# Hidden Symmetry Subgroup Problems

Thomas Decker, Gábor Ivanyos, Miklos Santha, and Pawel Wocjan

arXiv:1107.2189v1 [quant-ph]

November 6, 2011

The main goal of quantum computing is to identify suitable classes of problems for which quantum algorithms can be found that provide a significant speed-up over their classical counterparts. The vast majority of such examples that has been found consists of group-theoretical problems that can be formulated within the framework of the hidden subgroup problem (HSP). While no classical algorithm is known to solve this problem with polynomial query complexity, the problem is computationally solvable in quantum polynomial time for every abelian group [17, 2, 12].

Several attempts were made to extend the quantum solution of the abelian HSP to other problems. Most of the research focused on the HSP in non-abelian groups since these include several algorithmically important problems. While some progress has been made in this direction [1, 6, 8, 9, 11, 13, 14], it is already known that the methods for solving the abelian case fail for several interesting non-abelian groups [16, 10].

Another idea for generalizing the problem was proposed by Childs, Schulman and Vazirani [3] who considered algebraic sets hidden by black-box functions. One of these problems is the hidden polynomial problem (HPP) where the hidden object is a polynomial. Childs et al. showed that the quantum query complexity of this problem is polynomial in the logarithm of the field size for a constant degree and a constant number of variables. The question of the time complexity was left open and to the best of our knowledge, no efficient quantum algorithm has been proposed for the general HPP yet, not even for the simplest problem of hidden quadratic polynomials in one variable (HQPP).

In Ref. [5], Decker, Draisma and Wocjan defined a related problem that we refer to as the hidden polynomial graph problem (HPGP) to distinguish it from the HPP. Here, similarly to the HPP, the hidden object is a polynomial, but the oracle is more powerful because it can also be queried on the graphs that are defined by the polynomial functions. They obtained a polynomial time quantum algorithm that correctly identifies the hidden polynomial when the degree and the number of variables are considered to be constant and the characteristic of the underlying field is not in a finite set of exceptional characteristics.

We advocate a third possible approach to find hidden structures. We consider a group $G$ with an action $\circ : G \times M \to M$ on a finite set $M$, and we suppose that we have a black-box function whose level sets define a partition of $M$. The object we would like to recover is the group of symmetries of this partition inside $G$, i.e., in the set $\mathcal{H}$ of all possible subgroups we look for the group $H \in \mathcal{H}$ whose orbits under the action coincide with the classes of the partition. We call this problem the hidden symmetry subgroup problem (HSSP).

**Definition.** HSSP$(G, M, \circ, \mathcal{H})$.
*Oracle input:* A function $f$ from $M$ to some finite set $S$ such that for some subgroup $H \in \mathcal{H}$, we have $f(x) = f(y)$ iff the orbits $H \circ x$ and $H \circ y$ are the same.
*Output:* $H$.

It is easy to see that the HSP is a special case of the HSSP when the group acts on itself and the action corresponds to the group operation. But, for some actions, the HSSP is provably harder than any HSP. We show that Grover's search can be cast as an HSSP, establishing that certain cases of the HSSP have exponential quantum query complexity. This is in contrast to the HSP

that has polynomial quantum query complexity for all groups [7]. It is also worth to note that the hidden shifted multiplicative character problem of van Dam, Hallgren and Ip [4] is a version of the HSSP with an additional promise on the input, which makes it easier to solve.

The potential of the HSSP lies mainly in the possibility of extending the HSP techniques to more general group actions that still admit efficient quantum procedures. We demonstrate the power of this new approach by designing and improving quantum algorithms for several algebraic problems. To achieve this, we reduce both the HQPP and the univariate HPGP to appropriate HSSPs for which we can give efficient quantum solutions in some interesting cases. Besides the construction of efficient algorithms, the formulation of problems as HSSP can also shed new light on their structure. For example, the apparent difficulty of the HQPP over prime fields might be explained by the equivalence of this problem to the HSP in the dihedral group, a connection discovered via their relations to the HSSP.

To establish our algorithmic results, we first concentrate on the question of whether the HSSP can be reduced in some cases to the related HSP that we obtain by forgetting about the action. We design a reduction scheme, which involves the generalization of bases known from the theory of permutation groups. We are able to show that when the action has an efficiently computable generalized base then the HSSP is indeed efficiently reducible to the related HSP. Then we describe a probabilistic construction of such bases for a large class of Frobenius groups. Therefore, the above reduction applies to these groups. These groups include among others a large variety of affine groups $\mathrm{Aff}_q(H) := \mathbb{F}_q \rtimes H$ with $H \leq \mathbb{F}_q^\times$ and the HSSP is efficiently solvable for these groups by a quantum algorithm when $\mathcal{H}$ consists of the conjugates of $H$.

