

# Master's Degree in Quantum Technologies

Academic Year: 2024 – 2025

## Enhanced Digitized Adiabatic Quantum Factorization Algorithm Using Null-Space Encoding

Author: Felip Pellicer Benedicto

Directors: Alan Costa dos Santos, Juan José García-Ripoll

# CONTENTS

<b>Abstract</b>	<b>iii</b>
<b>Resumen</b>	<b>iv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Circuit Model of Quantum Computation . . . . .	1
1.2 Adiabatic Quantum Computation . . . . .	2
1.2.1 Adiabatic Quantum Annealers . . . . .	3
1.3 Quantum Approximate Optimization Algorithm . . . . .	4
<b>2 Digitized Factorization</b>	<b>6</b>
2.1 Shor's Factorization Algorithm . . . . .	6
2.2 Adiabatic Factorization Algorithm . . . . .	7
2.3 Digitized Adiabatic Quantum Factorization . . . . .	8
2.3.1 QAOA for Linearized Adiabatic Factorization . . . . .	10
2.4 Algorithms Implementation: Methods . . . . .	11
2.4.1 Initial State . . . . .	11
2.4.2 Parameter Initialization . . . . .	12
2.4.3 Classical optimizer . . . . .	13
<b>3 Results</b>	<b>15</b>
<b>4 Discussion</b>	<b>18</b>
4.1 Future prospects . . . . .	20
<b>A Appendix</b>	<b>21</b>
A.1 Information Table for All Problem Instances . . . . .	21
A.2 Fidelity Plots . . . . .	22
A.3 Cost vs Layers . . . . .	24
A.4 Populations . . . . .	25
A.5 Energy Spectrums . . . . .	27
<b>Bibliography</b>	<b>29</b>

## ABSTRACT

Integer factorization is a computational problem of fundamental importance in cybersecurity and secure communications, as its difficulty forms the basis of modern public-key cryptography. While Shor's algorithm can solve this problem efficiently on a universal quantum computer, near-term devices require alternative approaches. The Adiabatic Factorization Algorithm and its digitized counterparts offer a promising NISQ-era pathway but suffer from high-order many-body interactions that are difficult to implement. In this work, we propose a modified QAOA-based factorization protocol that simplifies the interacting Hamiltonian to include only two-body terms, significantly reducing its experimental complexity. Numerical simulations show that this method achieves comparable or higher fidelities than the standard protocol, while requiring fewer quantum resources and converging more rapidly for problem instances up to eight qubits. We analyze the characteristic fidelity behavior introduced by the Hamiltonian modification. Additionally, we report on simulations with alternative cost-function definitions that frequently yielded improved performance.

## RESUMEN

La factorización de números enteros es un problema computacional de gran relevancia en los campos de la ciberseguridad y las comunicaciones seguras, ya que su dificultad sirve como base para la criptografía de clave pública moderna. Mientras que el algoritmo de Shor resuelve este problema de forma eficiente en un ordenador cuántico universal, los dispositivos a corto plazo requieren de enfoques diferentes. El Algoritmo de Factorización Adiabática y sus versiones digitalizadas ofrecen un prometedor camino a seguir en la era NISQ (por sus siglas en inglés *Noisy Intermediate-Scale Quantum*), pero sufren de interacciones de muchos cuerpos que son difíciles de implementar. En este trabajo, proponemos un protocolo de factorización basado en QAOA modificado que simplifica el Hamiltoniano de interacción para incluir únicamente interacciones de dos cuerpos, reduciendo significativamente su complejidad experimental. Simulaciones numéricas demuestran que este método logra fidelidades comparables o mayores a las obtenidas con el protocolo estándar, a la vez que requiere un menor número de recursos cuánticos y convergiendo más rápidamente para problemas de hasta ocho qubits. Analizamos el comportamiento característico en la evolución de la fidelidad introducido por la modificación en el Hamiltoniano. Además, utilizamos definiciones alternativas en la función de coste que normalmente conllevaron mejoras de rendimiento.

## 1

# INTRODUCTION

Quantum computing has emerged as the most promising paradigm for solving problems that are classically intractable. A central example is the integer factorization problem, which consists of decomposing a semiprime number  $N$  into its prime constituents. While seemingly simple, no known classical algorithm can factorize large integers efficiently, and the best classical methods — such as the general number field sieve — scale superpolynomially with input size [1]. This computational asymmetry forms the foundation of widely used cryptographic protocols, most notably RSA (Rivest-Shamir-Adleman), whose security relies on the practical difficulty of factorizing large semiprimes [2].

One of the most celebrated achievements in quantum computing was the discovery of Shor's algorithm [3], which demonstrated that integer factorization can be solved exponentially faster on a quantum computer than with the best-known classical algorithm, thereby posing a direct threat to RSA-based cryptography. However, the full realization of this algorithm is currently challenging due to quantum hardware limitations in Noisy Intermediate-Scale Quantum (NISQ) devices.

The constraints imposed by the NISQ era have motivated alternative methods to attempt to solve the same problems by using fewer quantum resources. One such approach is the Adiabatic Quantum Computation (AQC) [4], which takes advantage of the robustness of adiabatic evolution to bring the system from a known state to a final state that encodes the solution of a problem. Another approach is the Variational Quantum Algorithm (VQA) [5], which is a hybrid algorithm that uses quantum hardware for state evolution, and classical routines for optimization purposes.

In this work, we propose and analyze a version of the Digitized Adiabatic Quantum Factorization [6] algorithm that incorporates a variation in the cost Hamiltonian. By this, we aim to provide a more resource-efficient and scalable method for integer factorization.

## 1.1 CIRCUIT MODEL OF QUANTUM COMPUTATION

The circuit or gate-based model of quantum computation is the most widely studied framework and the foundation of many quantum algorithms, including Shor's and Grover's algorithms [7]. In this model, computation proceeds through the application of a sequence of unitary gates, which evolve the state of the qubits in a discrete, step-wise fashion.

Mathematically, a quantum circuit implements a unitary transformation  $U$  on the initial quantum state, typically chosen as  $|0\rangle^{\otimes n}$ . This transformation is decomposed into a series of quantum gates from a universal set of gates. Measurement in the computational basis is performed at the end of the circuit to extract classical information from the quantum circuit.

Universality is a crucial property of this model, as it ensures that any unitary transformation — and therefore any quantum algorithm — can be implemented using only a finite set of gates. This makes

the circuit model a general-purpose framework, capable of simulating any other model of quantum computation.

Gate-based quantum computation aligns well with digital control paradigms, and most existing quantum hardware platforms, such as superconducting qubits and trapped ions, are designed to implement this model. However, the depth and width of circuits that can be reliably executed on near-term devices are limited by noise, decoherence, and imperfect gate fidelities.

## 1.2 ADIABATIC QUANTUM COMPUTATION

The adiabatic theorem of quantum mechanics provides the foundation for an alternative model of quantum computation based on continuous-time evolution. Consider a time-dependent Hamiltonian  $H(t)$  with a discrete and non-degenerate spectrum. Thus we can define its instantaneous eigenstates and eigenenergies by

$$\hat{H}(t) |n(t)\rangle = E_n(t) |n(t)\rangle. \quad (1.1)$$

As depicted in Fig. 1.1, the adiabatic theorem states that a quantum system initially prepared in an eigenstate  $|n(0)\rangle$  of  $H(0)$  will remain in the corresponding instantaneous eigenstate  $|n(t)\rangle$  throughout the evolution, provided the spectrum remains gapped and the Hamiltonian changes sufficiently slowly [8]. This condition is generally formulated as

$$T \gg \frac{\mathcal{F}}{\mathcal{G}^2}, \quad \mathcal{F} = \max_{0 \leq s \leq 1} |\langle k | \frac{d}{ds} \hat{H}(s) | n \rangle|, \quad \mathcal{G} = \min_{0 \leq s \leq 1} |g_{nk}(s)|, \quad (1.2)$$

where  $T$  is the total runtime,  $g_{nk}(s) = E_n(s) - E_k(s)$  is the instantaneous energy gap between levels  $n$  and  $k$ , and  $s = t/T$  is the normalized time. In practice, satisfying the adiabatic condition typically requires very long evolution times, which makes implementations vulnerable to decoherence and other noise sources.

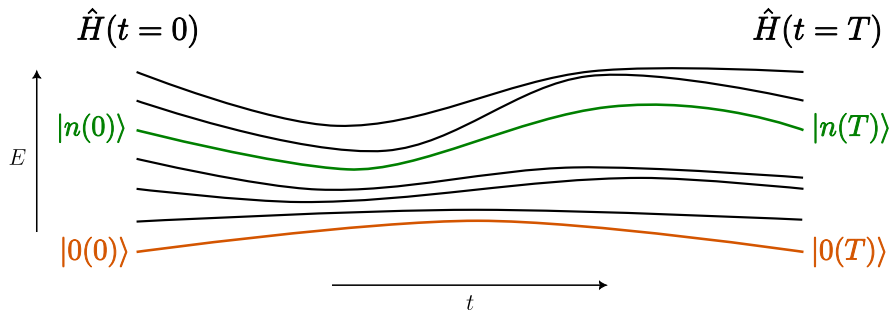


Figure 1.1: Schematic of an adiabatic passage. The orange line represents the Hamiltonian's ground state, while the green a Hamiltonian's eigenstate different from the ground state.

Despite the adiabatic theorem works for any eigenstate, in practice it is customary to focus on ground state adiabatic passages. This is because ground states are typically more robust against decoherence and thermal excitations, whenever they are energetically isolated from higher-energy levels. Moreover, for many computational problems, particularly those related to optimization problems, it is possible to construct a Hamiltonian  $\hat{H}_P$  whose ground state encodes the solution to the instance under consideration.

In the adiabatic quantum computation model, the Hamiltonian is interpolated between an initial

Hamiltonian  $\hat{H}_0$ , with a known and easily preparable ground state, and the problem Hamiltonian  $\hat{H}_P$ , according to a schedule [4]:

$$\hat{H}(t) = [1 - f(t)]\hat{H}_0 + f(t)\hat{H}_P, \quad f(t) \in [0, 1], \quad (1.3)$$

where  $f(t)$  is a smooth, monotonic function such that  $f(0) = 0$  and  $f(T) = 1$ . The problem Hamiltonian  $\hat{H}_P$  is designed so that its ground state corresponds to the solution of the computational task.

Aharonov et al. [9] proved that this model is computationally equivalent to the standard circuit model, meaning that any adiabatic process can, in principle, be reproduced digitally with comparable efficiency. This equivalence opens the door to a variety of gate-based approaches that draw inspiration from adiabatic evolution while remaining fully compatible with the circuit model of quantum computation.

### 1.2.1 ADIABATIC QUANTUM ANNEALERS

An important and widely studied application of adiabatic evolution in quantum devices is Adiabatic Quantum Annealing (AQA), where the goal is to find low-energy configurations of a classical cost function mapped onto a quantum Hamiltonian. AQA is most often applied to Quadratic Unconstrained Binary Optimization (QUBO) problems [10], which can be exactly reformulated as a 2-body interaction Ising Hamiltonian of the form [4]

$$\hat{H}_P = \sum_i h_i \hat{\sigma}_i^z + \sum_{i < j} J_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z, \quad (1.4)$$

where  $h_i$  are local fields,  $J_{ij}$  represent coupling strengths between qubits, and  $\hat{\sigma}_i^z$  are Pauli-Z operators acting on the  $i$ -th qubit, with eigenstates  $|0\rangle$  and  $|1\rangle$  satisfying  $\hat{\sigma}^z |0\rangle = |0\rangle$  and  $\hat{\sigma}^z |1\rangle = -|1\rangle$ . The task is to drive the system from an initial, easily preparable ground state towards the ground state of  $\hat{H}_P$ , which encodes the optimal solution to the problem at hand.

In a typical AQA protocol, the evolution begins with an initial Hamiltonian of a system with a X-oriented field component of the form

$$\hat{H}_0 = \sum_i \hat{\sigma}_i^x. \quad (1.5)$$

where  $\hat{\sigma}^x = |0\rangle\langle 1| + |1\rangle\langle 0|$  and whose ground state is straightforward to prepare. The system is then driven according to the interpolation scheme in Eq. (1.3). The aim is to adiabatically steer the system from the easily preparable ground state  $H_0$  to the ground state of  $H_P$ , which encodes the solution to the problem of interest.

