Encoding and decoding stabilizer codes :

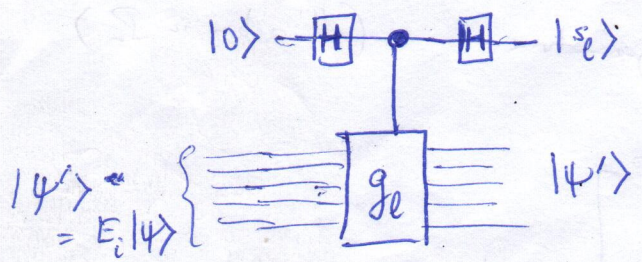
$S = \langle g_1, g_2, \ldots, g_{n-k} \rangle \leq \mathcal{P}_n$
a stabilizer group with indep generators g_ℓ.

Decoding first : As previously discussed, decoding via syndromes entails determining from $E_i|\psi\rangle$ (with $C(S)\backslash S$ and Q_S) the syndrome $\underline{s} = (s_1, s_2, \ldots, s_{n-k})$ of the error operator E_i.

Recall that $s_\ell = \begin{cases} 0 & \text{if } E_i \text{ commutes with } g_\ell \quad (\text{i.e., } E_i|\psi\rangle \text{ lies in the } (+1)\text{-eigenspace of } g_\ell) \\ 1 & \text{if } E_i \text{ anticommutes with } g_\ell \quad (\text{i.e., } E_i|\psi\rangle \text{ lies in the } (-1)\text{-eigenspace of } g_\ell) \end{cases}$

In principle, s_ℓ (for each $\ell \in \{1, \ldots, n-k\}$) can be determined by measuring the observable g_ℓ.

But here's a "simpler" quantum circuit for the same:



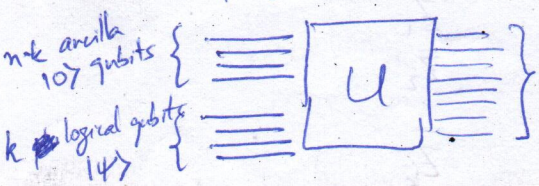
Exercise: Show that if $|\psi'\rangle$ lies in the $+1$-eigenspace of g_ℓ, then the output of this circuit is $|0\rangle|\psi'\rangle$; and if $|\psi'\rangle$ lies in the -1-eigenspace of g_ℓ, then the output is $|1\rangle|\psi'\rangle$.

[Solution: Let $g_\ell|\psi'\rangle = \lambda|\psi'\rangle$ where $\lambda \in \{+1, -1\}$. Then, easy computations will show that the output of the circuit is $\left(\frac{1+\lambda}{2}|0\rangle + \frac{1-\lambda}{2}|1\rangle\right)|\psi'\rangle = \begin{cases} |0\rangle|\psi'\rangle \text{ if } \lambda = +1 \\ |1\rangle|\psi'\rangle \text{ if } \lambda = -1 \end{cases}$.]

Encoding Q_S is an $[[n,k]]$ QSC.

~~Encoding is an operation ... converted into physical qubits lying inside the code space Q_S.~~

An encoder is a unitary operator that converts k logical qubits along with $n-k$ ancilla qubits (typically prepared in the $\underbrace{10\ldots0}_{n-k}\rangle$ state) into n physical qubits lying within the code space Q_S.



$|\varphi\rangle \in Q_S$.

To describe one particular method of encoding, we need the notion of

logical-X and logical-Z operators

called $\bar{X}$ $\bar{Z}$

Those operators belong to $C(S)\setminus S$ (recall that $E \in C(S)\setminus S$ takes $|\varphi\rangle \in Q_S$ to some $|\varphi'\rangle \in Q_S$)

and act like the standard X and Z operators on the k logical qubits, but on the n physical qubits of the code space.

$$|b_1 b_2 \cdots b_i \cdots b_k\rangle \xrightarrow{\text{Encoding}} |\varphi\rangle$$
$$\downarrow X_i \qquad\qquad \downarrow \bar{X}_i$$
$$|b_1 b_2 \cdots \bar{b}_i \cdots b_k\rangle \xrightarrow{\text{Encoding}} |\varphi'\rangle$$

$$|b_1 \cdots b_i \cdots b_k\rangle \xrightarrow{\text{Enc}} |\varphi\rangle$$
$$\downarrow Z_i \qquad\qquad \downarrow \bar{Z}_i$$
$$(-1)^{b_i} |b_1 \cdots b_i \cdots b_k\rangle \xrightarrow{\text{Enc}} |\varphi''\rangle$$

Existence / Construction of $\bar{X}$ and $\bar{Z}$ operators:

$S = \langle g_1, g_2, \ldots, g_{n-k} \rangle$ $n-k$ indep. generators (all action in P_n)

Check matrix representation

$$H = \left[\begin{array}{c|c} X(\underline{a}) & Z(\underline{b}) \\ \hline & \\ & \\ & \end{array}\right]_{(n-k)\times 2n}$$

Note that $X(\underline{a}')\,Z(\underline{b}') \in C(S)$ iff $[\underline{b}' \mid \underline{a}'] \in$ nullspace(H)

$\dim(\text{nullspace}(H)) = 2n - \text{rank}(H) = 2n - (n-k) = n+k.$

So, $C(S) \le P_n$ is a subgroup, having $n+k$ indep. generators

Of these $g_1, \ldots, g_{n-k}$ are mutually commuting operators.

The remaining $2k$ generators can be chosen so that they form "hyperbolic pairs" $(\bar{X}_i, \bar{Z}_i)$, $i = 1, 2, \ldots, k$

Each $\bar{X}_i$ (resp. $\bar{Z}_i$) commutes with all other generators, except $\bar{Z}_i$ (resp. $\bar{X}_i$)

g_1, g_2, $\ldots$, g_{n-k}

$\bar{X}_1$ $\bar{Z}_1$

$\bar{X}_2$ $\bar{Z}_2$

$\bar{X}_k$ $\bar{Z}_k$

(An explanation for this will be given in the lectures on EAQECCs)

To explicitly describe the construction of the $\bar{X}_i$ and $\bar{Z}_i$ generators, we bring the check matrix H into "standard form"

[This ~~description~~ procedure is due to Gottesmann in his 1997 PhD thesis]

Note that a pair of generators g_i, g_j can be replaced by $(g_i, g_i g_j)$

In the $(\underline{a}, \underline{b})$ vector representation, this is equivalent to replacing $(\underline{a}, \underline{b}) \leftarrow g_i$, $(\underline{a}', \underline{b}') \leftarrow g_j$ by $(\underline{a}, \underline{b}) \leftarrow g_i$, $(\underline{a} \oplus \underline{a}', \underline{b} \oplus \underline{b}') \leftarrow g_i g_j$.

