rows)

$$\mathcal{H}\mathcal{G} = \begin{pmatrix} H \\ F \end{pmatrix}(G \quad E) = \begin{pmatrix} HG & HE \\ FG & FE \end{pmatrix} = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \equiv \wedge$$

(HG, HE: $n-k$ rows; FG, FE: k rows; HG, FE: k columns; HE, FG: $n-k$ columns)

$HE = I$ ← columns of E are errors whose C-syndromes are the standard basis

$G^T F^T = I$ ← columns of F^T are errors whose $C^\perp$-syndromes are the standard basis

$HG = 0$ ← C and $C^\perp$ are orthogonal

$FE = 0$ ← two sets of errors are orthogonal

Freedom:

① Columns of G (H^T) can be any l.i. vectors in C ($C^\perp$)

② Can add any vector in C ($C^\perp$) to any column of E (F^T).

③ Once G and E are picked, however, H and F are determined by $\mathcal{H} = \wedge \mathcal{G}^{-1}$

Examples

① 3-bit repetition code $[3,1,3]$

$$\mathcal{G} = \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{array}\right), \qquad \mathcal{H} = \left(\begin{array}{ccc|c} 1 & 1 & 0 & \\ 0 & 1 & 1 & \\ \hline 0 & 1 & 0 & \end{array}\right)$$

All Hamming codes are $d=3$.

② 7-bit Hamming code $[7,4,3]$ ← use NkC Ex. 10.20 on columns of H

$C^\perp$

$$\mathcal{G} = \left(\begin{array}{cccc|ccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}\right)$$

$$\mathcal{H} = \left(\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right)$$

The dual of the 7-bit Hamming code is $[7,3,4]$

use 10.20 on rows of G

$C \subset C^\perp$

Standard form

$(n-k)\times k$

$$H = (I_{n-k} \;\; A) \qquad G = \begin{pmatrix} A \\ I_k \end{pmatrix}$$

$$\mathcal{H} = \begin{pmatrix} I_{n-k} & A \\ 0 & I_k \end{pmatrix} \qquad \mathcal{G} = \begin{pmatrix} A & I_{n-k} \\ I_k & 0 \end{pmatrix}$$

CSS codes

Crucial fact from classical linear codes:

$$\sum_{z\in C} (-1)^{y\cdot z} = \begin{cases} |C| = 2^k, & y \in C^\perp \\ 0, & y \notin C^\perp \end{cases}$$

$y\cdot z = y^T z$

Proof: $\sum_{z\in C} (-1)^{y\cdot z} = \sum_{x\in\{0,1\}^k} (-1)^{y^T G\cdot x} = 0$ unless $y^T G = 0$

$z = Gx$

$G^T y = 0$

i.e., $y \in C^\perp$

$y \longrightarrow |y^T\rangle = |y\rangle$

C_1 $[n, k_1]$ G_1 $n \times k_1$, H_1 $(n-k_1) \times n$ — C_1 corrects up to t_1 errors

$C_2 \subset C_1$

C_2 $[n, k_2]$ G_2 $n \times k_2$, H_2 $(n-k_2) \times n$ — $C_2^\perp$ corrects up to t_2 errors

$k_2 < k_1$

Weakly self-dual code C

$C_2 = C \in C^\perp = C_1 = C_2^\perp$

Quantum code (logical) states:

$y, z \in C_1$ are equivalent if $\exists\ w \in C_2$ s.t. $y = z \oplus w$.

The equivalence classes are the cosets of C_2 in C_1.

$2^{k_1 - k_2}$ cosets

$$y \in C_1: \quad |\bar{y}\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} |y \oplus w\rangle$$

2^{k_2} terms in sum

one for each equivalence class (coset of C_2 in C_1)

$$\langle \bar{y} | \bar{y}' \rangle = \delta_{yy'} \quad \text{coset-wise}$$

$2^{k_1 - k_2}$ code states encoding $k_1 - k_2 = k$ logical qubits in n physical qubits

$[n, k]$ quantum code

Apply the crucial property:

$$H^{\otimes n}|\bar{y}\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} \frac{1}{\sqrt{2^n}} \sum_z (-1)^{z\cdot(y\oplus w)} |z\rangle$$

$$= \frac{1}{\sqrt{2^{n-k_2}}} \sum_z (-1)^{z\cdot y} |z\rangle \underbrace{\frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{z\cdot w}}$$

$$= \begin{cases} \sqrt{2^{k_2}}, & z \in C_2^\perp \\ 0, & z \notin C_2^\perp \end{cases}$$

$$= \frac{1}{\sqrt{2^{n-k_2}}} \sum_{z \in C_2^\perp} (-1)^{z\cdot y} |z\rangle$$

↑ 2^{n-k_2} terms in sum

Shifting y by $w \in C_2$ has no effect because $z \cdot w = 0$ if $z \in C_2^\perp$.

