The exercises come from Ronald de Wolf's lecture notes [dW19, Chapters 13].

Exercises

1.) (**H**) [dW19, Exercise 13.1]: The following problem is a decision version of the factoring problem:

Given positive integers N and k, decide if N has a prime factor $p \in \{k, \ldots, N-1\}$.

Show that if you can solve this decision problem efficiently (i.e., in time polynomial in the input length $n = \lceil \log N \rceil$), then you can also find the prime factors of N efficiently.

2.) [dW19, Exercise 13.3]: This exercise shows how to use BQP-algorithms as subroutines in other BQP-algorithms.

(a) (**H**) Suppose L is a language in BQP. Let f be the corresponding Boolean function, so $f(x) = 1$ iff $x \in L$. Show that there is a $w \leq \text{poly}(n)$ and a polynomial-size quantum circuit U that implements the following map for all $x \in \{0,1\}^n$:

$$|x, 0^{w+1}\rangle \mapsto \sqrt{p}|x, f(x)\rangle|\phi(x)\rangle + \sqrt{1-p}|x, 1-f(x)\rangle|\psi(x)\rangle,$$

where $p \geq 1 - \exp(-n)$, and $|\phi(x)\rangle$ and $|\psi(x)\rangle$ are states of the w-qubit workspace.

(b) Show that there is a polynomial-size quantum circuit V that (when restricted to the subspace where the workspace qubits are $|0\rangle$) is $\exp(-n)$-close in operator norm to the following unitary:

$$O_f : |x, b, 0^w\rangle \mapsto |x, b \oplus f(x), 0^w\rangle,$$

for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$.

(c) (**H**) Suppose L is a language in BQP, and you have a polynomial-size quantum circuit for another language L' that uses queries to the language L (i.e., applications of the unitary O_f). Show that the language L' is also in BQP: there is a polynomial-size quantum circuit for L' that doesn't need queries to L.

Hints

Exercise 1: Use binary search, running the algorithm with different choices of k to "zoom in" on the largest prime factor.

Exercise 2.a: Use the Chernoff bound, e.g., as in the last item of [dW19, Appendix B.2] to make the error probability exponentially small.

Exercise 2.c: Use the error analysis of homework Nr. 4 [dW19, Exercise 4.4].

References

[dW19] Ronald de Wolf. Quantum computing: Lecture notes (version 5), 2019. arXiv: `1907.09415v5`