OPTIMAL QUANTUM ALGORITHM FOR POLYNOMIAL INTERPOLATION

ANDREW M. CHILDS[*,†], WIM VAN DAM[‡], SHIH-HAN HUNG[†], AND IGOR E. SHPARLINSKI[§]

Let $f(X) = c_d X^d + \cdots + c_1 X + c_0 \in \mathbb{F}_q[X]$ be an unknown polynomial of degree d, specified by its coefficient vector $c \in \mathbb{F}_q^{d+1}$. Suppose q and d are known and we are given a black box that evaluates f on any desired $x \in \mathbb{F}_q$. We are interested in determining how many queries are required to determine the vector $c \in \mathbb{F}_q^{d+1}$.

The classical query complexity of this problem is well known: $d+1$ queries to f are clearly sufficient and are also necessary to determine the polynomial, even with bounded error. Shamir used this fact to construct a cryptographic protocol that divides a secret into $d+1$ parts such that knowledge of all the parts can be used to infer the secret, but any d parts give no information about the secret [17]. The security protocol relies on the fact that if f is chosen uniformly at random, and if we only know d function values $f(x_1), \ldots, f(x_d)$, then we cannot guess the value $f(x_{d+1})$ for a point $x_{d+1} \notin \{x_1, \ldots, x_d\}$ with probability greater than $1/q$ (that is, there is no advantage over random guessing).

We [6] describe an optimal quantum algorithm that uses k quantum queries to infer the coefficients of an unknown polynomial $f \in \mathbb{F}_q[X]$ of known degree d. Using this algorithm, we show that the lower bounds in previous works [11,14] are tight: $k = d/2+1/2$ queries suffice to solve the problem with constant success probability. While the success probability at this value of k has a q-independent lower bound, it decreases rapidly with k, scaling like $1/k!$. This raises the question of how the success probability increases as we make more queries. We show that there is a sharp transition as k is increased: with $k = d/2 + 1$ queries, the algorithm succeeds with a probability that approaches 1 for large q. We also show that our algorithm is precisely optimal: it achieves the highest possible success probability of any k-query algorithm.

Finally, we consider the gate complexity of polynomial interpolation. We call an algorithm *gate-efficient* if it can be implemented with a number of 2-qubit gates that is only larger than its query complexity by a factor $\mathrm{poly}(\log q)$. We construct a gate-efficient variant of the optimal algorithm that achieves almost the same success probability.

Our algorithm can be applied to improve results of Boneh and Zhandry giving quantum attacks on certain cryptographic protocols [3]. For a version of the Shamir secret sharing scheme where the shares can be quantum superpositions, their d-query interpolation algorithm shows that a subset of only d parties can recover the secret. Our algorithm considerably strengthens this, showing that a subset of $d/2+1/2$ parties can recover the secret with constant probability, and $d/2+1$ can recover it with probability $1 - O(1/q)$. Boneh and Zhandry also formulate a model of quantum message-authentication codes (MACs), where the goal is to tag messages in a way that authenticates the sender. Informally, a MAC is called d-time if, given the ability to create d valid message-tag pairs, an attacker cannot forge another valid message-tag pair. Boneh and Zhandry show that there are $(d+1)$-wise independent functions that are not d-time quantum MACs. Our result improves to show that there are $(d+1)$-wise independent functions that are not $(d/2+1/2)$-time quantum MACs.

[*]Department of Computer Science and Institute for Advanced Computer Studies, University of Maryland
[†]Joint Center for Quantum Information and Computer Science, University of Maryland
[‡]Departments of Computer Science and Physics, University of California, Santa Barbara
[§]Department of Pure Mathematics, University of New South Wales

References

[1] Dave Bacon, Andrew M. Childs, and Wim van Dam, *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, Proceedings of the 46th IEEE Symposium on Foundations of Computer Science, 2005, pp. 469–478, available at arXiv:quant-ph/0504083.

[2] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf, *Quantum lower bounds by polynomials*, Journal of the ACM, Vol. 48, no. 4, pp. 778–797 (2001), available at quant-ph/9802049.

[3] Dan Boneh and Mark Zhandry, *Quantum-secure message authentication codes*, Proceedings of Eurocrypt 2013, 2013, pp. 592–608.

[4] François Charles and Bjorn Poonen, *Bertini irreducibility theorems over finite fields*, Journal of the American Mathematical Society, Vol. 29, pp. 81–94 (2016).

[5] Andrew M. Childs and Wim van Dam, *Quantum algorithm for a generalized hidden shift problem*, Proceedings of the 18th ACM-SIAM Symposium on Discrete Algorithms, 2007, pp. 1225–1234, available at arXiv:quant-ph/0507190.

[6] Andrew M. Childs, Wim van Dam, Shih-Han Hung, and Igor E. Shparlinski, *Optimal quantum algorithm for polynomial interpolation* (2015), available at arXiv:1509.09271.

[7] Wim van Dam, *Quantum oracle interrogation: Getting all information for almost half the price*, Proceedings of the 39th IEEE Symposium on Foundations of Computer Science, 1998, pp. 362–367, available at arXiv:quant-ph/9805006.

[8] Thomas Decker, Jan Draisma, and Pawel Wocjan, *Efficient quantum algorithm for identifying hidden polynomials*, Quantum Information and Computation, Vol. 9, no. 3, pp. 215–230 (2009), available at arXiv:0706.1219.

[9] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser, *Limit on the speed of quantum computation in determining parity*, Physical Review Letters, Vol. 81, no. 24, pp. 5442–5444 (1998), available at quant-ph/9802045.

[10] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2013.

[11] Daniel M. Kane and Samuel A. Kutin, *Quantum interpolation of polynomials*, Quantum Information and Computation, Vol. 11, no. 1, pp. 95–103 (2011), available at arXiv:0909.5683.

[12] Arnold Knopfmacher and John Knopfmacher, *Counting polynomials with a given number of zeros in a finite field*, Linear and Multilinear Algebra, Vol. 26, no. 4, pp. 287–292 (1990).

[13] Serge Lang and André Weil, *Number of points of varieties in finite fields*, American Journal of Mathematics, Vol. 76, pp. 819–827 (1954).

[14] David A. Meyer and James Pommersheim, *On the uselessness of quantum queries*, Theoretical Computer Science, Vol. 412, no. 51, pp. 7068–7074 (2011), available at arXiv:1004.1434.

[15] Ashley Montanaro, *The quantum query complexity of learning multilinear polynomials*, Information Processing Letters, Vol. 112, no. 11, pp. 438–442 (2012), available at arXiv:1105.3310.

[16] Gerald M. Pitstick, João R. Cruz, and Robert J. Mulholland, *A novel interpretation of Prony's method*, Proceedings of the IEEE, Vol. 76, no. 8, pp. 1052–1053 (1988).

[17] Adi Shamir, *How to share a secret*, Communications of the ACM, Vol. 22, no. 11, pp. 612–613 (1979).