General errors:

e a bit-flip error, $\le t_1$ 1s in flip positions

$$X_e = \bigotimes_{j=1}^n X_j^{e_j}$$

f a sign-flip error, $\le t_2$ 1s in flip positions

$$Z_f = \bigotimes_{j=1}^n Z_j^{f_j}$$

$$|\bar{y}\rangle \otimes |0\rangle \otimes |0\rangle \xrightarrow{\chi_e Q_f \text{ errors}} \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{(y+w)\cdot f} |y \oplus w \oplus e\rangle \otimes |0\rangle \otimes |0\rangle$$

$H_1(y \oplus w \oplus e) = H_1 e$

$y \in C_1$

$w \in C_2 \subset C_1$

$y \oplus w \in C_1$

$n-k_1$ ancilla qubits to which we will write the $n-k_1$ parity checks H_1, performed using C-NOTs from the working qubits to the ancilla qubits

k_2 ancilla qubits to which we will write the k_2 parity checks G_2^T, performed using C-NOTs from the working qubits to the ancilla qubits

$$\xrightarrow{H_1 \text{ parity checks}} \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{(y+w)\cdot f} |y \oplus w \oplus e\rangle \otimes |H_1 e\rangle \otimes |0\rangle$$

Now correct the bit flips using the syndrome $H_1 e$ to apply appropriate C-NOTs to the working qubits, typically with multiple controls on the ancilla qubits

$$\xrightarrow{\text{bit-flip correction}} \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{(y+w)\cdot f} |y \oplus w\rangle \otimes |H_1 e\rangle \otimes |0\rangle$$

Now do Hadamards on all the working qubits to turn the phase flips into bit flips

$$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{(y+w)\cdot f} \frac{1}{\sqrt{2^n}} \sum_z (-1)^{(y+w)\cdot z} |z\rangle \otimes |H_1 e\rangle \otimes |0\rangle$$

$z' = z \oplus f$

$$= \frac{1}{\sqrt{2^{n_1}}} \sum_{z'} (-1)^{y \cdot z'} |z' \oplus f\rangle \otimes |H_1 e\rangle \otimes |0\rangle$$

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{w \cdot z'} = \begin{cases} 2^{k_2}, & z' \in C_2^{\perp} \\ 0, & z' \notin C_2^{\perp} \end{cases}$$

$$= \frac{(-1)^{\cdot}}{\sqrt{2^{n-k_2}}} \sum_{z \in C_2^{\perp}} (-1)^{y \cdot z} |z \oplus f\rangle \otimes |H_1 e\rangle \otimes |0\rangle$$

Now the sign flips have become bit flips

$G_2^T(z \oplus f) = G_2^T f$, $z \in C_2^{\perp}$

$\xrightarrow{G_2^T \text{ parity checks}}$ $$\frac{1}{\sqrt{2^{n-k_2}}} \sum_{z \in C_2^{\perp}} (-1)^{y \cdot z} |z \oplus f\rangle \otimes |H_1 e\rangle \otimes |G_2^T f\rangle$$

Now correct the sign flips using the syndrome $G_2^T f$ to apply appropriate C-NOTs to the working qubits, typically with multiple controls on the ancilla qubits

$\xrightarrow{\text{sign-flip Corrections}}$ $$\underbrace{\frac{1}{\sqrt{2^{n-k_2}}} \sum_{z \in C_2^{\perp}} (-1)^{y \cdot z} |z\rangle \otimes |H_1 e\rangle \otimes |G_2^T f\rangle}_{H^{\otimes n} |\bar{y}\rangle}$$

Apply Hadamards to the working qubits to restore the uncorrupted logical state

$$\xrightarrow[H^{\otimes n}]{} |\bar{y}\rangle \otimes \underbrace{|H_1 e\rangle \otimes |G_2^T f\rangle}$$

ancilla qubits are left holding the error syndromes, which could be read out by a measurement

Can correct all errors of the form $X_e Z_f$, where $w(e) \le t_1$ and $w(f) \le t_2$. This means that we can correct arbitrary errors on up to $t = \min(t_1, t_2)$ qubits.

An arbitrary single-qubit error can be written as a linear combination of I, X, Y, Z, so an arbitrary $\le t$-qubit error is a linear combination of Pauli products with at most t X, Y, Z's in each term. Each term is thus of the form $X_e Z_f$, $w(e) \le t$, $w(f) \le t$, and is corrected. By our general results, the linear combination of all the terms is also corrected.