This procedure is feasible for problems that can be expressed in the QUBO form, as they can be mapped to an Ising Hamiltonian with only two-body interactions. This approach has been physically implemented in superconducting-qubit devices, most notably in the commercial quantum annealers developed by D-Wave. However, as we shall see in chapter 2, the problem of interest in this thesis, integer factorization, does not directly fall into the QUBO class, as its Hamiltonian contains three- and four-body interaction terms.

### 1.3 QUANTUM APPROXIMATE OPTIMIZATION ALGORITHM

As mentioned previously, AQC is naturally formulated in platforms where fields and controls evolve continuously in time. Implementing this paradigm directly on gate-based quantum devices, however, can be challenging, since these platforms rely on discrete operations. A way to bridge this gap is provided by the Quantum Approximate Optimization Algorithm (QAOA), a hybrid quantum-classical method introduced by Farhi et al. [11] to tackle combinatorial optimization problems. The algorithm aims to approximate the ground state of a cost Hamiltonian whose minimum encodes the optimal solution. Thanks to its shallow circuit depth and variational structure, which delegates part of the computational workload to a classical optimizer, QAOA is particularly well suited to near-term quantum devices.

At its core, QAOA constructs a parametrized quantum state (ansatz) by sequentially applying two alternating types of unitaries derived from two Hamiltonians:

- The cost Hamiltonian  $H_C$ , which encodes the objective function of the optimization problem. This is typically written in the form of an Ising Hamiltonian.
- The mixing Hamiltonian  $H_M$ , which introduces transitions between computational basis states to enable exploration of the solution space. A common choice, justified by Eq. (1.5), is:

$$\hat{H}_M = \sum_i \hat{\sigma}_i^x, \quad (1.6)$$

where  $\hat{\sigma}_i^x$  is the Pauli-X operator acting on qubit  $i$ .

The algorithm starts with the initial state  $|\psi_0\rangle = |+\rangle^{\otimes n}$ , which is the ground state of  $H_M$  and a uniform superposition over all computational basis states, where  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . The QAOA ansatz with  $p$  layers is constructed as:

$$|\psi_p(\boldsymbol{\gamma}, \boldsymbol{\beta})\rangle = e^{-i\beta_p \hat{H}_M} e^{-i\gamma_p \hat{H}_C} \dots e^{-i\beta_1 \hat{H}_M} e^{-i\gamma_1 \hat{H}_C} |+\rangle^{\otimes n}, \quad (1.7)$$

where  $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_p)$  and  $\boldsymbol{\beta} = (\beta_1, \dots, \beta_p)$  are real variational parameters to be optimized.

The performance of a QAOA instance is assessed by evaluating the expectation value of the cost Hamiltonian in the ansatz state:

$$F_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) = \langle \psi_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) | \hat{H}_C | \psi_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) \rangle. \quad (1.8)$$

This expectation value serves as the cost function for the classical optimizer. The parameters  $(\boldsymbol{\gamma}, \boldsymbol{\beta})$  are iteratively updated to minimize  $F_p$ , with quantum circuits being re-evaluated at each step until convergence.

The Quantum Approximate Optimization Algorithm stands out as one of the most promising approaches for near-term quantum advantage. From a complexity-theoretic perspective, Farhi et al. [13] argue that sampling from the output distribution of even the shallowest version of QAOA ( $p = 1$ ) may already be classically intractable, highlighting its potential as an early demonstration of quantum supremacy.

Beyond this theoretical motivation, QAOA is attractive because of its relatively simple structure



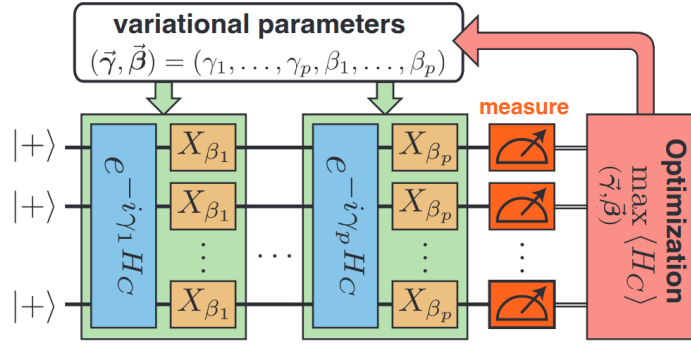


Figure 1.2: Diagram of a  $p$ -layer QAOA circuit. Starting from the initial state  $|+\rangle^{\otimes n}$ , the circuit alternates between applying the unitaries  $e^{-i\gamma_i H_C}$  and  $e^{-i\beta_i H_M}$  for  $i = 1$  to  $p$ . The final state is measured to estimate the expectation value  $\langle H_C \rangle$ , which is passed to a classical optimizer. This process is repeated until convergence.

Source: Adapted from Zhou et al., 2019. [12]

and hardware efficiency. Ho and Hsieh [14] introduce a related variational protocol (VQCS), showing that alternating unitaries generated by simple, local Hamiltonians can efficiently prepare non-trivial quantum states and can be implemented on current platforms such as trapped ions and superconducting qubits.

Additionally, QAOA's modularity and variational flexibility make it adaptable to a wide range of applications, including factorization. In particular, Anschuetz et al. [15] demonstrate a QAOA-inspired approach to integer factorization, showing that hybrid quantum-classical heuristics can extend QAOA's reach to classically hard problems even on today's noisy devices.

The Quantum Approximate Optimization Algorithm has been extensively investigated since its introduction, leading to a broad landscape of theoretical analyses, practical implementations, and performance-enhancement techniques. Numerous variants have been proposed, ranging from modified ansatzes to parameter initialization heuristics and adaptive layer-scaling procedures. This diversity reflects both the flexibility of the QAOA framework and the complexity of identifying implementations that perform well across different problem instances. This richness also underscores the importance of carefully specifying the algorithmic configuration adopted in any particular study, so that performance comparisons can be made in a meaningful way.

## DIGITIZED FACTORIZATION

This chapter explores two quantum approaches to the factorization problem. First, we review Shor's algorithm and its quantum Fourier transform-based structure. Next, we introduce an alternative method for factorization based on adiabatic quantum computation, referred to as *adiabatic factorization* [16], which may serve as a potentially viable approach for factorization on analog quantum computers. We briefly discuss the limitations of this method, primarily arising from the implementation of many-qubit gates, which pose significant challenges in practical experimental settings. To address this issue, we present our solution in the form of a *linearized adiabatic* Hamiltonian for factorization. Finally, we conclude this section with a discussion of the methods employed to implement each algorithm, setting the stage for subsequent comparisons and analysis.

### 2.1 SHOR'S FACTORIZATION ALGORITHM

In computer science, an algorithm is considered to be efficient when the number of steps of the algorithm grows as a polynomial in the input size. For the problem of integer factorization, the input is a semiprime number  $N$ , and the input size is measured as the number of bits required to represent it, i.e.,  $\log N$ . The best known classical algorithm for factorizing scales superpolynomially with input size, making the problem computationally hard for large  $N$ .

$$\mathcal{O}\left(\exp\left(c(\log N)^{1/3}(\log \log N)^{2/3}\right)\right). \quad (2.1)$$

In 1994, Peter Shor introduced a quantum algorithm that factorizes integers in polynomial time, marking a landmark result in quantum computing. Shor's algorithm runs in time

$$\mathcal{O}((\log N)^3), \quad (2.2)$$

dramatically outperforming the best classical method [7]. The algorithm relies on the quantum circuit model, making it a gate-based approach to factorization and one of the strongest motivations for the development of quantum computers.

The core idea of Shor's algorithm is to reduce factorization to the problem of order finding: given a number  $a$  coprime to  $N$ , find the smallest integer  $r$  such that

$$a^r = 1 \pmod{N}. \quad (2.3)$$

Once the order  $r$  is known, under certain conditions, one can recover a nontrivial factor of  $N$  using elementary number-theoretic arguments [7].

The quantum part of the algorithm is used to efficiently find this order  $r$  using period-finding

techniques. This is achieved by preparing a quantum superposition and applying the quantum Fourier transform (QFT) to extract information about the period of the function  $f(x) = a^x \bmod N$ . The classical post-processing step then uses continued fractions to extract  $r$  and attempt to derive the prime factors of  $N$ .

Despite its theoretical significance, implementing Shor's algorithm at scale requires a large number of qubits, long coherence times, and fault-tolerant error correction, which remain beyond the reach of current quantum hardware. As such, while Shor's algorithm remains the most efficient known method for factorizing in the long-term quantum regime, alternative approaches — such as adiabatic and variational algorithms — are being explored for use in the NISQ era.

## 2.2 ADIABATIC FACTORIZATION ALGORITHM

Before introducing the details of the adiabatic factorization algorithm, it is important to clarify its relationship to Shor's algorithm. Although both approaches aim to solve the integer factorization problem, the adiabatic method presented here is not an adiabatic implementation of Shor's algorithm. Instead, it represents a distinct strategy for factorization based on adiabatic evolution, which we refer to in this work as *adiabatic factorization*.

The problem of integer factorization can be formulated as a constrained search over pairs of natural numbers  $p$  and  $q$  such that

$$N = p \times q. \quad (2.4)$$

In the context of adiabatic quantum computation we aim to encode this constraint into the ground state of a problem Hamiltonian, allowing the solution to emerge through adiabatic evolution.

To encode candidate solutions  $p$  and  $q$ , we adopt a binary representation of natural numbers. Any natural number  $X$  can be expressed as:

$$X = \sum_{j=0}^{n_{\text{bits}}-1} 2^j x_j, \quad (2.5)$$

where each  $x_j \in \{0, 1\}$  and the bit string  $\mathbf{x} = x_{n_{\text{bits}}-1} \dots x_0$  represents the binary encoding of  $X$ . In their approach, Peng et al. [16] exploit the fact that the factors  $p$  and  $q$  of an odd composite number can be rewritten as:

$$\begin{cases} p = 2p' + 1 \\ q = 2q' + 1 \end{cases}. \quad (2.6)$$

It can be proved that the  $n_p$  and  $n_q$  are an upper bound on the number of qubits required to represent  $p'$  and  $q'$ , respectively:

$$\begin{cases} n_p = m(\lfloor \sqrt{N} \rfloor_o) - 1 \\ n_q = m\left(\left\lfloor \frac{N}{3} \right\rfloor\right) - 1 \end{cases}, \quad (2.7)$$

where  $\lfloor a \rfloor_o$  ( $\lfloor a \rfloor_o$ ) denotes the largest (odd) integer not larger than  $a$ , while  $m(b)$  denotes the smallest number of bits required for representing  $b$  [16]. Then, the adiabatic factorization algorithm will make

use of  $n = n_p + n_q$  qubits. The full quantum state

$$|\Psi\rangle = |\Psi_{p'}\rangle \otimes |\Psi_{q'}\rangle, \quad (2.8)$$

where  $|\Psi_{p'}\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_{n_p}\rangle$  and  $|\Psi_{q'}\rangle = |\psi_{n_p+1}\rangle \otimes \cdots \otimes |\psi_{n_p+n_q}\rangle$ .

To encode the factorization constraint into the adiabatic quantum framework, we define the objective function as [16]:

$$f(p, q) = (N - p \times q)^2, \quad (2.9)$$

such that its global minimum  $f(p, q) = 0$  corresponds to valid factors. Translating this into a Hamiltonian acting on the computational basis, we obtain the quadratic problem Hamiltonian:

$$\hat{H}_{\text{QP}} = \left[ N\mathbb{1} - \left( \sum_{\ell=1}^{n_p} 2^\ell \hat{x}_\ell + \mathbb{1} \right) \left( \sum_{m=1}^{n_q} 2^m \hat{y}_m + \mathbb{1} \right) \right]^2, \quad (2.10)$$

where  $\hat{x}_\ell = \frac{\mathbb{1} - \hat{\sigma}_\ell^z}{2}$  and  $\hat{y}_m = \frac{\mathbb{1} - \hat{\sigma}_m^z}{2}$  are the number operators acting on the qubits encoding  $p'$  and  $q'$ , respectively. The solution to the factorization problem is encoded in the ground state of  $\hat{H}_{\text{QP}}$ .

The initial state of the system is prepared as:

$$|\psi(0)\rangle = |+\rangle^{\otimes n}, \quad (2.11)$$

corresponding to the ground state of the initial Hamiltonian  $\hat{H}_0$  defined in Eq. (1.5). Following the adiabatic theorem, if the evolution from  $\hat{H}_0$  to  $\hat{H}_{\text{QP}}$  is slow enough, the system will remain in the instantaneous ground state, reaching the ground state of  $\hat{H}_{\text{QP}}$  at the end of the protocol. This final state encodes the solution to the factorization problem.

