

## Quantum Computing — Assignment 9

Due: Wednesday, 08.07., 14:15

### Exercise 1

20 Points

The hidden subgroup problem is the following problem:

Let  $(G, +)$  be a finitely generated group,  $X$  any finite set, and  $f : G \rightarrow X$  a function that satisfies the following promise:

There is a subgroup  $H \leq G$  such that

$$f(g) = f(g') \text{ iff } g + H = g' + H.$$

Given a QGA for  $U : |g\rangle|x\rangle \mapsto |g\rangle|x \oplus f(g)\rangle$  (for  $g \in G, x \in X$  and a suitable operation  $\oplus$  on  $X$ ), find a generating set for  $H$ .

We will see in the lecture that there is an efficient quantum algorithm for the hidden subgroup problem for certain abelian groups. Also, many problems for which we already know efficient quantum algorithms are actually instances of the hidden subgroup problem.

Therefore, write the following problems as instances of the hidden subgroup problem (not necessarily over abelian groups).

- (a) Deutsch's problem,
- (b) Simon's problem (which is given in Exercise 3 of Assignment 5),
- (c) period finding,
- (d) discrete logarithm,
- (e) the graph isomorphism problem (given graphs  $G_1, G_2$ , is  $G_1 \cong G_2$ ?).  
*Hint:* First rewrite the graph isomorphism problem in terms of automorphisms of one graph.