Steane code

$C_1 = C = (7\text{-bit Hamming code}) \longleftarrow [7, 4, 3]$ $\quad k_1 = 4$

$C_2 = C^\perp \subset C_1^\perp$ $\quad C^\perp \in C$ $\quad k_2 = 3$

$k = k_1 - k_2 = 1$

$\uparrow$

$[7, 3, 4]$ classical code

$C_2^\perp \subset C_1 = C$ corrects $t = 1$ error, so our quantum code is a $[7, 1]$ code that corrects single-qubit errors.

$$G_1 = \begin{pmatrix} 0&0&1&1 \\ 0&1&0&1 \\ 0&1&1&1 \\ 1&0&0&1 \\ 1&0&1&1 \\ 1&1&0&1 \\ 1&1&1&1 \end{pmatrix} = H_2^\perp \qquad H_1 = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix} = G_2^\perp$$

Cosets of C_2 in C_1:

$$C_2 = \begin{pmatrix} 0&0&0&1&0&1&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&1&1&1&0&1&0 \\ 0&1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0&0 \\ 0&1&1&0&0&1&1&0 \\ 0&1&1&1&0&0&0&1 \end{pmatrix}$$

all codewords in C_2 except 0 have weight 4

$$C_2 \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1&1&1&0&1&0&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&1&0&0&0&1&0&1 \\ 1&0&1&1&0&1&0&0 \\ 1&0&1&0&0&0&1&1 \\ 1&0&0&1&1&0&0&1 \\ 1&0&0&0&1&1&1&0 \end{pmatrix}$$

all codewords here have weight 8, except the leftmost, which has weight 7

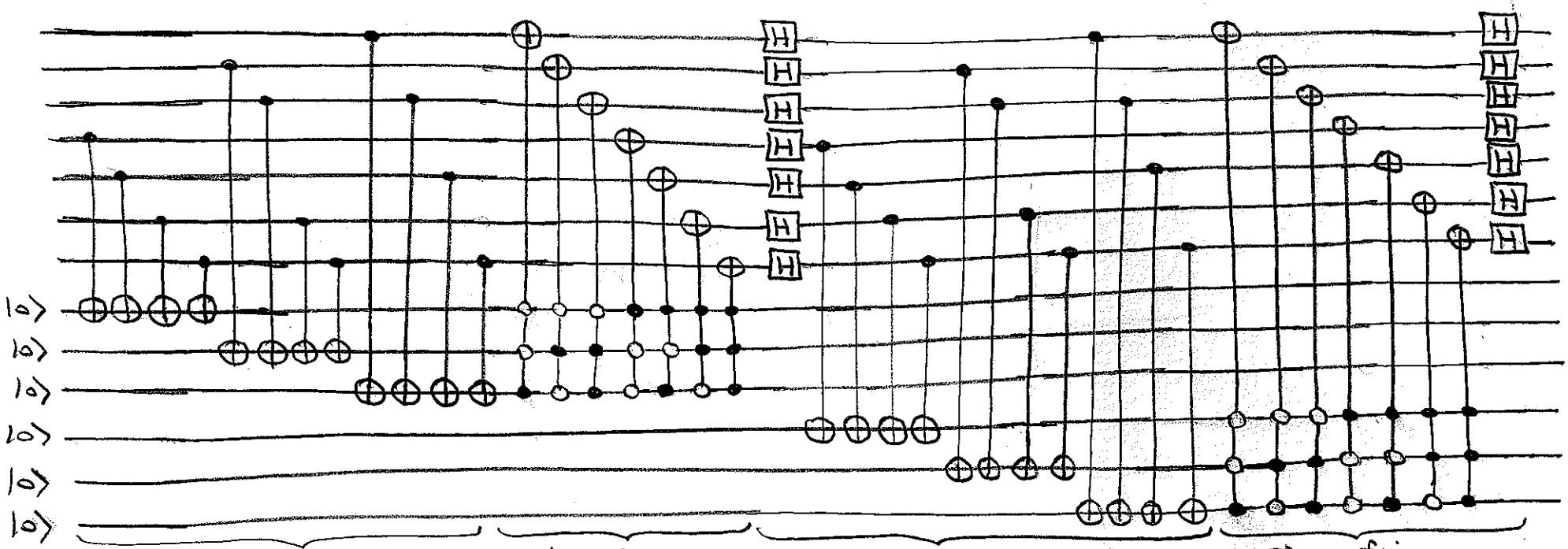
Logical basis states:

$$|\bar{0}\rangle = \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |0001111\rangle + |0110011\rangle + |1010101\rangle + |0111100\rangle + |1100110\rangle + |1011010\rangle + |1101001\rangle\big)$$

$$|\bar{1}\rangle = \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |1110000\rangle + |1001100\rangle + |0101010\rangle + |1000011\rangle + |0011001\rangle + |0100101\rangle + |1101001\rangle\big)$$

(5) Steane code:

Syndrome detection and correction



This last string of H's can be moved to here by changing the X's on the working qubits to Z's

Once the H's are moved, the bit-flip correction can be put after them.

The Steane code can correct all errors of the form

$$\bigotimes_{j=1}^{7} X_j^{e_j} \bigotimes_{k=1}^{7} Z_k^{f_k}, \qquad e \text{ and } f \text{ are single bit flips},$$

which means it can correct all single-qubit errors. It can also correct some two-qubit errors. Indeed, the number of errors it can correct is

$$(1 + 7) \times (1 + 7) = 64.$$

(1: no X; 7: X on any qubit; 1: no Z; 7: Z on any qubit)

These 64 errors are mapped to 64 $\perp$ 2-d subspaces, which fill the entire $2^7 = 128$ dimensional of the 7-qubit Hilbert space.