Despite its conceptual clarity, the Hamiltonian  $\hat{H}_{\text{QP}}$  includes multiqubit interactions, such as three- and four-body terms of the form  $\hat{\sigma}_\ell^z \hat{\sigma}_m^z \hat{\sigma}_k^z$  and  $\hat{\sigma}_\ell^z \hat{\sigma}_m^z \hat{\sigma}_k^z \hat{\sigma}_n^z$ . These many-body interactions are difficult to implement, since they require one to bring all involved qubits together and make them interact in a controlled way, resulting in prone-to-error processes. The need to avoid those terms is of pivotal interest to provide efficient quantum algorithms.

## 2.3 DIGITIZED ADIABATIC QUANTUM FACTORIZATION

Although the adiabatic model is often formulated in terms of continuous time evolution, it can be simulated efficiently using gate-based quantum computation through a process known as digitization.

In the digitized approach, the continuous adiabatic evolution governed by a time-dependent Hamiltonian as of Eq. (1.3) is approximated by a sequence of quantum gates through trotterization, breaking the total evolution into small time slices. Each slice is implemented as a layer in a quantum circuit, simulating the adiabatic trajectory step by step.

This method was successfully demonstrated by Hegade et al. [6], where the authors implemented a digitized adiabatic factorization algorithm on superconducting hardware. They successfully factorized numbers  $N = 21$ ,  $N = 91$ , and  $N = 217$ , and also proved enhancements by introducing an additional layer in the algorithm due to application of counter-adiabatic driving theories.

### QAOA FOR STANDARD ADIABATIC FACTORIZATION

In some sense, QAOA can be viewed as a shortcut to adiabaticity implemented in the circuit model for quantum computation. Rather than performing a slow, continuous evolution, QAOA uses a fixed-depth quantum circuit composed of alternating unitaries derived from the mixing and problem Hamiltonians. The parameters of these unitaries are optimized variationally to prepare a state that approximates the solution.

Díez-Valle et al. [17] demonstrate that QAOA and quantum annealing share fundamental structural features. Their results provide strong evidence that smooth annealing paths can be reconstructed from the optimal parameters of QAOA, reinforcing the view of QAOA as a digitized, variationally optimized form of adiabatic evolution.

In summary, the ingredients to build and execute the QAOA algorithm applied to integer factorization — or what we will call the “standard protocol” — are:

- A Hamiltonian  $\hat{H}_{\text{QP}}$ , Eq. (2.10), that encodes the solution to the factorization problem in its ground state.
- A mixing Hamiltonian  $\hat{H}_{\text{M}}$  that does not commute with  $\hat{H}_{\text{QP}}$ , e.g., Eq. (1.6).
- A quantum circuit that implements the state evolution given by Eq. (1.7).
- A classical optimizer to find the circuit’s optimal parameters.
- A cost function given by  $F_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) = \langle \psi_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) | \hat{H}_{\text{QP}} | \psi_p(\boldsymbol{\gamma}, \boldsymbol{\beta}) \rangle$ .

Due to the form of Eq. (2.10), the problem Hamiltonian can be expressed as:

$$\hat{H}_{\text{QP}} = n\mathbb{1} + \sum_i a_i \hat{\sigma}_i^z + \sum_{ij} b_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z + \sum_{ijk} c_{ijk} \hat{\sigma}_i^z \hat{\sigma}_j^z \hat{\sigma}_k^z + \sum_{ijkl} d_{ijkl} \hat{\sigma}_i^z \hat{\sigma}_j^z \hat{\sigma}_k^z \hat{\sigma}_l^z \quad (2.12)$$

Then, the part of  $e^{-i\gamma\hat{H}_{\text{QP}}}$  corresponding to the term  $a_i \hat{\sigma}_i^z$  is

$$e^{-i\gamma a_i \hat{\sigma}_i^z} = e^{-i\gamma a_i} |0\rangle \langle 0| + e^{i\gamma a_i} |1\rangle \langle 1| = R_Z(2\gamma a_i), \quad (2.13)$$

the part corresponding to  $b_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z$  is

$$\begin{aligned} e^{-i\gamma b_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z} \\ = e^{-i\gamma b_{ij}} |00\rangle \langle 00| + e^{i\gamma b_{ij}} |10\rangle \langle 10| + e^{i\gamma b_{ij}} |01\rangle \langle 01| + e^{-i\gamma b_{ij}} |11\rangle \langle 11| \\ = R_{ZZ}(2\gamma b_{ij}), \end{aligned} \quad (2.14)$$

and so on for the higher-order terms. Similarly, the mixing Hamiltonian  $\hat{H}_{\text{M}}$  gives rise to individual X-rotations at the end of each QAOA layer. With all this, one constructs the QAOA circuit — such as the circuit shown in Fig. 2.1 used for factorization of the number  $N = 35$ .

A related study by Anschuetz et al. [15] applies a similar method, combined with additional preprocessing and simplifications, to factorize numbers as large as 291311. Building on this idea, Karamlou et al. [18] used classical preprocessing heuristics to factorize 1099551473989, 3127, and 6557 using only 3, 4, and 5 qubits, respectively. In contrast, our goal is not to optimize for specific instances, but rather to analyze the general, standard approach to quantum factorization without relying

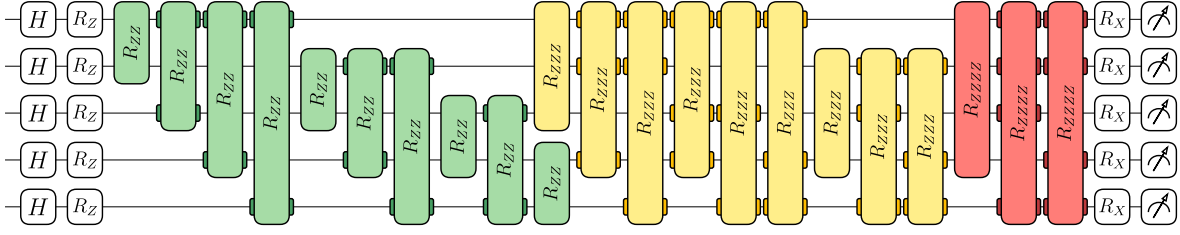


Figure 2.1: One-layer circuit for factorizing the number  $N = 35$  using the standard QAOA protocol. Notice the presence of three- and four-qubit gates, highlighted in yellow and red, respectively. Rotation angles are omitted for simplicity.

on ad-hoc techniques. The motivation comes from establishing a broadly applicable framework, valid for any input  $N$ , while avoiding the need for modifications to the underlying factorization algorithm.

### 2.3.1 QAOA FOR LINEARIZED ADIABATIC FACTORIZATION

As mentioned in the introduction to Section 2.2, the adiabatic factorization algorithm needs to deal with the difficulty of implementing three- and four-body interaction terms. In the digitized version of this problem, like QAOA, this difficulty is bypassed by assuming that all three- and four-qubit gates — see e.g. Fig. 2.1 — can be efficiently implemented in a digital computer. However, for universal computers available so far, these gates are not efficiently implemented and we need to decompose them in multiple two-qubit gates, as shown in Fig. 2.2, what might result in lower fidelities at the end of the quantum circuit in a real scenario.

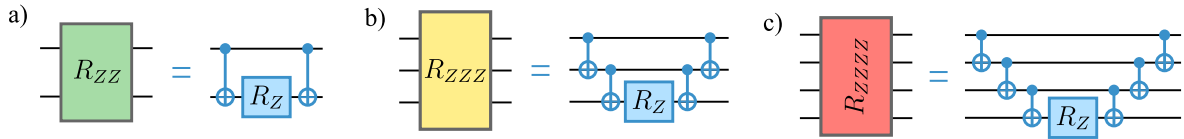


Figure 2.2: Decomposition of (a) two-, (b) three-, and (c) four-qubit Z-rotation gates in CNOTs and single-qubit Z-rotations.

To mitigate this issue, we propose a linearized problem Hamiltonian inspired by the same factorization condition, defined as:

$$\hat{H}_{LP} = N\mathbb{1} - \left( \sum_{\ell=1}^{n_p} 2^\ell \hat{x}_\ell + \mathbb{1} \right) \left( \sum_{m=1}^{n_q} 2^m \hat{y}_m + \mathbb{1} \right). \quad (2.15)$$

Unlike the original Hamiltonian  $\hat{H}_{QP}$ , whose ground state encodes the solution,  $\hat{H}_{LP}$  contains only two-body terms and is therefore easier to implement (see Fig. 2.3), but the factorization solution corresponds to an eigenstate with eigenvalue zero rather than the ground state. In other words, here we consider that the solution of the factorization is encoded in the *null-space* of the Hamiltonian, composed by eigenstates with eigenvalue 0. This approach does not impose limitations on the algorithm, since the adiabatic theorem is not restricted to ground states but applies to any non-degenerate eigenstate. Therefore, the adiabatic theorem supports that it is possible to target this eigenstate through a suitable adiabatic or variational process. Based on this idea, our proposal is to replace the original Hamiltonian in the QAOA layers with  $\hat{H}_{LP}$ , leveraging the possibility of starting from an eigenstate near the middle of the initial Hamiltonian's spectrum and evolving under  $\hat{H}_{LP}$  to preserve this eigenstate structure, ultimately reaching the correct factorization solution, which also lies near the center of the spectrum.

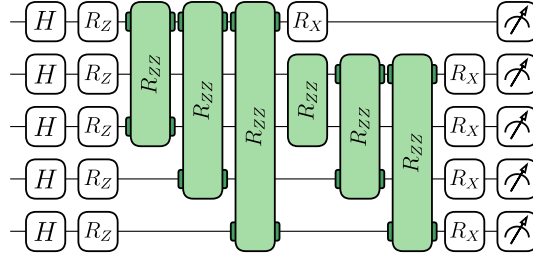


Figure 2.3: One-layer circuit for factorizing the number  $N = 35$  using our protocol, evolving the state with the linear Hamiltonian  $H_{LP}$ . Notice the simplification with respect to Fig. 2.1 due to the absence of three- and four-qubit gates.

## 2.4 ALGORITHMS IMPLEMENTATION: METHODS

In this work, we use the basic formulation of QAOA as a reference framework. To enable a fair comparison between the standard factorization protocol and our alternative variant, we configure the algorithm — including choices for parameter initialization and classical optimization — so that the standard protocol performs as effectively as possible. This approach ensures that any observed differences in performance arise from the protocol itself rather than from specific details of the QAOA setup.

For the numerical simulations, several software frameworks are available, including PennyLane and Qiskit. However, in this study we opted for a direct state-vector simulation implemented in NumPy, where circuit layers are applied through explicit matrix multiplications. This strategy avoids the overhead associated with gate-by-gate simulation and provides a more transparent view of the algorithmic dynamics, while remaining computationally efficient at the scale considered here.

To facilitate reproducibility, the complete implementation together with the numerical procedures and data analysis scripts has been made publicly available in a GitHub repository<sup>1</sup>.

### 2.4.1 INITIAL STATE

In line with the adiabatic theorem, which states that a quantum system prepared in an eigenstate of a slowly varying Hamiltonian will remain in its instantaneous eigenstate, we aim to initialize the system in an eigenstate of the mixing Hamiltonian  $\hat{H}_M$ . Ideally, this initial state should occupy a similar region of the spectrum as the target solution under the problem Hamiltonian  $\hat{H}_P$ , so that the variational evolution requires minimal spectral “rearrangement.” The specific choice of initial state depends on the protocol used:

- **standard protocol** ( $\hat{H}_P = \hat{H}_{QP}$ ): The solution corresponds to the ground state of the problem Hamiltonian. To reflect this structure, we initialize the system in the ground state of the mixing Hamiltonian,

$$|\psi(0)\rangle = |+\rangle^{\otimes n},$$

which is both easy to prepare and spectrally aligned with low-energy states of  $\hat{H}_P$ .

- **linear protocols** ( $\hat{H}_P = \hat{H}_{LP}$ ): Here, the correct solution lies near the center of the spectrum rather than at its bottom. Then, we choose an eigenstate of  $\hat{H}_M$  that is approximately centered in its spectrum,

$$|\psi(0)\rangle = |+-+ - + \dots\rangle.$$

<sup>1</sup><https://github.com/fpllcr/master-thesis>

For problems with an odd number of qubits, this configuration cannot be perfectly centered, but QAOA's non-adiabatic nature tolerates this slight asymmetry without degrading performance.

