On the Complexity of Decoded Quantum Interferometry

Kunal Marwaha[1], Bill Fefferman[1], Alexandru Gheorghiu[2], and Vojtech Havlicek[2]

[1]University of Chicago
[2]IBM Quantum

Extended abstract

1 Background

Exponential quantum speedups are the main reason for interest in quantum computing, but they are also quite *rare*. Examples include Shor's algorithm for factoring and computing the discrete logarithm [Sho94], sampling from random quantum circuits [AA11; BJS11; AC16; BFNV19; MT19], and interactive tests of quantumness [BCMVV21; KCVY22]. The classical hardness of these tasks is based either on established cryptographic assumptions or well-founded complexity-theoretic assumptions, such as the non-collapse of the polynomial hierarchy.

If we hope to find more examples of exponential quantum speedup, where should we look? One promising idea is known as "Regev's reduction" or the "quantum decoding problem": use a decoder of a linear code C to find small codewords in its *dual* code $C^\perp$ [AR03; Reg09; CT24]. Regev used this idea to give evidence that the cryptographic primitive Learning With Errors (LWE) is quantum resistant. Yamakawa and Zhandry used this idea to construct the first random oracle problem with exponential quantum speedup [YZ24]. This has led to several new candidates to demonstrate verifiable quantum advantage (e.g. [CT24; BNZ25; Ghe25; BDG+26]).

Recently, an algorithm built on top of Regev's reduction, Decoded Quantum Interferometry (DQI) [JSW+25] attracted much attention. It solves a combinatorial optimization problem called *Max-LINSAT* in which we are given as input a matrix $B \in \mathbb{F}_p^{m\times n}$ as well as sets $F_1, F_2, \dots F_m \subset \mathbb{F}_p$. The goal is to find a vector $x \in \mathbb{F}_p^n$, satisfying as many constraints of the form $\sum_{ij} B_{ij}x_j \in F_i$ as possible, for $i \leq m$. This linear system is taken to be overdetermined ($m > n$). While it is known that finding a close-to-optimal solution is NP-hard in this regime [Tre14], DQI aims to output solutions satisfying an expected number of constraints that is *greater* than what can be achieved by classical polynomial-time algorithms, but not so many constraints as to solve an NP-hard problem.

There has been much activity in understanding how DQI and its variants can lead to quantum advantage [CT25; BGKL25; SLS+25; AGL25; Par25; KOW25; KSG+25], but it remains open if one can rigorously justify a quantum speedup by DQI. Here we make partial progress towards this end by studying classical *simulability* of the DQI algorithm.

2 Our results

We give evidence that DQI is not classically simulable, and narrow down its possible sources of quantum advantage:

1. *DQI resists classical simulation algorithms that leverage sparsity.* Schwarz and van den Nest [SN13] showed that if Shor's algorithm had a *sparse* output distribution, it can be classically simulated by a variant of the Kushilevitz-Mansour (KM) algorithm [GL89; KM91]. The simulation algorithm works because the Fourier transform of Shor's algorithm has a simple structure. We prove that the Fourier transform of DQI shares this structure, and so any assignment x with $\geq 1/\text{poly}(n)$ probability weight can be found using KM. However, Shor's algorithm resists the simulation algorithm because no output probability is $\geq 1/\text{poly}(n)$. We prove that this is also true for DQI. This suggests that the source of classical hardness in simulating DQI has a structural similarity to that in Shor's algorithm.

2. *DQI is not a source of sampling-based quantum supremacy.* Many quantum circuits cannot be classically simulated in any level of the polynomial hierarchy because of an argument known as *quantum supremacy* [BJS11]. There are many examples: random circuits, circuits that solve BQP-complete problems, and even models with very little power, such as IQP and the one clean qubit model DQC1 [MT19]. In contrast, we show how to sample the output distribution produced by DQI in the third level of the polynomial hierarchy.[1] This means DQI cannot be used to construct a quantum supremacy argument. If DQI is hard to simulate, the reason does **not** come from the hardness of computing conditional output probabilities, as it does in these other models.

3. *DQI implements an existential coding theory bound with no known classical algorithm.* We show that for the finite field $\mathbb{F}_2$, the DQI algorithm and problem appear in fundamental results of classical coding theory. The performance of DQI is controlled by the strength of the associated decoding algorithm. This can be restated as: "the covering radius of a linear code C is controlled by the decoding threshold of its dual code $C^\perp$". An existential proof matching the performance of DQI appeared in the coding theory literature as early as 1990 [Tie90]. This invokes a duality between C and $C^\perp$ that is essentially a Fourier transform. We show how this proof [Tie90] *implements* DQI when viewed as a quantum circuit. A constructive classical proof of this result would dequantize DQI, but all classical proofs of this result and underlying ideas are existential [Mac63; Del73; Tie90; FT05; NS09; Sam23].

