CMPT 409/981: Quantum Circuits and Compilation
Assignment 3 solutions

December 6, 2022

Question 1 [10 points]: Exact synthesis over the reals

1. (1 point) Observe that for any $U \in \{X, CX, CCX, H\}$ we have $\sqrt{2}^{lde(U)}U$ is an integer matrix — that is, its entries lie in $\mathbb{Z} \subset \mathbb{Z}[\sqrt{2}]$. On the other hand $lde(CH) = 1$ and further note that

$$\sqrt{2}CH = \begin{bmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

is a non-integer matrix over $\mathbb{Z}[\sqrt{2}]$. Hence it suffices to show that for any two matrices U, V over $\mathbb{Z}[\sqrt{2}]$ satisfying $\sqrt{2}^{lde(U)}U$ and $\sqrt{2}^{lde(V)}V$ are contained in $\mathbb{Z}$. Clearly

$$\sqrt{2}^{lde(U)}U\sqrt{2}^{lde(V)}V = \sqrt{2}^{lde(U)+lde(V)}UV$$

satisfies that $\sqrt{2}^{lde(U)+lde(V)}UV$ is contained in $\mathbb{Z}$, but it may be the case that $lde(UV) < lde(U)+lde(V)$, i.e. $\sqrt{2}^{lde(U)+lde(V)}UV$ is divisible by $\sqrt{2}^k$. In this case we can observe that k must be even since the only integers divisible by $\sqrt{2}$ are even integers and hence also divisible by 2. Hence $\frac{1}{2^k}\sqrt{2}^{lde(U)+lde(V)}UV = \sqrt{2}^{lde(U)+lde(V)-k}UV$ remains in $\mathbb{Z}$.

Just noting that (the integral part of) CH is not contained in $\mathbb{Z}$ was enough for full marks here — the full proof was not needed, but it is enlightening to see how one can show it.

2. (1 point) First suppose $u \equiv v \mod 2$. Hence

$$a + b\sqrt{2} = c + d\sqrt{2} + 2(e + f\sqrt{2}) = (c + 2e) + (b + 2f)\sqrt{2}$$

so $a \equiv b \mod 2$ and $c \equiv d \mod 2$.

Now suppose $a \equiv b \mod 2$ and $c \equiv d \mod 2$. Then

$$a + b\sqrt{2} = (c + 2e) + (d + 2f)\sqrt{2} = c + d\sqrt{2} + 2(e + f\sqrt{2})$$

and hence $u \equiv v \mod 2$.

3. (1 point) Suppose $u \equiv v \mod 2$ for some $u, v \neq 0$. Then

$$u + v = (a + c) + (b + d)\sqrt{2} = 2w$$

for some $w \in \mathbb{Z}[\sqrt{2}]$ because $a \equiv c \mod 2$ and $b \equiv d \mod 2$. Hence $\frac{u \pm v}{\sqrt{2}} = \sqrt{2}w$ as required.

4. (3 points) This question was a bit tricky as written (though it is doable as written). The question is really asking you to show that if $\vec{u} \neq \sqrt{2}\vec{v}$ for some $\vec{v} \in \mathbb{Z}[\sqrt{2}]^d$, then there exists an entry $u_i \neq \sqrt{2}v_i$ for any $v_i \in \mathbb{Z}[\sqrt{2}]$ such that there is another entry of $\vec{u}$ which equivalent mod 2. This then allows us to reduce the vector by adding those two entries together to get something which is divisible by $\sqrt{2}$.

   To that end, suppose $\vec{u} \neq \sqrt{2}\vec{v}$ for any such $\vec{v}$ and let $u_i \neq \sqrt{2}v_i$ for any $v_i \in \mathbb{Z}[\sqrt{2}]$. Then since

$$a + b\sqrt{2}$$

   is necessarily divisible by $\sqrt{2}$ if $a \equiv 0 \mod 2$ (explicitly, $2k + b\sqrt{2} = \sqrt{2}(b + k\sqrt{2})$), we have two cases to consider:

