MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Department of Physics, EECS, and Department of Applied Math

6.443J/8.371J/18.409/MAS.865 Spring 2006

Quantum Information Science

Problem Set #2 Solutions

(due 02-Mar-06)

Problem 1: (Measurements and stabilizers)

(a) Let M be an n-qubit measurement operator described by a product of Pauli matrices. If it commutes with all the generators, we have

$$g_i M |\psi\rangle = M g_i |\psi\rangle = M |\psi\rangle .$$

Thus $M|\psi\rangle$ is in the subspace stabilized by $S = \langle g_1, \ldots, g_n\rangle$. This is possible only if $M|\psi\rangle = c|\psi\rangle$, and because $M^2 = 1$, we can say that either M or $-M$ is already in the stabilizer. If M was in the stabilizer, the state is already in the $+1$ eigenstate of M and measuring M does not disturb the state or the stabilizer. If $-M$ was in the stabilizer, the state must have been in the -1 eigenstate of M. Therefore in this case, after measuring M, the state remains in the -1 eigenstate of M, and the stabilizer remains unchanged as well.

However, if M anticommutes with $g_1, \ldots, g_j$ and commutes with $g_{k>j}$, the situation is different. Let us multiply the generators $g_2, \ldots, g_j$ with g_1, obtaining $g_2' = g_1 g_2$ and so on. $S' = \langle g_1, g_2', \ldots, g_j', g_{j+1}, \ldots, g_n\rangle$. Without loss of generality, we can thus write the stabilizer in such a way that M anticommutes with the first generator, and commutes with the rest. After measuring M and obtaining the result $k = \{0,1\}$, the state is an eigenstate of M, stabilized by $(-1)^k M$. The generator g_1 does not stabilize it anymore, and $(-1)^k M$ can not be constructed from the rest of the generators (because then it would commute with g_1), therefore the new stabilizer is now $S = \langle (-1)^k M, g_2' \ldots, g_j', g_{j+1}, \ldots, g_n\rangle$.

(b) The state stabilized by $\langle XX, ZZ\rangle$ is $|00+11\rangle/\sqrt{2}$. We want to measure IY. This anticommutes with both XX and ZZ. Let us then write the stabilizer as $S = \langle XX, (XX)(ZZ)\rangle = \langle XX, -YY\rangle$. After measuring IY and obtaining $k = \{0,1\}$, the resulting stabilizer and state will be

$$\begin{aligned} \langle IY, -YY\rangle = &\ \langle IY, -YI\rangle, & |\psi_0\rangle = |y-\rangle|y+\rangle, && \text{for}\, k=0, \\ \langle -IY, -YY\rangle = &\ \langle -IY, YI\rangle, & |\psi_1\rangle = |y+\rangle|y-\rangle, && \text{for}\, k=1. \end{aligned}$$

(c) Let us start in $|\psi\rangle \otimes |0\rangle$. This state is stabilized by $I \otimes Z$ and one more unknown stabilizer generator. After measuring $Y \otimes X$, the state will be in an eigenstate of $Y \otimes X$. If it becomes a -1 eigenstate, we wish to do an operation to turn it into a $+1$ eigenstate of $Y \otimes X$. Let $|\psi^-\rangle$ be a -1 eigenstate of $Y \otimes X$. Because the previous stabilizer element $I \otimes Z$ anticommutes with $Y \otimes X$, we can use it for this purpose.

$$(Y \otimes X)(I \otimes Z)\left|\psi^-\right\rangle = -(I \otimes Z)(Y \otimes X)\left|\psi^-\right\rangle = +(I \otimes Z)\left|\psi^-\right\rangle,$$

therefore applying $I \otimes Z$ after measuring -1 will steer the post-measurement state into the $+1$ eigenstate of $Y \otimes X$.

The second measurement is $I \otimes Y$. We will now use the same trick, and correct the -1 eigenstate by applying the element $Y \otimes X$ from the previous stabilizer that anticommuted with the measurement $I \otimes Y$.

