Industrial and
Systems Engineering

An Infeasible-Inexact Quantum Interior Point Method for Convex Quadratic Symmetric Cone Optimization

BRANDON AUGUSTINO [1], GIACOMO NANNICINI [2], TAMÁS TERLAKY[1], AND LUIS F. ZULUAGA[1]

[1]Department of Industrial and Systems Engineering, Lehigh University, Bethlehem, PA
[2]IBM T.J. Watson Research Center, Yorktown Heights, NY

bra216@lehigh.edu

ISE Technical Report 21T-010

LEHIGH UNIVERSITY

A Quantum Interior Point Method for Convex Quadratic Symmetric Cone Optimization Problems

Brandon Augustino, Giacomo Nannicini, Tamás Terlaky, Luis F. Zuluaga

April 29, 2021

Abstract

We present a provably convergent quantum interior point method for convex quadratic symmetric optimization problems. We provide explicit definitions for the Newton linear system corresponding to the Nesterov-Todd search direction, and show how to solve these symmetrized linear systems using a quantum computer. These results are based on recent progress in quantum linear system solvers and on the block-encoding technique. In the presence of quantum-accessible storage (also known as QRAM), we are able to obtain speedups in terms of the size of the problem, at the price of a worse dependence on the condition number. In fact, the bottleneck for the quantum interior point method is in extracting a classical estimate of the solution to the quantum Newton linear system in order to proceed to the next iteration.

1 Introduction

In this paper, we develop Quantum Interior Point Methods (QIPMs) for solving Convex Quadratic Optimization problems (CQOPs) over the product of symmetric positive definite matrices, second-order cones, and nonnegative orthants. Following [18], we present our work under the framework of Euclidean Jordan algebras, as the symmetric cones we study are simply cones of squares of some Euclidean Jordan algebras.

A Jordan Algebra J is a finite dimensional vector space with a bilinear map $\circ : J \times J \to J$. Recall that Jordan algebras satisfy the following properties for all $(\mathbf{x}, y) \in J \times J$:

(i) $x \circ y = y \circ x$

(ii) $x \circ (x^2 \circ y) = x^2 \circ (x \circ y)$ where $x^2 = \mathbf{x} \circ x$.

Additionally, $(J, \circ)$ is said to be a Euclidean Jordan algebra if for $(\mathbf{x}, y, \mathbf{z}) \in J \times J \times J$ there exists a symmetric positive definite bilinear form $\langle \cdot, \cdot \rangle$ such that $\langle \mathbf{x} \circ y, \mathbf{z} \rangle = \langle \mathbf{x}, y \circ \mathbf{z} \rangle$. In what follows, we let $\mathcal{J}$ denote the product of p Euclidean Jordan algebras $(\mathcal{J}_i, \circ)$ with identity element $\mathbf{e}_i$ satisfying $\mathbf{x}_i \circ \mathbf{e}_i = \mathbf{x}_i$ for all $\mathbf{x}_i \in \mathcal{J}_i$. Thus,

$$\mathcal{J} = \{\mathbf{x} = (\mathbf{x}_i)_{i=1}^p : \mathbf{x}_i \in \mathcal{J}_i, i = 1, \ldots, p\}$$

with $\mathbf{x} \circ \mathbf{y} = (\mathbf{x}_i \circ \mathbf{y}_i)_{i=1}^p$ for all $\mathbf{x}, y \in \mathcal{J}$ the identity element of $\mathcal{J}$ is similarly defined as $e = (e_i)_{i=1}^p$.

Next, let $\mathcal{K}$ be the cone of squares of $\mathcal{J}$ such that $\mathcal{K}$ is defined as

$$\mathcal{K} = \{\mathbf{x}^2 : \mathbf{x} \in \mathcal{J}\},$$

and note that $\mathcal{K}$ is thus a symmetric cone. That is, $\mathcal{K}$ is a closed, pointed convex cone that is self dual. In this paper, we consider the following CQOP over symmetric cones:

$$\begin{aligned} z_P = \min\ f(\mathbf{x}) := \frac{1}{2}\langle \mathbf{x}, \mathcal{H}(\mathbf{x})\rangle + \langle \mathbf{c}, \mathbf{x}\rangle \\ \text{s.t. } \mathcal{A}(\mathbf{x}) = b,\ \mathbf{x} \in \mathcal{K}, \end{aligned} \tag{1}$$

where $c \in \mathcal{J}$ and $b \in \mathbb{R}^m$ are given data, $\mathcal{A} : \mathcal{J} \to \mathbb{R}^m$ is a linear map, and $\mathcal{H}$ is a self-adjoint positive semidefinite linear operator on $\mathcal{J}$. Similarly, the dual problem of (1) is given by

$$\begin{aligned} z_D = \max\ f(\mathbf{x}) &:= -\frac{1}{2}\langle \mathbf{x}, \mathcal{H}(\mathbf{x})\rangle + b^\top y \\ \text{s.t. } \mathcal{A}^\top y + \mathbf{z} &= \nabla f(\mathbf{x}) = \mathcal{H}(\mathbf{x}) + \mathbf{c},\ \mathbf{z} \in \mathcal{K}, \end{aligned} \tag{2}$$

where $\mathcal{A}^\top$ denotes the adjoint of $\mathcal{A}$. As in the case in [18], in what follows, we rely on the following assumptions. First, it is assumed that both (1) and (2) are strictly feasible. Hence, there exists $(\mathbf{x}, y, \mathbf{z})$ satisfying the linear constraints of (1) and (2) and $\mathbf{x}, \mathbf{z} \in \text{int}(\mathcal{K})$ where $\text{int}(\mathcal{K})$ denotes the interior of $\mathcal{K}$. Second, $\mathcal{A}$ is assumed to be surjective, implying that $\mathcal{A}\mathcal{A}^\top$ is non-singular, and thus the psuedoinverse of $\mathcal{A}$, $\mathcal{A}^+ = \mathcal{A}^\top(\mathcal{A}\mathcal{A}^\top)^{-1}$, is well defined.

Note that linear symmetric cone optimization problems are simply a special case of the problem given by (1) which corresponds to when $\mathcal{H} = \mathbf{0}$. That is, if we take $\mathcal{K} = S_n^+$ we have a linear semidefinite optimization problem (LSDO), and similarly, taking $\mathcal{K} = \mathbb{R}^n_+$ yields a linearly constrained convex quadratic optimization problem (LCCQO). Similar to SDOPs, we have we have polynomial-time algorithms for solving QCOs over symmetric cones. The ellipsoid algorithm is the first algorithm proven to solve LOs in polynomial time [16]. Later, Karmarkar introduced his interior point method (IPM) for LOs, which improved the complexity of the ellipsoid method in [11]. Nesterov and Nemirovsky are responsible for the first polynomial time IPM for SDOPs [21], whose framework utilizes efficiently computable self-concordant barrier functions. As discussed in [22], SOCOPs can be solved using the approach to solve SDOPs, using IPMs to solve SOCOPs directly have an iteration bound that depends on the number of cones r. This iteration bound is lower than the iteration bound corresponding to classical IPMs for SDOPs, which depend on the number of variables n, and for SOCOPs, n may in fact be much larger than N [22].

The first effort at a quantum interior point method for over symmetric cones comes from [15], who developed a QIPM for SOCOPs. By employing quantum random access memory (QRAM) and quantum linear system solvers developed by [5], the authors in [15] claim to be able to efficiently solve the Newton linear system in each iteration. As such, they claim an ϵ-approximate solution to an SOCOP can be found with their algorithm in time

$$\tilde{O}\left(n\sqrt{r}\frac{\kappa\mu}{\delta^2}\log\frac{1}{\epsilon}\log\left(\frac{\kappa\mu}{\delta}\right)\right)$$

where ϵ is the optimality gap, κ is an upper bound for the condition number of the Newton systems, $\mu \leq \sqrt{n}$ is a factor coming from quantum linear system solvers and δ is a lower bound for the distance to the cones associated with the intermediate solutions of the algorithm.

Although the authors in [15] provide a foundation for a QIPM for SOCOPs, the algorithm is not valid for solving SOCOPs. This is due to two reasons, (i) they do not take the proper precautions in order to guarantee the solution to the Newton system is an element of $\mathcal{J}$ and (ii) the authors do not account for the errors introduced from using quantum linear system solvers to solve the Newton system. As such, the algorithm in [15] cannot be applied to SOCOPs; we discuss this in more detail subsequently in the paper. Additional safeguards must be taken into account in order to ensure that the solutions to the so called Newton linear system belong to $\mathcal{J}$. Thus, we make use of the classical inexact-infeasible interior point method from Li and Toh [18] in order to account for these aspects.

There was a significant effort extend the search direction results for SDOPs to SOCOPs in order to ensure that the solutions to the Newton linear system commute. In studying a primal-dual approach to SDOPs and SOCOPs, Alder and Alizadeh [1] developed the SOCOP analog of the Alizadeh-Haeberly-Overton (AHO) [2] search direction for SDOPs. Similarly, Faybusovich provided analysis for the Nesterov-Todd method for SOCOPs [7]. Further, both Monteiro [20] and Tsuchiya [29] conduct analysis on various search directions for SOCOPs using Jordan algebraic techniques. In this work, we only consider the Nesterov-Todd (NT) [23, 28] direction.

In this paper we present a inexact-infeasible quantum interior point method (II-QIPM) for QCOPs over symmetric cones that follows the general scheme of [15], but we take safeguards from the classical IPM literature in order to ensure the validity and convergence of the algorithm. In particular, we *(i)* modify the

Newton linear system to use the Nesterov-Todd (NT) [23, 28] search direction in a way that accounts for the errors naturally introduced by Quantum Linear System solvers; *(ii)* we describe how to construct the corresponding linear system with the use of quantum-accessible data structures, making use of the block encoding techniques from [5, 8] and *(iii)* provide a detailed analysis of the corresponding running time. To the best of our knowledge, this paper serves yields the first provably convergent quantum interior point method designed for SOCOPs.

The running time of the II-QIPM discussed in this paper, when using the Nesterov-Todd direction, is

$$\tilde{O}\left(\frac{n^{8.5}}{\epsilon}\kappa^3\rho^3\right),$$

where $\rho > 0$ is a constant. In light of the overall cost of our II-QIPM, we have identified three challenges hindering the development of efficient Quantum Interior Point Methods. First, the inexactness of quantum linear system solvers requires the use of the infeasible-inexact IPM framework as a foundation, and thus, with respect to the iteration bound, the dependence on n increases from $O(\sqrt{n})$ (as in feasible IPMs) to $O(n^2)$. A related concern is that the overall cost depends on the size of the solution, which for II-IPMs, depend on the dimension n, and a constant $\rho > 0$, for which there does not exist established bounds, but can be exponentially large even in the case of linear optimization. Second, the inefficiency of constructing block encodings in a purely quantum manner leads to the use of a tomography subroutine. Performing this step in a purely quantum manner can lead to a quadratic dependence on the condition number of the matrices involved in the block encoding. As a consequence, the remaining $O(n^5)$ of the total $O(n^7)$ dependence on n in the running time is attributed to the use of this tomography subroutine, as the solution size has a dependence on the dimension of $O(n^{1.5})$ and the tomography error scales quadratically. Finally, upon solving the Newton linear system, the amplitude amplification step of QLSA induces a linear dependence on the condition number, κ. We address each of these concerns in more detail later in the manuscript. Compared to the running time of the quantum MWU method, the main advantage is that we gain polylogarithmic dependence on $1/\epsilon$, but this comes at a cost of worse dependence on other parameters, most notably n and κ. Now, compared to classical methodologies, this implies an $O(n)$ advantage with respect to classical II-IPMs, but an $O(\sqrt{n})$ disadvantage when compared to classical small-neighborhood feasible IPM variants. Of course, these classical IPM methodologies do not depend on κ.

In light of lower bounds on κ, an important observation of our paper is that we do not expect a quantum algorithm based on solving the Newton linear system with a QLSA (e.g., the II-QIPM presented in this paper, based on [13], as well as [4, 15]) to be faster than a classical algorithm when exact solutions are required. Briefly, the argument is as follows. It is known [9] that the dependence of QLSAs on κ cannot be reduced to $\kappa^{1-\delta}$ for any $\delta > 0$ unless BQP = PSPACE. At the same time, the condition number of the Newton linear system goes to infinity as the solution approaches optimality, as discussed subsequently in this paper. Hence, the running time of QLSA-based interior point methods scales unfavorably. On the other hand, such quantum algorithms could still have an advantage when few iterations are sufficient, and κ could be small; this can be the case, e.g., in certain machine learning applications [15]. Another way to circumvent these results would be to develop a QLSA with better κ dependence at the expense of some other parameters (e.g., giving up polylogarithmic dependence on the size of the matrix, since the II-QIPM has polynomial dependence on this parameter anyway).

The rest of this paper is organized as follows. In Section 2, we introduce some necessary details on Jordan Algebras and symmetric cones. Section 3 presents the requisite quantum data structures, and quantum linear system solution techniques. In Section 4 we discuss the classical interior point method, in addition to important theoretical results from the IPM literature. In Section 6 we provide a Inexact-Infeasible Quantum Interior Point Method for QCOPs over symmetric cones and theoretical analysis of the running time for this Quantum Interior Point Method. Section 7 concludes the paper.

2 Euclidean Jordan Algebras

Let $(\mathcal{J}, \circ)$ be a Euclidean Jordan algebra with a unique identity element $\mathbf{e}$. We say that $\mathbf{c} \in \mathcal{J}$ is an *idempotent* if it is a nonzero element satisfying $\mathbf{c}^2 = \mathbf{c}$. Further, an idempotent is said to be primitive if it cannot be written as the sum of two idempotents. A complete set of idemopotents is a set of idempotents $\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$ satisfying $\mathbf{c}_i \circ \mathbf{c_j} = \mathbf{0}$ for all $i \neq j$ and additionally $\mathbf{c}_1 + \cdots + \mathbf{c}_k = \mathbf{e}$. Further, for $\mathbf{x} \in \mathcal{J}$ the smallest integer such that $\{\mathbf{e}, \mathbf{x}, \ldots, \mathbf{x}^k\}$ is linearly independent is said to be the degree of $\mathbf{x}$. We denote by r the rank of $\mathcal{J}$, and note that the maximum number of primitive idempotents is less than or equal to r. A Jordan frame is a complete set of orthogonal idempotents $\{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$.

Theorem 1. *[6, Theorem III.1.2] Let $\mathcal{J}$ be an Euclidean Jordan algebra with rank r and unit element $\mathbf{e}$. Then, for any $\mathbf{x} \in \mathcal{J}$, there exists a Jordan frame $\{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$ and real numbers $\lambda_1, \ldots, \lambda_r$ such that $\mathbf{x} = \lambda_1 \mathbf{c}_1 + \cdots + \lambda_r \mathbf{c}_r$. The numbers λ_i, $i = 1, \ldots, r$ are uniquely determined by $\mathbf{x}$, and they are called the eigenvalues of $\mathbf{x}$.*

For every $\mathbf{x} \in \mathcal{J}$, we order the eigenvalues of $\mathbf{x}$ in increasing order, that is, $\lambda_1 \geq \cdots \geq \lambda_r$. If we have $\lambda_1 \geq \cdots \geq \lambda_r \geq 0$ we say that $\mathbf{x}$ is positive semidefinite and we write $\mathbf{x} \succeq 0$. Similarly, if the eigenvalues are all strictly greater than 0, than $\mathbf{x}$ is said to be positive definite, which we denote by $\mathbf{x} \succ 0$.

By Theorem 1, for any $\mathbf{x} \in \mathcal{J}$, we define

$$\operatorname{tr}(\mathbf{x}) := \lambda_1 + \cdots + \lambda_r, \quad \det(\mathbf{x}) := \lambda_1, \ldots, \lambda_r. \tag{3}$$

Following from [6, Proposition II.2.2], for all $\mathbf{x}, \mathbf{y} \in Jcal$ we have

$$\det(\mathbf{x} \circ \mathbf{y}) = \det(\mathbf{x}) \circ \det(\mathbf{y})$$

and $\operatorname{tr}(\mathbf{e}) = r$, $\det(\mathbf{e}) = 1$.

Consider $\mathbf{x} \in \mathcal{J}$, for any continuous function $f(\cdot)$ defined on an open set containing the set of eigenvalues $\Lambda(\mathbf{x}) = \{\lambda_1, \ldots, \lambda_r\}$, we can define

$$f(\mathbf{x}) = f(\lambda_1)\mathbf{c}_1 + \cdots + f(\lambda_r)\mathbf{c}_r.$$

One can easily verify that the following identities are well-defined:

$$\begin{aligned}
\mathbf{x}^{-1} &:= \lambda_1^{-1}\mathbf{c}_1 + \cdots + \lambda_r^{-1}\mathbf{c}_r, \text{ if } \lambda_i \neq 0 \ \forall i \\
\mathbf{x}^{1/2} &:= \lambda_1^{1/2}\mathbf{c}_1 + \cdots + \lambda_r^{1/2}\mathbf{c}_r, \text{ if } \lambda_i \geq 0 \ \forall i \\
||\mathbf{x}||_2 &:= \max\{|\lambda_1|, \ldots, |\lambda_r|\} \\
\log\det(\mathbf{x}) &: -\log(\lambda_1) + \cdots + \log(\lambda_r), \text{ if } \lambda_i > 0 \ \forall i.
\end{aligned}$$

Further, by [6, Proposition III.4.2] we have

$$\begin{aligned}
\nabla \log\det(\mathbf{x}) &= \mathbf{x}^{-1}, \text{ and} \\
\nabla^2 \log\det(\mathbf{x}) &= \mathbf{Q}(\mathbf{x}^{-1}).
\end{aligned}$$

By [6, Proposition III.1.5], we can define an inner product on $\mathcal{J}$ as follows:

$$\langle \mathbf{x}, \mathbf{y} \rangle = \operatorname{tr}(\mathbf{x} \circ \mathbf{y}) \ \forall \mathbf{x}, \mathbf{y} \in \mathcal{J}. \tag{4}$$

Note that $\langle \cdot, \cdot \rangle$ is an associative operation due to the fact that $\operatorname{tr}(\cdot)$ is associative [6, Proposition II.4.3] and we have $\langle \mathbf{x} \circ \mathbf{y}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{y} \circ \mathbf{z} \rangle$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{J}$. Hence, the norm is given by the inner product $\langle \cdot, \cdot \rangle$ as

$$||\mathbf{x}|| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = (\lambda_1^2 + \cdots + \lambda_r^2)^{1/2}. \tag{5}$$

Then, for a given linear operator $\mathcal{B}$ defined on $\mathcal{J}$, we denote by $||\mathcal{B}||_2$ the operator norm induced by $|| \cdot ||$.

