Abstract

A recent breakthrough in Edmonds’ problem showed that the noncommutative rank can be computed in deterministic polynomial time, and various algorithms for it were devised. However, only quite complicated algorithms are known for finding a so-called shrunk subspace, which acts as a dual certificate for the value of the noncommutative rank. In particular, the operator Sinkhorn algorithm, perhaps the simplest algorithm to compute the noncommutative rank with operator scaling, does not find a shrunk subspace. Finding a shrunk subspace plays a key role in applications, such as separation in the Brascamp-Lieb polytope, one-parameter subgroups in the null-cone membership problem, and primal-dual algorithms for matroid intersection and fractional matroid matching.

In this paper, we provide a simple Sinkhorn-style algorithm to find the smallest shrunk subspace over the complex field in deterministic polynomial time. To this end, we introduce a generalization of the operator scaling problem, where the spectra of the marginals must be majorized by specified vectors. Then we design an efficient Sinkhorn-style algorithm for the generalized operator scaling problem. Applying this to the shrunk subspace problem, we show that a sufficiently long run of the algorithm also finds an approximate shrunk subspace close to the minimum exact shrunk subspace. Finally, we show that the approximate shrunk subspace can be rounded if it is sufficiently close. Along the way, we also provide a simple randomized algorithm to find the smallest shrunk subspace.

As applications, we design a faster algorithm for fractional linear matroid matching and efficient weak membership and optimization algorithms for the rank-2 Brascamp-Lieb polytope.
1 Introduction

Let \( \mathcal{A} \subseteq \mathbb{C}^{n \times n} \) be a matrix space spanned by \( A_1, \ldots, A_p \in \mathbb{C}^{n \times n} \). Edmonds’ problem is to decide whether \( \mathcal{A} \) has a matrix of full rank, denoted \( \text{rank} \mathcal{A} = n \). There is a simple randomized algorithm for Edmonds’ problem, but derandomizing it is a central question in polynomial identity testing. The completeness of the determinant for polynomial identity testing [Val79] implies that a positive solution to Edmonds’ problem would imply historically intractable circuit lower bounds [KI04], so it comes as no surprise that Edmonds’ problem remains open.

The noncommutative Edmonds problem is to compute a relaxed notion of rank known as the noncommutative rank \( \text{nc-rank} \mathcal{A} \) defined as

\[
\text{nc-rank} \mathcal{A} = \min \{ n - \dim U + \dim \mathcal{A}(U) : U \text{ subspace of } \mathbb{C}^n \},
\]

where \( \mathcal{A}(U) = \langle Au : A \in \mathcal{A}, u \in U \rangle \). Equivalently, \( \text{nc-rank} \mathcal{A} = n - c \), where \( c \) is the largest difference between \( \dim U \) and \( \dim \mathcal{A}(U) \). We call such a subspace \( U \) a \( c \)-shrunk subspace. If \( \mathcal{A} \) is an yes instance of the Edmonds problem, then clearly \( \text{nc-rank} \mathcal{A} = \text{rank} \mathcal{A} = n \), i.e., \( \dim U = \dim \mathcal{A}(U) \) for all subspaces \( U \). The noncommutative Edmonds problem is equivalent to testing the identity of noncommutative rational formulae [FR04], and arises in diverse contexts such as the invariant theory of quivers [DM17] and statistical estimation [AKRS21].

Maximum bipartite matching can be formulated as a special case of this problem, and the \( c \)-shrunk subspace amounts to the “maximum deficiency set” from Hall’s theorem. Several independent works by Garg, Gurvits, Oliveira, Wigderson [GGOW16], Ivanyos, Quiao, Subramanyam [IQS18], and Hamada and Hirai [HH21] exhibited deterministic polynomial-time algorithms for the noncommutative Edmonds’ problem, showing that the noncommutative version of the problem is significantly easier.

The three algorithms have very different approaches. [GGOW16], following [Gur04], reduces the problem to the boundedness of a certain optimization problem over matrix groups known as the capacity. The algorithm for solving this optimization problem, known as operator scaling, is a delightfully simple generalization of Sinkhorn’s algorithm [Sin64] for re-weighting (or “scaling”) the rows and columns of a nonnegative matrix to make it doubly stochastic (matrix scaling). However, the iterative algorithm lacks one key feature shared by a more sophisticated submodular minimization approach of [HH21] and algebraic approach of [IQS18]: the optimization algorithm of [GGOW16] does not produce a \( c \)-shrunk subspace.

The \( c \)-shrunk subspace can be viewed as a certificate bounding the noncommutative rank, and such certificates are useful in optimization applications (e.g. dual certificates) as well as computational invariant theory (it can be viewed as a 1-parameter subgroup taking the tuple of matrices to the origin). For instance, the \( c \)-shrunk subspace arises as a dual certificate in algorithms for the weighted matroid intersection problem and its generalizations [Van92, CLV01a, GP13]. Also, finding a \( c \)-shrunk subspace is crucial in a weak separation algorithm for the Brascamp-Lieb polytope by [GGOW18].

Geometric invariant theory provides another motivation for finding shrunk subspaces - in the \( m = n \) case, the group \( G = \text{SL}(n) \times \text{SL}(n) \) (pairs of matrices with determinant one) naturally acts on the tuple \( (A_1, \ldots, A_p) \) generating \( \mathcal{A} \) by \( (g, h) \cdot (A_1, \ldots, A_p) = (gA_1h^\dagger, \ldots, gA_p h^\dagger) \). This is the well-studied left-right action. It is known that all homogeneous invariant polynomials invariant under this group action vanish on the tuple \( (A_1, \ldots, A_p) \), i.e. the tuple is in the null-cone, if and only if \( \mathcal{A} \) has a shrunk subspace [BD06]. The Hilbert-Mumford criterion states that null-cone membership holds if and only if there is a one-parameter subgroup (1-PSG) of \( G \) driving the Euclidean norm.
of \((A_1, \ldots, A_p)\) to zero \cite{MFK94}. 1-PSG’s are deterministic certificates of null-cone membership, as opposed to oracle access to a random invariant polynomial. Shrunk subspaces encode such 1-PSG’s, and \(c\)-shrunk subspaces correspond to 1-PSG’s driving the tuple to the origin the “fastest.” Efficiently deciding null-cone membership for general linear group actions remains an interesting open problem.

1.1 Our contribution

We show how to modify the Sinkhorn-style operator scaling algorithm from \cite{GGOW16} to find the smallest \(c\)-shrunk subspace of \(A\). We view our result as evidence that continuous optimization is a viable, or at least competitive, approach to polynomial identity testing problems in invariant theory. Along the way, we find a simple randomized algorithm to find the smallest \(c\)-shrunk subspace of \(A\) using Wong sequences. Even when allowing randomness, the sophisticated deterministic algorithms of \cite{HH21} and \cite{IQS18} were the only known methods to find a \(c\)-shrunk subspace.

The idea of the deterministic iterative algorithm is as follows. Gurvits’s original operator Sinkhorn algorithm \cite{Gur04} can be seen as alternating minimization of an objective function (Equation 2.5) on the space of (pairs of) positive-definite matrices. When the objective function is unbounded, a sufficiently long run of Gurvits’s algorithm yields an approximate shrunk subspace, a notion we define formally in Definition 3.7. It is easy to modify the objective function (Equation 3.6) to yield an approximate \(c\)-shrunk subspace; see Section 3.1 for how to read off the maximum deficiency subset in the case of matrix scaling. Even so, it is not obvious how to obtain a true \(c\)-shrunk subspace from a mere approximate one. It is not clear that every approximately \(c\)-shrunk subspace is close to some \(c\)-shrunk subspace, let alone how to find the nearby true shrunk subspace.

To fix this issue, we further “perturb” the objective function (Equation 3.7) to find an \(\varepsilon\)-approximate \(c\)-shrunk subspace of dimension at most the dimension \(r^*\) of the true smallest \(c\)-shrunk subspace in time polynomial in \(\log(1/\varepsilon)\) and the input size - see Algorithm 4, and for the algorithm’s guarantees see Theorem 3.12. It is well-known that the true smallest \(c\)-shrunk subspace is unique, and we show it has polynomial bit complexity (Theorem 3.14). This follows from the analysis of our simple randomized algorithm to output the smallest \(c\)-shrunk subspace. Finally, we show a stability result for the smallest \(c\)-shrunk subspace, namely that an \(\exp(-\text{poly})\)-approximate \(c\)-shrunk subspace of dimension at most \(r^*\) is actually \(\exp(-\text{poly})\)-close to the true smallest \(c\)-shrunk subspace (Theorem 3.13). Together with our bit complexity bound, this shows our main result (Theorem 3.15): we can round our approximate \(c\)-shrunk subspace to the true smallest \(c\)-shrunk subspace.

1.2 Applications: rank-2 Brascamp-Lieb polytope and fractional linear matroid matching

As an application of our methods, we prove several algorithmic results about the Brascamp-Lieb polytope (BL polytope for short) \cite{BCCT08}. The BL polytope for full row-rank matrices \(B_i \in \mathbb{C}^{n_i \times n}\)
\((i = 1, \ldots, p)\) is the set of \(x \in \mathbb{R}^p\) such that
\[
\sum_{i=1}^{p} x_i \dim(B_iW) \geq \dim(W) \quad (W: \text{subspace of } \mathbb{C}^n)
\]
\[
\sum_{i=1}^{p} x_in_i = n,
\]
\[
\sum_{i=1}^{p} x_i \geq 0. \quad (i = 1, \ldots, p)
\]

The BL polytope with \(n_i = r\) for all \(i\) is called the rank-\(r\) BL polytope. We denote this polytope \(BL(B_1, \ldots, B_p)\) or concisely \(BL(B)\), where \(B = (B_1, \ldots, B_p)\).

It was shown in [BCCT08] that the BL polytope determines the finiteness of the Brascamp-Lieb inequalities in functional analysis, and [GGOW18] exhibited a separation algorithm for \(x \in \mathbb{Q}^p\) that runs in time polynomial in the sizes of \(B_i\) and the common denominator of entries of \(x\). Indeed, they reduced the separation problem to computing the noncommutative rank of a pseudopolynomial-size matrix space \(A\) with the following property. If \(x \in BL(B)\), then nc-rank \(A\) is full. If \(x \notin BL(B)\), then a shrunk subspace gives a violating subspace \(W\), i.e., \(\sum_{i=1}^{p} x_i \dim(B_iW) > \dim W\). The former can be verified by the operator Sinkhorn algorithm, but the latter cannot; they used an algebraic algorithm of [IQS18] separately to this end.

The BL polytope is significant in combinatorial optimization because various important polytopes are special cases of even low-rank BL polytopes. The rank-1 BL polytope is simply the base polytope of a linear matroid [Bar98] (over \(\mathbb{C}\)). [GGOW18] showed that the rank-2 BL polytope includes the common base polytope of two linear matroids. Indeed, we can observe that the rank-2 BL polytope is precisely the perfect fractional linear matroid matching polytope [Van92], which includes the fractional perfect matching polytope and the common base polytope and is totally dual half-integral [GP13]. The polytope obtained by removing the constraint \(\sum_i n_ix_i = n\) (after rewriting the inequalities in down-monotone form) is known as the fractional linear matroid matching polytope, and we refer to it as \(P(B)\). The maximum fractional linear matroid matching problem is to find \(x \in P(B)\) that maximizes \(\sum_i x_i\). This problem generalizes the maximum matroid intersection problem. The dual certificate, known as a minimum 2-cover, is a pair \((S, T)\) of subspaces such that \(\dim S + \dim T = k\) and \(\dim(S \cap \text{row } B_i) + \dim(T \cap \text{row } B_i) \geq 2\) for all \(i\), where \(k\) is twice the optimal value and \(T\) is the row-space of \(B_i\). Finding the minimum 2-cover in the special case of linear matroid intersection amounts to the submodular minimization formulation of the dual of maximum matroid intersection, which in the special case of bipartite matching is equivalent to finding the minimum cover (the dual problem to finding the maximum matching). The BL polytope can also be seen as a slice of a moment polytope, a certain polytope associated to a vector in a representation of a linear algebraic group. For more information about moment polytopes see [BFG+19]. Efficiently deciding membership in BL polytopes could lead to efficient algorithms for moment polytope membership, an open problem in computational invariant theory.

[CLV01a] gave an algorithm to solve the maximum fractional linear matroid matching problem with polynomially many calls to certain matroid oracles, and [GP13] showed how to use polynomially many calls to the algorithm of [CLV01a] to optimize linear functionals over the perfect fractional linear matroid matching polytope. Nonetheless, no algorithm for membership in rank-2 BL polytopes is known to be polynomial time! This is because the recursive nature of the oracle calls in [CLV01a, GP13] naively lead to bit complexity explosions of intermediate numbers.

The difficulty of optimization on BL polytopes is perhaps unsurprising. It is unclear how to
decide if a given inequality is valid for the polytope and in fact, it is not known that membership in the rank-2 BL polytope is in coNP! One could hope that a violating subspace could act as a coNP certificate for membership, but it is not known whether every inequality can be witnessed by a subspace of polynomial bit complexity.

As an application of our modified Sinkhorn algorithm, we prove the following two results in Section 7.

**Theorem 1.1** (informal, see Theorem 7.4). There is a deterministic algorithm that finds a $(1 - \varepsilon)$-maximum fractional linear matroid matching in $O(n^5(n + p))$ time for any $\varepsilon > 0$, where $n$ is the dimension of the ground space and $p$ is the number of matrices $B_i$.

**Theorem 1.2.** Membership in the rank-2 BL polytope is in $\text{NP} \cap \text{coNP}$.

The idea of the first result is as follows. First, we use the recent connection between a matrix space spanned by rank-2 skew-symmetric matrices and fractional linear matroid matching [OS22]. They showed that the noncommutative rank of such matrix spaces is twice the size of the maximum fractional linear matroid matching. We show that by applying our operator scaling algorithm to the matrix space, we can obtain a $(1 - \varepsilon)$-maximum fractional linear matroid matching.

Let us consider the second result. It is easy to show that the membership in the rank-2 BL polytope is in NP. Any $x \in BL(B)$ can be decomposed into a convex combination of half-integral vertices, so these vertices and convex coefficients form a certificate with polynomial bit complexity. Note that the membership of a half-integral vector can be checked in polynomial time by the result of [GGOW18] because the common denominator is a constant. In contrast, a coNP certificate is more intricate. As mentioned above, a violating subspace may not have bounded bit complexity. However, we can exploit half-integrality of $BL(B)$ (in the rank-2 case) and the fact that all facet-defining inequalities have coefficients in $\{0, 1, 2\}$ to provide a coNP certificate. The certificate for $x \notin BL(B)$ are $p$ affinely independent half-integral points $x^{(i)}$ ($i = 1, \ldots, p$) in $BL(B)$ satisfying a valid inequality for $P(B)$ (and hence for $BL(B)$) at equality, with $x^*$ violating this inequality. To verify that the corresponding inequality is valid, the verifier needs to also check that a point close to the centroid of the $x^{(i)}$’s is not in $P(B)$, and this (and the membership of the $x^{(i)}$’s) can be checked efficiently using [GGOW18] since the denominators are small. Details are given in a proof at the end of Section 7.3.

**A pseudopolynomial weighted algorithm for rank-2 $P(B)$**

Another option for the coNP certificate is through a formulation of the weighted fractional linear matroid matching problem as another scaling problem similar to the one used for the shrunk subspace problem. A natural extension of the Sinkhorn-style algorithm for the scaling problem (Algorithm 8) yields an algorithm that runs in time polynomial in the size of $B_i$ and the magnitude of weight:

**Theorem 1.3.** There is a deterministic algorithm to compute a point $x$ such that $w^Tx \geq \max\{w^Ty : y \in P(B)\} - \varepsilon$ in time polynomial in the input size of $B_i$, $\|w\|_1$, and $1/\varepsilon$.

Theorem 7.11 gives the precise time complexity. Using this algorithm, one can define an appropriate coNP certificate that can be verified in polynomial time.
An $\varepsilon$-membership algorithm for rank-2 $P(B)$

We have mentioned the link between the BL polytope and the moment polytope. [BFG+19] gave a randomized algorithm to decide the $\varepsilon$-membership problem for the moment polytope (to decide whether a point is $\varepsilon$-far from the moment polytope or $\varepsilon$-far from its complement) that runs in polynomial time in the input size and $1/\varepsilon$. Their analysis showed that the dependence on the common denominator in [GGOW18] is essentially not necessary. If one could show that the moment polytopes have a polynomial radius and inverse polynomial in-radius, a randomized algorithm for $\varepsilon$-optimization in time polynomial in $1/\varepsilon$ and the input size would follow by general reductions between membership, separation, and optimization [LSV18].

However, no inverse polynomial lower bound is known for the in-radius of moment polytopes, and even if this were the case, the BL polytope is only a slice of the full moment polytope. Nonetheless, we directly (without using Theorem 1.3) show the following:

**Theorem 1.4.** There is a deterministic algorithm (Algorithm 7) to decide the $\varepsilon$-membership problem for rank-2 $P(B)$ in time polynomial in the input size and $1/\varepsilon$.

The algorithm is yet another variant of the Sinkhorn-style algorithm described in [GGOW18]. As with [BFG+19], there is no dependence on the common denominator for the point in question. As $P(B)$ contains the origin and the simplex, and hence has polynomial in-radius, this result and [LSV18] imply a different algorithm, albeit a much slower randomized one, with guarantees matching Theorem 1.3. Without Theorem 1.3, Theorem 1.4 with only implies membership in $P(B)$ is in coMA due to the randomization in [LSV18].

1.3 Related work

Matrix scaling is a classic problem commonly appearing in various fields such as optimization, statistics, economics, and physics. See the comprehensive survey of Idel [Ide16] and references therein. The Sinkhorn algorithm is the standard algorithm for matrix scaling. Although the Sinkhorn algorithm converges to an approximate doubly stochastic matrix if a given matrix admits such scaling, it is nontrivial what happens if it diverges. [GR13] showed that the Sinkhorn algorithm has only two accumulation points by information geometry with the Kullback-Leibler divergence (KL-divergence). [Aas14] showed that the accumulation points exhibit a block diagonal structure which can be characterized combinatorially. Recently, Hayashi and Hirai [HH22] proved that one can obtain a Hall blocker (dual certificate showing that a given matrix has no scaling) by the Sinkhorn iteration.

Their analysis also used information geometry with the KL-divergence. However, it is unknown whether a similar result holds in operator scaling. A major obstacle is that the underlying geometry of operator scaling is unknown. The operator Sinkhorn algorithm is not an alternating minimization of the KL-divergence or other well-known divergences in quantum information theory [MS22]. We discuss in Section 3.1 how, when specialized to matrix scaling case, our algorithm results in a quite different method to find a Hall blocker from the Sinkhorn iteration.

