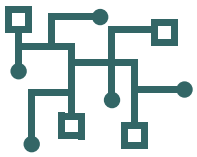

ISE

Industrial and
Systems Engineering

An Inexact-Feasible Quantum Interior Point Method for Semidefinite 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-008

LEHIGH
UNIVERSITY

A Feasible-Inexact Quantum Interior Point Method for Semidefinite Optimization

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

April 29, 2021

Abstract

We present a provably convergent quantum interior point method for semidefinite optimization problems, building on recent advances in quantum linear system solvers. The quantization of classical interior point methods is the subject of several recent papers in the literature. We compare the theoretical performance of classical and quantum interior point methods with respect to various input parameters, concluding that based on the current state of the art, our algorithm is the first convergent QIPM that provides a speedup in terms of the size of the problem.

1 Introduction

We develop a quantum interior point method (QIPM) for the solution of semidefinite optimization problems (SDOPs). Letting $b \in \mathbb{R}^m$, matrices $A^{(1)}, \dots, A^{(m)}, C \in \mathcal{S}^n$, where $\mathcal{S}^n$ is the subspace of $n \times n$ symmetric matrices, we consider the primal SDOP given as

$$z_P = \inf_X \left\{ \operatorname{tr}(CX) : \operatorname{tr}(A^i X) = b_i,\ \forall i \in [m], X \succeq 0 \right\} \tag{1}$$

where where $\operatorname{tr}(\cdot)$ denotes the trace of a symmetric matrix, $[m] = \{1, \dots, m\}$, and $U \succeq V$ indicates that $U - V$ is a symmetric positive semidefinite matrix. We further assume that the matrices $A^{(1)}, \dots, A^{(m)}$ are linearly independent. Letting $S \in \mathcal{S}$ denote the slack matrix of the dual problem, i.e.,

$$S = C - \sum_{i \in [m]} y_i A^{(i)} \succeq 0, \tag{2}$$

the associated dual problem is given as

$$z_D = \sup_{y,S} \left\{ b^\top y : \sum_{i=1}^m y_i A^i + S = C,\ S \succeq 0, y \in \mathbb{R}^m \right\}. \tag{3}$$

Although duality results are generally weaker for SDO when compared to linear optimization, if strong duality holds optimal solutions exist for both the primal and dual SDOP, and their optimal objective values are equal, i.e., $z_P = z_D$.

In classical computing, interior point methods (IPMs) are algorithms that are able to solve convex optimization problems, and in particular semidefinite optimization (SDO) problems in polynomial time. This dates back to the ellipsoid algorithm [26] for LOPs. Karmarkar improved on the complexity of the ellipsoid method when he presented his interior point method (IPM) for LOPs in [20]. The first polynomial time IPM for SDOPs is attributed to Nesterov and Nemirovskii [34, 35]. Their framework employs efficiently-computable self-concordant barrier functions.

In turn, SDO provides a framework that allows to formulate keystone problems in control [6], statistics, information theory [39], machine learning [28, 49], finance [12, 50], an most notably in Quantum Information

Science [14, 48], to name a few. Additionally, SDO can provide tight approximations for various combinatorial optimization problems [16]. SDOPs are attractive since they exhibit practical efficiency [2, 42, 44], tractability [1, 34]. Further, for more theoretical considerations, SDO can be used to study the properties of convex optimization problems [6]. Linear optimization problems (LOPs) are a special case of SDOPs in which each of the constraint matrices is a diagonal matrix. Considering the vast number of applications of SDOPs, it is natural to ask if quantum computers can accelerate their solution. Several works have investigated this avenue of research, which we discuss next.

1.1 Literature Review

As an alternative to using interior point methods to solve SDOPs, quantized variants of the the classical matrix multiplicative weights update (MWU) algorithm of Arora and Kale [3] have been developed with notable gains. The running time of the classical MWU method is given by

$$\mathcal{O}\left(nms \cdot \text{poly}\left(\frac{Rr}{\epsilon}\right)\right),$$

where s denotes the maximum number of non-zero entries per row, R is an upper bounds on the trace of an optimal primal solution, r is an upper bound on the ℓ_1-norm of the dual solution, and ϵ is an additive error to which the optimal objective value is approximated. The general schema of MWU algorithms is to alternate between candidate solutions to the primal and dual SDO problems, but without the solving of linear systems.

Brandão and Svore [8], and van Apeldoorn et al. [47] provided the first quantum SDO solvers based on the Arora-Kale framework. These efforts were subsequently improved by [17, 46], who were able to utilize Gibbs sampling in order to reduce the running time of QMWU algorithms to:

$$\tilde{\mathcal{O}}\left(\left(\sqrt{m}+\sqrt{n}\frac{Rr}{\epsilon}\right)s\left(\frac{Rr}{\epsilon}\right)^4\right).$$

One can observe that these methods achieve running times with a more favorable dependence on m and n in comparison to classical IPM solvers, their polynomial dependence on the parameters R, r and $1/\epsilon$ is exponentially slower than classical IPMs, which depend logarithmically on these quantities. Additionally, this running time depends on $1/\epsilon$, meaning if ϵ is part of the input, the running time is not polynomial in the typical sense.

Not surprisingly, there have been well-known efforts to develop Quantum IPMs (QIPMs) for SDO. The QIPM presented by Kerenidis and Prakash [23] initiated the research direction of quantizing interior point methods to solve SDOPs. The key bottleneck of classical interior point methods for SDO comes from solving the Newton linear system in each iteration. To improve the efficiency of this step, the authors construct block encodings of the Newton linear system matrix. With the use of quantum random access memory (QRAM), the system can be efficiently constructed, and subsequently solved in time polylogarithmic in n. As the solution of the Newton linear system is the most expensive step in classical IPMs, the hope is to obtain a quantum advantage. The algorithm presented in [23] exhibits a worst cast running time of

$$\tilde{O}\left(\frac{n^{2.5}}{\xi^2}\mu\kappa^3 \log\left(\frac{1}{\epsilon}\right)\right)$$

for SDOs, where ϵ is the optimality gap tolerance to which we solve the SDOP, ξ is a feasibility tolerance, κ is an upper bound for the condition number of the Newton systems, and μ is upper bounded by the largest Frobenius norm of the Newton systems. The term $\tilde{O}\left(\frac{n^2\kappa^2}{\xi^2}\right)$ comes from a tomography subroutine that is used to map the quantum-mechanical encoding of the solution of the linear system, to a classical description used to construct the subsequent iterate. This reconstruction is performed in each step to ℓ_2-norm error ξ/κ. When this algorithm is applied to solve LOPs, the running time is

$$\tilde{O}\left(\frac{n^{1.5}}{\xi^2}\mu\kappa^3 \log\left(\frac{1}{\epsilon}\right)\right).$$

Similar ideas have been used in other recent papers [24, 10], all of which follow the same structure: a classical interior point method is applied, but the Netwon linear system (or equivalent) is solved using a quantum linear system algorithm in an effort at improving the running time. The solution of the linear system is extracted from the quantum computer via tomography. The analysis of the algorithms requires nontrivial machinery and has led to interesting developments. However, the analysis of [23] is heavily based on classical exact IPMs, and does not account for some challenges that arise when translating those algorithms to the quantum setting. Similar challenges are found in [24, 10]. These challenges are discussed below, and addressed in this paper for the specific case of semidefinite optimization.

The QIPM of [23] directly quantizes the classical IPM described in [5]. This leads to two major issues. The first is that this algorithm does not guarantee that the solutions to the Newton linear system remain symmetric [29]. As a consequence, the algorithm described in [23] is not guaranteed to converge when applied to SDOPs. In the case of LOPs, symmetry is not an issue as all of the matrices are diagonal, yet with SDOPs, additional safeguards must be employed to guarantee that the resulting solution will be symmetric; numerous techniques have been proposed for this purpose. The use of scaling matrices in order to provide primal-dual symmetric search directions has been well studied in the classical literature, and these search directions are typically classified among the families of search directions introduced by Kojima, Shindoh, and Hara [27], Monteiro and Zhang [30, 31, 32, 51], Monteiro and Tsuchiya [33], and Tseng [45]. We refer the reader to an overview of these search directions by Todd [29].

The second major issue is that the analysis of the IPM in [5] assumes that the Newton linear systems are solved exactly. This cannot be done in the quantum setting, because nonnegligible errors are introduced in the tomography step, even if the quantum linear systems algorithm can solve the problem with high precision. Notably, if a classical exact-feasible IPM is use as the foundation in a straightforward manner, the primal and dual directions resulting from tomography are not orthogonal, therefore the convergence proof of [5] no longer applies[1]. To ensure convergence when the search directions are not exact, we must rely on *infeasible inexact* IPMs.

Augustino et al. [4] subsequently devised the first provably convergent QIPM for SDO by quantizing the classical Inexact-Infeasible Interior Point Method for SDO of Zhou and Toh [52]. By using residual terms to account for the inexactness introduced by quantum linear system solvers, they are able to address many issues arising from the challenge of quantizing interior point methods that were overlooked by previous efforts in the literature. Further, they provide results on formulating, loading and solving the Newton linear systems that arise when using the AHO [1], HKM (independently discovered by Monteiro [31], Helmberg et al. [19] and Kojima et al. [27]), and NT [34] directions. Their algorithm has an overall running time, when using the HKM direction, of

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

where $\rho > 0$ is the size of the initial solution and is generally considered a constant in many papers (i.e., it is often ignored in the running time analysis). The analysis identifies three major challenges hindering the development of efficient QIPMs. Though convergent, using inexact-infeasible IPMs as a foundation leads to an iteration bound with a dependence on n of $O(n^2)$ compared to the $O(\sqrt{n})$ dependence exhibited by feasible IPMs. This is further compounded by the fact that inexactness of the search direction compels one to introduce a dependence between the maximum tomography error at each iteration and the problem parameters, contributing a factor $O(\frac{1}{\epsilon}n^4\varrho^2)$, where ϱ is the size of the intermediate solutions of the Newton linear systems. They show in the paper that $\varrho = O(\kappa\rho n^{1.5})$, thus making the greatest contribution to the overall running time. Second, the quadratic dependence on the reciprocal of the precision of the tomography subroutine plays an important role: if the dependence could be reduced to linear, the factor ϱ^2 would become ϱ, immediately yielding a noticeable speedup. Finally, due to use of a QLSA for the solution of the Newton linear system, we pick up a running time dependence on the condition number κ, and it is known that κ can grow very large (in fact, as discussed in this paper, $\kappa \to \infty$ as we approach optimality) when solving SDOPs. The II-QIPM has better dependence on $1/\epsilon$ than the quantum MWU, but this comes at a cost

[1]Without the assumption $\mathrm{tr}(dSdY) = 0$, Lemma 6.3 in [23] fails, and it is not clear how to amend the subsequent analysis using the same framework (classically or in the quantum setting).

of much worse dependence on other parameters, most notably n and κ. Compared to classical IPM, there does not seem to be an advantage in any parameter: classical IPMs (with running time $O(n^{6.5}\log 1/\epsilon)$ on dense problems) are still superior to quantum algorithms for virtually every classical application. This was also observed in [7] for a specific application in combinatorial optimization. Hence, the inability to directly quantize exact-feasible IPMs, and the overall running time of inexact-infeasible QIPMs motivates the study of quantizing inexact, but feasible, interior point methods.

1.2 Contributions of this paper

This paper develops the first convergent QIPM for SDO to provide a speedup in terms of the size of the problem n. By using the nullspace representation of the Newton linear system, we are able to quantize an Inexact-Feasible algorithm which converges to an ϵ-approximate solution to an SDOP in $O\left(\sqrt{n}\log\left(\frac{1}{\epsilon}\right)\right)$ iterations. That is, we define the primal and dual search directions ΔX and ΔS as linear combinations of the elements of two bases that are orthogonal to one another. In this way, we can eschew the need to use the inexact-infeasible IPM framework as a foundation, as we display that substituting in these basic representations of our search directions allows us to solve a Newton system which always has a strictly complementary solution regardless of the errors introduced from our use of QSLA.

In this preliminary technical report, we present the first correct QIPM for SDO, as well as for linear optimization (LO). This of course opens the door for the use of Quantum Computing on the large number of applications in the areas mentioned above. Also, it provides an alternative way for Quantum Computers to address the approximate solution of combinatorial optimization problems. The running time of the algorithm presented in this work is

$$\tilde{O}\left(\frac{n^{2.5}}{\epsilon}\varrho^2\kappa\right).$$

We find that we achieve significant speedups in terms of n, at the cost of linear dependence on the condition number κ. Thus an open question is whether or not QIPMs can be implemented without utilizing an algorithmic framework that applies tomography in every iteration.

The rest of this paper is organized as follows. In Section 2, we introduce our notation, some necessary concepts in linear algebra, and basic quantum procedures. In Section 3 we discuss the classical interior point method. Section 4 provides technical results that are crucial to the convergence analysis. In Section 5 we discuss its quantization, providing a theoretical analysis of the running time for the Quantum Interior Point Method. Section 6 concludes the paper.