Given the fact that "$\circ$" is a bilinear map, it follows that the linear map $L(\mathbf{x}) : \mathcal{J} \to \mathcal{J}$ satisfying $L(\mathbf{x})\mathbf{y} = \mathbf{x} \circ \mathbf{y}$ for any $\mathbf{x} \in \mathcal{J}$. Further, it is easily verified that by the definition of "$\circ$" we also have $L(\mathbf{x})L(\mathbf{x}^2) = L(\mathbf{x}^2)L(\mathbf{x})$ and $\langle L(\mathbf{x})\mathbf{z}, \mathbf{y}\rangle = \langle \mathbf{z}, L(\mathbf{x})\mathbf{y}\rangle$. Additionally, we denote by $\mathbf{Q}(\mathbf{x})$ the quadratic representation associated with $\mathbf{x}$, given by:

$$\mathbf{Q}(\mathbf{x}) := 2L^2(\mathbf{x}) - L(\mathbf{x}^2).$$

Note that by its very definition, for $\mathbf{Q}(\cdot)$ we have $\langle \mathbf{Q}(\mathbf{x})\mathbf{y}, \mathbf{z}\rangle = \langle \mathbf{y}, \mathbf{Q}(\mathbf{x})\mathbf{z}\rangle$. Therefore, we can also observe that $L(\mathbf{x})$ and $\mathbf{Q}(\mathbf{x})$ are both self-adjoint linear operators on $\mathcal{J}$. Further, we have the following result from [25].

Lemma 1. *[25, Lemma 12] Given the spectral decomposition $\mathbf{x} = \lambda_1\mathbf{c}_1 + \cdots \lambda_r\mathbf{c}_r$ in a rank r Euclidean Jordan algebra, we have that:*

1. *The operators $L(\mathbf{x})$ and $\mathbf{Q}(\mathbf{x})$ share a common system of eigenvalues*
2. *The eigenvalues of $L(\mathbf{x})$ are given by $\{(\lambda_i + \lambda_j)/2 : 1 \le i, j \le r\}$. Hence, $||L(\mathbf{x})||_2 = ||\mathbf{x}||_2$. Also, $\mathbf{x} \succeq 0$ $(\succ 0)$ if and only if $L(\mathbf{x})$ is positive semidefinite (positive definite).*
3. *The eigenvalues of $\mathbf{Q}(\mathbf{x})$ are given by $\{\lambda_i\lambda_j : 1 \le i, j \le r\}$. Hence, $||\mathbf{Q}(\mathbf{x})||_2 = ||\mathbf{x}||_2^2$.*
4. $||\mathbf{x} \circ \mathbf{y}|| \le ||\mathbf{x}|| ||\mathbf{y}||$.

The following result from [18] details useful identities that will be utilized later in the paper.

Lemma 2. *[18, Lemma 2] The quadratic representation $\mathbf{Q}$ satisfies the following properties:*

1. $\mathbf{Q}(\mathbf{Q}(\mathbf{x})\mathbf{y}) = \mathbf{Q}(\mathbf{x})\mathbf{Q}(\mathbf{y})\mathbf{Q}(\mathbf{x})$ *[6, Proposition II.3.3]*
2. $\mathbf{Q}(\mathbf{x}^{-1/2})\mathbf{x} = \mathbf{e}$, $\mathbf{Q}(\mathbf{x})^{-1} = \mathbf{Q}(\mathbf{x}^{-1})$, $\mathbf{Q}(\mathbf{x})\mathbf{x}^{-1} = \mathbf{x}$ *[6, Proposition II.3.1]*
3. $\mathrm{tr}\,(\mathbf{Q}(\mathbf{x})\mathbf{y}) = \langle \mathbf{x}^2, \mathbf{y}\rangle$
4. $\det(\mathbf{Q}(\mathbf{x})\mathbf{y}) = \det(\mathbf{x}^2)\det(\mathbf{y})$ *[6, Proposition III.4.2]*

As a consequence of item 1 of Lemma 2, we have

$$\mathbf{Q}(\mathbf{x}^2) = \mathbf{Q}(\mathbf{x})^2, \quad \mathbf{Q}(\mathbf{x}^{1/2}) = \mathbf{Q}(\mathbf{x})^{1/2} \text{ if } \mathbf{x} \succeq 0.$$

Recall that one for an Euclidean Jordan algebra $\mathcal{J}$, we define its cone of squares to be the set

$$\mathcal{K} := \{\mathbf{x}^2 \mid \mathbf{x} \in \mathcal{J}\}$$

and we have the following result.

Theorem 2. *[6, Theorem III.2.1, Theorem III.3.1] A cone is symmetric if and only if it is the cone of squares of an Euclidean Jordan algebra. Furthermore, $\mathcal{K} = \{\mathbf{x} \in \mathcal{J} \ : \ xs \succeq 0\}$ and $\mathrm{int}(\mathcal{K}) = \{\mathbf{x} \in \mathcal{J} \ : \ x \succ 0\}$.*

Additionally we have the following result from [25] which will be applied frequently in the rest of the paper.

Lemma 3. *[25, Proposition 21, Lemma 30] Let $\mathbf{x}, \mathbf{z}, \mathbf{p} \in \mathrm{int}(\mathcal{K})$. Define $\hat{\mathbf{x}} = \mathbf{Q}(\mathbf{p})\mathbf{x}$ and $\hat{\mathbf{z}} = \mathbf{Q}(\mathbf{p}^{-1})\mathbf{z}$, then*

1. *$\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}$ and $\mathbf{Q}(\mathbf{z}^{1/2})\mathbf{x}$ have the same spectrum*
2. *$\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}$ and $\mathbf{Q}(\hat{\mathbf{x}}^{1/2})\hat{\mathbf{z}}$ have the same spectrum*
3. *$\lambda_{\max}(\mathbf{x} \circ \mathbf{z}) \ge \lambda_{\max}(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z})$ with equality holding if $L(\mathbf{x})$, $L(\mathbf{z})$ commute*
4. *$\lambda_{\max}(\mathbf{x} \circ \mathbf{z}) \le \lambda_{\max}(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z})$ with equality holding if $L(\mathbf{x})$, $L(\mathbf{z})$ commute; see also [27, Thm. 4]*

Before concluding this section, in line with [18] we provide a brief description of the three symmetric cones studied in this paper, using the methodology of Jordan frames.

Semidefinite cone. Let $\mathcal{J} = \mathcal{S}^n$, where $\mathcal{S}^n \subseteq \mathbb{R}^{n\times n}$ denotes the cone of $n \times n$ symmetric matrices. If we define $\circ$ to be the operator

$$X \circ Y = \frac{1}{2}(XY + YX),$$

it follows that $(\mathcal{S}^n, \circ)$ is an Euclidean Jordan algebra. Note that in this case, the unit element is the $n \times n$ identity matrix I and the corresponding cone of squares $\mathcal{S}^n_+$ is the cone of positive semidefinite matrices in $\mathcal{S}^n$. Then, for any $X \in \mathcal{S}^n$, X has the eigenvalue decomposition

$$X = \lambda_1 \mathbf{q}_1 \mathbf{q}_1^\top + \cdots + \lambda_n \mathbf{q}_n \mathbf{q}_n^\top$$

where the set $\{\mathbf{q}_1\mathbf{q}_1^\top, \dots, \mathbf{q}_n\mathbf{q}_n^\top\}$ forms a Jordan frame. Note that in this instance,

$$\det(X) = \lambda_1 \cdots \lambda_n$$
$$\operatorname{tr}(X) = \lambda_1 + \cdots + \lambda_n$$

and thus we have

$$\langle X, Y\rangle = \operatorname{tr}(X \circ Y) = \operatorname{tr}(XY).$$

Additionally, from [18], we have

$$L(X) = X \otimes I, \quad \mathbf{Q}(X) = X \otimes X \tag{6}$$

where $G \otimes H$ denotes the symmetric Kronecker product of two $n \times n$ matrices G and H given by

$$(G \otimes H)(M) := \frac{1}{2}(GMH^\top + HMG^\top)\ \forall M \in \mathcal{S}^n. \tag{7}$$

Second-order Cone. Let $\mathcal{J} = \mathbb{R}^n$, where for each vector $\mathbf{x} \in \mathbb{R}^n$ we write $\mathbf{x} = (x_0, \bar{\mathbf{x}})$ where $x_0 \in \mathbb{R}$ denotes the first element of $\mathbf{x}$ and $\overline{xb} \in \mathbb{R}^{n-1}$ is the subvector containing the remaining $n-1$ elements. Following [18], define $\circ$ to be the operator

$$\mathbf{x} \circ \mathbf{y} = (\mathbf{x}^\top \mathbf{y}; x_0\bar{\mathbf{y}} + y_0\bar{\mathbf{x}})$$

and note that the unit element in this case is given by $\mathbf{e} = (1; \mathbf{0}) \in \mathbb{R}^n$. Further, the cone of squares is defined as

$$\mathcal{Q}^n = \{\mathbf{x} \in \mathbb{R}^n \ : \ ||\bar{\mathbf{x}}|| \leq x_0\},$$

where $\mathcal{Q}^n$ is a second-order cone. Now, for any $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x}$ has the eigenvalue decomposition given by

$$\mathbf{x} = (x_0 + ||\bar{x}||)\mathbf{c}_1 + (x_0 - ||\bar{x}||)\mathbf{c}_2,$$

where

$$\mathbf{c}_1 = \begin{cases} \left(\frac{1}{2}; \frac{\bar{\mathbf{x}}}{||\bar{\mathbf{x}}||}\right) & \bar{\mathbf{x}} \neq 0 \\ \left(\frac{1}{2}; \frac{1}{2}; \mathbf{0}\right) & \bar{\mathbf{x}} = 0 \end{cases}$$

and $\mathbf{c}_2 = \mathbf{e} - \mathbf{c}_1$. Therefore, $\lambda_{1,2} = x_0 \pm ||\bar{\mathbf{x}}||$ and

$$\det(\mathbf{x}) = 2x_0$$
$$\operatorname{tr}(\mathbf{x}) = x_0^2 - ||\bar{\mathbf{x}}||^2.$$

Then, for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$:

$$\langle \mathbf{x}, \mathbf{y}\rangle := \operatorname{tr}(\mathbf{x} \circ \mathbf{y}) = 2\mathbf{x}^\top \mathbf{y}.$$

Further, we have

$$L(\mathbf{x}) = \begin{bmatrix} x_0 & \bar{\mathbf{x}}^\top \\ \bar{\mathbf{x}} & x_0 I \end{bmatrix} \tag{8}$$

$$\mathbf{Q}(\mathbf{x}) = 2L^2(\mathbf{x}) - L(\mathbf{x}^2) = 2\mathbf{x}\mathbf{x}^\top - \det(\mathbf{x})R, \tag{9}$$

where R is a diagonal matrix with $R_{1,1} = 1$ and $R_{i,i} = -1$ for $i = 2, \ldots, n$. It follows that if $\det(\mathbf{x}) \neq 0$, then

$$\mathbf{x}^{-1} = \lambda_1^{-1}\mathbf{c}_1 + \lambda_2^{-1}\mathbf{c}_2 = \frac{1}{\det(\mathbf{x})}R\mathbf{x} \tag{10}$$

$$\mathbf{Q}(\mathbf{x}^{-1}) = \frac{1}{\det(\mathbf{x})^2}R\mathbf{Q}(\mathbf{x})R. \tag{11}$$

Nonnegative orthants. Let $\mathcal{J} = \mathbb{R}^n$, i.e., the n-dimensioanl real vector space and define $\mathbf{x} \circ \mathbf{y} = (x_i y_i)_{i=1}^n$. In this case, the unit element is the n-dimensioanl all-ones vector $\mathbf{e} = (1, \ldots, 1) \in \mathbb{R}^n$, and the cone of squares is $\mathbb{R}_+^n = \{\mathbf{x} \,:\, x_i \geq 0, \ \forall i = 1, \ldots, n\}$. Additionally, each $\mathbf{x} \in \mathbb{R}^n$ has the eigenvalue decomposition

$$\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n$$

where $\mathbf{e}_i$ is the unit vector with ith element equal to 1 and all elements being 0. Hence, it follows

$$\det(\mathbf{x}) = x_1 + \cdots + x_n$$
$$\operatorname{tr}(\mathbf{x}) = x_1 \cdots x_n,$$

and

$$\langle \mathbf{x}, \mathbf{y} \rangle = \operatorname{tr}(\mathbf{x} \circ \mathbf{y}) = \mathbf{x}^\top \mathbf{y}.$$

Finally, note that here

$$L(\mathbf{x}) = \operatorname{diag}(\mathbf{x}), \ \mathbf{Q}(\mathbf{x}) = \operatorname{diag}(\mathbf{x}^2), \ \mathbf{Q}(\mathbf{x}^{-1}) = \operatorname{diag}(\mathbf{x}^{-2}).$$

3 Quantum Data Structures and Quantum Linear Algebra

The II-QIPM makes extensive use of linear algebra subroutines; notably, matrix multiplication, matrix powers, and matrix-vector products. We perform all these operations in the framework of block encodings. Before giving formal definitions and a summary of useful results from the literature, we give an informal introduction.

3.1 Basic concepts on block-encoded matrices

The II-QIPM described in this paper makes extensive use of linear algebra subroutines; notably, matrix multiplication, matrix powers, and matrix-vector products. We perform all these operations in the framework of block encodings. Before giving formal definitions and an overview of key results from the literature, we give an informal introduction to convey intuition.

To get a basic understanding of how to perform matrix-vector and matrix-matrix multiplication using this framework, suppose we want to multiply A by some vector b. We assume that b is encoded in the quantum state $|b\rangle$, which we want to update as follows:

$$|b\rangle \rightarrow \frac{A\,|b\rangle}{\|A\,|b\rangle\,\|}.$$

A block encoding U of A is a unitary such that:

$$U = \begin{pmatrix} \frac{A}{\alpha} & \cdot \\ \cdot & \cdot \end{pmatrix},$$

where α is a normalization factor. In particular, if A is an s-qubit operator, an (α, a, δ)-block encoding of A uses a extra qubits and implements A up to total error δ. Hence, we have

$$\begin{aligned} U|b\rangle|0\rangle^{\otimes a} &\approx \begin{pmatrix} \frac{A}{\alpha} & \cdot \\ \cdot & \cdot \end{pmatrix} \begin{pmatrix} |b\rangle \\ 0 \end{pmatrix} \\ &= \frac{1}{\alpha} A|b\rangle|0\rangle^{\otimes a} + |\cdot\rangle, \end{aligned}$$

and performing $\approx \frac{\alpha}{\|A|b\rangle\|}$ rounds of amplitude amplification yields $\frac{A|b\rangle}{\|A|b\rangle\|}$ with high probability, see e.g., [5].

For matrix multiplication, let U be an (α, a, δ)-block-encoding of an s-qubit operator A, and V be a (β, b, ξ)-block-encoding of an s-qubit operator B. Then we have

$$UV = \begin{pmatrix} \frac{B}{\beta} & \cdot \\ \cdot & \cdot \end{pmatrix} \begin{pmatrix} \frac{A}{\alpha} & \cdot \\ \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \frac{AB}{\alpha\beta} & \cdot \\ \cdot & \cdot \end{pmatrix},$$

which yields an $(\alpha\beta, a+b, \alpha\xi + \beta\delta)$-block-encoding of AB.

