The profound study of nature is the most fertile source of mathematical discovery. - Joseph Fourier

Problem Set 9

PCMI USS, Summer 2023

1. (**Who's in control here?**)

   (a) Let C_1 represent the CNOT (controlled-NOT) operation, with the first qubit being the control bit, and the second being the target qubit. Remind yourself how CNOT works, and write down the matrix form of C_1 with respect to the standard ordered basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $\mathbf{C}^2 \otimes \mathbf{C}^2$.

   (b) Now let C_2 be the CNOT operation where the second qubit is the control and the first is the target. Write the matrix for C_2. Write the quantum circuit representation for C_1 and C_2. (By convention, the first qubit is the top wire, and the second qubit is the bottom wire.)

   (c) Now consider the ordered Hadamard basis $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$. Explain how you know that this is an orthogonal basis of $\mathbf{C}^2 \otimes \mathbf{C}^2$. Apply C_1 to each of these basis elements, and express your answers in the Hadamard basis.

   (d) Use your answer to (c) to write the matrix of C_1 in the Hadamard basis. What do you observe?

   (e) Let $H_2 = H \otimes H$ be the usual Hadamard transformation on $\mathbf{C}^2 \otimes \mathbf{C}^2$. Since this is the transformation that takes the standard basis to the Hadamard basis, explain why your result from (d) proves the matrix equation $H_2 C_1 H_2 = C_2$. Draw a quantum circuit diagram to express the operator $H_2 C_1 H_2$ and a quantum circuit diagram to express the operator C_2. You have shown that these circuits are *equivalent*; the two circuits compute the same unitary operator.

   (f) You conclude from (e) that the basis change $H \otimes H$ interchanges to roles of the control and target bits! Maybe you find this cool and strange in a quantumy kind of way. However, your uncle Vince is skeptical. "There's no way this can be right! I mean, the operation C_1 uses the first bit as a control, so C_1 does not change the first qubit at all; the second qubit does change, depending on the value of the first qubit. So it shouldn't matter what basis you use. The operator $H \otimes H$ changes basis on the first qubit, and separately on the second qubit, there's no way that's going to change which qubit is the control." Does Vince have a point? If you disagree, what can you say to convince Vince?

2. (**Circulant Matrices**)

   (a) Let A be an $N \times N$ matrix. For convenience, index the rows and columns of A by $0, \ldots, N-1$. We say that A is a *circulant matrix* if the entry A_{jk} depends only on the difference $j - k \mod N$. To get the idea, write down a general 4×4 circulant matrix.

(b) Let C_N be the set of all $N \times N$ circulant matrices. Is C_N a vector subspace of the space of all $N \times N$ matrices? If so, what is the dimension of C_N? Can you find a nice basis?

(c) Do your basis elements commute with each other? Does that mean that any two circulant matrices commute?

(d) Is C_N closed under matrix multiplication?

(e) Show that the Fourier transform diagonalizes any circulant matrix. [You might recall results from the last problem set, where you showed that the shift operator is diagonalized by F.] If A is a circulant with first column $(x_0, \dots, x_{N-1})$, write an expression for the eigenvalues of A.

(f) Is the converse true? That is, if A is diagonalized by F, must A be a circulant matrix?

3. (**Selective Phase Change**) Suppose there is a function $f : \{0, \dots, N-1\} \to \mathbb{Z}_2$ and λ is a unit complex number. You wish to create a quantum circuit to perform a λ phase on all basis states $|s\rangle$ where $f(s) = 1$, and leave the other basis states unphased. That is you wish to perform the map $Q : \mathbf{C}^N \to \mathbf{C}^N$ that acts on the standard basis by

$$Q|j\rangle = \begin{cases} |j\rangle & \text{if } f(j) = 0 \\ \lambda|j\rangle & \text{if } f(j) = 1. \end{cases}$$

You are given oracle access to the values of f. As usual the oracle $\mathcal{O}_f$ operates on $\mathbf{C}^N \otimes \mathbf{C}^2$ (query tensor response), by

$$\mathcal{O}_f|x, b\rangle = |x, b \oplus f(x)\rangle.$$

(a) Suppose $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$. Write an expression for $Q|\psi\rangle$. (If notationally convenient, introduce the set $S = f^{-1}(1)$.)

(b) Suppose you take the state $|\psi\rangle|0\rangle$ and apply $\mathcal{O}_f$. What is the state of your system now?

(c) Let R_λ be the single qubit operation that fixes $|0\rangle$ and sends $|1\rangle$ to $\lambda|1\rangle$. Explain why R_λ is unitary.

(d) Take your the output state you computed in (b), and now apply R_λ to the second register. What is the state of your system now? Give your best incorrect argument that you have computed $Q|\psi\rangle$, and have your groupmates refute it (or refute it yourself.)

(e) What can you do now finish the computation of $Q|\psi\rangle$?

4. (**The Group Algebra**) Let G be an abelian group, and let $N = |G|$. The *group algebra* of G over $\mathbf{C}$ is a vector space $\mathbf{C}^G$ with one basis element $|g\rangle$ for each $g \in G$. Thus every element $|\psi\rangle$ in $\mathbf{C}^G$ can be written uniquely as

$$|\psi\rangle = \sum_{g \in G} \alpha_g |g\rangle,$$

where each $\alpha_g \in \mathbf{C}$

(a) Convince yourself that $\mathbf{C}^G$ is an N-dimensional complex inner product space, and further that the equation

$$|g_1\rangle|g_2\rangle = |g_1 + g_2\rangle$$

can be used to turn $\mathbf{C}^G$ into a commutative ring. (Thus we say that $\mathbf{C}^G$ is an *algebra* over $\mathbf{C}$.)

(b) Let $G = \mathbb{Z}_N$. Describe $\mathbf{C}^G$ in your own terms. Sometimes people say that the group algebra of $\mathbb{Z}_N$ is the $N \times N$ circulant matrices. Does this make intuitive sense? Make it rigorous by showing that $\mathbf{C}^{\mathbb{Z}_N}$ is isomorphic to the algebra of circulant matrices.

(c) Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Can you find a subspace of 4×4 matrices that you could call the group algebra of G (in a way similar to (b)). What about other abelian groups?

(d) If G is a group, then the *character group* of G, denoted $\hat{G}$, is the set of all characters of G under pointwise multiplication. Show that this gives $\hat{G}$ the structure of an abelian group. Give some examples. Are G and $\hat{G}$ isomorphic in your examples?

(e) The Fourier transform over an arbitrary abelian group can then be defined as a linear map $F_G : \mathbf{C}^G \to \mathbf{C}^{\hat{G}}$ with

$$F_G|g\rangle = \frac{1}{\sqrt{N}} \sum_{\chi \in \hat{G}} \chi(g)|\chi\rangle$$

Understand how the cases $G = \mathbb{Z}_N$ and $G = (\mathbb{Z}_2)^n$ work.

(f) Let G be an abelian group. Let $a \in G$ and consider the operator $T_a : \mathbf{C}^G \to \mathbf{C}^G$ defined on a basis by

$$T_a|g\rangle = |g + a\rangle.$$

Compute $F_G T_a F_G^\dagger$ and show that this operator is diagonal in the character basis. How about $F_G^\dagger T_a F_G$?

(g) The result of (f) is a generalization of the fact the the usual Fourier transform F_N (over $\mathbb{Z}_N$) diagonalizes the shift operator. What other statements about the usual discrete Fourier transform carry over to arbirtrary abelian groups? E.g., what is the circuit complexity of computing the Fourier transform over G?

(h) Does any of this work for nonabelian groups?