Problem 6. «Boolean hidden shift and quantum computings»

Special Prize from the Program Committee!

The following long-standing problem is known. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a given Boolean function. Determine the hidden nonzero shift $a \in \mathbb{F}_2^n$ for the function, i.e. a vector such that $f_a(x) = f(x \oplus a)$ for all $x \in \mathbb{F}_2^n$. And do it having a limited access to an oracle. Such a problem is called the **Boolean hidden shift problem** (BHSP).

In order to solve this problem on a quantum computer, an oracle that computes the shifted function in the phase is used. This oracle can be implemented using only one query to an oracle that computes the function in a register. The phase oracle is $O_{f_a} : |x\rangle \mapsto (-1)^{f(x \oplus a)}|x\rangle$. The **quantum query complexity** is the minimum number of oracle O_{f_a} accesses needed in the worst case to solve the problem.

There are two classes of Boolean functions for which the quantum query complexity is minimal and maximal respectively:

- for any bent function, i. e. a function in even number of variables that is on the maximal possible Hamming distance from the set of all affine functions, one quantum query suffices to solve the problem exactly [1];
- for any delta function, i. e. $f(x) = \delta_{x,x_0}$ for some $x_0 \in \mathbb{F}_2^n$, the quantum query complexity is $\Theta\left(2^{n/2}\right)$, which is equivalent to Grover's search [2,3].

For any Boolean function f in n variables

$$Q\left(BHSP_f\right) = O\left(2^{n/2}\right),$$

where $Q\left(BHSP_f\right)$ is the bounded error quantum query complexity of the BHSP for f. Moreover, it holds [4]

$$Q\left(BHSP_f\right) \leqslant \frac{\pi}{4}\frac{2^{n/2}}{\sqrt{\mathrm{wt}(f)}} + O\left(\sqrt{\mathrm{wt}(f)}\right),$$

when $1 \leqslant \mathrm{wt}(f) \leqslant 2^{n-1}$, where $\mathrm{wt}(f)$ is the Hamming weight of f.

Turn to the next page.

The problem to solve is the following: identify natural classes of Boolean functions in even number of variables lying between the two extreme cases of bent and delta functions and characterize the quantum query complexity of the BHSP for these functions [4].

[1] M. Rotteler. Quantum algorithms for highly non-linear Boolean functions // Proceedings of the 21st ACM-SIAM Symposium on Discrete Algorithms (SODA 2010), pp. 448–457. SIAM, 2010.

[2] L. K. Grover. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996), pp. 212–219. ACM, 1996.

[3] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing // SIAM Journal on Computing, V. 26, I. 5, pp. 1510–1523, 1997.

[4] A. M. Childs, R. Kothari, M. Ozols, M. Roetteler. Easy and Hard Functions for the Boolean Hidden Shift Problem // Proceedings of TQC 2013, LIPIcs, V. 22, pp. 50–79, 2013.