2 Preliminaries

We denote by $A \otimes B$ the tensor product of two matrices. Given two vectors x, y, we denote by $x \circ y$ the concatenation of the two vectors. For $a \in \mathbb{R}^n$, we denote its amplitude encoding by $|a\rangle$, defined as

$$|a\rangle = \frac{1}{\|a\|}\sum_{j\in[n]} a_j |j\rangle .$$

Notice that $|a\rangle$ is a $(\log n)$-qubit state; we assume that the sizes of all spaces are powers of 2 for simplicity. All logarithms are base 2. The smallest and largest singular values of a matrix A are denoted $\sigma_{\min}(A), \sigma_{\max}(A)$, and the smallest and largest eigenvalues are denoted $\lambda_{\min}(A), \lambda_{\max}(A)$. The condition number of A is $\kappa(A) = \frac{\lambda_{\max}(A)}{\lambda_{\min}(A)}$.

2.1 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:

$$|b\rangle \to \frac{A|b\rangle}{\|A|b\rangle\|}.$$

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., [11].

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. [11] 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 [11] 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 [18] 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 [23, 11].

2.2 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 [11, 15], which provide improvements over the framework discussed in [21, 23].

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*

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

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

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

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

yielding

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

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 [11] for an extensive discussion on this topic.

Proposition 1 (Lemma 50 in [15])**.** *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 $O(\text{poly}(w \log \frac{1}{\xi}))$ 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 $O(\text{poly}(w \log \frac{1}{\xi}))$ and such that $U_R^\dagger U_L$ is an $(\|A\|_F, w+2, \xi)$-block-encoding of A.

Proposition 2 (Lemma 52 in [15]). *(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 [11]). *(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 [11]). *(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 [11]). *(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 [11]). *(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 1 (Theorem 30 in [11]). *(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 [11])**.** *(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 $O(\mathrm{poly}(\log n, \log\frac{1}{\xi}))$.

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

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

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

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

□

2.3 Extracting the solution of a linear system: tomography algorithm

In each iteration of our IF-QIPM, we solve a linear system of equations (known as the Newton linear system) to obtain search directions to progress to the next iterate. Due to the structure of the Newton linear system presented in this work, the solutions, Δy and $\Delta\zeta$, are encoded as quantum states, classical description is necessary to construct the Newton linear system for the subsequent iteration. Hence, in order to update the current solutions to the primal and dual SDOPs, X and (y, S), we require a procedure to map $|\Delta y\rangle$ and

$|\Delta\zeta\rangle$ to a classical solution pair $(\Delta y, \Delta\zeta)$. For this task, we use the state tomography algorithm of [23]. In our setting, this is faster than other tomography (e.g., [25, 38]), thanks to the assumption that we can apply a unitary that prepares the state, and its controlled version. We report the full algorithm for completeness.

Algorithm 1 Vector state tomography algorithm [23]

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

1. **Amplitude estimation**
   (a) Measure $N = \frac{36m\ln m}{\delta^2}$ copies of $|x\rangle$ in the standard basis
   (b) Obtain estimates $p_i = \frac{n_i}{N}$ where n_i is the number of times outcome i is observed.
   (c) Store $\sqrt{p_i}$, $i \in [m]$ in QRAM data structure
   (d) Efficiently prepare $|p\rangle = \sum_{i\in[m]} \sqrt{p_i}|i\rangle$.
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
   (c) Obtain
   $$\frac{1}{2}\sum_{i\in[m]} [(x_i + \sqrt{p_i}|0,i\rangle + (x_i - \sqrt{p_i})|1,i\rangle].$$
   (d) 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 $b \in \{0,1\}$.
   (e) Set $\sigma_i = 1$ if $n(0,i) > 0.4p_iN$ and -1 otherwise.
3. Output the unit vector $\tilde{x}$ with $\tilde{x}_i = \sigma_i\sqrt{p_i}$.

The following result from [23] certifies the correctness of Algorithm 1.

Theorem 2 (Thrm. 4.3 in [23])**.** *Algorithm 1 produces an estimate $\tilde{x} \in \mathbb{R}^m$ with $||\tilde{x}||_2 = 1$ such that $||\tilde{x} - x||_2 \leq \sqrt{7}\xi$ with probability at least $(1 - \frac{1}{m^{0.83}})$. The running time of the algorithm is $\tilde{O}(mT_U/\delta^2)$, where T_U is the time required by unitary U.*

We can summarize the role the tomography algorithm plays in QIPMs as follows. Solving the Newton linear system outputs a quantum state $|\Delta y \circ \Delta\zeta\rangle$, and we wish to recover a classical estimate $\overline{\Delta y}, \overline{\Delta\zeta}$, such that

$$\|(\Delta y - \overline{\Delta y}) + (\Delta\zeta - \overline{\Delta\zeta})\| \leq \xi.$$

To accomplish this, we observe a large number of samples from $|\Delta y \circ \Delta\zeta\rangle$ to estimate the absolute value of its entries. Subsequently, using the controlled state preparation subcircuit and interference with Hadamard gates, we create a state that allows to estimate the sign of each entry. Notice that the error bound is relative to the normalized state $|x\rangle$; several parts of the QIPM require an error bound with respect to the unnormalized real vector x, therefore we have to adjust the tolerance ξ accordingly.

3 Primal and Dual SDOs and the Central Path

Recall that the matrices $A^{(1)}, \ldots, A^{(m)}$ are linearly independent by assumption, and $S \in \mathcal{S}$ is the slack matrix of the dual problem, see (2). We denote the feasible sets of (1) and (3) by

$$\mathcal{P} = \left\{ X \middle| \operatorname{tr}(A^{(k)}X) = b_k \ \forall k \in [m], X \succeq 0 \right\}$$
$$\mathcal{D} = \left\{ (y, S) \;\middle|\; \sum_{k\in[m]} y_k A^{(k)} - S = C, S \succeq 0, y \in \mathbb{R}^m \right\}.$$

For a feasible IPM we must assume that a strictly feasible pair X and (y, S) with $X \succ 0$ and $S \succ 0$ exists, i.e., the interior point condition is satisfied [13]. It is known that with the self-dual embedding model this condition may be assumed without loss of generality [13]. With the interior point condition satisfied, it is guaranteed that the primal and dual optimal sets:

$$\mathcal{P}^* = \{X \in \mathcal{P} | \operatorname{tr}(CX) = z_{P^*}\}$$
$$\mathcal{D}^* = \left\{(y, S) \in \mathcal{D} \;\middle|\; b^\top y = z_{D^*}\right\}$$

are nonempty and bounded. Hence, there exists an optimal primal-dual pair with zero duality gap. In particular, we have optimal solutions (X^*) and (y^*, S^*) satisfying

$$\operatorname{tr}(CX^*) - b^\top y^* = \operatorname{tr}(X^*S^*) = 0, \tag{4}$$

which implies $X^*S^* = S^*X^* = 0$ as X^* and S^* are symmetric positive semidefinite matrices. However, for primal-dual IPMs, the complementarity condition $XS = 0$ is perturbed to:

$$XS = \nu I, \tag{5}$$

where I is the $n \times n$ identity matrix, and $\nu > 0$ is the so-called central path parameter, which is progressively reduced to zero in the course of the algorithm.

For all $\nu > 0$, assuming the interior point condition and linear independence of the matrices $A^{(i)}$, the central path equation system

$$\begin{aligned} \operatorname{tr}(A^{(i)}X) &= b_i \ \forall i \in [m], \ X \succ 0 \\ \sum_{i\in[m]} y_i A^{(i)} + S &= C, \ S \succ 0 \\ XS &= \nu I, \end{aligned} \tag{6}$$

has a unique solution [34]. The set of solutions for all $\nu > 0$ gives the central path for the primal and dual SDOPs. In IPMs we aim to follow the central path as $\nu \to 0$, i.e., as we approach optimality. However, in reality we simply seek to stay close to the path.

3.1 Symmetrizing the Newton System

As has been extensively studied in the literature of IPMs (see, e.g., [1, 36, 37]), the Newton steps ΔS and ΔX have to be symmetric matrices. More specifically, even though ΔS is guaranteed to be symmetric by the definition of a dual feasible solution, there is no symmetric ΔX that solves system. Thus, we need a different approach to guarantee symmetry.

In an effort to generalize the scaling methods required for primal-dual symmetry to the quantum setting, following Zhang [51], we define the linear transformation $H_P(M)$ that symmetrizes a matrix M for a given invertible matrix P:

$$H_P(M) = \frac{1}{2}\left[PMP^{-1} + P^{-\top}M^\top P^\top\right]. \tag{7}$$

Observe that $H_P(M) = \nu I \iff M = \nu I$; we can then write the central path equations in symmetric form as: $H_P(XS) = \nu I$. In this light, we can also symmetrize the Newton system $X\Delta S + S\Delta X = \nu I - SX$ as

$$H_P(X\Delta S + S\Delta X) = \sigma\nu I - H_P(XS). \tag{8}$$

Finally, equation (8) can be expressed as:

$$\begin{aligned} P(X\Delta S + \Delta X S)P^{-1} + P^{-\top}(\Delta S X + S\Delta X)P^{\top} \\ = 2\nu I - PXSP^{-1} - P^{-\top}SXP^{\top}. \end{aligned} \tag{9}$$

We then need to choose P to obtain specific instances of this system. We present results involving three possible choice of P: $P = I$, the AHO direction [1]; $P = S^{1/2}$, the HKM direction [19]; and $P = W^{-1/2}$, where W is the Nesterov-Todd [37] scaling matrix, defined as:

$$\begin{aligned} W &= S^{-1/2}(S^{1/2}XS^{1/2})^{1/2}S^{-1/2} \\ &= X^{1/2}(X^{1/2}SX^{1/2})^{-1/2}X^{1/2}. \end{aligned} \tag{10}$$

3.2 The Nullspace Representation of the Newton Linear System

In what follows, we make extensive use of the matrix functions **svec** and **smat**, which are defined as follows.

Definition 2. *For $U \in \mathbb{R}^{n\times n}$, $\mathbf{svec}(U) \in \mathbb{R}^{\frac{1}{2}n(n+1)}$ is given by*

$$\mathbf{svec}(U) = \left(u_{11}, \sqrt{2}u_{21}, \ldots, \sqrt{2}u_{n1}, u_{22}, \sqrt{2}u_{32}\ldots, \sqrt{2}u_{n2}, \ldots, u_{nn}\right)^{\top}.$$

Further, the operator **smat** *is the inverse operator of* **svec**. *That is,*

$$\mathbf{smat}\left[\mathbf{svec}(U)\right] = U.$$

The definition of the **svec** operator gives rise to the definition of the *symmetric* Kronecker product.

Definition 3. *The symmetric Kronecker product can be defined for any two (not necissarily symmetric) matrices $G, H \in \mathbb{R}^{n\times n}$ as a mapping on a vector $\boldsymbol{svec}(V)$ where $V \in \mathcal{S}^{n\times n}$:*

$$(G \otimes_s H)\boldsymbol{svec}(V) = \frac{1}{2}\boldsymbol{svec}(HVG^{\top} + GVH^{\top}).$$

From Schake [40], the symmetric Kronecker product satisfies the following properties which we will use in our analysis:

Proposition 9. *1. $(\alpha A) \otimes_s B = A \otimes_s (\alpha B) = \alpha(A \otimes_s B)$ for all $\alpha \in \mathbb{R}$, $A, B \in \mathbb{R}^{n\times n}$*

2. $(A + B) \otimes_s C = A \otimes_s C + B \otimes_s C$ for all $A, B, C \in \mathbb{R}^{n\times n}$

3. $A \otimes (B + C) = A \otimes_s B + A \otimes_s C$ for all $A, B, C \in \mathbb{R}^{n\times n}$

4. $(A \otimes_s B)(C \otimes_s D) = \frac{1}{2}(AC \otimes_s BD + AD \otimes_s BC)$ for all $A, B, C, D \in \mathbb{R}^{n\times n}$

Let

$$\begin{aligned} \mathcal{A}^T &= [\mathbf{vec}(A^{(1)})\mathbf{vec}(A^{(2)})\cdots\mathbf{vec}(A^{(m)})], \text{ and} \\ \mathcal{A}_s^T &= [\mathbf{svec}(A^{(1)})\mathbf{svec}(A^{(2)})\cdots\mathbf{svec}(A^{(m)})]. \end{aligned}$$

Following Todd et al. [43], we can rewrite the Newton linear system using the **svec** notation as follows:

$$\begin{pmatrix} 0 & \mathcal{A}_s & 0 \\ \mathcal{A}_s^{\top} & 0 & \mathcal{I} \\ 0 & \mathcal{E} & \mathcal{F} \end{pmatrix} \begin{pmatrix} \Delta y \\ \mathbf{svec}(\Delta X) \\ \mathbf{svec}(\Delta S) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \mathbf{svec}(R_c) \end{pmatrix} \tag{11}$$

where $\mathcal{I}$ is the identity matrix of order $\frac{n(n+1)}{2}$ and

$$\begin{aligned}\mathcal{E} &= P \otimes_s P^{-\top} S,\\ \mathcal{F} &= PX \otimes_s P^{-\top},\\ R_c &= \sigma\nu I - H_p(XS).\end{aligned}$$

One can note that the matrices $\mathcal{E}$ and $\mathcal{F}$ are nonsingular whenever X and S are positive definite matrices [43]. We have:

$$\mathcal{E} = P \otimes_s P^{-\top} S = (I \otimes_s P^{-\top} S P^{-1})(P \otimes_s P) \tag{12a}$$

$$\mathcal{F} = PX \otimes_s P^{-\top} = (PXP^{\top} \otimes_s I)(P^{-\top} \otimes_s P^{-\top}), \tag{12b}$$

where the equalities follow from the properties of the symmetric Kronecker product detailed earlier.

