Quantum algorithms (CMSC 858Q) Spring 2017

ASSIGNMENT 2 due Thursday, March 16 (in class)

Problem 1 (*Weak Fourier sampling fails for the symmetric group*).

Consider the hidden subgroup problem in an arbitrary finite group G.

a. Compute the distributions over $\hat{G}$ that are observed when we perform weak Fourier sampling in two cases: the hidden subgroup is trivial, or the hidden subgroup is $\{1, \pi\}$ where π is an involution. Your answer should be expressed in terms of the characters of G.

b. Show that the total variation distance between these two distributions is upper bounded by $\sqrt{\frac{1}{|G|} \sum_{\sigma \in \hat{G}} |\chi_\sigma(\pi)|^2}$.

c. Prove that $\sum_{\sigma \in \hat{G}} |\chi_\sigma(\pi)|^2 = |G|/|\mathrm{conj}(\pi)|$, where $\mathrm{conj}(\pi)$ denotes the conjugacy class of G to which π belongs. (Hint: Use the orthogonality relations for the character table of G.)

d. Let $G = S_n$, the symmetric group on n items, and find a choice of π for which the total variation distance is exponentially small in n. This shows that weak Fourier sampling fails to solve the hidden subgroup problem in S_n.

In fact, there are considerably stronger results about the power of Fourier sampling for the HSP in S_n. Strong Fourier sampling fails (measuring in *any* basis), and indeed, joint measurments on $\Omega(n \log n)$ registers are required.

Problem 2 (*Nonabelian Fourier sampling for the dihedral group*).

In lecture, we attacked the hidden subgroup problem over the dihedral group of order $2N$,

$$D_N := \langle r, s \colon r^2 = s^N = rsrs = 1 \rangle,$$

using the Fourier transform over the cyclic group $\mathbb{Z}_N$. In this problem you will show that this is essentially the same as performing the nonabelian Fourier transform over D_N. You will also give a representation-theoretic interpretation of Kuperberg's algorithm.

For reference, the irreducible representations of D_N are as follows: there are two one-dimensional irreps, σ_{triv} and σ_{sign}, with

$$\sigma_{\mathrm{triv}}(r) := 1 \qquad \sigma_{\mathrm{triv}}(s) := 1$$
$$\sigma_{\mathrm{sign}}(r) := -1 \qquad \sigma_{\mathrm{sign}}(s) := 1;$$

and $\lceil N/2 \rceil - 1$ two-dimensional irreps, σ_j for $j = 1, 2, \ldots, \lceil N/2 \rceil - 1$, with

$$\sigma_j(r) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_j(s) := \begin{pmatrix} \omega_N^j & 0 \\ 0 & \omega_N^{-j} \end{pmatrix}.$$

(If N is even then there are two additional one-dimensional irreps, but let us assume for simplicity that N is odd.)

a. Consider the HSP in D_N with the hidden subgroup $\{1, rs^\alpha\}$. Write down the state obtained by Fourier sampling over D_N, assuming you measure a two-dimensional irrep σ_j. Compare to the possible states obtained by Fourier sampling over $\mathbb{Z}_N$, obtaining some measurement outcome $k \in \mathbb{Z}_N$ with $k \neq 0$, and describe a correspondence between the two procedures. (Hint: There are more possible values of k than values of j, so each value of j must correspond to multiple values of k.)

b. Describe a similar correspondence between the one-dimensional irreps of D_N and the state obtained when Fourier sampling over $\mathbb{Z}_N$ yields the measurement outcome 0.

c. Decompose the representation $\sigma_j \otimes \sigma_k$ as a direct sum of irreducible representations of D_N.

d. In view of the correspondence established in parts a and b, interpret the combination operation used in Kuperberg's algorithm in the light of representation theory.

e. *Challenge problem:* Give a quantum circuit for F_{D_N} that uses $F_{\mathbb{Z}_N}$ as a subroutine.

Problem 3 (*Classical random walk on glued trees*).

Consider a graph obtained by taking the union of two balanced binary trees of height n and joining their leaves by some cycle that alternates between the two sets of leaves. Suppose that a classical random walk (either continuous- or discrete-time, according to your preference) starts at the root of one of the trees. Prove that the probability of reaching the opposite root after any amount of time has passed is $2^{-\Omega(n)}$.

Problem 4 (*The spectrum of a product of reflections*).

In lecture, we defined a discrete-time quantum walk on an n-vertex graph as the product of a reflection on $\mathbb{C}^n \otimes \mathbb{C}^n$ and the same reflection with the two systems interchanged. To analyze the walk, we computed the spectrum of this product of reflections. In this problem, you will generalize that calculation to the product of two arbitrary reflections.

Consider two subspaces

$$\mathcal{A} := \mathrm{span}\{|\psi_1\rangle, \ldots, |\psi_a\rangle\} \qquad\qquad \mathcal{B} := \mathrm{span}\{|\phi_1\rangle, \ldots, |\phi_b\rangle\}$$

of $\mathbb{C}^m$, where $\langle\psi_j|\psi_k\rangle = \delta_{jk}$ and $\langle\phi_j|\phi_k\rangle = \delta_{jk}$. Let

$$\Pi := \sum_{j=1}^{a} |\psi_j\rangle\langle\psi_j| \qquad\qquad \Sigma := \sum_{j=1}^{b} |\phi_j\rangle\langle\phi_j|$$

denote projections onto the two subspaces, let $R := 2\Pi - I_m$ and $S := 2\Sigma - I_m$ denote reflections about the subspaces, and let $U := RS$ denote their product. Finally, let D denote the $a \times b$ matrix with entries $D_{jk} = \langle\psi_j|\phi_k\rangle$. You will show how the spectrum of U can be obtained from the singular value decomposition of D.

a. Let $|\alpha\rangle$ and $|\beta\rangle$ denote left and right singular vectors of D, respectively, with the same singular value σ. The left singular vector $|\alpha\rangle \in \mathbb{C}^a$ can be mapped to a vector $A|\alpha\rangle \in \mathbb{C}^m$ by applying the isometry $A := \sum_{j=1}^{a} |\psi_j\rangle\langle j|$. Similarly, the right singular vector $|\beta\rangle \in \mathbb{C}^b$ can be mapped to a vector $B|\beta\rangle \in \mathbb{C}^m$ by the isometry $B := \sum_{j=1}^{b} |\phi_j\rangle\langle j|$. Show that the subspace $\mathrm{span}\{A|\alpha\rangle, B|\beta\rangle\}$ is invariant under the action of U.

b. Diagonalize the action of U within this subspace to obtain one or two eigenvectors of U. When do you obtain one, and when do you obtain two?

c. Compute the eigenvalues of U corresponding to these eigenvectors.

d. How many eigenvectors of U are obtained by the procedure outlined above? What are the remaining eigenvectors of U and their corresponding eigenvalues?