**Organization of the paper.** The paper is organized as follows. In Section 2, we introduce necessary concepts and definitions. Section 3 describes our algorithms at a high level first for the simpler matrix scaling setting and then for the operator scaling setting. In Section 4, we introduce majorized operator scaling and our Sinkhorn-style algorithm. Section 5 discusses how to find an
approximate shrunk subspace with Sinkhorn iteration and Section 6 shows how to round it to the smallest $c$-shrunk subspace. In Section 7, we present applications of our algorithms to fractional linear matroid matching and the membership problem in the BL polytope.

2 Definitions and preliminaries

Notation. Throughout the paper, $p$ will denote the number of Kraus operators. Note that if the Kraus operators are $m \times n$ matrices then we can assume without loss of generality that $p \leq mn$. An upper bound on any entry of any of the Kraus operators is denoted by $M$. For a positive integer $i$, we define $[i] := \{1, \ldots, i\}$. For a vector $a$, the Euclidian norm is denoted by $\|a\|$ and the $\ell^p$ norm is by $\|a\|_p$. The all-one vector of length $n$ is denoted by $\mathbf{1}_n$. For a complex matrix $A$, the Hermitian conjugate, transpose, and complex conjugate of $A$ is denoted by $A^\dagger$, $A^T$, and $\overline{A}$, respectively. The Frobenius norm of $A$ is denoted by $\|A\|_F$ and the operator norm (i.e., the largest singular value) is by $\|A\|_1$. We denote the orthogonal projection onto a subspace $U$ by $\pi_U$. For a Hermitian matrix $A$, we denote by $\lambda(A)$ the vector whose entries are the eigenvalues of $A$ in nonincreasing order (unless stated otherwise). The matrix square root and matrix exponential of $A$ are denoted by $\sqrt{X}$ (or $X^{1/2}$) and $e^A$, respectively.

2.1 Matrix spaces and shrunk subspaces

Let $A$ be a matrix space spanned by $A_1, \ldots, A_p \in \mathbb{C}^{m \times n}$. We present a few equivalent definitions of the noncommutative rank of $A$. The first three are easily seen to be equivalent; the fourth is non-trivial. Only the fourth hints at the reason for the name - the matrices $X_i$ can be thought of as non-commuting indeterminates.

Definition 2.1 (noncommutative rank). The noncommutative rank of a matrix space $A = \langle A_1, \ldots, A_p \rangle \subseteq \mathbb{C}^{m \times n}$ (denoted by nc-rank $A$) is equivalently defined as follows.

1. (Fortin and Reutenauer [FR04]) Let $0_{s,t}$ denote an $s \times t$ zero matrix.

   \[
   \text{nc-rank } A = \min \left\{ m + n - s - t : P, Q \in GL(n), PA_iQ = \begin{bmatrix} * & * \\ * & 0_{s,t} \end{bmatrix} (i = 1, \ldots, p) \right\} \tag{2.1}
   \]

2. (Hirai and Hamada [HH21])

   \[
   \text{nc-rank } A = \min \{ m + n - \dim L - \dim R : L, R \text{ subspaces}, A_i(L, R) = \{0\} \text{ for all } i \}, \tag{2.2}
   \]

   where $A_i(L, R) = \{x^\dagger A_i y : x \in L, y \in R\}$. The minimization problem in (2.2), called the minimum vanishing subspace problem, is submodular function minimization on the product of the lattice of all vector subspaces and its order-reversed lattice. Namely, if $(L, R)$ and $(L', R')$ both attain the minimum, so do their join $(L + L', R \cap R')$ and meet $(L \cap L', R + R')$.

3. (Ivanyos et al. [IKQS15], Garg et al. [GGOW19])

   \[
   \text{nc-rank } A = \min \{ n - \dim U + \dim A(U) : U \text{ subspace of } \mathbb{C}^n \}, \tag{2.3}
   \]

   where $A(U) = \langle Au : A \in A, u \in U \rangle$. A subspace $U$ is called a $c$-shrunk subspace of $A$ if $\dim U - \dim A(U) \geq c$. The right-hand side of (2.3) equals $\min\{n-c : \exists c$-shrunk subspace of $A\}$.  


4. (Ivanyos, Qiao, and Subrahmanyan [IQS18])

\[
\text{nc-rank}\ A = \sup_{d=1}^{\infty} \max \left\{ \frac{1}{d} \text{rank} \left( \sum_{i=1}^{p} A_i \otimes X_i \right) : X_i \in \mathbb{C}^{d \times d} \right\}.
\] (2.4)

The minimum \(d\) that attains the supremum is called the minimum blow-up size of \(A\). It is known that the minimum blow-up size \(d\) of any matrix subspace is at most \(n - 1\) [DM17].

Feasible solutions of (2.1), (2.2), and (2.3) can be converted to each other. Given a feasible solution \((P, Q)\) of (2.1), let \(L\) and \(R\) be the subspaces spanned by the last \(s\) columns and \(t\) rows of \(P\) and \(Q\), respectively. Then, \((L, R)\) is a feasible solution of (2.2) with the same objective value. If \((L, R)\) is a feasible solution of (2.2), then \(A(L) \subseteq R^\perp\), so any feasible solution of (2.2) gives that of (2.3) without increasing the objective value. Finally, given a subspace \(U\), one can make an \((n - \text{dim } A(U)) \times \text{dim } U\) zero block by an appropriate basis change. Thus, the optimal value of (2.3) is at least that of (2.1).

We focus in particular on Item 2, the minimum vanishing subspace problem. In analogy with bipartite matching, if a \(c\)-shrunk subspace \(U\) is analogous to a violation of Hall’s condition with maximum defect, then the pair \(((A(U))^\perp, U)\) is analogous to a maximum independent set. We give such sets a name.

**Definition 2.2 (Independent set).** A pair of subspaces \(L \subseteq \mathbb{C}^n\) and \(R \subseteq \mathbb{C}^m\) is said to be independent if \(L \subseteq (AR)^\perp\), or equivalently if for all \(v \in L, w \in R\) we have

\[
w^\dagger A_i v = 0.
\]

The size of an independent set is defined as \(\text{dim } L + \text{dim } R\), and the maximum size of an independent set is equal to \(m + n - \text{nc-rank } A\).

The lattice of maximum independent sets has a unique maximum element \((L^*, R^*)\), which we call the dominant independent set, so that \(R^*\) is the smallest \(c\)-shrunk subspace. Let \(\ell^* = \text{dim } L^*, r^* = \text{dim } R^*,\) and \(k^* = \text{nc-rank } A\) so that \(\ell^* + r^* = n + m - k^*\).

### 2.2 Operator scaling

For a tuple \(A_1, \ldots, A_p\) of matrices in \(\mathbb{C}^{m \times n}\), we can associate the completely positive map (CP map for short) \(\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m}\) given by

\[
\Phi : X \mapsto \sum_{i=1}^{p} A_i X A_i^\dagger
\]

and \(A_1, \ldots, A_p\) are called the Kraus operators for \(\Phi\). The adjoint map \(\Phi^* : \mathbb{C}^{m \times m} \to \mathbb{C}^{n \times n}\) is given by \(\Phi^* : X \mapsto \sum_{i=1}^{p} A_i^\dagger X A_i\). For matrices \(B \in \mathbb{C}^{m \times m}\) and \(C \in \mathbb{C}^{n \times n}\), the operator \(\Phi_{B,C}\) with Kraus operators \(BA_1 C^\dagger, \ldots, BA_p C^\dagger\) is called a scaling of \(\Phi\) by \(B, C\). For \(n = m\), the operator \(\Phi\) is said to be \(\varepsilon\)-doubly stochastic if

\[
\|\Phi(I_n) - I_n\|_F, \|\Phi^*(I_n) - I_n\|_F \leq \varepsilon.
\]

We say that \(\Phi\) is scalable to doubly stochastic if \(\Phi\) has an \(\varepsilon\)-doubly stochastic scaling for every \(\varepsilon > 0\). There is a variational characterization of scalability through the following optimization problem
over positive-definite matrices. Define the capacity\(^1\) of \(\Phi\) as
\[
\text{cap } \Phi = \inf_{X > 0, Y > 0} \text{Tr } \Phi(X^{-1})Y^{-1} + \log \det X + \log \det Y.
\] (2.5)

Gurvits’ theorem, which was proven independently in the context of quiver representations by King [Kin94], states the following.

**Theorem 2.3** (Gurvits [Gur04]). For a CP map \(\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{n \times n}\), the following are equivalent:

1. \(\text{nc-rank } A = n\), where \(A\) is the matrix space spanned by the Kraus operators of \(\Phi\).
2. \(\Phi\) is scalable to doubly stochastic.
3. \(\text{cap } \Phi > -\infty\).

[GGOW19] showed that the capacity can be computed efficiently by a simple alternating minimization algorithm, which shows that deciding whether the noncommutative rank is full can be done in polynomial time.

**Remark 2.4** (Geodesic convexity). The objective function in the above optimization problem is not jointly convex in \(X\) and \(Y\), nor is it known to become convex under any simple change of variables. However, it is *geodesically convex*, i.e. convex along the curves of the form \(\sqrt{X}e^{H_1 t} \sqrt{X}, \sqrt{Y}e^{H_2 t} \sqrt{Y}\) through \((X,Y)\). These curves are the geodesics for a certain Riemannian metric on the manifold of positive definite matrices [Bha09]. For fixed \(Y\), the function is (Euclidean) convex in \(X\) under the change of variables \(X \leftarrow X^{-1}\) or \(X \leftarrow e^X\). The domains \(X > 0\) and \(X \geq I_n\) are both Euclidean convex and geodesically convex. All the objective functions we consider will have both joint geodesic convexity and Euclidean convexity in each matrix considered alone. We will not need to make use of geodesic convexity until Section 7.

Lastly, we describe the interaction between independent sets and CP maps. One verifies that \((L,R)\) is an independent set if and only if
\[
\text{Tr } \pi_L \Phi(\pi_R) = 0.
\] (2.6)

Furthermore, we can think of \((L^\perp, R^\perp)\) as a “cover” for \(\Phi\). In particular, by expanding \(I_n = \pi_R + \pi_{R^\perp}\) and \(I_m = \pi_L + \pi_{L^\perp}\) the above identity implies the following inequality:
\[
\text{Tr } \pi_{R^\perp} \Phi^*(I_m) + \text{Tr } \pi_{L^\perp} \Phi(I_n) \geq \text{Tr } \Phi(I_n).
\] (2.7)

### 3 Algorithm and analysis

Here we describe our algorithm at a high level. Before explaining it for shrunk subspace, we describe our ideas in a simpler case of matrix scaling. Then, we will see how these ideas generalize to the shrunk subspace problem.

---

\(^1\)Remark that the original definition of the capacity by [Gur04] is \(\text{cap'} \Phi = \inf_{X > 0} \frac{\det \Phi(X)}{\det X}\). One can check that \(\text{cap } \Phi = m + \log \text{cap'} \Phi\).
3.1 Warm-up: Finding Hall blockers in matrix scaling

Let \( A \in \mathbb{R}^{m \times n} \) be a nonnegative matrix and \( G = ([m], [n]; E) \) be the support graph of \( A \). That is, \( G \) is the bipartite graph with the vertex sets \([m], [n]\) and the edge set \( E = \{ij : A_{ij} \neq 0\} \). Our goal is to find a Hall blocker in \( G \), i.e., a column subset \( S \subseteq [n] \) such that \(|S| - |\Gamma(S)| = n - k^* \), where \( \Gamma(S) \) is the set of neighbors of \( S \) and \( k^* \) is the size of a maximum matching in \( G \). Note that this is equivalent to finding an independent set \((L, R)\) of \( G \) such that \(|L| + |R| \geq m + n - k^* \).

The classical Sinkhorn-Knopp theorem characterizes the scalability to a doubly stochastic matrix with the existence of a perfect matching in the support graph. We start with a generalization of the Sinkhorn-Knopp theorem to rectangular matrices and maximum matching.

**Definition 3.1 (Substochastic scalability of matrices).** We say a nonnegative matrix \( A \in \mathbb{R}^{m \times n} \) is **doubly substochastic** if
\[
A1_n \leq 1_m \quad \text{and} \quad A^T1_m \leq 1_n,
\]
where \( \leq \) denotes the usual element-wise order. We refer to \( \sum_{i,j} A_{ij} \) as the **size** of \( A \). We say that \( A \) is **\( k \)-scalable** if for every \( \varepsilon > 0 \), there is a scaling of \( A \) which is doubly substochastic and has size at least \( k - \varepsilon \).

Similar to the scalability to doubly stochastic matrices, one can characterize the \( k \)-scalability by a convex optimization problem. Let
\[
f_k(x, y, z) := \sum_{i,j} A_{ij} e^{z - y_i - x_j} + \sum_{j=1}^n x_j + \sum_{i=1}^m y_i - kz \tag{3.1}
\]
and
\[
\mathcal{D} := \{(x, y, z) : x \geq 0_n, y \geq 0_m, z \geq 0\} \subseteq \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}. \tag{3.2}
\]
We define the \( k \)-capacity of \( A \) by \( \text{cap}_k(A) := \inf_{(x,y,z) \in \mathcal{D}} f_k(x, y, z) \). By convex analysis, one can prove the following theorem. We do not provide the proof here; we will prove a generalization of this theorem for operator scaling in Theorem 3.9.

**Theorem 3.2 (Matrix scaling version of Theorem 3.9).** For a nonnegative matrix \( A \in \mathbb{R}^{m \times n} \), the following are equivalent:
1. There exists an independent set \((L, R)\) of \( G \) with \(|L| + |R| \geq m + n - k\).
2. \( A \) is \( k \)-scalable.
3. \( \text{cap}_k A > -\infty \).

One can check the finiteness of \( \text{cap}_k A \) and find a \( k \)-scaling (if it exists) with a variant of the Sinkhorn algorithm. In each iteration, we first scale up the whole matrix so that its size is at least \( k \). Then, if the scaled matrix violates the column sum constraint (resp. the row sum constraint), we scale down columns (resp. rows) to satisfy the constraint. We will repeat this until we find a \( k \)-scaling of size at least \((1 - \varepsilon)k\). Indeed, this is equivalent to applying alternating minimization of \( f_k(x, y, z) \). One can show that if \( A \) is \( k \)-scalable, then this algorithm finds a desired \( k \)-scaling in polynomially many iterations. To find the cardinality \( k^* \) of the maximum matching, we can simply do a binary search on \( k \).
Finding a Hall blocker with Sinkhorn iteration

If $A$ is not $k$- scalable, then the algorithm diverges even for $k' = k - 1/2$. Suppose that we have $(x, y, z) \in \mathcal{D}$ such that $f_{k'}(x, y, z)$ is very small. Can we find an independent set of size greater than $m + n - k$ from $(x, y, z)$? Indeed, one can obtain such an independent set by a simple rounding method.

**Lemma 3.3.** Suppose that $(x, y, z) \in \mathcal{D}$ satisfies $f_{k'}(x, y, z) \leq -C$ for some sufficiently large $C > 0$ and $k' := k - 1/2$. Then, there exists an independent set of size greater than $m + n - k$ and one can efficiently find it from $(x, y, z)$.

**Proof.** Let us first find a fractional cover of size at most $k$. Recall that a fractional cover of $G$ is a pair $\tilde{x}, \tilde{y} \in \mathbb{R}_{\geq 0}^{n}$ such that $\tilde{x}_{i} + \tilde{y}_{j} \geq 1$ for $i, j \in G$ and its size is $\sum_{i} \tilde{x}_{i} + \sum_{j} \tilde{y}_{j}$; the minimum size of a fractional cover is dual to the maximum size of a perfect matching.

Let $S := k'z - \sum_{j} x_{j} - \sum_{i} y_{i}$. Then $S$ is at least $C$ because the remaining term in $f_{k'}$ is always positive. Furthermore, $-x_{i} - y_{j} + z \leq \ln(S/A_{ij})$ for any $i j \in E$. Set $\tilde{x} = x/z, \tilde{y} = y/z$. Then $\tilde{x}_{j} + \tilde{y}_{i} \geq 1 - \ln(S/A_{ij})/z \geq 1 - k' \ln(S/A_{ij})/S$, and $\sum_{j} \tilde{x}_{j} + \sum_{i} \tilde{y}_{i} \leq k' - S/z < k'$. By making $C$, and hence $S$, large enough and renormalizing $\tilde{x}, \tilde{y}$ slightly, we can further convert this to a fractional cover of value less than $k$.

Once we obtain a fractional cover $(\tilde{x}, \tilde{y})$ of size less than $k$, we can round it to an independent set of size greater than $m + n - k$ as follows. For simplicity, assume that $k$ is an integer (even if $k$ is not an integer, a similar argument works with $\lfloor k \rfloor$ instead of $k$). Sort the rows and columns so that $\tilde{x}_{1} \geq \cdots \geq \tilde{x}_{n}$ and $\tilde{y}_{1} \geq \cdots \geq \tilde{y}_{m}$. Consider the set $I$ of indices $(i, j) \in [m] \times [n]$ such that $i + j = k + 1$. Note that $|I| = k$. Then we have $\frac{1}{k} \sum_{(i, j) \in I} (\tilde{x}_{j} + \tilde{y}_{i}) \leq \frac{1}{k} (\sum_{j} \tilde{x}_{j} + \sum_{i} \tilde{y}_{i}) < 1$. Therefore, there exists $(i, j) \in I$ such that $\tilde{x}_{j} + \tilde{y}_{i} < 1$. Since $\tilde{x}_{j}, \tilde{y}_{i}$ are non-increasing, we have $\tilde{x}_{j'} + \tilde{y}_{i'} < 1$ for $i' \geq i$, $j' \geq j$. Because $(\tilde{x}, \tilde{y})$ is a fractional cover, this implies that $L = \{i, \ldots, m\}$, $R = \{j, \ldots, n\}$ form an independent set. The size of $(L, R)$ is $(m-i+1) + (n-j+1) = m + n - k + 1$.

Therefore, running the variant of the Sinkhorn algorithm for $k = k^{*} + 1$, we obtain a maximum independent set of size $m + n - k^{*}$ witnessing that the size of maximum matching is $k^{*}$.

Finding the smallest Hall blocker with perturbed capacity

Now let us consider a slightly more refined problem. Can we find the smallest minimizer $S^{*}$ of the surplus function $|G(S)| - |S|$? Note that the surplus function is submodular and hence the minimizers form a distributive lattice, so the smallest minimizer exists. Again, this is equivalent to finding the independent set $(L^{*}, R^{*})$ such that $|L^{*}| + |R^{*}| = m + n - k^{*}$ and $|R^{*}|$ is smallest.