Thus, we can perform elementary row operations on the check matrix without disturbing/changing the group, S, that the resulting operator ~~gates~~ generate.

$$H = \begin{matrix} n-k \text{ rows} \\ \{ \end{matrix} \left[\begin{array}{c:c} \overbrace{\quad}^{n \text{ cols}} & \overbrace{\quad}^{n \text{ cols}} \end{array}\right] \xrightarrow{\text{row reduction}} \begin{matrix} r \\ n-k-r \end{matrix} \left\{\begin{array}{c} \overset{r}{\cdots} \quad \overset{n-r}{\cdots} \quad \overset{r}{\cdots} \quad \overset{n-r}{\cdots} \\ \left[\begin{array}{cc:cc} I & A & B & C \\ 0 & 0 & D & E \end{array}\right] \end{array}\right.$$

(plus possible permutation of columns; the X-columns and the Z-columns need to be permuted in exactly the same way to preserve symplectic products)

Next, apply row reduction to the E part: (let $\text{rank}(E) = n-k-r-s$)

$$\begin{matrix} r \\ n-k-r-s \\ s \end{matrix} \left\{\begin{array}{c} \overset{r}{\cdots} \quad \overset{n-k-r-s}{\cdots} \quad \overset{k+s}{\cdots} \quad \overset{r}{\cdots} \quad \overset{n-k-r-s}{\cdots} \quad \overset{k+s}{\cdots} \\ \left[\begin{array}{ccc:ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D_1 & I & E_2 \\ 0 & 0 & 0 & D_2 & 0 & 0 \end{array}\right] \end{array}\right.$$

But in order for the first r rows above to have zero symplectic product with the last s rows, we must have $D_2 = 0$, which essentially means that $s = 0$.

Thus, we can bring the check matrix into the following "standard form"

$$\begin{matrix} r \\ n-k-r \end{matrix} \left\{\begin{array}{c} \overset{r}{\cdots} \quad \overset{n-k-r}{\cdots} \quad \overset{k}{\cdots} \quad \overset{r}{\cdots} \quad \overset{n-k-r}{\cdots} \quad \overset{k}{\cdots} \\ \left[\begin{array}{ccc:ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \end{array}\right] \end{array}\right. \leftarrow \text{these generators only have a } Z \text{ part.}$$

Now, let us identify the $\bar{X}$ operators first ($\bar{Z}$ operators next) in the nullspace of the "standard form" H.

Generically, the vector form of each $\bar{X}$ operator will be $[u_1\ u_2\ u_3 \vdots v_1\ v_2\ v_3]$ (blocks: r, $n-k-r$, k, r, $n-k-r$, k)

Note however that any $M \in C(S) \setminus S$ can be replaced by $g_l \cdot M$, also in $C(S) \setminus S$.

Thus, using the identity matrices in the std-form check matrix, we can reduce a generic $\bar{X}$ operator to bring it into the form

$$[0\ u_2\ u_3 \vdots v_1\ 0\ v_3].$$

Such an $\bar{X}$ must satisfy

$$\begin{bmatrix} I & A_1 & A_2 & \vdots & B & C_1 & C_2 \\ 0 & 0 & 0 & \vdots & D & I & E \end{bmatrix} \begin{bmatrix} v_1^T \\ 0^T \\ v_3^T \\ \hline 0^T \\ u_2^T \\ u_3^T \end{bmatrix} = \underline{0}.$$

i.e.,
$$\begin{aligned} v_1^T + A_2 v_3^T + C_1 u_2^T + C_2 u_3^T &= \underline{0} \\ u_2^T + E u_3^T &= \underline{0}. \end{aligned}$$

To obtain k $\bar{X}$ operators in one go, we need to construct a $k \times 2n$ matrix $[0\ U_2\ U_3 \vdots V_1\ 0\ V_3]$ ← "$\bar{X}$ matrix"

such that
$$\begin{aligned} V_1^T + A_2 V_3^T + C_1 U_2^T + C_2 U_3^T &= 0 \\ U_2^T + E U_3^T &= 0 \end{aligned}$$
| all modulo-2 arithmetic

Moreover, since the symplectic products between the rows of the "$\bar{X}$ matrix" must be 0, we also have

$$U_3 V_3^T = V_3 U_3^T$$

One choice of U_2, U_3, V_1, V_3 that will work is:

$$U_3 = I, \quad V_3 = 0, \quad U_2 = E^T, \quad V_1 = E^T C_1^T + C_2^T.$$

(Other choices are also possible, but we will stick to this one for further development.)

Thus, the $\bar{X}$ matrix is $\left[\begin{array}{ccc|ccc} 0 & E^T & I & E^T C_1^T + C_2^T & 0 & 0 \end{array}\right]$

Next, for the $\bar{Z}$ operators ... (given a set of $\bar{X}$ operators, these are uniquely defined, up to multiplication by operators in S.)

As argued for $\bar{X}$

$\bar{Z}$ matrix can be taken to be of the form $\left[\begin{array}{ccc|ccc} 0 & U_2' & U_3' & V_1' & 0 & V_3' \end{array}\right]$

Since the $\bar{Z}$ operators also arise from vectors in the nullspace of H, we must have

$$V_1'^T + A_2 V_3'^T + C_1 U_2'^T + C_2 U_3'^T = 0$$

$$U_2'^T + E U_3'^T = 0$$

Commutativity with $\bar{Z}$: $U_3' V_3'^T = V_3' U_3'^T$.

$(\bar{X}_i, \bar{Z}_i)$ hyperbolic pairs: $U_3' V_3^T + V_3' U_3^T = I$.

Since $U_3 = I$, $V_3 = 0$, the last equation above yields $V_3' = I$.

This, from the commutativity equations, yields $U_3' = U_3'^T$.

We can eliminate the X-part from all $\bar{Z}$ operators (this is a valid choice to make) by setting $U_2' = U_3' = 0$.

Thus,

$\bar{Z}$ matrix is $\left[\begin{array}{ccc|ccc} 0 & 0 & 0 & A_2^T & 0 & I \end{array}\right]$

Exercise (4): For the 7-qubit Steane code, bring the H matrix into std form and identify the $\bar{X}$ and $\bar{Z}$ operators.

For encoding purposes, since encoding must be a linear operator, it suffices to have a means of producing encoded states for $|b_1 b_2 \dots b_k\rangle$, $b_i \in \{0,1\}\ \forall i$

In fact, given the logical-X operators $\bar{X}_1, \bar{X}_2, \dots, \bar{X}_k$,

it suffices to have a means of producing an encoded state $|\varphi\rangle$ for $\underbrace{|0\dots0\rangle}_{k \text{ qubits}}$.