For our work, we slightly modify the system (11) by introducing a residual term $r_c \in \mathcal{S}^{n\times n}$ which captures the errors introduced by QLSA.

$$\begin{pmatrix} 0 & \mathcal{A}_s & 0 \\ \mathcal{A}_s^{\top} & 0 & \mathcal{I} \\ 0 & \mathcal{E} & \mathcal{F} \end{pmatrix} \begin{pmatrix} \Delta y \\ \mathbf{svec}(\Delta X) \\ \mathbf{svec}(\Delta S) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \mathbf{svec}(R_c + r_c) \end{pmatrix} \tag{13}$$

The ensuing result from [43] establishes the uniqueness of the solution to the system (13).

Theorem 3 (Thrm. 3.1 in [43])**.** *Suppose X and S are positive definite. Then the system of equations* (13) *has a unique solution $(\Delta X, \Delta y, \Delta S) \in \mathcal{S}_+^n \times \mathbb{R}^m \times \mathcal{S}_+^n$ if $\mathcal{E}^{-1}F$ is positive definite (not necissarily summetric). In particular, this holds when X, S and $H_P(XS)$ are positive semidefinite.*

Proof. In what follows, positive definiteness does not imply symmetry. We seek to show that the system

$$\begin{pmatrix} 0 & \mathcal{A}_s & 0 \\ \mathcal{A}_s^{\top} & 0 & \mathcal{I} \\ 0 & \mathcal{E} & \mathcal{F} \end{pmatrix} \begin{pmatrix} \Delta y \\ \mathbf{svec}(\Delta X) \\ \mathbf{svec}(\Delta S) \end{pmatrix} = 0 \tag{14}$$

is satisfied only by the trivial solution. From (12a) it follows that $\mathcal{E}$ is invertible. Hence, applying block Gaussian elimination to (13) yields the Schur complement equation:

$$(\mathcal{A}_s \mathcal{E}^{-1} \mathcal{F} \mathcal{A}_s^{\top}) \Delta y = 0. \tag{15}$$

By assumption, $\mathcal{E}^{-1}\mathcal{F} \succ 0$ and $\mathcal{A}$ has full row rank, implying that the matrix $\mathcal{A}_s \mathcal{E}^{-1} \mathcal{F} \mathcal{A}_s^{\top}$ is positive definite, therefore $\Delta y = 0$. Thus the second equation in (14) gives $\Delta S = -\mathbf{smat}(\mathcal{A}_s^{\top} \Delta y) = 0$ and the from the third equation it follows $\Delta X = -\mathcal{E}^{-1}\mathcal{F}\Delta S = 0$. This completes the proof. □

However, the Newton linear system as given by (13) cannot be solved directly using a quantum computer. Indeed, by using QLSA, there is no way to guarantee the first two block equations in this system can be satisfied exactly. Given the result of Lemma **??**, we can re-write the optimality conditions as

$$\begin{aligned} \Delta X &\in \mathcal{N}(\mathcal{A}_s) \\ \Delta S &\in \mathcal{R}(\mathcal{A}_s) \\ (P \otimes_s P^{-\top} S)\mathbf{svec}(\Delta X) + (PX \otimes P^{-\top})\mathbf{svec}(\Delta S) &= \mathbf{svec}(2\nu' I - PSXP^{-1} - P^{-\top} X S P^{\top}), \end{aligned} \tag{16}$$

where $\mathcal{N}(\mathcal{A}_s)$ denotes the nullspace of $\mathcal{A}_s$ and $\mathcal{R}(\mathcal{A}_s)$ denotes the rowspace of $\mathcal{A}_s$.

For $\mathcal{R}(\mathcal{A}_s)$, we can choose

$$\{\mathbf{svec}(A^{(1)})\mathbf{svec}(A^{(2)}) \cdots \mathbf{svec}(A^{(m)})\}$$

as our basis. Then, we can calculate a basis of $\mathcal{N}(\mathcal{A}_s)$ using either Gauss elimination or the QR-Factorization of $\mathcal{A}_s$. Given the fact that $\mathcal{A}_s \in \mathbb{R}^{m\times\frac{n(n+1)}{2}}$, one can observe $\mathcal{A}_s^\top \in \mathbb{R}^{\frac{n(n+1)}{2}\times m}$. The QR factorization of $\mathcal{A}_s^\top$ is defined as

$$\mathcal{A}_s^\top = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix} \begin{bmatrix} R \\ 0 \end{bmatrix},$$

where $Q_1 \in \mathbb{R}^{m\times\frac{n(n+1)}{2}}$ and $Q_2 \in \mathbb{R}^{\frac{n(n+1)}{2}\times\left(\frac{n(n+1)}{2}-m\right)}$. Then, it follows that the columns of Q_2 form a basis for the null space of $\mathcal{A}_s$. Hence, ΔX and ΔS can be written as

$$\mathbf{svec}(\Delta X) = \sum_{i=1}^{\frac{n(n+1)}{2}-m} \Delta\zeta_i Q_2^i = Q_2\Delta\zeta, \tag{17a}$$

$$\mathbf{svec}(\Delta S) = -\sum_{i=1}^{m} \Delta y_i \mathbf{svec}(A^{(i)}) = -\mathcal{A}_s^\top \Delta y \tag{17b}$$

where Q_2^i denotes the i^{th} column of Q_2.

The following result establishes the Newton linear system to be solved at each iteration of the IF-QIPM:

Theorem 4. *Let P be an appropriate scaling matrix to guarantee primal-dual symmetry and define*

$$\begin{aligned} \mathcal{E} &= (P \otimes_s P^{-\top} S), \\ \mathcal{F} &= (PX \otimes_s P^{-\top}), \\ R_c &= 2\sigma\nu' I - PXSP^{-1} - P^{-\top} SXP^\top. \end{aligned}$$

Then, letting $r_c \in \mathcal{S}^{n\times n}$ be a residual term which captures the errors introduced by QLSA, the Newton linear system for the IF-QIPM is given by

$$\begin{bmatrix} \mathcal{E}Q_2 & \mathcal{F}(-\mathcal{A}_s^\top) \end{bmatrix} \begin{bmatrix} \Delta\zeta \\ \Delta y \end{bmatrix} = \boldsymbol{svec}(R_c + r_c). \tag{18}$$

Proof. Substituting equations (17a) and (17b) into the left hand side of the third equation in system (13) yields yields

$$\begin{aligned} (P \otimes_s P^{-\top} S)\mathbf{svec}(\Delta X) + (PX \otimes_s P^{-\top})\mathbf{svec}(\Delta S) &= (P \otimes_s P^{-\top} S)(Q_2\Delta\zeta) + (PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top \Delta y) \\ &= [(P \otimes_s P^{-\top} S)Q_2]\Delta\zeta + [-(PX \otimes_s P^{-\top})\mathcal{A}_s^\top]\Delta y. \end{aligned}$$

□

Upon using QLSA to solve the system (18) for $(\Delta\zeta, \Delta y)$, we will need to map classical estimates $(\overline{\Delta\zeta}, \overline{\Delta y})$ of this quantum solution to a classical estimate $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$ in order to proceed to the next iteration. Defining $f(\overline{\Delta\zeta})$ and $f(\overline{\Delta y})$ by (17a) and (17b), respectively, there is a mapping

$$\mathcal{M} : (\overline{\Delta\zeta}, \overline{\Delta y}) \to (f(\overline{\Delta\zeta}), \overline{\Delta y}, f(\overline{\Delta y}))$$

from this classical estimate, to a point $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$. One can observe that the mapping we employ one-to-one. Indeed, by assumption $\mathcal{A}_s$, and consequently Q_2, are row-wise and column-wise full rank, respectively. Therefore, in equations (17a) and (17b), the quantities $\mathbf{svec}(\Delta X)$ and $\mathbf{svec}(\Delta S)$ are uniquely determined by $\Delta\zeta$ and Δy.

In solving the system (18) using QLSA, indeed Δy and $\Delta\zeta$ will each be calculated with some error. Yet, by using the bases of the nullspace and the rowspace to calculate ΔX and ΔS, we ensure that these search directions are always coming from orthogonal subspaces, regardless of the errors introduced by QLSA or the length of the stepsize. We formalize this result in the following proposition.

Proposition 10. *Let $(\overline{\Delta\zeta}, \overline{\Delta y})$ be our classical estimate of the solution to* (18)*. Then,*

$$\overline{\Delta\zeta} = \Delta\zeta + \xi_\zeta \text{ and } \overline{\Delta y} = \Delta y + \xi_y,$$

where ξ_ζ and ξ_y denote the errors introduced to our solution of the system (18) *via the use of QSLA. Letting $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$ be the solution to* (13) *induced by $(\overline{\Delta\zeta}, \overline{\Delta y})$, for any step size α, we have*

$$\mathcal{A}_s(\boldsymbol{svec}(X) + \alpha\boldsymbol{svec}(\overline{\Delta X})) = b, \text{ and } \mathcal{A}_s^\top(y + \alpha\overline{\Delta y}) + (\boldsymbol{svec}(S) + \alpha\boldsymbol{svec}(\overline{\Delta S})) = \boldsymbol{svec}(C).$$

Proof. First, note

$$\begin{aligned}
\mathcal{A}_s(\mathbf{svec}(X) + \alpha\mathbf{svec}(\overline{\Delta X})) &= \mathcal{A}_s X + \alpha\mathcal{A}_s\mathbf{svec}(\overline{\Delta X}) \\
&= \mathcal{A}_s\mathbf{svec}(X) + \alpha\mathcal{A}_s\mathbf{svec}(\overline{\Delta X}) \\
&= b + \alpha\mathcal{A}_s[Q_2(\overline{\Delta\zeta})] \\
&= b + \alpha\mathcal{A}_s[Q_2(\Delta\zeta + \xi_\zeta)] \\
&= b + \alpha[\mathcal{A}_s Q_2(\Delta\zeta + \xi_\zeta)] \\
&= b + \alpha[0 \cdot (\Delta\zeta + \xi_\zeta)] \\
&= b.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathcal{A}_s^\top(y + \alpha\overline{\Delta y}) + (\mathbf{svec}(S) + \alpha\mathbf{svec}(\overline{\Delta S})) &= [\mathcal{A}_s^\top y + \mathbf{svec}(S)] + [\mathcal{A}_s^\top \alpha\overline{\Delta y} + \alpha\mathbf{svec}(\overline{\Delta S})] \\
&= \mathbf{svec}(C) + \alpha[\mathcal{A}_s^\top \overline{\Delta y} + \mathbf{svec}(\overline{\Delta S})] \\
&= \mathbf{svec}(C) + \alpha[\mathcal{A}_s^\top(\overline{\Delta y} - \overline{\Delta y})] \\
&= \mathbf{svec}(C).
\end{aligned}$$

□

Having established the fact that our search directions computed from classical estimates of the quantum solution to (18) preserve primal and dual feasibility, we next certify the validity of using the system (18) to obtain a solution to the system (13). Further, we demonstrate that if the system (13) has a unique solution, than the system (18) does as well.