By the Dulmage-Mendelsohn decomposition, $R^{*}$ is the set of vertices exposed (i.e., not covered) by some maximum matching (see, e.g., [Mur09, Section 2.2.3]). Therefore, there exists a $k^{*}$-scaling of $A$ such that the $i$th column sum is at most $1 - 1/n$ for $i \in R^{*}$ and at most 1 elsewhere. For a fixed candidate of $R^{*}$, we can check if there is such a scaling by matrix scaling with specified marginals. The obvious problem here is that the number of candidates is exponential.

We can address this issue with a perturbed version of $k$-capacity. Let $r^{*}$ be the size of $R^{*}$. We say $(k, r)$ is violated by an independent set $(L, R)$ either if $|L| + |R| > m + n - k$ or if $|L| + |R| = m + n - k$ and $|R| > r$. The key observation here is that one can also check whether $(k, r)$ is violated by
\((L^*, R^*)\) or not by a similar scaling problem as above. Let

\[
f_{k,r}(x,y,z) := \sum_{i,j} A_{ij} e^{z_{-y_i-x_j}} + \sum_{j=1}^r x_j^+ + \sum_{j=r+1}^m \left(1 - \frac{1}{n}\right) x_j^+ + \sum_{i=1}^m y_i - k z,
\]

where \(x_1^+ \geq \cdots \geq x_n^+\) denotes the entries of \(x\) in a non-increasing order. Since \(f_{k,r}(x,y,z) = f_k(x,y,z) - \frac{1}{n} \sum_{i=1}^m y_i\), the new function \(f_{k,r}\) can be considered as a “perturbed” objective function. Note that \(f_{k,r}\) is still a convex function. Let \(\text{cap}_{k,r} A := \inf_{(x,y,z) \in D} f_{k,r}(x,y,z)\). Again, one can prove that \(\text{cap}_{k,r}\) gives the desired characterization of tuple \((k,r)\).

**Theorem 3.4** (Matrix scaling version of Theorem 3.10). For a non-negative matrix \(A \in \mathbb{R}^{m \times n}\) and \(0 \leq k, r \leq n\) integers, the following are equivalent:

1. \((k,r) \leq (k^*, r^*)\) in lexicographic order, i.e. there is no independent set violating \((k,r)\).
2. \(\text{cap}_{k,r} A > -\infty\).

We can tweak the Sinkhorn algorithm to check the finiteness of \(\text{cap}_{k,r} A\) (and even find the desired scaling if it exists) in polynomial time. So we can find \(r^*\) by binary search. Furthermore, by a similar rounding argument as above, given \((x,y,z) \in D\) with sufficiently small \(f_{k,r}(x,y,z)\), it is possible to find an independent set \((L,R)\) violating \((k,r)\). So, applying it for \(k = k^*\) and \(r = r^* + 1\), one can find the desired smallest minimizer \(R^*\).

### Majorization scaling of matrices

The above scaling problem—finding a \(k\)-scaling with the column sums at most \(1 - 1/n\) for \(r^*\) columns and at most 1 elsewhere—can be cast as a more general scaling problem, which we call majorization scaling.

**Definition 3.5** (Majorization scalability of matrices). For a vector \(x \in \mathbb{R}^n\), let \(x^+ \in \mathbb{R}^n\) denote \(x\) sorted in non-increasing order. The vector \(x \in \mathbb{R}^n\) is weakly majorized by \(y \in \mathbb{R}^n\), denoted by \(x \preceq y\), if

\[
\sum_{i=1}^s x_i^+ \leq \sum_{i=1}^s y_i^+
\]

for each \(s \in [n]\). For non-increasing vectors \(\alpha \in \mathbb{R}^n\) and \(\beta \in \mathbb{R}^m\), we say \(A\) is \((\alpha,\beta)\)-majorized if

\[
A 1_n \preceq \alpha, \quad A^T 1_m \preceq \beta.
\]

We say \(A\) is \(k\)-scalable to \((\alpha,\beta)\) if for every \(\varepsilon > 0\), there is a scaling of \(A\) which is \((\alpha,\beta)\)-majorized and has size at least \(k - \varepsilon\).

Interestingly, the majorization scalability is also characterized by convex optimization. Define

\[
f_k^{\alpha,\beta}(x,y,z) := \sum_{i,j} A_{ij} e^{z_{-y_i-x_j}} + \sum_{j=1}^n \alpha_j x_j^+ + \sum_{i=1}^m \beta_j y_i^+ - k z,
\]

(3.4)
and define the \((\alpha, \beta)\)-capacity of \(A\) by \(\text{cap}_{k}^{\alpha,\beta} := \inf_{(x,y,z) \in \mathcal{D}} f_{k}^{\alpha,\beta}(x, y, z)\). Note that the above \((k, r)\)-capacity is the special case

\[
\alpha = (1, \ldots, 1, 1 - 1/n, \ldots, 1 - 1/n), \quad \beta = 1_m.
\]

Again by convex optimization, we can show the following theorem.

**Theorem 3.6** (Matrix scaling version of Theorem 4.3). For a non-negative matrix \(A \in \mathbb{R}^{m \times n}\) and \(0 \leq k, r \leq n\) integers, the following are equivalent:

1. there exists a \(k\)-scaling to \((\alpha, \beta)\)
2. \(\text{cap}_{k}^{\alpha,\beta} A > -\infty\).

Furthermore, if there exists a \(k\)-scaling to \((\alpha, \beta)\), we can find it with a variant of the Sinkhorn algorithm.

We will prove a generalization of this theorem to operator scaling in Section 4. To our knowledge, even for the matrix scaling setting, our majorization scaling is novel.

### 3.2 High-level description of algorithm

Now we describe our algorithm (Algorithm 1, ROUNDSUBSPACES) for the shrunk subspace problem at a high level, together with the theorems and concepts needed to analyze it.

Before doing so, we need to define an approximate notion of shrunk subspaces. We define approximate shrunk subspaces by instead defining approximate independent sets.

**Definition 3.7** (Approximate independent set). Say a pair of subspaces \(L \subseteq \mathbb{C}^n, R \subseteq \mathbb{C}^m\), is \(\epsilon\)-independent if for all \(v \in L, w \in R\) we have

\[
|w^\dagger A_i v| \leq \epsilon \|w\| \cdot \|v\|.
\]

Our algorithm will find the value of \(k^* = \text{nc-rank} A\) and then the value of \(r^*\), the minimum value of \(\dim R\) for \((L, R)\) a maximum independent set. For a candidate pair of values \((k, r)\), we say \((k, r)\) is violated by a pair of subspaces \((L, R)\) if either \(\dim L + \dim R > m + n - k\) or if \(\dim L + \dim R = m + n - k\) and \(\dim R < r\). Note that \((k^*, r^*)\) is the largest pair (in lexicographic order) with no violating independent set, so if we can test whether \((k, r)\) has a violating independent set we can find \(k^*\) and \(r^*\) using binary search.

### Characterization of noncommutative rank

We begin by characterizing the noncommutative rank with optimization. Like the Sinkhorn-Knopp theorem, Gurvits’s theorem (Theorem 2.3) doesn’t directly answer the problem of distinguishing if \(\text{nc-rank} A \geq k\) for other \(1 \leq k \leq n\). There is a trick [GGOW19, Theorem A.4] to reduce to the case \(k = n\), which is analogous to adding dummy vertices to a bipartite graph in order to reduce maximum matching to perfect matching. Here we show how to do it directly using a modified scaling problem.
Definition 3.8 (Substochastic scalability). We say a CP map \( \Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m} \) is doubly substochastic if
\[
\Phi(I_n) \preceq I_n \quad \text{and} \quad \Phi^*(I_m) \preceq I_n,
\]
where \( \preceq \) denotes the Loewner ordering. We refer to \( \text{Tr} \Phi(I_n) \) as the size of \( \Phi \). We say that \( \Phi \) is \( k \)-scalable if for every \( \varepsilon > 0 \), there is a scaling of \( \Phi \) which is doubly substochastic and has size at least \( k - \varepsilon \).

There is also a variational characterization of the \( k \)-scalability of CP maps analogous to that of non-negative matrices. Consider the domain
\[
D := \{(X,Y,z) : X \succeq I_n, Y \succeq I_m, z \geq 0\} \subseteq \mathbb{C}^{n \times n} \times \mathbb{C}^{m \times m} \times \mathbb{R},
\]
and the following function
\[
f_k(X,Y,z) := \text{Tr}(\Phi(X^{-1})Y^{-1}e^z) + \log \det(X) + \log \det(Y) - kz.
\]
on \( D \). Note that \( \text{cap}_n \Phi = \text{cap} \Phi \). We will show the following generalization of Gurvits’ theorem.

Theorem 3.9. For a CP map \( \Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m} \), the following are equivalent:

1. \( \text{nc-rank} \mathcal{A} \geq k \).
2. \( \Phi \) is \( k \)-scalable.
3. \( \text{cap}_k \Phi > -\infty \).

The above theorem characterizes the maximum size of an independent set as \( m + n - k^* \), where \( k^* \) is the largest \( k \) such that \( \text{cap}_k \Phi > -\infty \). Because \( \text{cap}_n \Phi = \text{cap} \Phi \), Theorem 3.9 implies Gurvits’ theorem. We will not explicitly prove Theorem 3.9 because it is implied by stronger theorems stated later on (Theorems 3.10 and 4.3).

Characterization of \( r^* \) and rounding

We would also like to characterize \( r^* \), i.e. how small \( R \) can be in a maximum independent set \((L,R)\). For this we will need a perturbed version of \( f_k \). For a Hermitian matrix \( H \in \mathbb{C}^{n \times n} \), let \( \lambda(H) \in \mathbb{R}^n \) denote the spectrum of \( H \) in non-increasing order. Define the function
\[
f_{k,r}(X,Y,z) := f_k(X,Y,z) - \frac{1}{n} \sum_{i=n-r+1}^{n} \lambda_i(\log(X))
\]
on \( D \), and again define
\[
\text{cap}_{k,r} \Phi = \inf_{T \in D} f_{k,r}(T).
\]
We show that this optimization problem characterizes the dimensions of the dominant independent set. In fact one can use the slightly larger quantity \( \text{cap}_{k',r} \Phi \) for \( k' = k - \frac{1}{2n} \); this will turn out to be helpful in finding independent sets.

Theorem 3.10. For a CP map \( \Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m} \) and \( 0 \leq k, r \leq n \) integers, the following are equivalent:
1. \((k, r) \leq (k^*, r^*)\) in lexicographic order, i.e. there is no independent set violating \((k, r)\).

2. \(\text{cap}_{k,r} \Phi > -\infty\).

3. \(\text{cap}_{k,r} \Phi > -\infty\) for \(k' = k - \frac{1}{2n}\).

Note that \(\text{cap}_{k,0} \Phi = \text{cap}_k \Phi\), so Theorem 3.10 implies the equivalence between (1) and (3) in Theorem 3.9. There will also be a scaling characterization analogous to of (2) in Theorem 2.3 and Theorem 3.9, but the cap equivalence will hold at a more general level described in Section 4. Fortunately, there is an optimization algorithm to decide the finiteness of \(\text{cap}_k \Phi\) and \(\text{cap}_{k,r} \Phi\), and if \(\text{cap}_{k,r} \Phi = -\infty\), we can also use the optimization problem to find an approximate independent set \((L, R)\) that violates \((k, r)\).

Firstly, there is an optimization algorithm, \texttt{SINKHORNDECISION}(\Phi, k, r) (Algorithm 3), which can decide whether \(\text{cap}_{k,r} \Phi\) is finite in time \(\text{poly}(\log M, n, m)\). Formally:

**Theorem 3.11.** \texttt{DECISIONSINKHORN}(\Phi, k, r) (Algorithm 3) correctly decides whether \(\text{cap}_{k,r} \Phi > -\infty\) or not and takes \(O((m+n+p)(k(n+m)^4 \log(m+n)+n(n+m)^2 \log Mp))\) arithmetic operations if \(r = 0\) and \(O((m+n+p)(k^{n^2}+n+m)^4 \log(m+n)+n(n+m)^2 \log Mp))\) operations if \(r > 0\).

Secondly, there is another algorithm, \texttt{APPROXINDEP}, which on input \(\Phi\) with \(\text{cap}_{k,r} \Phi = -\infty\) outputs an \(\varepsilon\)-independent set \((L, R)\) violating \((k, r)\) in time \(\text{poly}(\log M, n, m, \log(1/\varepsilon))\).

**Theorem 3.12.** If \(\text{cap}_{k,r} \Phi = -\infty\), \texttt{APPROXINDEP}(\Phi, k, r, \varepsilon) (Algorithm 4) produces an \(\varepsilon\)-independent set violating \((k, r)\) and requires \(O(k^2n^3(m+n)^3(m+n+p)\log(2e^2nk^2/\varepsilon))\) arithmetic operations.

Here it may be helpful to consider the difference between the operator scaling and matrix scaling cases. In the matrix scaling case discussed in Section 3.1, there was no need to round the independent set (Hall blocker). This is because of the discrete nature of the covers - they are finite subsets of indices. In the operator scaling case, however, the independent sets range over all subspaces. One can slightly perturb an independent set to obtain another approximate independent set - without some additional rounding, we can never be sure we didn’t find one of these slightly perturbed versions of the true one. From another viewpoint, in the operator scaling case there are many possible eigenbases for approximate minimizers of the objective function.

If we choose \(k = k^*, r = r^* + 1\) and \(\varepsilon\) small enough, but still inverse exponential, the next theorem shows the only approximate independent set that can be found is very close to the dominant independent set. For a subspace \(S \subseteq C^n\), let \(\pi_S\) denote the orthogonal projection to \(S\).

**Theorem 3.13.** Suppose the Kraus operators of \(\Phi\) have integer entries of absolute value at most \(M\), and that \((L, R)\) is an \(\varepsilon\)-independent set for \(\Phi\) that violates \((k^*, r^* + 1)\). For \(\varepsilon \leq \varepsilon_0 = e^{O(n^{(n+m) \log(m+n)+n \log M})}\), we have

\[
\|\pi_L - \pi_{L^*}\|_2, \|\pi_R - \pi_{R^*}\|_2 = e^{O(n^2(n+m) \log(m+n)+n^2 \log M)p}\varepsilon =: M_0\varepsilon
\]

The proof of this theorem is inspired by the modular lattice property of the maximum independent sets - if an \(\varepsilon\)-independent set violates \((k^*, r^* + 1)\) and it is sufficiently far from \((L^*, R^*)\), then we can combine them using something similar to the lattice operation to obtain an \(\varepsilon'\)-independent set \((L, R)\) where \(\dim R < \dim R^*\) and \(\varepsilon'\) is larger, but not too much larger, than \(\varepsilon\). The technical work of the proof is in defining the approximate version of the lattice operation and showing that \(\dim R \geq \dim R^*\) for \(\varepsilon\) small enough.
Finally, we show that the orthogonal projection to $R^*$ has rational entries with exponential denominators. This shows we only need to find an approximate independent set that is exponentially close to the true one, and then we can round to the dominant independent set.

**Theorem 3.14.** The entries of $\pi_{R^*}$ are rational numbers with common denominator at most $M_1 = e^{O(n^5 \log(Mn))}$.

Putting these things together, we obtain Algorithm 1 and the following main theorem of this paper.

**Algorithm ROUNDSUBSPACES($A$):**

**Input:** A matrix space $A$.

**Output:** The dominant independent set $(L^*, R^*)$ for $A$.

**Algorithm:** Set constants $M_0 = e^{O(n^2(n+m)\log(m+n)+n^2 \log Mp)}$ and $M_1 = e^{O(n^5 \log(Mn))}$ as in Theorems 3.13 and 3.14.

1. Using binary search over $k$ and DECISIONSINKHORN($\Phi, k, 0$), determine $k^*$, the largest $k$ such that $\text{cap}_k \Phi > -\infty$.

2. Using binary search over $r$ and DECISIONSINKHORN($\Phi, k^*, r$), determine $r^*$, the largest $r$ such that $\text{cap}_{k^*, r} \Phi > -\infty$.

3. Using APPROXINDEP($\Phi, k^*, r^* + 1, \epsilon$) for $\epsilon = 1/2M_0M_1^2$, find an $\epsilon$-independent set $(L, R)$ that violates $(k^*, r^* + 1)$.

4. Using the continued fraction expansion, round each entry of $\pi_R$ to the nearest rational number with denominator at most $M_1$. Let $R'$ be the image of the rounded matrix.

5. **Output** $(A(R')^\perp, R')$.

**Algorithm 1:** Optimization algorithm to output the smallest shrunk subspace.

**Theorem 3.15.** ROUNDSUBSPACES (Algorithm 1) finds the dominant independent set (and hence smallest shrunk subspace) in $O(n^7(m+n)^3(m+n+p)((m+n)\log(m+n)+n^3 \log(Mnp))$ arithmetic operations. Furthermore, the bit complexity of intermediate numbers is $\text{poly}(m, n, p, \log M)$. As the input size is $mnp \log M$, the time complexity is at most the tenth power of the input size.

**Remark 3.16** (finite arithmetic). In the following sections, we describe our algorithms assuming that we can compute the exact eigenvalue decomposition of Hermitian matrices and the exact values of simple functions, e.g., log, exp, and square root, for the simplicity of exposition. In Appendix B, we show how to modify them to polynomial time algorithms in the finite arithmetic model with only polynomially many bits.

### 4 Majorization scaling

To describe SINKHORNDECISION, we’ll cast it as a special case of a more general problem we call majorization scaling.
Definition 4.1 (Majorization scalability). For a vector \( x \in \mathbb{R}^n \), let \( x^\downarrow \in \mathbb{R}^n \) denote \( x \) sorted in non-increasing order. The vector \( x \in \mathbb{R}^n \) is weakly majorized by \( y \in \mathbb{R}^n \), denoted by \( x \preceq y \), if
\[
\sum_{i=1}^s x_i^\downarrow \leq \sum_{i=1}^s y_i^\downarrow
\]
for each \( s \in [n] \). For non-increasing vectors \( \alpha \in \mathbb{R}^n \) and \( \beta \in \mathbb{R}^m \), we say \( \Phi \) is \((\alpha, \beta)\)-majorized if
\[
\lambda(\Phi^*(I_m)) \leq \alpha, \quad \lambda(\Phi(I_n)) \leq \beta.
\]
We say \( \Phi \) is \( k \)-scalable to \((\alpha, \beta)\) if for every \( \varepsilon > 0 \), there is a scaling of \( \Phi \) which is \((\alpha, \beta)\)-majorized and has size at least \( k - \varepsilon \).