Indeed,

$$\begin{array}{ccc} \underbrace{|0\dots0\rangle}_{k \text{ qubits}} & \xrightarrow{\text{Enc}} & |\varphi\rangle \\ \Big\downarrow X_1^{b_1} X_2^{b_2} \dots X_k^{b_k} & & \Big\downarrow \bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} \\ |b_1 b_2 \dots b_k\rangle & \xrightarrow{\text{Enc}} & |\varphi'\rangle \end{array}$$

For $|0\dots0\rangle$, we will find it convenient to use the encoded state

$$\underbrace{\left(\frac{1}{|S|}\sum_{M \in S} M\right)}_{\text{projector onto } Q_S} \underbrace{|00\dots0\rangle}_{n \text{ qubits}} =: |\bar{0}\rangle$$

Then, $|b_1 b_2 \dots b_k\rangle$ is encoded as $\bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} |\bar{0}\rangle$

See Enc-9 page for an argument that shows that the states $\bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} |\bar{0}\rangle$ are mutually orthogonal as $(b_1 \dots b_k)$ ranges over $\{0,1\}^k$.

The $\bar{X}_i^{b_i}$ operations can be realized through controlled $\bar{X}_i$ operators, where $|b_i\rangle$ acts as the control qubit.

However, the projector $\frac{1}{|S|}\sum_{M \in S} M$ is not a unitary operation. (It is not invertible, as it projects $\mathbb{C}^{2^n}$ onto a 2^k-dim'l subspace Q_S.)

Some simplifications are possible:

$$|b_1 b_2 \dots b_k\rangle \longmapsto \bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} \left(\frac{1}{|S|}\sum_{M \in S} M\right) |00\dots0\rangle \quad (n \text{ qubits})$$

$$= \left(\frac{1}{|S|}\sum_{M \in S} M\right) \bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} |00\dots0\rangle$$

$$\propto (I+g_1)(I+g_2)\dots(I+g_{n-k})\, \bar{X}_1^{b_1} \bar{X}_2^{b_2} \dots \bar{X}_k^{b_k} |00\dots0\rangle$$

Since the $\bar{X}_i$ operators commute with all operators in S

Some simplifications are possible:

n physical qubits

$$|b_1 b_2 \cdots b_k\rangle \longmapsto \bar{X}_1^{b_1} \bar{X}_2^{b_2} \cdots \bar{X}_k^{b_k} \underbrace{\left(\frac{1}{|S|}\sum_{M\in S} M\right)}_{\text{write this as } \frac{1}{|S|}(I+g_1)(I+g_2)\cdots(I+g_{n-k})} |00\ldots0\rangle$$

$$\propto \bar{X}_1^{b_1} \bar{X}_2^{b_2} \cdots \bar{X}_k^{b_k} (I+g_1)(I+g_2)\cdots(I+g_r)(I+g_{r+1})\cdots(I+g_{n-k}) |00\ldots0\rangle$$

$$= \bar{X}_1^{b_1} \bar{X}_2^{b_2} \cdots \bar{X}_k^{b_k} (I+g_1)(I+g_2)\cdots(I+g_r)\,|00\ldots0\rangle$$

since for $j > r$, g_j is composed only of I and Z operators, which have no influence on $|00\ldots0\rangle$.

Since the $\bar{X}_i$ operators commute with all the $(I+g_j)$ operators

$$\cdot = \prod_{j=1}^{r}(I+g_j) \prod_{i=1}^{k} \bar{X}_i^{b_i} |00\ldots0\rangle$$

Next, observe that from the form of the $\bar{X}$ matrix, each $\bar{X}_i$ is of the form

$M_{i,1} \otimes \ldots \otimes M_{i,n}$, with $M_{i,\ell} \in \{I, Z\}$ for $1 \le \ell \le r$

These $M_{i,\ell}$'s have no effect on $|0\rangle$, so can effectively be replaced by I's:

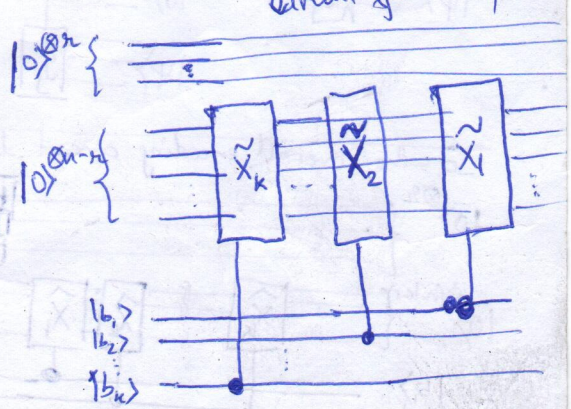
$$\underbrace{I \otimes \ldots \otimes I}_{I^{\otimes r}} \otimes \underbrace{M_{i,r+1} \otimes \ldots M_{i,n}}_{=:\tilde{X}_i}$$

Then,

$$\prod_{j=1}^{r}(I+g_j) \prod_{i=1}^{k} \bar{X}_i^{b_i} |00\ldots0\rangle = \prod_{j=1}^{r}(I+g_j) \left(I^{\otimes r} \otimes \tilde{X}_i^{b_i}\right)|00\ldots0\rangle$$

$$= \prod_{j=1}^{r}(I+g_j) \left(\underbrace{|0\ldots0\rangle}_{r} \otimes \prod_{i=1}^{k} \tilde{X}_i^{b_i} \underbrace{|0\ldots0\rangle}_{n-r} \right)$$

Circuit for this part

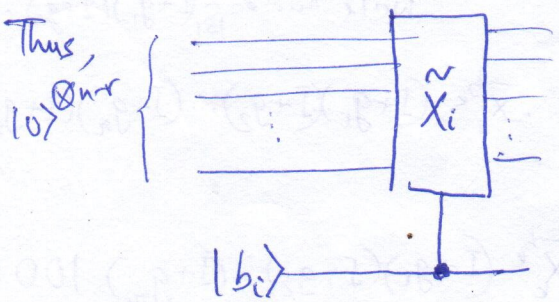


Next ... how to realize $\prod_{j=1}^{r}(I+g_j)$

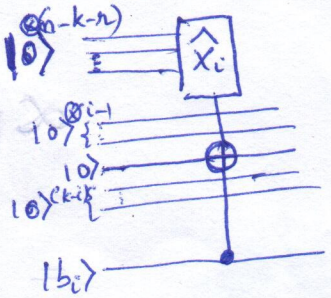
Also, ... merging the last k of the $|0\rangle^{\otimes n-r}$ qubit lines with the $|b_1 \ldots b_k\rangle$ qubit lines

Next, we observe that even the $\tilde{X}_i$ part of each $\bar{X}_i$ operator has additional structure — it is of the form $\underbrace{M_{i,r+1} \otimes \ldots \otimes M_{i,n-k}}_{\text{Call this } \hat{X}_i} \otimes I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(k-i)}$ (X at the $(n-k+i)^{th}$ position)

