Quantum Proofs, Semester A 2024

Homework # 2 **due: 5pm, January 15th, 2024**

Ground rules:

Homework is due through Moodle. If you are having issues with this, email the instructor (thomas.vidick@weizmann.ac.il) or drop your work in my mailbox at the top of the central stairs in Ziskind. Solutions can be latexed or handwritten. In the latter case, please make sure that your handwriting is legible. Special care should be taken in writing up a precise solution. If I am not able to follow the logic in your argument, if there is a small gap or an uncovered case, you will lose points.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded.

The first two exercises are background calculations that are useful to understand the lectures. The first one "should" be routine, but it may be new to students with no background in quantum information; if you are not yet familiar with the Schmidt decomposition then now is the time to learn it! The second exercise requires more steps (the statement is shorter, but I expect its solution to be longer, than that of the first exercise), but there is no subtlety — I want you to gain a good understanding of how a general measurement can be performed in the elementary circuit formalism from class.
The third exercise is almost done is lecture (on 02/01); I am asking you to go over it by yourselves to make sure you get all the terms in the Kitaev construction. The fourth exercise is longer, and requires more ideas, than the others. As noted in the exercise I am not asking you to formally show soundness of your construction — I am only asking for a clear description of your construction, from which the desired properties should be clear.

Any changes since the first posting will be marked in blue.

Problems:

1. (2 points) **Product test**

   Consider the following quantum algorithm, that takes as input two $2n$-qubit quantum states $|\psi\rangle$ and $|\psi'\rangle$ as input:

   (a) Initialize an ancilla qubit in state $|0\rangle$;

   (b) Apply a Hadamard on the ancilla;

(c) Controlled on the ancilla being in state $|1\rangle$, exchange the first n qubits of $|\psi\rangle$ with the first n qubits of $|\psi'\rangle$;

(d) Apply a Hadamard on the ancilla;

(e) Measure the ancilla in the computational basis. Accept if the outcome is 0.

To be clear, on an input of the special form $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$, $|\psi'\rangle = |\phi'_1\rangle \otimes |\phi'_2\rangle$ where each $|\phi_i\rangle, |\phi'_i\rangle$ is on n qubits for $i \in \{1, 2\}$, this algorithm generates the following sequence of states:

$$\begin{aligned}
|\phi_1\rangle|\phi_2\rangle|\phi'_1\rangle|\phi'_2\rangle &\mapsto |0\rangle|\phi_1\rangle|\phi_2\rangle|\phi'_1\rangle|\phi'_2\rangle \\
&\mapsto |+\rangle|\phi_1\rangle|\phi_2\rangle|\phi'_1\rangle|\phi'_2\rangle \\
&\mapsto \frac{1}{\sqrt{2}}\big(|0\rangle|\phi_1\rangle|\phi_2\rangle|\phi'_1\rangle|\phi'_2\rangle + |1\rangle|\phi'_1\rangle|\phi_2\rangle|\phi_1\rangle|\phi'_2\rangle\big) \\
&\mapsto \frac{1}{\sqrt{2}}\big(|+\rangle|\phi_1\rangle|\phi_2\rangle|\phi'_1\rangle|\phi'_2\rangle + |-\rangle|\phi'_1\rangle|\phi_2\rangle|\phi_1\rangle|\phi'_2\rangle\big) ,
\end{aligned}$$

followed by a measurement of the first qubit in the standard basis.

(a) For input states in product form as above, compute the probability that this algorithm accepts.

(b) Now suppose that the input is two copies of the *same* arbitrary pure state $|\psi\rangle = |\psi'\rangle$. Compute the probability that the algorithm accepts, as a function of the reduced density matrix ρ of $|\psi\rangle$ on the first n qubits. *[Hint: You should know that $|\psi\rangle$ can be written in the form $|\psi\rangle = \sum_i \sqrt{\lambda_i}|u_i\rangle|v_i\rangle$, for orthonormal families $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ — this is called the "Schmidt decomposition". Then, $\rho = \sum_i \lambda_i |u_i\rangle\langle u_i|$. Use the Schmidt decomposition to analyze the algorithm.]*

(c) Deduce that, if the algorithm accepts $|\psi\rangle$ and $|\psi'\rangle = |\psi\rangle$ with probability at least $1 - \varepsilon$, then $|\psi\rangle$ is within trace distance at most η of a product state — give an upper bound on η as a function of ε.