4. *DQI prepares a quantum harmonic oscillator state.* A fundamental object in physics is the quantum harmonic oscillator, which describes the behavior of a particle within a quadratic energy potential. We interpret DQI as preparing a state in a quantum harmonic oscillator *embedded* in the space of possible assignments $\mathbb{F}_p^n$. The embedding only allows eigenstates of the oscillator that are below some energy threshold which equals the decoding threshold of the instance. Each position x in the oscillator is a superposition over the exponentially many assignments that satisfy $\frac{m}{2} + x$ clauses. The DQI algorithm could prepare any state in this oscillator, but the optimal state is localized around the largest possible position in the oscillator subject to the energy threshold. This means DQI samples from the *exponentially many* assignments satisfying a good number of clauses. By contrast, we do not know any classical algorithm to sample from the set of assignments satisfying a fixed number of clauses.

3 Techniques

We combine techniques from several disciplines while aiming to make each proof accessible. We view this as a feature, since ideas related to Regev's reduction have been studied across research

[1] A randomized classical machine can efficiently sample from DQI's output distribution with access to NP oracle.

domains.

Our first result uses the Fourier coefficient estimation algorithm of Goldreich-Levin and Kushilevitz-Mansour [GL89; KM91] and its quantum variant due to van den Nest and Schwarz [SN13].

The second result relies on a classic theorem of Stockmeyer [Sto83], which uses an NP oracle to approximately compute exponentially-sized sums of non-negative values. Since we can classically compute the unnormalized probability, we can approximately compute *conditional probabilities* in $\mathsf{BPP}^{\mathsf{NP}}$, and then approximately sample from $\mathcal{D}$ bit-by-bit.

The results in coding theory employ a discrete analog of the Hermite polynomials known as the *Kravchuk polynomials* [Kra29]. These are orthogonal with respect to the *binomial* distribution and Hamming association scheme. One can derive our statements (and the prior work) starting from a first-principles study of these polynomials. For example, the existential coding theory bound hinges on the *MacWilliams identity* [Mac63], which relates the distribution of codewords in a code C and in its dual code $C^{\perp}$. This identity can be interpreted as a discrete Fourier transform associated with the Kravchuk polynomials. One can understand the optimal performance of DQI as arising from extremal properties of these polynomials [IS98; KS21].

The physics argument crucially requires a *spectrum-preserving* discretization of a harmonic oscillator that [AS90; CF24]. Once this is chosen, it is straightforward to embed the oscillator in a quantum computer. When storing a linear code into the oscillator, we prove that the position operator imbues a bosonic structure on the eigenstates. This implies the existence of a state concentrated on the position matching the optimal performance of DQI. Using the Hamming bound, we show the amplitudes of this state are exponentially small, so the support is exponentially large.

4 Outlook

When a new quantum algorithm is proposed, it is important to evaluate whether it can be classically simulated. For example, some proposals for quantum machine learning were dequantized because the algorithm could be directly simulated [Tan19; CGL+20].

In the case of DQI, we argue that it is hard to classically simulate, and the sources of this hardness are structurally more similar to Shor's algorithm than sampling-based quantum supremacy. But it remains open if the *optimization* problem DQI solves is classically hard.

Our findings suggest two ideas that naturally generalize DQI to other algorithms with plausible quantum advantage:

1. We have shown how DQI implements a known existential bound using a Fourier transform. Do such bounds occur elsewhere in coding theory; if so, can they be made into a quantum algorithm? Can one construct DQI-like algorithms that implement more general transforms, such as transforms associated with representations of non-abelian groups [LH25; BNZ25]?

2. We have shown how a quantum computer can contain information in the states of a harmonic oscillator. In DQI, this information is a specific subset of codewords. Can other information, perhaps beyond coding theory, be stored in a harmonic oscillator? Can one use this framework to learn properties of a known hash function that are hard to learn classically?

References

[AA11] Scott Aaronson and Alex Arkhipov. "The computational complexity of linear optics". In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. 2011, pp. 333–342.

[AC16] Scott Aaronson and Lijie Chen. "Complexity-theoretic foundations of quantum supremacy experiments". In: *arXiv preprint arXiv:1612.05903* (2016).