   - $a \equiv b \equiv 1 \mod 2$, or
   - $a \equiv 1 \mod 2$ and $b \equiv 0 \mod 2$

   case 1: $a \equiv b \equiv 1 \mod 2$**.** We note first that $|u_i|^2 \equiv 1 + 2\sqrt{2} \mod 2$ in this case. Since $||\vec{u}||^2 = \sum_{i=1}^{d} |u_i|^2 = 2^k$, we know that the $\sqrt{2}$ parts of all $|u_i|^2$ must cancel. Since the $\sqrt{2}$ part of $|u_i|^2$ is $2 \mod 4$, we know for the $\sqrt{2}$ parts to cancel there must be some entry u_j with the $\sqrt{2}$ part of $|u_j|^2$ not equal to $0 \mod 4$. Suppose $u_j = a + b\sqrt{2}$. Then $|u_j|^2 = a^2 + 2b^2 + 2ab\sqrt{2}$. Note that $2ab \equiv 0 \mod 4$ if either a or b is even, hence $u_j \equiv 1 + \sqrt{2} \equiv u_i \mod 2$.

   case 2: $a \equiv 1 \mod 2$**,** $b \equiv 0 \mod 2$**.** Again looking the the norm condition $||\vec{u}||^2 = \sum_{i=1}^{d} |u_i|^2 = 2^k$ we see that the integer parts of all $|u_i|^2$ must sum to $0 \mod 2$. Hence there must be some u_j such that $u_j \equiv 1 + b\sqrt{2} \mod 2$. Now, if $b \equiv 0$ we have $u_i \equiv u_j \mod 2$, otherwise $u_j \equiv 1 + \sqrt{2} \mod 2$ and we can apply the previous case to find a third entry u_k such that $u_j \equiv u_k$.

5. (2 points) By induction on the number of entries of $\vec{u}$ which are not divisible by $\sqrt{2}$. If there are zero such entries, then $\vec{u} = \sqrt{2}\vec{v}$ as required. For any other number of such entries k, let $u_i \neq \sqrt{2}v_i$ for any $v_i \in \mathbb{Z}[\sqrt{2}]$. Then by the previous question there exists some other entry u_j such that $u_i \equiv u_j \mod 2$. Then

$$H \begin{bmatrix} u_i \\ u_j \end{bmatrix} = \begin{bmatrix} \frac{u_i + u_j}{\sqrt{2}} \\ \frac{u_i - u_j}{\sqrt{2}} \end{bmatrix} = \sqrt{2} \begin{bmatrix} v_i \\ v_j \end{bmatrix}$$

   where the last equality holds by question 1.3. Now since $H_{i,j}\vec{u}$ applies the H gate to the i and j rows of $\vec{u}$, the number of entries of $H_{i,j}\vec{u}$ which are not divisible by $\sqrt{2}$ are $k - 2$, completing the proof.

6. (2 points) We need to synthesize the following matrix:

$$\frac{1}{2\sqrt{2}}\begin{bmatrix} 0 & 0 & 2\sqrt{2} & 0 \\ \sqrt{2} & 1+\sqrt{2} & 0 & -1+\sqrt{2} \\ \sqrt{2} & 1-\sqrt{2} & 0 & -1-\sqrt{2} \\ 2 & -\sqrt{2} & 0 & \sqrt{2} \end{bmatrix}$$

Starting from the first column we have

$$\frac{1}{2}\begin{bmatrix} 0 \\ 1 \\ 1 \\ \sqrt{2} \end{bmatrix}$$

so our first move is to apply a H gate to rows 2 and 3:

$$H_{2,3}\frac{1}{4}\begin{bmatrix} 0 \\ 1 \\ 1 \\ \sqrt{2} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 0 \\ \sqrt{2} \\ 0 \\ \sqrt{2} \end{bmatrix}$$