2. (2 points) **Measuring a Hermitian operator**

Let $q \geq 1$ and H a Hermitian matrix on the space $\mathcal{H} = (\mathbb{C}^2)^{\otimes q}$ of q qubits such that $\|H\| \leq 1$. Describe a measurement procedure on $\mathcal{H}$ that returns an outcome $b \in [-1, 1]$ such that for any density ρ on q qubits, on expectation, $\mathbf{E}[b] = \mathrm{Tr}(H\rho)$. The "measurement procedure" is only allowed to perform *arbitrary unitary* operations, ancilla creation in state $|0\rangle$, and measurements in the *standard* basis.

3. (2 points) **Basic properties of the Feynman-Kitaev construction**

Let V_z be a QMA verifier circuit with T gates (represented by unitaries $U_1, U_2, \ldots, U_T$, each acting at most 2 qubits), q proof qubits, and m ancilla qubits. Consider the

Feynman-Kitaev Hamiltonian H corresponding to V_z,

$$H_z = \sum_{j=1}^{m} H_j^{(A)} + \sum_{t=0}^{T-1} H^{(t \to t+1)} + H^{(O)} \ ,$$

as described in class. In particular, recall that

$$H^{(t \to t+1)} = \frac{1}{2}\big(\mathbb{I} \otimes |t+1\rangle_C - U_{t+1}^\dagger \otimes |t\rangle\big)\big(\mathbb{I} \otimes \langle t+1|_C - U_{t+1} \otimes \langle t|\big) \ .^{1}$$

Let H'_z be the same as H_z, with the term $H^{(O)}$ omitted.

(a) Show that any ground state of H'_z must also be a ground state of each of the individual terms $H_j^{(A)}$ and $H^{(t \to t+1)}$.

(b) Determine the ground energy of H'_z.

(c) Determine the dimension of the ground space of H'_z, and give a basis for this ground space.

4. (5 points) **QMA with log-depth verifier**

(a) Let V be a QMA verification circuit acting on q proof qubits, m ancilla qubits, and with T gates in total, such that the completeness and soundness parameters of V are $1-2^{-p(n)}$ and $2^{-p(n)}$ respectively. Show that there is a verification circuit V', acting on q proof qubits and $O((q+m)T)$ ancilla qubits and with $O((q+m)T)$ gates, such that V' has the same completeness and soundness parameters as V (i.e. V' performs the same computation as V) and furthermore each qubit of V' (proof or ancilla) takes part in a *constant* number of gates.

(b) Show how to appropriately modify the Feynman-Kitaev construction (with unary clock) so that when it is applied to V', it returns a local Hamiltonian such that furthermore each qubit is acted on by at most a *constant* number of local terms. Here, you do not need to prove soundness of your modified construction; only state what modification you suggest making to satisfy the "constant degree" constraint. *[Hint: be mindful of the clock qubits!]*

(c) Show that for any promise problem $L = (L_y, L_n)$ in QMA, there is a polynomial-time computable family of verifiers $z \mapsto V_z$ for L such that for each z, V_z is specified by a quantum circuit of depth $O(\log |z|)$.[2] Here the constant implicit in $O(\cdot)$ may depend on L, but not on z. *[Hint: use the previous questions. It only remains to design a logarithmic-depth* QMA *verifier for verifying a local Hamiltonian as in part (b). Describe how this verifier proceeds, and argue that it has the required depth. You are not asked to formally show soundness of the verifier.]*

[1] In class, apparently, there was a typo $t-2 \leftrightarrow t+1$.

[2] The depth of a circuit is the smallest number of layers that its gates can be organized in. Multiple gates are allowed to operate in parallel if they act on disjoint sets of wires.