## 2

### 2.4.2 PARAMETER INITIALIZATION

In multi-layer QAOA, increasing the number of layers also increases the number of parameters to be optimized. Finding global optima is considerably simpler for  $p = 1$  (i.e., two parameters) than for circuits with many layers. Moreover, when a new layer is added, the previously optimized solution remains valid within the enlarged parameter space: the parameters corresponding to the first  $p$  layers can be initialized with their previously optimized values, while the newly introduced parameters can be set to zero. Consequently, adding an additional layer ( $p \rightarrow p + 1$ ) can only maintain or improve performance relative to the previous iteration.

This observation motivates a progressive training strategy, often referred to as an *incremental* approach, which proceeds as follows [12]:

1. Analyze the cost function landscape for  $p = 1$  to select initial parameters  $\gamma_1$  and  $\beta_1$  close to the optimal region (Fig. 2.4).
2. Optimize QAOA with  $p = 1$  to obtain the parameters  $\tilde{\gamma}_1$  and  $\tilde{\beta}_1$ .
3. Optimize QAOA with  $p = 2$ , initializing  $\gamma_1 = \tilde{\gamma}_1$  and  $\beta_1 = \tilde{\beta}_1$ , and selecting suitable initial values for  $\gamma_2$  and  $\beta_2$  using an appropriate heuristic. This yields the updated parameters  $\tilde{\gamma}_1, \tilde{\gamma}_2, \tilde{\beta}_1, \tilde{\beta}_2$ .
4. Repeat this procedure iteratively up to the desired depth  $p$ , each time initializing with the optimized parameters from the previous iteration and applying a strategy to set the new layer's parameters.

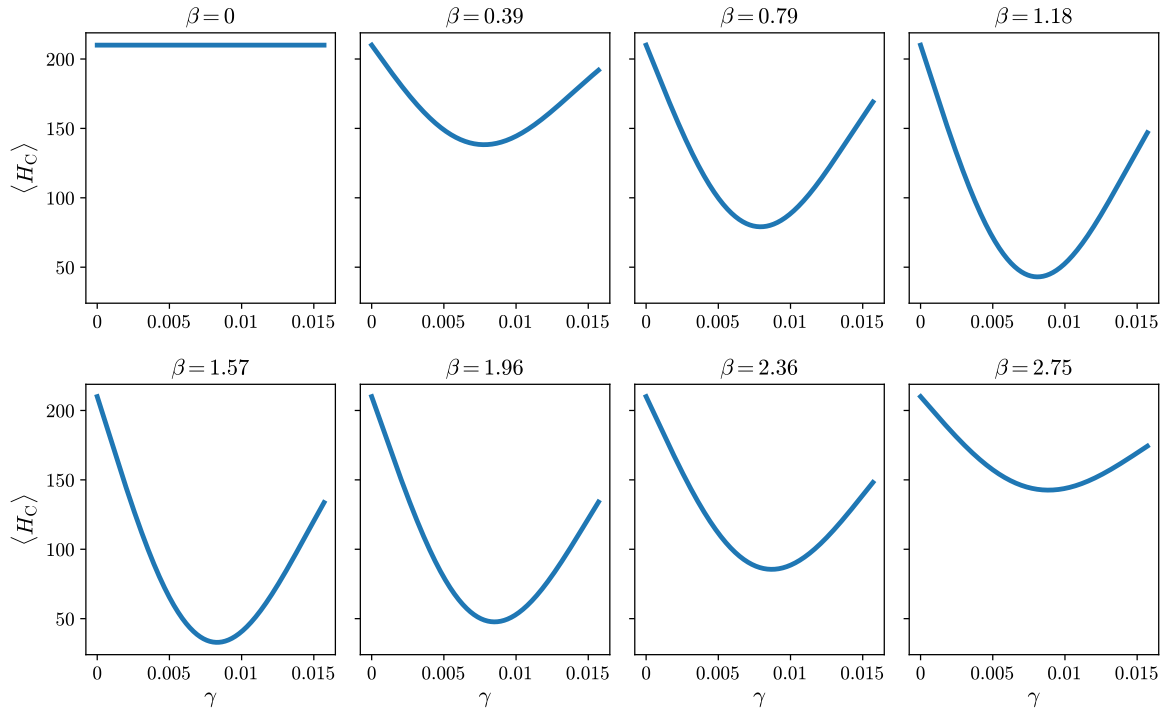


Figure 2.4: Cost function profile for the quadratic Hamiltonian when  $N = 21$ . After this analysis,  $\gamma_0 = 0.0075$  and  $\beta_0 = 1.57$  are used as initial parameters for  $p = 1$ . Maximum  $\gamma$  is determined as the value that causes angle folding for the maximum energy eigenvalue, i.e.  $e^{-i\gamma_{\max} E_{\max}} = e^{-2\pi i}$ .



As aforementioned, adding a new QAOA layer requires a suitable heuristic to initialize the additional variational parameters. Beyond random initialization, two specific strategies have been considered in this work:

- **Parameter interpolation.** This method, adopted by Zhou et al. [12], linearly interpolates the trajectory traced by the optimized parameters at depth  $p$  to generate an initial guess for depth  $p + 1$ . Such interpolation is particularly effective for problems like MaxCut and QUBO, where the optimal parameters often evolve monotonically in an adiabatic-like fashion.
- **Alternative heuristic.** This approach, which achieved superior performance for both the standard and linearized protocols in our experiments, initializes the new parameters as

$$\begin{cases} \gamma_{p+1} \leftarrow \tilde{\gamma}_p, \\ \beta_{p+1} \leftarrow 0. \end{cases} \quad (2.16)$$

Two factors motivated the adoption of this alternative strategy. First, the interpolation heuristic performs poorly for the linearized protocol, frequently leading to trapping in local minima. Second, integer factorization differs fundamentally from MaxCut and QUBO problems: there is no evidence that optimal parameters follow adiabatic-like trajectories, and our results confirm that they do not (see Fig. 2.5 and Fig. 2.6). The fact that the alternative heuristic also outperforms interpolation for the standard protocol ensures a fair basis for comparison, as both protocols are evaluated under the most favorable optimization setup for the reference (standard) implementation.

### 2.4.3 CLASSICAL OPTIMIZER

A wide variety of classical optimizers have been employed within QAOA, as reviewed in the literature [19]. In this work, we focused on optimizers available in the SciPy library and tested representative classes: bounded vs. unbounded and gradient-free vs. gradient-based.

Gradient-free methods such as Nelder-Mead showed promising performance for small problems but scale poorly with the number of parameters, and were therefore discarded. Cobyla exhibited poor convergence and frequent trapping in local minima, even for few-qubit cases, making it unsuitable for this study. Among gradient-based methods, the best performance was obtained with BFGS and its bounded variant L-BFGS-B:

- **L-BFGS-B.** This bounded optimizer is well-suited for QUBO and MaxCut problems, where parameter symmetries justify restricting  $\gamma$  and  $\beta$  to specific intervals. Under such constraints, L-BFGS-B often produces adiabatic-like parameter trajectories, with  $\gamma$  starting near zero and increasing smoothly, while  $\beta$  decreases monotonically toward zero.
- **BFGS.** As an unbounded optimizer, BFGS allows variational parameters to take any real value. In all tested cases up to 8 qubits, BFGS consistently outperformed L-BFGS-B, likely because its unbounded nature helps it escape local minima that trap the bounded optimizer (see Fig. 2.5).

Based on these findings, BFGS is selected as the classical optimizer for all experiments. This choice complements the other elements of our QAOA setup, ensuring a consistent and high-performance framework for comparing the standard protocol and the proposed linearized protocol.

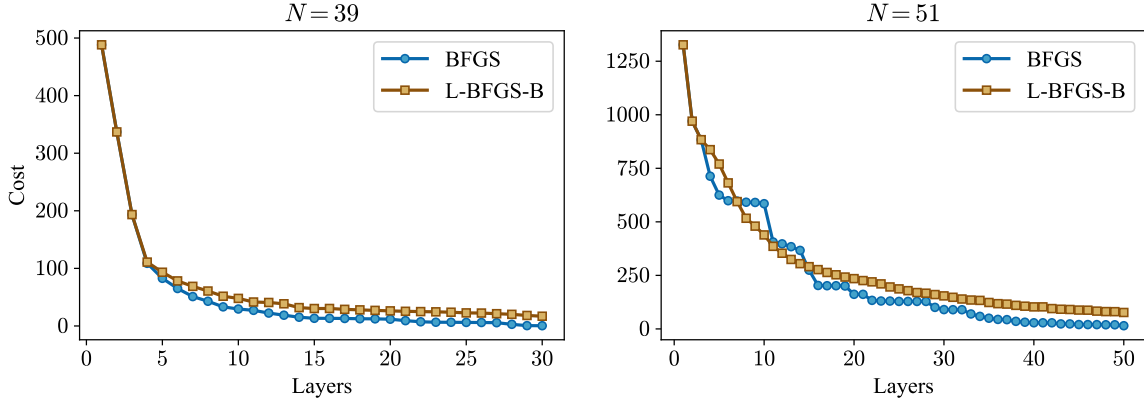


Figure 2.5: Cost evolution comparison between BFGS and L-BFGS-B for factorizing  $N = 39$  and  $N = 51$  using the standard protocol. The performance gap was observed consistently up to 8-qubit problems.

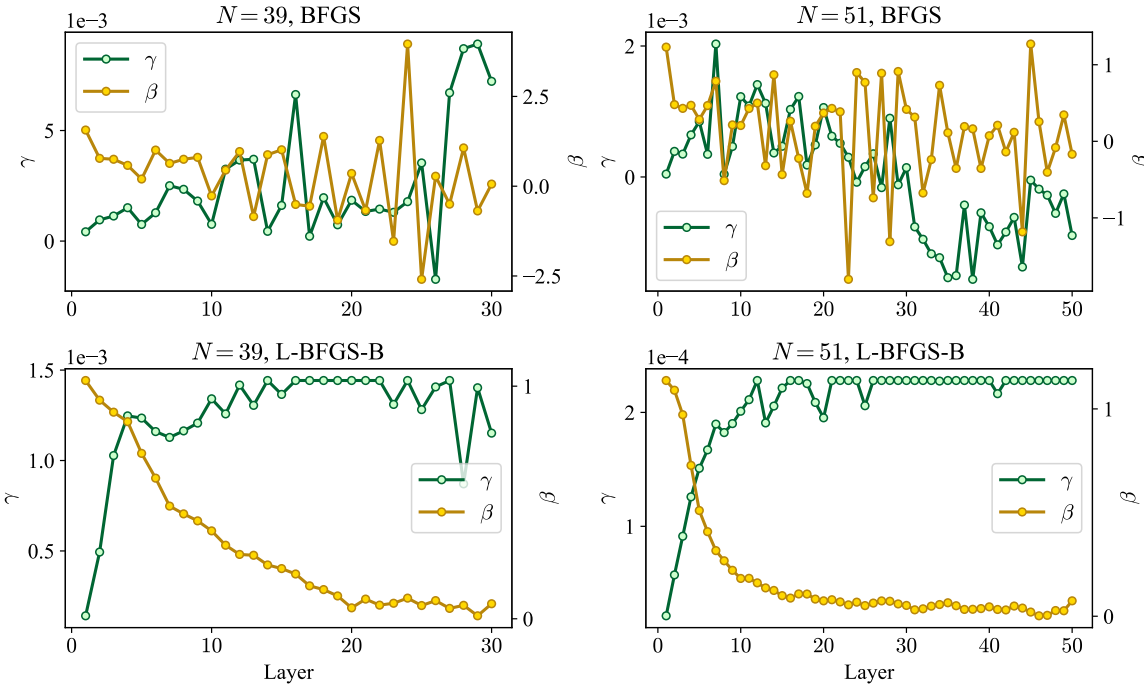


Figure 2.6: Variational parameter evolution for  $N = 39$  and  $N = 51$  using BFGS and L-BFGS-B. An adiabatic-like trajectory emerges under L-BFGS-B due to parameter bounds.

In summary, the methodological strategy to implement all QAOA circuits adopted through this thesis is as follows:

- **Initial state:**  $|+\rangle^{\otimes n}$  for the standard protocol, and  $|+-+ - + \dots\rangle$  for linear protocol.
- **Layer-by-layer training:** QAOA parameters are optimized incrementally, starting from  $p = 1$  and using previously optimized parameters as initialization for deeper circuits.
- **Parameter initialization:** New layers are initialized using the heuristic  $\gamma_{p+1} \leftarrow \tilde{\gamma}_p$ ,  $\beta_{p+1} \leftarrow 0$ , which outperforms interpolation strategies.
- **Classical optimizer:** The gradient-based, unbounded BFGS method is employed, providing superior convergence compared to bounded alternatives.

