# 2021 Quantum Computing Homework Nr. 10

András Gilyén

November 23, 2021

Homework exercises with a bonus exercise (Exercise 3) providing the possibility to earn 5 bonus points. On the last page you can find some hints where indicated by (**H**).

## Reminder

Let us recall the definition of the language class QMA.

**Definition 1** (The language class QMA)**.** *Let $L \subseteq \{0,1\}^*$ be a language. The language $L$ belongs to the class* QMA *if there exists a classical Truing machine $T$ that on input $x \in \{0,1\}^*$ outputs the description of a quantum circuit $V_x$ in time $\mathcal{O}(\mathrm{poly}\,|x|)$ that acts on $n_{|x|} + m_{|x|} = \mathcal{O}(\mathrm{poly}\,|x|)$ qubits* and also two numbers $0 \leq b_{|x|} < a_{|x|} \leq 1$ satisfying $\frac{1}{a_{|x|}-b_{|x|}} = \mathcal{O}(\mathrm{poly}\,|x|)$, such that for*

$x \in L$ : *there exists an $m_{|x|}$-qubit witness $|\psi\rangle$ such that upon measuring the state $V_x|0\rangle^{\otimes n_{|x|}}|\psi\rangle$ the probability of finding the 1st qubit in state $|0\rangle$ has probability at least $a_{|x|}$,*

$x \notin L$ : *for any $m_{|x|}$-qubit state $|\phi\rangle$ upon measuring the state $V_x|0\rangle^{\otimes n_{|x|}}|\phi\rangle$ the probability of finding the 1st qubit in state $|0\rangle$ has probability at most $b_{|x|}$.*

## Exercises

**1.**) From Ronald's lecture notes [dW19, Chapter 12 Exercise 2]

**2.**) From Ronald's lecture notes [dW19, Chapter 12 Exercise 3]:

**3.**) [Fast QMA gap amplification] In classical computing when one works with the complexity class MA, the witness can be reused by running the verification circuit several times. Thus one can exponentially boost the gap between acceptance / rejection probabilities. However, in QMA there is a measurement involved in the defintion that could destroy the witness state, so it is not immediately clear if one can boost the success probability without requesting additional copies of the witness state. This obstacle was overcome by Marriott and Watrous. Here you can give a simpler and improved version of their result.

Suppose that $L \in$ QMA as in Definition 1. Modify the verifier circuit $V_x$ such that the acceptance probability thresholds become $a' := 1-\varepsilon$ and $b' := \varepsilon$ using singular value transformation of degree $\mathcal{O}\left(\frac{1}{\sqrt{a_{|x|}}-\sqrt{b_{|x|}}}\log\left(\frac{1}{\varepsilon}\right)\right)$.

(a) Give a good lower bound on $\left\|\left(\langle 0| \otimes I_{n_{|x|}+m_{|x|}-1}\right) V_x \left(|0\rangle^{\otimes n_{|x|}} \otimes I_{m_{|x|}}\right)\right\|$ for $x \in L$.

(b) Give a good upper bound on $\left\|\left(\langle 0| \otimes I_{n_{|x|}+m_{|x|}-1}\right) V_x \left(|0\rangle^{\otimes n_{|x|}} \otimes I_{m_{|x|}}\right)\right\|$ for $x \notin L$.

(c) How does $\|A\|$ relate to the largest singular value of $A$?

(d) Use singular value transformation of degree $\mathcal{O}\left(\frac{1}{\sqrt{a_{|x|}}-\sqrt{b_{|x|}}}\log\left(\frac{1}{\varepsilon}\right)\right)$ to boost the acceptance probability thresholds to $a' := 1-\varepsilon$ and $b' := \varepsilon$. (**H**)

*By $|x|$ here we denote the length of the string $x$, rather than its Hamming weight. Whenever we use $|x|$ as an index that quantity can only depend on $|x|$ rather than $x$. For technical reasons we also assume that $a_{|x|}, b_{|x|}, n_{|x|}, m_{|x|}$ are calssically computable in time $\mathcal{O}(\mathrm{poly}\,|x|)$.

## Hints

Exercise 3: Recall quantum singular value transformation from Homework Sheet Nr. 8. You may use the fact that for every $t, \delta, \varepsilon \in (0,1)$ there is an efficiently computable odd polynomial $P\colon [-1,1] \mapsto [-1,1]$ of degree $\mathcal{O}\left(\frac{\log(1/\varepsilon)}{\delta}\right)$ such that $P(x) \geq 1-\varepsilon$ for every $x \in [t+\delta, 1]$ and $|P(x)| \leq \varepsilon$ for every $x \in [0, t-\delta]$.

## References

[dW19] Ronald de Wolf. Quantum computing: Lecture notes, 2019. arXiv: 1907.09415