For matrix inversion, let U be a (α, a, δ)-block encoding of A which can be implemented with complexity T_U. Then, Chakraborty et al. [5] prove that we can implement a block encoding V of the inverse of A:

$$V = \begin{pmatrix} \frac{A^{-1}}{2\kappa} & \cdot \\ \cdot & \cdot \end{pmatrix}$$

Hence, given A as a block encoding and $|b\rangle$, we can solve the linear system

$$Ax = b$$

by outputting the state

$$\frac{A^{-1}|b\rangle}{\|A^{-1}|b\rangle\|},$$

computed as :

$$V|b\rangle|0\rangle^{\otimes a} = \frac{1}{2\kappa} A^{-1}|b\rangle|0\rangle^{\otimes a} + |\cdot\rangle.$$

To construct a block encoding of the matrices used by the II-QIPM, e.g., the matrices $A^{(1)}, \ldots, A^{(k)}$, we use the following construction, see [5] for details. Suppose we want to construct a matrix A and we have a way of constructing the quantum states $|\psi_i\rangle = \sum_j \frac{A_{ij}}{\|A_i\|} |i, j\rangle$, where A_i is the i-th row of A, and $|\phi_i\rangle = \sum_i \frac{\|A_i\|}{\|A\|_F} |i, j\rangle$. Then we construct:

$$U_R^\dagger U_L = \begin{pmatrix} - & \langle\psi_1| & - & \cdot \\ & \vdots & & \\ - & \langle\psi_n| & - & \cdot \\ & \cdot & & \cdot \end{pmatrix} \begin{pmatrix} | & & | & \\ |\phi_1\rangle & \cdots & |\phi_n\rangle & \cdot \\ | & & | & \\ \cdot & & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} [\langle\psi_i|\phi_j\rangle]_{i,j\in[n]} & \cdot \\ \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \frac{A}{\|A\|_F} & \cdot \\ \cdot & \cdot \end{pmatrix},$$

where we used the fact that

$$\langle\psi_i|\phi_j\rangle = \frac{A_{ij}}{\|A\|_F}.$$

Thus, $U_R^\dagger U_L$ is a block encoding of A with normalization factor $\|A\|_F$. For the above construction to work, we must have a procedure to prepare U_R, U_L. Note that these unitaries are easy to obtain starting from controlled operations to prepare the states $|\psi_i\rangle, |\phi_i\rangle$, i.e., operations of the form $|i\rangle|0\rangle \to |i\rangle|\psi_i\rangle$, $|j\rangle|0\rangle \to |j\rangle|\phi_j\rangle$, and these controlled operations can in turn be constructed with a procedure similar to the state preparation algorithm of Grover and Rudolph [**?**] for efficiently integrable distributions. This can be made more efficient if we allow pre-processing to create certain data structures that can be stored in quantum-accessible storage, i.e., QRAM. A quantum RAM (QRAM) is a form of storage that allows for querying a superposition of addresses. Given a QRAM that stores the classical vector $v_j \in \mathbb{R}^{2^q}$, and a quantum state $\sum_{j=0}^{2^q-1} \alpha_j |j\rangle$, the QRAM asumption is that the following mapping can be performed in time $O(q)$, i.e., polylogarithmic in the size of the vector:

$$\sum_{j=0}^{2^q-1} \alpha_j |j\rangle \otimes |0\rangle \to \sum_{j=0}^{2^q-1} (\alpha_j |j\rangle \otimes |v_j\rangle).$$

Throughout this paper, we assume that we have access to a QRAM that is large enough to store all input matrices, i.e., $O(mn^2)$. For more details about the QRAM data structure to prepare the amplitude encoding of a vector, or the matrices U_R, U_L discussed above, we refer the reader to [14, 5].

3.2 Useful results on block-encoded matrices

We now provide formal definitions for the concepts informally discussed in the previous section, as well as other results that are used in the remainder of this paper. The material in this section is mostly taken from [5, 8], which provide improvements over the framework discussed in [12, 14].

Definition 1 (Block encoding)**.** *Let $A \in \mathbb{C}^{2^w \times 2^w}$ be a w-qubit operator. Then, an $(w + a)$-qubit unitary U is an (α, a, ξ)-block encoding of A if $U = \begin{pmatrix} \widetilde{A} & \cdot \\ \cdot & \cdot \end{pmatrix}$, such that*

$$\|\alpha\widetilde{A} - A\| \le \xi$$

An (α, a, ξ)-block encoding of A is said to be efficient if it can be implemented in time $T_U = O(\mathrm{poly}(w))$.

Note that this only possible for matrices with $\|A\|_2 \le 1$, so we allow A to be scaled by some constant:

$$U \approx \begin{pmatrix} \frac{A}{\alpha} & \cdot \\ \cdot & \cdot \end{pmatrix},$$

yielding

$$\|A - \alpha(\langle 0|^{\otimes a} \otimes I_{2^w})U(|0\rangle^{\otimes a} \otimes I_{2^w})\| \le \xi.$$

The next proposition formalizes an idea discussed in the previous section. We do not provide details on the necessary data structure, referring the reader to [5] for an extensive discussion on this topic.

Proposition 1 (Lemma 50 in [8])**.** *Let $A \in \mathbb{C}^{m\times m}$ with $m = 2^w$ and $\xi > 0$.*

(i) Fix $q \in [0, 2]$. If $A^{(q)}$ and $(A^{(2-q)})^\dagger$ are both stored in QRAM data structures, then there exist unitaries U_R and U_L that can be implemented in time $O(\mathrm{poly}(w \log \frac{1}{\xi}))$ and such that $U_R^\dagger U_L$ is a $(\mu_q(A), w+2, \xi)$-block-encoding of A.

(ii) If A is stored in a QRAM data structure, then there exist unitaries U_R and U_L that can be implemented in time $O(\mathrm{poly}(w \log \frac{1}{\xi}))$ and such that $U_R^\dagger U_L$ is an $(\|A\|_F, w + 2, \xi)$-block-encoding of A.

Proposition 2 (Lemma 52 in [8])**.** *(Linear combination of block-encoded matrices, with weights given by the coefficients of a basis state) Let $A = \sum_{j=1}^m y_j A^j$ be an s-qubit operator, where A^j are matrices. Suppose P_L, P_R is a (β, b, ξ_1)-state-preparation pair for y, $W = \sum_{j=0}^{m-1} |j\rangle\langle j| \otimes U_j + ((I - \sum_{j=0}^{m-1} |j\rangle\langle j|) \otimes I_a \otimes I_s)$ is an $(s + a + b)$-qubit unitary with the property that U_j is an (α, a, ξ_2)-block-encoding of A^j. Then we can implement a $(\alpha\beta, a + b, \alpha\xi_1 + \alpha\beta\xi_2)$-block-encoding of A with a single use of W, P_R and $P_L^\dagger$.*

The following two propositions are critical to the efficiency of the II-QIPM. They state that one can construct a block encoding as a product of two block encoded matrices, with overhead that is merely polylogarithmic in the size of the matrices. The difference between the two propositions is that in the second one, the normalization factor of the block encoding of the product is fixed, rather than depending on the input.

Proposition 3 (Lemma 4 [5])**.** *(Product of block-encoded matrices) If U is an (α, a, δ)-block-encoding of an s-qubit operator A, and V is a (β, b, ξ)-block-encoding of an s-qubit operator B, then $(I_b \otimes U)(I_a \otimes V)$ is an $(\alpha\beta, a+b, \alpha\xi + \beta\delta)$-block-encoding of AB.*

Proposition 4 (Lemma 5 in [5])**.** *(Product of preamplified block-encoded matrices) Given an (α, a, δ)-block-encoding U of an s-qubit operator A, and a (β, b, ξ)-block-encoding V of an s-qubit operator B, with $\alpha \geq 1, \beta \geq 1$, then we can implement a $(2, a+b+2, \sqrt{2}(\delta + \xi + \gamma)$-block-encoding of AB in time $O((\alpha(T_U + a) + \beta(T_V + b)) \log \frac{1}{\gamma})$, where T_U and T_V are the implementation times for U and V, respectively.*

Additionally, the following two propositions indicate that if one has a block encoded matrix, one can implement a block encoding of powers of that matrix – most notably, we can implement the inverse matrix.

Proposition 5 (Lemma 9 in [5])**.** *(Implementing negative powers of Hermitian matrices) Let $p \in (0, \infty)$, $\kappa \geq 2$ and H a Hermitian matrix such that $I/\kappa \preceq H \preceq I$. Suppose that*

$$\delta = o\left(\frac{\xi}{\kappa^{1+p}(1+p)\log^3 \frac{\kappa^{1+p}}{\xi}}\right)$$

and U is an (α, a, δ)-block-encoding of H, that can be implemented using T_U elementary gates. Then, for any ξ, we can implement a unitary $\tilde{U}$ which is a $(2\kappa^p, a + O(\log(\kappa^{1+p} \log 1/\xi), \xi)$-block-encoding of H^{-p} in cost

$$O\left(\alpha\kappa(a + T_U)(1+p)\log^2\left(\frac{\kappa^{1+p}}{\xi}\right)\right).$$

Proposition 6 (Lemma 10 in [5])**.** *(Implementing positive powers of Hermitian matrices) Let $p \in (0, 1]$, $\kappa \geq 2$ and H a Hermitian matrix such that $I/\kappa \preceq H \preceq I$. Suppose that*

$$\delta = o\left(\frac{\xi}{\kappa \log^3 \frac{\kappa}{\xi}}\right)$$

and U is an (α, a, δ)-block-encoding of H, that can be implemented using T_U elementary gates. Then, for any ξ, we can implement a unitary $\tilde{U}$ which is a $(2, a + O(\log\log(1/\xi)), \xi)$-block-encoding of H^p in cost

$$O\left(\alpha\kappa(a + T_U)\log^2\left(\frac{\kappa}{\xi}\right)\right).$$

Theorem 3 (Theorem 30 in [5])**.** *(Solution of linear system) Let $p \in (0, \infty)$, $\kappa \geq 2$ and H a Hermitian matrix such that its nonzero eigenvalues lie in $[-1, -1/\kappa] \cup [1/\kappa, 1]$. Suppose that*

$$\delta = o\left(\frac{\xi}{\kappa^2 \log^3 \frac{\kappa^2}{\xi}}\right)$$

and U is an (α, a, δ)-block-encoding of H, that can be implemented using T_U elementary gates. Suppose further that we can prepare a state $|b\rangle$ that is spanned by H using T_b elementary gates. Then, for any ξ, we can output a state that is ξ-close to $H^{-1}|b\rangle / \|H^{-1}b\|$ at cost

$$O\left(\kappa\left(\alpha(a + T_U)\log^2\left(\frac{\kappa}{\xi}\right) + T_b\right)\log\kappa\right).$$

Proposition 7 (Corollary 32 in [5])**.** *(Norm estimation) Let $p \in (0, \infty)$, $\kappa \geq 2$ and H a Hermitian matrix such that its nonzero eigenvalues lie in $[-1, -1/\kappa] \cup [1/\kappa, 1]$. Suppose that*

$$\delta = o\left(\frac{\xi}{\kappa^2 \log^3 \frac{\kappa^2}{\xi}}\right)$$

and U is an (α, a, δ)-block-encoding of H, that can be implemented using T_U elementary gates. Suppose further that we can prepare a state $|b\rangle$ that is spanned by H using T_b elementary gates. Then we can output $\tilde{e}$ such that

$$(1-\xi)\|H^{-1}|b\rangle\| \leq \tilde{e} \leq (1+\xi)\|H^{-1}|b\rangle\|$$

at cost

$$O\left(\frac{\kappa}{\xi}\left(\alpha(a+T_U)\log^2\left(\frac{\kappa}{\xi}\right)+T_b\right)\log^3\kappa \log\frac{\log\kappa}{\delta}\right).$$

Proposition 8. *Let*

$$A = \begin{pmatrix} M_{11} & \dots & M_{1c} \\ \vdots & \ddots & \vdots \\ M_{r1} & \dots & M_{rc} \end{pmatrix} \in \mathbb{R}^{n\times n},$$

where each M_{ij} is a matrix, of appropriate dimension, that is stored in a QRAM data structure, or is a tensor product of two matrices stored in a QRAM data structure. Suppose further the norms of each row/column are classically known. Then we can construct a $(\|A\|_F, O(\log n), \xi)$-block-encoding of A in time $O(\text{poly}(\log n, \log\frac{1}{\xi}))$.

Proof. Let $M^0_{ij} \in \mathbb{R}^{n\times n}$ denote the matrix in which M_{ij} appears in the same entry as in A, but that all other entries of M^0_{ij} are 0. Then, A can be written as a linear combination of the n^2 M^0_{ij} matrices as follows:

$$A = \sum_{i=1}^{n}\sum_{j=1}^{n} M^0_{ij}.$$

Then, similarly, suppose U_A is a block encoding of A. Letting U^0_{ij} denote a block encoding of $M^0_{ij} \in \mathbb{R}^{n\times n}$, applying Proposition 2, in time $O(\text{poly}(\log n, \log\frac{1}{\xi}))$ we can construct U_A as a linear combination of each U^0_{ij}:

$$U_A = \sum_{i=1}^{n}\sum_{j=1}^{n} U^0_{ij}.$$

□

3.3 Tomography

In each iteration of our QIPM, we solve a linear system of equations known as the Newton linear system in order to update our solutions to the optimization problem at hand. The solutions to the Newton linear system, $\Delta\mathbf{x}$, Δy and $\Delta\mathbf{z}$, are obtained using quantum linear system solvers, and hence are quantum states. Thus, in order to be able to classically update our solutions, we require a procedure to map the quantum states $\Delta\mathbf{x}$, Δy and $\Delta\mathbf{z}$ to a classical solution $(\Delta\mathbf{x}, \Delta y, \Delta\mathbf{z})$.

For this task, we can make use of the efficient vector state tomography algorithm from [13]. Note that this tomography algorithm is simpler than those found in O'Donnell and Wright [22] the alternative approach of using compressed sensing [13]. This can be attributed to the fact that Kerenidis and Prakash [13] assume that we can apply the unitary that prepares the state, at its controlled version.

Algorithm 1 Vector state tomography algorithm [13]

Input: Access to a unitary U such that $U|0\rangle = |\mathbf{x}\rangle = \sum_{i\in[m]} x_i|i\rangle$ and to its controlled version

1. **Amplitude estimation**
   (a) Measure $N = \frac{36m\ln m}{\delta^2}$ copies of $|\mathbf{x}\rangle$ in the standard basis and obtain estimates $p_i = \frac{n_i}{N}$ where n_i is the number of times outcome i is observed.
   (b) Store $\sqrt{p_i}$, $i \in [m]$ in QRAM data structure so that $|p\rangle = \sum_{i\in[m]} \sqrt{p_i}|i\rangle$ can be prepared efficiently.
2. **Sign estimation**
   (a) Create $N = \frac{36m\ln m}{\delta^2}$ copies of the state $\frac{1}{\sqrt{2}}|0\rangle \sum_{i\in[m]} x_i|i\rangle + \frac{1}{\sqrt{2}}|1\rangle \sum_{i\in[m]} \sqrt{p_i}|i\rangle$ using a control qubit.
   (b) Apply a Hadamard gate on the first qubit of each copy of the state to obtain $\frac{1}{2}\sum_{i\in[m]}[(x_i + \sqrt{p_i}|0,i\rangle + (x_i - \sqrt{p_i})|1,i\rangle]$.
   (c) Measure each copy in the standard basis and maintain counts $n(b,i)$ of the number of times outcome $|b,i\rangle$ is observed for $b \in \{0,1\}$.
   (d) Set $\sigma_i = 1$ if $n(0,i) > 0.4p_iN$ and -1 otherwise.
3. Output the unit vector $\tilde{\mathbf{x}}$ with $\tilde{\mathbf{x}}_i = \sigma_i\sqrt{p_i}$.

The following result from [13] certifies the correctness of Algorithm 1.

Theorem 4. *Algorithm 1 produces an estimate $\tilde{\mathbf{x}} \in \mathbb{R}^m$ with $||\tilde{\mathbf{x}}||_2 = 1$ such that $||\tilde{\mathbf{x}} - \mathbf{x}||_2 \le \sqrt{7}\delta$ with probability at least $(1 - \frac{1}{m^{0.83}})$.*

We can summarize the role the tomography algorithm plays in QIPMs as follows. Solving the Newton linear system will output the quantum state $\Delta\mathbf{x} \circ \Delta y \circ \Delta\mathbf{z}$, and we wish to recover a classical estimate of this state $\overline{\Delta\mathbf{x}} \circ \overline{\Delta y} \circ \overline{\Delta\mathbf{z}}$ such that

$$||\Delta\mathbf{x} \circ \Delta y \circ \Delta\mathbf{z} - \overline{\Delta\mathbf{x}} \circ \overline{\Delta y} \circ \overline{\Delta\mathbf{z}}|| \le \delta.$$

To accomplish this, we create a large number of samples of our state $\Delta\mathbf{x} \circ \Delta y \circ \Delta\mathbf{z}$, and then estimate the absolute value of the entries of $\Delta\mathbf{x} \circ \Delta y \circ \Delta\mathbf{z}$. Subsequently, we measure each copy of our state, and record the number of times each outcome is observed such that we can estimate the sign associated with each element. Finally, our estimate of the classical state $\overline{\Delta\mathbf{x}} \circ \overline{\Delta y} \circ \overline{\Delta\mathbf{z}}$ is used to update the current solution in each iterate of the QIPM:

$$\mathbf{x}' = \mathbf{x} + \overline{\Delta\mathbf{x}}$$
$$y' = y + \overline{\Delta y}$$
$$\mathbf{z}' = \mathbf{z} + \overline{\Delta\mathbf{z}}.$$

4 The Classical Inexact-Infeasible Interior Point Method

In this section, we provide a detailed overview of the Classical II-IPM, and important theoretical results from the literature.

4.1 Primal and Dual QCOPs and the Central Path

Letting $\nu > 0$, perturbed Karush-Kuhn-Tucker (KKT) optimality conditions of (1) and (2) are given by

$$\begin{pmatrix} -\nabla f(\mathbf{x}) + \mathcal{A}^\top y + \mathbf{z} \\ \mathcal{A}(\mathbf{x}) - b \\ \mathbf{x} \circ \mathbf{z} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \nu\mathbf{e} \end{pmatrix}, \quad \mathbf{x}, \mathbf{z} \in \mathcal{K}. \tag{12}$$

Consider the last equation of (12), which is a relaxation of the complementarity conditions

$$\mathbf{x} \circ \mathbf{z} = 0, \;\; \mathbf{x}, \mathbf{z} \in \mathcal{K}.$$

Just like the case of SDO, linearizing this equation may not lead to a solution which is an element of $\mathcal{J}$, and thus we must first symmetrize the equation before linearizing. Therefore, we replace the last equation of (12) with

$$H_{\mathbf{p}}(\mathbf{x}, \mathbf{z}) = \mathbf{Q}(\mathbf{p})\mathbf{x} \circ \mathbf{Q}(\mathbf{p}^{-1})\mathbf{z} = \nu\mathbf{e}. \tag{13}$$

As shown by [24, Lemma 28], for $\mathbf{x}, \mathbf{z}, \mathbf{p} \in \mathcal{J}$, if $\mathbf{x}, \mathbf{z} \succ 0$ and $\mathbf{p}$ is invertible, then $H_p(\mathbf{x}, \mathbf{z}) = \nu\mathbf{e}$ if and only if $\mathbf{x} \circ \mathbf{z} = \nu\mathbf{e}$.