Our next move is to sum rows 2 and 4:

$$H_{2,4}H_{2,3}\frac{1}{4}\begin{bmatrix} 0 \\ 1 \\ 1 \\ \sqrt{2} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Finally we need to get the 1 into the top position, so we apply a two-level X gate:

$$X_{1,2}H_{2,4}H_{2,3}\frac{1}{4}\begin{bmatrix} 0 \\ 1 \\ 1 \\ \sqrt{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Looking at the bigger picture, this is where we're at:

$$X_{1,2}H_{2,4}H_{2,3}\frac{1}{2\sqrt{2}}\begin{bmatrix} 0 & 0 & 2\sqrt{2} & 0 \\ \sqrt{2} & 1+\sqrt{2} & 0 & -1+\sqrt{2} \\ \sqrt{2} & 1-\sqrt{2} & 0 & -1-\sqrt{2} \\ 2 & -\sqrt{2} & 0 & \sqrt{2} \end{bmatrix} = \frac{1}{2\sqrt{2}}\begin{bmatrix} 2\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 2\sqrt{2} & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & -2 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Moving on to the next column, we just need to add the last two rows:

$$H_{3,4}\frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ \sqrt{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

We also need to swap rows 2 and 3 to get the one in the right position. Now let's take a look at the entire matrix again:

$$X_{2,3}H_{3,4}X_{1,2}\frac{1}{\sqrt{2}}\begin{bmatrix}\sqrt{2} & 0 & 0 & 0\\ 0 & 0 & \sqrt{2} & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

So we're done! The final circuit is the reverse of this sequence of two-level operators, explicitly

$$U = H_{2,3}H_{2,4}X_{1,2}H_{3,4}X_{2,3}$$

Question 2 [10 points]: The Matsumoto-Amano normal form

1. (1 point) Note: I made a mistake here. To show that $CH = (H \mid SH)C'$ for some circuit C' over $\mathcal{C}_0$ we technically need to show that for every gate $g \in \mathcal{C}_0$, both gH and gSH can be written in this form. The question only asked to show that gH can be written in this form, so you won't be docked marks for that, but let's see the full solution.

   We prove by case distinction

   - $IH = HI$ trivially
   - $SH = SH$ trivially
   - $XH = HSSHH = HSS$
   - $\omega H = H\omega$ since ω is a scalar
   - $ISH = SHI$ trivially
   - $SSH = HX$ from the identity $X = HSSH$
   - XSH. This is the hardest case and can be shown by observing that $XS = \omega^2 SZX$:

   $$XSH = \omega^2 SZXH = SZHSS\omega^2 = SHXSS\omega^2$$

2. (4 points) Induction on the length of the sequence $C_1HC_2H\cdots C_{k-1}HC_k$. If $k = 1$ or 2 then C_1HC_2 can be written in the form $(I \mid H \mid SH)C'$ by the previous question. Now consider a sequence of length $k+1$, $C_1HC_2H\cdots C_{k-1}HC_kHC_{k+1}$. By the inductive hypothesis, write

   $$C_1HC_2H\cdots C_{k-1}HC_kHC_{k+1} = (I \mid H \mid SH)C'HC_{k+1}$$

   We know $C'HC_{k+1} = (H \mid SH)C''$ for some C'', hence we have the sequence

   $$(I \mid H \mid SH)(H \mid SH)C''$$

   To finish the proof it suffices to consider every possible case: $IH = H$ and $ISH = SH$ are both in the correct form. $HH = I$ and $SHH = IS$ are again both in the correct form. For HSH note that $HSH = S^\dagger HS^\dagger\omega = SZHSZ\omega = SHXSZ\omega$ which is in the right form. Likewise, $SHSH = HS^\dagger$ which is in the correct form.

3. (1 point) Again we have a simple case distinction:

- $IT = TI$ trivially
- $ST = TS$ trivially
- $XT = T^\dagger X\omega = TS^\dagger\omega$

4. (4 points) Induction on the length of the sequence $C_1TC_2T\cdots C_{k-1}TC_k$. The $k = 1$ or $k = 2$ cases are trivial. For a sequence of length $k + 1$,

$$C_1TC_2T\cdots C_{k-1}TC_kTC_{k+1} = (T \mid I)(HT \mid SHT)^*CTC_{k+1}.$$

Writing $C = (I \mid H \mid SH)C'$ and noting that $C'TC_{k+1} = TC''$ we have

$$(T \mid I)(HT \mid SHT)^*(I \mid H \mid SH)C'TC_{k+1} = (T \mid I)(HT \mid SHT)^*(I \mid H \mid SH)TC''$$

If we have $(T \mid I)(HT \mid SHT)^*(H \mid SH)TC'' = (T \mid I)(HT \mid SHT)^*C''$ so we're done. If on the other hand we have $(T \mid I)(HT \mid SHT)^*TC''$, then right-multiplying T, HT, or SHT by T gives us a Clifford which can be absorbed into C''. Finally if we have TC'' then we're in the correct form, which takes care of every possible case and finishes the proof.