Proposition 11. *Suppose X and S are positive definite. Then, any solution $(\Delta\zeta, \Delta y)$ of the system* (18)*, provides a solution $(\Delta X, \Delta y, \Delta S)$ to the system* (13)*.*

Proof. Let $(\overline{\Delta\zeta}, \overline{\Delta y})$ be a solution to (18). Further, applying equations (17a) and (17b), let

$$\begin{aligned}
\mathbf{svec}(\overline{\Delta X}) &= \sum_{i=1}^{\frac{n(n+1)}{2}-m} \overline{\Delta\zeta_i} Q_2^i = Q_2\overline{\Delta\zeta}, \\
\mathbf{svec}(\overline{\Delta S}) &= -\sum_{i=1}^{m} \overline{\Delta y_i}\mathbf{svec}(A^{(i)}) = -\mathcal{A}_s^\top\overline{\Delta y}.
\end{aligned}$$

We seek to show that $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$ satisfies the system (13). For the third block equation in (13) we have

$$\begin{aligned}
\mathbf{svec}(R_c + r_c) &= [(P \otimes_s P^{-\top}S)Q_2]\overline{\Delta\zeta} + [(PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top)]\overline{\Delta y} \\
&= (P \otimes_s P^{-\top}S)(Q_2\overline{\Delta\zeta}) + (PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top\overline{\Delta y}) \\
&= (P \otimes_s P^{-\top}S)\mathbf{svec}(\overline{\Delta X}) + (PX \otimes_s P^{-\top})\mathbf{svec}(\overline{\Delta S}),
\end{aligned}$$

Similarly, we have

$$\mathcal{A}_s\mathbf{svec}(\overline{\Delta X}) = \mathcal{A}_s Q_2\overline{\Delta\zeta} = (\mathcal{A}_s Q_2)\overline{\Delta\zeta} = 0,$$

and

$$\mathcal{A}_s^\top \overline{\Delta y} + \mathcal{I}\mathbf{svec}(\overline{\Delta S}) = \mathcal{A}_s^\top \overline{\Delta y} + (-\mathcal{A}_s^\top \overline{\Delta y}) = \mathcal{A}_s^\top (\overline{\Delta y} - \overline{\Delta y}) = 0,$$

for the first and second block equations in (13), respectively. This completes the proof. □

Proposition 12. *Suppose X and S are positive definite. If $(\Delta\zeta, \Delta y)$ is a solution to the system (18), then this solution is unique.*

Proof. Suppose (in order to arrive at a contradiction) that the system (18) has solutions $(\overline{\Delta\zeta}, \overline{\Delta y})$ and $(\widetilde{\Delta\zeta}, \widetilde{\Delta y})$ with

$$(\overline{\Delta\zeta}, \overline{\Delta y}) \neq (\widetilde{\Delta\zeta}, \widetilde{\Delta y}).$$

Further, let $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$ and $(\widetilde{\Delta X}, \widetilde{\Delta y}, \widetilde{\Delta S})$ be the solutions to (13) resulting from $(\overline{\Delta\zeta}, \overline{\Delta y})$ and $(\widetilde{\Delta\zeta}, \widetilde{\Delta y})$, respectively. Recall that we have assumed the matrices $A^{(1)}, \ldots, A^m$ are linearly independent. Hence, $\mathcal{A}_s$ has full row rank and likewise, Q_2 has full column rank. As such, the mapping $\mathcal{M} : (\Delta\zeta, \Delta y) \to (\Delta X, \Delta y, \Delta S)$ is defined using the continuous linear equations (17a) and (17b) in which $\mathbf{svec}(\Delta X)$ is uniquely determined by $\Delta\zeta$ and $\mathbf{svec}(\Delta S)$ is uniquely determined by Δy, respectively. Thus, the mapping $\mathcal{M} : (\Delta\zeta, \Delta y) \to (\Delta X, \Delta y, \Delta S)$ is one-to-one, so for $(\overline{\Delta\zeta}, \overline{\Delta y}) \neq (\widetilde{\Delta\zeta}, \widetilde{\Delta y})$, we must have

$$(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S}) \neq (\widetilde{\Delta X}, \widetilde{\Delta y}, \widetilde{\Delta S}).$$

Applying Prop. 11, both $(\overline{\Delta X}, \overline{\Delta y}, \overline{\Delta S})$ and $(\widetilde{\Delta X}, \widetilde{\Delta y}, \widetilde{\Delta S})$ solve the system the system (13), meaning this system has multiple solutions. Yet, from Theorem 3, we get a contradiction as the system (13) can only have one solution so we must have

$$(\overline{\Delta\zeta}, \overline{\Delta y}) = (\widetilde{\Delta\zeta}, \widetilde{\Delta y}).$$

□

Theorem 5. *The pair (X, S) is a maximally complementary solution pair.*

Proof. □

Let us define the sets of *interior feasible solutions* by

$$F^0(\mathcal{P}) = \{X \in \mathcal{S}^n \ : \ A_i \bullet X = b_i, \ i = 1, \ldots, m, X \succ 0\}$$
$$F^0(\mathcal{D}) = \{(y, S) \in \mathbb{R}^m \times \mathcal{S}^n \ : \ \sum_{i=1}^m y_i A_i + S = C, S \succ 0\}.$$

Following the general theory of the inexact Newton method, we assume that the residual term r_c satisfies

$$\|r_c\|_F \leq \beta \|R_c\|_F \tag{19}$$

for some $\beta \in (0, 1)$. In this work we consider the narrow (or, Frobenius) neighborhood

$$\mathcal{N}_F(\gamma) = \left\{ (X, y, S) \in F^0(\mathcal{P}) \times F^0(\mathcal{D}) \middle| \|X^{1/2} S X^{1/2} - \nu I\|_F = \left[\sum_{i=1}^n (\lambda_i(XS) - \nu)^2 \right]^{1/2} \leq \gamma\nu \right\}.$$

Another popular alternative is the so called *negative infinity neighborhood* that is a *large neighborhood*, defined as

$$\mathcal{N}_\infty^-(1 - \gamma) = \{(X, y, S) \in F^0(\mathcal{P}) \times F^0(\mathcal{D}) | \lambda_{\min}(XS) \geq \gamma\nu\},$$

where $\gamma \in (0, 1)$. It is well known that classical feasible primal-dual path following IPMs that use the former neighborhood exhibit an iteration complexity of the order $O(\sqrt{n}L)$ whereas long-step IPMs, using the latter neighborhood, have iteration complexity $O(nL)$. However, in practice the long step algorithms tend to converge faster than the short step counterpart, which raises the question of whether or not the

same will hold true for QIPMs. In this work, we only conduct our analysis for the narrow (or Frobenius) neighborhood, so moving forward we define our centrality measure at a point $(X, S) \in \mathcal{S}^n_+ \times \mathcal{S}^n_+$ to be

$$d(X, S) = \|X^{1/2} S X^{1/2} - \nu I\|_F = \left[\sum_{i=1}^{n} (\lambda_i(XS) - \nu)^2\right]^{1/2}. \tag{20}$$

The following result from [32] plays a crucial role in the analysis required to establish polynomial convergence of our IF-QIPM.

Lemma 1 (Lemma 2.1 in [32])**.** *Suppose that $(X, S) \in \mathcal{S}^n_{++} \times \mathcal{S}^n_{++}$, $Q \in \mathbb{R}^{n\times n}$ is a nonsingular matrix and $\nu = \frac{X\bullet S}{n}$. Then:*

(a) $d(\widetilde{X}, \widetilde{S}) = d(X, S)$ where $\widetilde{X} = QXQ^\top$ and $\widetilde{S} = Q^{-\top} S Q^{-1}$.

(b) $d(X, S) \le \|H_Q(XS - \nu I)\|_F$ with equality holding if $QXSQ^{-1} \in \mathcal{S}^n$.

Proof. Our proof follows from that of [32]. *(a)*: First, due to the fact $\widetilde{X}\widetilde{S} = QXSQ^{-1}$, we have that XS and $\widetilde{X}\widetilde{S}$ are similar matrix which have the same spectrum. Hence,

$$d(\widetilde{X}, \widetilde{S}) = d(X, S)$$

since we can only express $d(X, S)$ in terms of the eigenvalues of XS.

From Lemma 3.3 of [31], for any $E \in \mathcal{S}^n$ and any nonsingular matrix $T \in \mathbb{R}^{n\times n}$ we have $\|E\|_F \le \|H_T(E)\|_F$. Then, let $E = X^{\frac{1}{2}} S X^{\frac{1}{2}} - \nu I$ and $T = QX^{\frac{1}{2}}$, the inequality follows from observing

$$H_T(E) = H_Q(XS - \nu I).$$

If however, $QXSQ^{-1} \in \mathcal{S}^n$, then

$$H_Q(XS - \nu I) = QXSQ^{-1} - \nu I$$

and thus

$$\begin{aligned}\|H_Q(XS - \nu I)\|_F = \|QXSQ^{-1} - \nu I\|_F &= \left[\sum_{i=1}^{n} \left(\lambda_i[QXSQ^{-1}] - \nu\right)^2\right]^{1/2} \\ &= \left[\sum_{i=1}^{n} (\lambda_i[XS] - \nu)^2\right]^{1/2} = d(X, S).\end{aligned}$$

□

4 Technical Results

In this section, we adapt the analysis of [32] to account for the inexactness of the complementarity condition, such that we can prove the polynomial convergence of the IF-QIPM presented in Section 5. Though in this work we chose the Nesterov-Todd direciton $P = W^{-1/2}$, the convergence analysis we perform is left in general terms of P, and holds for any member of the Monteiro and Zhang family of directions, which includes the AHO and HKM directions.

Following [32], in this section we assume that $(X, y, S) \in \mathcal{S}^n_{++} \times \mathbb{R}^m \times \mathcal{S}^n_{++}$ and that $P \in \mathbb{R}^{n\times n}$ is a nonsingular matrix. Additionally, we assume $(\Delta X, \Delta y, \Delta S)$ is a solution of the system

$$H_P(\Delta X S + X \Delta S) = \sigma\nu I - H_P(XS) + r_c \tag{21a}$$

$$\sum_{i=1}^{m} \Delta y A^{(i)} + \Delta S = C - S - \sum_{i=1}^{m} y_i A^{(i)} \tag{21b}$$

$$A^{(i)} \bullet \Delta X = b_i - A^{(i)} \bullet X, \quad \forall i \in [m]. \tag{21c}$$

for some $\sigma \in [0,1]$. Recall that $(\Delta X, \Delta y, \Delta S)$ is our classical estimate of the solution to the system (13) obtained from our classical estimate $(\Delta\zeta, \Delta y)$ of the solution to the quantum Newton linear system (18). That is,

$$(\Delta X, \Delta y, \Delta S) = \left(\mathbf{smat}(Q_2\zeta), \Delta y, -\mathbf{smat}(\mathcal{A}_s^\top \Delta y)\right).$$

Further, for $\alpha \in \mathbb{R}$ we define the quantities:

$$\widetilde{X} = PXP^\top, \qquad \widetilde{S} = P^{-\top}SP^{-1}, \tag{22}$$

$$\widetilde{\Delta X} = P\Delta XP^\top, \qquad \widetilde{\Delta S} = P^{-\top}\Delta SP^{-1}, \tag{23}$$

$$X(\alpha) = X + \alpha\Delta X, \qquad S(\alpha) = S + \alpha\Delta S, \qquad y(\alpha) = y + \alpha\Delta y, \tag{24}$$

$$\widetilde{X}(\alpha) = PX(\alpha)P^\top = \widetilde{X} + \alpha\widetilde{\Delta X}, \tag{25}$$

$$\widetilde{S}(\alpha) = P^{-\top}S(\alpha)P^{-1} = \widetilde{S} + \alpha\widetilde{\Delta S}, \tag{26}$$

$$\mathcal{W}_X = \widetilde{X}^{-1/2}\left[\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S} - \sigma\nu I - r_c\right]\widetilde{X}^{1/2}, \tag{27}$$

and

$$\nu = \frac{X \bullet S}{n} = \frac{\widetilde{X} \bullet \widetilde{S}}{n}, \quad \nu(\alpha) = \frac{X(\alpha) \bullet S(\alpha)}{n} = \frac{\widetilde{X}(\alpha) \bullet \widetilde{S}(\alpha)}{n}. \tag{28}$$

Lemma 2 (Lemma 3.1 in [32])**.** *$(\Delta X, \Delta S, \Delta y)$ is a solution of the system (21) if and only if $(\widetilde{\Delta X}, \widetilde{\Delta S}, \Delta y)$ is a solution of the system*

$$H_I(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S}) = \sigma\nu I - H_I(\widetilde{X}\widetilde{S}) + r_c \tag{29a}$$

$$\sum_{i=1}^m \Delta y \widetilde{A}^{(i)} + \widetilde{\Delta S} = \widetilde{C} - \widetilde{S} - \sum_{i=1}^m y_i \widetilde{A}^{(i)} \tag{29b}$$

$$A^{(i)} \bullet \Delta X = b_i - A^{(i)} \bullet X, \quad \forall i \in [m]. \tag{29c}$$

where $\widetilde{C} = P^{-\top}CP^{-1}$ and $\widetilde{A}^{(i)} = P^{-\top}\widetilde{A}^{(i)}P^{-1}$ for $i \in [m]$.

Proof. The proof follows as a consequence of equations (21), (22) and (23). □

For the rest of this section, we work under the assumption

$$(X, y, S) \in F^0(\mathcal{P}) \times F^0(\mathcal{D}).$$

Further, for the residual term, in addition to the condition given in (19) we assume that r_c is chosen in each iteration to satisfy

$$\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\|_F \leq \beta \|\widetilde{X}^{-1/2} R_c \widetilde{X}^{1/2}\|_F \tag{30}$$

for some $\beta \in (0,1)$. Note that in light of the fact that r_c already satisfies (19) this assumption is not too strong, as we will show that β is typically small.