Following [18], for $\mathbf{x}, \mathbf{z} \succ 0$, we assume $\mathbf{p}$ is an element of a commutative class defined by

$$\mathcal{C}(\mathbf{x}, \mathbf{z}) = \{\mathbf{p} \in \text{int}(\mathcal{K}) \mid L(\mathbf{Q}(\mathbf{p})\mathbf{x}), L(\mathbf{Q}(\mathbf{p}^{-1})\mathbf{z}) \text{ commute}\}.$$

Defining

$$\begin{aligned} \hat{\mathbf{x}} &= \mathbf{Q}(\mathbf{p})\mathbf{x}, \text{ and} \\ \hat{\mathbf{z}} &= \mathbf{Q}(\mathbf{p})\mathbf{z}, \end{aligned}$$

then for any $\mathbf{p} \in \mathcal{C}(\mathbf{x}, \mathbf{z})$ it follows

$$H_{\mathbf{p}}(\mathbf{x}, \mathbf{z}) = \hat{\mathbf{x}} \circ \hat{\mathbf{z}} = \mathbf{Q}(\hat{\mathbf{x}}^{1/2})\hat{\mathbf{z}}. \tag{14}$$

Some search directions which are members of $C(\mathbf{x}, \mathbf{z})$ include the Helmberg-Kojima-Monteiro (HKM) direction $\mathbf{p} = \mathbf{x}^{-1/2}$ [10, 17, 19] and the Nesterov-Todd (NT) direction [28] $\mathbf{p} = \mathbf{w}^{-1/2}$ where $\mathbf{w}$ is the Nesterov-Todd scaling element. Note that for the Nesterov-Todd direction, $\mathbf{p}$ can be explicitly defined as

$$\mathbf{p} = \left[\mathbf{Q}(\mathbf{x}^{1/2})\left(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}\right)^{-1/2}\right]^{-1/2} = \left[\mathbf{Q}(\mathbf{z}^{-1/2})\left(\mathbf{Q}(\mathbf{z}^{1/2})\mathbf{x}\right)^{1/2}\right]^{-1/2} \tag{15}$$

and note that $\mathbf{Q}(\mathbf{w})\mathbf{z} = \mathbf{x}$. Additionally, as noted in [18], it can be easily verified that

$$\begin{aligned} \mathbf{Q}(\mathbf{w})\mathbf{z} = \mathbf{Q}(p^{-2})\mathbf{z} &= \mathbf{Q}(\mathbf{Q}(\mathbf{x}^{1/2})(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z})^{-1/2})\mathbf{z} \\ &= \mathbf{Q}(\mathbf{x}^{1/2})\mathbf{Q}((\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z})^{-1/2})(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}) \\ &= \mathbf{Q}(x^{1/2})\mathbf{e} \\ &= \mathbf{x}, \end{aligned}$$

where the last two inequalities result from Lemma 2. Additionally, when we employ the Nesterov-Todd direction, it follows

$$\mathbf{Q}(\mathbf{p}^{-1})\mathbf{z} = \mathbf{Q}(\mathbf{p})\mathbf{Q}(\mathbf{w}) = \mathbf{Q}(\mathbf{p})\mathbf{x}. \tag{16}$$

As in [18], in this work we only consider p to be the Nesterov-Todd scaling element. Note that this choice has many practical advantages. First and foremost, the NT scaling element simplifies the complexity analysis and provides the best iteration complexity. Further, as long as the optimization problem at hand has a solution, choosing the NT direction guarantees we converge to the optimal solution. This is not the case for all search directions, for example the Alizedah-Haeberly-Overton (AHO) direction can only certify local convergence.

Let $L = ||\mathcal{H}||_2$ be a Lipschitz constant associated with $\nabla f(\mathbf{x})$ from (1) such that

$$||\nabla f(\mathbf{x}) - \nabla f(\mathbf{y})|| = ||\mathcal{H}(\mathbf{x}) - \mathcal{H}(\mathbf{y}) \leq L||\mathbf{x} - \mathbf{y}||. \tag{17}$$

Next, consider an initial point $(\mathbf{x}_0, y_0, \mathbf{z}_0)$ such that for a given constant $\rho > 0$ we have

$$\mathbf{x}_0 = \mathbf{z}_0 = \rho \mathbf{e}. \tag{18}$$

Then, for $\gamma_p, \gamma_d > 0$ with $\gamma_p \leq \gamma_d$ such that $\gamma_d + L\gamma_p \in (0,1)$, we choose ρ sufficiently large in order to guarantee that the following conditions are satisfied:

$$(1-\gamma_p)\mathbf{x}_0 \succ \mathbf{x}_* \succeq 0, \quad (1-(\gamma_d + L\gamma_p))\mathbf{z}_0 \succ \mathbf{z}_* \succeq 0, \tag{19}$$

$$\operatorname{tr}(\mathbf{x}_*) + \operatorname{tr}(\mathbf{z}_*) \leq n\rho \tag{20}$$

where $(\mathbf{x}_*, y_*, \mathbf{z}_*)$ is a solution to (1) and (2).

Next, note that $n = \operatorname{tr}(\mathbf{e})$ and consider the quantities

$$\mu_0 = \frac{\langle \mathbf{x}_0, \mathbf{z}_0 \rangle}{n} = \rho^2, \tag{21a}$$

$$R_0^p = \mathcal{A}(\mathbf{x}_0) - b, \tag{21b}$$

$$R_0^d = -\nabla f(\mathbf{x}_0) + \mathcal{A}^\top y_0 + \mathbf{z}_0. \tag{21c}$$

Then, for any $\theta, \nu \in (0,1]$, the *infeasible* KKT system is given by

$$\begin{pmatrix} -\nabla f(\mathbf{x}) + \mathcal{A}^\top y + \mathbf{z} \\ \mathcal{A}(\mathbf{x}) - b \\ H_{\mathbf{p}}(\mathbf{x}, \mathbf{z}) \end{pmatrix} = \begin{pmatrix} \theta R_0^d \\ \theta R_0^p \\ \nu \mu_0 \mathbf{e} \end{pmatrix}, \quad \mathbf{x}, \mathbf{z} \succ 0. \tag{22}$$

Recalling our assumptions that there exists $(\mathbf{x}, y, \mathbf{z})$ satisfying the linear constraints of (1) and (2) for $\mathbf{x}, \mathbf{z} \in \operatorname{int}(\mathcal{K})$ and that $\mathcal{A}$ is surjective, it follows that the system (22) has a unique solution. From here, we can define the *infeasible central path* to be the set

$$\mathcal{P} = \{(\theta, \nu, \mathbf{x}, y, \mathbf{z}) \mid \theta, \nu > 0, \mathbf{x}, \mathbf{z} \in \operatorname{int}(\mathcal{K}),\ y \in \mathbb{R}^m,\ (22) \text{ holds}\}.$$

The general framework of a primal-dual infeasible path-following algorithm is as follows. We seek to generate a sequence of points $(\mathbf{x}^k, y^k, \mathbf{z}^k)$ such that $(\theta^k, \nu^k, \mathbf{x}^k, y^k, \mathbf{z}^k) \in \mathcal{P}$ and $(\mathbf{x}^k, y^k, \mathbf{z}^k)$ converges to a solution of (1) and (2) as $\theta^k \to 0$ and $\nu^k \to 0$. In practice, these points do not lie directly on the central path $\mathcal{P}$, but rather they exist in a neighborhood of $\mathcal{P}$. Choosing $\gamma \in (0,1)$, we can define this neighborhood of $\mathcal{P}$ to be

$$\mathcal{N} = \begin{Bmatrix} (\theta, \nu, \mathbf{x}, y, \mathbf{z}) \in (0,1] \times (0,1] \times \operatorname{int}(\mathcal{K}) \times \mathbb{R}^m \times \operatorname{int}(\mathcal{K}) : \theta \leq \nu \\ \mathcal{A}(\mathbf{x}) - b = \theta(R_0^p + \zeta^p), ||\mathcal{A}^+ \zeta^p|| \leq \gamma_p \rho \\ -\nabla f(\mathbf{x}) + \mathcal{A}^\top y + \mathbf{z} = \theta(R_0^d + \zeta^d), ||\zeta^d|| \leq \gamma_d \rho \\ ||Q(\mathbf{x}^{1/2})\mathbf{z} - \nu\mu_0 I|| \leq \gamma \nu \mu_0 \end{Bmatrix}. \tag{23}$$

In light of (18) letting $\theta_0 = \nu_0 = 1$ implies $(\theta_0, \nu_0, \mathbf{x}_0, y_0, \mathbf{z}_0) \in \mathcal{N}$. Further, from the definition of $\mathcal{N}$ and applying Lemma 3 we arrive at the following result from [18]

Lemma 4. *Lemma 4 in [18] Suppose $(\theta, \nu, \mathbf{x}, y, \mathbf{z}) \in \mathcal{N}$ and $\mathbf{p} \in \mathcal{C}(\mathbf{x}, \mathbf{z})$. Then*

$$(1-\gamma)\nu\mu_0 \mathbf{e} \preceq H_{\mathbf{p}}(\mathbf{x}, \mathbf{z}) \preceq (1+\gamma)\nu\mu_0 \mathbf{e} \tag{24}$$

$$(1-\gamma)\nu\mu_0 \mathbf{e} \leq \frac{\langle \mathbf{x}, \mathbf{z} \rangle}{n} \leq (1+\gamma)\nu\mu_0 \mathbf{e} \tag{25}$$

Proof. First, let

$$\begin{aligned}
\hat{\mathbf{x}} &= \mathbf{Q}(\mathbf{p})\mathbf{x} \\
\hat{\mathbf{z}} &= \mathbf{Q}(\mathbf{p}^{-1})\mathbf{z} \\
\mu &= \nu\mu_0.
\end{aligned}$$

Then, applying Lemma 3 and (16), it follows that

$$H_{\mathbf{p}}(\mathbf{x},\mathbf{z}) = \mathbf{Q}(\hat{\mathbf{x}}^{1/2})\hat{z} \text{ and } \mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}$$

have the same spectrum. Therefore we have

$$\begin{aligned}
|\lambda_{\min}(H_{\mathbf{p}}(\mathbf{x},\mathbf{z})) - \mu| &= |\lambda_{\min}(\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z}) - \mu| \\
&= |\lambda_{\min}\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z} - \mu\mathbf{e}| \\
&\leq ||\lambda_{\min}\mathbf{Q}(\mathbf{x}^{1/2})\mathbf{z} - \mu\mathbf{e}|| \leq \gamma\mu.
\end{aligned}$$

Hence,

$$\lambda_{\min}(H_{\mathbf{p}}(\mathbf{x},\mathbf{z}) - (1-\gamma)\mu\mathbf{e}) = \lambda_{\min}(H_{\mathbf{p}}(\mathbf{x},\mathbf{z})) - (1-\gamma)\mu \geq 0$$

which implies $H_{\mathbf{p}}(\mathbf{x},\mathbf{z}) \succeq (1-\gamma)\mu\mathbf{e}$. As noted in [18], the right hand side of (24) can be proved in a similar fashion.

Next, (25) follows from (24) combined with the fact that

$$\begin{aligned}
\operatorname{tr}(H_{\mathbf{p}}(\mathbf{x},\mathbf{z})) = \langle\hat{\mathbf{x}},\hat{\mathbf{z}}\rangle &= \langle\mathbf{Q}(\mathbf{p})\mathbf{x}, \mathbf{Q}(\mathbf{p}^{-1})\mathbf{z}\rangle \\
&= \langle\mathbf{x}, \mathbf{Q}(\mathbf{p})\mathbf{Q}(\mathbf{p}^{-1})\mathbf{z}\rangle \\
&= \langle\mathbf{x},\mathbf{z}\rangle.
\end{aligned}$$

□

The following two lemmas from [18] will be necessary for the analysis on the iteration bound later in the paper.

Lemma 5. *[18, Lemma 5] For any r_p and r_d satisfying $||r_d|| \leq \gamma_d\rho$ and $||\mathcal{A}^+ r_p|| \leq \gamma_p\rho$ there exists $(\tilde{\mathbf{x}}, \tilde{y}, \tilde{\mathbf{z}})$ that satisfies the following conditions*

$$-\nabla f(\tilde{\mathbf{x}}) + \mathcal{A}^\top y + \tilde{\mathbf{z}} = R_0^d + r_d \tag{26a}$$

$$\mathcal{A}(\tilde{\mathbf{x}}) - b = R_0^p + r_p \tag{26b}$$

$$(1-\gamma_p)\rho\mathbf{e} \preceq \tilde{\mathbf{x}} \preceq (1-\gamma_p)\rho\mathbf{e} \tag{26c}$$

$$[1-(\gamma_d + L\gamma_p)]\rho\mathbf{e} \preceq \tilde{\mathbf{z}} \preceq [1+(\gamma_d + L\gamma_p)]\rho\mathbf{e} \tag{26d}$$

Proof. As done in [18], define

$$\begin{aligned}
\tilde{\mathbf{x}} &= \mathbf{x}_0 + \mathcal{A}^+ r_p, \\
\tilde{y} &= y_0, \\
\tilde{\mathbf{z}} &= \mathbf{z}_0 + r_d + \nabla f(\tilde{\mathbf{x}}) - \nabla f(\mathbf{x}_0),
\end{aligned}$$

then (26a)-(26c) follow trivially. Then, in order to establish (26d), one must verify that

$$\begin{aligned}
||r_d + \nabla f(\tilde{\mathbf{x}}) - \nabla f(\mathbf{x}_0)|| &\leq ||r_d|| + ||\nabla f(\tilde{\mathbf{x}}) - \nabla f(\mathbf{x}_0)|| \\
&\leq (\gamma_d + L\gamma_p)\rho.
\end{aligned}$$

□

Lemma 6. *[18, Lemma 6] Given the initial conditions* (18), (19) *and* (20)*, for any* $(\theta, \nu, \mathbf{x}, y, \mathbf{z}) \in \mathcal{N}$*, we have*

$$\theta \operatorname{tr}(\mathbf{x}) \leq \frac{6\nu\rho n}{1-(\gamma_d + L\gamma_p)}, \quad \theta \operatorname{tr}(\mathbf{z}) \leq \frac{6\nu\rho n}{1-\gamma_p}.$$

Proof. Following [18], the proof of this result is a modification of the proof of Lemma 2 in [31]. Consider $(\theta, \nu, \mathbf{x}, y, \mathbf{z}) \in \mathcal{N}$, it follows

$$\begin{aligned} -\nabla f(\tilde{\mathbf{x}}) + \mathcal{A}^\top y + \tilde{\mathbf{z}} &= \theta(R_0^d + r_d), \quad ||r_d|| \leq \gamma_d \rho, \\ \mathcal{A}(\tilde{\mathbf{x}}) - b &= \theta(R_0^p + r_p), \quad ||\mathcal{A}^+ r_p|| \leq \gamma_p \rho. \end{aligned}$$

Then, applying Lemma 5, there exists a solution $(\tilde{\mathbf{x}}, \tilde{y}, \tilde{\mathbf{z}})$ such that the conditions (26a) and (26d) are satisfied. Further, consider a solution to (1) and (2), denoted $(\tilde{\mathbf{x}}_*, \tilde{y}_*, \tilde{\mathbf{z}}_*)$ given from (19). Such a solution satisfies

$$\begin{aligned} \mathcal{A}(\mathbf{x}_*) - b &= 0, \\ -\nabla f(\mathbf{x}_*) + \mathcal{A}^\top y_* + \mathbf{z}_* &= 0. \end{aligned}$$

Next, define

$$\begin{aligned} \bar{\mathbf{x}} &= (1-\theta)\mathbf{x}_* + \theta\tilde{\mathbf{x}} - \mathbf{x}, \\ \bar{y} &= (1-\theta)y_* + \theta\tilde{y} - y, \\ \bar{\mathbf{z}} &= (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} - \mathbf{z}. \end{aligned}$$

As a consequence,

$$\mathcal{A}(\bar{\mathbf{x}}) = 0, \text{ and } \mathcal{A}^\top(\bar{y}) + \bar{\mathbf{z}} = \mathcal{H}\bar{\mathbf{x}},$$

and therefore $\langle \bar{\mathbf{x}}, \bar{\mathbf{z}} \rangle = \langle \bar{\mathbf{x}}, \mathcal{H}(\bar{\mathbf{x}}) \rangle$. Using this result, and the fact that $\mathcal{H} \succeq 0$ yields

$$\begin{aligned} &\langle (1-\theta)\mathbf{x}_* + \theta\tilde{\mathbf{x}}, \mathbf{z} \rangle + \langle \mathbf{x}, (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} \rangle \\ &= \langle (1-\theta)\mathbf{x}_* + \theta\tilde{\mathbf{x}}, (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle - \langle \bar{\mathbf{x}}, \mathcal{H}(\bar{\mathbf{x}}) \rangle \\ &\leq \langle (1-\theta)\mathbf{x}_* + \theta\tilde{\mathbf{x}}, (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle. \end{aligned} \tag{27}$$