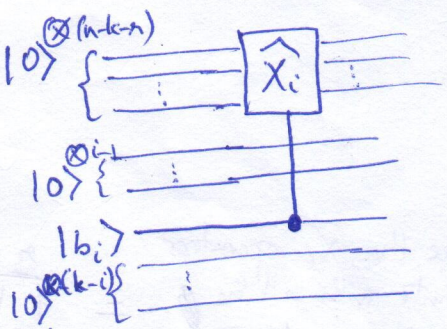
Thus, $|0\rangle^{\otimes n-r}$



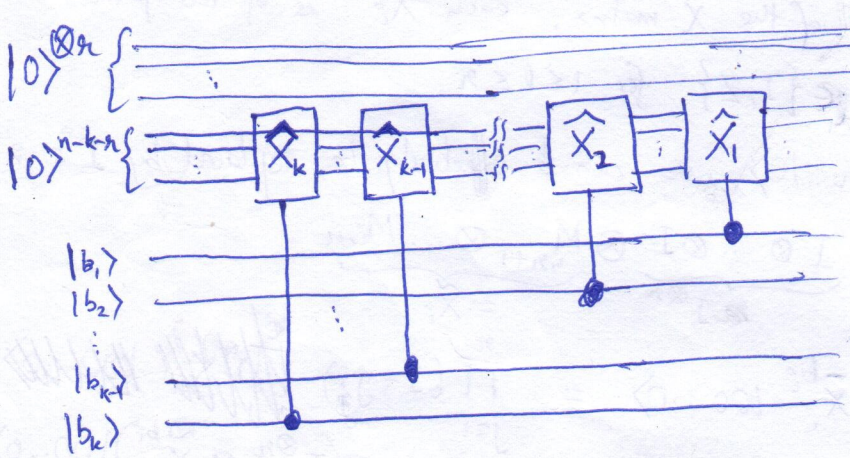
$\equiv$



$\equiv$



With this, the encoding circuit for the $|0\rangle^{\otimes r} \otimes \prod_{i=1}^{k} \tilde{X}_i^{b_i} |0\rangle^{\otimes n-r}$ part becomes.



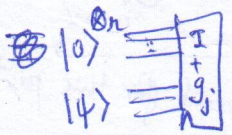
After this come the $(I + g_j)$ operations.

These lines will be used to control the g_j generator

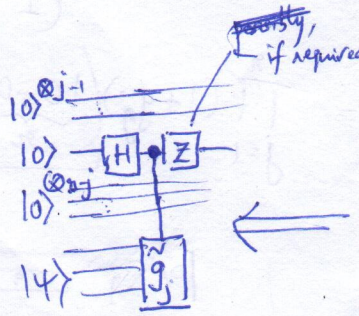
The idea here is the g_j generator, for any $j \in [n]$, has exactly one X in its first n qubit positions. (This X could also have a Z partnering it.) The remaining $n-1$ positions (out of the first n) are all populated by I or Z which do not have any influence on a $|0\rangle$ qubit.

So, let us write $g_j = M_1 \otimes \ldots \otimes M_n \otimes \tilde{g}_j$

M_ℓ here equals I or Z if $\ell \neq j$ and equals X or XZ if $\ell = j$



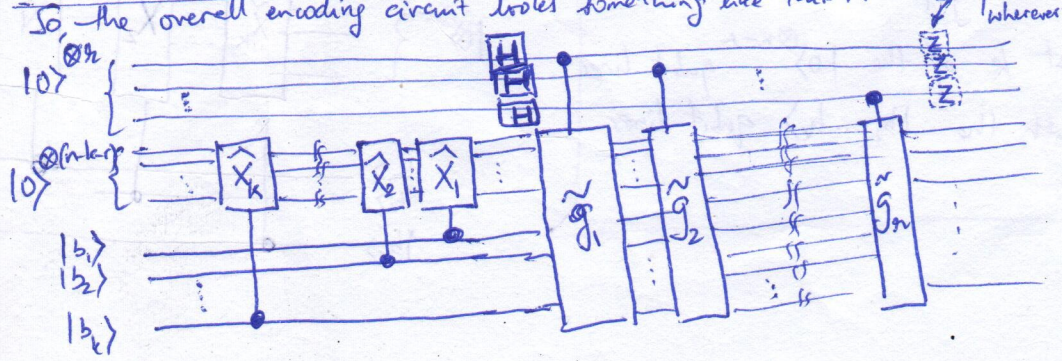
$\equiv$



$\Leftarrow$

Then, $I + g_j$ acting on $|0\rangle^{\otimes r} \otimes |\psi\rangle$ is simply $|0\rangle^{\otimes j-1} \otimes (|0\rangle + \underset{\text{possibly}}{Z}|1\rangle) \otimes |0\rangle^{\otimes(n-j)} \otimes (I + \tilde{g}_j)|\psi\rangle$

So, the overall encoding circuit looks something like this..



Claim: The states $\bar{X}_1^{b_1} \cdots \bar{X}_k^{b_k} |\bar{0}\rangle$, as $(b_1 \cdots b_k)$ ranges over $\{0,1\}^k$, form an ON basis of the code space Q_S.

Proof: Since $|\bar{0}\rangle \in Q_S$ and the $\bar{X}_i$ operators are all in $C(S) \setminus S$, the states $\bar{X}_1^{b_1} \cdots \bar{X}_k^{b_k} |\bar{0}\rangle$ are all in Q_S as well.

[If $|\varphi\rangle \in Q_S$ and $E \in C(S)$, then $E|\varphi\rangle = EM|\varphi\rangle$ for any $M \in S$
$= ME|\varphi\rangle$ (as $EM = ME$)
$\Rightarrow E|\varphi\rangle$ is in the $+1$-eigenspace for all $M \in S$
$\Rightarrow E|\varphi\rangle \in Q_S$]

To show orthogonality of any pair of these states consider

$$\left(\bar{X}_1^{b_1} \cdots \bar{X}_k^{b_k} |\bar{0}\rangle,\ \bar{X}_1^{b_1'} \cdots \bar{X}_k^{b_k'} |\bar{0}\rangle\right) \quad \text{for } (b_1 \cdots b_k) \neq (b_1' \cdots b_k')$$

$$= \langle \bar{0} | \underbrace{\bar{X}_1^{e_1} \cdots \bar{X}_k^{e_k}}_{\text{call this } \bar{X}} |\bar{0}\rangle \qquad \text{where } e_\ell = b_\ell \oplus b_\ell'$$

$$= \langle \underbrace{0 \cdots 0}_{n \text{ qubits}} | P \bar{X} P | \underbrace{0 \cdots 0}_{n \text{ qubits}} \rangle \qquad \text{where } P = \frac{1}{|S|} \sum_{M \in S} M$$

$$= \langle 0 \cdots 0 | P \bar{X} | 0 \cdots 0 \rangle \qquad \left(\text{since } P\bar{X}P = P \cdot P\bar{X} = P^2 \bar{X} = P\bar{X}\right)$$

$$= \frac{1}{|S|} \sum_{M \in S} \langle 0 \cdots 0 | M \bar{X} | 0 \cdots 0 \rangle$$