Lemma 3. *The following relations hold:*

$$H_{\widetilde{X}^{1/2}}(\mathcal{W}_X) = 0, \tag{31}$$

$$\widetilde{\Delta X} \bullet \widetilde{\Delta S} = \Delta X \bullet \Delta S = 0. \tag{32}$$

Proof. Equation (31) is a direct consequence of (29a). Further from our assumption

$$(X, y, S) \in F^0(\mathcal{P}) \times F^0(\mathcal{D}),$$

and applying equations (21a), (21b) and (23) yields the two identities in (32). □

Lemma 4. *For all $\alpha \in \mathbb{R}$ we have*

$$\nu(\alpha) = (1 - \alpha + \sigma\alpha)\nu + \alpha\frac{\operatorname{tr}(r_c)}{n}, \tag{33}$$

$$\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I\right]\widetilde{X}^{1/2} = (1-\alpha)(\widetilde{X}^{1/2}\widetilde{S}\widetilde{X}^{1/2} - \nu I) + \alpha\mathcal{W}_X + \alpha^2\widetilde{X}^{-1/2}\widetilde{\Delta X}\widetilde{\Delta S}\widetilde{X}^{1/2} + \alpha\widetilde{X}^{-1/2}\left[r_c - \frac{\operatorname{tr}(r_c)}{n}I\right]\widetilde{X}^{1/2} \tag{34}$$

Proof. From (24) we have

$$X(\alpha)S(\alpha) = (X + \alpha\Delta X)(S + \alpha\Delta S) = XS + \alpha(X\Delta S + \Delta X S) + \alpha^2\Delta X\Delta S$$

Hence, by the linearity of $H_P(\cdot)$ and equation (21a), it follows

$$\begin{aligned} X(\alpha)S(\alpha) = (X + \alpha\Delta X)(S + \alpha\Delta S) &= H_P(XS) + \alpha H_P(X\Delta S + \Delta X S) + \alpha^2 H_P(\Delta X\Delta S) \\ &= H_P(XS) + \alpha H_P(X\Delta S + \Delta X S) + \alpha^2 H_P(\Delta X\Delta S) \\ &= H_P(XS) + \alpha[H_P(\sigma\nu I - XS) + r_c] + \alpha^2 H_P(\Delta X\Delta S) \\ &= (1-\alpha)H_P(XS) + \alpha\sigma\nu I + \alpha r_c + \alpha^2 H_P(\Delta X\Delta S). \end{aligned}$$

Now, for $M \in \mathbb{R}^{n\times n}$ we have $\operatorname{tr}(H_P(M)) = \operatorname{tr}(M)$, and thus

$$\begin{aligned} X(\alpha) \bullet S(\alpha) &= \operatorname{tr}[X(\alpha)S(\alpha)] = \operatorname{tr}[H_P(X(\alpha)S(\alpha)] \\ &= \operatorname{tr}[(1-\alpha)H_P(XS) + \alpha\sigma\nu I + \alpha r_c + \alpha^2 H_P(\Delta X\Delta S)] \\ &= (1-\alpha)\operatorname{tr}[H_P(XS)] + \alpha\sigma\nu I + \alpha\operatorname{tr}(r_c) + \alpha^2\operatorname{tr}[H_P(\Delta X\Delta S)] \\ &= (1-\alpha)X \bullet S + \alpha\sigma\nu n + \alpha\operatorname{tr}(r_c) + \alpha^2\Delta X \bullet \Delta S \\ &= (1-\alpha)X \bullet S + \alpha\sigma\nu n + \alpha\operatorname{tr}(r_c), \end{aligned}$$

where the final equality follows from (32). Dividing the above expression by n and applying (28) yields (33).

From here, we apply equations (25), (26), (33) and (27), and it follows:

$$\begin{aligned} \widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I &= (\widetilde{X} + \alpha\widetilde{\Delta X})(\widetilde{S} + \alpha\widetilde{\Delta S}) - \nu(\alpha)I \\ &= \widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \nu(\alpha)I \\ &= (1-\alpha)\widetilde{X}\widetilde{S} + \alpha\widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \nu(\alpha)I \\ &= (1-\alpha)\widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \nu(\alpha)I \\ &= (1-\alpha)\widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \nu(\alpha)I + \underbrace{(\alpha r_c - \alpha r_c)}_{=0} \\ &= (1-\alpha)\widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \left[(1-\alpha+\sigma\alpha)\nu + \frac{\alpha\operatorname{tr}(r_c)}{n}\right]I + (\alpha r_c - \alpha r_c) \\ &= (1-\alpha)\widetilde{X}\widetilde{S} + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S}) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} - \left[(1-\alpha+\sigma\alpha)\nu + \frac{\alpha\operatorname{tr}(r_c)}{n}\right]I + \alpha r_c - \alpha r_c \\ &= (1-\alpha)(\widetilde{X}\widetilde{S} - \nu I) + \alpha(\widetilde{\Delta X}\widetilde{S} + \widetilde{X}\widetilde{\Delta S} + \widetilde{X}\widetilde{S} - \sigma\nu I - r_c) + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} + \alpha\left[r_c - \frac{\operatorname{tr}(r_c)}{n}I\right] \\ &= (1-\alpha)(\widetilde{X}\widetilde{S} - \nu I) + \alpha\widetilde{X}^{1/2}\mathcal{W}_X\widetilde{X}^{-1/2} + \alpha^2\widetilde{\Delta X}\widetilde{\Delta S} + \alpha\left[r_c - \frac{\operatorname{tr}(r_c)}{n}I\right], \end{aligned}$$

which holds for any $\alpha \in \mathbb{R}$. Multiplying on the left by $\widetilde{X}^{-1/2}$ and on the right by $\widetilde{X}^{1/2}$ gives (34). □

The following result from [32] plays a crucial role in the analysis.

Lemma 5 (Lemma 3.5 in [32]). *Let $M \in \mathbb{R}^{n\times n}$ be such that $H_Q(M) = 0$ for some nonsingular $Q \in \mathbb{R}^{n\times n}$. Then,*

$$\|H_I(M)\|_F \leq \frac{1}{2}\|M - M^\top\|_F, \tag{35}$$

$$\|M\|_F \leq \frac{\sqrt{2}}{2}\|M - M^\top\|_F. \tag{36}$$

In particular, if $M = U_1 + U_2$ for some $U_1 \in \mathcal{S}^n$ and $U_2 \in \mathbb{R}^{n\times n}$, then

$$\|M\|_F \leq \sqrt{2}\|U_2\|_F.$$

Proof. Our proof follows that of [32]. Let

$$U = \frac{M + M^\top}{2} \in \mathcal{S}^n, \text{ and } \widehat{U} = \frac{M - M^\top}{2} \in \mathcal{S}^n_-.$$

Now, one can observe $M = U + \widehat{U}$ and $U \bullet \widehat{U} = 0$. Noting these facts, along with our assumption $H_Q(M) = 0$, applying the identity

$$\|B + B^\top\|_F^2 = 2\left(\|B\|_F^2 + \operatorname{tr}(B^2)\right)$$

for $B \in \mathbb{R}^{n\times n}$ we have

$$\begin{aligned}
0 = 2\|H_Q(M)\|_F^2 &= \frac{1}{2}\|QMQ^{-1} + (QMQ^{-1})^\top\|_F^2 \\
&= \|QWQ^{-1}\|_F^2 + \operatorname{tr}\left[(QWQ^{-1})^2\right] = \|QWQ^{-1}\|_F^2 + \operatorname{tr}\left[M^2\right] \\
&\geq \operatorname{tr}\left[(U + \widehat{U})^2\right] \\
&= \operatorname{tr}\left[U^2 + U\widehat{U} + \widehat{U}U + \widehat{U}^2\right] \\
&= \|U\|_F^2 + 2U \bullet \widehat{U} + \operatorname{tr}(\widehat{U}^2) \\
&= \|U\|_F^2 - \|\widehat{U}\|_F^2.
\end{aligned}$$

Thus, (35) follows as the above implies $\|U\|_F \leq \|\widehat{U}\|_F$. Then, combining (35) with the fact that $U \bullet \widehat{U} = 0$ yields

$$\|M\|_F^2 = \|U + \widehat{U}\|_F^2 = \|U\|_F^2 + \|\widehat{U}\|_F^2 \leq 2\|\widehat{U}\|_F^2,$$

from which we obtain (36). To complete the proof of the lemma, one can note

$$\|M - M^\top\|_F = \|U_2 - U_2^\top\|_F \leq 2\|U_2\|_F,$$

and therefore by (36) we obtain the result $\|M\|_F \leq \sqrt{2}\|U_2\|_F$. □

We can now use the above result in order to prove the following lemma, which is adapted from Lemma 3.5 in [32].

Lemma 6. *For every $\theta \in \mathbb{R}$, we have*

$$\|\mathcal{W}_X\|_F \leq \sqrt{2}\delta_x \left\|\widetilde{S}^{1/2}\widetilde{X}^{1/2} - \theta\nu\widetilde{S}^{-1/2}\widetilde{X}^{-1/2}\right\| + \sqrt{2}\left\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\right\|, \tag{37}$$

and

$$\begin{aligned}
\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \leq (1-\alpha)d(\widetilde{X},\widetilde{S}) + \alpha^2\delta_x\delta_s + \alpha\left\|\widetilde{X}^{-1/2}\left[r_c - \frac{\operatorname{tr}(r_c)}{n}I\right]\widetilde{X}^{1/2}\right\| \\
+ \alpha\sqrt{2}\left\|\widetilde{S}^{1/2}\widetilde{X}^{1/2} - \theta\nu\widetilde{S}^{-1/2}\widetilde{X}^{-1/2}\right\| + \sqrt{2}\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\|,
\end{aligned} \tag{38}$$

for all $\alpha \in [0,1]$*, where*

$$\delta_x = \left\| \widetilde{X}^{-1/2} \widetilde{\Delta X} \widetilde{S}^{1/2} \right\|_F, \quad \delta_s = \left\| \widetilde{S}^{-1/2} \widetilde{\Delta S} \widetilde{X}^{1/2} \right\|_F. \tag{39}$$

Proof. Let $\theta \in \mathbb{R}$ be given. By (27), we have $\mathcal{W}_X = U_1 + U_2$, where

$$\begin{aligned} U_1 &= \widetilde{X}^{1/2} \widetilde{\Delta S} \widetilde{X}^{1/2} + \theta\nu \widetilde{X}^{-1/2} \widetilde{\Delta X} \widetilde{X}^{-1/2} + \widetilde{X}^{1/2} \widetilde{S} \widetilde{X}^{1/2} - \sigma\nu I \in \mathcal{S}^n \\ U_2 &= \widetilde{X}^{-1/2} \widetilde{\Delta X} \widetilde{S}^{1/2} \left(\widetilde{S}^{1/2} \widetilde{X}^{1/2} - \theta\nu \widetilde{S}^{-1/2} \widetilde{X}^{-1/2} \right) - \widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2} \end{aligned}$$

Then, applying (31), it follows $H_Q(\mathcal{W}_X) = 0$ for $Q = \widetilde{X}^{1/2}$. This fact, combined with Lemma 5 and the fact that $\|AB\|_F \leq \|A\|_F \|B\|$ for every $A, B \in \mathbb{R}^{n \times n}$, from the definition of U_2 and δ_x it follows

$$\|\mathcal{W}_X\|_F \leq \sqrt{2} \|U_2\|_F \leq \sqrt{2} \delta_x \left\| \widetilde{S}^{1/2} \widetilde{X}^{1/2} - \theta\nu \widetilde{S}^{-1/2} \widetilde{X}^{-1/2} - \delta_x^{-1} \widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2} \right\|,$$

i.e., (37) holds. From here, we apply (20) and (34), and note that for $\alpha \in [0,1]$, by the definition of δ_x and δ_s we have:

$$\begin{aligned} \left\| \widetilde{X}^{-1/2} \left[\widetilde{X}(\alpha) \widetilde{S}(\alpha) - \nu(\alpha) I \right] \widetilde{X}^{1/2} \right\|_F &\leq (1-\alpha) \left\| \widetilde{X}^{1/2} \widetilde{S} \widetilde{X}^{1/2} - \nu I \right\|_F + \alpha \|\mathcal{W}_X\|_F + \alpha \delta_x \delta_s \\ &= (1-\alpha) d(\widetilde{X}, \widetilde{S}) + \alpha \|\mathcal{W}_X\|_F + \alpha^2 \delta_x \delta_s. \end{aligned}$$

Combining the above result with (37) implies (38) and the proof is complete. □

For ease of notation, for the coming results we follow [32] in defining the quantity

$$\Phi_\theta(A, B) = \left\| A^{1/2} B^{1/2} - \theta \frac{A \bullet B}{n} A^{-1/2} B^{-1/2} \right\|_F \tag{40}$$

for every $(A, B) \in \mathcal{S}^n_{++} \times \mathcal{S}^n_{++}$ and $\theta \in \mathbb{R}$.