From here, we apply (20), (25), (26c), (26d), (27), and note that $\langle \mathbf{x}_*, \mathbf{z}_* \rangle = 0$, and $\langle \mathbf{x}_*, \mathbf{z} \rangle$, $\langle \mathbf{x}, \mathbf{z}_* \rangle \geq 0$. Then, we have

$$\begin{aligned} &\theta\rho[(1-(\gamma_d + L\gamma_p))\langle \mathbf{e}, \mathbf{z} \rangle + (1-\gamma_p)\langle \mathbf{e}, \mathbf{z} \rangle] \\ &\leq \theta(\langle \tilde{\mathbf{z}}, \mathbf{x} \rangle + \langle \tilde{\mathbf{x}}, \mathbf{z} \rangle) \\ &\leq \langle (1-\theta)\mathbf{x}_* + \theta\tilde{\mathbf{x}}, z \rangle + \langle \mathbf{x}, (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} \rangle \\ &\leq \langle (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{x}}, (1-\theta)\mathbf{z}_* + \theta\tilde{\mathbf{z}} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle \\ &\leq \theta(1-\theta)(\langle \mathbf{x}_*, \tilde{\mathbf{z}} \rangle + \langle \tilde{\mathbf{x}}, \mathbf{z}_* \rangle) + \theta^2 \langle \tilde{\mathbf{x}}, \tilde{\mathbf{z}} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle \\ &\leq \theta(1-\theta)(1+\gamma_d + L\gamma_p)\rho(\langle \mathbf{x}_*, \mathbf{e} \rangle + \langle \mathbf{e}, \mathbf{z}_* \rangle) \\ &\quad + \theta^2(1+\gamma_p)(1+\gamma_d + L\gamma_p)\rho^2 n + (1+\gamma)\nu\mu_0 n \\ &\leq 6\nu\rho n. \end{aligned}$$

□

4.2 An Inexact-Infeasible Interior Point Method

Let $\eta_1 \in (0,1]$, $\eta_2 \in (0,1)$ with $\eta_1 \geq \eta_2$ and $\nu_0, \theta_0 = 1$. Then, given a current point $(\theta_k, \nu_k, \mathbf{x}_k, y_k, \mathbf{z}_k) \in \mathcal{N}$, we try to generate a new point

$$(\theta_{k+1}, \nu_{k+1}, \mathbf{x}_{k+1}, y_{k+1}, \mathbf{z}_{k+1}) \in \mathcal{N}$$

by computing a search direction $(\Delta \mathbf{x}_k, \Delta y_k, \Delta \mathbf{z}_k)$ which solves the following system of equations

$$\begin{pmatrix} -\mathcal{H} & \mathcal{A}^\top & I \\ \mathcal{A} & 0 & 0 \\ E_k & 0 & F_k \end{pmatrix} \begin{pmatrix} \Delta \mathbf{x}_k \\ \Delta y_k \\ \Delta \mathbf{z}_k \end{pmatrix} = \begin{pmatrix} -\eta_1 (R_k^d + r_k^d) \\ -\eta_1 (R_k^p + r_k^p) \\ R^c + r_k^c \end{pmatrix}. \tag{28}$$

Note that here,

$$\begin{aligned} E_k &= L(\mathbf{Q}(\mathbf{p}_k^{-1})\mathbf{z}_k)\mathbf{Q}(\mathbf{p}_k), \\ F_k &= L(\mathbf{Q}(\mathbf{p}_k)\mathbf{x}_k)\mathbf{Q}(\mathbf{p}_k^{-1}), \\ R_k^d &= -\nabla f(\mathbf{x}_k) + \mathcal{A}^\top y_k + \mathbf{z}_k, \\ R_k^p &= \mathcal{A}(\mathbf{x}_k) - b, \\ R_k^c &= (1-\eta_2)\nu_k \mu_0 \mathbf{e} - H_{\mathbf{p}_k}(\mathbf{x}_k, \mathbf{z}_k) \end{aligned}$$

and $\mathbf{p}_k = \mathbf{w}_k^{-1/2}$ where $\mathbf{w}_k$ is the NT scaling element at iteration k. Note that the last equation in (28) corresponds to the symmetrization of the relaxed complementarity condition, given by

$$H_{\mathbf{p}_k}(\mathbf{x}_k, \mathbf{z}_k) + H_{\mathbf{p}_k}(\Delta \mathbf{x}_k, \mathbf{z}_k) + H_{\mathbf{p}_k}(\mathbf{x}_k, \Delta \mathbf{z}_k) = (1-\eta_2)\nu \mu_0 \mathbf{e} + r_k^c. \tag{29}$$

We say that a solution $(\Delta \mathbf{x}_k, \Delta y_k, \Delta \mathbf{z}_k)$ resulting from solving (28) is an inexact search direction. Note that R_k^d, R_k^p and R_k^c are residual terms for the infeasibilities and complementarity, whereas r_k^d, r_k^p and r_k^c correspond to the residuals with respect to the inexactness in the system (28).

Next, consider a sequence $\{\vartheta\}_{k=1}^{\infty}$ over the interval $(0, 1]$ such that

$$\bar{\vartheta} = \sum_{k=0}^{\infty} \vartheta_k < \infty.$$

Then, from [18], it follows that the residual components corresponding to inexactness, r_k^d, r_k^p and r_k^c, must satisfy the following conditions

$$||\mathcal{A}^+ r_k^p|| \leq \gamma_p \rho \theta_k \vartheta_k, \quad ||r_k^d|| \leq \gamma_d \rho \theta_k \vartheta_k, \quad ||r_k^c|| \leq \frac{1}{2}(1-\eta_2)\gamma \nu_k \mu_0. \tag{30}$$

Algorithm 2 details the Infeasible-Inexact IPM for QCO over symmetric cones as given in [18].

Algorithm 2 Infeasible-inexact interior point method.

Input: $\nu_0, \theta_0 = 1$,
parameters $\epsilon, \delta > 0$, $\eta_1, \eta_2 \in (0, 1]$ with $\eta_1 \geq \eta_2$, $\gamma_1, \gamma_2, \in (0, 1)$
such that $\gamma_p \leq \gamma_d$ and $\gamma_d + L\gamma_p \leq 1$. Pick a sequence $\{\vartheta_i\}_{i=0}^{\infty}$ in $(0, 1]$, such that $\bar{\vartheta} = \sum_{i=0}^{\infty} \vartheta_i < \infty$, and choose $(\mathbf{x}_0, y_0, \mathbf{z}_0)$ satisfying (18)-(20)
while $\nu > \epsilon$ **do**

(Let the current and the next iterate be $(\theta_k, \nu_k, \mathbf{x}_k, y_k, \mathbf{z}_k)$ and $(\theta_{k+1}, \nu_{k+1}, \mathbf{x}_{k+1}, y_{k+1}, \mathbf{z}_{k+1})$, respectively)

1. Solve the Newton linear system to obtain inexact search direction $(\Delta \mathbf{x}_k, \Delta y_k, \Delta \mathbf{z}_k)$
2. Set
$$\alpha_k = \max\left\{\alpha \;:\; \alpha \in \left[0, \min\left(1, \frac{1}{\eta_1(1+\bar{\vartheta})}\right)\right],\; (\theta_k(\alpha), \nu_k(\alpha), \mathbf{x}_k(\alpha), y_k(\alpha), \mathbf{z}_k(\alpha)) \in \mathcal{N}\right\}$$

$$\mathbf{x}_{k+1} \leftarrow \mathbf{x}_k + \alpha_k \Delta \mathbf{x}_k,\; y_{k+1} \leftarrow y_k + \alpha_k \Delta y_k \text{ and } \mathbf{z}_{k+1} \leftarrow \mathbf{z}_k + \alpha_k \Delta \mathbf{z}_k$$
$$\nu_{k+1} \leftarrow (1-\alpha\eta_1)\nu_k, \text{ and } \theta_{k+1} \leftarrow (1-\alpha\eta_1)\theta_k$$

end

Now, let $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ denote the step lengths which resulting from the previous k iterations. Following [18], we assume that $\alpha_i \in \mathcal{I}$ for $i = 0, \ldots, k-1$ where

$$\mathcal{I} := \left[0, \min\left\{1, \frac{1}{\eta_1(1+\bar{\vartheta})}\right\}\right]. \tag{31}$$

Then, letting

$$\begin{aligned} R_k^p(\alpha) &= \mathcal{A}(\mathbf{x}_k(\alpha)) - b, \\ R_k^d(\alpha) &= -\nabla f(\mathbf{x}_k(\alpha)) + \mathcal{A}^\top y_k(\alpha) + \mathbf{z}_k(\alpha) \end{aligned}$$

denote the primal and dual infeasibilities corresponding to $(\theta_k, \nu_k, \mathbf{x}_k, y_k, \mathbf{z}_k)$. We seek to demonstrate that the first two inequalities of $\mathcal{N}$ are satisfied by $R_k^p(\alpha)$ and $R_k^d(\alpha)$ for $\alpha \in \mathcal{I}$.

Lemma 7. *[18, Lemma 7] Suppose the step lengths α_i associated with the iterates $(\theta_i, \nu_i, \mathbf{x}_i, y_i, \mathbf{z}_i)$ are restricted to be in the interval $\mathcal{I}$ for $i = 0, \ldots, k-1$. Then we have*

$$\begin{aligned} R_k^p(\alpha) &= \theta_k(\alpha)(R_0^p + \zeta_k^p(\alpha)), \\ R_k^d(\alpha) &= \theta_k(\alpha)(R_0^d + \zeta_k^d(\alpha)) \end{aligned}$$

where

$$||\mathcal{A}^+\zeta_k^p(\alpha)|| \le \gamma_p\rho, \quad ||\zeta_k^d(\alpha)|| \le \gamma_d\rho, \quad \forall \alpha \in \mathcal{I}.$$

Proof. The result for $R_k^p(\alpha)$ follows from the inexact interior-point method for linear SDO provided in [31]. It follows

$$R_k^p(\alpha) = \theta_k(\alpha)(R_0^p + \zeta_k^p(\alpha)),$$

where

$$\begin{aligned} \zeta_k^p(\alpha) &= \zeta_k^p - \frac{\alpha\eta_1}{(1-\alpha\eta_1)\theta_k} r_k^p \\ &= -\sum_{i=1}^{k-1} \frac{\alpha_i\eta_1}{(1-\alpha_i\eta_1)\theta_i} - \frac{\alpha\eta_1}{(1-\alpha\eta_1)\theta_k} r_k^p. \end{aligned} \tag{32}$$

Next, noting $(\theta_k, \nu_k, \mathbf{x}_k, y_k, \mathbf{z}_k) \in \mathcal{N}$ it follows

$$\begin{aligned} R_k^d(\alpha) &= -\nabla f(\mathbf{x}_k(\alpha)) + \mathcal{A}^\top y_k(\alpha) + \mathbf{z}_k(\alpha) \\ &= -\nabla f(\mathbf{x}_k) + \mathcal{A}^\top y_k + \mathbf{z}_k - \alpha[-\mathcal{H}(\Delta\mathbf{x}_k) + \mathcal{A}^\top \Delta y_k + \Delta\mathbf{z}_k] \\ &= R_k^d - \alpha\eta_1(R_k^d + r_k^d) \\ &= (1-\alpha\eta_1)\theta_k(R_0^d + \zeta_k^d) - \alpha\eta_1 r_k^d \\ &= (1-\alpha\eta_1)\theta_k\left(R_0^d + \zeta_k^d) - \frac{\alpha\eta_1}{(1-\alpha\eta_1)\theta_k} r_k^d\right) \\ &= \theta(\alpha)(R_0^d + \zeta_k^d(\alpha)), \end{aligned}$$

for

$$\begin{aligned} \zeta_k^d(\alpha) &= \zeta_k^d - \frac{\alpha\eta_1}{(1-\alpha\eta_1)\theta_k} r_k^d \\ &= -\sum_{i=1}^{k-1} \frac{\alpha_i\eta_1}{(1-\alpha_i\eta_1)\theta_i} - \frac{\alpha\eta_1}{(1-\alpha\eta_1)\theta_k} r_k^d. \end{aligned} \tag{33}$$

Recalling the fact that $\alpha_i \le \frac{1}{\eta_1(1+\bar{\vartheta})}$, its follows from (32) and (33)

$$||\mathcal{A}^+\zeta_k^p(\alpha)|| \le \gamma_p\rho, \quad ||\zeta_k^d(\alpha)|| \le \gamma_d\rho, \quad \forall \alpha \in \mathcal{I},$$

and the proof is complete. ☐

In what follows, set

$$\bar{\alpha} = \min\left\{1, \frac{1}{\eta_1(1+\bar{\vartheta})}, \frac{0.5(1-\eta_2)\gamma\nu_k\mu_0}{||H_{\mathbf{p}_k}(\Delta\mathbf{x}_k, \Delta\mathbf{z}_k)||}\right\}. \tag{34}$$

The following result from [18] verifies the final condition of $\mathcal{N}$, is a generalization of Lemma 4.2 in [30].

Lemma 8. *[18, Lemma 8] For $(\theta_k, \nu_k, \mathbf{x}_k, y_k, \mathbf{z}_k) \in \mathcal{N}$ and $\Delta\mathbf{x}_k$, $\Delta\mathbf{z}_k$ satisfying (28), we have*

(a)

$$\begin{aligned} H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha)) = (1-\alpha)H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha)) + \alpha(1-\eta_2)\nu_k\mu_0\mathbf{e} + \alpha r_k^c \\ + \alpha^2 H_{\mathbf{p}_k}(\Delta\mathbf{x}_k(\alpha), \Delta\mathbf{z}_k(\alpha)) \end{aligned}$$

(b) For all $\alpha \in [0, \bar{\alpha}_k]$,

$$(1-\gamma)\nu_k(\alpha)\mu_0 \le \lambda_i\left(\mathbf{Q}(\mathbf{x}_k(\alpha)^{1/2})\mathbf{z}_k(\alpha)\right) \le (1+\gamma)\nu_k(\alpha)\mu_0$$

(c) For all $\alpha \in [0, \bar{\alpha}_k]$, $\mathbf{x}_k(\alpha) \succ 0$, and $\mathbf{z}_k(\alpha) \succ 0$.

Proof. The proof of part (a) following from application of equation (29). Next, for part (b), we have

$$\begin{aligned} &\lambda_{\min}(H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha))) \\ &\ge (1-\alpha)(1-\gamma)\nu_k\mu_0 + \alpha(1-\eta_2)\nu_k\mu_0 - \alpha||r_k^c|| - \alpha||H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha))|| \\ &= \alpha\gamma(1-\eta_2)\nu_k\mu_0 - \alpha||r_k^c|| - \alpha^2||H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha))|| + (1-\gamma)\nu_k(\alpha)\mu_0 \\ &\ge 0.5\alpha(1-\eta_2)\nu_k\mu_0 - \alpha||r_k^c|| - \alpha^2||H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha))|| + (1-\gamma)\nu_k(\alpha)\mu_0 \\ &\ge (1-\gamma)\nu_k(\alpha)\mu_0 \end{aligned} \tag{35}$$

for $\alpha \in [0, \bar{\alpha}_k]$. Next, define

$$\begin{aligned} \hat{\mathbf{x}}_k(\alpha) &= \mathbf{Q}(\mathbf{p}_k)\mathbf{x}_k(\alpha) \\ \hat{\mathbf{z}}_k(\alpha) &= \mathbf{Q}(\mathbf{p}_k^{-1})\mathbf{z}_k(\alpha). \end{aligned}$$

Then, applying Lemma 3 it follows

$$\lambda_{\min}\left(\mathbf{Q}(\mathbf{x}_k(\alpha))\mathbf{z}_k(\alpha)\right) = \lambda_{\min}\left(\mathbf{Q}(\hat{\mathbf{x}}_k(\alpha))\hat{\mathbf{z}}_k(\alpha)\right) \ge \lambda_{\min}(\hat{\mathbf{x}}_k(\alpha) \circ \hat{\mathbf{z}}_k(\alpha)).$$

Now, as noted in [18], using the fact $H_{\mathbf{p}_k}(\mathbf{x}_k(\alpha), \mathbf{z}_k(\alpha)) = \hat{\mathbf{x}}_k(\alpha) \circ \hat{\mathbf{z}}_k(\alpha)$ and using (35) yields $\lambda_{\min}\left(\mathbf{Q}(\mathbf{x}_k(\alpha))\mathbf{z}_k(\alpha)\right) \ge (1-\gamma)\nu_k(\alpha)\mu_0 \;\; \forall \alpha \in [0, \bar{\alpha}_k]$. The result $\lambda_{\max}\left(\mathbf{Q}(\mathbf{x}_k(\alpha))\mathbf{z}_k(\alpha)\right) \le (1+\gamma)\nu_k(\alpha)\mu_0$ can be proved in a similar manner.