Together, these decisions define a robust and fair QAOA implementation, enabling meaningful comparisons between different problem Hamiltonians and protocols.

## RESULTS

This chapter presents the numerical experiments performed to compare the performance of the standard QAOA protocol with the proposed linearized protocol. The standard protocol is evaluated in its original formulation, while the linearized protocol is analyzed under two different cost functions to determine which provides the most favorable performance. Table 3.1 summarizes the three protocols considered throughout this chapter.

Protocol	Mixing Hamiltonian	Problem Hamiltonian	Cost function
standard	$\hat{H}_M$	$\hat{H}_{QP}$	$\langle \hat{H}_{QP} \rangle$
linear_quadratic	$\hat{H}_M$	$\hat{H}_{LP}$	$\langle \hat{H}_{QP} \rangle$
linear_abs	$\hat{H}_M$	$\hat{H}_{LP}$	$\langle  \hat{H}_{LP}  \rangle$

Table 3.1: Overview of QAOA protocols analyzed in this work.

The primary evaluation metric throughout this chapter is the *fidelity*, which directly corresponds to the probability of successfully obtaining the correct factors of the integer to be factorized. Using fidelity as a baseline metric allows for a clear and consistent comparison between protocols.

All practical aspects of the QAOA setup — including initialization heuristics and the choice of classical optimizer — were fixed and justified in section 2.4 to ensure fair and consistent comparisons. The focus here is exclusively on evaluating and contrasting the protocols across problem instances of increasing size under these controlled conditions.

As representative examples, we present detailed results for the semiprime integers  $N = 25$ ,  $N = 77$ , and  $N = 143$ . A complete set of results can be found in the accompanying GitHub repository and is summarized in the appendix A. Table 3.2 provides an overview of these selected test cases, including relevant problem parameters and solution encodings.

$N$	$n$ (# qubits)	$p$ ( $p'$ )	$q$ ( $q'$ )	$n_p$	$n_q$	$p_{\text{bitstring}}$	$q_{\text{bitstring}}$	solution(s)
25	4	5 (2)	5 (2)	2	2	10	10	0101
77	6	7 (3)	11 (5)	2	4	11	0101	111010
143	8	11 (5)	13 (6)	3	5	101	00110	10101100, 01110100

Table 3.2: Overview of semiprime test instances used as representative examples.

Firstly, we evaluate the fidelities achieved by the different protocols as a function of the number of QAOA layers (Fig. 3.1). Three distinct trends are observed:

- For  $N = 25$ , the standard protocol performs better at shallow depths, but both linear protocols eventually surpass it.

- For  $N = 77$ , both linear protocols consistently outperform the standard protocol across all layers.
- For  $N = 143$ , the standard protocol initially leads, until a sudden fidelity jump in one of the linear protocols overtakes it.

As the problem size increases, the third behavior—a sudden jump in fidelity—appears more frequently (see Fig. A.1). Although the cost-function landscape evolves more smoothly (see Fig. A.3), the fidelity of linear protocols often exhibits these abrupt improvements. The underlying reasons for this phenomenon will be analyzed in Chapter 4.

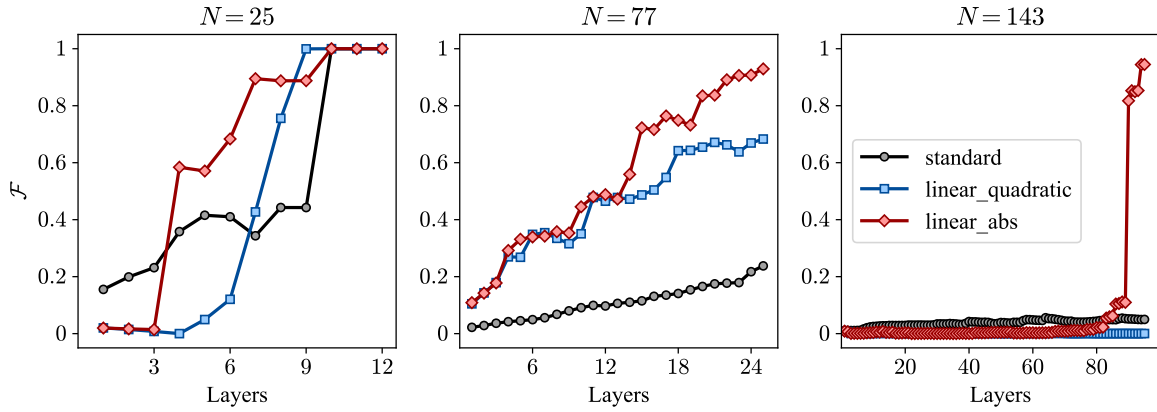


Figure 3.1: Fidelity versus QAOA layer depth. Larger problems require deeper circuits to achieve significant fidelities.

To complement the fidelity analysis, Fig. 3.2 depicts the state populations at the end of each protocol, with valid solutions highlighted by dark-colored bars.

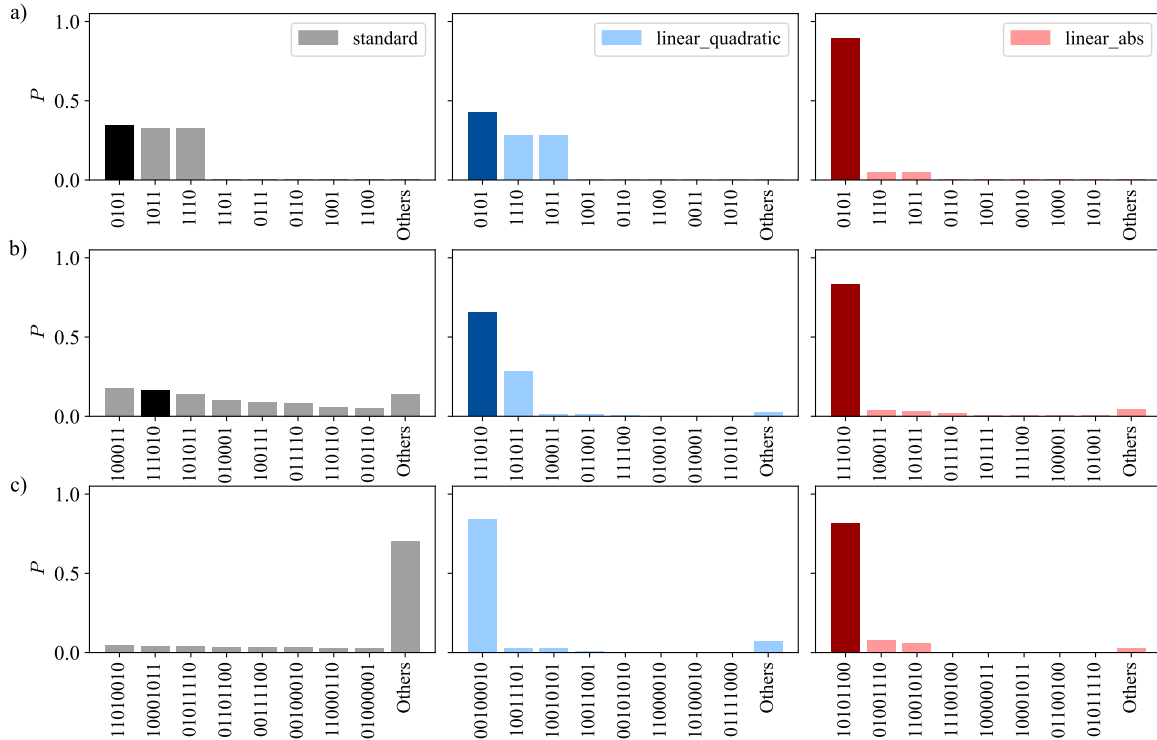


Figure 3.2: Final state populations for (a)  $N = 25$ , (b)  $N = 77$ , and (c)  $N = 143$ . The number of layers was fixed as the minimum required to reach at least 80% fidelity by any protocol. Solution states are shown as dark-colored bars.

Although fidelity as a function of depth already demonstrates the improved performance of the `linear` protocols, it is essential to evaluate them in terms of quantum resources — which is the central goal of this work. Specifically, we compare protocols using the number of two-qubit gates as the resource metric (Fig. 3.3). In these terms, the advantage of the `linear` protocols becomes clearer: they achieve significantly higher fidelities while requiring far fewer quantum operations.

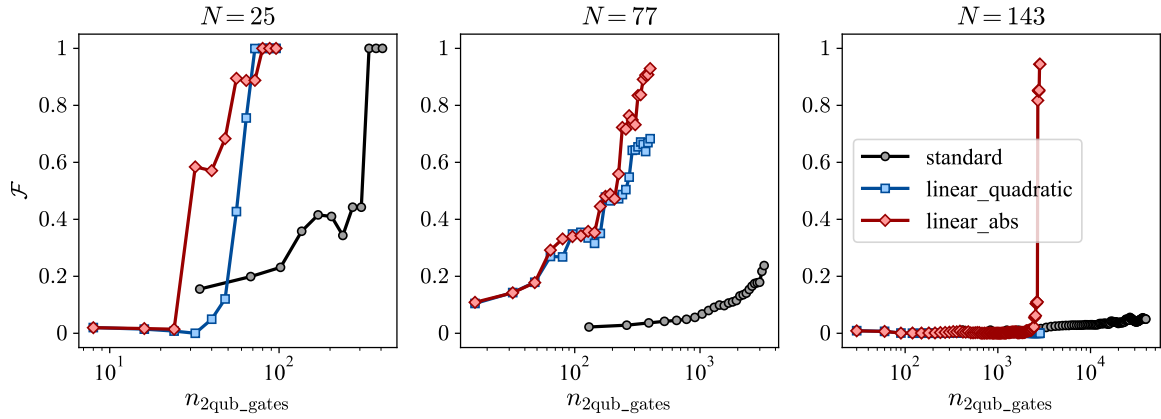


Figure 3.3: Fidelity versus the number of two-qubit gates. This metric highlights the resource efficiency of the `linear` protocols.

## DISCUSSION

The numerical results allow us to assess how the proposed linearized QAOA protocols compare to the standard formulation and to evaluate the role of the cost function in shaping their performance.

### STANDARD VERSUS LINEAR\_QUADRATIC PROTOCOLS

Since both the standard and linear\_quadratic protocols are optimized with respect to the same cost function,  $\langle \hat{H}_{QP} \rangle$ , their performance can be directly compared. In most cases, the data indicate that the linear\_quadratic protocol reaches relevant solutions with acceptable fidelity at shallower circuit depths. Moreover, when performance is measured against the number of two-qubit gates — a more meaningful indicator of quantum resource requirements — the linear protocol consistently requires fewer resources to achieve comparable or superior fidelities.

However, in some problem instances like  $N = 143$  in Fig. 3.1 and Fig. 3.3, it may initially appear that the algorithm performs better under the standard protocol than under linear\_quadratic. In terms of fidelity alone, this is technically correct, but the fidelities in this regime are so low that the difference is not practically significant. In contrast, the cost plots in Fig. A.3 reveal a different picture: the linear\_quadratic protocol consistently achieves lower cost values. This behavior indicates that it is progressing toward a better population transfer to the target state, which should ultimately translate into higher fidelity at later stages.

### IMPACT OF THE COST FUNCTION

The choice of cost function proves to be a decisive factor. Between the two linearized protocols, linear\_abs generally outperforms linear\_quadratic, achieving higher fidelities at lower resource counts. This highlights that even within a fixed ansatz structure, selecting a cost function that better reflects the problem's energy landscape can significantly enhance performance. This observation could motivate further investigation into whether alternative ways of defining the cost function might offer performance benefits.

### SUDDEN FIDELITY JUMPS IN LINEAR PROTOCOLS

One of the most distinctive features of the linear protocols is the occurrence of abrupt fidelity jumps as the number of QAOA layers increases. This contrasts with the smoother fidelity evolution observed for the standard protocol, a behavior consistently seen across the problem sizes studied (see Fig. A.1). To understand this behavior, we analyzed the spectra of the problem Hamiltonians  $\hat{H}_{LP}$  and  $\hat{H}_{QP}$ , shown in Fig. 4.1. We find that the spectrum of  $\hat{H}_{LP}$  is more widely spread, leading to larger separations between relevant energy levels. Such a structure tends to promote population transfer in discrete steps, which aligns with the observed fidelity jumps. Conversely, the denser spectrum of  $\hat{H}_{QP}$  supports a more gradual redistribution of amplitude during the variational evolution.