Thus, it suffices to show that $M|0\cdots0\rangle$ is orthogonal to $\bar{X}|0\cdots0\rangle$ for any $M \in S$ and any nontrivial $\bar{X}$ (i.e., $\bar{X} \neq I$)

Now, the vector form of M is some linear combination of the rows of the standard-form check matrix $\begin{matrix} r \\ n-r \end{matrix}\left\{\left[\begin{array}{ccc:ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \end{array}\right]\right.$

① If this linear combination involves at least one of the first r rows of the check matrix, then the vector form of M is of the form $[\underbrace{\tilde{a}_0}_{r}\ \underbrace{\tilde{a}_1}_{n-r}\ \underbrace{\tilde{a}_2}_{n-r} \mid \underbrace{\tilde{b}_0}_{r}\ \underbrace{\tilde{b}_1}_{n-r}\ \underbrace{\tilde{b}_2}_{n-r}]$ with $\tilde{a}_0 \neq 0 \cdots 0$

Then $M|0\cdots0\rangle = |\underbrace{\tilde{a}_0}_{r}\ \tilde{a}_1\ \tilde{a}_2\rangle$ with $\tilde{a}_0 \neq \underbrace{0 \cdots 0}_{r}$. Since $Z(\tilde{b})|0\cdots0\rangle = |0\cdots0\rangle$

OTOH, the vector form of $\bar{X}$ is some lin. comb. of the rows of the $\bar{X}$ matrix $[\underbrace{0}_{r}\ \underbrace{E^T}_{n}\ \underbrace{I}_{n} \mid E G_1^T + G_2^T\ 0\ 0]$

In particular, it is of the form $[\underbrace{0 \cdots 0}_{r}\ \tilde{u}_2\ \tilde{u}_3 \mid \tilde{v}_1\ 0\ 0]$; hence $\bar{X}|0\cdots0\rangle = |\underbrace{0 \cdots 0}_{r}\ \tilde{u}_2\ \tilde{u}_3\rangle$

Thus $M|0\cdots0\rangle = |\underbrace{\tilde{a}_0}_{\neq 0\cdots0} \tilde{a}_1 \tilde{a}_2\rangle$ is orthogonal to $\bar{X}|0\cdots0\rangle = |\underbrace{0\cdots0}_{n} \tilde{u}_2 \tilde{u}_3\rangle$

(2) If the vector form of M is a lin. comb. that involves none of the first n rows of the check matrix, then it is of the form $[\underbrace{0\cdots0}_{n} \,|\, * * *]$

So, $M|0\cdots0\rangle = |0\cdots0\rangle$.

OTOH, a nontrivial lin. comb. of the rows of the $\bar{X}$ matrix will be of the form

$$[\underbrace{0\cdots0}_{n} \tilde{u}_2 \underbrace{\tilde{u}_3}_{\neq 0\cdots0 \text{ } k \text{ times}} \,|\, * * *]$$

$\Rightarrow \bar{X}|0\cdots0\rangle = |0\cdots0 \tilde{u}_2 \tilde{u}_3\rangle_{\neq 0\cdots0}$ which is $\perp$ to $M|0\cdots0\rangle = |0\cdots0\rangle$

Thus, combining (1) and (2) above, we conclude that $\sum_{M \in S} \langle 0\cdots0|M\bar{X}|0\cdots0\rangle = 0$

$\Rightarrow \bar{X}_1^{b_1} \cdots \bar{X}_k^{b_k}|\bar{0}\rangle \perp \bar{X}_1^{b_1'} \cdots \bar{X}_k^{b_k'}|\bar{0}\rangle$.

∎

So far... $S = \langle g_1, \dots g_{n-k} \rangle$, g_i's are indep generators

Standard form of check matrix:

$$H = \begin{array}{c} r \\ n-k-r \end{array} \left\{ \begin{array}{c|ccc|ccc} \overbrace{I}^{r} & \overbrace{A_1}^{n-k-r} & \overbrace{A_2}^{k} & \overbrace{B}^{r} & \overbrace{C_1}^{n-k-r} & \overbrace{C_2}^{k} \\ 0 & 0 & 0 & D & I & E \end{array} \right]_{(n-k)\times 2n}$$

$\bar{X}$ matrix (These operators are in $C(S)$, and commute among themselves)

$$\left[\begin{array}{ccc|ccc} \overbrace{0}^{r} & \overbrace{E^T}^{n-k-r} & \overbrace{I}^{k} & \overbrace{E^T C_1^T + C_2^T}^{r} & \overbrace{0}^{n-k-r} & \overbrace{0}^{k} \end{array} \right]_{k\times 2n}$$

$\bar{Z}$ matrix

These operators are in $C(S)$, commute among themselves and form hyperbolic pairs with the $\bar{X}$ operators

$$\left[\begin{array}{ccc|ccc} \overbrace{0}^{r} & \overbrace{0}^{n-k-r} & \overbrace{0}^{k} & \overbrace{A_2^T}^{r} & \overbrace{0}^{n-k-r} & \overbrace{I}^{k} \end{array} \right]_{k\times 2n}$$

The picture so far is the following:

H matrix: $g_1, g_2, \dots, g_{n-k}$ | $\bar{H}$ matrix: $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_{n-k}$

To complete the picture, we produce $\bar{g}_i$ operators that form hyperbolic pairs with the g_i operators, while commuting with everything else

$\bar{Z}_1, \bar{Z}_2, \dots, \bar{Z}_k$ | $\bar{X}_1, \bar{X}_2, \dots, \bar{X}_k$

$$\bar{H} = \begin{array}{c} r \\ n-k-r \end{array} \left\{ \begin{array}{ccc|ccc} \overbrace{0}^{r} & \overbrace{0}^{n-k-r} & \overbrace{0}^{k} & \overbrace{I}^{r} & \overbrace{0}^{n-k-r} & \overbrace{0}^{k} \\ 0 & I & 0 & G^T & 0 & 0 \end{array} \right]$$

We will return to this later

Def: A (maximal) symplectic subset of $\mathcal{P}_n$ is a set of Pauli operators $\{\bar{Z}_1, \dots, \bar{Z}_n, \bar{X}_1, \dots, \bar{X}_n\}$ such that

- $[\bar{Z}_i, \bar{Z}_j] = 0$, $[\bar{X}_i, \bar{X}_j] = 0$
- $[\bar{Z}_i, \bar{X}_j] = 0$ if $i \neq j$, $\{\bar{Z}_i, \bar{X}_i\} = 0$.