Finally, for part (c), consider $\hat{\mathbf{x}}_k(\alpha)$ and $\hat{\mathbf{z}}_k(\alpha)$ as defined in part (b). Noting that $\mathbf{p}_k \succ 0$, we have $\mathbf{Q}(\mathbf{p}_k)\mathbf{x} \succ 0$ if and only if $\mathbf{x} \succ 0$. Suppose, in order to arrive at a contradiction, that $\mathbf{x} \not\succ 0$ for all $\alpha \in [0, \bar{\alpha}_k]$. There exists an $\alpha^* \in [0, \bar{\alpha}_k]$ by the continuity of $\lambda_{\min}(\cdot)$, which satisfies

$$\begin{aligned} \lambda_{\min}(\hat{\mathbf{x}}_k(\alpha^*)) = 0, \text{ and} \\ \hat{\mathbf{x}}_k(\alpha) \succeq 0 \end{aligned}$$

for all $\alpha \in [0, \bar{\alpha}_k]$. Next, set

$$v^* = \mathbf{Q}(\hat{\mathbf{x}}_k(\alpha^*)^{1/2})\hat{\mathbf{z}}_k(\alpha^*)$$

Now, by the proof of (b), it follows

$$\lambda_{\min}(v^*) \ge (1-\gamma)\nu_k(\alpha^*)\mu_0 > 0$$

meaning $\det(v^*) > 0$. However, by Lemma 3,

$$\det(v^*) = \det(\hat{\mathbf{x}}_k(\alpha^*))\det(\hat{\mathbf{z}}_k(\alpha^*)) = 0.$$

Therefore, we arrive at a contradiction, and thus $\mathbf{x} \succ 0$ for all $\alpha \in [0, \bar{\alpha}_k]$. The proof for $\mathbf{z} \succ 0$ for all $\alpha \in [0, \bar{\alpha}_k]$ follows the same steps. □

Lemma 9. *[18, Lemma 9] Under the conditions in Lemmas 7 and 8, for any $\alpha \in [0, \bar{\alpha}_k]$ we have*

$$(\theta(\alpha), \nu(\alpha), \mathbf{x}(\alpha), y(\alpha), \mathbf{z}(\alpha)) \in \mathcal{N}.$$

Proof. The result follows from Lemmas 7 and 8. □

Lemma 10. *[18, Lemma 10] Suppose the conditions in* (18), (19) *and* (20) *hold. Then*

$$||H_{\mathbf{p}_k}(\Delta\mathbf{x}_k, \Delta\mathbf{z}_k)|| = \frac{O(1)}{(1 - (\gamma_d + L\gamma_p))^2} n^2 \nu_k \mu_0. \tag{36}$$

Our proof of Lemma 10 follows from [18] and is quite involved. Thus, we prove this result in Section 6.1

5 An Infeasible-Inexact Quantum Interior Point Method for Symmetric Cone Optimization

We quantize the II-IPM by closely following Algorithm 2. The resulting scheme is described in Algorithm 3. The algorithm has the following parameters: the accuracy δ to which a classical description of the linear system solutions is estimated via tomography, and the optimality gap tolerance ϵ to which we solve the QCOP. Additionally, details for all steps of Algorithm 3 are discussed subsequently in this paper.

In steps (1) and (2) of Algorithm 3 we require classical matrix multiplication and inversion. These steps can be carried out in time $\mathcal{O}(n^\omega)$ where $\omega = 2.37$ is the matrix multiplication exponent [26, 3]. Note that in practice, this step is typically performed with a linear systems algorithm and requires time $\mathcal{O}(n^3)$. A detailed analysis for step (2) can be found in the following subsection.

In steps (3) and (4), we employ a QLSA and the tomography routine (Algorithm 1) to reconstruct, with high probability, a classical description of the solution to the Newton linear system. Finally, we classically perform line search in step (5) to determine α in order to subsequently update the current solutions to the SDOP S and Y, and the central path parameter ν.

Algorithm 3 Quantum infeasible-inexact interior point method

Input: $\nu_0, \theta_0 = 1$,
parameters $\epsilon, \delta > 0$, $\eta_1, \eta_2 \in (0,1]$ with $\eta_1 \geq \eta_2$, $\gamma_1, \gamma_2, \in (0,1)$
such that $\gamma_p \leq \gamma_d$ and $\gamma_d + L\gamma_p \leq 1$. Pick a sequence $\{\vartheta_i\}_{i=0}^{\infty}$ in $(0,1]$, such that $\bar{\vartheta} = \sum_{i=0}^{\infty} \vartheta_i < \infty$, and choose $(\mathbf{x}_0, y_0, \mathbf{z}_0)$ satisfying (18)-(20) and store in QRAM

while $\nu > \epsilon$ **do**

1. Compute $\mathbf{x}^{1/2}$ (or $\mathbf{z}^{-1/2}$) classically.
2. Compute scaling matrix $\mathbf{p}$ right hand side matrix and necessary matrix products for Newton system factorization and store in QRAM
3. Use block encodings, solve the Newton linear system to construct inexact search direction $|\Delta\mathbf{x}_k \circ \Delta y_k \circ \Delta\mathbf{z}_k\rangle$ and estimate $||\Delta\mathbf{x}_k \circ \Delta y_k \circ \Delta\mathbf{z}_k||$.
4. Obtain classical estimate of $\Delta\mathbf{x}_k \circ \Delta y_k \circ \Delta\mathbf{z}_k$ using vector state tomography.
5. Set

$$\alpha_k = \max\left\{\alpha \; : \; \alpha \in \left[0, \min\left(1, \frac{1}{\eta_1(1+\bar{\vartheta})}\right)\right], \; (\theta_k(\alpha), \nu_k(\alpha), \mathbf{x}_k(\alpha), y_k(\alpha), \mathbf{z}_k(\alpha)) \in \mathcal{N}\right\}$$

$$\mathbf{x}_{k+1} \leftarrow \mathbf{x}_k + \alpha_k \Delta\mathbf{x}_k, \; y_{k+1} \leftarrow y_k + \alpha_k \Delta y_k \text{ and } \mathbf{z}_{k+1} \leftarrow \mathbf{z}_k + \alpha_k \Delta\mathbf{z}_k$$
$$\nu_{k+1} \leftarrow (1 - \alpha\eta_1)\nu_k, \text{ and } \theta_{k+1} \leftarrow (1 - \alpha\eta_1)\theta_k$$

end

5.1 Implementing the Quantum Newton linear system

For the version of our QIPM that uses the NT direction, we factorize the corresponding linear system matrix and construct block encodings for its factors. Note that in principle we construct a $(2, \tilde{O}(1), \xi)$-block-encoding for $W = S^{-1/2}(S^{1/2}YS^{1/2})^{1/2}S^{-1/2}$ in time $\tilde{O}(\|S\|_F^4 \kappa_S^5 \kappa_Y)$, starting from the individual factors S, Y and with repeated applications of Prop.s 4, 5 and 6. However this due to the heavy dependence on the condition number, we choose to classically compute all the factors (including matrix powers), and store them in QRAM. This is more efficient: all the involved matrices are $n \times n$, so classical computation of matrix powers has negligible cost compared to the solution of the Newton linear system, which is of size $O(n^2 \times n^2)$, and we can avoid increasing the dependence on the condition number. The following two propositions establish how one can construct block encodings of these factors, and bound the corresponding running time.

Proposition 9. *Let*

$$M_1 = \begin{pmatrix} -\mathcal{H}/2 & \mathcal{A}^\top/2 & I/2 \\ \mathcal{A}/2 & 0 & 0 \\ E_k/2 & 0 & F_k/2 \end{pmatrix}.$$

If $\mathcal{A}, P^{-1}$, PY, and SP^{-1} are stored in QRAM. Then, a $(\|M_1\|_F, O(\log n), \xi/(\|M_1\|_F \kappa^2 \log^2 \frac{\kappa}{\xi}))$-block encoding of M_1 can be constructed in time $\tilde{O}(1)$.

Proposition 10. *Let*

$$M_2 = \begin{pmatrix} -\mathcal{H}/2 & \mathcal{A}^\top/2 & I/2 \\ \mathcal{A}/2 & 0 & 0 \\ E_k/2 & 0 & F_k/2 \end{pmatrix}.$$

If $\mathcal{A}, P^{-1}$, YP, and $P^{-1}S$ are stored in QRAM. Then, a $(\|M_2\|_F, O(\log n), \xi/(\|M_2\|_F \kappa^2 \log^2 \frac{\kappa}{\xi}))$-block encoding of M_2 can be constructed in time $\tilde{O}(1)$.

Proof. The proof of both preceding propositions follows from Prop. 8. □

Proposition 11. *The Nesterov-Todd linear system matrix can be written compactly as:*

$$M_{NT} = \begin{pmatrix} -\mathcal{H} & \mathcal{A}^\top & I \\ \mathcal{A} & 0 & 0 \\ E_k & 0 & F_k \end{pmatrix}, \tag{37}$$

If $\mathcal{A}, P^{-1}$, YP, PY, $P^{-1}S$, SP^{-1} are stored in QRAM, then a $(\|M_{NT}\|_F, O(\log n), \xi/(\kappa^2 \log^2 \frac{\kappa}{\xi}))$-block encoding of (37), can be constructed in time $\tilde{O}(1)$.

Proof. Carrying out the calculations shows that (37) corresponds to the Nesterov-Todd linear system. We construct the two following block encodings:

$$M_1 = \begin{pmatrix} -\mathcal{H}/2 & \mathcal{A}^\top/2 & I/2 \\ \mathcal{A}/2 & 0 & 0 \\ E_k/2 & 0 & F_k/2 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} -\mathcal{H}/2 & \mathcal{A}^\top/2 & I/2 \\ \mathcal{A}/2 & 0 & 0 \\ E_k/2 & 0 & F_k/2 \end{pmatrix},$$

using Prop.s 9-10. We choose the precision of this step so that we obtain $(\|M_1\|_F, O(\log n), \xi/(\|M_1\|_F \kappa^2 \log^2 \frac{\kappa}{\xi}))$ and $(\|M_2\|_F, O(\log n), \xi/(\|M_2\|_F \kappa^2 \log^2 \frac{\kappa}{\xi}))$-block encodings, respectively, where κ refers to the condition number of (37), here and below. We add these two block encodings together using Proposition 2, obtaining a $(\max\{\|M_1\|_F, \|M_2\|_F\}, O(\log n), \xi/(\kappa^2 \log^2 \frac{\kappa}{\xi}))$-block encoding of (37), in time $\tilde{O}(1)$. Since $\max\{\|M_1\|_F, \|M_2\|_F\} = O(\|M_{\mathrm{NT}}\|_F)$, we obtain the claimed result. □

The construction described in Prop. 11 is only one of the possible ways to obtain a block encoding of the Newton linear system corresponding to the Nesterov-Todd direction. We choose this specific decomposition because among the ones that we analyzed, it minimizes the amount of classical work while yielding the same running time of the quantum subroutine. We now use the factorization to solve the Newton system.

Theorem 5. *There is a quantum algorithm that given*

$$\left| -\eta_1 (R_0^p + r_k^p) \circ -\eta_1 (R_0^d + r_k^d) \circ ((1-\eta_2)\nu\mu_0 I - SY - YS) \right\rangle$$

and access to QRAM data structures encoding $\mathcal{A}, P, Y, S, P^{-1}$, outputs a state ξ-close to $|\Delta x \circ \Delta S \circ \Delta Y\rangle$ in time:

$$\tilde{O}(\kappa \max\{\|M_1\|_F, \|M_2\|_F\}),$$

using the NT direction. We can also output an estimate of $\|\Delta x \circ \Delta S \circ \Delta Y\|$ with relative error δ by increasing the running time by a factor $\frac{1}{\delta}$.

Proof. This is a direct consequence of Prop. 11 and Thm. 3. □

6 Analysis of the II-QIPM for Symmetric Cone Optimization

6.1 Convergence

The following result, provides the iteration bound for the II-QIPM for Symmetric cone optimization.

Theorem 6. *Let $\epsilon > 0$ be a given tolerance. Suppose the conditions (18), (19) and (20) hold. At each iteration of the II-QIPM, set the step length $\alpha_k = \bar{\alpha}_k$. Then, $\nu_k \leq \epsilon$ for $k = O(n^2 \ln(1/\epsilon))$.*

Proof. From (34), applying Lemmas 9 and 10, we have

$$\alpha_i \geq \bar{\alpha} := \min\left\{1, \frac{1}{\eta_1(1+\bar{\vartheta}}, \frac{O(1)}{n^2}\right\}, \quad i = 0, \ldots, k.$$

Hence,

$$\nu_k = \prod_{i=0}^{k-1}(1-\alpha_i\eta_2) \leq (1-\alpha_i\eta_2)^k \leq \varepsilon$$

for $k = O(n^2 \ln(\varepsilon))$. □

6.2 Running Time Analysis

Recall the bounds on the inexactness residuals:

$$\|r_k^d\| \leq \hat{\vartheta}\gamma_1\rho\theta_k\vartheta_k, \|r_k^p\| \leq \gamma_1\rho\theta_k\vartheta_k, \|r_k^c\| \leq \frac{1}{2}(1-\eta_2)\gamma_2\nu_k\rho^2.$$

By Thm. 6, the II-QIPM requires $O(n^2 \ln 1/\epsilon)$ iterations. In each iteration, we must prepare and solve the NT linear system; we denote the running time to do so by T_{LS}. Note that we do not indicate the dependency on the precision of the solution, as it is polylogarithmic and would be neglected in $\tilde{O}$ notation anyway. Furthermore, we must apply the state tomography algorithm to obtain a classical description of the solution of the Newton linear system; we denote the corresponding running time by $T_{TO}(\xi)$ for precision ξ. The total running time of the algorithm is therefore $O(\sum_{k=1}^{\beta n^2 \log(1/\epsilon)} T_{TO}(\xi_k)T_{LS})$, where ξ_k is the precision at iteration k.

Let us know expand this expression using the running times for the state tomography algorithm described in Section 3.3. At iteration k, we must choose ξ_k satisfying:

$$\xi_k = \frac{1}{\varrho}\min\{\|r_k^d\|, \|r_k^p\|, \|r_k^c\|\},$$

where ϱ is the maximum norm of a solution to the Newton linear system. This is due to the fact that the tomography error bound is additive, and naturally assumes that the vector to be extracted has unit norm: to ensure that we satisfy the error bound for the unscaled vector, we need to divide ξ_k by the maximum norm of a solution vector. Setting ϑ_k according to (**??**), we simply have $\vartheta_k = \frac{1}{\log n \log 1/\epsilon}$ before convergence, for sufficiently large n. Hence we must ensure:

$$\|r_k^d\| \leq \alpha_d(1-\frac{c}{n^2})^k\frac{1}{\log n \log 1/\epsilon}$$
$$\|r_k^p\| \leq \alpha_p(1-\frac{c}{n^2})^k\frac{1}{\log n \log 1/\epsilon}$$
$$\|r_k^c\| \leq \alpha_c(1-\frac{c}{n^2})^k,$$

We choose $c = 1$; any constant would do, but $c = 1$ simplifies some of the calculations. We can then take the error ξ_k to be:

$$\min\{\alpha_d, \alpha_p, \alpha_c\}\left(\frac{n^2-1}{n^2}\right)^k\frac{1}{\log n \log 1/\epsilon}.$$

We define $1/\alpha := \min\{\alpha_d, \alpha_p, \alpha_c\}$ for ease of notation. The expression of the total running time of the algorithm, $O(\sum_{k=1}^{\beta n^2 \log(1/\epsilon)} T_{TO}(\xi_k)T_{LS})$, can be rewritten as:

$$\sum_{k=1}^{\beta n^2 \log(1/\epsilon)} \frac{n^2\varrho^2}{\xi_k^2}T_{LS} = \alpha T_{LS} n^2 \log^2 n \log^2(1/\epsilon)\varrho^2 \sum_{k=1}^{\beta n^2 \log(1/\epsilon)}\left(\frac{n^2}{n^2-1}\right)^{2k} \leq$$
$$\alpha T_{LS} n^2 \log^2 n \log^2(1/\epsilon)\varrho^2 \sum_{k=1}^{2\beta n^2 \log(1/\epsilon)}\left(\frac{n^2}{n^2-1}\right)^{k}.$$

Computing the geometric series yields:

$$\sum_{k=1}^{2\beta n^2\log(1/\epsilon)}\left(\frac{n^2}{n^2-1}\right)^k=\frac{1-\left(\frac{n^2}{n^2-1}\right)^{2\beta n^2\log(1/\epsilon)}}{1-\frac{n^2}{n^2-1}}-1=(n^2-1)\left(\left(\frac{n^2}{n^2-1}\right)^{2\beta n^2\log(1/\epsilon)}-1\right)-1.$$

We now use the fact that $\lim_{x\to\infty}\left(\frac{x+1}{x}\right)^x=e$. Thus, the last term in the above expression goes to $e^{\log(1/\epsilon)}=O(\frac{1}{\epsilon})$ for large n. We hence get a total running time of:

$$\tilde{O}\left(\frac{n^4}{\epsilon}\varrho^2T_{LS}\right).$$

Notice that the time to classically compute matrices and their inverses is subsumed by this. We also remark that if we had access to a state tomography algorithm with only linear dependence on the inverse error, i.e., $1/\xi$ rather than $1/\xi^2$, this would only decrease the ϱ dependency from ϱ^2 to ϱ. From here, we can note that an upper bound on the size of the solution ϱ can be given by $\varrho\leq O(\kappa(A)\rho n^{1.5})$, which implies an overall running time of

$$\tilde{O}\left(\frac{n^{8.5}}{\epsilon}\rho^2\kappa^3\right).$$

7 Conclusion

In this work we provide the first quantum interior point method that is valid for QCOPs over symmetric cones. Further, we provide explicit definitions for the Newton linear system corresponding to the Nesterov-Todd (NT) search direction, as well as factorizations and results on constructing these matrices in a quantum setting. Our results demonstrate that by making use of QRAM and block encoding techniques, we are able to efficiently compute the scaling matrices needed for primal-dual symmetry and solve our Newton linear system efficiently using quantum linear solvers. Our work builds upon recently developed techniques for quantum linear algebra, and opens the for for a myriad of applications in optimization.

