CMPT 409/981: Quantum Circuits and Compilation
Assignment 3

Due November 18th at the start of class
on paper or by email to the instructor

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

In this question we will investigate the number-theoretic characterization and synthesis of circuits over $\mathcal{G} = \{X, CX, CCX, H, CH\}$. Recall that $CX = CNOT$, CCX is the Toffoli gate, and CH is the controlled-Hadamard gate

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

We will denote circuits over $\mathcal{G}$ by $\langle G \rangle$ and unitaries over a ring $\mathcal{R}$ by $\mathcal{U}(\mathcal{R})$. We define the rings

- $\mathbb{D} = \{\frac{a}{2^b} \mid a, b \in \mathbb{Z}\}$
- $\mathbb{D}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{D}\}$
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

where $\mathbb{Z}[\sqrt{2}]$ is the ring of integers of $\mathbb{D}[\sqrt{2}]$. As in the Clifford+T case, $lde(u)$ for $u \in \mathbb{D}[\sqrt{2}]$ is the **smallest k** such that $\sqrt{2}^k u \in \mathbb{Z}[\sqrt{2}]$. We extend lde to vectors and matrices in the obvious way — i.e. the smallest k such that $\sqrt{2}^k U$ has entries in $\mathbb{Z}[\sqrt{2}]$ for a matrix U.

Observe that

$$\langle \mathcal{G} \rangle \subseteq \mathcal{U}(\mathcal{R})$$

We will show that $\langle \mathcal{G} \rangle \supseteq \mathcal{U}(\mathcal{R})$ by giving an **exact synthesis method** for $\mathcal{U}(\mathcal{R})$.

1. Show first that CH **cannot** be written as a circuit over $\{X, CX, CCX, H\}$ (hint: look at the entries of $\sqrt{2}^{lde(U)} U$ for any $U \in \{X, CX, CCX, H\}$. Can you see any property which is preserved by multiplication and that X, CX, CCX and H gates satisfy but CH does not?)

2. Recall that $a \equiv b \mod 2$ for $a, b \in \mathcal{R}$ means there exists some $k \in \mathcal{R}$ such that $a = b + 2k$, where $\mathcal{R}$ is a ring such as $\mathbb{Z}$ or $\mathbb{Z}[\sqrt{2}]$.

   Let $u, v \in \mathbb{Z}[\sqrt{2}]$ and suppose $u = a + b\sqrt{2}$, $v = c + d\sqrt{2}$. Show that $u \equiv v \mod 2$ if and only if $a \equiv c \mod 2$ and $b \equiv d \mod 2$.

3. Show that for $u, v \in \mathbb{Z}[\sqrt{2}]$, if $u \equiv v \mod 2$ and $u, v \neq 0$, then $\frac{u \pm v}{\sqrt{2}} = \sqrt{2}w$ where $w \in \mathbb{Z}[\sqrt{2}]$.

4. Given a vector $\vec{u} \in \mathbb{Z}[\sqrt{2}]^d$ (i.e. a dimension d vector $\vec{u}$ over $\mathbb{Z}[\sqrt{2}]$) such that $||\vec{u}||^2 = \sum_{i=1}^d |u_i|^2 = 2^k$ for some $k \geq 1$, show that either

   - $\vec{u} = \sqrt{2}\vec{v}$ for some $\vec{v} \in \mathbb{Z}[\sqrt{2}]^d$ (i.e. $\vec{u}$ is divisible by $\sqrt{2}$), or
   - there exist two entries u_i, u_j of $\vec{u}$ such that $u_i \equiv u_j \mod 2$.

   Hint: remember that for any $u \in \mathbb{Z}[\sqrt{2}]$, $\sqrt{2}u \in \mathbb{Z}[\sqrt{2}]$.

5. Recall that for a 2×2 matrix U, a two-level $d \times d$ matrix $U_{i,j}$ is one that **acts like U on the subspace span$\{|i\rangle, |j\rangle\}$ of $\mathbb{C}^d$, and the identity everywhere else**. Explicitly,

$$U_{i,j}|i\rangle = \langle 0|U|0\rangle|i\rangle + \langle 1|U|0\rangle|j\rangle$$
$$U_{i,j}|j\rangle = \langle 1|U|0\rangle|i\rangle + \langle 1|U|1\rangle|j\rangle$$
$$U_{i,j}|h\rangle = |h\rangle, \qquad h \neq i, j$$

   Show that for $\vec{u} \in \mathbb{Z}[\sqrt{2}]^d$ where $||\vec{u}||^2 = 2^k$, $k \geq 1$. there exist a sequence $U_1 \cdots U_k$ of two-level matrices $H_{i,j}$ of dimension $d \times d$ such that $U_1 \cdots U_k\vec{u} = \sqrt{2}\vec{v}$ for some vector $v \in \mathbb{Z}[\sqrt{2}]^d$ of norm $||\vec{v}||^2 = 2^{k-1}$.

   The fact that $||\vec{v}||^2 = 2^{k-1}$ assures us that this process is terminating, and in particular terminates when we reach norm $||\vec{u}||^2 = 1$, at which point

$$\vec{u} = (-1)^b|i\rangle = Z_{0,i}^b X_{0,i}|0\rangle = H_{0,i}X_{0,i}^b H_{0,i}X_{0,i}|0\rangle$$

   for some i, giving us our column lemma for this gate set.