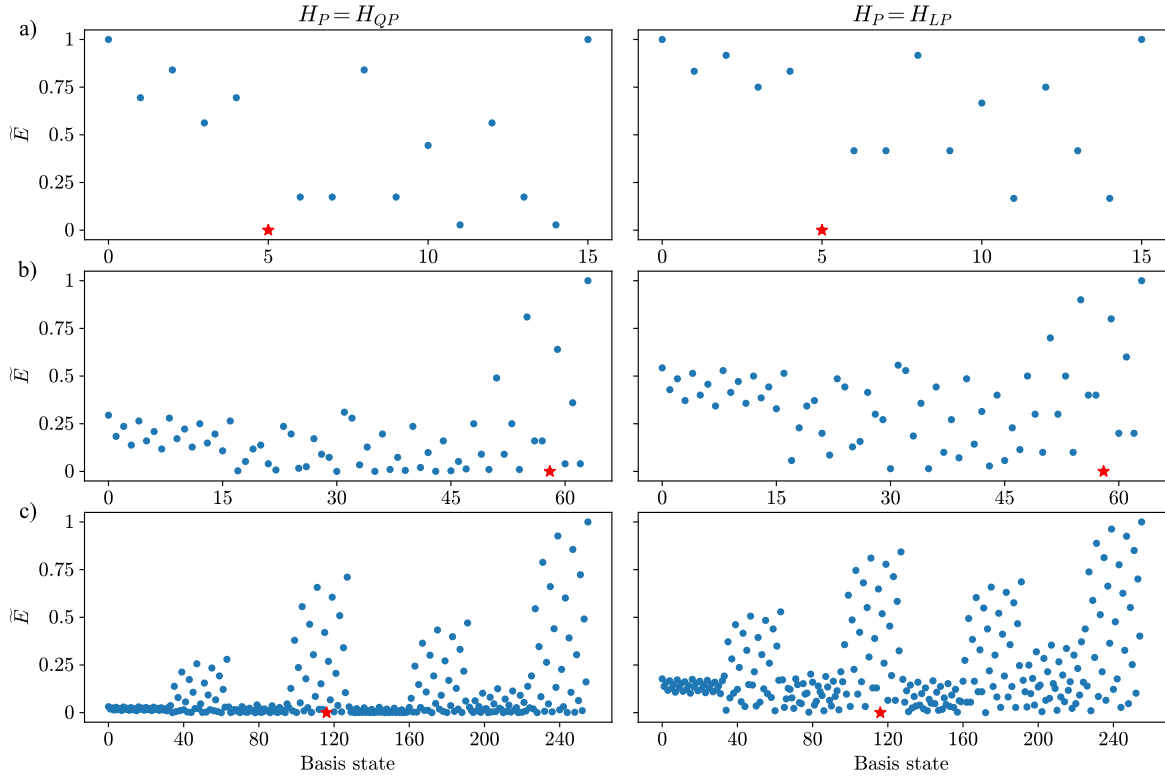


Figure 4.1: Energy spectra for (a)  $N = 25$ , (b)  $N = 77$ , and (c)  $N = 143$ . The horizontal axis shows the decimal encoding of computational basis states, while the vertical axis indicates the normalized eigenenergies. The eigenstate corresponding to the solution ( $\tilde{E} = 0$ ) is marked as a red star.

This qualitative picture is further supported by the numerical results summarized in Table 4.1. To quantify the spread of the spectra, we use the root-mean-square (RMS) distance of the eigenvalues with respect to the target energy, which provides a compact measure of how widely distributed the eigenvalues are for each Hamiltonian:

$$\text{RMS} = \sqrt{\frac{1}{d} \sum_{i=1}^d \tilde{E}_i^2}, \quad (4.1)$$

where  $\tilde{E}_i$  is the normalized energy of the  $i$ -th eigenstate and  $d$  the dimension of the Hilbert space associated to the problem instance.

The results confirm that  $\hat{H}_{LP}$  consistently exhibits larger RMS distances than  $\hat{H}_{QP}$  across the problem sizes studied, in agreement with the visual differences in Fig. 4.1. Together, the table and spectra illustrate that the wider separation of eigenvalues in  $\hat{H}_{LP}$  explains the step-like fidelity behavior observed in the linear protocol.

Protocol	$n$					
	3	4	5	6	7	8
standard	0.59	0.58	0.26	0.24	0.20	0.21
linear	0.70	0.68	0.41	0.37	0.32	0.32

Table 4.1: Root-mean-square (RMS) distance of the energy spectrum from the target state, used as a measure of how widely the eigenvalues are distributed for each Hamiltonian and problem size.

## 4.1 FUTURE PROSPECTS

While the current study focuses on semiprime integers  $N$  of moderate size, extending the analysis to larger numbers is pivotal to properly determine whether our results persist in more challenging regimes of factorization. Such investigations would provide a clearer assessment of the asymptotic potential of linearized QAOA and inform the design of more resource-efficient formulations. From an experimental standpoint, our approach offers the additional advantage of requiring only simple quantum circuits, with operations involving at most two qubits. This reduction in circuit complexity significantly enhances the feasibility of near-term realizations on existing hardware.



## A

## APPENDIX

## A.1 INFORMATION TABLE FOR ALL PROBLEM INSTANCES

$N$	$n$ (# qubits)	$p$ ( $p'$ )	$q$ ( $q'$ )	$n_p$	$n_q$	$p_{\text{bitstring}}$	$q_{\text{bitstring}}$	solution(s)
15	3	3 (1)	5 (2)	1	2	1	10	101
21	3	3 (1)	7 (3)	1	2	1	11	111
25	4	5 (2)	5 (2)	2	2	10	10	0101
35	5	5 (2)	7 (3)	2	3	10	011	01110, 11010
39	5	3 (1)	13 (6)	2	3	01	110	10011
51	6	3 (1)	17 (8)	2	4	01	1000	100001
77	6	7 (3)	11 (5)	2	4	11	0101	111010
87	7	3 (1)	29 (14)	3	4	001	1110	1000111
95	7	5 (2)	19 (9)	3	4	010	1001	0101001
115	8	5 (2)	23 (11)	3	5	010	01011	01011010
119	8	7 (3)	17 (8)	3	5	011	01000	11000010
143	8	11 (5)	13 (6)	3	5	101	00110	10101100, 01110100

Table A.1: Overview of all semiprime test instances studied in this work.

## A.2 FIDELITY PLOTS

### FIDELITY VS LAYERS

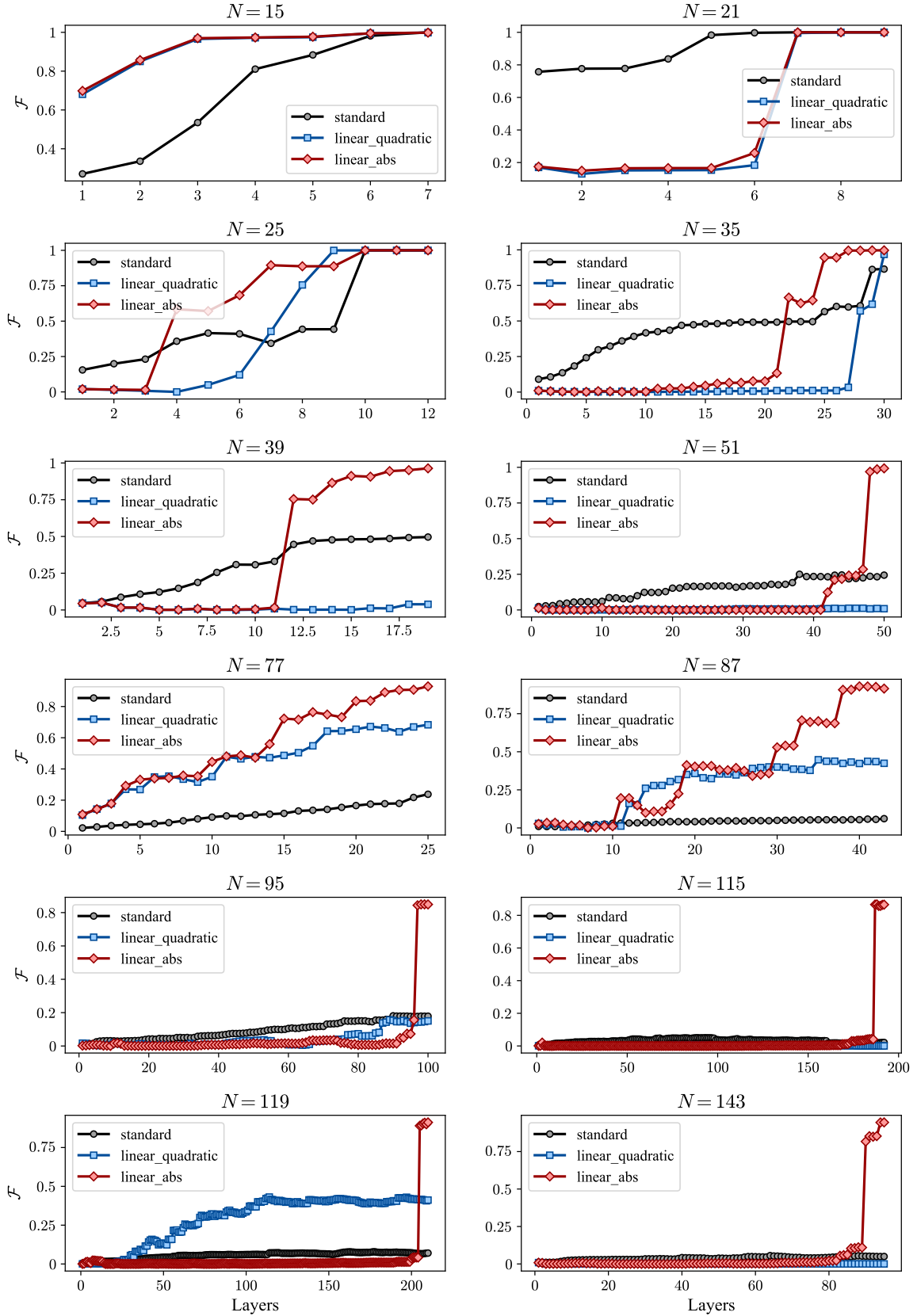


Figure A.1: Fidelity versus QAOA layer depth for all factorization instances.

## FIDELITY VS NUMBER OF TWO-QUBIT GATES

A

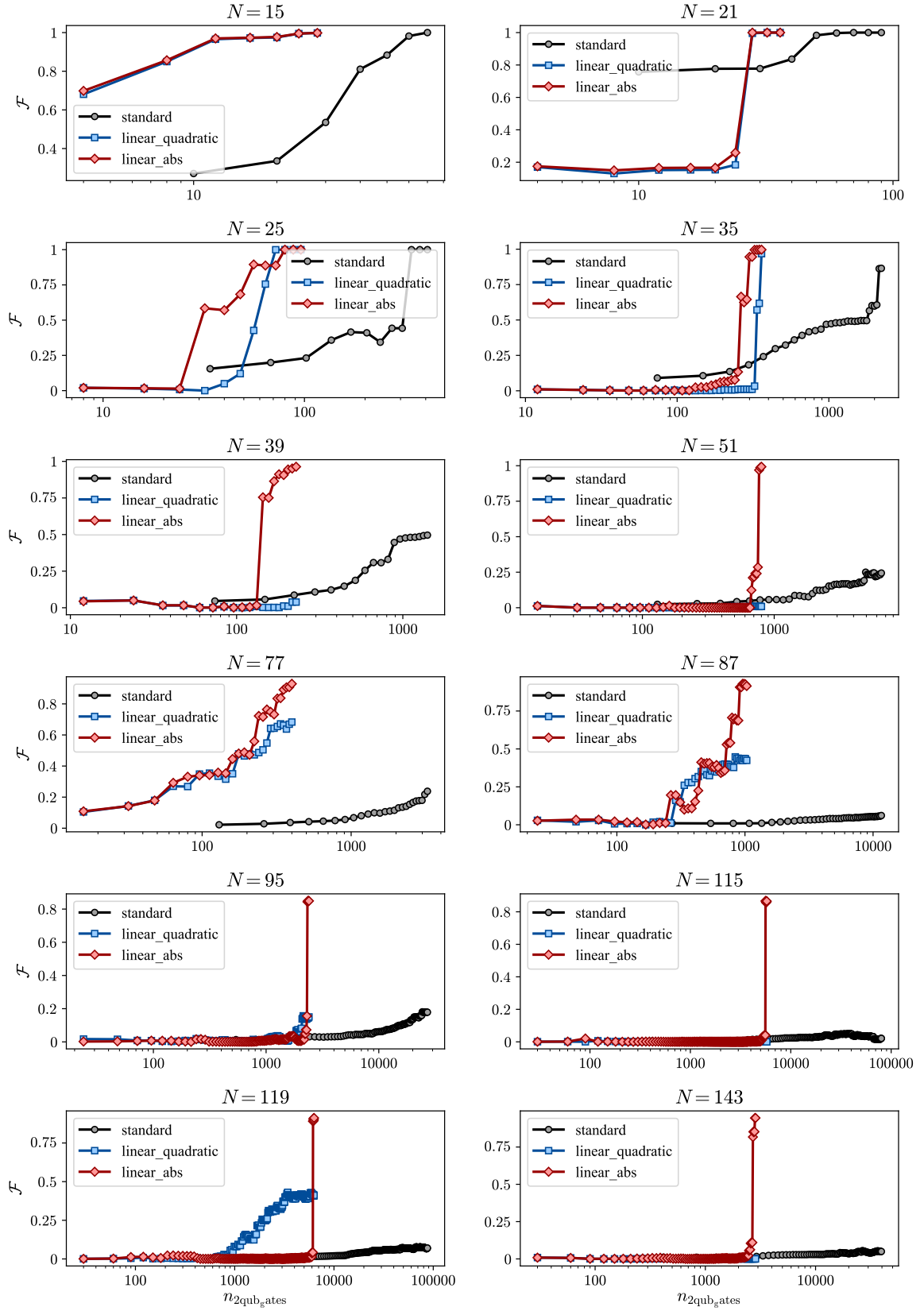


Figure A.2: Fidelity versus number of two-qubit gates for all factorization instances.

