Quantum complexity, relativized worlds, and oracle separations

by Dimitrios I. Myrisiotis.

Abstract.

The complexity class QMA, defined by Watrous, in 2000, is the quantum analogue of MA, defined by Babai, in 1985, which, in turn, is a generalization of the class NP. The class MA generalizes the class NP in the sense that the verification procedure of the purported proof, put forth by the prover, is carried out by a probabilistic machine, rather than a deterministic one—as the definition of the class NP demands.

In 2014, Grilo, Kerenidis, and Sikora, proved that the quantum proof, in the setting of QMA, may always be replaced by, an appropriately defined, quantum subset state—without any conceptual loss. That is, $\mathsf{QMA} \subseteq \mathsf{SQMA}$. Grilo et al., named their new class SQMA, for *subset-state quantum Merlin-Arthur*. Thus, one could write that $\mathsf{SQMA} = \mathsf{QMA}$, as the inclusion $\mathsf{SQMA} \subseteq \mathsf{QMA}$ holds trivially.

After this result, by Grilo, Kerenidis, and Sikora, Fefferman and Kimmel, in 2015, used this new characterization of QMA, and further proved that there exists some quantum oracle $\mathcal{A}$—similar to that Aaronson and Kuperberg introduced, and used, in 2006, to show that $\mathsf{QMA}_1^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}}$—which is such that $\mathsf{QMA}^{\mathcal{A}} = \mathsf{SQMA}^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}}$. Here, QCMA is that version of QMA, defined by Aharonov, and Naveh, in 2002, in which the purported proof is purely-classical, that is, a bitstring, and QMA_1 is the *perfect completeness* version of QMA. In their separation, Fefferman and Kimmel introduced, and used, an interesting template to obtain oracle separations against the class QCMA.

Drawing upon this recent result, by Fefferman and Kimmel, we prove that there exists some quantum oracle $\mathcal{A}$, such that $\mathsf{SQMA}_1^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}}$. We note that the class SQMA_1 is the *perfect completeness* version of the class SQMA. In our proof, we used the template of Fefferman and Kimmel, a modified version of their basic quantum oracle construction, as well as the basic decision problem, that they themselves used for their separation. Note that our result implies that of Fefferman and Kimmel, as the inclusion $\mathsf{SQMA}_1 \subseteq \mathsf{SQMA}$ holds.

After we state and prove our result, we take a detour to explore a bit the world of oracle separations, both in the classical and the quantum setting. That is, we explore some results, and their underlying methods, about classical and quantum oracles being employed for proving separations—about classical, or quantum, complexity classes. Hence, we investigate some gems pertaining to the, not few at all, nor uninteresting, privileged relativized worlds.

Finally, we return, to the research setting, to approach the open question of whether there exists some classical, or quantum, oracle $\mathcal{A}$, such that $\mathsf{QMA}_1^{\mathcal{A}} \not\subseteq \mathsf{SQMA}_1^{\mathcal{A}}$, or not. We record our efforts, and some of our first ideas, thus far.