(d) For the state $|\psi\rangle \otimes |0\rangle$ we have normalizer operations $\bar{X} = XI$ and $\bar{Z} = ZI$. These normalizer elements anticommute with the new stabilizer operation $g_1 = YX$. However, the old stabilizer element $g_0 = IZ$ also anticommutes with $g_1 = YX$. We can use it to make new normalizer elements $\bar{X}_1 = (XI)(IZ) = XZ$ and $\bar{Z}_1 = (ZI)(IZ) = ZZ$. This can be seen from

$$(\bar{X}g_0)g_1(\bar{X}g_0)^\dagger = \bar{X}g_0g_1g_0^\dagger\bar{X}^\dagger = -\bar{X}g_1g_0g_0^\dagger\bar{X}^\dagger = -\bar{X}g_1\bar{X}^\dagger = g_1\bar{X}\bar{X}^\dagger = g_1,$$

which means that $\bar{X}_1 = \bar{X}g_0$ is a new normalizer element for stabilizer $S_1 = \langle g_1 \rangle$.

Next we measure IY. This again anticommutes with both $\bar{X}_1$ and $\bar{Z}_1$, while we have thrown the stabilizer element $g_1 = XY$. This changes the operators into $\bar{X}_2 = (XZ)(XY) = -iIX$ and $\bar{Z}_2 = (ZZ)(XY) = YX$.

(e) If we started in the state $|\psi\rangle \otimes |0+1\rangle/\sqrt{2}$, it would be stabilized by $I \otimes X$ and some other stabilizer generator $P \otimes I$. However, this one will be important now, because the first measurement $Y \otimes X$ commutes with $I \otimes X$. If element $P \otimes I$ also commuted with $Y \otimes X$, we would always measure $+1$. However, if it did not commute with $Y \otimes X$, we would need to use $P \otimes I$ for the correction. The correction operator after the second measurement (i.e. $I \otimes Y$) remains $Y \otimes X$.

Problem 2: (Passive error correction and decoherence free subspaces)

(a) The stabilizer for code with $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$ is $S = \langle ZZI, IZZ \rangle$. We want to show that errors $E \in \{XII, IXI, IIX\}$ can be corrected with this code. Let us use the error-correction conditions, and look at E_jE_k. The possibilities are $E_iE_k \in \{III, XXI, XIX, IXX\}$. We can see that $(XXI)(IZZ)(XXI) = -IZZ \notin S$, which means that XXI is not in the normalizer of S. Also $(XIX)(ZZI)(XIX) = -ZZI$ and $(IXX)(ZZI)(IXX) = -ZZI$. Therefore none of E_iE_k belong to $N(S) - S$, and the set of errors E is correctable.

(b) By inspection, $E_1 = ZIZ$ does not cause any error on the codewords. Thus our code is a *decoherence free subspace*(DFS) for the error E_1.

(c) If all of errors E_i belong to the stablizer of C, then it is obvious that C is a DFS for the set of errors E_i.

(d) All single qubit errors on any number of n bits can not belong to a single stabilizer, because stabilizer elements commute with each other. However, X_k and Z_k don't.

(e) We have $A = \{U_1 = YYY, U_2 = ZZZ\}$ and $B = \{U_1 = ZYX, U_2 = YZI\}$. For set A, we have $U_1U_2 = (iX)(iX)(iX) = -iX_L$, which is the logical X operation and multiplication by an unimportant phase. For set B, we have $U_1U_2 = (-iX)(iX)(X) = X_L$.

(f) Let us assume the errors occur as $U_2E_1U_1$. Because $E_1 = XII$ anticommutes with U_2 for both sets, we can write $U_2E_1U_1 = -E_1U_2U_1 = -E_1X_L$. The operation X_L commutes with the code stabilizer, therefore it does not change the stabilizer. We thus need to prove that the error $-E_1$ is correctable by code C. We see that $(-E_1)(-E_1) = III \in S$. The error-correction conditions then state that $-E_1$ is correctable for code $C(S)$.

