

Beyond Black Boxes: Gate-Level Oracles for Quantum Advantage

Gabriel Escrig^{1,*}, R. Campos¹, M. A. Martin-Delgado^{1,2}

¹*Departamento de Física Teórica, Universidad Complutense de Madrid.*

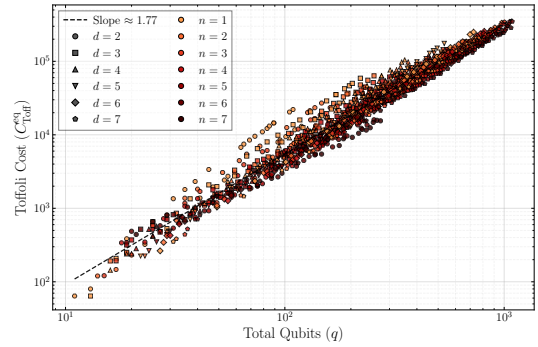
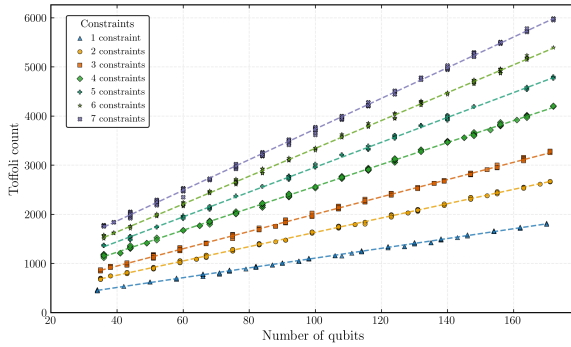
²*CCS-Center for Computational Simulation, Universidad Politécnica de Madrid.*

*e-mail: gescrig@ucm.es

While quantum algorithms promise significant speedups for combinatorial optimization, the true compilation overhead is often hidden behind abstract black-box oracles. This abstraction threatens to negate theoretical quantum advantages when algorithms are compiled down to fault-tolerant hardware. Drawing on our recent publications [1, 2], this work bridges the gap between algorithmic theory and physical implementation by presenting a fully explicit, gate-level synthesis framework for exact integer optimization—specifically targeting Integer Linear Programming (ILP) [1] and bounded non-linear Diophantine equations [2]. Unlike standard hybrid approaches, our architecture relies on purely quantum arithmetic. By coherently encoding integer variables in superposition and evaluating arithmetic constraints on-the-fly via two’s complement logic, we achieve a fully quantum workflow that strictly avoids both quantum-RAM assumptions and classical pre/post-processing.

For Integer Linear Programming, an NP-complete problem central to industrial optimization, we introduce a fully quantum Metropolis–Hastings algorithm that implements a coherent random walk over the discrete feasible region. Each step is a unitary update that prepares candidate moves and reversibly evaluates the objective alongside a dedicated constraint-satisfaction counter to ensure feasibility. At the logical level, the complete algorithmic construction requires only $\mathcal{O}(n \log N)$ qubits to represent n variables over the interval $[-N, N - 1]$, establishing a resource-characterized baseline that thermalizes toward optimal feasible solutions.

To tackle non-linear Diophantine systems, which lie at the core of cryptography and remain classically intractable in the worst case, we deploy a tailored reversible framework based on amplitude amplification. Unlike linear problems, evaluating arbitrary polynomials coherently requires complex arithmetic management. We solve this by introducing an explicit, garbage-free evaluation oracle. By computing polynomial constraints via in-place arithmetic and intelligently routing operations into a single recycled accumulator, this strategy successfully avoids the massive spatial overhead typically associated with uncomputing intermediate polynomial products. Analytically, we formally prove that the spatial complexity is bounded by $q = \mathcal{O}((n + d^2) \log N)$ logical qubits for a maximum degree d , with a non-Clifford Toffoli depth upper-bounded by $\mathcal{O}(q^2)$.



The primary strength of this work lies in its explicit construction validated by numerical circuit simulations, allowing for exact resource counts rather than mere asymptotic bounds. As illustrated in the plots above, both frameworks exhibit highly optimized and predictable overheads. Specifically, the left panel demonstrates that the Toffoli cost for the ILP architecture scales strictly linearly with the logical qubit count. Conversely, the right panel shows that synthesizing non-linear Diophantine polynomials achieves a highly efficient subquadratic Toffoli scaling. By replacing abstract black boxes with rigorous architectural synthesis, we guarantee that the necessary quantum arithmetic acts as a strictly bounded polynomial overhead. This ensures that the theoretical algorithmic advantage—whether thermalizing towards an optimal ILP solution or achieving a definitive quadratic speedup in Diophantine search—is successfully preserved at the fault-tolerant circuit level.

[1] G. Escrig, R. Campos, M. A. Martin-Delgado, *Resource-Scalable Fully Quantum Metropolis-Hastings for Integer Linear Programming*, arXiv:2602.11285 (2026).

[2] G. Escrig, M. A. Martin-Delgado, *From Hilbert’s Tenth Problem to Quantum Speedup: Explicit Oracles for Bounded Diophantine Systems*, arXiv:2605.13980 (2026).