Question 3 [3 points]: Linear reversible synthesis

1. (2 points) We have

$$A_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Let $E_{i,j}$ be the elementary row operation adding row i to row j, and $S_{i,j}$ be the row operation swapping rows i and j. Then it can be observed that

$$E_{4,5}E_{3,5}S_{3,4}E_{2,1}S_{2,4}E_{1,3}A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$E_{4,5}E_{4,3}E_{3,1}S_{3,4}E_{2,5}E_{2,1}S_{1,4}A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

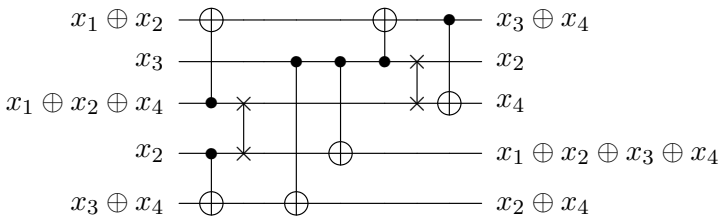
Hence

$$A = S_{1,4}E_{2,1}E_{2,5}S_{4,3}E_{3,1}E_{4,3}E_{4,5}E_{4,5}E_{3,5}S_{3,4}E_{2,1}S_{2,4}E_{1,3} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

2. (1 point) Applying Gaussian elimination to the matrix A above we get

$$E_{4,5}E_{3,1}S_{3,4}E_{2,5}E_{2,4}E_{2,1}S_{2,3}E_{1,3}A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

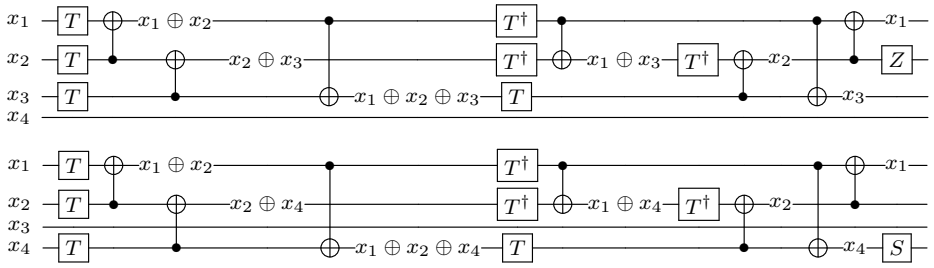
giving the circuit



which has 6 $CNOT$ gates and 2 swaps (12 $CNOT$ total), down from 9 $CNOT$ gates and 4 swap gates (21 $CNOT$ total) if we had just used our initial factorization of A.

Question 4 [2 points]: The Phase Polynomial method

To calculate the phase polynomial, we annotate the circuit (in two pieces) and collect the terms:



$$\begin{aligned} P(\vec{x}) &= x_1 + x_2 + x_3 - (x_1 \oplus x_2) - (x_2 \oplus x_3) + (x_1 \oplus x_2 \oplus x_3) - (x_1 \oplus x_3) + 4x_2 \\ &\quad + x_1 + x_2 + x_4 - (x_1 \oplus x_2) - (x_2 \oplus x_4) + (x_1 \oplus x_2 \oplus x_4) - (x_1 \oplus x_4) + 2x_4 \\ &= 2x_1 + 6x_2 + x_3 + 3x_4 - 2(x_1 \oplus x_2) - (x_2 \oplus x_3) + (x_1 \oplus x_2 \oplus x_3) - (x_1 \oplus x_3) \\ &\quad - (x_2 \oplus x_4) + (x_1 \oplus x_2 \oplus x_4) - (x_1 \oplus x_4) \end{aligned}$$

Recalling from class that since $T^2 = S$, we only need one T gate for each *odd* coefficient we find that re-synthesis will give a circuit with 8 T gates, down from the original 14. This can actually then be reduced to 7 T gates using some slightly more exotic optimizations...