The Pauli operators are $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
Let $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

1. [**2 marks**] *Universality*

   Is the following gate set universal?

   $$A = \{CNOT, X, Z\}$$

2. [**3 marks**]

   Give a protocol that wins the following game with probability $\frac{2}{3}$.

   An adversary does one of the following (with no restriction on the probability with which she chooses option 1 or 2):

   1) Gives you either $|0\rangle$ or $|1\rangle$, with equal probability.

   OR

   2) Gives you $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

   You must guess whether the adversary performed 1) or 2).

3. *SWAP testing* [**7 marks**]

   Let $SWAP$ denote the two-qubit gate that swaps the two qubits. So $SWAP|a\rangle|b\rangle = |b\rangle|a\rangle$.

   Recall that $SWAP$ has eigenvalues 1 and -1.

   (a) Give a 3-qubit circuit for measuring the eigenvalues of the $SWAP$ operator on a 2-qubit input (and one ancilla qubit). You may use a controlled-$SWAP$ gate, and any other standard quantum gates.

   (b) Note that for any one-qubit state $|\psi\rangle$, $SWAP|\psi\rangle|\psi\rangle = |\psi\rangle|\psi\rangle$, and thus $|\psi\rangle|\psi\rangle$ lies in the eigenspace of eigenvalue $+1$.

   Let $|\psi^\perp\rangle$ denote a one-qubit state that is orthogonal to $|\psi\rangle$ (so $\langle\psi|\psi^\perp\rangle = 0$).

   Find a 2-qubit state $|\psi_{sym}\rangle$ in the $+1$ eigenspace of $SWAP$ and a 2-qubit state $|\psi_{antisym}\rangle$ in the -1 eigenspace of $SWAP$ such that

   $$|\psi\rangle|\psi^\perp\rangle = \frac{1}{\sqrt{2}}|\psi_{sym}\rangle + \frac{1}{\sqrt{2}}|\psi_{antisym}\rangle.$$

   (You can express $|\psi_{sym}\rangle$ and $|\psi_{antisym}\rangle$ in terms of $|\psi\rangle$ and $|\psi^\perp\rangle$.)

   (c) Suppose you are given one of two states, for an unknown $|\psi\rangle$:

   i. $|\psi\rangle|\psi\rangle$
   or
   ii. $|\psi\rangle|\psi^\perp\rangle$

   Show how to guess which situation is the case with probability $\frac{2}{3}$ of guessing correctly (without making assumptions about the a priori probability of these two possibilities).

4. *Hadamard test* **[3 marks]**

   Consider two quantum states $|\psi\rangle$ and $|\phi\rangle = U|\psi\rangle$, and suppose we are able to implement a controlled-U. Suppose we start in the state $(|0\rangle + |1\rangle)|\psi\rangle$ and apply the controlled-U, followed by a Hadamard gate and measurement on the control qubit. What is the probability of measuring a $|0\rangle$ on the first qubit? (your answer should depend on $\langle\psi|\phi\rangle$)

5. **[3 marks]** For any subspace S of the vector space $\{0,1\}^n$ (over $\mathbf{Z}_2$) define $S^\perp = \{\mathbf{t} \in \{0,1\}^n \mid \mathbf{s}\cdot\mathbf{t} = 0 \text{ for all } \mathbf{s} \in S\}$.

   Let $|\mathbf{x}+S\rangle = \frac{1}{\sqrt{|S|}}\sum_{\mathbf{y}\in S}|\mathbf{x}\oplus\mathbf{y}\rangle$. Show that

$$H^{\otimes n}|\mathbf{x}+S\rangle = \sqrt{\frac{|S|}{2^n}}\sum_{\mathbf{z}\in S^\perp}(-1)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle.$$

   Hint: Show that for any $\mathbf{z} \in Z_2^n$, either $\mathbf{z} \in S^\perp$ or $\mathbf{z}$ is perpendicular to exactly half of the elements of S.

6. **[2 marks]** *eigenvalues of the QFT*

   (a) Find a concise description of the operation formed by the square of QFT_N.

   (b) What is smallest positive integer m such that $QFT_N^m = I$?

7. **[4 marks]** Consider the cyclic shift operator S on three qubits:

$$|x\rangle|y\rangle|z\rangle \mapsto |z\rangle|x\rangle|y\rangle$$

   for all $x, y, z \in \{0,1\}$.

   (a) What are the eigenvalues of S?

   (b) For each eigenvalue, write a basis of eigenvectors for the corresponding eigenspace.

   (c) Express the state

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

   as a linear combination of the given eigenvectors.

   (d) Express the state $|0\rangle|0\rangle|1\rangle$ as a linear combination of the given eigenvectors.

8. **[3 marks]** *Modular arithmetic and factoring*

   Let r be the order of 2 mod 35.

   (a) **1 mark** Find r.

   (b) **1 mark** What is 2^{601} mod 35?

   (c) **1 mark** Find GCD$(35, 2^{\frac{r}{2}} - 1)$ and GCD$(35, 2^{\frac{r}{2}} + 1)$.