If the error is $E_1 = ZIZ$, it commutes with U_2 from set A, giving $U_2E_1U_1 = E_1U_2U_1$, making the error E_1 appear after applying X_L. However, E_1 belongs to the stabilizer of code C, and as such, is "passively" corrected.

For the set B and error $E_1 = ZIZ$, we have $U_2E_1U_1 = (ZYX)(ZIZ)(YZI) = -(ZIZ)(ZYX)(YZI) = (-ZIZ)X_L$. This means that error ZIZ between U_1 and U_2 is equivalent to error $E_1' = -ZIZ$ after applying U_2U_1. When we multiply this new error E_1' by the stabilizer element ZIZ, we see that it is nothing but an overall minus sign, which is also harmless.

(g) We can write $U_2EU_1 = (U_2EU_2^\dagger)U_2U_1$. We will then analyze $\bar{E} = U_2EU_2^\dagger$ as the error. The error correction condition tells us that $\bar{E}\bar{E}^\dagger = U_2EE^\dagger U_2^\dagger$ can not belong to $N(S) - S$ for the error to be correctable. The same holds for $U_1^\dagger EE^\dagger U_1$.

(h) If a code C is a DFS for errors $\{E_j\}$, to keep the DFS condition for $U_2E_jU_1$ we need to have $U_2E_jU_1 |\psi\rangle = d_j |\psi\rangle$. This means that

$$E_jU_1 |\psi\rangle = c_jU_1 |\psi\rangle = d_jU_2^\dagger |\psi\rangle .$$

Because this should hold for all j, we require $d_j = c_j$, $U_2^\dagger = U_1$ and that U_1 belongs to the normalizer of C, to keep $U_1 |\psi\rangle = |\psi'\rangle$ in the code, and thus to have $E_j |\psi'\rangle = c_j |\psi'\rangle$.

Problem 3: (Topological QEC: Projective Plane Codes)

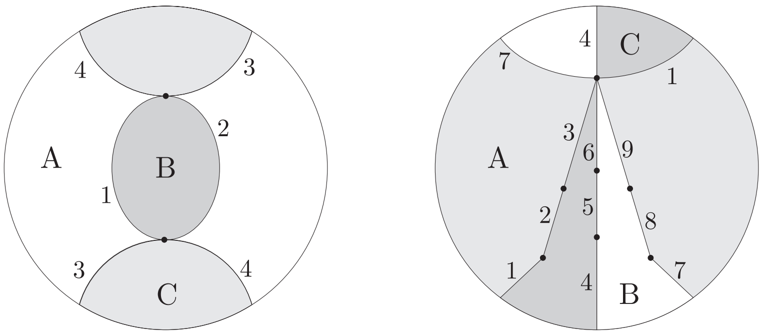
(a) Our cellulation of $\Re P^2$ has 3 faces, 2 vertices and 4 edges. This gives stabilizers

$$\begin{aligned} A_\mathrm{B} &= Z_1Z_2, \qquad B = X_1X_2X_3X_4. \\ A_\mathrm{C} &= Z_3Z_4, \end{aligned}$$

and a redundant $A_\mathrm{A} = Z_1Z_2Z_3Z_4 = A_\mathrm{B}A_\mathrm{C}$. We thus have a code on four qubits with three stabilizers. This means the stabilized subspace is two-dimensional. What are the codewords? We can find them by hand. The two-dimensional subspace for the first two qubits stabilized by Z_1Z_2 contains $|00\rangle$ and $|11\rangle$. The same holds for qubits 3 and 4. Requiring $X_1X_2X_3X_4$ to stabilize the state of the four qubits, we find that

$$|\psi_1\rangle = |0000 + 1111\rangle /\sqrt{2} \qquad \text{and} \qquad |\psi_2\rangle = |0011 + 1100\rangle /\sqrt{2}$$

are stabilized by $S = \{A_\mathrm{B}, A_\mathrm{C}, B\}$.