A Proofs taken from other papers

A.1 Proof of Lemma 10

Consider the quantities

$$\begin{aligned}\hat{\mathbf{x}}_k&=\mathbf{Q}(\mathbf{p}_k)\mathbf{x}_k, & \hat{\mathbf{z}}_k&=\mathbf{Q}(\mathbf{p}_k^{-1})\mathbf{z}_k,\\ \Delta\hat{\mathbf{x}}_k&=\mathbf{Q}(\mathbf{p}_k)\Delta\mathbf{x}_k, & \Delta\hat{\mathbf{z}}_k&=\mathbf{Q}(\mathbf{p}_k^{-1})\Delta\mathbf{z}_k,\\ \hat{E}_k&=E_k\mathbf{Q}(\mathbf{p}_k^{-1})=L(\hat{\mathbf{z}}_k), & \hat{F}_k&=F_k\mathbf{Q}(\mathbf{p}_k)=L(\hat{\mathbf{x}}_k).\end{aligned}$$

Following from (16), note that

$$\hat{\mathbf{z}}_k=\hat{\mathbf{x}}_k,\quad \hat{E}_k=\hat{F}_k. \tag{38}$$

Next, define the spectral decomposition of $\hat{\mathbf{x}}$ and $\hat{\mathbf{z}}$ as

$$\hat{\mathbf{x}}=\hat{\mathbf{z}}=\lambda_1^kc_1^k+\cdots+\lambda_r^kc_r^k. \tag{39}$$

Then, applying (24), it follows

$$(1-\gamma)\nu_k\mu_0\leq(\lambda_1^k)^2\leq\cdots\leq(\lambda_r^k)^2\leq(1+\gamma)\nu_k\mu_0. \tag{40}$$

Defining $\hat{S}_k=\hat{E}_k\hat{F}_k=(\hat{E}_k)^2$, by Lemma 1, we have that the eigenvalues of $\hat{S}_k$ are then

$$\Lambda(\hat{S}_k)=\left\{\frac{1}{4}(\lambda_i^k+\lambda_j^k)^2\ :\ 1\leq i,j\leq r\right\}.$$

Hence, by (40),

$$||\hat{S}_k||_2 \le (1+\gamma)\nu_k\mu_0, \quad ||\hat{S}_k^{-1}||_2 \le \frac{1}{(1-\gamma)\nu_k\mu_0}. \tag{41}$$

Next, following [18] we state a series of lemmas which will allow us to complete our proof of Lemma 10.

Lemma 11. *[18, Lemma 11] For any* $\mathbf{u} \in \mathcal{J}$*,*

$$||\mathbf{Q}(\mathbf{p}_k)\mathbf{u}||^2 \le \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{z}_k)||_2||\mathbf{u}||^2,$$
$$||\mathbf{Q}(\mathbf{p}_k^{-1})\mathbf{u}||^2 \le \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{x}_k)||_2||\mathbf{u}||^2$$

Proof. First, note that by Lemma 3, $\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{x}_k$, $\mathbf{Q}(\mathbf{x}_k^{1/2})\mathbf{z}_k$, $\mathbf{Q}(\hat{\mathbf{x}}_k^{1/2})\hat{\mathbf{z}}_k$ and $H_{\mathbf{p}_k}(\mathbf{x}_k, \mathbf{z}_k)$ have the same spectrum. Hence,

$$(1-\gamma)\nu_k\mu_0 \le \lambda_{\min}\left(\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{x}_k\right) \le \lambda_{\max}\left(\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{x}_k\right) \le (1+\gamma)\nu_k\mu_0 \tag{42a}$$
$$(1-\gamma)\nu_k\mu_0 \le \lambda_{\min}\left(\mathbf{Q}(\mathbf{x}_k^{1/2})\mathbf{z}_k\right) \le \lambda_{\max}\left(\mathbf{Q}(\mathbf{x}_k^{1/2})\mathbf{z}_k\right) \le (1+\gamma)\nu_k\mu_0. \tag{42b}$$

Next, following [18] set $\mathbf{v}_k = \mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{x}_k$. Then, applying (15) it follows that

$$\mathbf{p}_k^{-2} = \mathbf{Q}(\mathbf{z}_k^{-1/2})\mathbf{v}_k.$$

Hence, from (42a) we have

$$\begin{aligned}
||\mathbf{Q}(\mathbf{p}_k)\mathbf{u}||^2 &= \langle \mathbf{u}, \mathbf{Q}(\mathbf{p}_k^2)\mathbf{u}\rangle \\
&= \langle \mathbf{u}, \left[\mathbf{Q}(\mathbf{z}_k^{-1/2})\mathbf{Q}(\mathbf{v}_k^{1/2})\mathbf{Q}(\mathbf{z}_k^{-1/2})\right]^{-1}\mathbf{u}\rangle \\
&= \langle \mathbf{u}, \mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{Q}(\mathbf{v}_k^{-1/2})\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{u}\rangle \\
&= \langle \mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{u}, \mathbf{Q}(\mathbf{v}_k^{-1/2})\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{u}\rangle \\
&\le \lambda_{\max}(\mathbf{Q}(\mathbf{v})^{-1/2})||\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{u}||^2 \\
&\le \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{u}||^2 \\
&\le \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{z}_k^{1/2})||_2||\mathbf{u}||^2
\end{aligned}$$

The second inequality in the Lemma can be proved in a similar manner. □

Lemma 12. *[18, Lemma 12]*

$$||\Delta\hat{\mathbf{x}}_k||^2 + ||\Delta\hat{\mathbf{z}}_k||^2 + (2\langle\Delta\hat{\mathbf{x}}, \Delta\hat{\mathbf{z}}\rangle = ||\hat{S}_k^{-1/2}(R_k^c + r_k^c)||^2,$$
$$||H_{\mathbf{p}_k}(\Delta\mathbf{x}_k, \Delta\mathbf{z}_k)|| \le \frac{1}{2}\left(||\Delta\hat{\mathbf{x}}_k||^2 + ||\Delta\hat{\mathbf{z}}_k||^2\right)$$

Proof. First, we can rewrite the last equation (the symmetric linearized completmentarity condition) of (28) as

$$\hat{E}_k(\Delta\hat{\mathbf{x}}) + \hat{F}_k(\Delta\hat{\mathbf{z}}) = R_k^c + r_k^c. \tag{43}$$

Then, left-multiplying (43) by $\hat{S}_k^{-1/2}$ yields

$$\Delta\hat{\mathbf{x}} + \Delta\hat{\mathbf{z}} = \hat{S}_k^{-1/2}(R_k^c + r_k^c)$$

from which the first equation of the Lemma follows. As for the second inequality, by applying Lemma (1), note that

$$\begin{aligned}||H_{\mathbf{p}_k}(\Delta\mathbf{x}_k,\Delta\mathbf{z}_k)|| &= ||\Delta\hat{\mathbf{x}}\circ\Delta\hat{\mathbf{z}}|| \\ &\le ||\Delta\hat{\mathbf{x}}||||\Delta\hat{\mathbf{z}}|| \\ &\le \frac{1}{2}\left(||\Delta\hat{\mathbf{x}}||^2+||\Delta\hat{\mathbf{z}}||^2\right),\end{aligned}$$

and the proof is complete. □

Lemma 13. *[18, Lemma 13]*

$$||\hat{S}_k^{-1/2}(R_k^c+r_k^c)||^2 = O(n\nu_k\mu_0).$$

Proof. Applying (30) and (41) yields

$$\begin{aligned}||\hat{S}_k^{-1/2}r_k^c||^2 &\le ||\hat{S}_k^{-1}||_2||r_k^c||^2 \\ &\le \frac{1}{4}\cdot\frac{[(1-\eta_2)\gamma\nu_k\mu_0]^2}{(1-\gamma)\nu_k\mu_0} \\ &= \frac{(1-\eta_2)\gamma\nu_k\mu_0}{4(1-\gamma)}.\end{aligned} \tag{44}$$

Next, from (39), we have

$$\lambda(R_k^c) = (1-\eta_2)\nu_k\mu_0 - \lambda(\hat{\mathbf{x}})^2.$$

Hence, it follows

$$\begin{aligned}||\hat{S}_k^{-1/2}R_k^c||^2 &\le ||\hat{S}_k^{-1}||_2||R_k^c||^2 \\ &\le \frac{1}{(1-\gamma)\nu_k\mu_0}\sum_{i=0}^{r}\left((1-\eta_2)\nu_k\mu_0-(\lambda_i^k)^2\right) \\ &\le \frac{n\nu_k\mu_0}{1-\gamma}(\gamma+\eta_2)^2,\end{aligned} \tag{45}$$

where the last inequatlity follows from (40). As noted in [18], the result in the lemma follows from (44) and (45), which completes the proof. □

In the rest of the analysis, we follow [18] in that we consider an auxiliary point $(\tilde{\mathbf{x}},\tilde{y},\tilde{\mathbf{z}})$, which is guaranteed to exist by Lemma 5. Now, at the k-th iteration, by Lemma 7 we have

$$-\nabla f(\mathbf{x}_k)+\mathcal{A}^\top y_k+\mathbf{z}_k = \theta(R_0^d+\zeta_k^d), \quad ||\zeta_k^d||\le\gamma_d\rho \tag{46}$$

$$\mathcal{A}(\mathbf{x}_k)-b = \theta(R_0^p+\zeta_k^p), \quad ||\mathcal{A}^+\zeta_k^p||\le\gamma_p\rho. \tag{47}$$

Then, applying Lemma 5 there exists a point $(\tilde{\mathbf{x}},\tilde{y},\tilde{\mathbf{z}})$ which satisfies

$$-\nabla f(\mathbf{x}_k)+\mathcal{A}^\top y_k+\mathbf{z}_k = R_0^d+\zeta_k^d \tag{48}$$

$$\mathcal{A}(\mathbf{x}_k)-b = R_0^p+\zeta_k^p \tag{49}$$

$$(1-\gamma_p)\rho\mathbf{e}\preceq\tilde{\mathbf{x}}\preceq(1+\gamma_p)\rho\mathbf{e} \tag{50}$$

$$[1-(\gamma_d+L\gamma_p)]\rho\mathbf{e}\preceq\tilde{\mathbf{z}}\preceq[1+(\gamma_d+L\gamma_p)]\rho\mathbf{e}. \tag{51}$$

Lemma 14. *[18, Lemma 14] Let*

$$\begin{aligned}\bar{\mathbf{x}}_k &= \mathbf{x}_k-\mathbf{x}_*-\theta(\tilde{\mathbf{x}}-\mathbf{x}_*) \\ \bar{\mathbf{z}}_k &= \mathbf{z}_k-\mathbf{z}_*-\theta(\tilde{\mathbf{z}}-\mathbf{z}_*).\end{aligned}$$

The following equations hold:

$$\langle \bar{\mathbf{x}}_k, \bar{\mathbf{z}}_k \rangle = \langle \bar{\mathbf{x}}_k, \mathcal{H}\bar{\mathbf{x}}_k \rangle, \tag{52}$$

$$\begin{aligned}&\langle \Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*) + \eta_1\mathcal{A}^+ r_k^p, \Delta\mathbf{z}_k + \eta_1\theta_k(\tilde{\mathbf{z}}_k - \mathbf{z}_*) + \eta_1 r_k^d\rangle \\ &= \langle \Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*) + \eta_1\mathcal{A}^+ r_k^p, \mathcal{H}(\Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*))\rangle.\end{aligned} \tag{53}$$

Proof. Applying (46)-(49), and noting the fact that

$$\begin{aligned}\mathcal{A}\mathbf{x}_* - b &= 0 \\ -\nabla f(\mathbf{x}_*) + \mathcal{A}^\top y_* + z_* &= 0,\end{aligned}$$

it follows

$$\begin{aligned}\mathcal{A}\bar{\mathbf{x}}_k &= 0 \\ \mathcal{A}^\top(y_k - y_* - \theta_k(\tilde{y}_k - y_*)) + \bar{\mathbf{z}}_k &= \mathcal{H}(\bar{\mathbf{x}}_k),\end{aligned}$$

from which (52) follows. Next, again using (46)-(49), by (28)

$$\begin{aligned}\mathcal{A}\left(\Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*) + \eta_1\mathcal{A}^+ r_k^p\right) &= 0 \\ \mathcal{A}^\top(\Delta y_k + \eta_1\theta_k(\tilde{y}_k - y_*)) + (\Delta\mathbf{z}_k + \eta_1\theta_k(\tilde{\mathbf{z}}_k - \mathbf{z}_*)) + \eta_1 r_k^d &= \mathcal{H}(\Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*)).\end{aligned}$$

The last equation implies (53) and the proof is complete. □

Next, consider the quantities

$$T_1 = \left(||\Delta\hat{\mathbf{x}}_k||^2 + ||\Delta\hat{\mathbf{z}}_k||^2\right)^{1/2}, \tag{54}$$

$$T_2 = \left(||\mathbf{Q}(\mathbf{p}_k)(\tilde{\mathbf{x}}_k - \mathbf{x}_k)||^2 + ||\mathbf{Q}(\mathbf{p}_k^{-1})(\tilde{\mathbf{z}}_k - \mathbf{z}_k)||^2\right)^{1/2}, \tag{55}$$

$$T_3 = \left(||\mathbf{Q}(\mathbf{p}_k)\mathcal{A}^+ r_k^p||^2 + ||\mathbf{Q}(\mathbf{p}_k^{-1}) r_k^d||^2\right)^{1/2}, \tag{56}$$

$$T_4 = ||\mathbf{Q}(\mathbf{p}_k^{-1})\mathcal{H}(\mathcal{A}^+ r_k^p)||. \tag{57}$$

Lemma 15. *[18, Lemma 15]*

$$T_1 \le 2\eta_2(\theta_k T_2 + T_3 + T_4) + \sqrt{T_5},$$

where

$$T_5 = ||\hat{S}_k^{-1/2}(R_k^c + r_k^c)||^2 + 2\eta_1^2\theta_k^2\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle + 2\eta_1^2(\theta_k T_2 T_3 + T_3^2 + \theta_k T_2 T_3).$$

Proof. Noting (53) yields

$$\begin{aligned}-\langle \Delta\hat{\mathbf{x}}_k, \Delta\hat{\mathbf{z}}_k\rangle &= -\langle \Delta\mathbf{x}_k, \Delta\mathbf{z}_k\rangle \\ =\ & \eta_1\theta_k\left[\langle \Delta\mathbf{x}_k, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle + \langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \Delta\mathbf{z}\rangle\right] \\ &+ \eta_1\left[\langle \tilde{\mathbf{x}}_k, r_k^d\rangle + \langle \mathcal{A}^+ r_k^p, \Delta\mathbf{z}_k\rangle\right] \\ &+ \eta_1^2\theta_k\left[\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, r_k^d\rangle + \langle \mathcal{A}^+ r_k^p, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle\right] \\ &+ \eta_1^2\langle \mathcal{A}^+ r_k^p, r_k^d\rangle + \eta_1^2\theta_k^2\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle \\ &- \eta_1\langle \mathcal{A}^+ r_k^p, \mathcal{H}(\Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*))\rangle \\ &- \langle \Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*), \mathcal{H}(\Delta\mathbf{x}_k + \eta_1\theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*))\rangle.\end{aligned}$$

Next, using the Cachy-Schwartz inequality, along with the fact that

$$ac + bd \le \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2},$$

for $a, b, c, d \geq 0$, we also have:

$$
\begin{aligned}
&|\langle \Delta \mathbf{x}_k, \tilde{\mathbf{z}}_k - \mathbf{z}_* \rangle + \langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \Delta \mathbf{x}_k \rangle| \\
&= |\langle \Delta \hat{\mathbf{x}}_k, \mathbf{Q}(\mathbf{p}_k^{-1})(\tilde{\mathbf{z}}_k - \mathbf{z}_*) \rangle + \langle \mathbf{Q}(\mathbf{p}_k)(\tilde{\mathbf{x}}_k - \mathbf{x}_*), \Delta \hat{\mathbf{z}}_k \rangle| \leq T_1 T_2 \\
&|\langle \Delta \mathbf{x}_k, r_k^d \rangle + \langle \mathcal{A}^+ r_k^p, \Delta \mathbf{z}_k \rangle| \leq T_1 T_3 \\
&|\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, r_k^d \rangle + \mathcal{A}^+ r_k^p, \tilde{\mathbf{z}}_k - \mathbf{z}_* \rangle| \leq T_2 T_3 \\
&|\langle \mathcal{A}^+ r_k^p, r_k^d \rangle| \leq T_3 \\
&|\langle \mathcal{A}^+ r_k^p, \mathcal{H}(\tilde{\mathbf{x}}_k - \mathbf{x}_k) \rangle| \leq T_2 T_4 \\
&|\langle \mathcal{A}^+ r_k^p, \mathcal{H}(\Delta \mathbf{x}_k) \rangle| \leq T_1 T_4 \\
&- \langle \delta \mathbf{x}_k + \eta_1 \theta_k (\tilde{\mathbf{x}}_k - \mathbf{x}_*), \mathcal{H}(\Delta \mathbf{x}_k + \eta_1 \theta_k (\tilde{\mathbf{x}}_k - \mathbf{x}_*)) \rangle \leq 0.
\end{aligned}
$$

Applying the above inequalities along with Lemma 12 yields

$$
\begin{aligned}
T_1^2 &= ||\hat{S}_k^{-1/2}(R_k^c + r_k^c)||^2 - 2\langle \Delta \hat{\mathbf{x}}_k, \Delta \hat{\mathbf{z}}_k \rangle \\
&\leq 2\left(\eta_1 \theta_k T_1 T_2 + \eta_1 T_1 T_3 + \eta_1^2 \theta_k T_1 T_3 + \eta_1^2 T_3^2\right) \\
&\quad + 2\left(\eta_1^2 \theta_k T_2 T_4 + \eta_1 T_1 T_4\right) \\
&\quad + ||\hat{S}_k^{-1/2}(R_k^c + r_k^c)||^2 + 2\eta_1^2 \theta_k^2 \langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}}_k - \mathbf{z}_* \rangle \\
&= 2\eta_1 T_1 (\theta_k T_2 + T_3 + T_4) + T_5.
\end{aligned}
$$

Next, note that the quadratic function

$$t^2 - 2\eta_1(\theta_k T_2 + T_3 + T_4)t - T_5$$

the positive root

$$t_+ = \eta_1(\theta_k T_2 + T_3 + T_4) + \sqrt{\eta_1^2(\theta_k T_2 + T_3 + T_4)^2 + T_5},$$

which is unique, and positive for $t > t_+$. Therefore, it must hold

$$T_1 \leq t_+ \leq 2\eta_1(\theta_k T_2 + T_3 + T_4) + \sqrt{T_5}$$

and the proof is complete. □

Lemma 16. *[18, Lemma 16] We have*

$$T_3^2 = \frac{O(1)}{(1 - (\gamma_d + L\gamma_p))^2} n^2 \nu_k \mu_0.$$

Proof. It follows from (30)

$$||\mathcal{A}^+ r_k^p|| \leq \theta_k \gamma_p \rho, \quad ||r_k^d|| \leq \theta_k \gamma_d \rho. \tag{58}$$