Definition 4.2 (Down-closure of permutahedron). We denote
\[
P_\alpha := \{ x \in \mathbb{R}^n_{\geq 0} : x \preceq \alpha \};
\]
it is the down-closure of the permutahedron of \( \alpha \).

Note that \( \Phi \) is \( k \)-scalable if and only if it is \( k \)-scalable to \((1_n, 1_m)\), the appropriate length all-ones vectors. We'll show a variational characterization of majorization scalability as well. For decreasing vectors \( \alpha, \beta \in \mathbb{R}^d \) and \( k \geq 0 \), consider the following objective function:
\[
f_{k}^{\alpha, \beta}(X, Y, z) = \text{Tr} \Phi(X^{-1})Y^{-1}e^z + \alpha \cdot \lambda(\log X) + \beta \cdot \lambda(\log Y) - kz,
\]
and define the \( \alpha, \beta \) capacity as
\[
\text{cap}_{k}^{\alpha, \beta} \Phi = \inf_{\Upsilon \in \mathcal{D}} f_{k}^{\alpha, \beta}(\Upsilon).
\]
Note that \( f_{k}^{1_n, 1_m} = f_k \) (and hence \( \text{cap}_{k}^{1_n, 1_m} \Phi = \text{cap}_k \Phi \)) and if we set
\[
\alpha_r = (1, \ldots, 1, 1 - 1/n, \ldots, 1 - 1/n),
\]
i.e. \( n - r \) ones followed by \( r \) entries equal to \( 1 - 1/n \), then we have \( f_{k}^{\alpha_r, 1_m} = f_{k,r} \) and \( \text{cap}_{k}^{\alpha_r, 1_m} \Phi = \text{cap}_{k,r} \Phi \). Note that \( \text{cap}_{k}^{\alpha, \beta} \Phi \) is unitarily invariant, i.e. \( \text{cap}_{k}^{\alpha, \beta} \Phi_{U,V} = \text{cap}_{k}^{\alpha, \beta} \Phi \) for any \( U, V \) unitary.

The finiteness of \( \text{cap}_{k}^{\alpha, \beta} \Phi \) characterizes majorization scalability:

**Theorem 4.3.** \( \text{cap}_{k}^{\alpha, \beta} \Phi > -\infty \) if and only if \( \Phi \) is \( k \)-scalable to \((\alpha, \beta)\).

The proof goes through a notion of scaling by triangular matrices considered in [Fra18]. We postpone the proof to Section 4.3 because it is not needed for the description of our majorization scaling algorithm. Note that Theorem 4.3 implies the equivalence between (2) and (3) of Theorem 3.9.

4.1 Sinkhorn algorithm for majorization scaling

Here we describe a Sinkhorn-style algorithm, \text{MAJSINKHORN}, for finding a scaling of \( \Phi \) to \((\alpha, \beta)\) with size \( k \). The idea is alternating minimization of the function \( f_{k}^{\alpha, \beta} \) (see (4.1) for definition). We describe how to update \( X, Y, z \) efficiently.
Update of $X$.

First, we describe the subroutine $\text{KLProject}$ for how to update $X$ while fixing $Y$ and $z$. It suffices to solve

$$\begin{align*}
\text{minimize} & \quad \text{Tr}(X^{-1}C) + \alpha \cdot \lambda(\log X) \\
\text{subject to} & \quad X \succeq I,
\end{align*}$$

where $C = e^z\Phi^*(Y^{-1}) \succeq O$. Let $X = Ue^{\text{diag}(x)}U^*$, where $U$ is an unitary matrix and $x \geq 0$ is a nonnegative vector with nondecreasing entries, i.e., $x_1 \geq \cdots \geq x_n \geq 0$. We can get rid of $U$ using $\text{Tr}(X^{-1}C) = \text{Tr}(Ue^{\text{diag}(-x)}U^*C) \geq e^{\text{diag}(-x)} \cdot \lambda(C)$, where the equality is attained when $U$ diagonalizes $C$, and the other term $\alpha \cdot \lambda(\log X)$ does not depend on $U$. Thus, we obtain an equivalent optimization problem only in $x$.

$$\begin{align*}
\text{minimize} & \quad \sum_{i=1}^n \lambda_i(C)e^{-x_i} + \alpha_i x_i \\
\text{subject to} & \quad x_1 \geq \cdots \geq x_n \geq 0.
\end{align*}$$ (4.2)

We show that this problem is the dual of generalized KL-projection of $\lambda(C)$ onto $P_\alpha$, (the down-closure of) the permutahedron of $\alpha$.

**Definition 4.4** (Generalized KL divergence). For two nonnegative vectors $p, q \in \mathbb{R}^n$, define

$$D(p\|q) = \sum_{i=1}^n p_i \log \frac{p_i}{q_i} - p_i + q_i$$

define $D(P_\alpha\|q)$ to be $\min_{p\in P_\alpha} D(p\|q)$.

KL-projection onto the permutahedron of $\alpha$ can be solved in $O(n^2)$ time, see e.g., [SHK+12]. Furthermore, we can construct the optimal $x$ from a dual optimal solution.

**Lemma 4.5.** Let $q = \lambda(C)$. The dual of (4.2) is equivalent to the following convex optimization:

$$\begin{align*}
\text{minimize} & \quad D(p\|q) \\
\text{subject to} & \quad p(S) \leq \sum_{i=1}^{|S|} \alpha_i \quad (S \subseteq [n]) \\
& \quad p \geq 0,
\end{align*}$$ (4.3)

i.e. the generalized KL projection of $q$ onto $P_\alpha$. In particular, the value of (4.2) is $\text{Tr} C - D(P_\alpha\|q)$. Furthermore, we can solve (4.2) as well as (4.3) in $O(n^2)$ time.

**Proof.** Note that $q_1 \geq \cdots \geq q_n$. First observe that any optimal solution $p^*$ also obeys the same ordering, i.e., $p^*_1 \geq \cdots \geq p^*_n$. To see this, suppose for the contrary that $p^*_i < p^*_j$ for some $i < j$. Let $p$ be a vector obtained by swapping the $i$th entry with the $j$th entry in $p^*$. Then, $p$ is also feasible and

$$D(p\|q) - D(p^*\|q) = (p^*_j - p^*_i) \log \frac{p^*_j}{q_j} + (p^*_i - p^*_j) \log \frac{p^*_i}{q_i} \leq (p^*_j - p^*_i) \log \frac{p^*_j}{q_j} = \frac{p^*_j}{p^*_i} - 1,$$

i.e. $D(p\|q) \geq D(p^*\|q)$.
so \( D(p\|q) < D(p^*\|q) \), which is a contradiction.

Hence, it suffices to consider constraints \( \sum_{i=1}^{j} p_i \leq \sum_{i=1}^{j} \alpha_i \) for \( j = 1, \ldots, n \). The Lagrangian of the problem (4.3) is

\[
L(p, y) = \sum_{i=1}^{n} \left( p_i \log \frac{p_i}{q_i} - p_i + q_i \right) + \sum_{j=1}^{n} y_j \sum_{i=1}^{j} (p_i - \alpha_i),
\]

where \( y_j \geq 0 \) \( (j = 1, \ldots, n) \) is a dual variable. Solving \( \frac{\partial L}{\partial p_i} = 0 \), we obtain

\[
p_i = q_i \exp \left( -\sum_{j=1}^{n} y_j \right).
\]

Substituting this, we obtain dual problem:

\[
\begin{align*}
\text{maximize} & \quad -\sum_{i=1}^{n} q_i \exp \left( -\sum_{j=1}^{n} y_j \right) - \alpha_i \sum_{j=i}^{n} y_j + \sum_{i=1}^{n} q_i \\
\text{subject to} & \quad y_1, \ldots, y_n \geq 0.
\end{align*}
\]  

(4.4)

Changing a variable to \( x_i = \sum_{j=i}^{n} y_j \), we obtain (4.2) (with an extra constant \( \sum_{i=1}^{n} q_i = \text{Tr} C \) in the objective function). Note that (4.2) satisfies the Slater condition, so the strong duality holds.

The algorithm for solving (4.2) works as follows. First, it computes the KL-projection of \( q \) onto the permutahedron of \( \alpha \) as well as the corresponding dual variable \( y' \), which can be found in \( O(n^2) \) time by e.g. [SHK+12, LW16]. Then, the optimal solution \( y \) of (4.4) can be obtained by setting negative entries of \( y' \) to zero [LW16, Theorem 3.3]. Once we have an optimal solution \( y \) of (4.4), the optimal solution \( x \) of (4.3) is given by \( x_i = \sum_{j=i}^{n} y_j \).

**Remark 4.6** (The case \( \alpha = 1_n \)). In this case, the update step is very simple. The algorithm reduces to the variant of the Sinkhorn algorithm mentioned in Section 3.1 - one simply chooses \( X \) to be diagonal in the same basis as \( C \), and then sets each eigenvalue \( x_i \geq 1 \) of \( X \) to scale down the corresponding eigenvalue \( \lambda_i \) of \( C \) so that \( x_i^{-1} \lambda_i \geq 1 \) (and if already \( \lambda_i \leq 1, x_i = 1 \)). In the matrix scaling case, this amounts to scaling down the columns which have sums larger than 1 so that they have unit sum.

Computing the matrix \( C \) takes \( O(m^2 n + mn^2 + pm^2) \) time and computing the eigen-decomposition of \( C \) takes \( O(n^3) \) time. Overall, the time complexity of update of \( X \) is \( O(n^3 + m^2 n + mn^2 + pm^2) = O((m + n)^3 + pm^2) \) time.

**Update of \( Y \).**

We can also update \( Y \) in \( O((m + n)^3 + pm^2) \) time mutatis mutandis.

**Update of \( z \).**

Let \( a = \text{Tr}(\Phi(X^{-1})Y^{-1}) \). Set \( z \leftarrow \log(k/a) \) if \( a \leq k \). Otherwise, set \( z = 0 \).

### 4.2 Analysis of MajSinkhorn

Here we describe the runtime of MajSinkhorn. The proof of our progress bounds requires an inequality relating products of matrices and spectra of logarithms by majorization.
Algorithm **MajSinkhorn**($\Phi, \alpha, \beta, \varepsilon$):

**Input:** A CP map $\Phi : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{m \times m}$, non-increasing vectors $\alpha \in \mathbb{R}^n, \beta \in \mathbb{R}^m$, and a parameter $\varepsilon > 0$.

**Output:** A scaling of $\Phi$ that is $(\alpha, \beta)$-majorized and has size at least $(1 - \varepsilon)k$.

**Algorithm:** Set $X = I_n, Y = I_m, z = 0$. For $t \in \{0, \ldots, T\}$:

1. Let $a = \text{Tr} \Phi(X^{-1})Y^{-1}$. Set $z \leftarrow \log(k/a)$ if $a \leq k$. Otherwise, set $z = 0$.

2. Set $\mu = \lambda(e^zX^{-1}\Phi^*(Y^{-1}))$ and $\nu = \lambda(e^zY^{-1}\Phi(X^{-1}))$. Using KLProject, compute the divergences $\varepsilon_X := D(P_\alpha || \mu)$ and $\varepsilon_Y := D(P_\beta || \nu)$, where $P_\alpha$ and $P_\beta$ are the down-closure of the permutahedron of $\alpha$ and $\beta$, respectively.

   If $\varepsilon_X, \varepsilon_Y \leq \min\{\alpha_1, \beta_1\} \varepsilon^2$:
   **Output** $e^{z - \varepsilon \Phi_{Y^{-1/2}Z^{-1/2}}}$.

   Else:
   
   If $\varepsilon_X \geq \varepsilon_Y$:
   Using KLProject, set
   
   $X = \arg\min_{X \succeq I_n} \text{Tr}(X^{-1}C e^z) + \alpha \cdot \lambda(\log X)$.

   Else:
   Using KLProject, set
   
   $Y = \arg\min_{Y \succeq I_m} \text{Tr}(Y^{-1}C e^z) + \beta \cdot \lambda(\log Y)$.

**Algorithm 2:** Algorithm for majorization scaling.

**Lemma 4.7.** Let $X, Z \succ 0$ and $\alpha \in \mathbb{R}^n$ nondecreasing. Then

$$\alpha \cdot \lambda(\log X^{1/2}ZX^{1/2}) \leq \alpha \cdot \lambda(\log Z) + \alpha \cdot \lambda(\log X).$$

This is equivalent to $\lambda(\log(XZ)) \leq \lambda(\log X) + \lambda(\log Z)$ for $X, Z$ positive definite, which is due to Lidskii [Bha13, Corollary III.4.6]. We include a different proof in Section 4.3 for completeness. We now analyze **MajSinkhorn**. The following lemma describes progress in terms of the KL projection.

**Lemma 4.8.** Let $X \succeq I_n$ and $C \succeq 0$ be $n \times n$ matrices, and let $\alpha \in \mathbb{R}^n$ be a non-increasing vector. Let $\mu = \lambda(X^{-1/2}CX^{-1/2})$. Then

$$\text{Tr}(X^{-1}C) + \alpha \cdot \log(X) \geq D(P_\alpha || \mu) + \text{Tr} C - D(P_\alpha || \lambda(C)).$$

In particular, the progress made in the $X$ update of **MajSinkhorn** is at least $D(P_\alpha || \mu) \geq \varepsilon^2/2$.

**Proof.** The proof is a change of variables argument. By Lemma 4.5 and because $X \succeq I_n$, we can
write
\[
\text{Tr } C - D(P_\alpha||\lambda(C)) = \inf_{\tilde{X} \succeq I_n} \text{Tr}(\tilde{X}^{-1} C) + \alpha \cdot \lambda(\log \tilde{X})
\]
\[
\leq \inf_{\tilde{X} \succeq X} \text{Tr}(\tilde{X}^{-1} C) + \alpha \cdot \lambda(\log \tilde{X})
\]
\[
= \inf_{Z \succeq I_n} \text{Tr}(Z^{-1} X^{-1/2}C X^{-1/2}) + \alpha \cdot \lambda(\log(X^{1/2}Z X^{1/2}))
\]
\[
\leq \inf_{Z \succeq I_n} \left[ \text{Tr}(Z^{-1} X^{-1/2}C X^{-1/2}) + \alpha \cdot \lambda(\log Z) \right] + \alpha \cdot \lambda(\log X)
\]
\[
= \text{Tr}(X^{-1/2}C X^{-1/2}) - D(P_\alpha || \mu) + \alpha \cdot \lambda(\log X).
\]

The second equality used the change of variables \( \tilde{X} = X^{1/2}Z X^{1/2} \), the second inequality used Lemma 4.7, and the final equality used Lemma 4.5 again. Rearranging the terms yields the inequality.

For the progress claim, observe that in the \( X \) update the terms in the function depending on \( X \) change from \( \text{Tr}X^{-1}C + \alpha \cdot \log(X) \) to \( \min_X(\text{Tr}(X^{-1}C) + \alpha \cdot \log(X)) \), which is equal to \( \text{Tr}C - D(P_\alpha || \lambda(C)) \) by Lemma 4.5.

We can now prove our running time bounds.

**Theorem 4.9.** Suppose \( \Phi \) has size at most 1. If \( \text{cap}^{\alpha,\beta} \Phi \) is finite, \text{MajSinkhorn} terminates in
\[
2 \cdot \frac{1 - \text{cap}^{\alpha,\beta} \Phi}{\min\{\alpha_1, \beta_1\} \varepsilon^2}
\]
steps, and the output is an \((\alpha, \beta)\) scaling of \( \Phi \) of size at least \((1 - \varepsilon)k\).

**Proof.** First we verify that, assuming termination, the output is an \((\alpha, \beta)\) scaling of \( \Phi \) of size \( k - \varepsilon \). Set \( \tilde{\Phi} = e^\varepsilon \Phi_{Y^{-1/2}X^{-1/2}} \). By the assumption that we have terminated, for \( \mu = \lambda(\tilde{\Phi}^*(I_n)) \) and \( \nu = \lambda(\tilde{\Phi}(I_n)) \), we have \( D(P_\alpha || \mu), D(P_\beta || \nu) \leq \min\{\alpha_1, \beta_1\} \varepsilon^2 \). By Lemma 4.10, we have \( e^{-\varepsilon} \mu \preceq \alpha \) and \( e^{-\varepsilon} \nu \preceq \beta \), so the output \( e^{-\varepsilon} \Phi_{Y^{-1/2}X^{-1/2}} \) is \((\alpha, \beta)\)-majorized. Because \( \tilde{\Phi} \) has size at least \( k \) by the \( z \)-update, \( e^{\varepsilon} \Phi_{Y^{-1/2}X^{-1/2}} \) has size \( e^{-\varepsilon}k \geq (1 - \varepsilon)k \).

Now let’s verify the running time. First note that the algorithm is alternating minimization, so the objective function decreases throughout the algorithm. The only step for which this is non-trivial is the \( z \) update step. This follows from the fact that the function \( g_\lambda(z) := \lambda e^z - 1 \) is minimized on the domain \( z > 0 \) at \( z = \max\{0, -\log(\lambda)\} \), which can be shown by straightforward calculus. We now claim that each time the algorithm does not terminate, it decreases the objective function \( f_k^{\alpha,\beta} \) by \( \min\{\alpha_1, \beta_1\} \varepsilon^2 \). Initially, the function value is at most 1 by our assumption on the size. By definition, \( f_k^{\alpha,\beta}(X, Y, z) \geq \text{cap}^{\alpha,\beta} \Phi \). This implies the desired running time bound. For the progress bound, by Lemma 4.8 the change in the objective function by an \( X \) (resp. \( Y \)) update is at least \( D(P_\alpha || \mu) \) (resp. \( D(P_\beta || \nu) \)), whichever is larger. Whenever the algorithm doesn’t terminate, the larger of the two of these is at least \( \min\{\alpha_1, \beta_1\} \varepsilon^2 \).

The next lemma shows that if a vector is closed to being majorized, one can scale it down slightly and it will become majorized.