(b) For the second cellulation, the stabilizers are

$$\begin{aligned} &B_1 = X_1X_2, \qquad B_3 = X_4X_5, \qquad B_5 = X_7X_8, \qquad A_\mathrm{A} = Z_1Z_2Z_3Z_7Z_8Z_9, \\ &B_2 = X_2X_3, \qquad B_4 = X_5X_6, \qquad B_6 = X_8X_9, \qquad A_\mathrm{B} = Z_4Z_5Z_6Z_7Z_8Z_9, \end{aligned}$$

and $A_\mathrm{C} = Z_1Z_2Z_3Z_4Z_5Z_6 = A_\mathrm{A}A_\mathrm{B}$ and $B_7 = X_1X_3X_4X_6X_8X_9 = B_1B_2B_3B_4B_5B_6$ that are redundant, because they can be obtained by multiplying the stabilizers above. What are the codewords?

There are two of them, because we have 9 qubits and 8 stabilizers. It is a little more tricky to find them this time, but it can be done by hand. Of course, if one realizes that the stabilizer generators are almost the Shor code stabilizers, just with $X \leftrightarrow Z$. This means that the codewords will be the Shor code codewords, with states in the x-basis (i.e. $|+\rangle$ and $|-\rangle$) exchanged for states in the z-basis (i.e. $|0\rangle$ and $|1\rangle$) and vice versa.

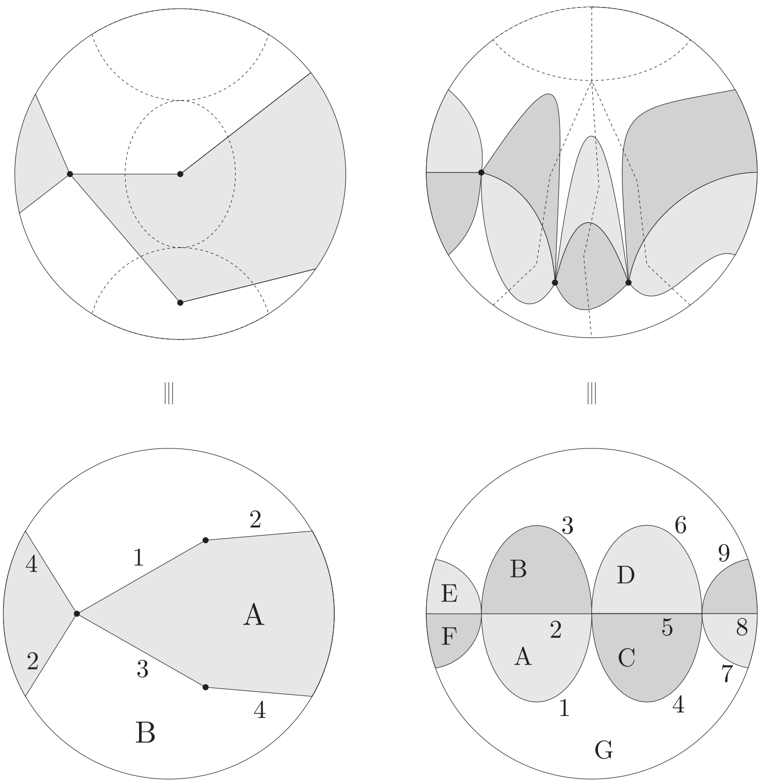
$$\begin{aligned} \text{Shor 9-qubit code :} \quad & \tfrac{1}{8}\big(\,|000\rangle \pm |111\rangle\,\big)^{\otimes 3} \\ \text{this code (dual to the Shor code) :} \quad & \tfrac{1}{8}\big(\,|{+}{+}{+}\rangle \pm |{-}{-}{-}\rangle\,\big)^{\otimes 3} \end{aligned}$$