(Here, $[A,B]$ is the commutator $AB - BA$ and $\{A,B\}$ is the anticommutator $AB + BA$)

In other words, each $\bar{X}_i$ (resp. $\bar{Z}_i$) anti-commutes with its corresponding $\bar{Z}_i$ (resp $\bar{X}_i$) but commutes with all other operators.

Eg., $\{Z_1, \dots, Z_n, X_1, \dots, X_n\}$ is a (maximal) symplectic subset of $\mathcal{P}_n$

where $Z_i = I^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}$

and $X_i = I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}$

Theorem: Let $\bar{\mathcal{A}} = \{\bar{Z}_1, \dots, \bar{Z}_n, \bar{X}_1, \dots, \bar{X}_n\}$ and $\hat{\mathcal{A}} = \{\hat{Z}_1, \dots, \hat{Z}_n, \hat{X}_1, \dots, \hat{X}_n\}$ be two maximal symplectic subsets of $\mathcal{P}_n$. Then, there exists a unitary matrix U s.t. $\bar{\mathcal{A}} = U \hat{\mathcal{A}} U^\dagger$ up to an overall phase.

Proof: Note that $\bar{S} = \langle \bar{Z}_1, \dots, \bar{Z}_n \rangle$ and $\hat{S} = \langle \hat{Z}_1, \dots, \hat{Z}_n \rangle$ are two stabilizer subgroups of $\mathcal{P}_n$ with n indep. generators each.

Before proving this, we need a lemma:

Lemma: If $\{\bar{Z}_1, \dots, \bar{Z}_n, \bar{X}_1, \dots, \bar{X}_n\}$ is a (maximal) symplectic subset, then $\bar{Z}_1, \dots, \bar{Z}_n$ are n independent Pauli operators, as are $\bar{X}_1, \dots, \bar{X}_n$.

Proof: If $\bar{Z}_j$ is expressible as a product of the form $\prod_{i \in I, i \neq j} \bar{Z}_i$ for some index set $I \subseteq [n]$, then since $\bar{X}_j$ commutes with each $\bar{Z}_i$, $i \neq j$, it would commute with $\bar{Z}_j = \prod_{i \in I, i \neq j} \bar{Z}_i$. Contradiction

Proof of Thm: Let $\bar{S} = \langle \bar{Z}_1, \ldots, \bar{Z}_n \rangle$ and $\hat{S} = \langle \hat{Z}_1, \ldots, \hat{Z}_n \rangle$. These are stabilizer subgroups of $\mathcal{P}_n$

Proof of Thm: If any of these Pauli operators squares to $-I$, then replace it by $i \cdot$ (that operator). Thus all $\bar{Z}_i, \hat{Z}_i, \bar{X}_i, \hat{X}_i$ square to I.

Let $\bar{S} = \langle \bar{Z}_1, \ldots, \bar{Z}_n \rangle$, $\hat{S} = \langle \hat{Z}_1, \ldots, \hat{Z}_n \rangle$

These are abelian subgroups of $\mathcal{P}_n$ not containing $-I$; hence are stabilizer subgroups. The corresp QECCs $\bar{Q}$ and $\hat{Q}$, are 1-dimensional. Let $|\bar{0}\rangle$ and $|\hat{0}\rangle$ be the unique (up to global phase) states lying in $\bar{Q}$ and $\hat{Q}$ respectively.

For $\underline{b} = (b_1 \ldots b_n) \in \{0,1\}^n$, set

$$|\underline{\bar{b}}\rangle = \bar{X}_1^{b_1} \bar{X}_2^{b_2} \ldots \bar{X}_n^{b_n} |\bar{0}\rangle$$

and $$|\underline{\hat{b}}\rangle = \hat{X}_1^{b_1} \hat{X}_2^{b_2} \ldots \hat{X}_n^{b_n} |\hat{0}\rangle.$$

Claim: As $\underline{b}$ ranges over $\{0,1\}^n$, $\{|\underline{\bar{b}}\rangle\}$ forms an ON basis of $\mathbb{C}^{2^n}$, as does $\{|\underline{\hat{b}}\rangle\}$.

Proof: Consider distinct binary n-tuples $\underline{b}$ and $\underline{b}'$:

$$\langle \underline{\bar{b}} | \underline{\bar{b}'} \rangle = \langle \bar{0} | \underbrace{\bar{X}_1^{b_1} \ldots \bar{X}_n^{b_n} \cdot \bar{X}_1^{b_1'} \ldots \bar{X}_n^{b_n'}}_{= \bar{X}_1^{e_1} \ldots \bar{X}_n^{e_n}} |\bar{0}\rangle$$

with $e_j = b_j \oplus b_j'$. Not all e_j's are 0.

$$= \langle \bar{0} | \bar{X}_1^{e_1} \ldots \bar{X}_n^{e_n} | \bar{0} \rangle$$

for some j: $e_j \neq 0$ $\rightarrow$

$$= \langle \bar{0} | \bar{X}_1^{e_1} \ldots \bar{X}_j^{e_j} \ldots \bar{X}_n^{e_n} \bar{Z}_j | \bar{0} \rangle$$

$$= \langle \bar{0} | (-\bar{Z}_j) \bar{X}_1^{e_1} \ldots \bar{X}_j^{e_j} \ldots \bar{X}_n^{e_n} | \bar{0} \rangle$$

as $\bar{Z}_j$ anti-commutes with $\bar{X}_j$ but commutes with all other $\bar{X}_i$'s.

$$= -\langle \bar{0} | \bar{X}_1^{e_1} \ldots \bar{X}_n^{e_n} | \bar{0} \rangle$$

$$= -\langle \underline{\bar{b}} | \underline{\bar{b}'} \rangle$$

Hence, $\langle \underline{\bar{b}} | \underline{\bar{b}'} \rangle = 0$

Let U be the change of basis matrix

$$U = \sum_{\underline{b}} |\underline{b}\rangle\langle\hat{\underline{b}}| \qquad (\text{and } U^\dagger = U^{-1} = \sum_{\underline{b}} |\hat{\underline{b}}\rangle\langle\underline{b}|)$$