[AR03] Dorit Aharonov and Oded Regev. *A Lattice Problem in Quantum NP*. 2003. arXiv: quant-ph/0307220.

[AGL25] Eric R Anschuetz, David Gamarnik, and Jonathan Z Lu. "Decoded quantum interferometry requires structure". In: (2025). arXiv: 2509.14509.

[AS90] Natig M Atakishiev and Sergei K Suslov. "Difference analogs of the harmonic oscillator". In: *Theoretical and Mathematical Physics* 85.1 (1990), pp. 1055–1062. DOI: 10.1007/BF01017247.

[BNZ25] John Bostanci, Barak Nehoran, and Mark Zhandry. "A General Quantum Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. 2025. DOI: 10.1145/3717823.3718195. arXiv: 2411.00529.

[BFNV19] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. "On the complexity and verification of quantum random circuit sampling". In: *Nature Physics* 15.2 (2019), pp. 159–163.

[BCMVV21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. "A cryptographic test of quantumness and certifiable randomness from a single quantum device". In: *Journal of the ACM (JACM)* 68.5 (2021), pp. 1–47.

[BJS11] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 467.2126 (2011). arXiv: 1005.1407.

[BDG+26] Pierre Briaud, Itai Dinur, Riddhi Ghosal, Aayush Jain, Paul Lou, and Amit Sahai. "Quantum Advantage via Solving Multivariate Polynomials". In: *Proceedings of the 2026 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2026, pp. 1383–1423. DOI: 10.1137/1.9781611978971.52.

[BGKL25] Kaifeng Bu, Weichen Gu, Dax Enshan Koh, and Xiang Li. *Decoded Quantum Interferometry Under Noise*. 2025. arXiv: 2508.10725.

[CT24] André Chailloux and Jean-Pierre Tillich. "The Quantum Decoding Problem". In: *Leibniz Int. Proc. Inf.* 310 (2024), 6:1–6:14. DOI: 10.4230/LIPIcs.TQC.2024.6. arXiv: 2310.20651.

[CT25] André Chailloux and Jean-Pierre Tillich. "Quantum Advantage from Soft Decoders". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. STOC '25. Prague, Czechia, 2025. DOI: 10.1145/3717823.3718319. arXiv: 2411.12553.

[CF24] Quentin Chauleur and Erwan Faou. "Discrete quantum harmonic oscillator and Kravchuk transform". In: *ESAIM: Mathematical Modelling and Numerical Analysis* 58.6 (2024), pp. 2155–2186. DOI: 10.1051/m2an/2024001.

[CGL+20] Nai-Hui Chia, András Gilyén, Tongyang Li, Han-Hsuan Lin, Ewin Tang, and Chunhao Wang. "Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing Quantum machine learning". In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 2020. DOI: 10.1145/3357713.3384314. arXiv: 1910.06151.

[Del73] Philippe Delsarte. "An algebraic approach to the association schemes of coding theory". In: *Philips Res. Rep. Suppl.* 10 (1973), pp. vi+–97.

[FT05] Joel Friedman and Jean-Pierre Tillich. "Generalized Alon–Boppana Theorems and Error-Correcting Codes". In: *SIAM Journal on Discrete Mathematics* 19.3 (2005), pp. 700–718. DOI: 10.1137/S0895480102408353.

[Ghe25] Andru Gheorghiu. *Can We Get Verifiable Quantum Advantage from Forrelation*. Talk at Quantum Industry Day 2025, Simons Institute for the Theory of Computing. IBM Quantum. Oct. 2025. URL: https://www.youtube.com/live/lZmk1IrobSo.

[GL89] Oded Goldreich and Leonid A Levin. "A hard-core predicate for all one-way functions". In: *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. 1989, pp. 25–32. DOI: 10.1145/73007.73010.

[IS98] Mourad EH Ismail and Plamen Simeonov. "Strong asymptotics for Krawtchouk polynomials". In: *Journal of computational and applied mathematics* 100.2 (1998), pp. 121–144. DOI: 10.1016/S0377-0427(98)00183-6.

[JSW+25] Stephen P. Jordan, Noah Shutty, Mary Wootters, Adam Zalcman, Alexander Schmidhuber, Robbie King, Sergei V. Isakov, Tanuj Khattar, and Ryan Babbush. *Optimization by Decoded Quantum Interferometry*. 2025. arXiv: 2408.08292.