Let us also explain a simple numerical method of finding the codewords. For every element g of the stabilizer, the states it stabilizes belong to the zero eigenspace of $\mathbb{I} - g$. Let us then form a matrix $M = \sum_i(\mathbb{I} - g_i)$ and find its eigenvalues and eigenvectors. Note that all of the g_i commute, so we know they can be simultaneously diagonalized. The $\lambda = 0$ eigenspace of M is the stabilized subspace. We find these codewords:

$$|\psi_1\rangle = \frac{1}{8}\,|000 + 011 + 101 + 110\rangle^{\otimes 3}\,, \qquad |\psi_2\rangle = \frac{1}{8}\,|001 + 010 + 100 + 111\rangle^{\otimes 3}\,.$$

It is easy to check that we have found the codewords for the dual to the Shor 9-qubit code.

(c) The dual to the cellulations above is found by drawing an edge across every edge we had, and connecting them to vertices inside the faces. This practically changes every Z in a stabilizer element into an X, and vice versa. The dual cellulations for parts (a) and (b) are



The stabilizers for the dual code to the one of part (a) are

$$B_1 = X_1X_2, \qquad B_2 = X_3X_4, \qquad A = Z_1Z_2Z_3Z_4,$$

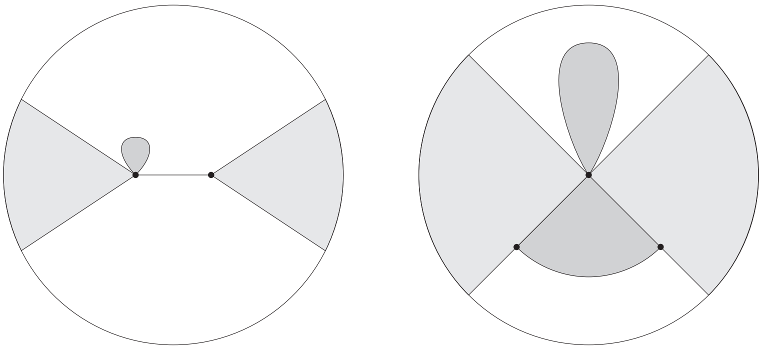
giving codewords

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big(|{+}{+}{+}{+}\rangle + |{-}{-}{-}{-}\rangle\big) \qquad \text{and} \qquad |\psi_2\rangle = \frac{1}{\sqrt{2}}\big(|{+}{+}{-}{-}\rangle + |{-}{-}{+}{+}\rangle\big).$$

For the dual to part (b), we have the stabilizers for the Shor 9-qubit code,

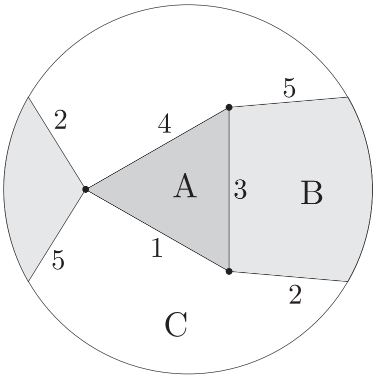
$$\begin{array}{llll} A_A = Z_1Z_2, & A_C = Z_4Z_5, & A_E = Z_7Z_8, & B_1 = X_1X_2X_3X_7X_8X_9, \\ A_B = Z_2Z_3, & A_D = Z_5Z_6, & A_F = Z_8Z_9, & B_2 = X_4X_5X_6X_7X_8X_9. \end{array}$$

(d) We will prove the following: if there is such a bad edge, the cellulation does not give us a set of stabilizers. Note, that it is possible that a cellulation without such a "weird" edge could be bad as well, the reader is invited to work out why the second depicted cellulation is not valid as well.



Let us concentrate on the "weird" edge. Note that anything can happen inside the shaded regions. Because the special edge has the same face on both sides, one of the stabilizer operators will be $Z_wZ_1\ldots Z_n$ where $Z_1\ldots Z_n$ are all the edges that appear around the white face of the cellulation. Another stabilizer operator from one of the vertices on the edge will be $X_wX_1X_nX_{\text{gray inside}}$ We can already see that these two do not commute, because they contain three common Z's and X's. Thus such a cellulation does not give a valid stabilizer code.