Then, noting that for any $\mathbf{u} \succeq 0$, $||\mathbf{Q}(\mathbf{u})||_2 = \lambda_{\max}^2(\mathbf{u}) \leq \operatorname{tr}(\mathbf{u})^2$, applying Lemma 11 yields

$$
\begin{aligned}
||\mathbf{Q}(\mathbf{p}_k)\mathcal{A}^+ r_k^p||^2 &\leq \frac{1}{(1-\gamma)\nu_k \mu_0} ||\mathcal{A}^+ r_k^p||^2 ||\mathbf{Q}(\mathbf{z}_k)||_2 \\
&\leq \frac{\gamma_p^2 \rho^2}{(1-\gamma)\nu_k \mu_0} ||\mathbf{Q}(\mathbf{z}_k)||_2 \\
&\leq \frac{\gamma_p^2 \rho^2}{(1-\gamma)\nu_k \mu_0} \theta_k^2 \operatorname{tr}(\mathbf{z}_k)^2 \\
&= \frac{\gamma_p^2 \rho^2}{(1-\gamma)\nu_k \mu_0} \frac{36}{(1-\gamma_p)^2} n^2 \nu_k^2 \rho^2 \\
&= \frac{O(1)}{(1-\gamma_p)^2} n^2 \nu_k \mu_0,
\end{aligned}
$$

where the final equality follows from utilizing Lemma 6. Again we apply Lemma 6, and arrive at

$$\begin{aligned}||\mathbf{Q}(\mathbf{p}_k^{-1})r_k^d||^2 &\leq \frac{1}{(1-\gamma)\nu_k\mu_0}||r_k^d||^2||\mathbf{Q}(\mathbf{x}_k)||_2 \\ &\leq \frac{\gamma_d^2\rho^2}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{x}_k)||_2 \\ &\leq \frac{\gamma_d^2\rho^2}{(1-\gamma)\nu_k\mu_0}\theta_k^2 \operatorname{tr}(\mathbf{x}_k)^2 \\ &= \frac{\gamma_d^2\rho^2}{(1-\gamma)\nu_k\mu_0}\frac{36}{(1-(1-\gamma_d+L\gamma_p))^2}n^2\nu_k^2\rho^2 \\ &= \frac{O(1)}{(1-(1-\gamma_d+L\gamma_p))^2}n^2\nu_k\mu_0,\end{aligned}$$

and the proof is complete. □

Lemma 17. *[18, Lemma 17] Under the conditions* (18), (19), *and* (20),

$$\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}}_k - \mathbf{z}_* \rangle \leq 4n\mu_0.$$

Proof. The result follows from applying (50), (51) along with [31, Lemma 11]. □

Lemma 18. *[18, Lemma 18] Under the conditions* (18), (19), *and* (20),

$$\theta_k^2 T_2^2 = O(n^2\nu_k\mu_0).$$

Proof. From [6, Proposition III.2.2], for any invertible $\mathbf{u} \in \mathcal{J}$, and $\mathbf{x} \succ 0$, we have $\mathbf{Q}(\mathbf{u})\mathbf{x} \succ 0$. Hence, for any $\mathbf{x} \succ 0$,

$$||\mathbf{Q}(\mathbf{u})\mathbf{x}|| \leq \operatorname{tr}(\mathbf{Q}(\mathbf{u})\mathbf{x}) = \langle \mathbf{Q}(\mathbf{u})\mathbf{x}, \mathbf{e}\rangle = \langle \mathbf{u}^2, \mathbf{x}\rangle. \tag{59}$$

Now, letting

$$\mathbf{v}_k = \mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{x}_k,$$

by (15) it follows

$$\mathbf{p}^{-2} = \mathbf{Q}(\mathbf{z}_k^{-1/2})v_k^{1/2}.$$

From here, we apply (59) combined with the fact that

$$0 \prec \tilde{\mathbf{x}}_k - \mathbf{x}_* \preceq (1+\gamma_p)\rho\mathbf{e}$$

which yields

$$\begin{aligned}||\mathbf{Q}(\mathbf{p}_k)(\tilde{\mathbf{x}}_k - \mathbf{x}_*)|| &\leq \langle \mathbf{p}_k^2, \tilde{\mathbf{x}}_k - \mathbf{x}_*\rangle \\ &= \langle \mathbf{Q}(\mathbf{p}_k^{-2})\mathbf{p}_k^2, \mathbf{Q}(\mathbf{p}_k^2)(\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &= \langle \mathbf{p}_k^{-2}, \left(\mathbf{Q}(\mathbf{p}_k^{-2})\right)^{-1}(\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &= \langle \mathbf{Q}(\mathbf{z}_k^{-1/2})\mathbf{v}_k^{1/2}, \left[\mathbf{Q}(\mathbf{z}_k^{-1/2})\mathbf{Q}(\mathbf{v}_k^{1/2})\mathbf{Q}(\mathbf{z}_k^{-1/2})\right]^{-1}(\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &= \langle \mathbf{Q}(\mathbf{z}_k^{-1/2})\mathbf{v}_k^{1/2}, \left[\mathbf{Q}(\mathbf{z}_k^{1/2})\mathbf{Q}(\mathbf{v}_k^{-1/2})\mathbf{Q}(\mathbf{z}_k^{1/2})\right](\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &= \langle \mathbf{Q}(\mathbf{v}_k^{-1/2})\mathbf{v}_k^{1/2}, \mathbf{Q}(\mathbf{z}_k^{1/2})(\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &= \langle \mathbf{v}_k^{-1/2}, \mathbf{Q}(\mathbf{z}_k^{1/2})(\tilde{\mathbf{x}}_k - \mathbf{x}_*)\rangle \\ &\leq \frac{1}{\lambda_{\min}(\mathbf{v}_k)^{1/2}}\langle \mathbf{z}_k, \tilde{\mathbf{x}}_k - \mathbf{x}_*\rangle \\ &\leq \frac{1}{\sqrt{(1-\gamma)\nu_k\mu_0}}\langle \mathbf{z}_k, \tilde{\mathbf{x}}_k - \mathbf{x}_*\rangle.\end{aligned}$$

On the other hand, for

$$0 \prec \tilde{\mathbf{z}}_k - \mathbf{z}_* \preceq (1+\gamma_d + L\gamma_p)\rho\mathbf{e}$$

it follows

$$||\mathbf{Q}(\mathbf{p}_k^{-1}(\tilde{\mathbf{z}}_k - \mathbf{z}_*)|| \leq \frac{1}{\sqrt{(1-\gamma)\nu_k\mu_0}}\langle \mathbf{x}_k, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle.$$

Thus,

$$\begin{aligned}\theta_k^2 T_2^2 &\leq \theta_k^2 \left(||\mathbf{Q}(\mathbf{p}_k)(\tilde{\mathbf{x}}_k - \mathbf{x}_*)|| + ||\mathbf{Q}(\mathbf{p}_k^{-1})(\tilde{\mathbf{z}}_k - \mathbf{z}_*)||\right)^2 \\ &\leq \frac{\theta_k^2}{(1-\gamma)\nu_k\mu_0}\left(\langle \mathbf{z}_k, \tilde{\mathbf{x}} - \mathbf{x}_*\rangle + \langle \mathbf{x}_k, \tilde{\mathbf{z}} - \mathbf{z}_*\rangle\right)^2.\end{aligned}$$

Now, recall that

$$\begin{aligned}\langle \mathbf{x}_*, \mathbf{z}_*\rangle &= 0, \\ \langle \mathbf{x}_k, \mathbf{z}_*\rangle, \langle \mathbf{x}_*, \mathbf{z}_k\rangle, \langle \tilde{\mathbf{x}}_k, \mathbf{z}_*\rangle, \langle \tilde{\mathbf{z}}_k, \mathbf{x}_*\rangle &\geq 0.\end{aligned}$$

These inequalities, combined with (52) give

$$\begin{aligned}&\theta_k\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \mathbf{z}_k\rangle + \theta_k\langle \mathbf{x}_k, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle \\ = \;& \langle \mathbf{z}_k, \mathbf{z}_k\rangle - \langle \mathbf{x}_k, \mathbf{z}_*\rangle - \langle \mathbf{x}_*, \mathbf{z}_k\rangle + \langle \mathbf{x}_*, \mathbf{z}_*\rangle \\ & + \theta_k\left(\langle\rangle + \langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \mathbf{z}_*\rangle\right) \\ & + \theta_k^2\langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}}_k - \mathbf{z}_*\rangle \\ & - \langle \mathbf{x}_k - \mathbf{x}_* - \theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*), \mathcal{H}(\mathbf{x}_k - \mathbf{x}_* - \theta_k(\tilde{\mathbf{x}}_k - \mathbf{x}_*))\rangle \\ \leq \;& \langle \mathbf{x}_k, \mathbf{z}_k\rangle + \theta_k\left(\langle \mathbf{x}_*, \tilde{\mathbf{z}}_k\rangle + \langle \tilde{\mathbf{x}}_k, \mathbf{z}_*\rangle\right) + \theta_k^2\langle \tilde{\mathbf{x}}_k, \tilde{\mathbf{z}}_k\rangle \\ \leq \;& (1+\gamma)\nu_k\mu_0 n + \theta_k(1+\gamma_d + L\gamma_p)\rho(\langle \mathbf{x}_*, \mathbf{e}\rangle + \mathbf{e}\mathbf{z}_*) \\ & + \theta_k^2(1+\gamma_p)(1+\gamma_d+L\gamma_p)\rho^2 n \\ \leq \;& 8\nu_k\mu_0 n.\end{aligned}$$

Therefore, $\theta_k^2 T_2^2 = O(n^2\nu_k\mu_0)$ and the proof is complete. □

Lemma 19. *[18, Lemma 19]*

$$\theta_k^2 T_2^2 = O(n^2\nu_k\mu_0).$$

Proof. From Lemma 11 it follows

$$\begin{aligned}T_4^2 &\leq \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{x}_k)||_2||\mathcal{H}(\mathcal{A}^+ r_k^p)||^2 \\ &\leq \frac{1}{(1-\gamma)\nu_k\mu_0}||\mathbf{Q}(\mathbf{x}_k)||_2 L^2||\mathcal{A}^+ r_k^p||^2 \\ &\leq \frac{\gamma_p^2\rho^2L^2}{(1-\gamma)\nu_k\mu_0}\theta_k^2||\mathbf{Q}(\mathbf{x}_k)||_2 \\ &\leq \frac{\gamma_p^2L^2}{(1-\gamma)\nu_k\mu_0}\frac{O(1)}{(1-(\gamma_d+L\gamma_p))^2}n^2\nu_k^2\rho^2 \\ &= \frac{O(1)}{(1-(\gamma_d+L\gamma_p))^2}n^2\nu_k\mu_0.\end{aligned}$$

□

Finally, this last Lemma and proof give us Lemma 10.

Lemma 20. *[18, Lemma 20]*

$$T_1^2 = \frac{O(1)}{(1-(\gamma_d + L\gamma_p))^2} n^2 \nu_k \mu_0.$$

Proof. To obtain the result, we follow [18] in applying Lemmas 15 and 19 along with the fact that $(a+b)^2 \leq 2a^2 + 2b^2$, which gives

$$\begin{aligned} T_1^2 \leq & \left(2\eta_1(\theta_k T_2 + T_3 + T_4) + \sqrt{T_5}\right)^2 \\ \leq & \ 8(\theta_k T_2 + T_3 + T_4)^2 + 2T_5 \\ \leq & \ 8(\theta_k T_2 + T_3 + T_4)^2 + 2||\hat{S}_k^{-1/2}(R_k^c + r_k^c)||^2 \\ & + 4\theta_k^2 \langle \tilde{\mathbf{x}}_k - \mathbf{x}_*, \tilde{\mathbf{z}} - \mathbf{z}_* \rangle \\ & + 4\theta_k T_2 T_3 + 4T_3^2 + 4\theta_k T_2 T_4 \\ \leq & \ \frac{O(1)}{(1-(\gamma_d + L\gamma_p))^2} n^2 \nu_k \mu_0 + O(n^2 \nu_k \mu_0). \end{aligned}$$

□

Therefore,

$$||H_{\mathbf{p}_k}(\Delta \mathbf{x}_k, \Delta \mathbf{z}_k)|| \leq \frac{1}{2} T_1^2 = \frac{O(1)}{(1-(\gamma_d + L\gamma_p))^2} n^2 \nu_k \mu_0$$

by Lemmas 12 and 20.

References

[1] Ilan Adler and Farid Alizadeh. *Primal-dual interior point algorithms for convex quadratically constrained and semidefinite optimization problems.* Rutgers University. Rutgers Center for Operations Research [RUTCOR], 1995.

[2] Farid Alizadeh, Jean-Pierre A Haeberly, and Michael L Overton. Primal-dual interior-point methods for semidefinite programming: convergence rates, stability and numerical results. *SIAM Journal on Optimization*, 8(3):746–768, 1998.

[3] Peter Bürgisser, Michael Clausen, and Mohammad A Shokrollahi. *Algebraic complexity theory*, volume 315. Springer Science & Business Media, 2013.

[4] PAM Casares and MA Martin-Delgado. A quantum interior-point predictor-corrector algorithm for linear programming. *arXiv preprint arXiv:1902.06749*, 2019.

[5] Shantanav Chakraborty, András Gilyén, and Stacey Jeffery. The power of block-encoded matrix powers: improved regression techniques via faster Hamiltonian simulation. *arXiv preprint arXiv:1804.01973*, 2018.

[6] Jacques Faraut. Analysis on symmetric cones. *Oxford mathematical monographs*, 1994.

[7] Leonid Faybusovich. Linear systems in jordan algebras and primal-dual interior-point algorithms. *Journal of computational and applied mathematics*, 86(1):149–175, 1997.

[8] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019.

[9] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[10] Christoph Helmberg, Franz Rendl, Robert J Vanderbei, and Henry Wolkowicz. An interior-point method for semidefinite programming. *SIAM Journal on Optimization*, 6(2):342–361, 1996.

[11] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, (4):373–395, 1984.

[12] Iordanis Kerenidis and Anupam Prakash. Quantum recommendation systems. *arXiv preprint arXiv:1603.08675*, 2016.

[13] Iordanis Kerenidis and Anupam Prakash. A quantum interior point method for LPs and SDPs. *arXiv preprint arXiv:1808.09266*, 2018.

[14] Iordanis Kerenidis and Anupam Prakash. Quantum gradient descent for linear systems and least squares. *Physical Review A*, 101(2):022316, 2020.

[15] Iordanis Kerenidis, Anupam Prakash, and Daniel Szilagyi. A quantum interior-point method for second-order cone programming. 2019.

[16] Leonid G Khachiyan. Polynomial algorithms in linear programming. *USSR Computational Mathematics and Mathematical Physics*, 20(1):53–72, 1980.

[17] Masakazu Kojima, Susumu Shindoh, and Shinji Hara. Interior-point methods for the monotone semidefinite linear complementarity problem in symmetric matrices. *SIAM Journal on Optimization*, 7(1):86–125, 1997.

[18] Lu Li and Kim-Chuan Toh. A polynomial-time inexact interior-point method for convex quadratic symmetric cone programming. *J. Math. Ind*, 2:199–212, 2010.

[19] Renato DC Monteiro. Primal–dual path-following algorithms for semidefinite programming. *SIAM Journal on Optimization*, 7(3):663–678, 1997.

[20] Renato DC Monteiro and Takashi Tsuchiya. Polynomial convergence of primal-dual algorithms for the second-order cone program based on the mz-family of directions. *Mathematical programming*, 88(1):61–83, 2000.

[21] Yurii E Nesterov and Arkadi Nemirovskii. A general approach to polynomial-time algorithms design for convex programming. *Report, Central Economical and Mathematical Institute, USSR Academy of Sciences, Moscow*, 1988.

[22] Yurii E Nesterov and Arkadi Nemirovskii. *Interior-Point Polynomial Algorithms in Convex Programming*, volume 13. SIAM, 1995.

[23] Yurii E Nesterov and Michael J Todd. Self-scaled barriers and interior-point methods for convex programming. *Mathematics of Operations Research*, 22(1):1–42, 1997.

[24] SH Schmieta and Farid Alizadeh. Associative and jordan algebras, and polynomial time interior-point algorithms for symmetric cones. *Mathematics of Operations Research*, 26(3):543–564, 2001.

[25] SH Schmieta and Farid Alizadeh. Extension of primal-dual interior point algorithms to symmetric cones. *Mathematical Programming*, 96(3):409–438, 2003.

[26] Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.

[27] Jos F Sturm. Similarity and other spectral relations for symmetric cones. *Linear Algebra and its applications*, 312(1-3):135–154, 2000.

[28] Michael J Todd, Kim-Chuan Toh, and Reha H Tütüncü. On the Nesterov–Todd direction in semidefinite programming. *SIAM Journal on Optimization*, 8(3):769–796, 1998.

[29] Takashi Tsuchiya. A polynomial primal-dual path-following algorithm for second-order cone programming. *Research Memorandum*, 649, 1997.

[30] Yin Zhang. On extending some primal–dual interior-point algorithms from linear programming to semidefinite programming. *SIAM Journal on Optimization*, 8(2):365–386, 1998.

[31] Guanglu Zhou and Kim-Chuan Toh. Polynomiality of an inexact infeasible interior point algorithm for semidefinite programming. *Mathematical programming*, 99(2):261–282, 2004.