[KCVY22] Gregory D Kahanamoku-Meyer, Soonwon Choi, Umesh V Vazirani, and Norman Y Yao. "Classically verifiable quantum advantage from a computational Bell test". In: *Nature Physics* 18.8 (2022), pp. 918–924.

[KSG+25] Tanuj Khattar, Noah Shutty, Craig Gidney, Adam Zalcman, Noureldin Yosri, Dmitri Maslov, Ryan Babbush, and Stephen P Jordan. *Verifiable quantum advantage via optimized DQI circuits*. 2025. arXiv: 2510.10967.

[KS21] Naomi Kirshner and Alex Samorodnitsky. "A moment ratio bound for polynomials and some extremal properties of Krawchouk polynomials and Hamming spheres". In: *IEEE Transactions on Information Theory* 67.6 (2021), pp. 3509–3541. arXiv: 1909.11929.

[KOW25] Robin Kothari, Ryan O'Donnell, and Kewen Wu. *No exponential quantum speedup for SIS$^\infty$ anymore*. 2025. arXiv: 2510.07515.

[Kra29] Mikhail Krawtchouk. "Sur une généralisation des polynômes d'Hermite". In: *Comptes Rendus* 189.620-622 (1929), pp. 5–3.

[KM91] Eyal Kushilevitz and Yishay Mansour. "Learning decision trees using the Fourier spectrum". In: *Proceedings of the twenty-third annual ACM symposium on Theory of computing*. 1991, pp. 455–464. DOI: 10.1145/103418.103466.

[LH25] Martin Larocca and Vojtech Havlicek. "Quantum algorithms for representation-theoretic multiplicities". In: *Physical Review Letters* 135.1 (2025). DOI: 10.1103/k5tx-xtr3. arXiv: 2407.17649.

[Mac63] Jessie MacWilliams. "A theorem on the distribution of weights in a systematic code". In: *Bell System Technical Journal* 42.1 (1963), pp. 79–94. DOI: 10.1002/j.1538-7305.1963.tb04003.x.

[MT19] Tomoyuki Morimae and Suguru Tamaki. "Fine-grained quantum computational supremacy". In: *IEICE Technical Report* 119.191 (2019). arXiv: 1901.01637.

[NS09] Michael Navon and Alex Samorodnitsky. "Linear programming bounds for codes via a covering argument". In: *Discrete & Computational Geometry* 41.2 (2009), pp. 199–207. DOI: 10.1007/s00454-008-9128-0. arXiv: math/0702425.

[Par25] Ojas Parekh. *No quantum advantage in decoded quantum interferometry for maxcut*. 2025. arXiv: 2509.19966.

[Reg09] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Journal of the ACM (JACM)* 56.6 (2009), pp. 1–40. DOI: 10.1145/1568318.1568324. arXiv: 2401.03703.

[Sam23] Alex Samorodnitsky. "One more proof of the first linear programming bound for binary codes and two conjectures". In: *Israel Journal of Mathematics* 256.2 (2023), pp. 639–673. DOI: 10.1007/s11856-023-2514-8. arXiv: 2104.14587.

[SLS+25] Alexander Schmidhuber, Jonathan Z Lu, Noah Shutty, Stephen Jordan, Alexander Poremba, and Yihui Quek. *Hamiltonian decoded quantum interferometry*. 2025. arXiv: 2510.07913.

[SN13] Martin Schwarz and Maarten van den Nest. *Simulating Quantum Circuits with Sparse Output Distributions*. 2013. arXiv: 1310.6749.

[Sho94] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[Sto83] Larry Stockmeyer. "The complexity of approximate counting". In: *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*. STOC '83. New York, NY, USA: Association for Computing Machinery, 1983. DOI: 10.1145/800061.808740.

[Tan19] Ewin Tang. "A quantum-inspired classical algorithm for recommendation systems". In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. Association for Computing Machinery, 2019. DOI: 10.1145/3313276.3316310. arXiv: 1807.04271.

[Tie90] AA Tietavainen. "An upper bound on the covering radius as a function of the dual distance". In: *IEEE transactions on information theory* 36.6 (1990). DOI: 10.1109/18.59949.

[Tre14] Luca Trevisan. "Inapproximability of combinatorial optimization problems". In: *Paradigms of Combinatorial Optimization: Problems and New Approaches* (2014), pp. 381–434.

[YZ24] Takashi Yamakawa and Mark Zhandry. "Verifiable quantum advantage without structure". In: *Journal of the ACM* 71.3 (2024), pp. 1–50. DOI: 10.1145/3658665. arXiv: 2204.02063.