**Theorem.** *Let $q$ be a prime power and let $H \leq \mathbb{F}_q^*$ such that $1 < |H| < q-1$. Then the following results hold for the HSSP over $\mathrm{Aff}_q(H)$.*

*(a) It can be solved in quantum polynomial time when $q$ is prime and $|H| = \Omega(q/\mathrm{polylog}(q))$.*

*(b) It can be solved in quantum polynomial time when $q$ is the power of a fixed prime.*

The authors are indebted to an anonymous referee for pointing out that result (a) of the above theorem is actually not new. It was essentially proven in [15] in the context of hidden shift problems, using a very similar reduction technique.

We then establish several surprising connections between hidden polynomial problems and the HSSP. In fact, the HQPP turns out to be equivalent in a very strong sense to the HSSP over a related affine group. Combined with the reduction to the related HSP, we are able to give the first ever quantum polynomial time solution for the HQPP over fields of constant characteristic. We then give a quantum reduction of the multivariate quadratic HPP to the HQPP, which implies that over fields of constant characteristic this multivariate problem is also solvable in quantum polynomial time.

**Theorem.** *The $n$-variate hidden quadratic polynomial problem can be solved by a polynomial time quantum algorithm over fields of constant characteristic.*

Finally, for dealing with the HPGP, we define a class of semidirect product groups which we call function graph groups. We show that the HPGP for univariate polynomials of degree at most $d$ coincides with the HSSP over a corresponding function graph group. These groups turn out to have a base of size $d$, and therefore our general reduction to the related HSP applies. Based on this reduction, we improve the results of Ref. [5] by showing that there is a quantum polynomial time algorithm for the HPGP over every field when the degree of the polynomials is constant.

**Theorem.** *If $d$ is constant then the $n$-variate hidden polynomial graph problem of degree $d$ can be solved efficiently by a polynomial time quantum algorithm.*

## References


[1] D. Bacon, A. Childs and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In: *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 469–478, 2005.

[2] D. Boneh and R. Lipton. Quantum cryptanalysis of hidden linear functions. In: *Proceedings of Crypto'95*, LNCS vol. 963, pp. 427–437, 1995.

[3] A. Childs, L. Schulman, U. Vazirani. Quantum Algorithms for Hidden Nonlinear Structures. In: *Proceedings of the 48th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 395–404, 2007.

[4] W. van Dam, S. Hallgren and L. Ip, Quantum algorithms for some hidden shift problems. In: *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms (SODA'03)*, pp. 489–498 (2003)

[5] T. Decker, J. Draisma, and P. Wocjan. Quantum algorithm for identifying hidden polynomial function graphs. Quantum Information and Computation, Vol. 9, pp. 0215 – 0230, 2009.

[6] A. Denney, C. Moore and A. Russell. Finding conjugate stabilizer subgroups in $PSL(2;q)$ and related groups. Quantum Information and Computation, 10, pp. 282–291, 2010.

[7] M. Ettinger, P. Høyer and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. Information Processing Letters, 91(1) pp. 43–4, 2004.

[8] K. Friedl, G. Ivanyos, F. Magniez, M. Santha and P. Sen. Hidden translation and orbit coset in quantum computing. In: *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC)*, pp. 1–9, 2003.

[9] Grigni, M., Schulman, L., Vazirani, M., Vazirani, U. Quantum mechanical algorithms for the nonabelian Hidden Subgroup Problem. In: *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC)*, pp. 68–74, 2001.

[10] S. Hallgren, C. Moore, M. Rötteler, A. Russell, P. Sen. Limitations of quantum coset states for graph isomorphism. In: *Proceedings of the 38th ACM Symposium on Theory of Computing (STOC)*, pp. 604–617, 2006.

[11] S. Hallgren, A. Russell, A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. SIAM Journal on Computing, 32(4), pp. 916–934, 2003.

[12] A. Y. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. arXiv:quant-ph/9511026v1

[13] G. Kuperberg. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. SIAM Journal on Computing, Vol. 35, pp. 170–188, 2005.

[14] C. Moore, D. Rockmore, A. Russell and L. J. Schulman. The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups. In: *Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms,* pp. 1113–1122, 2004.

[15] C. Moore, D. Rockmore, A. Russell and L. J. Schulman. The power of strong Fourier sampling: quantum algorithms for affine groups and hidden shifts. SIAM Journal on Computing, 37(3), pp. 938-958, 2007.

[16] C. Moore, A. Russell and L. J. Schulman. The symmetric group defies strong Fourier sampling. In: *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 479–488, 2005.

[17] P. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. SIAM Journal on Computing, 26(5):1484–1509, 1997.