**Lemma 4.10** (Rescaling to majorize). Let \( \varepsilon > 0 \). If \( D(P_\alpha || q) \leq \alpha_1 \varepsilon^2 \), then \( e^{-\varepsilon}q \preceq \alpha \).
Proof. Assume \( q \) is in decreasing order. If \( q \preceq \alpha \), the claim holds vacuously, so assume that this is not the case. Let \( L = \log \max_k (\sum_{i=1}^k q_i)/(\sum_{i=1}^k \alpha_i) > 0 \), so that \( L \) is the smallest number such that \( e^{-L} q \preceq \alpha \). Let \( i^* \) be the constraint where \( e^{-L} q \preceq \alpha \) is tight, i.e., \( \sum_{i=1}^{i^*} e^{-L} q_i = \sum_{i=1}^{i^*} \alpha_i \). It suffices to show that \( L \leq \varepsilon \). We know from Lemma 4.5 that

\[
D(P_\alpha \| q) = \sum_{i=1}^n q_i - \min_{x_1 \geq x_2 \geq \cdots \geq x_n} \sum_{i=1}^n q_i e^{-x_i} + \alpha_i x_i.
\]

If we set \( x_i = L \cdot 1_{[i^*]} \), then

\[
D(P_\alpha \| q) \geq \sum_{i=1}^{i^*} q_i - e^{-L} \sum_{i=1}^{i^*} q_i - L \sum_{i=1}^{i^*} \alpha_i \\
= (e^{-L} - 1 - L) \sum_{i=1}^{i^*} \alpha_i \geq \frac{L^2}{2} \sum_{i=1}^{i^*} \alpha_i \geq \frac{L^2}{2} \alpha_1. \tag*{\Box}
\]

4.3 Triangular scaling and the proof of Theorem 4.3

The proof of Theorem 4.3 will go through triangular scaling, a notion studied in [Fra18]. Our capacity lower bounds in the next section will also rely on triangular scaling.

Definition 4.11 (Scalability and triangular scalability). We say \( \Phi_{B,C} \) is a triangular scaling of \( \Phi \) if \( B \in \mathbb{C}^{m \times m}, C \in \mathbb{C}^{n \times n} \) are upper triangular. For non-increasing, nonnegative vectors \( \alpha \in \mathbb{R}^n, \beta \in \mathbb{R}^m \) we say \( \Phi \) is \( (\alpha, \beta) \)-scalable (resp. triangularly scalable) if for every \( \varepsilon > 0 \) there is a scaling (resp. triangular scaling) \( \tilde{\Phi} \) satisfying

\[
\|\tilde{\Phi}^*(I_m) - \text{diag}(\alpha)\|_F \leq \varepsilon \quad \text{and} \quad \|\tilde{\Phi}(I_n) - \text{diag}(\beta)\|_F \leq \varepsilon.
\]

We next introduce the corresponding notion of capacity.

Definition 4.12 (Triangular scaling capacity). First, for a positive-semidefinite matrix \( Y \) we define

\[
\log \det(\nu, Y) := \sum_i (\nu_i - \nu_{i+1}) \log \text{pm}_i Y,
\]

where \( \text{pm}_i \) denotes the \( i^{th} \) leading principal minor of \( Y \). Let

\[
g_{\alpha,\beta}(X,Y) = \text{Tr} \Phi(X^{-1})Y^{-1} + \log \det(\alpha, X) + \log \det(\beta, Y),
\]

and let \( \text{cap}_{\alpha,\beta} \Phi \) be defined by \( \text{cap}_{\alpha,\beta} = \inf_{X > 0, Y > 0} g_{\alpha,\beta}(X,Y) \).

It is known that \( \text{cap}_{\alpha,\beta} \Phi > -\infty \) characterizes \((\alpha, \beta)\)-triangular scalability, and \( \text{cap}_{\alpha,\beta} \tilde{\Phi} \) for random scalings \( \tilde{\Phi} \) of \( \Phi \) characterizes \((\alpha, \beta)\)-scalability. The next theorem collects this and several other known properties of the capacity.

Theorem 4.13 ([Fra18]). Let \( \Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m} \) be a CP map.

1. \( \Phi \) is \((\alpha, \beta)\)-triangularly scalable if and only if \( \text{cap}_{\alpha,\beta} \Phi > -\infty \).
2. Φ is \((\alpha, \beta)\)-scalable if and only if there are unitary matrices \(U \in \mathbb{C}^{m \times m}, V \in \mathbb{C}^{n \times n}\) such that
\[
cap_{\alpha, \beta} \Phi_{U, V} > -\infty.
\]

3. If \(\alpha, \beta\) are integral, the set of matrices \(A \in \mathbb{C}^{m \times m}, B \in \mathbb{C}^{n \times n}\) such that \(\cap_{\alpha, \beta} \Phi_{A, B} = -\infty\) is an affine variety generated by polynomials of degree at most \(2(\sum_i \alpha_i)^2\).

4. The set of nonnegative, decreasing vectors \(\alpha, \beta\) such that \(\cap_{\alpha, \beta} \Phi = -\infty\) (i.e. such that \(\Phi\) is \((\alpha, \beta)\)-triangularly scalable) is a polyhedral cone cut out by inequalities with Boolean coefficients. The same is true of the set of \(\alpha, \beta\) such that \(\Phi\) is \((\alpha, \beta)\)-scalable.

5. The function \((\alpha, \beta) \mapsto \cap_{\alpha, \beta} \Phi\) is concave over the set of nonnegative, decreasing vectors \((\alpha, \beta)\) when we take \(0 \log 0 := 0\).

[Fra18] actually used a slightly different expression for the capacity, but we show in Lemma 4.22 that one is (an affine function of) the logarithm of the other. We now collect a few properties of \(\log \det (\mu, \cdot)\).

**Lemma 4.14.**

1. If \(b\) is lower triangular, then
\[
\log \det (\mu, bXb^\dagger) = \log \det (\mu, bb^\dagger) + \log \det (\mu, X).
\]

2. If \(\mu \preceq \alpha\) and \(X \succeq I_n\), then
\[
\log \det (\mu, X) \geq \lambda (\log X) \cdot \alpha.
\]

If also \(\sum \alpha_i = \sum \mu_i\), then the inequality holds with only the constraint \(X \succ 0\).

3. If \(X\) is diagonal then
\[
\log \det (\alpha, X) = \lambda (\log X) \cdot \alpha.
\]

**Proof.** Item 1 is [Fra18, Lemma 15]. For Item 2, we have
\[
\log \det (\mu, X) = \sum_i (\mu_i - \mu_{i+1}) \log \rho_m, X
\]
\[
\leq \sum_i (\mu_i - \mu_{i+1}) \log \prod_{j=1}^i \lambda_j (X)
\]
\[
= \sum_i (\mu_i - \mu_{i+1}) \sum_{j=1}^i \lambda_j (\log X) = \mu \cdot \lambda (\log X) \leq \alpha \cdot \lambda (\log X).
\]

In the inequality we used interlacing, in the final equality we used partial summation, and in the final equality we used \(\nu \preceq \beta\) and the fact that \(\lambda (\log X) \geq 0\). If \(\sum \alpha_i = \sum \mu_i\) we can reduce to the case \(X \succeq I_n\) by multiplying by an appropriate scalar. The third item is a straightforward calculation.

We have the following inequality relating the capacity for majorization scaling with the one for triangular scaling.
Lemma 4.15. For any \( \mu \preceq \alpha, \nu \preceq \beta \) and \( \sum_i \mu_i = \sum_i \nu_i = k \), we have
\[
\text{cap}_{\mu,\nu} \Phi \leq \text{cap}^{\alpha,\beta} \Phi.
\]

Proof. By the inequality in Item 2 of Lemma 4.14,
\[
\text{cap}^{\alpha,\beta} \Phi \geq \inf_{(X,Y,z) \in D} \text{Tr} \Phi(X^{-1})Y^{-1}e^z + \log \det(\mu, X) + \log \det(\nu, Y) - k_z
\]
\[
= \inf_{X \succeq I, Y \succeq I} \text{Tr} \Phi((X^{-1})^{-1})(Y^{-1})^{-1} + \log \det(\mu, X^{-1}) + \log \det(\nu, Y^{-1})
\]
\[
= \inf_{X,Y \succeq 0} \text{Tr} \Phi(X^{-1})Y^{-1} + \log \det(\mu, X) + \log \det(\nu, Y).
\]

Finally, we prove Theorem 4.3.

Proof of Theorem 4.3. We have already seen in Theorem 4.9 that if \( \text{cap}^{\alpha,\beta} \Phi \) is finite, then for any \( \varepsilon > 0 \), \textsc{MajSinkhorn} finds a scaling of \( \Phi \) that is majorized by \( (\alpha, \beta) \) and has size \( k(1 - \varepsilon) \). Therefore, it suffices to show that \( \Phi \) is not \( k \)-scalable to \( (\alpha, \beta) \) if \( \text{cap}^{\alpha,\beta} \Phi = -\infty \).

Suppose for the contrary that \( \text{cap}^{\alpha,\beta} \Phi = -\infty \) and \( \Phi \) is \( k \)-scalable to \( (\alpha, \beta) \). Then, by compactness, there exists some \( \mu \leq \alpha, \nu \leq \beta \) such that \( \sum_i \mu_i = \sum_i \nu_i = k \) such that \( \Phi \) is \( (\mu, \nu) \)-scalable. By unitary invariance of \( \text{cap}^{\alpha,\beta} \Phi \), we have \( \text{cap}^{\alpha,\beta} \Phi_{U,V} = -\infty \) for all unitary matrices \( U, V \). By Lemma 4.15, \( \text{cap}_{\mu,\nu} \Phi_{U,V} = -\infty \). By Item 2 of Theorem 4.13, this contradicts \( \Phi \) being \( (\mu, \nu) \)-scalable.

As a side benefit, the properties of \( \log \det(\mu, \cdot) \) give a quick proof of Lemma 4.7.

Proof of Lemma 4.7. Without loss of generality, \( X^{1/2}ZX^{1/2} \) is diagonal. Then by Item 3 of Lemma 4.14,
\[
\alpha \cdot \lambda(\log X^{1/2}ZX^{1/2}) = \log \det(\alpha, X^{1/2}ZX^{1/2})
\]
Choose \( U \) unitary so that \( X^{1/2}U \) is lower triangular. Then
\[
\log \det(\alpha, X^{1/2}ZX^{1/2}) = \log \det(\alpha, X^{1/2}UU^\dagger ZU^\dagger X^{1/2})
\]
\[
= \log \det(\alpha, X) + \log \det(\alpha, U^\dagger ZU)
\]
\[
\leq \alpha \cdot \lambda(\log X) + \alpha \cdot \lambda(\log Z).
\]
The second equality used Item 2 of Lemma 4.14, and the inequality used Item 2 of Lemma 4.14 and the unitary invariance of \( \lambda(\log Z) \).

4.4 Capacity lower bounds

Theorem 4.16. Suppose the Kraus operators of \( \Phi \) have Gaussian integer entries. Then \( \text{cap}^{\alpha,\beta} \Phi \) is either \( -\infty \) or
\[
- \text{cap}^{\alpha,\beta} \Phi = O(k(n + m) \log(m + n) + k \log p).
\]

Before proving the theorem, we combine it with Theorem 4.9 and one small lemma about how normalizing affects the capacity to obtain a concrete bound for how many steps \textsc{MajSinkhorn} requires.

Lemma 4.17 (Capacity under scalar multiplication). Let \( 0 < c < 1 \). Then
\[
\text{cap}^{\alpha,\beta} c\Phi \geq \text{cap}^{\alpha,\beta} \Phi + (\sum_i \alpha_i) \log c.
\]
Proof. This is a change of variables argument. Let $X = X/c$.

$$\text{cap}_{k,r} \ c\Phi = \inf_{X,Y \geq I, z \geq 0} \text{Tr} \ Y^{-1} \Phi((X/c)^{-1}) e^z + \alpha \cdot \lambda(\log X) + \beta \cdot \lambda(\log Y) - kr$$

$$= \inf_{X,Y \geq I, z \geq 0} \text{Tr} \ Y^{-1} \Phi (X^{-1}) e^z + \alpha \cdot \lambda(\log X) + (\log c) I_n + \beta \cdot \lambda(\log Y) - kr$$

$$\geq \inf_{X,Y \geq I, z \geq 0} \text{Tr} \ Y^{-1} \Phi (X^{-1}) e^z + \alpha \cdot \lambda(\log X) + \sum_i \alpha_i \log c + \beta \cdot \lambda(\log Y) - kr$$

$$= \text{cap}_{k,r} \ c\Phi + \sum_i \alpha_i \log c. \qed$$

**Corollary 4.18.** Suppose the Kraus operators of $\Phi$ have Gaussian integer entries and $\text{cap}_{\alpha,\beta} \Phi$ is finite. Then MAJSINKHORN terminates in

$$O\left(\frac{k(n+m)\log(m+n) + (\sum_i \alpha_i) \log pnnM}{\min\{\alpha_1, \beta_1\} \varepsilon^2}\right)$$

steps, and the output is an $(\alpha, \beta)$ scaling of $\Phi$ of size at least $(1 - \varepsilon)k$.

**Proof.** At the first step of MAJSINKHORN we normalize $\Phi$ to obtain $\tilde{\Phi}$ of size at most 1. This entails dividing by a constant $1 \leq c \leq pnnM^2$. By Lemma 4.17, $\text{cap}_{\alpha,\beta} \tilde{\Phi} = \text{cap}_{k,r} \tilde{\Phi} + (\sum_i \alpha_i) \log c$. Theorem 4.9 shows that MAJSINKHORN terminates in at most $2(1 - \text{cap}_{\alpha,\beta} \tilde{\Phi}) / \min\{\alpha_1, \beta_1\} \varepsilon^2$ further steps; plugging in our estimate for $\text{cap}_{\alpha,\beta} \tilde{\Phi}$ completes the proof. \qed

We now collect a few lemmas needed for the proof of Theorem 4.16. Our main tool is Theorem 4.15 and known capacity lower bounds from [Fra18] for the capacity $\text{cap}_{\mu,\nu}$ for triangular scaling. From a compactness argument similar to the proof of Theorem 4.3, we know that there is some $\mu \preceq \alpha, \nu \preceq \beta$ and unitaries $U, V$ such that $\text{cap}_{\mu,\nu} \Phi_{U,V} > 0$. If the bit complexity of $U, V$ is controlled, then we can use known capacity lower bounds. Fortunately, Theorem 4.13 tells us that we have $\text{cap}_{\mu,\nu} \Phi_{A,B} > 0$ for random matrices. The next lemma combines Theorem 4.13 with Schwarz-Zippel to see how large a range we need to take for the random entries of $A, B$. A similar argument appeared in the capacity lower bounds of [BFG+19]. We’ll need a quick folklore bound on the bit complexity of vertices of polyhedra generated by Boolean inequalities.

**Observation 4.19.** Let $P = \{x : a_i \cdot x \geq b_i, i \in [m]\} \subseteq \mathbb{R}^n$ be a polytope where $a_i \in \{0, 1\}^n$ and $b_i \in \{0, 1\}$. Then every vertex of $P$ is the ratio of an integral vector with entries at most $e^{O(n \log n)}$ in absolute value with an integer at most $e^{O(n \log n)}$. As a consequence, any polyhedral cone inside the nonnegative orthant of $\mathbb{R}^n$ cut out by inequalities with Boolean coefficients is the conic hull of some number of integer vectors with entries at most $e^{O(n \log n)}$.

**Proof.** Each vertex is a basic feasible solution, i.e. is obtained from setting some entries to zero and the rest according to the equation $Ax = b$ where $A$ is some invertible square submatrix of the $m \times n$ matrix with entries $(a_{ij})$ and $b$ is the corresponding subset of the entries of $b_1, \ldots, b_m$. By Cramer’s rule, the $i^{th}$ entry of $x = A^{-1}b$ is obtained by $\det A(i) / \det A$ where $A(i)$ has the $i^{th}$ column of $A$ replaced by $b$. Thus $\det A$ is a common denominator. By Hadamard’s inequality, $\det A, \det A(i) \leq n^{n/2} = e^{O(n \log n)}$. For the statement about cones, we simply take the intersection of the cone with the simplex and apply the theorem to this polytope. The extreme points of the polytope generate the extremal rays of the cone. \qed

26
Lemma 4.20. Suppose there are some invertible matrices $A', B'$ such that $\text{cap}_{\mu, \nu} \Phi_{A', B'} > 0$. Then there is a pair of invertible matrices $A, B$ with integer entries at most $e^{O((n + m)\log(n + m))}$ such that $\text{cap}_{\mu, \nu} \Phi_{A, B} > 0$.

Proof. By Item 4 of Theorem 4.13, the set of $\mu, \nu$ such that there exists invertible $A, B$ such that $\text{cap}_{\mu, \nu} \Phi_{A, B} > -\infty$ (i.e. such that $\Phi_{A, B}$ is $(\mu, \nu)$-scalable) is a polyhedral cone by Item 4 of Theorem 4.13. Thus it is enough to check that $\text{cap}_{\mu, \nu} \Phi_{A, B} > -\infty$ for $n + m$ (the ambient dimension) many extremal rays $(\mu_i, \nu_i)$ which have $(\mu, \nu)$ is in their conic hull. Because the cone is cut out by Boolean inequalities, the extremal rays of the cone have integral entries of magnitude $e^{O((n + m)\log(n + m))}$ by Observation 4.19. By Item 3 of Theorem 4.13, as $\mu_i, \nu_i$ are integral then the set of pairs $A, B$ such that $\text{cap}_{\mu_i, \nu_i} \Phi_{A, B} = -\infty$ is a variety $\mathcal{V}(\mu_i, \nu_i)$ generated by polynomials of degree $2(\mu_i \cdot 1)^2 = e^{O((n + m)\log(n + m))}$. For each $i$ there exists $A, B$ such that $\text{cap}_{\mu_i, \nu_i} \Phi_{A, B} > -\infty$, so there is some nonzero polynomial $p_i$ of degree $e^{O(n + m)\log(n + m)}$ in the ideal of $\mathcal{V}(\mu_i, \nu_i)$ such that $p_i(A, B) \neq 0$. By the Schwarz-Zippel lemma, for $A, B$ with i.i.d. random entries in $[0, (m + n)e^{O((n + m)\log(n + m))}]$ there is a nonzero probability that $p_i(A, B) \neq 0$ for all $i$ - so that there is some $A, B$ such that $\text{cap}_{\mu_i, \nu_i} \Phi_{A, B} > -\infty$ for all $i$ and hence $\text{cap}_{\mu, \nu} \Phi_{A, B} > -\infty$. \hfill \qed

Next we recall the capacity lower bound we need from [Fra18], which is for a slightly different capacity.

Theorem 4.21 ([Fra18, Theorem 50]). Define

$$
\text{cap}(\Phi, \mu, \nu) := \inf_{g, h \text{ upper triangular, invertible}} e^{-H(\mu)} \frac{\det(\nu, \Phi(hh^\dagger))}{\det(\mu, h^\dagger h)}.
$$

If $\mu, \nu$ are rational with common denominator at most $e^b$ and $\sum \mu_i = \sum \nu_i = 1$, then

either $\text{cap}(\Phi, \mu, \nu) = 0$ or $\text{cap}(\Phi, \mu, \nu) \geq e^{-O(b + \log p)}$.