## A.3 COST VS LAYERS

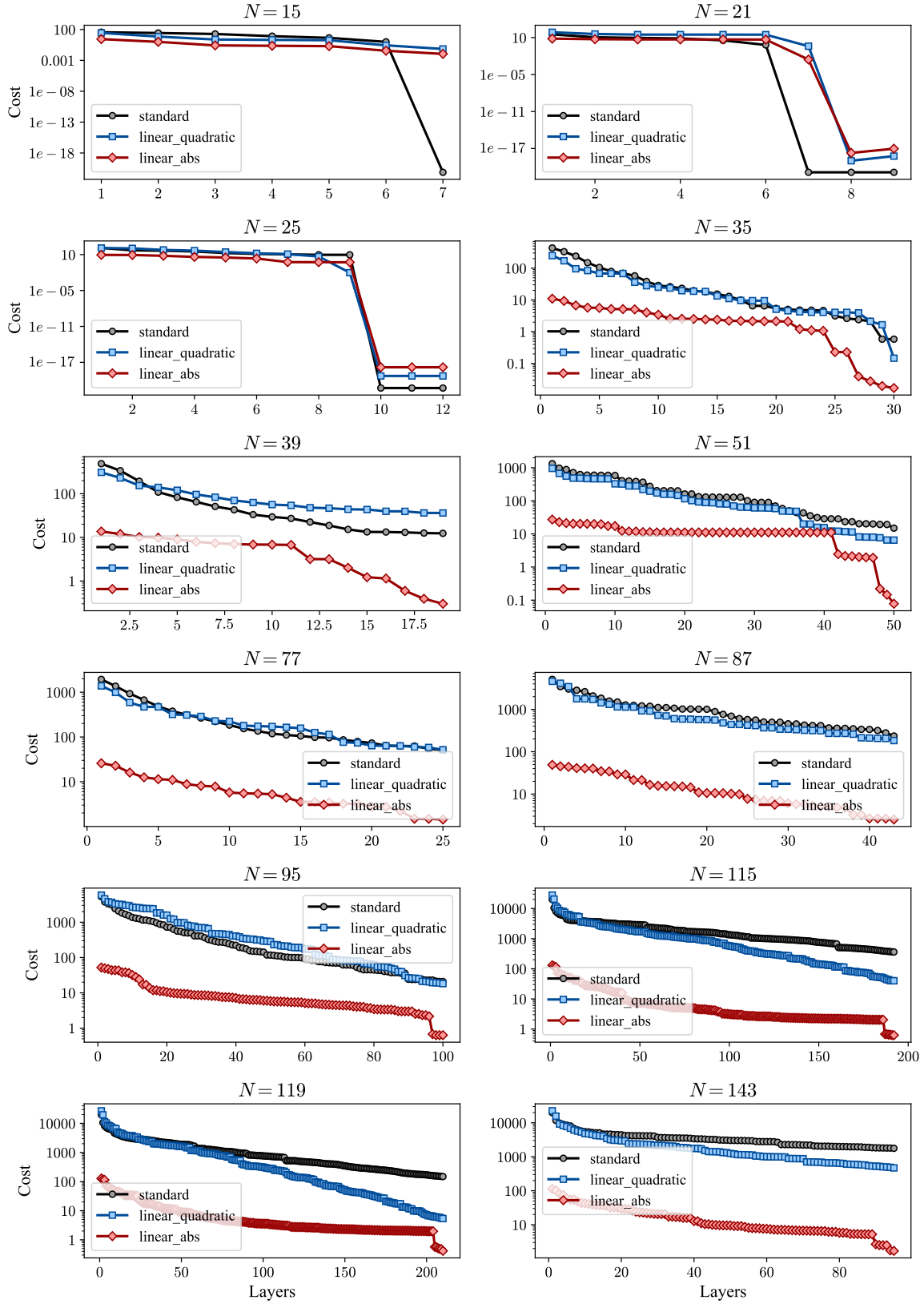
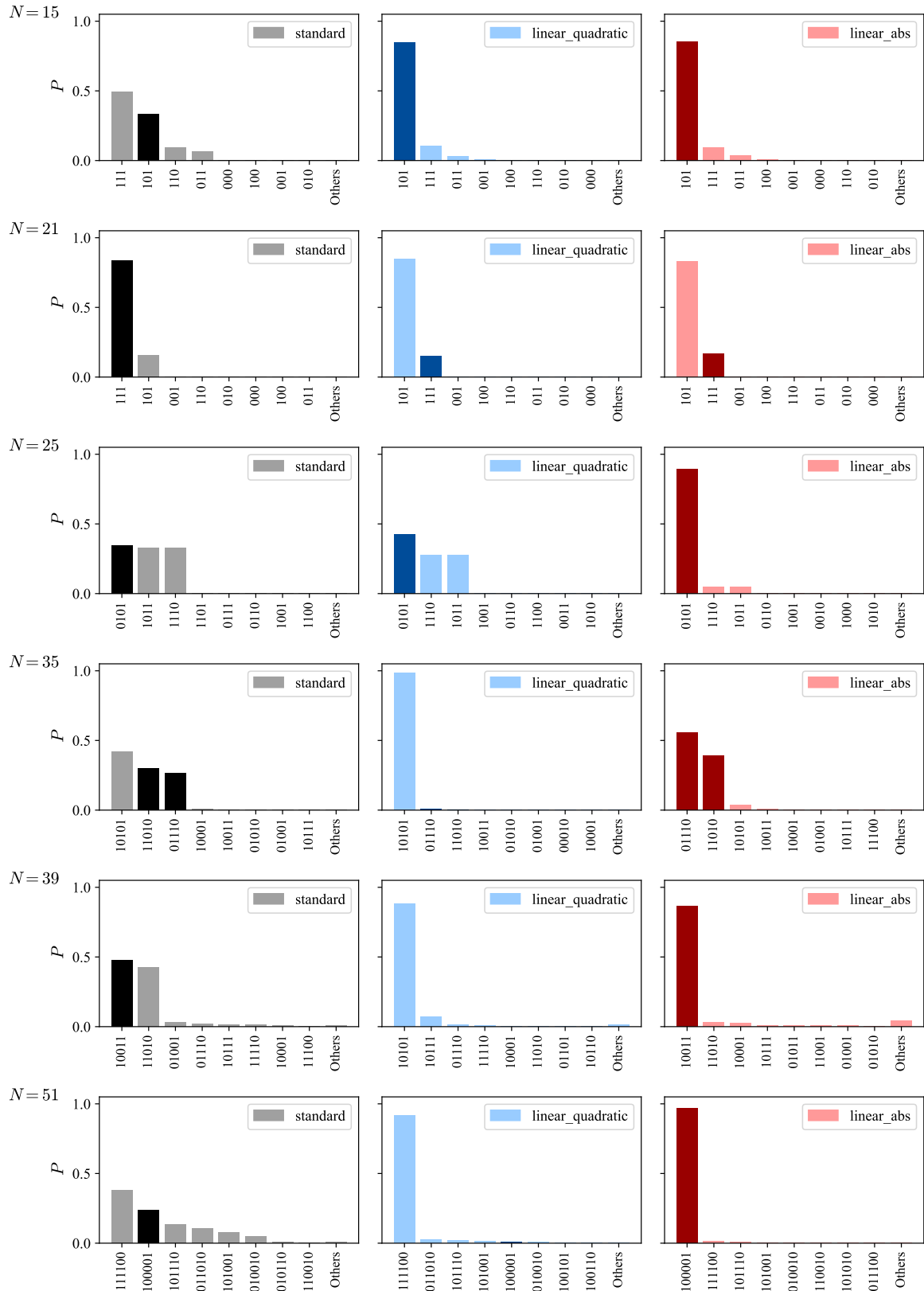


Figure A.3: Cost function versus QAOA layer depth for all factorization instances. Notice that `linear_abs` protocol has a different cost function from `standard` and `linear_quadratic`, and therefore they are not directly comparable.