Consider, for any $\hat{\underline{b}}$:

$$\overline{Z}_j \underbrace{U|\hat{\underline{b}}\rangle}_{=|\underline{b}\rangle} = \overline{Z}_j \overline{X}_1^{b_1} \cdots \overline{X}_n^{b_n} |\overline{0}\rangle$$

$$= \underbrace{(-1)^{b_j}}_{\text{because } \overline{Z}_j \text{ anticommutes with } \overline{X}_j} \overline{X}_1^{b_1} \cdots \overline{X}_n^{b_n} \underbrace{\overline{Z}_j |\overline{0}\rangle}_{=|\overline{0}\rangle}$$

$$= (-1)^{b_j} |\underline{b}\rangle$$

and $U \hat{Z}_j |\hat{\underline{b}}\rangle = U \underbrace{\hat{Z}_j \hat{X}_1^{b_1} \cdots \hat{X}_n^{b_n} |\hat{0}\rangle}_{= (-1)^{b_j} \hat{X}_1^{b_1} \cdots \hat{X}_n^{b_n} \hat{Z}_j}$

$$= U (-1)^{b_j} \hat{X}_1^{b_1} \cdots \hat{X}_n^{b_n} |\hat{0}\rangle \qquad \text{as } \hat{Z}_j|\hat{0}\rangle = |\hat{0}\rangle$$

$$= (-1)^{b_j} \underbrace{U|\hat{b}\rangle}_{=|\underline{b}\rangle}$$

$$= (-1)^{b_j} |\underline{b}\rangle$$

Since the $\hat{\underline{b}}$'s form a basis of $\mathbb{C}^{2^n}$, it follows that

$$U \hat{Z}_j = \overline{Z}_j U \quad , \text{ ie., } \overline{Z}_j = U \hat{Z}_j U^\dagger.$$

Similarly it can be argued that $U \hat{X}_j = \overline{X}_j U$, ie., $\overline{X}_j = U \hat{X}_j U^\dagger$ ▨

Here, one shows that

$$U \hat{X}_j |\hat{\underline{b}}\rangle = \overline{X}_j U |\hat{\underline{b}}\rangle = \overline{X}_j |\underline{b}\rangle$$

$$= |b_1 \cdots (1 \oplus b_j) \cdots b_n\rangle$$

Now, let us return to

$$H = \begin{matrix} r \\ n-k-r \end{matrix} \begin{bmatrix} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \end{bmatrix}$$

(columns: r, $n-k-r$, k, r, $n-k-r$, k)

$$\overline{Z} : \; k \begin{bmatrix} 0 & 0 & 0 & A_2^T & 0 & I \end{bmatrix}$$

$$\overline{H} : \begin{bmatrix} 0 & 0 & 0 & I & 0 & 0 \\ 0 & I & 0 & C_1^T & 0 & 0 \end{bmatrix}$$

$$\overline{X} : \begin{bmatrix} 0 & E^T & I & E^T C_1^T + C_2^T & 0 & 0 \end{bmatrix}$$

call these $\overline{Z}_{k+1} \cdots \overline{Z}_n$ ← $g_1, \ldots, g_{n-k}$

call these $\overline{X}_{k+1} \cdots \overline{X}_n$ ← $\overline{g}_1, \ldots, \overline{g}_{n-k}$

$\overline{Z}_1, \ldots, \overline{Z}_k$; $\overline{X}_1, \ldots, \overline{X}_k$

Consider $\hat{\mathcal{A}} = \{Z_1, \dots, Z_n, X_1, \dots, X_n\}$.

Then, $|\hat{b}\rangle = |b\rangle$: standard basis of $\mathbb{C}^{2^n}$ for all $b \in \{0,1\}^n$

The basis change matrix U maps $|b\rangle$ to $\underbrace{\bar{X}_1^{b_1} \cdots \bar{X}_n^{b_n} |\bar{0}\rangle}_{=: |\bar{b}\rangle}$

$$|b_1 b_2 \cdots b_n\rangle \longmapsto \bar{X}_1^{b_1} \bar{X}_2^{b_2} \cdots \bar{X}_n^{b_n} (I+g_1)\cdots(I+g_{n-k})(I+\bar{Z}_1)\cdots(I+\bar{Z}_k) |100\cdots0\rangle$$

As before, we note that $g_{r+1}, \dots, g_{n-k}$, as well as $\bar{Z}_1, \dots, \bar{Z}_k$ are composed only of Z operators; which have no effect on $|100\cdots0\rangle$

Thus, $|b_1 b_2 \cdots b_n\rangle \longmapsto \bar{X}_1^{b_1} \bar{X}_2^{b_2} \cdots \bar{X}_n^{b_n} (I+g_1)(I+g_2)\cdots(I+g_r)|100\cdots0\rangle$

$$= \bar{X}_{k+1}^{b_{k+1}}(I+g_1)\,\bar{X}_{k+2}^{b_{k+2}}(I+g_2)\cdots\bar{X}_{k+r}^{b_{k+r}}(I+g_r)\,\bar{X}_{k+r+1}^{b_{k+r+1}}\cdots\bar{X}_n^{b_n}\,\bar{X}_1^{b_1}\cdots\bar{X}_k^{b_k}|100\cdots0\rangle$$

Now, $\bar{X}_{k+i} = \bar{g}_i$ for $1 \le i \le n-k$

In particular, $\bar{X}_{k+i} = \bar{g}_i = Z_i$ for $1 \le i \le r$ (std. Z operator acting on i^{th} qubit) from the form of the H matrix

and $\bar{X}_{k+i} = \bar{g}_i = (\text{possible } Z\text{s acting on some of the first } r \text{ qubits}) \otimes X_i$ for $r+1 \le i \le n-k$

(X-flip operator on i^{th} qubit)

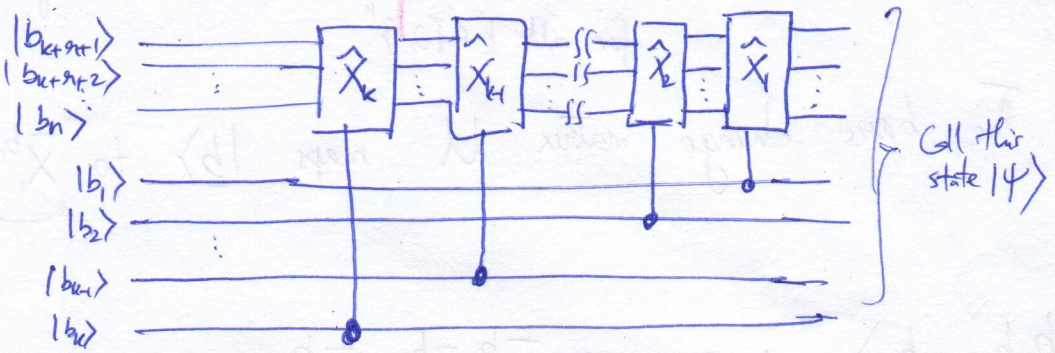
Thus, $|b_1 b_2 \cdots b_n\rangle \longmapsto Z_1^{b_{k+1}}(I+g_1)\,Z_2^{b_{k+2}}(I+g_2)\cdots Z_r^{b_{k+r}}(I+g_r)$