The expression for capacity in the previous theorem is related to our expression cap$\mu, \nu  \Phi$ by an affine transformation:

Lemma 4.22. We have

$$
\text{cap}_{\mu, \nu} \Phi = \nu \cdot 1 + \log \text{cap}(\Phi, \mu, \nu) + H(\nu) + H(\mu)
$$

where $H$ denotes the Shannon entropy. In particular, $\text{cap}_{\mu, \nu} \Phi$ and log$\text{cap}(\Phi, \mu, \nu)$ are either both finite or both $-\infty$.

Proof. The identity follows by holding one of the variables fixed and optimizing over the other in the objective function for $\text{cap}_{\mu, \nu} \Phi$. Recall that

$$
\text{cap}_{\mu, \nu} \Phi = \inf_{X, Y > 0} \text{Tr} \Phi(X^{-1})Y^{-1} + \log \det(\mu, X) + \log \det(\nu, Y).
$$

Infimizing over $Y$ with $X$ held fixed leads us to choose $Y = g^\dagger g$ for $g$ upper triangular such that $g^{-1} \Phi(X^{-1})g^{-1} \to \text{diag}(\nu)$, or $g' \text{diag}(\nu)g' \Phi(X)$. If no such $g$ exists, then the infimum over $Y$ alone is infinite. The proof is straightforward calculus, but we omit it and refer to [FW20, Theorem 5.7].
Plugging this family of \(Y\) values and taking a limit yields
\[
cap_{\mu,\nu} \Phi = \inf_{X \succ 0} \nu \cdot 1 + \log \det(\mu, X) + \log \det(\nu, g^\dagger g).
\]

One checks using Item 1 of Lemma 4.14 that
\[
\log \det(\nu, g^\dagger \text{diag}(\nu)g) = \log \det(\nu, g^\dagger g) + \log \det(\nu, \text{diag}(\nu)) = \log \det(\nu, g^\dagger g) - H(\nu).
\]
Thus \(\log \det(\nu, g^\dagger g) = \log \det(\nu, \text{diag}(\nu)) = \log \det(\nu, \text{diag}(\nu)) - H(\nu)\). We now have
\[
cap_{\mu,\nu} \Phi = \nu \cdot 1 + \inf_{X \succ 0} \log \det(\mu, X) + \log \det(\nu, \Phi(X^{-1})) + H(\nu).
\]
Writing \(X^{-1} = hh^\dagger\) for \(h\) upper triangular using the Cholesky decomposition, we find
\[
cap_{\mu,\nu} \Phi = \nu \cdot 1 + \inf_{h} \log \det(\mu, h^{-\dagger} h^{-1}) + \log \det(\nu, \Phi(hh^\dagger)) + H(\nu)
= \nu \cdot 1 + \inf_{h} -\log \det(\mu, h^\dagger h) + \log \det(\nu, \Phi(hh^\dagger)) + H(\nu)
= \log \cap(\Phi, \mu, \nu) + H(\nu) + H(\mu) + \nu \cdot 1.
\]

We now combine the previous lemma with Theorem 4.21 to obtain a lower bound on \(\cap_{\mu,\nu} \Phi\).

**Theorem 4.23 (Capacity lower bound for \(\cap_{\mu,\nu} \Phi\)).** Let the \(p\) Kraus operators of \(\Phi\) have Gaussian integer entries, and let \(\mu \cdot 1 = \nu \cdot 1 = k\). If \(\cap_{\mu,\nu}(\Phi) > -\infty\) we have
\[
-\cap_{\mu,\nu}(\Phi) = O(k(n + m) \log(m + n) + k \log p).
\]

**Proof.** From Theorem 4.21, we know that either \(\cap(\Phi, \mu, \nu) = 0\) or \(\cap(\Phi, \mu, \nu) \geq e^{-O(b + \log p)}\) where \(e^b\) is a common denominator of \(\mu, \nu\) for \(\mu, \nu\) summing to 1. In our setting \(\mu\) and \(\nu\) sum to \(k\), so we observe
\[
cap_{k\mu, k\nu} \Phi = k\nu \cdot 1 + \log \cap(\Phi, k\mu, k\nu) + H(k\nu) + H(k\mu)
\geq k(\log \cap(\Phi, \mu, \nu) + H(\mu))
\geq -O(k(b + \log p)).
\]
where we used in the first inequality that the expression for \(\log \cap(\Phi, \mu, \nu) + H(\mu)\) scales linearly in \(k\) and that the other terms are nonnegative. The last line was by Lemma 4.22 and the fact that \(H(\mu) \geq 0\). Changing variables, for \(\mu, \nu\) summing to \(k\), we have \(-\cap_{\mu,\nu}(\Phi) = O(k(b + \log p))\), where \(e^b\) is a common denominator of \(\mu/k, \nu/k\).

Using the concavity of \(\cap_{\mu,\nu} \Phi\) in \(\mu, \nu\) (Item 5 of Theorem 4.13), we know that the capacity is minimized at an extreme point of the polytope of \(\mu, \nu\) such that \(\cap_{\mu,\nu} \Phi > -\infty\) and \(\sum \mu_i = \sum \nu_i = 1\). It remains to bound the common denominators of the extreme points of the polytope, which is cut out by Boolean inequalities by Item 4 of Theorem 4.13. By Observation 4.19, the each vertex of such a polytope is a rational vector with common denominator \(e^{O((n+m) \log(n+m))}\). \(\square\)

**Lemma 4.24 (capacity under scaling).** For \(h, g\) upper triangular,
\[
\cap_{\mu,\nu} \Phi_{g,h} = \cap_{\mu,\nu} \Phi - \log \det(\mu, g^\dagger g) - \log \det(\nu, h^\dagger h).
\]
Both $g \geq 4.13$, there is a pair of unitaries $U, V$ do this, we first show that for small enough DecisionSinkhorn In this section we describe and analyze 5.1 Deciding finiteness of capacity with DecisionSinkhorn Then any scaling $\tilde{\Phi}$ of $\Phi$ satisfies one of the following: 1. $\text{Tr} \tilde{\Phi}(I_n) \leq k - 1/3$. 2. $D(P_{1_n}||\mu) = \Omega(1/n)$ 3. $D(P_{1_m}||\nu) = \Omega(1/m)$, where $\mu$ and $\nu$ denote the spectrum of $\tilde{\Phi}(I_n)$ and $\tilde{\Phi}^*(I_n)$, respectively. Similarly, if $\cap k_{k,r} \Phi = -\infty$, then any scaling $\tilde{\Phi}$ of $\Phi$ satisfies one of the following: 1. $\text{Tr} \tilde{\Phi}(I_n) \leq k - 1/3$. 2. $D(P_{1_n}||\mu) = \Omega(1/n)$ 3. $D(P_{1_m}||\nu) = \Omega(1/m)$, where $\mu$ and $\nu$ denote the spectrum of $\tilde{\Phi}(I_n)$ and $\tilde{\Phi}^*(I_n)$, respectively. Similarly, if $\cap k_{k,r} \Phi = -\infty$, then any scaling $\tilde{\Phi}$ of $\Phi$ satisfies one of the following:
Algorithm DECISIONSINKHORN($\Phi, k, r$):

**Input:** A CP map $\Phi : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{m \times m}$, integers $k, r \leq n$.

**Output:** Either **Unbounded** if $\text{cap}_{k,r} \Phi = -\infty$ or **Bounded** if not.

**Algorithm:**

1. Normalize $\Phi$ to have size at most 1.
2. If $r = 0$, run MAJSINKHORN($\Phi, 1_n, 1_m, k, \varepsilon_1$) for $\varepsilon_1 = O((m + n)^{-1/2})$ and
   \[ T = O(k(n + m)^2 \log(m + n) + n \log Mp) \]
   iterations. If MAJSINKHORN terminates, output **Bounded**; otherwise output **Unbounded**.
3. If $r > 0$, run MAJSINKHORN($\Phi, \alpha_r, 1_m, k, \varepsilon_2$) for $\varepsilon_2 = O(1/\sqrt{(m + n)n^2})$ and
   \[ T = O(kn^2(n + m)^2 \log(m + n) + n \log Mp) \]
   iterations. If MAJSINKHORN terminates, output **Bounded**; otherwise output **Unbounded**.

**Algorithm 3:** Algorithm for deciding finiteness of $\text{cap}_{k,r} \Phi$.

1. $\text{Tr} \tilde{\Phi}(I_n) \leq k - 1/4n$.
2. $D(P_{\alpha_r} \parallel |\mu|) = \Omega(1/n^3)$
3. $D(P_{\alpha_m} \parallel |\nu|) = \Omega(1/mn^2)$.

**Proof.** We begin with $f_k$; the proof for $f_{k,r}$ is similar. If $f_k$ is unbounded, then there is an independent set of $\Phi$ of size bigger than $m + n - k$. This implies that the same is true for the scaling $\tilde{\Phi}$ at each step; let $(L, R)$ be such an independent set for $\tilde{\Phi}$. By Equation 2.7,
   \[ \text{Tr} \Pi_{L \tilde{\Phi}} \tilde{\Phi}(I_m) + \text{Tr} \Pi_{L \tilde{\Phi}} \tilde{\Phi}(I_n) \geq \text{Tr} \tilde{\Phi}(I_n). \] (5.1)
   Let $\ell' = \dim L$, $r' = \dim R$ and note that $\ell' + r' \leq k - 1$. By the Courant-Fisher min-max theorem, $\text{Tr} \Pi_{L \tilde{\Phi}} \tilde{\Phi}(I_m) \leq \sum_{i=1}^{\ell'} \mu_i + \sum_{i=1}^{\ell'} \nu_i$. By Equation 5.1, either $\tilde{\Phi}$ has size at most $k - 1/3$ or $\sum_{i=1}^{\ell'} \mu_i + \sum_{i=1}^{\ell'} \nu_i \geq k - 1/3$. If the latter holds, then either $\sum_{i=1}^{\ell'} \mu_i \geq r' + 1/3$ or $\sum_{i=1}^{\ell'} \nu_i \geq \ell' + 1/3$ holds since $r' + \ell' \leq k - 1$. If the former of these two inequalities holds, then $\|p - \mu\|_1 \geq 1/3$ for any $p \in P_n$. Now either $\sum_{i=1}^{\ell'} \mu_i > 2n$ in which case Lemma 4.10 implies $D(P_n \parallel |\mu|)$ is at least a constant, or $\sum_{i=1}^{\ell'} \mu_i \leq 2n$ in which case Lemma 5.2 implies $D(P_n \parallel |\mu|) = \Omega(1/n)$. Similarly, if $\sum_{i=1}^{\ell'} \nu_i \geq \ell' + 1/3$, then $D(P_{\alpha_m} \parallel |\nu|) = \Omega(1/m)$.

For $f_{k,r}$, the proof of the first item is the same. It remains only to prove the second item. The proof proceeds the same, except if $f_{k,r}$ is unbounded we have that $(L, R)$ violates $(k, r)$. So either $\ell' + r' < k$, in which case the proof proceeds as for $f_k$, or $\ell' + r' = k$ and $r' > n - r$. In that case, we obtain that either the size of $\tilde{\Phi}$ is at most $k - 1/4n$ or $\sum_{i=1}^{r'} \mu_i + \sum_{i=1}^{\ell'} \nu_i \geq k - 1/4n$. If the latter holds, then either $\sum_{i=1}^{r'} \mu_i \geq r' - 1/2n$ or $\sum_{i=1}^{\ell'} \nu_i \geq 1 + 1/4n$. If the former holds, note that $\sum_{i=1}^{r'} p_i \leq r' - 1/n$ for $p \leq \alpha_r$ because $r' > n - r$. Thus $\|p - \mu\|_1$ is $\Omega(1/n)$. Similar reasoning
shows \( \|p - \nu\|_1 \) is \( \Omega(1/n) \) if \( \sum'_{i=1} u_i \geq 1 + 1/4n \). We can now proceed using Pinsker’s inequality as we did for \( f_k \) to get the bound \( \Omega(1/n^2 \max\{n, m\}) \) for either divergence.

\[ \text{Lemma 5.2 (Unnormalized Pinsker (cf. [vAGL+20]))} \]

Let \( p \) and \( q \) be vectors in \( \mathbb{R}^n \). Suppose \( \text{supp } p \subseteq \text{supp } q \). Then

\[
D(p||q) \geq \min \left\{ \frac{1}{4}\|q\|_1 \|p - q\|_1^2, (1 - \ln 2)\|p - q\|_1 \right\}.
\]

**Proof.** Let \( s = 1/\sum q_i \). Then \( D(sp||sq) = sD(p||q) \). By [vAGL+20, Lemma 2.1], \( D(sp||sq) \geq \frac{1}{4}\|sp - sq\|_1^2 \) if \( \|sp - sq\|_1 \leq 1 \) and \( (1 - \ln 2)\|sp - sq\|_1 \) otherwise. In the first case \( D(p||q) \geq s\|p - q\|_1^2 \), and in the second case \( D(p||q) \geq (1 - \ln 2)\|p - q\|_1 \).

We are now ready to prove the correctness of the algorithm.

**Proof of Theorem 3.11.** If \( \text{cap}_{k,r} \Phi > -\infty \), Corollary 4.18 implies that \textsc{MajSinkhorn} will terminate in the number of iterations \( T \) described in both the \( r = 0 \) and \( r > 0 \) cases of \textsc{DecisionSinkhorn}. Now suppose \( \text{cap}_{k,r} \Phi = -\infty \). First consider the case \( r = 0 \), i.e. \( \text{cap}_k \Phi = -\infty \). We claim \textsc{MajSinkhorn}(\( \Phi, 1_n, 1_m, k, \varepsilon_1 \)) never terminates for \( \varepsilon_1 = O((m + n)^{-1/2}) \). Because \( \text{cap}_k \Phi = -\infty \), one of the three conditions 1, 2, 3 in Lemma 5.1 holds for the scaling \( \hat{\Phi} = e^\Phi \Phi X^{-1/2} Y^{-1/2} \) after the \( z \) update step. After the \( z \) update, Item 1 cannot hold. Thus one of Items 2 or 3 holds, so the algorithm does not terminate. The proof for the case \( r > 0 \) is identical but we use the part of Lemma 5.1 that assumes \( \text{cap}_{k,r} \Phi = -\infty \).

For the running times, we have seen in Section 4.1 that both the \( X \) and \( Y \) update take \( O((m + n)^2(m + n + p)) \) arithmetic operations. Combining with the bound on the number of iterations yields the stated bound on the number of arithmetic operations.

### 5.2 Finding approximate independent sets with \textsc{ApproximateIndep}

We now describe and analyze the algorithm \textsc{ApproximateIndep} for finding an approximate independent set.

**Theorem 5.3.** Let \( k' = k - 1/2n \). If \( (X, Y, z) \in \mathcal{D} \) are such that \( f_{k',r}(X, Y, z) \leq -C \), then the procedure in steps 3 and 4 of Algorithm 4 for

\[
\varepsilon := 2enk^2 e^{-C/k^2}
\]

produces an \( \varepsilon \)-independent set \((L, R)\) that violates \((k, r)\).

**Proof of Theorem 5.3.** Suppose \( (X, Y, z) \in \mathcal{D} \) are such that \( f_{k',r}(X, Y, z) \leq -C \). As in Algorithm 4, let \( u_1, \ldots, u_n \) and \( v_1, \ldots, v_m \) be the eigenvectors of \( X, Y \) in order of decreasing eigenvalue. In this basis we can write \( X, Y = e^{\text{diag}(x)} e^{\text{diag}(y)} \). Consider the matrix \( M_{ij} = \text{Tr} v_i v_j^\dagger \Phi(u_i u_j^\dagger) \) so that

\[
f_{k',r}(X, Y, z) = \sum_{ij} M_{ij} e^{-\|y_i - x_j + z + x \cdot \alpha_t + y \cdot 1 - k'z |} \leq -C.
\]

Note that \( z \geq C/k \) by nonnegativity of \( x, y \).

Let \((\tilde{x}, \tilde{y}) = (x, y)/z\) so that \( \tilde{x} \cdot \alpha_t + \tilde{y} \cdot 1 \leq k' - C/z \leq k' \). Our goal is to show that \( \tilde{x}_{t+1} + \tilde{y}_{s+1} \leq 1 - 1/2nk \) for some \( 0 \leq s \leq m - 1, 0 \leq t \leq n - 1 \) such that \( s + t = k - 1 \) or \( s + t \in \{k - 1, k\} \)
Algorithm APPROXINDEP(Φ, k, r, ε):

Input: A CP map Φ : C^n×n → C^m×m, integers k, r ≤ n such that cap_{k,r} Φ = −∞, and a parameter ε > 0.

Output: An ε-independent set (L, R) violating (k, r).

Algorithm:

1. Normalize Φ to have size at most 1 and set k′ = k − 1/2n.
2. Run MajSinkhorn(Φ, α_r, 1_m, k′, 0) for T = 4k^2(m + n)n^3 log(2e^2nk^2/ε) iterations. Let X, Y, z be the variables in the final step of the algorithm.

3. Let S be the set of integral pairs i ∈ {0 ≤ i ≤ m − 1} for time parameter ε. Hence the pair \( (L, R) \) satisfies Tr π_L Φ(π_R) ≤ ε. If so, output (L, R).

Algorithm 4: Algorithm for finding approximate independent sets.

and t > n − r. By the ordering on x and y, for i > t, j > s we have \( M_{ij} e^{z−x_i−y_j} = M_{ij} e^{z/2nk} \), so by the assumption that \( f_{k′,r}(X, Y, z) \leq −C \) we have \( S e^{z/2nk} − k z \leq −C \) where \( S := \sum i > s, j > t M_{ij} \).

We can write \( S e^{z/2nk} − k z = 2nk^2 g_\lambda (z') \) for \( g_\lambda (z) := e^z − z \) with \( \lambda := S/2nk^2 \) and \( z' = z/2nk \). As the function \( g_\lambda (z) \) takes its minimum at \( z = \max\{0, −\log \lambda\} \), which attains value \( \lambda \) if \( \lambda > 1 \) and \( 1 + \log \lambda \) otherwise, we must have \( \lambda \leq 1 \) and \( 1 + \log \lambda \leq −C/2nk^2 \). That is, \( \log S/2nk^2 \leq 1 − C/2nk^2 \), or \( S \leq 2nk^2 e^{1−C/2nk^2} =: \varepsilon \). Hence the pair \( L = (u_{i+1}, \ldots, u_m), R = (v_{j+1}, \ldots, v_n) \) satisfies Tr π_L Φ(π_R) ≤ ε, which implies ε-independence. The assumption that \( s + t = k − 1 \) or \( s + t ∈ (k, k − 1) \) and \( t > n − r \) implies \( (L, R) \), which has dimensions \( m − s \) and \( n − t \), violates (k, r).