Lemma 7 (Lemma 3.7 in [32])**.** *If* $d(X, S) \leq \gamma\nu$ *for some* $\gamma \in (0,1)$*, then*

$$\left\| \widetilde{X}^{-1/2} \widetilde{S}^{-1/2} \right\|^2 \leq \frac{1}{(1-\gamma)\nu} \tag{41}$$

$$\left[\Phi_\theta(\widetilde{X}, \widetilde{S}) \right]^2 \leq \frac{\gamma^2 + (1-\theta)^2 n}{1-\gamma} \nu. \tag{42}$$

Proof. By the definition of (20), along with our assumption that $d(X, S) \leq \gamma\nu$, it follows that $\lambda_{\min}[XS] \geq (1-\gamma)\nu$. These facts, combined with (22) yield

$$\begin{aligned} \left\| \widetilde{X}^{-1/2} \widetilde{S}^{-1/2} \right\|^2 = \left\| \widetilde{X}^{-1/2} \widetilde{S}^{-1} \widetilde{X}^{-1/2} \right\| &= \frac{1}{\lambda_{\min}\left[\widetilde{X}^{1/2} \widetilde{S} \widetilde{X}^{1/2} \right]} = \frac{1}{\lambda_{\min}\left[\widetilde{X} \widetilde{S} \right]} \\ = \frac{1}{\lambda_{\min}[PXSP^{-1}]} = \frac{1}{\lambda_{\min}[XS]} &\leq \frac{1}{(1-\gamma)\nu}, \end{aligned}$$

and thus (41) holds. Next, we use (40), (28), (41), (20) along with Lemma 1(a) our assumption $d(X, S) \leq \gamma\nu$ and the fact that the matrices $\widetilde{X}^{1/2} \widetilde{S} \widetilde{X}^{1/2} - \nu I$ and I are orthogonal, so that we have

$$\begin{aligned} \left[\Phi_\theta(\widetilde{X}, \widetilde{S}) \right]^2 = \left\| \widetilde{X}^{1/2} \widetilde{S}^{1/2} - \theta\nu \widetilde{X}^{-1/2} \widetilde{S}^{-1/2} \right\|_F^2 &\leq \left\| \widetilde{X}^{1/2} \widetilde{S} \widetilde{X}^{1/2} \right\|^2 \left\| \widetilde{X}^{1/2} \widetilde{S}^{1/2} - \theta\nu I \right\|_F^2 \\ &\leq \frac{1}{(1-\gamma)\nu} \left(\left\| \widetilde{X}^{1/2} \widetilde{S}^{1/2} - \nu I \right\|_F^2 + \|\nu I - \theta\nu I\|_F^2 \right) \\ &= \frac{1}{(1-\gamma)\nu} \left(d(X, S)^2 + (1-\theta)^2 \nu^2 n \right) \leq \frac{\gamma^2 + (1-\theta)^2 n}{1-\gamma} \nu, \end{aligned}$$

i.e., (42) holds. □

Lemma 8. *For $\beta \in (0,1)$ we have*

$$\|r_c\|_F \le \beta\gamma\sigma\nu. \tag{43}$$

$$\left\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\right\|_F \le \beta\gamma\sigma\nu, \tag{44}$$

$$\left\|\widetilde{X}^{-1/2}\left[r_c - \frac{\mathrm{tr}\,(r_c)}{n} I\right]\widetilde{X}^{1/2}\right\|_F \le 2\beta\gamma\sigma\nu. \tag{45}$$

Proof. From equation (29a), $R_c = \sigma\nu I - H_I(\widetilde{X}, \widetilde{S})$, we first note that

$$\begin{aligned}\widetilde{X}^{-1/2} R_c \widetilde{X}^{1/2} = \widetilde{X}^{-1/2} H_I(\sigma\nu I - \widetilde{X}\widetilde{S})\widetilde{X}^{1/2} &= \widetilde{X}^{-1/2}[\sigma\nu I - \widetilde{X}\widetilde{S}]\widetilde{X}^{1/2} \\ &= \sigma\nu I - \widetilde{X}^{-1/2}\widetilde{X}\widetilde{S}\widetilde{X}^{1/2} \\ &= \sigma\nu I - \widetilde{X}^{1/2}\widetilde{S}\widetilde{X}^{1/2}.\end{aligned}$$

Thus, it follows

$$\|\widetilde{X}^{-1/2} R_c \widetilde{X}^{1/2}\|_F = \|\sigma\nu I - \widetilde{X}^{1/2}\widetilde{S}\widetilde{X}^{1/2}\|_F = \|\widetilde{X}^{1/2}\widetilde{S}\widetilde{X}^{1/2} - \sigma\nu I\|_F = d_\sigma(\widetilde{X}, \widetilde{S}).$$

Further, applying Lemma 1(b) one can observe

$$\|H_I(\widetilde{X}, \widetilde{S}) - \sigma\nu I\| = d_\sigma(\widetilde{X}, \widetilde{S}) = d_\sigma(X, S) \le \sigma\gamma\nu.$$

Hence, by our assumption in equation (30), it follows

$$\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\|_F \le \beta \|\widetilde{X}^{-1/2} R_c \widetilde{X}^{1/2}\|_F \le \beta\sigma\gamma\nu.$$

Finally, noting the fact that for two matrices $A, B \in \mathbb{R}^{n\times n}$, $\mathrm{tr}\,(AB) \le \|A\|_F \|B\|_F$, we take $A = r_c$ and $B = I$ such that

$$\mathrm{tr}\,(r_c) = \mathrm{tr}\,(r_c I) \le \|r_c\|_F \|I\|_F = \sqrt{n}\|r_c\|_F.$$

Then, noting that $\|r_c\|_F \le \beta\|R_c\| \le \beta\sigma\gamma\nu$, it follows

$$\begin{aligned}\left\|\widetilde{X}^{-1/2}\left[r_c - \frac{\mathrm{tr}\,(r_c)}{n} I\right]\widetilde{X}^{1/2}\right\|_F &\le \left\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\right\|_F + \left\|\frac{\mathrm{tr}\,(r_c)}{n} I\right\|_F \\ &= \left\|\widetilde{X}^{-1/2} r_c \widetilde{X}^{1/2}\right\|_F + \frac{|\mathrm{tr}\,(r_c)|}{n}\|I\|_F \\ &\le \beta\sigma\gamma\nu + \frac{|\mathrm{tr}\,(r_c)|}{n}\sqrt{n} \\ &= \beta\sigma\gamma\nu + \frac{|\mathrm{tr}\,(r_c)|}{\sqrt{n}} \\ &\le \beta\sigma\gamma\nu + \frac{\sqrt{n}\|r_c\|_F}{\sqrt{n}} \\ &= \beta\sigma\gamma\nu + \|r_c\|_F \le 2\beta\sigma\gamma\nu.\end{aligned}$$

□

Lemma 9. *If $(X, y, S) \in \mathcal{N}_F(\gamma)$ for some $\gamma > 0$ satisfying*

$$2\sqrt{2}\frac{\gamma}{1-\gamma} \le 1, \tag{46}$$

and $\beta \in (0,1)$ such that for $\eta > 0$,

$$\beta \le \eta \frac{1}{\sigma(1-\gamma)^{1/2}} \sqrt{\frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma}},$$

then

$$\max\{\delta_x, \delta_s\} \leq 2(1+\eta)\Phi_\sigma(\widetilde{X}, \widetilde{S}),$$

where δ_x, δ_s *and* $\Phi_\sigma(\cdot,\cdot)$ *are defined by* (39) *and* (40).

Proof. From (27), one can see

$$\begin{aligned}\widetilde{X}^{1/2}\widetilde{\Delta S}\widetilde{S}^{-1/2} + \widetilde{X}^{-1/2}\widetilde{\Delta X}\widetilde{S}^{1/2} &= \mathcal{W}_X\widetilde{X}^{-1/2}\widetilde{S}^{-1/2} + \sigma\nu\widetilde{X}^{-1/2}\widetilde{S}^{-1/2} - \widetilde{X}^{1/2}\widetilde{S}^{1/2} \\ &\quad + (\widetilde{X}^{-1/2}r_c\widetilde{X}^{1/2})\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}. \end{aligned} \tag{47}$$

Now,

$$\sqrt{\left[\Phi_\sigma(\widetilde{X}, \widetilde{S})\right]^2} \leq \sqrt{\frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma}}\nu = \sqrt{\frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma}}\nu^{1/2}.$$

Hence,

$$\beta\sigma\nu^{1/2} \leq \eta\frac{1}{\sigma(1-\gamma)^{1/2}}\sqrt{\frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma}}\sigma\nu^{1/2} = \frac{\eta}{(1-\gamma)^{1/2}}\sqrt{\frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma}}\nu^{1/2} = \frac{\eta}{(1-\gamma)^{1/2}}\left[\Phi_\sigma(\widetilde{X}, \widetilde{S})\right].$$

Next, from (32), observe that the two terms on the left hand side of (47) are orthogonal. Combining this fact with (39), (47), (40), (28), (37) with $\theta = 1$, (41), (42) with $\theta = 1$ and (46), it follows

$$\begin{aligned}
\max\{\delta_x, \delta_s\} &\leq (\delta_x + \delta_s)^{1/2} = \left(\left\|\widetilde{X}^{-1/2}\widetilde{\Delta X}\widetilde{S}^{1/2}\right\|_F^2 + \left\|\widetilde{S}^{-1/2}\widetilde{\Delta S}\widetilde{X}^{1/2}\right\|_F^2\right)^{1/2} \\
&= \left\|\widetilde{X}^{-1/2}\widetilde{\Delta X}\widetilde{S}^{1/2} + \widetilde{X}^{1/2}\widetilde{\Delta S}\widetilde{S}^{-1/2}\right\|_F \\
&\leq \|\mathcal{W}_X\|_F\left\|\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}\right\| + \left\|\widetilde{X}^{1/2}\widetilde{S}^{1/2} - \sigma\nu\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}\right\| \\
&\leq \sqrt{2}\delta_x\left\|\widetilde{X}^{1/2}\widetilde{S}^{1/2} - \nu\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}\right\|\left\|\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}\right\| + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + (1+\sqrt{2})\left\|\widetilde{X}^{-1/2}r_c\widetilde{X}^{1/2}\right\|_F\left\|\widetilde{X}^{-1/2}\widetilde{S}^{-1/2}\right\| \\
&\leq \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + (1+\sqrt{2})\beta\sigma\gamma\nu\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} \\
&= \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \left[(1+\sqrt{2})\frac{\gamma}{(1-\gamma)^{1/2}}\right]\beta\sigma\nu^{1/2} \\
&\leq \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \left[(1+\sqrt{2})\frac{\gamma}{(1-\gamma)^{1/2}}\right]\frac{\eta}{(1-\gamma)^{1/2}}\left[\Phi_\sigma(\widetilde{X}, \widetilde{S})\right] \\
&= \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \left[(1+\sqrt{2})\frac{\gamma}{(1-\gamma)}\right]\eta\Phi_\sigma(\widetilde{X}, \widetilde{S}) \\
&\leq \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \left[2\sqrt{2}\frac{\gamma}{(1-\gamma)}\right]\eta\Phi_\sigma(\widetilde{X}, \widetilde{S}) \\
&\leq \sqrt{2}\delta_x\frac{\gamma\nu^{1/2}}{(1-\gamma)^{1/2}}\frac{1}{(1-\gamma)^{1/2}\nu^{1/2}} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \eta\Phi_\sigma(\widetilde{X}, \widetilde{S}) \\
&\leq \frac{\delta_x}{2} + \Phi_\sigma(\widetilde{X}, \widetilde{S}) + \eta\Phi_\sigma(\widetilde{X}, \widetilde{S}) \leq \frac{1}{2}\max\{\delta_x, \delta_s\} + (1+\eta)\Phi_\sigma(\widetilde{X}, \widetilde{S}),
\end{aligned}$$

and the proof is complete. □

The final result of this section follows from the above lemmas.

Lemma 10. *If $(X, y, S) \in \mathcal{N}_F(\gamma)$ for some $\gamma > 0$ satisfying (46), then, for every $\alpha \in [0, 1]$, $\beta \in (0, 1)$, and $\eta > 0$, we have*

$$\begin{aligned}
&\left\| \widetilde{X}^{-1/2} \left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha) I \right] \widetilde{X}^{1/2} \right\|_F \\
&\quad \leq \left\{ (1-\alpha)\gamma + 2(1+\eta)\sqrt{2}\alpha \frac{\gamma \left[\gamma^2 + (1-\sigma)^2 n\right]^{1/2}}{1-\gamma} + (2(1+\eta))^2 \alpha^2 \frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma \right\} \nu
\end{aligned}$$

Proof. We apply (38) with $\theta = 1$, Lemma 1 (a), (22), the assumption $d(X, S) \leq \gamma\nu$, Lemma 8, Lemma 9 and (42) where we choose $\theta = 1$ and $\theta = \sigma$, one has

$$\begin{aligned}
&\left\| \widetilde{X}^{-1/2} \left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha) I \right] \widetilde{X}^{1/2} \right\|_F \\
&\quad \leq (1-\alpha) d(X, S) + \sqrt{2}\alpha\delta_x \Phi_1(\widetilde{X}, \widetilde{S}) + \alpha^2 \delta_x \delta_s + \alpha(2+\sqrt{2})\beta d_\sigma(X, S) \\
&\quad \leq (1-\alpha)\gamma\nu + 2(1+\eta)\sqrt{2}\alpha\Phi_\sigma(\widetilde{X}, \widetilde{S})\Phi_1(\widetilde{X}, \widetilde{S}) + (2(1+\eta))^2\alpha^2 \left[\Phi_\sigma(\widetilde{X}, \widetilde{S})\right]^2 + \alpha(2+\sqrt{2})\beta\sigma\gamma\nu \\
&\quad \leq \left\{ (1-\alpha)\gamma + 2(1+\eta)\sqrt{2}\alpha \frac{\gamma \left[\gamma^2 + (1-\sigma)^2 n\right]^{1/2}}{1-\gamma} + (2(1+\eta))^2 \alpha^2 \frac{\gamma^2 + (1-\sigma)^2 n}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma \right\} \nu.
\end{aligned}$$

□

5 An Inexact-Feasible Quantum Interior Point Method for SDOs

We quantize a general IF-IPM and the resulting scheme is described in Algorithm 2. Their is no classical counterpart in the literature for SDO, as the nullspace representation of the Newton system destroys the sparsity of the system, and thus impractical for classical computing. The algorithm has several parameters, the most important of which is the optimality gap tolerance ϵ. Details for all steps of Algorithm 2 are discussed subsequently in this paper.