$$\cdot \bar{X}_1^{b_1}\cdots\bar{X}_k^{b_k}\underbrace{\bar{X}_{k+r+1}^{b_{k+r+1}}\cdots\bar{X}_n^{b_n}|100\cdots0\rangle}_{= |0\rangle^{\otimes r} \otimes |b_{k+r+1}\cdots b_n\rangle \otimes |0\rangle^{\otimes k}}$$

$$= Z_1^{b_{k+1}}(I+g_1)\cdots Z_r^{b_{k+r}}(I+g_r)\left[|0\rangle^{\otimes r} \otimes \tilde{X}_1^{b_1}\cdots\tilde{X}_k^{b_k}|b_{k+r+1}\cdots b_n 0\cdots0\rangle\right]$$

since $X_i = I^{\otimes r} \otimes \tilde{X}_i$ for $1 \le i \le k$ — see p. ENC-7.

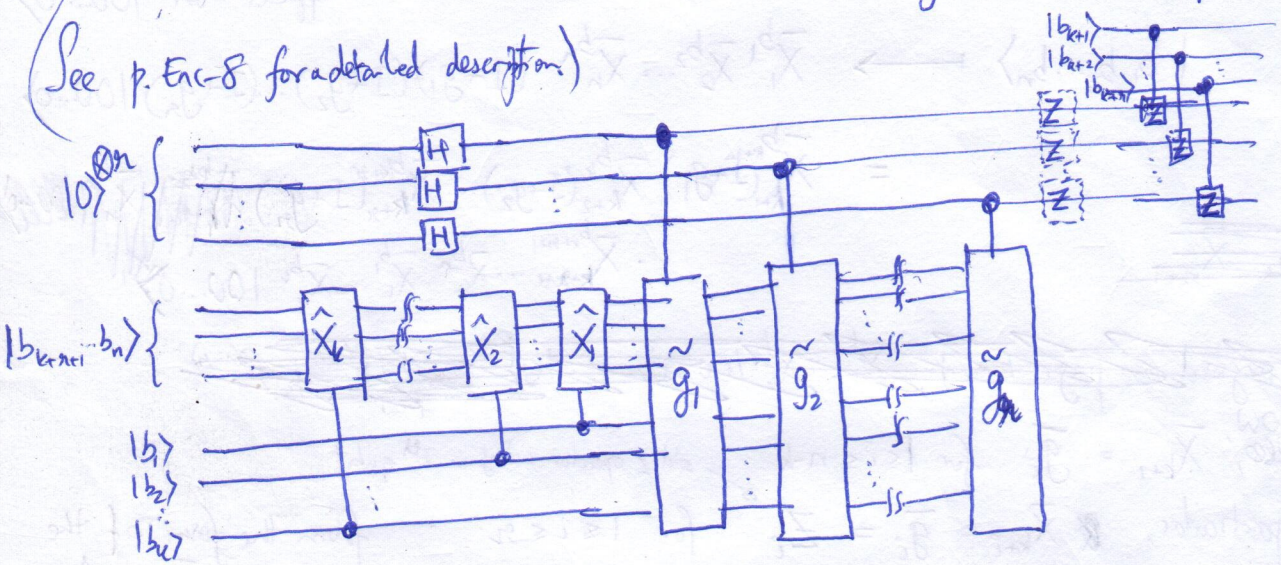
Now, as argued on p. Enc-8, $\tilde{X}_1^{b_1} \cdots \tilde{X}_k^{b_k} |b_{k+n+1} \cdots b_n \underbrace{0 \cdots 0}_{k}\rangle$ is realized as



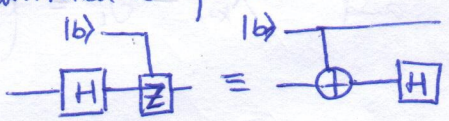
Next, $\prod_{i=1}^{n} (I + g_i)$ acting on $|0\rangle^{\otimes n} \otimes |\psi\rangle$, where $|\psi\rangle$ is the output above...

This can be followed by $\prod_{i=1}^{n} Z_i^{b_{k+i}}$, ie., controlled Z operators (controlled by $|b_{k+i}\rangle$) acting on the i^{th} qubit.

(See p. Enc-8 for a detailed description)

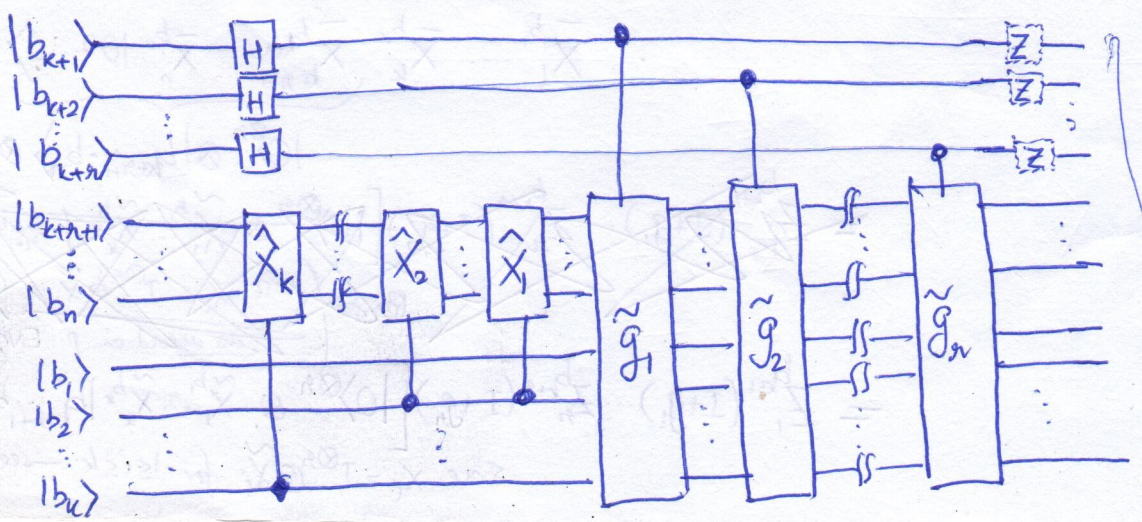


Finally, on the top n qubit lines, the final controlled-Z operator commute with std. Z, and with controlled-$\tilde{g}_j$. Moreover,



This is due to the fact that $XHH = HHZ$

With this, the final quantum circuit for the change of basis U operation is $\sum_b |b\rangle\langle b|$



$|b_1 \cdots b_n\rangle$

(the qubit lines are still in the index order $k+1, k+2, \ldots n$ followed by $1, 2, \ldots k$)