We show that such a pair \( (s, t) \) exists using the probabilistic method, assigning certain probabilities to each pair \( 0 ≤ i ≤ m − 1, 0 ≤ j ≤ n − 1 \) of integers such that \( i + j = k − 1 \) or \( i + j ∈ \{k − 1, k\} \) and \( j ≥ n − r \). We will assign them such that the joint random variable \( (i, j) \) drawn from this probability distribution has \( \mathbb{E}[\bar{x}_{j+1} + \bar{y}_{i+1}] ≤ 1 − 1/2nk \), and hence some particular \( (i, j) \) must satisfy \( \bar{x}_{j+1} + \bar{y}_{i+1} ≤ 1 − 1/2nk \).

We now show how to sample \( (i, j) \). We will construct a function \( h : [0, k] → [0, m − 1] \), choose \( γ \) uniformly at random on \( [0, k] \), and let \( (i, j) = [γ], [h(γ)] \). That is, \( (i, j) \) is chosen proportional to the time the curve \( (γ, h(γ)) \) spends in the cell \( [i, i + 1) × [j, j + 1) \) for time parameter \( γ \in [0, k] \).

The function \( g \) is defined as follows:

\[
h(γ) = \begin{cases} m − ℓ + \frac{1}{μ} (m − ℓ − γ) & 0 < γ < m − ℓ \\
                k − γ & m − ℓ ≤ γ < k 
\end{cases}
\]

See Figure 1 for an example. We first compute \( \mathbb{E}[\bar{x}_{j+1} + \bar{y}_{i+1}] = \mathbb{E}[\bar{x}_{j+1}] + \mathbb{E}[\bar{y}_{i+1}] \). First note that \( γ, g(γ) \) are both non-integral with probability 1, so \( \mathbb{E}[\bar{x}_{j+1}] = \mathbb{E}[\bar{x}_{j+1}] \) and \( \mathbb{E}[\bar{y}_{i+1}] = \mathbb{E}[\bar{y}_{i+1}] \).
Figure 1: An example of the function $h$ for $n = m = 7$, $\ell = 5$, $r = 4$ and hence $k = 14 - 9 = 5$. We choose this coordinate system for consistency with matrices. The red line is the curve $(\gamma, h(\gamma))$ for $\gamma \in [0, k]$. The blue points are the support of the probability distribution on $(i, j)$, for these points $(i, j)$ one can see that $i + j = k - 1$ or $i + j \in \{k - 1, k\}$ and $j > n - r$.

As $\gamma$ is chosen uniformly in $[0, k]$, 

$$
\mathbb{E}[\tilde{y}_{\lceil \gamma \rceil}] = \frac{1}{k} \left( \sum_{i=1}^{k} \tilde{y}_i \right) \leq \frac{1}{k} (\tilde{y} \cdot 1).
$$

By the same reasoning, the chance $\lceil h(\gamma) \rceil$ takes a particular value $t$ is $\frac{1}{k}$ if $1 \leq t \leq h(m - \ell) = n - r$. If, however, $t > n - r$, then the chance $\lceil h(\gamma) \rceil = t$ is at most $\mu/k$ because this corresponds to the region $\gamma \leq m - r$ where $h$ has slope $1/\mu$. Hence $\mathbb{E}[\tilde{x}_{\lceil \gamma \rceil}] \leq (\alpha_r \cdot \tilde{x})/k$, and so 

$$
\mathbb{E}[\tilde{x}_{j+1} + \tilde{y}_{i+1}] \leq \frac{1}{k} (y \cdot 1 + \alpha_r \cdot \tilde{x}) \leq k'/k = 1 - \frac{1}{2nk}.
$$

It remains to show that all $(i, j)$ in the support of the distribution satisfy $i + j = k - 1$ or $i + j \in \{k - 1, k\}$ and $j > n - r$. Conditioned on $\gamma$ in $(m - r, k)$, i.e. the unit slope part of $h$, with probability 1 we have $\lceil \gamma \rceil + \lceil h(\gamma) \rceil = k - 1$ because the line passes along the diagonal of the cells $[i, i + 1] \times [j, j + 1]$ where $i + j = k - 1$. Because $\mu = 1 - 1/n$, the curve $(\gamma, h(\gamma))$ lies between the curves $(\gamma, k - \gamma)$ and $(\gamma, k - \gamma + 1)$. Hence $\lceil \gamma \rceil + \lceil h(\gamma) \rceil$ is always $k - 1$ or $k$. If $h(\gamma) \in (n - r, n - r + 1)$ then $\gamma \in (m - \ell - 1, m - \ell)$ and we have $\lceil \gamma \rceil + \lceil h(\gamma) \rceil = k - 1$. Thus if we have $\lceil \gamma \rceil + \lceil h(\gamma) \rceil = k$ we also have $h(\gamma) \geq n - r + 1$ and hence $\lceil h(\gamma) \rceil > n - r$.

The following is an easy but handy corollary.

**Corollary 5.4.** If $(k, r)$ is not violated by any independent set $(L, R)$ of $\Phi$, then $\Phi$ is $k$-scalable to $(\alpha_r, 1_m)$.

**Proof.** We show the contraposition. If $\Phi$ is not $k$-scalable to $(\alpha_r, 1_m)$, then $\text{cap}_{k, r} \Phi = -\infty$ by Theorem 4.3. Then, by the precious theorem, there exists an $\varepsilon$-independent set violating $(k, r)$ for any $\varepsilon > 0$. By the compactness of approximate independent sets, there exists an independent set violating $(k, r)$. 

---

33
5.3 Independent sets and capacity: Proof of Theorem 3.10

First we have a decomposition lemma using the dominant independent set. Recall that \( k^* = \text{nc-rank} \mathcal{A} \) and \((\ell^*, r^*) = (\dim L^*, \dim R^*)\) where \((L^*, R^*)\) are the dominant independent set of \( \Phi \). Thus we have \( k^* = m + n - \ell^* - r^* \).

**Lemma 5.5.** Let \((L^*, R^*)\) be the dominant independent set of \( \Phi \). Then we can choose orthonormal bases for \( \mathbb{C}^m, \mathbb{C}^n \) in which

\[
A_i = \begin{bmatrix} B_i & C_i \\ D_i & 0 \end{bmatrix}
\]

where the operator \( \Gamma \) with \((m-\ell^*) \times r^* \) Kraus operators \( C_i \) is \((m-\ell^*)\)-scalable to \((1-1/n)1_{r^*}, 1_{m-\ell^*}\), and the operator \( \Psi \) with \( \ell^* \times (n - r^*) \) Kraus operators \( D_i \) is \((n - r^*)\)-scalable. As a consequence, \( \Phi \) is \( k^* \)-scalable to \((\alpha_{r^*}, 1_m)\).

**Proof.** We choose the orthonormal bases \( \{u_i\}, \{v_i\} \) for \( \mathbb{C}^m, \mathbb{C}^n \) so that \( L^* = \langle u_{m-\ell^*+1}, \ldots, u_m \rangle \) and \( R^* = \langle v_{n-r^*+1}, \ldots, v_n \rangle \). Define \( \Gamma, \Psi \) be defined as in the statement of the lemma. We claim that \( \Gamma \) has no non-trivial independent set of size at least \( r^* \) other than \( \{(0, r^*)\} \). For the sake of contradiction, suppose there exists an independent set \((L, R)\) for \( \Gamma \) of size \( r^* \) with \( L \neq \{0\} \). Then \((L^* + L, R)\) is an independent set for \( \Phi \) of size \( \ell^* + \dim L + \dim R = \ell^* + r^* \) with \( \dim R < r^* \), which contradicts the dominance of \((L^*, R^*)\). Thus, by Corollary 5.4, \( \Gamma \) is \((m - \ell^*)\)-scalable to \((1 - 1/n)1_{r^*}, 1_m)\).

Now let us see why \( \Psi \) is \((n - r^*)\)-scalable. If not, there exists an independent set \((L, R)\) for \( \Psi \) of size larger than \( \ell^* \) by Theorem 3.9. By the definition of \( \Psi \), \((L, R + R^*)\) is an independent set of \( \Phi \) of size \( \dim L + \dim R + r^* > \ell^* + r^* \), contradicting the dominance of \((L^*, R^*)\).

We now prove the claim about the scalability of \( \Phi \). Suppose the family of scalings guaranteed by the first part of the lemma for \( \Psi, \Gamma \) are \( \Psi_1, X_1, Y_1 \) and \( \Psi_2, X_2, Y_2 \), respectively. Let \( X(\gamma) := e^{\gamma \text{diag} 1_{[n-\ell^*]}} \), \( Y(\gamma) := e^{\gamma \text{diag} 1_{[m-\ell^*]}} \). One verifies that for \((X, Y) := (X(\gamma) \cdot (X_1 \oplus X_2), Y(\gamma) \cdot (Y_1 \oplus Y_2))\) the scaling \( e^\gamma \Phi_{X^{-1/2}, Y^{-1/2}} \) is the desired scaling as \( \gamma \rightarrow \infty \).

**Proof of Theorem 3.10.** Recall that we take \( k' = k - \frac{1}{2m} \). First note that \( \text{cap}_{k', r} \Phi < \text{cap}_{k', r} \Psi \) because \( f_{k, r} \) is dominated pointwise by \( f_{k', r} \) on \( \mathcal{D} \). Hence 2 implies 3.

We now show 1 implies 2. We first show that if \( L^*, R^* \) is the dominant independent set, then the scaling \( \tilde{\Phi} \) guaranteed by Lemma 5.5 is a \( k^* \)-scaling to \((\alpha_{r^*}, 1_m)\), and hence also a \( k^* \)-scaling to \((\alpha_r, 1_m)\) for any \( r \leq r^* \). Furthermore, \((1-1/k^*)\tilde{\Phi} \) is a \( k \)-scaling to \((\alpha_r, 1_m)\) for any \( k < k^* \) and any \( r \). The pairs \((k, r)\) satisfying these conditions are exactly those dominated by \((k^*, r^*)\) in lexicographic order, and hence by Theorem 4.3 for any such \((k, r)\) we have \( \text{cap}_{k^*, r} \Phi = \text{cap}_{k, r} \Phi > -\infty \).

Finally, we show 3 implies 1. Suppose \( \text{cap}_{k', r} \) is finite. By Theorem 4.3, for any \( \varepsilon > 0 \) the operator \( \Phi \) has a scaling \( \tilde{\Phi} \) that is \((\alpha_r, 1_m)\)-majorized and has size at least \( k' - \varepsilon \). The dominant independent sets of \( \Phi, \tilde{\Phi} \) are related by linear transformations, so it is enough to bound \( r^* = \dim R \geq r \) where \( L, R \) is the dominant independent set for \( \Phi \). First suppose \( k = k^* \) and \( r > r^* \). Because \((L, R)\) is independent for \( \Phi \), we have

\[
\text{Tr} \Pi_{R^*} \tilde{\Phi}^*(I_m) + \text{Tr} \Pi_{L^*} \tilde{\Phi}(I_n) \geq \text{Tr} \Phi(I_n) \geq k' - \varepsilon.
\]

Without loss of generality assume \( \Phi(I), \Phi(I)^* \) are diagonal with decreasing elements along the diagonal, and the diagonals are majorized by \( 1, \alpha_r \), respectively.

34
By the Courant-Fisher min-max theorem, \( \text{Tr} \tilde{\Phi}^*(I_m) \Pi_{R^2} \leq \sum_{i=1}^{n-r^*} \mu_i \) where \( \mu \) is the spectrum of \( \tilde{\Phi}^*(I) \). As \( \mu \) is majorized by \( \alpha_r \), we have \( \sum_{i=1}^{n-r^*} \mu_i \leq (n-r) + (1-1/n)(r-r^*) \leq n-r^*-1/n. \) As \( \tilde{\Phi}(I_n) \preceq I_m \), we have \( \text{Tr} \Pi_{L^2} \tilde{\Phi}(I_n) \leq n - \epsilon^2. \) Thus \( \text{Tr} \tilde{\Phi}^*(I_m) \Pi_{R^2} + \text{Tr} \Pi_{L^2} \tilde{\Phi}(I_n) \leq k^*-1/n. \) If \( \varepsilon < 1/(2n) \), this leads to the contradiction \( k^*-1/n < k^*/\varepsilon \leq k^*-1/n. \) A similar argument leads to a contradiction in the case \( k > k^* \). \hfill \Box

Now we prove Theorem 3.12.

**Proof of Theorem 3.12.** If \( \text{cap}_{k,r} \Phi = -\infty \), then by Theorem 3.10 we have \( \text{cap}_{k',r} \Phi = -\infty \). By (the proof of) Theorem 3.11, \( \text{MAJSINKHORN}(\Phi, \alpha_r, I_m, k', \varepsilon_2) \) does not terminate for \( \varepsilon_2 = O(1/\sqrt{(m+n)n^2}) \). By Lemma 4.8, \( f_{k',r}(X,Y,z) \leq 1 - \frac{1}{4} T \varepsilon_2^2 \) after \( T \) steps. Thus in \( 4(C+1)/\varepsilon_2^2 \) steps we have \( f_{k',r}(X,Y,z) \leq C. \) By Theorem 5.3, the procedure in steps 3 and 4 of \( \text{APPROXINDEP} \) for \( \varepsilon = 2enk^2e^{-C/nk^2} \) produces an \( \varepsilon \)-independent set \((L,R)\) that violates \((k,r)\). Thus \( C = nk^2 \log(2enk^2/\varepsilon) \) and hence we require \( T = 4k^2(m+n)n^2 \log(2enk^2/\varepsilon). \)

The number of arithmetic operations follows from the bound \( O((m+n)^2(m+n+p)) \) from Section 4.1 on the number operations required for each iteration of \( \text{MAJSINKHORN} \). The number of operations for Step 4 is dominated by the number of operations for Step 3. \hfill \Box

## 6 Rounding approximate shrunk subspaces

In this section, we prove that we can round an \( \varepsilon \)-approximate dominant independent set to the exact dominant independent set. To this end, we need a bit complexity bound of the dominant independent set. We present a simple randomized algorithm for finding the minimum shrunk subspace using the Wong sequence, from which the desired bit complexity bound follows.

### 6.1 Wong sequence

Here we describe how to use Wong sequences to find the minimum maximally shrunk subspace. We refer frequently to [IKQS15]; in that work they refer to a \( c \)-shrunk subspace as a \( c \)-singularity witness.

**Definition 6.1** (Wong sequence). For a matrix space \( A \subseteq \mathbb{C}^{n \times n} \) and \( A \in A \), the (second) Wong sequence of \((A,A)\) is defined as

\[
W_0 := \{0\}, \quad W_i := A(A^{-1}(W_{i-1})) \quad (i = 1, 2, \ldots),
\]

where \( A^{-1}(W_{i-1}) \) is the preimage of \( W_{i-1} \) under \( A \).

Here we summarize the necessary properties of the Wong sequence. Let \( c := n - \text{nc-rank} A \).

**Lemma 6.2 ([IKQS15, Lemma 9]).** For the Wong sequence \((W_i)\) of \((A,A)\), the following holds.

1. \( W_i \) is nonincreasing, i.e., \( W_{i-1} \subseteq W_i \) for \( i = 1, 2, \ldots \). (Hence there exists the limit of \( W_i \), which we denote by \( W_\infty \))

2. If \( A \in B \) satisfies \( \text{rank} A = \text{nc-rank} A \), then \( U^* := A^{-1} W_\infty \) is a \( c \)-shrunk subspace.

3. \( A^{-1} W_\infty \geq A^{-1} W_\infty \), where \( A^{-1} W_\infty := \bigcap_{B \in A} B^{-1} W_\infty \).
4. If a subspace $U$ satisfies $A^{-1}U \supseteq A^{-1}U$, then $U \supseteq W_\infty$.

**Lemma 6.3** (implicit in [IKQS15]). If $A \in \mathcal{A}$ satisfies $\text{rank } A = \text{nc-rank } A$, then $U^* = A^{-1}W_\infty$ is the minimum $c$-shrunk subspace. In particular, the limit $W_\infty$ of the Wong sequence is independent from the choice of $A$.

**Proof.** Take an arbitrary $c$-shrunk subspace $U$. Then,

$$\text{nc-rank } A = \text{rank } A$$

$$\leq \dim A(U) + \dim A(U^\perp)$$

$$= n - \dim U - \dim U^\perp + \dim A(U) + \dim A(U^\perp)$$

$$\leq n - \dim U + \dim A(U) + \dim A(U^\perp) - \dim U^\perp$$

$$(A(U) \subseteq A(U))$$

$$\leq n - \dim U + \dim A(U)$$

$$(\dim A(U^\perp) \leq \dim U^\perp)$$

$$\leq n - c$$

$$= \text{nc-rank } A.$$

Therefore, the above inequalities are tight. In particular, we have $A(U) = A(U)$ and $\dim U - \dim A(U) = n - \text{nc-rank } A = n - \text{rank } A = \dim \ker A$. From $\dim U - \dim A(U) = \dim \ker A$, we have $\ker A \subseteq U$. Therefore, $U = A^{-1}(A(U))$. Then, $A^{-1}(A(U)) = A^{-1}(A(U)) \supseteq U = A^{-1}(A(U))$.

By Lemma 6.2, $W_\infty \subseteq AU$. Hence, $U^* = A^{-1}W_\infty \subseteq A^{-1}(A(U)) = U$. \hfill \quare

Computing a basis of the Wong sequence $(W_i)$ may lead to an explosion of the bit complexity. Thankfully, one can use a clever trick proposed in [IKQS15] to compute a basis of $(W_i)$ with the bit complexity bounded. Let $M_A$ denote the maximum absolute value of any of the Gaussian integer entries of $A$. Let $A^+$ be a pseudoinverse of $A$ scaled to have Gaussian integer entries. Then, $W_i = (AA^+)^i \ker(AA^+)$ for $i \geq 1$ (see [IKQS15, Lemma 10]). First, we compute a basis $v_1, \ldots, v_{d_0}$ of $\ker(AA^+)$ by the Gaussian elimination. A basis of $W_i$ can be found by finding a maximum independent set from $\{A_jA^+v_q : j \in [p], q \in [d_0]\}$. To this end, it suffices to find a maximum independent column subset from a $n \times pd_0$ matrix, which takes $O(n^2pd_0) = O(pn^3)$ time. Similarly, a basis a basis $w_1, \ldots, w_{d'}$ of $W_i$, we can find a basis of $W_{i+1}$ by finding a maximum independent set from $A_jA^+w_q (j \in [p], q \in [d'])$ in $O(nm^3)$ time. In total, it takes $O(pn^4)$ time to compute a basis of $W_\infty$. The basis vector of $W_i$ constructed in this way is in the form of

$$(A_{j_1}A^+) \cdots (A_{j_k}A^+)v_k$$

for some $j_1, \ldots, j_k \in [p]$ and $k \in [d_0]$, so the bit complexity is polynomially bounded. Specifically, can take $A^+$ and $v_k$ to have integer entries at most $e^{O(n \log(M_A n))}$ in absolute value. For $v_k$ this follows because $\ker(AA^+) = \text{Im}(A)^\perp$. Hence we can take any basis vectors of $W_i$ to be integral with maximum entry $e^{O(n \log(M_A n) + 1 \log M)}$. Therefore we have the following.