## A.4 POPULATIONS

A



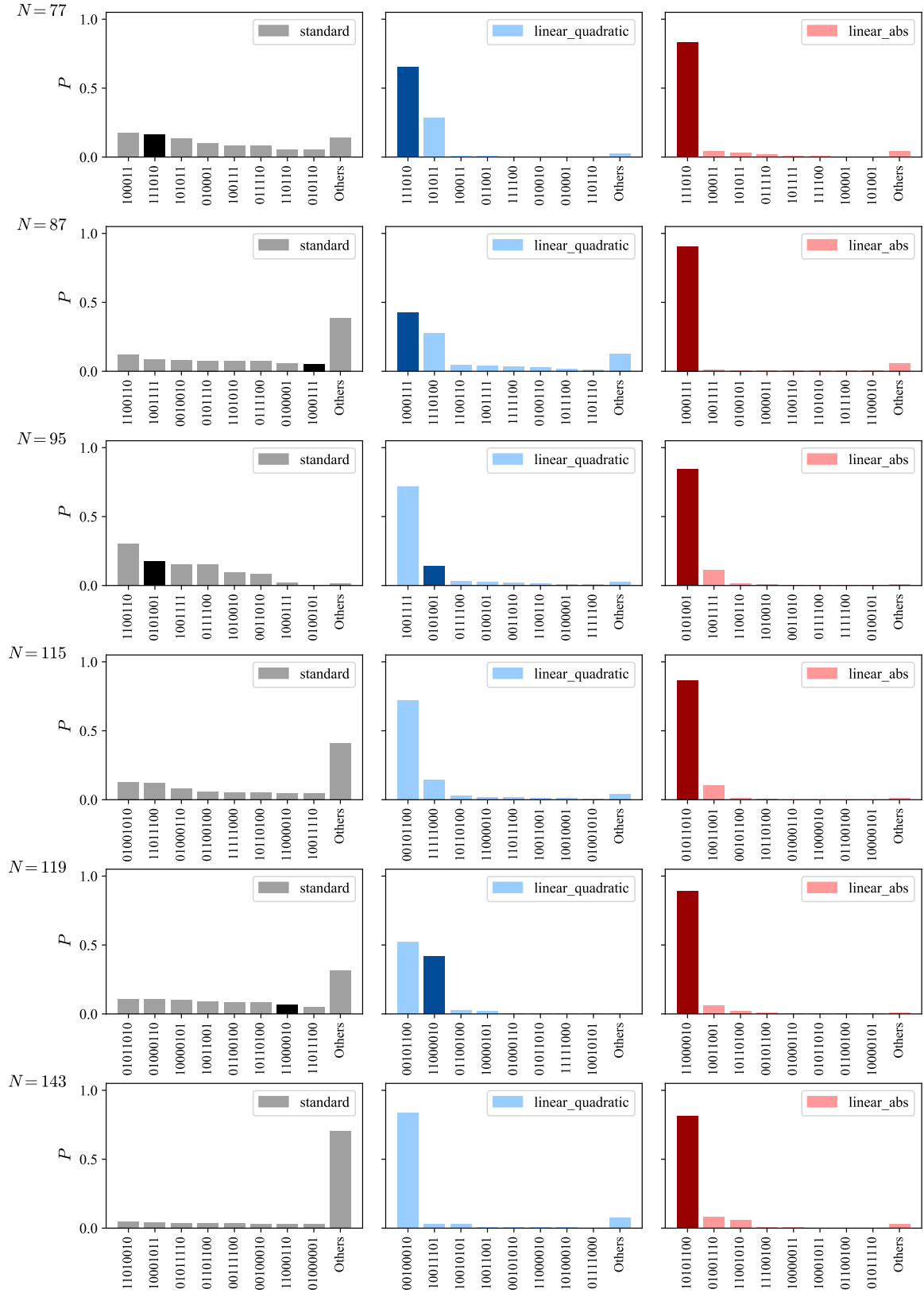
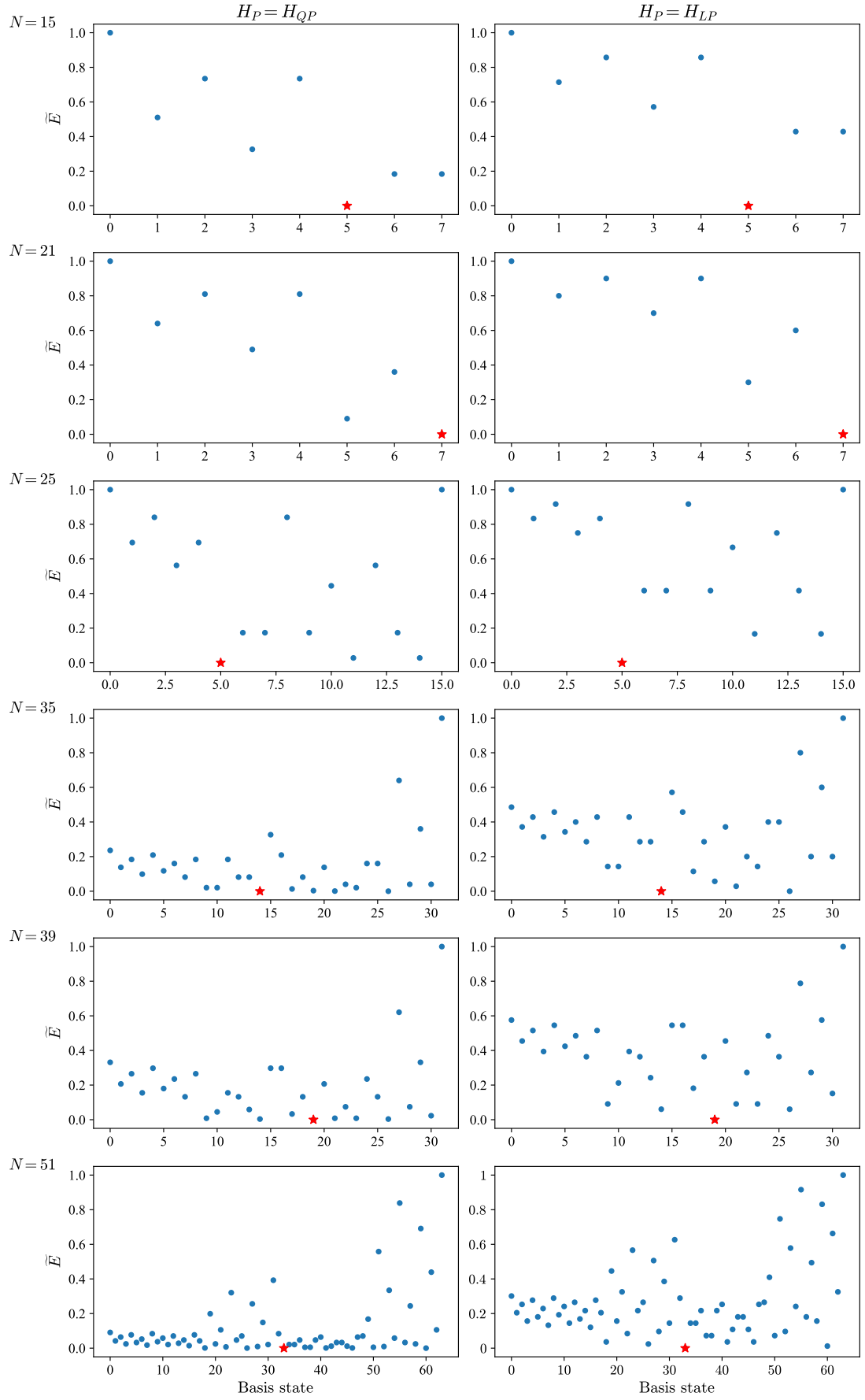


Figure A.4: Final state populations for all factorization instances. The number of layers was fixed as the minimum required to reach at least 80% fidelity by any protocol. Solution states are shown as dark-colored bars.

## A.5 ENERGY SPECTRUMS



A

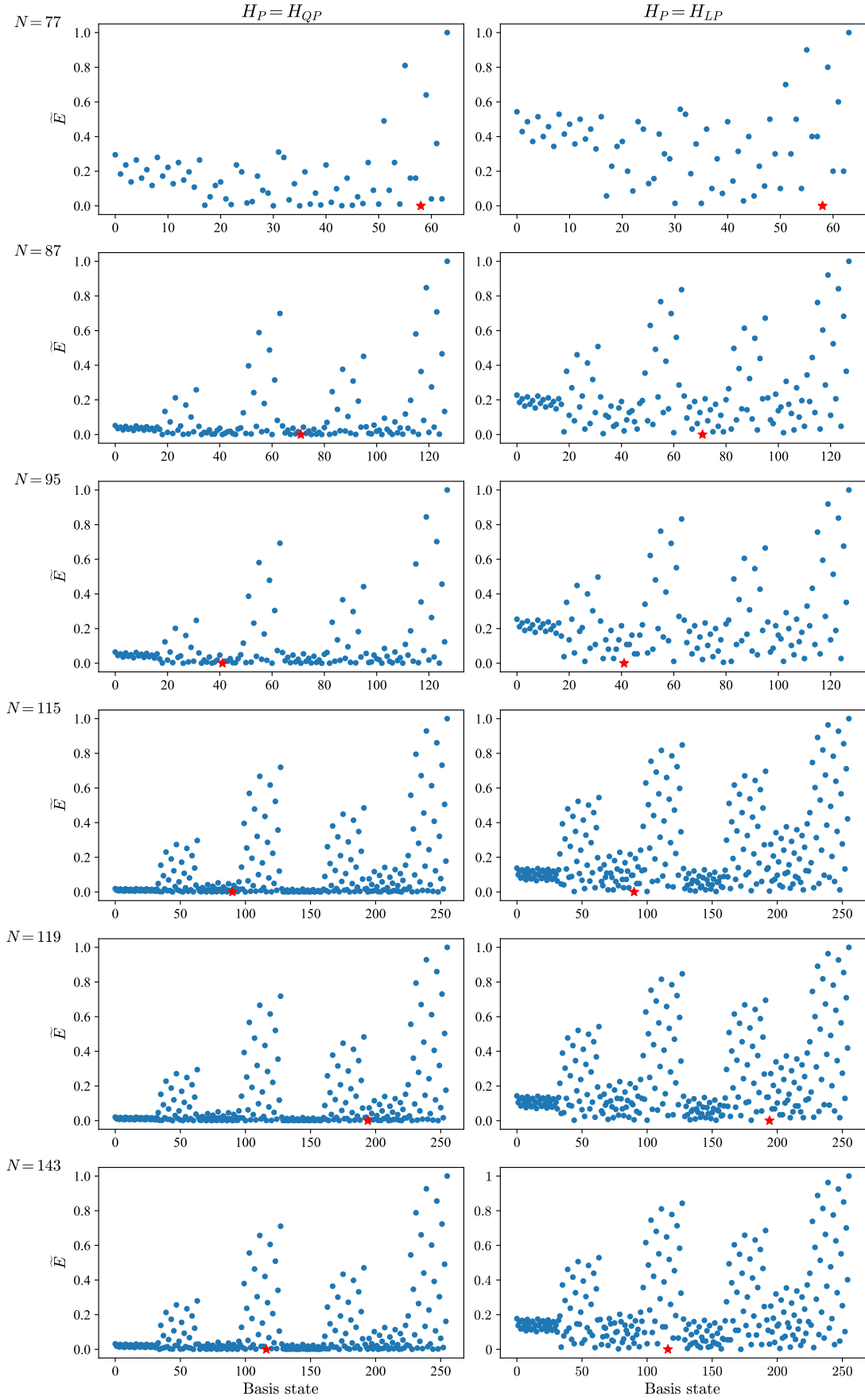


Figure A.5: Energy spectra for all factorization instances. The horizontal axis shows the decimal encoding of computational basis states, while the vertical axis indicates the normalized eigenenergies. Eigenstates corresponding to solutions are marked as red stars.



## BIBLIOGRAPHY

- [1] P.L. Montgomery. A survey of modern integer factorization algorithms. *CWI Quarterly*, 7(4):337—366, December 1994.
- [2] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
- [3] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Santa Fe, NM, USA, 1994. IEEE Comput. Soc. Press.
- [4] Tameem Albash and Daniel A. Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, January 2018.
- [5] M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. Variational Quantum Algorithms. *Nature Reviews Physics*, 3(9):625–644, August 2021. arXiv:2012.09265 [quant-ph].
- [6] Narendra N. Hegade, Koushik Paul, Francisco Albarrán-Arriagada, Xi Chen, and Enrique Solano. Digitized Adiabatic Quantum Factorization. *Physical Review A*, 104(5):L050403, November 2021. arXiv:2105.09480 [quant-ph].
- [7] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [8] M. S. Sarandy, L.-A. Wu, and D. A. Lidar. Consistency of the Adiabatic Theorem. *Quantum Information Processing*, 3(6):331–349, December 2004.
- [9] D. Aharonov, W. Van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 42–51, Rome, Italy, 2004. IEEE.
- [10] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum Annealing in the Transverse Ising Model. *Physical Review E*, 58(5):5355–5363, November 1998. arXiv:cond-mat/9804280.
- [11] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A Quantum Approximate Optimization Algorithm, November 2014. arXiv:1411.4028 [quant-ph].
- [12] Leo Zhou, Sheng-Tao Wang, Soonwon Choi, Hannes Pichler, and Mikhail D. Lukin. Quantum Approximate Optimization Algorithm: Performance, Mechanism, and Implementation on Near-Term Devices. *Physical Review X*, 10(2):021067, June 2020.
- [13] Edward Farhi and Aram W. Harrow. Quantum Supremacy through the Quantum Approximate Optimization Algorithm, October 2019. arXiv:1602.07674 [quant-ph].

- [14] Wen Wei Ho and Timothy H. Hsieh. Efficient variational simulation of non-trivial quantum states. *SciPost Physics*, 6(3):029, March 2019. arXiv:1803.00026 [cond-mat].
- [15] Eric R. Anschuetz, Jonathan P. Olson, Alán Aspuru-Guzik, and Yudong Cao. Variational Quantum Factoring, August 2018. arXiv:1808.08927 [quant-ph].
- [16] Xinhua Peng, Zeyang Liao, Nanyang Xu, Gan Qin, Xianyi Zhou, Dieter Suter, and Jiangfeng Du. A Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation. *Physical Review Letters*, 101(22):220405, November 2008. arXiv:0808.1935 [quant-ph].
- [17] Pablo Díez-Valle, Fernando J. Gómez-Ruiz, Diego Porras, and Juan José García-Ripoll. Universal Resources for QAOA and Quantum Annealing, June 2025. arXiv:2506.03241 [quant-ph].
- [18] Amir H. Karamlou, William A. Simon, Amara Katabarwa, Travis L. Scholten, Borja Peropadre, and Yudong Cao. Analyzing the Performance of Variational Quantum Factoring on a Superconducting Quantum Processor. *npj Quantum Information*, 7(1):156, October 2021. arXiv:2012.07825 [quant-ph].
- [19] Kostas Blekos, Dean Brand, Andrea Ceschini, Chiao-Hui Chou, Rui-Hao Li, Komal Pandya, and Alessandro Summer. A Review on Quantum Approximate Optimization Algorithm and its Variants. *Physics Reports*, 1068:1–66, June 2024. arXiv:2306.09198 [quant-ph].