(e) There are many examples of a five-edge cellulation. What happens when you try to have only a single vertex? We give an example that comes from the dual to (a) just by adding one more edge:



The stabilizers are

$$\begin{aligned} B_1 &= X_1X_2X_3, & A_A &= Z_1Z_3Z_4, \\ B_2 &= X_3X_4X_5, & A_B &= Z_2Z_3Z_5. \end{aligned}$$

These give codewords (found using the numerical procedure described above)

$$|\psi_1\rangle = \frac{1}{2}\,|00000 + 00111 + 11011 + 11100\rangle\,, \qquad |\psi_2\rangle = \frac{1}{2}\,|01001 + 10010 + 01110 + 10101\rangle\,.$$

Problem 4: (The Gottesman-Knill Theorem)

(a) Recall that

$$H = \frac{1}{\sqrt{2}}\left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right] \qquad \text{and} \qquad S = \left[\begin{array}{cc} 1 & 0 \\ 0 & i \end{array}\right].$$

We also know that $S^2 = Z$, $HZH = X$ and $ZX = iY$. Therefore by having H and S at our disposal, we can apply any Pauli operation (up to a phase), and H and S as well. The action of H and S on Pauli matrices is

$$\begin{aligned} H &: \{X \to Z, Y \to -Y, Z \to X\}, \\ S &: \{X \to Y, Y \to -X, Z \to Z\}. \end{aligned}$$

Any normalizer operation on the group G_1 is simply a permutation of the three generator elements $\{X, Y, Z\}$. How do we make any permutation? The first two elements, X and Y are effectively switched by applying $XS = HS^2HS$.

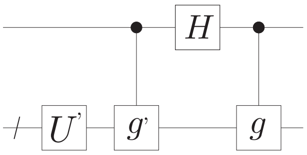
$$XS = HS^2HS \quad : \quad \{X \to -Y, Y \to -X, Z \to -Z\}.$$

We require the X to give an extra $-$ sign to both Y and Z, so that we obtain an overall minus phase, not just $Y \to -X$. The first and third elements, X and Z are switched by applying $iYH = ZXH = S^2HS^2HH = S^2HS^2$:

$$iYH = S^2HS^2 \quad : \quad \{X \to -Z, Y \to -Y, Z \to -X\}.$$

This is all we need to conclude that any normalizer operation on a single qubit can be done by using only H and S (up to an overall phase).

(b) We just proved that for a single qubit, we can apply a normalizer operation U just by using H and S. When we can apply any n-qubit normalizer operation using only H and S, we want to show that the circuit



applies U, if $U' |\psi\rangle \equiv \sqrt{2}\,\langle 0|\, U(|0\rangle \otimes |\psi\rangle)$ and that this U' is a normalizer operation we already know how to apply for n qubits.

First, the action of U. Let us rewrite it in block form (each block is $n \times n$) as

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} U' & a \\ b & c \end{bmatrix},$$

where U' was defined above, and a, b and c need to be found. The first condition on U is $UZ_1U^\dagger = X_1 \otimes g$, the second condition is $UX_1U^\dagger = Z_1 \otimes g'$. Writing these (and the unitarity condition $UU^\dagger = \mathbb{I}$) and solving for a, b and c we obtain

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} U' & g'U' \\ gU' & -gg'U' \end{bmatrix}.$$

It is now straightforward to verify that this exactly the action of the above circuit, that is

$$\begin{aligned} U &= (\text{controlled-}g)(H \otimes \mathbb{I})(\text{controlled-}g')(\mathbb{I} \otimes U') \\ &= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & g \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbb{I} & \mathbb{I} \\ \mathbb{I} & -\mathbb{I} \end{bmatrix} \begin{bmatrix} \mathbb{I} & 0 \\ 0 & g' \end{bmatrix} \begin{bmatrix} U' & 0 \\ 0 & U' \end{bmatrix}. \end{aligned}$$

Therefore we can apply any such normalizer operation U on $n+1$ qubits using only H, S and CNOT gates. The last comes from the fact that the controlled-g operation can be easily made from a CNOT sandwiched between some combination of H and S on the second qubit.