In our initialization steps, we must calculate bases of the nullspace, and rowspace of $\mathcal{A}_s$. For this step, one can either use Gauss elimination, or the QR-factorization of $\mathcal{A}_s$, which can be accomplished in time $O(n^3)$, but has been shown to exhibit a higher level of numerical stability compared to Gauss elimination. However, one should note that the calculation of these bases need only be carried out once. That is, we calculate $\mathcal{A}_s$ and Q_2 one time, and store these matrices in QRAM before the algorithm begins, as they remain unchanged for the duration of the algorithm. In steps (1) and (2) of Algorithm 2 we require classical matrix multiplication and inversion. These steps can be carried out in time $O(n^\omega)$ where $\omega = 2.37$ is the matrix multiplication exponent [9, 41]. Note that in practice, this step is typically performed with the standard Gaussian elimination and requires time $O(n^3)$. A detailed analysis for step (2) can be found in Proposition 15 for the NT direction. 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. Following Theorem 2, this can be accomplished in time $O\left(\frac{n^2\kappa^2}{\xi_k^2} T_{\text{LS}}\right)$ where, for the NT direction, T_{LS} is the time needed to prepare and solve the NT linear system, and ξ_k is the error tolerance, that is chosen according to a sequence described in Section 5.3. Then, in step 5, we use our classical estimates of Δy and $\Delta\zeta$ to classically calculate ΔX and ΔS. Finally, we classically update the current solutions to the SDOP X, y and S, and the central path parameter ν.

Algorithm 2 Quantum inexact-feasible interior point method

Input: Initialize $\nu_0, \theta_0 = 1$,
$\epsilon, \delta > 0$,
$\eta_1 \in (0, 1)$
Pick a feasible initial point $(X^0, y^0, S^0) \in \mathcal{N}$ and store in QRAM
Choose bases for $\mathcal{R}(\mathcal{A}_s)$ and $\mathcal{N}(\mathcal{A}_s)$, store $\mathcal{A}_s$ and Q_2 in QRAM
while $\nu > \epsilon$ **do**

1. Compute matrices X^{-1} and S^{-1} classically. Store these matrices in QRAM.
2. Compute scaling matrix P right hand side matrix and necessary matrix products for Newton system factorization and store in QRAM
3. Using block encodings, solve (18) to construct inexact search direction $|\Delta\zeta^k \circ \Delta y^k\rangle$ and estimate $||\Delta\zeta^k \circ \Delta y^k||$.
4. Obtain classical estimate of $\Delta\zeta^k \circ \Delta y^k$ using vector state tomography.
5. Use classical estimates of $\Delta\zeta^k \circ \Delta y^k$ to obtain classical estimates of $\Delta X^k \circ \Delta S^k$
6. $$X^{k+1} \leftarrow X^k + \alpha_k \Delta X^k,\ S^{k+1} \leftarrow S^k + \alpha_k \Delta S^k \text{ and } y^{k+1} \leftarrow y^k + \alpha_k \Delta y^k$$
$$\nu_{k+1} \leftarrow \nu_k(\alpha_k)$$

end

In the next subsections, we discuss the polynomial convergence of Algorithm 2, how to construct the Newton linear system for Nesterov-Todd direction, we show that the algorithm converges for a specific choice of the error parameters (based on the results of [52]), and provide a running time analysis for the chosen parameters.

5.1 Convergence

In order to have a convergent algorithm, we need to ensure that the errors ξ_k introduced from QLSA are properly chosen. At iteration k, we then choose ξ_k satisfying:

$$\xi_k = \frac{1}{\varrho}\|r_k\|. \tag{48}$$

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 relative (it is stated in additive form, but assumes that the vector to be extracted has unit norm): to ensure that we satisfy the absolute error bound for the unscaled vector, we need to divide ξ_k by the maximum norm of a solution vector. Hence, we must ensure

$$\|r\| \leq \alpha \left(1 - \frac{c}{\sqrt{n}}\right)^k,$$

so we choose ξ_k to be

$$\xi_k = \alpha \left(\frac{\sqrt{n} - 1}{\sqrt{n}}\right)^k. \tag{49}$$

Lemma 11. *Choosing ξ_k according to* (49)*, the inexact search direction computed at step* **??** *of Algorithm* **??** *satisfies* (**??**).

In the following result, we follow [32] in setting $\Gamma = \gamma$, for suitable choices of γ and δ, for one iteration of Algorithm 2 we have the following.

Theorem 6. *Let $\gamma, \Gamma \in (0,1)$, $\beta \in (0,1)$ and $\delta \in [0, n^{1/2})$ be constants satisfying*

$$\frac{2\sqrt{2}\gamma}{1-\gamma} \leq 1, \quad \beta \leq \frac{1}{25}\frac{1}{\sigma(1-\gamma)^{1/2}}\sqrt{\frac{\gamma^2+(1-\sigma)^2}{1-\gamma}}, \quad \frac{7.3264(\gamma^2+\delta^2)}{1-\gamma} + (2+\sqrt{2})\beta\sigma\gamma \leq \left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma - \frac{\sigma\gamma^2}{\sqrt{n}}. \tag{50}$$

Suppose that $(X, y, S) \in \mathcal{N}_F(\gamma)$ and let $(\Delta X, \Delta y, \Delta S)$ denote the solution of the system (13), where $\sigma = 1 - \delta/\sqrt{n}$, $\mu = (X \bullet S)/n$ and $P \in \mathbb{R}^{n\times n}$. Then,

(a) $(\widehat{X}, \hat{y}, \widehat{S}) = (X + \Delta X, y + \Delta y, S + \Delta S) \in \mathcal{N}_F(\Gamma)$;

(b) $\widehat{X} \bullet \widehat{S} = \left(1 - \frac{\delta}{\sqrt{n}}\right)(X \bullet S)$.

Proof. In the following proof, we seek to show that a new iterate, after a step in α in this direction satisfies

$$\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \leq \max\{\gamma,\Gamma\}\nu(\alpha) = \max\{\gamma,\Gamma\}(1-\alpha+\sigma\alpha)\nu + \alpha\max\{\gamma,\Gamma\}\frac{\operatorname{tr}(r_c)}{n}.$$

Since, we only make the assumption that $r_c \in \mathcal{S}^n$, we cannot make any conclusions regarding the sign of the quantity $\operatorname{tr}(r_c)$. Hence, noting that $\operatorname{tr}(r_c) \leq \sqrt{n}\|r_c\|_F = \sqrt{n}\sigma\gamma\nu$, it suffices to show

$$\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \leq \max\{\gamma,\Gamma\}(1-\alpha+\max\{\gamma,\Gamma\}\sigma\alpha)\nu - \alpha\frac{\sigma\gamma\nu}{\sqrt{n}}.$$

Thus, applying Lemma 10 with $\eta = \frac{1}{25}$, along with the definition of σ an (50), for all $\alpha \in [0,1]$ we have

$$\begin{aligned}
&\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha) - \nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \\
&\leq \left\{(1-\alpha)\gamma + 2(1+\eta)\sqrt{2}\alpha\frac{\gamma\left[\gamma^2+(1-\sigma)^2 n\right]^{1/2}}{1-\gamma} + [2(1+\eta)]^2\alpha^2\frac{\gamma^2+(1-\sigma)^2 n}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu \\
&= \left\{(1-\alpha)\gamma + 2.08\sqrt{2}\alpha\frac{\gamma\left[\gamma^2+(1-\sigma)^2 n\right]^{1/2}}{1-\gamma} + 4.3264\alpha^2\frac{\gamma^2+(1-\sigma)^2 n}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu \\
&\leq \left\{(1-\alpha)\gamma + 7.3264\alpha\frac{\gamma^2+(1-\sigma)^2 n}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu \\
&= \left\{(1-\alpha)\gamma + \alpha\frac{7.3264(\gamma^2+(1-\sigma)^2 n)}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu \\
&= \left\{(1-\alpha)\gamma + \alpha\frac{7.3264(\gamma^2+\delta^2)}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu.
\end{aligned}$$

Hence, it must be that

$$\left\{\alpha\frac{7.3264(\gamma^2+\delta^2)}{1-\gamma} + \alpha(2+\sqrt{2})\beta\sigma\gamma\right\}\nu \leq \alpha\left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma\nu - \alpha\max\{\gamma,\Gamma\}\frac{\sigma\gamma\nu}{\sqrt{n}}.$$

Dropping like terms on both sides of the inequality, this implies

$$\frac{7.3264(\gamma^2+\delta^2)}{1-\gamma} + (2+\sqrt{2})\beta\sigma\gamma \leq \left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma - \frac{\sigma\gamma^2}{\sqrt{n}} \leq \left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma - \max\{\gamma,\Gamma\}\frac{\sigma\gamma}{\sqrt{n}}.$$

Therefore, one can choose $\beta \in (0,1)$ such that

$$\beta \leq \frac{1}{\sigma\gamma}\cdot\frac{1}{[(2+\sqrt{2})]}\cdot\left[\left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma - \frac{\sigma\gamma}{\sqrt{n}} - \frac{7.3264(\gamma^2+\delta^2)}{1-\gamma}\right]$$

and then it follows

$$\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha)-\nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \leq \left\{(1-\alpha)\gamma+\alpha\left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma\right\}\nu+\alpha\max\{\gamma,\Gamma\}\frac{\mathrm{tr}\,(r_c)}{n}$$
$$=\{(1-\alpha)\gamma+\alpha\Gamma\sigma\}\,\nu+\alpha\max\{\gamma,\Gamma\}\frac{\mathrm{tr}\,(r_c)}{n}. \tag{51}$$

By equation (33)

$$\nu(\alpha)=(1-\alpha+\sigma\alpha)\nu+\alpha\frac{\mathrm{tr}\,(r_c)}{n}$$

and thus

$$\left\|\widetilde{X}^{-1/2}\left[\widetilde{X}(\alpha)\widetilde{S}(\alpha)-\nu(\alpha)I\right]\widetilde{X}^{1/2}\right\|_F \leq \max\{\gamma,\Gamma\}(1-\alpha+\alpha\sigma)\nu+\max\{\gamma,\Gamma\}\frac{\mathrm{tr}\,(r_c)}{n}=\max\{\gamma,\Gamma\}\nu(\alpha).$$

Therefore, defining

$$G(\alpha)=\left(\widetilde{X}^{-1/2}\widetilde{X}(\alpha)\widetilde{S}(\alpha)\widetilde{X}^{1/2}\right)/\nu(\alpha),$$

it follows $G(\alpha)$ is nonsingular for all $\alpha\in[0,1]$ as $\|G(\alpha)-I\|\leq\max\{\gamma,\Gamma\}<1$. As a consequence, $\widetilde{X}(\alpha)$ and $\widetilde{S}(\alpha)$ are also nonsingular for $\alpha\in[0,1]$.

Then, following [32] combining (25) and (26) with a simple continuity argument demonstrates that for each $\alpha\in[0,1]$ we have $\left(\widetilde{X}(\alpha),\widetilde{S}(\alpha)\right)$ and $(X(\alpha),S(\alpha))$ are elements of $\mathcal{S}^n_{++}\times\mathcal{S}^n_{++}$. Then, noting our assumption $(X,y,S)\in\mathcal{F}^0(\mathcal{P})\times\mathcal{F}^0(\mathcal{D})$, along with equations (21b) and (21c), one can observe that $(X(\alpha),y(\alpha),S(\alpha))$ satisfies

$$\sum_{i\in[m]}y_iA^{(i)}+S-C=0,$$
$$A^{(i)}\bullet X-b_i=0,\quad i=1,\ldots,m,$$

and thus $(X(\alpha),y(\alpha),S(\alpha))\in\mathcal{F}^0(\mathcal{P})\times\mathcal{F}^0(\mathcal{D})$ for every $\alpha\in[0,1]$. Finally, we apply Lemma 1(a) with $(X,S)=(X(1),S(1))$ and $Q=P$, along with Lemma 1(b) with $(X,S)=(\widetilde{X}(1),\widetilde{S}(1))$ and $Q=\widetilde{X}^{-1/2}$, and equations (25), (26), (33) with $\alpha=1$, and (51) with $\alpha=1$, which yields

$$d\,(X(1),S(1))=d\left(\widetilde{X}(1),\widetilde{S}(1)\right)\leq\left\|H_{\widetilde{X}^{-1/2}}\widetilde{X}(1)\widetilde{S}(1)-\nu(1)I\right\|_F$$
$$\leq\left\|\widetilde{X}^{-1/2}(\widetilde{X}(1)\widetilde{S}(1)-\nu(1)I)\widetilde{X}^{1/2}\right\|_F\leq\Gamma\nu(1).$$

Therefore, $(\widehat{X},\hat{y},\widehat{S})=(X+\Delta X,y+\Delta y,S+\Delta S)\in\mathcal{N}_F(\Gamma)$, and hence (a) holds. Further, (b) follows immediately from the definition of σ and equation (33) with $\alpha=1$. □

Following from Theorem 6, we obtain the convergence result for Algorithm 2.