6. Now synthesize a sequence of two-level H, X, and Z matrices implementing the following matrix:

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

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

Recall that single-qubit Clifford+T circuits are single-qubit circuits over $\{H, T, S := T^2\}$, while single-qubit Clifford circuits are those over $\{H, S\}$. We denote these by $\mathcal{T} = \langle H, T\rangle$ and $\mathcal{C} = \langle H, S\rangle$, respectively. In this question we will investigate a complete theory of single-qubit Clifford+T circuits due to Matsumoto and Amano.

Theorem 1 (Matsumoto-Amano normal form)**.** *Any single-qubit Clifford+T circuit can be written uniquely in the form*

$$(T \mid I)(HT \mid SHT)^*\mathcal{C}$$

*where the above expression should be interpreted as a **regular expression** and the final $\mathcal{C}$ means any single-qubit Clifford operator.*

For example, $TSHTHTHSH$, while $TTTTT$ is not.

1. A particularly important subset of $\mathcal{C}$ is the subset consisting of circuits over

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad S \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \qquad X := HSSH = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \omega := (HS)^3 = \begin{bmatrix} \omega & 0 \\ 0 & \omega \end{bmatrix}$$

   Show that for any circuit C over this set $\mathcal{C}_0 = \{I, S, X, \omega\}$,

$$CH = (H \mid SH)C'$$

   (i.e. $CH = HC'$ or $CH = SHC'$) for some (possibly empty) circuit C' over $\mathcal{C}_0$.

   Hint: it suffices to show that for every gate g in $\mathcal{C}_0$, there exists a circuit C' over $\mathcal{C}_0$ such that $gH = HC'$ or $gH = SHC'$.

2. Use the previous result to show that for any Clifford circuit C, $C = (I \mid H \mid SH)C'$ for some circuit C' over $\mathcal{C}_0$.

   Hint: write an arbitrary Clifford operator as $C_1HC_2H \cdots C_{k-1}HC_k$ where each C_i is a circuit over $\mathcal{C}_0$ and perform induction on k.

3. Show that for any circuit C over $\mathcal{C}_0$, there exists a circuit C' over $\mathcal{C}_0$ such that $CT = TC'$

   Hint: similar to CH, it suffices to show that for every gate g in $\mathcal{C}_0$, there exists a circuit C' over $\mathcal{C}$ such that $gT = TC'$.

4. Finally, show that for any circuit C over $\{H, T\}$, C can be written in Matsumoto-Amano normal form,

$$(T \mid I)(HT \mid SHT)^*\mathcal{C}.$$

   Hint: write $C = C_1TC_2T \cdots C_{k-1}TC_k$ where each C_i is Clifford and use induction over k

At this point you may notice that you've given a re-writing procedure which translates an arbitrary Clifford+T circuit (single qubit) into Matsumoto-Amano normal form. In particular, you will have only used commutation rules of the form $gH \to HC'$ and $gT \to TC'$, as well as some basic simplifications such as $TT \to S$, $HH \to I$, and $Ig \to g$ for any gate g.

It turns out that these normal forms are also *unique*, in that every distinct normal form circuit is equal to a distinct unitary matrix. Since we have a complete re-writing theory which produces unique normal forms and the re-write rules are T-count non-increasing, we know immediately that the Matsumoto-Amano normal form is in fact T-count minimal. In particular, for any T-count minimal circuit C, C can be re-written uniquely in Matsumoto-Amano normal form as a circuit C', where $\tau(C') \leq \tau(C)$ for $\tau(C)$ the T-count of C.

Question 3 [3 points]: Linear reversible synthesis

When re-synthesizing sub-circuits which involve ancillas, it is sometimes the case that you need to efficiently synthesize some "glue" mapping one linear combination of bits $|A_1\vec{x}\rangle$ to another $|A_2\vec{x}\rangle$ for A_1, A_2. Given two such linear operators

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

1. Find some 5×5 matrix A over $\mathbb{Z}_2$ such that $AA_1 = A_2$.

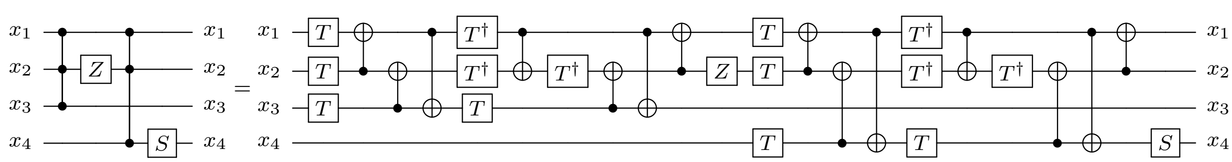
   Hint: use Gaussian elimination over $\mathbb{Z}_2$ to write A_1 and A_2 in reduced echelon form. Then note that if $E_1E_2 \cdots E_kA_1 = F_1F_2 \cdots F_lA_2$,

   $$(F_l^{-1} \cdots F_2^{-1}F_1^{-1}E_1E_2 \cdots E_k)A_1 = A_2$$

2. Synthesize a 5-qubit circuit over $CNOT$ and $SWAP$ gates implementing the unitary $U : |\vec{x}\rangle \mapsto |A\vec{x}\rangle$ where A is the unitary you found in the previous question. How does the number of gates compare to the length of your initial factorization $A = F_l^{-1} \cdots F_2^{-1}F_1^{-1}E_1E_2 \cdots E_k$?

Question 4 [2 points]: The Phase Polynomial method

Calculate the phase polynomial representation of the following $CNOT$-dihedral circuit:



How many T-gates are required to implement this operator via re-synthesis? Remember that $T^2 := S$.