It can be easily shown that U' is an unitary gate. However, for this construction to work, we need to show that U' is in the Normalizer. Let $h \in G_n$, $|\phi\rangle$ be an n qubit state. We then have,

$$\begin{aligned} U^{'}hU^{'\dagger}(|\phi\rangle) &= 2\,\langle 0|\, U(|0\rangle\,\langle 0| \otimes h)U^\dagger(|0\rangle \otimes |\phi\rangle) \\ &= \langle 0|\,(I + X_1 \otimes g)U(I_1 \otimes h)U^\dagger(|0\rangle \otimes |\phi\rangle) \end{aligned}$$

Since $U \in N_{n+1}$, $\exists \sigma \in G_1$, $\exists h^{'} \in G_n$ such that $U(I_1 \otimes h)U\dagger = \sigma \otimes h^{'}$. We then have two possiblities.

1. Either $\sigma \in [\pm I, \pm iI, \pm Z, \pm iZ]$, then $\langle 0|\, \sigma X_1\, |0\rangle = 0$, and the second term disappears;

$$\begin{aligned} U^{'}hU^{'\dagger}\,|\phi\rangle &= \langle 0|\,(\sigma \otimes h^{'})(|0\rangle \otimes |\phi\rangle \\ &= \langle 0|\,\sigma\,|0\rangle\, h^{'}\,|\phi\rangle\,, \end{aligned}$$

Note that $(\langle 0|\,\sigma\,|0\rangle) \in [\pm 1, \pm i]$ and $(h^{'}) \in G_n$. So in this case $(U^{'}hU^{'\dagger}) \in G_n$.

2. When $(\sigma) \in [\pm X, \pm iX, \pm Y, \pm iY]$. Then $\langle 0| \sigma |0\rangle = 0$, the first term disappears. Then we have

$$U^{'} h U^{'\dagger} |\phi\rangle = \langle 0| \sigma X_1 |0\rangle (gh^{'}) |\phi\rangle$$

It should be noted that $(\langle 0| \sigma X_1 |0\rangle) \in [\pm 1, \pm i]$ and $(gh^{'}) \in G_n$, so again we have $(U^{'} h U^{'\dagger}) \in G_n$. This shows that $U^{'}$ is in the Normalizer G_n.

Now we use the fact that we need at the most An^2 number of CNOT, Hadamard and phase gates to create any element in the normalizer N_n. The operator G representing the controlled-g gate in the given circuit may be expressed as $G = \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \otimes ... \otimes \sigma_n$, where σ_i are controlled Pauli gates. Now we prove the circuit complexity of the given construction is $O(n^2)$. We prove this by induction. From the above it is clear that U' requires $O(n^2)$ gates, the implmentation of g and g' requires $O(n)$ gates each. We need a H gate between g and g' gates to implement the U gate on $n+1$ qubits. Hence, the total number of gates required to implement U on $n+1$ qubits is $O(n^2 + 2n + 1)$ $= O((n+1)^2)$ hadamard, phase and CNOT gates. This completes the proof by induction.

(c) In the previous part of the problem we found that the specific type of U can be implemented in $O(n^2)$ Hadamard, phase and CNOT gates. Now any arbitrary normalizer operation U on $n+1$ qubits can be implemented using the construction in the previous problem by additional gates that can transform the elements X and Z to someother element in the Normalizer. The number of such gates required are constant in number. Hence, the implementation of any gate $U \in N(G_{n+1})$ requires $O(n^2)$ Hadamard, phase and CNOT gates.