Corollary 1. *Let γ, δ and β be constants in $(0,1)$ and satisfying*

$$\frac{2\sqrt{2}\gamma}{1-\gamma}\leq 1,\quad \beta\leq\frac{1}{25}\frac{1}{\sigma(1-\gamma)^{1/2}}\sqrt{\frac{\gamma^2+(1-\sigma)^2}{1-\gamma}},\quad \frac{7.3264(\gamma^2+\delta^2)}{1-\gamma}+(2+\sqrt{2})\beta\sigma\gamma\leq\left(1-\frac{\delta}{\sqrt{n}}\right)\Gamma-\frac{\sigma\gamma^2}{\sqrt{n}}.$$

Then, every iterate (X^k,y^k,S^k) generated by the IF-QIPM in Algorithm 2 is an element of the neighborhood $\mathcal{N}_F(\gamma)$, and satisfies the relation $X^k\bullet S^k=(1-\delta/\sqrt{n})^k(X^0\bullet S^0)$. Further, the IF-QIPM terminates in at most $O(\sqrt{n}L)$ iterations.

Examples of constants γ, δ and β satisfying the conditions of Corollary 1 for $\eta=1/25$ are $\gamma=\delta=\beta=1/20$.

5.2 Implementing the Nesterov-Todd linear system

As in [22] and [4], we factorize the NT Newton linear system given by (18), and construct block encodings for its factors. Further, as shown in [4], one can compute the Nesterov-Todd scaling matrix in a purely quantum manner by repeatedly apply Prop.s 4, 5 and 6 to construct a block encoding of

$$W = S^{-1/2}(S^{1/2}XS^{1/2})^{1/2}S^{-1/2}$$

in time $\tilde{O}(\|S\|_F^4\kappa_S^5\kappa_X)$. As such, the most efficient way to use block encodings and QSLA in an iterative algorithm like an IPM is to pre-compute any matrix inverses and products *classically* and store the results in QRAM such that the block encodings of the factors of the Newton linear system can be constructed in time $\tilde{O}(1)$. Note that the larger matrices appearing in the Newton system, namely $Q_2 \in \mathbb{R}^{\frac{n(n+1)}{2}\times(\frac{n(n+1)}{2}-m)}$ and $\mathcal{A}_s^\top \in \mathbb{R}^{\frac{n(n+1)}{2}\times m}$, are only calculated once before the algorithm begins so their size is not prohibitive. Hence, compared to solving the Newton linear system, classical computation of matrix powers and products has an insignificant cost, and we circumvent increased dependence on the condition number.

Proposition 13. *Let*

$$M_1 = \begin{bmatrix}(P \otimes_s P^{-\top}S)Q_2 & 0\end{bmatrix}.$$

If S, P, $P^{-\top}$, Q_2, and $P^{-\top}S$ 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 14. *Let*

$$M_2 = \begin{bmatrix}0 & (PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top)\end{bmatrix}.$$

If X, P, $P^{-\top}$, $\mathcal{A}_s$, PX and $P^{-\top}S$ 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 $\tilde{O}(1)$.

Proposition 15. *The Nesterov-Todd linear system matrix* (18) *can be written compactly as:*

$$M_{NT} = \begin{bmatrix}(P \otimes_s P^{-\top}S)Q_2 & (PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top)\end{bmatrix}. \tag{52}$$

If X, S, P, $P^{-\top}$, $-\mathcal{A}_s^\top$, Q_2, PX and $P^{-\top}S$ are stored in QRAM. Then a $(\|M_{NT}\|_F, O(\log n), \xi/(\|M_{NT}\|_f\kappa^2\log^2\frac{\kappa}{\xi}))$-block encoding of M_{NT} can be constructed in time $\tilde{O}(1)$.

Proof. Carrying out the calculations shows that (15) corresponds to the Nesterov-Todd linear system. We construct the two following block encodings:

$$M_1 = \begin{bmatrix}(P \otimes_s P^{-\top}S)Q_2 & 0\end{bmatrix}$$
$$M_2 = \begin{bmatrix}0 & (PX \otimes_s P^{-\top})(-\mathcal{A}_s^\top),\end{bmatrix}$$

using Prop.s 13-14. 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 (52), 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 (52), in time $\tilde{O}(1)$. Since $\max\{\|M_1\|_F, \|M_2\|_F\} = O(\|M_{\text{NT}}\|_F)$, we obtain the claimed result. □

One should note that the construction of the Newton linear system provided in Prop. 15 is only one of the many possible ways to obtain a block encoding of our Newton linear system while utilizing the Nesterov-Todd direction. Further, though the Nesterov-Todd direction is the search direction we study in this manuscript, note that our construction is written in general terms of P, thus this construction can be used for any suitable choice of P, such as the AHO ($P = I$) and HKM ($P = S^{1/2}$) directions. Next, we use our factorization to solve the Newton system.

Theorem 7. *There is a quantum algorithm, which given $|\boldsymbol{svec}(R_c + r_c)\rangle$ and access to QRAM data structures encoding P, $P^{-\top}$, $-\mathcal{A}_s^\top$, Q_2, PX and $P^{-\top}S$, outputs a state ξ-close to $|\Delta\zeta \circ \Delta y\rangle$ in time*

$$\tilde{O}(\kappa \max\{\|M_1\|_F, \|M_2\|_2\},$$

using the Nesterov-Todd direction. We can also output an estimate of $\|\Delta\zeta \circ \Delta y\|$ with relative error δ by increasing the running time by a factor of $\frac{1}{\delta}$.

Proof. This is a direct consequence of Prop. 15 and Thm. 1. □

5.3 Overall Running Time

The IF-QIPM requires $O(n^{1/2} \ln 1/\epsilon)$ iterations. In each iteration, we must prepare and solve the quantum NT Newton 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. 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 $O(\sum_{k=1}^{\beta n^{1/2} \log(1/\epsilon)} T_{TO}(\xi_k) T_{LS})$, where ξ_k is the precision at iteration k. For the moment, we are neglecting the complexity of the classical computations necessary for the scaling matrices; this complexity is discussed at the end of this section, where it is shown to be negligible compared to the running time of the remaining subroutines.

Let us know expand this expression using the running times for the state tomography algorithm described in Section 2.3, and $\xi_k \leq \|r_c^k\|$. We define for ease of notation. The expression of the total running time of the algorithm, $O(\sum_{k=1}^{\beta\sqrt{n}\log(1/\epsilon)} T_{TO}(\xi_k) T_{LS})$, can be rewritten as:

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

Computing the geometric series yields:

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

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:

$$\tilde{O}\left(\frac{n^{2.5}}{\epsilon}\varrho^2\kappa\right).$$

So far we have neglected the time of the classical computations for the scaling matrices, as well as to estimate the norm of the solution of the Newton linear system. For the first component, note that all the matrices involved in the computation of P have size $n \times n$, hence this time is n^ω; for the second component, as discussed in Sect. 5, it is negligible compared to tomography. Hence, the total running time is not affected.

6 Conclusion

In this work we present a provably convergent quantum interior point method for semidefinite optimization problems, building on recent advances in quantum linear system solvers. The quantization of classical

interior point methods is the subject of several recent papers in the literature. We compare the theoretical performance of classical and quantum interior point methods with respect to various input parameters, concluding that based on the current state of the art, our algorithm is the first convergent QIPM that provides a speedup in terms of the size of the problem.

A Proofs taken from other papers

References

[1] 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.

[2] Erling D Andersen and Knud D Andersen. The MOSEK interior point optimizer for linear programming: an implementation of the homogeneous algorithm. In *High Performance Optimization*, pages 197–232. Springer, 2000.

[3] Sanjeev Arora, Elad Hazan, and Satyen Kale. The multiplicative weights method: a meta-algorithm and its applications. *Theory of Computing, 8(6) 121-164*, 2012.

[4] Brandon R. Augustino, Giacomo Nannicini, Tamás Terlaky, and Luis Zuluaga. Quantum interior point methods for sdo: Challenges and advances. 2021.

[5] Aharon Ben-Tal and Arkadi Nemirovski. *Lectures on modern convex optimization: analysis, algorithms, and engineering applications*. SIAM, 2001.

[6] Stephen Boyd, Laurent El Ghaoui, Eric Feron, and Venkataramanan Balakrishnan. *Linear Matrix Inequalities in System and Control Theory*, volume 15. SIAM, 1994.

[7] Fernando GS L Brandao, Richard Kueng, and Daniel Stilck França. Faster quantum and classical sdp approximations for quadratic binary optimization. *arXiv preprint arXiv:1909.04613*, 2019.

[8] Fernando GSL Brandao and Krysta M Svore. Quantum speed-ups for solving semidefinite programs. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 415–426. IEEE, 2017.

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

[10] PAM Casares and MA Martin-Delgado. A quantum interior-point predictor–corrector algorithm for linear programming. *Journal of physics A: Mathematical and theoretical*, 53(44):445305, 2020.

[11] 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.

[12] Alexandre d'Aspremont, Laurent El Ghaoui, Michael I Jordan, and Gert RG Lanckriet. A direct formulation for sparse pca using semidefinite programming. *SIAM review*, 49(3):434–448, 2007.

[13] Etienne de Klerk, Cornelis Roos, and Tamás Terlaky. Initialization in semidefinite programming via a self-dual skew-symmetric embedding. *Operations Research Letters*, 20(5):213–221, 1997.

[14] Yonina C Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Transactions on Information Theory*, 49(2):446–456, 2003.

[15] 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.

[16] Michel X Goemans and David P Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM (JACM)*, 42(6):1115–1145, 1995.

[17] Sander Gribling. *Applications of Optimization to Factorization Ranks and Quantum Information Theory*. PhD. Thesis, CentER, Tilburg University, 2019.

[18] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv preprint quant-ph/0208112*, 2002.

[19] 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.

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

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

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

[23] Iordanis Kerenidis and Anupam Prakash. A quantum interior point method for LPs and SDPs. *ACM Transactions on Quantum Computing*, 1(1):1–32, 2020.

[24] Iordanis Kerenidis, Anupam Prakash, and Dániel Szilágyi. Quantum algorithms for second-order cone programming and support vector machines. *arXiv preprint arXiv:1908.06720*, 2019.

[25] Michael Keyl. Quantum state estimation and large deviations. *Reviews in Mathematical Physics*, 18(01):19–60, 2006.

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

[27] 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.

[28] Gert RG Lanckriet, Nello Cristianini, Peter Bartlett, Laurent El Ghaoui, and Michael I Jordan. Learning the kernel matrix with semidefinite programming. *Journal of Machine learning research*, 5(Jan):27–72, 2004.

[29] Todd Michael J. A study of search directions in primal-dual interior-point methods for semidefinite programming. *Optimization Methods and Software*, 11(1-4):1–46, 1999.

[30] RDC Monteiro. A unified analysis for a class of path-following primal-dual interior-point algorithms for semidefinite programming. *Mathematical Programming*, 1996.

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

[32] Renato DC Monteiro. Polynomial convergence of primal-dual algorithms for semidefinite programming based on the Monteiro and Zhang family of directions. *SIAM Journal on Optimization*, 8(3):797–812, 1998.

[33] Renato DC Monteiro and Takashi Tsuchiya. Polynomial convergence of a new family of primal-dual algorithms for semidefinite programming. *SIAM Journal on Optimization*, 9(3):551–577, 1999.

[34] 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.

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

[36] 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.

[37] Yurii E Nesterov and Michael J Todd. Primal-dual interior-point methods for self-scaled cones. *SIAM Journal on Optimization*, 8(2):324–364, 1998.

[38] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, pages 899–912, 2016.

[39] Eric M Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47(7):2921–2933, 2001.

[40] Kathrin Schacke. On the kronecker product. *Master's thesis, University of Waterloo*, 2004.

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

[42] Jos F Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11(1-4):625–653, 1999.

[43] 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.

[44] Kim-Chuan Toh, Michael J Todd, and Reha H Tütüncü. SDPT3—a MATLAB software package for semidefinite programming, version 1.3. *Optimization Methods and Software*, 11(1-4):545–581, 1999.

[45] Paul Tseng. Search directions and convergence analysis of some infeasibnle path-following methods for the monoton semi-definite LCP. *Optimization Methods and Software*, 9(4):245–268, 1998.

[46] Joran van Apeldoorn and András Gilyén. Improvements in quantum SDP-solving with applications. *arXiv preprint arXiv:1804.05058*, 2018.

[47] Joran Van Apeldoorn, András Gilyén, Sander Gribling, and Ronald de Wolf. Quantum sdp-solvers: Better upper and lower bounds. *Quantum*, 4:230, 2020.

[48] John Watrous. Semidefinite programs for completely bounded norms. *arXiv preprint arXiv:0901.4709*, 2009.

[49] Kilian Q Weinberger and Lawrence K Saul. Unsupervised learning of image manifolds by semidefinite programming. *International journal of computer vision*, 70(1):77–90, 2006.

[50] Henry Wolkowicz, Romesh Saigal, and Lieven Vandenberghe. *Handbook of semidefinite programming: theory, algorithms, and applications*, volume 27. Springer Science & Business Media, 2012.

[51] 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.

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