**Lemma 6.4.** A basis of the limit $W_\infty$ of the Wong sequence of $(A, \mathcal{A})$ can be computed in $O(pn^4)$ time. If $A$ has Gaussian integer entries with absolute value at most $M_A$ and $A$ has a basis with Gaussian integer entries of absolute value at most $M$, then the output basis will have Gaussian integer entries at most $e^{O(n^2 \log(M_A n) + n \log M)}$ in absolute value, as will all intermediate numbers.
6.2 A randomized algorithm for finding minimum optimal shrunk subspace

The matrix subspace

\[ \mathcal{A}^{(d)} = \langle A_i \otimes E_{jk} : i \in [p], j, k \in [d] \rangle \]

is called the \(A\)th blow-up space of \(\mathcal{A}\), where \(E_{jk}\) is the matrix with 1 at the \((j,k)\)-entry and 0 elsewhere. If \(d\) is the minimum blow-up size of \(\mathcal{A}\), then there exists a constant matrix \(A \in \mathcal{A}^{(d)}\) such that rank \(A = d\).\(\text{rank} \mathcal{A} = \text{rank}(\mathcal{A}^{(d)})\). We can find such a matrix \(A\) (with high probability) by substituting random integers to the entries of \(X_i\). Then, one can compute the limit \(W_\infty\) of the Wong sequence of \(\langle A, \mathcal{A}^{(d)} \rangle\) and \(U^* = A^{-1}W_\infty\) is the minimum \(dc\)-shrunk subspace of \(\mathcal{A}^{(d)}\) by Lemma 6.3. One can obtain the minimum \(c\)-shrunk subspace of \(\mathcal{A}\) from \(U^*\) by the following lemmas. In the following, we denote the set of \(d \times d\) complex matrices by \(M(d, \mathbb{C})\).

**Lemma 6.5** (cf. [IQS17, discussion above Proposition 5.2]). If a subspace \(W \subseteq \mathbb{C}^{nd}\) satisfies \((I \otimes M(d, \mathbb{C}))W = W\), then \(W = W_0 \otimes \mathbb{C}^d\). Moreover, we can take \(W_0 = \{ w \in \mathbb{C}^n : u \otimes e_i \in W \ 	ext{for all} \ i \in [d] \}\).

**Proof.** To see \(W_0 \otimes \mathbb{C}^d \subseteq W\), take \(w = w_0 \otimes v\) for \(w_0 \in W_0\) and \(v \in \mathbb{C}^d\) arbitrarily. Then, \(w = w_0 \otimes \sum_{i=1}^d v_i e_i = \sum_{i=1}^d w_0 (w_0 \otimes e_i) \in W\). On the other hand, take an arbitrary \(w \in W\) and write \(w = \sum_{j=1}^d w_j e_j \in W\), where \(w_j \in \mathbb{C}^d\) is the \(j\)th \(d\)-dimensional subvector of \(w\). Then, we have \((I \otimes E_{ij})w = w_j \otimes e_i \in W\) for \(i, j \in [d]\) by \((I \otimes M(d, \mathbb{C}))W = W\). Therefore, \(w_j \in W_0\) for \(j \in [d]\), which means \(w \in W_0 \otimes \mathbb{C}^d\). Hence \(W_0 \otimes \mathbb{C}^d \supseteq W\). \(\square\)

**Lemma 6.6.** Let \(U\) be a \(dc\)-shrunk subspace of \(\mathcal{A}^{(d)}\). Then, \(U = U_0 \otimes \mathbb{C}^d\) and \(U_0\) is a \(c\)-shrunk subspace for \(\mathcal{A}\). If \(U\) is minimum, then \(U_0\) is also minimum.

**Proof.** Below we denote \(\mathcal{A}^{(d)}\) by \(\mathcal{B}\) to simplify the notation. First note that, by construction, \(\mathcal{B}\) satisfies \((I \otimes M(d, \mathbb{C}))\mathcal{B} = \mathcal{B}\) and \(\mathcal{B}(I \otimes M(d, \mathbb{C})) = \mathcal{B}\). Let \(W = BU\). Then,

\[ (I \otimes M(d, \mathbb{C}))W = (I \otimes M(d, \mathbb{C}))BU = BU = W. \]

By the previous lemma, \(W = W_0 \otimes \mathbb{C}^d\). Let \(U' = (I \otimes M(d, \mathbb{C}))U\). Then, \(U' \supseteq U\) and \(BU' = \mathcal{B}(I \otimes M(d, \mathbb{C}))U = BU = W\), so

\[ dc \geq \dim U' - \dim BU' \geq \dim U - \dim BU = dc. \]

Thus, \(\dim U' = \dim U\) and hence \(U' = (I \otimes M(d, \mathbb{C}))U = U\). By the previous lemma, \(U = U_0 \otimes \mathbb{C}^d\). We have \(W_0 \subseteq AU_0\) since \(\mathcal{B} = \mathcal{A} \otimes M(d, \mathbb{C})\). Thus,

\[ \dim U_0 - \dim AU_0 \geq \dim U_0 - \dim W_0 = \frac{\dim U - \dim W}{d} = c \]

and \(U_0\) is a \(c\)-shrunk subspace for \(\mathcal{A}\).

Now suppose \(U\) is the minimum \(dc\)-shrunk subspace of \(\mathcal{A}^{(d)}\). If \(U'\) is a \(c\)-shrunk subspace of \(\mathcal{A}\), then \(U' \otimes \mathbb{C}^d\) is a \(dc\)-shrunk subspace of \(\mathcal{A}^{(d)}\). Therefore, \(U' \otimes \mathbb{C}^d \supseteq U = U_0 \otimes \mathbb{C}^d\) by minimality of \(U\). Hence, \(U' \supseteq U_0\). As this holds for any \(c\)-shrunk subspace of \(\mathcal{A}\), \(U_0\) is minimum. \(\square\)

We summarize our algorithm in Algorithm 5.

**Theorem 6.7.** Algorithm 5 finds the minimum \(c\)-shrunk subspace with probability at least \(1/2\). Furthermore, it makes \(O(pd^4n^4)\) arithmetic operations over \(\mathbb{Q}\) and the output as well as all intermediate vectors have Gaussian integer entries with magnitude at most \(e^{O(n^2d^2 \log(Mdn^4)+nd \log M)}\).
Algorithm RandomizedShrunkSubspace($A_1, \ldots, A_p, d, k$):

**Input:** Basis $A_i \in \mathbb{Z}[\sqrt{-1}]^{n \times n}$ ($i = 1, \ldots, p$) of $A$, the minimum blow-up size $d$ of $A$, and an upper bound $k$ of the noncommutative rank of $A$.

**Output:** The minimum $c$-shrunk subspace of $A$, where $c = n - nc$-rank $A$.

**Algorithm:**

1. Draw random $d \times d$ matrices $X_i$ ($i = 1, \ldots, p$), where each entry of $X_i$ is drawn from $\{0,1,\ldots,2dk-1\}$ independently.
2. Compute $A = \sum_{i=1}^{p} A_i \otimes X_i$.
3. Compute the Wong sequence $(W_i)$ of $(A, A^{(d)})$ and compute a basis of $U^* = A^{-1}W_\infty$.
4. Compute a basis of $U_0^* = \{ u \in \mathbb{C}^n : u \otimes e_i \in U^* \text{ for } i \in [d] \}$ by Gaussian elimination.
5. **output** $U_0^*$.

**Algorithm 5:** Randomized algorithm for finding the minimum shrunk subspace.

Proof. If $A$ is rank maximum in $A^{(d)}$, the output $U_0^*$ is the minimum $c$-shrunk subspace of $A$ by the above discussion. Hence, it suffices to bound the probability that $A$ attains the maximum rank in $A^{(d)}$. Let $k^*$ denote nc-rank $A$. Since $A^{(d)}$ contains a constant matrix of rank $dk^*$, there exists a $dk^* \times dk^*$ nonvanishing minor in $\sum_{i=1}^{p} A_i \otimes X_i$, where we regard each entry of $X_i$ as an indeterminate. The degree of the minor (as a polynomial) is $dk^*$. By the Schwartz-Zippel lemma, the minor does not vanish even with probability at least $1/2$ after substituting random integers from $\{0,1,\ldots,2dk-1\}$ to the indeterminates. Thus, the rank of $A$ is at least $dk$ with probability at least $1/2$, which completes the proof of the validity of the algorithm.

The running time is dominated by computing the Wong sequence of $(A, A^{(d)})$, which is $O(pd^4n^4)$ time by Lemma 6.4. By Lemma 6.4, the bases of the Wong sequence can be written down with Gaussian integer entries of magnitude at most $e^{O(n^2d^2\log(M_And)+nd\log M)}$. By construction we have $M_A \leq (2dk-1)M$, so this is at most $e^{O(n^2d^2\log(M_And)+nd\log M)}$.

Theorem 3.14 follows.

Proof of Theorem 3.14. By Theorem 6.7, the smallest shrunk subspace $R$ has a basis with Gaussian entries of magnitude at most $e^{O(n^2d^2\log(M_And)+nd\log M)} = e^{O(n^4\log(M_A))}$, where we use $d, k \leq n$. The orthogonal projection to $R$ is then proportional to a matrix with Gaussian integer entries of magnitude at most $e^{O(n^5\log(Mn))}$; see Theorem A.2.

6.3 Stability of approximate shrunk subspaces

We begin by proving a converse to Theorem 5.3, namely that approximate independent sets violating $(k, r)$ of certain dimensions imply low capacity is small. Combined with our capacity lower bounds, this implies a lower bound close to independent a pair of subspaces violating $(k^*, r^*)$ can be.
Lemma 6.8. Suppose \( \Phi \) has size at most 1 and \((L, R)\) is an \( \varepsilon \)-independent set that violates \((k, r)\). Then

\[
\text{cap}_{k,r} \Phi \leq 1 + \frac{1}{n}(1 + \log(np\varepsilon^2)).
\]

Proof. Let \( \dim L = \ell' \) and \( \dim R = r \). Choose orthonormal bases so that \( L = \langle e_{m-\ell'+1}, \ldots, e_m \rangle \) and \( R = \langle e_{n-r'+1}, \ldots, e_n \rangle \). In this basis the Kraus operators will take the form

\[
A_i = \begin{bmatrix} B_i & C_i \\ D_i & E_i \end{bmatrix}
\]

where \( E_i \) has largest singular value at most \( \varepsilon \) and hence squared Frobenius norm at most \( n\varepsilon^2 \). If we choose \( X = e^{\text{diag}(x)}, Y = e^{\text{diag}(y)} \), the objective function is of the form

\[
f(X, Y, z) = \sum_{i,j} e^{-y_i-x_j+z} \sum_s |(A_s)_{ij}|^2 + x^i \cdot \alpha_r + y \cdot 1 - k z.
\]

Now take \( x = t1_{\overline{L}}, y = t1_{\overline{R}} \), and \( z = t \). Observe that

\[
f(X, Y, z) \leq \sum_s \|A_s\|^2_{F} + e^t \sum_s \|E_s\|^2_{F} + t1_{\overline{R}} \cdot \alpha_r + (m-\ell')t - kt.
\]

Note that \( 1_{\overline{R}} \cdot \alpha_r < (n-r') \), so if \( \ell' + r' > \ell + r \) then \( t1_{\overline{R}} \cdot \alpha_r + (m-\ell')t - kt \leq -t \). If instead \( \ell' + r' = \ell + r \) but \( r < \ell \), then \( t1_{\overline{R}} \cdot \alpha_r + (m-\ell')t - kt \leq ((n-r')-1/n)t + (m-\ell')t - kt \leq -t/n \). In either case,

\[
f(X, Y, z) \leq \sum_s \|A_s\|^2_{F} + e^t \sum_s \|E_s\|^2_{F} - t/n \leq 1 + n\varepsilon^2 e^t - t/n.
\]

The last inequality follows from the assumption that \( \text{Tr} \Phi(I_n) \leq 1 \) and that \((L, R)\) is \( \varepsilon \)-independent. The result follows from setting \( t = \log(1/n\varepsilon^2) \). \( \square \)

We now combine the above result with our capacity lower bounds.

Theorem 6.9. Let \( \varepsilon_0 = \varepsilon_0(\Phi) \) be the minimum value of \( \varepsilon \) such that there is an \( \varepsilon \)-independent set of \( \Phi \) violating \((k^*, r^*)\). If \( \Phi \) has Kraus operators with integer entries at most \( M \), then

\[
\varepsilon_0 = e^{-O(k^*(n+m)\log(m+n)+n\log Mp)}
\]

Proof. Suppose there is an \( \varepsilon \)-independent set violating \((k^*, r^*)\). We rescale \( \Phi \) so that Lemma 6.8 applies. By the Gaussian integer assumption, \( c = \text{Tr} \Phi(I_n)^{-1} \leq 1 \). Thus \((L, R)\) remains an \( \varepsilon \)-independent set for \( c\Phi \).

From Lemma 6.8 we have \( \text{cap}_{k^*,r^*} c\Phi \leq 1 + \frac{1}{n}(1 + \log(np\varepsilon^2)) \). Therefore from Lemma 4.17 we have

\[
1 + \frac{1}{n}(1 + \log(np\varepsilon)) \geq \text{cap}_{k^*,r^*} \Phi + n \log c.
\]

Note that \( \log c \geq -\log(M^2 npm) \). Rearranging the terms and plugging in Theorem 4.16 yields

\[
\varepsilon \geq \frac{1}{np}e^{n(\text{cap}_{k^*,r^*} \Phi + n \log c - 1) - 1} = e^{-O(k^*(n+m)\log(m+n)+k^* \log p+n\log(M^2 pm n))}.
\]

Rearranging terms and using \( k^* \leq n \) completes the proof. \( \square \)
The bound on \( \varepsilon_0 \) from Theorem 6.9 together with the next theorem implies Theorem 3.13.

**Theorem 6.10.** Assume \( \|A_i\|_F \leq 1 \) for all \( i \), and that \((L, R)\) is an \( \varepsilon \)-approximate independent set of size \( q := \dim L^* + \dim R^* \) such that \( \dim R \leq \dim R^* \) and \( \varepsilon \leq \varepsilon_0 \). Then

\[
\|\pi_L - \pi_{L^*}\|_2, \|\pi_R - \pi_{R^*}\|_2 = O(\varepsilon_0^{-2n-1} \varepsilon).
\]

**Proof.** The idea is to find new approximate independent sets as follows: write \( L = H \oplus H' \) and \( R = K \oplus K' \), and hope that \((L^* + H, K')\) and \((H', R^* + K)\) are \( \varepsilon' \)-approximate independent sets for \( \varepsilon' \leq \varepsilon_0 \). One can check that the independent sets sizes sum to \( 2q \) provided \( H \cap L^*, K \cap R^* \) are empty, so either one is strictly larger than \( q \) and both are of size \( q \) and \( \dim(L^* + H) > \dim(L^*) \) and hence \( \dim K' < \dim R^* \). Unfortunately, this only works if every element in \( H \) is reasonably far from \( L^* \) and every element of \( H' \) is very close to \( L^* \) and the analogous property holds for \( K, R \).

There’s no reason to expect such a gap.

In order to fix this, we modify \( A_i, L \) and \( R \) so that there exist subspaces \( H, K \) with this property. Choose a basis such that the Kraus operators \( A_i \) are written

\[
A_i = \begin{bmatrix}
B_i & C_i \\
D_i & 0
\end{bmatrix}
\]

and the dominant independent set corresponds to the 0 block. Define \( X(t) = \text{diag}(t^{-1}1_{m-\ell} \oplus t1_\ell) \) and \( Y(t) = \text{diag}(t^{-1}1_{m-r} \oplus t1_r) \), and let the operator \( \tilde{\Phi} \) have Kraus operators

\[
\tilde{A}_i := X(t)A_iY(t) = \begin{bmatrix}
t^{-2}B_i & C_i \\
D_i & 0
\end{bmatrix}.
\]

By Lemma 6.11 below we have \( \text{cap}_{k,r} \tilde{\Phi} = \text{cap}_{k,r} \Phi \). Clearly \((L^*, R^*)\) is still an independent set for \( \tilde{\Phi} \) and \( \Phi \), and because \( \text{cap}_{k,r} \Phi > -\infty \) it is also dominant.

We take \( \tilde{L} = X(t)^{-1}L \) and \( \tilde{R} = Y(t)^{-1}R \). First note that \((\tilde{L}, \tilde{R})\) is a \( t^2 \varepsilon \)-independent set of \( \tilde{\Phi} \): for any unit vectors \( v \in L, w \in R \) we have

\[
\frac{(X(t)^{-1}v)^\dagger \tilde{A}_i(Y(t)^{-1}w)}{\|X(t)^{-1}v\|_2\|Y(t)^{-1}w\|_2} \leq t^{-2}\|v^\dagger A_iw\| \leq t^2 \varepsilon.
\]

For \( t \) large, \( X(t)^{-1} \) has the effect of moving vectors in \( L \) that are not in \( L^* \) closer to \((L^*)^\perp\). Setting \( t \) large tends to make more orthogonal with \( L^* \). If the distance from \( v \) to \( L^* \) is \( \delta \), then the distance from \( X(t)^{-1}v/\|X(t)^{-1}v\|_2^2 \) to \( L^* \) is

\[
t \delta \sqrt{t^2 \delta^2 + (1 - \delta^2)t^{-2}},
\]

as can be seen from writing \( v = \pi_L v + (I - \pi_{L^*})v \). We will choose \( t \) carefully so that vectors that are very close to \( L^* \) stay close, and vectors that are not close get mapped far from \( L^* \). Let \( \delta_i \) denote the singular values of the projections \( L \to (L^*)^\perp \) and \( R \to (R^*)^\perp \) in increasing order (so there are \( \ell + r = q \) total of them). More specifically, \( \delta_1 \leq \cdots \leq \delta_q \) are the singular values of \( Q_{(L^*)^\perp}^\dagger Q_L \) and \( Q_{(R^*)^\perp}^\dagger Q_R \), where \( Q_L \) denotes a matrix with \( Q_L^\dagger Q_L = I \) and \( \text{Im} Q_L = L \), and the others are defined similarly. By the \( \sin(\Theta) \) theorem, they are the sine of principal angles between
L and L* (resp. R and R*). Let $\delta := \max \delta_i$. This is the sine of the maximum principal angle, so we have $\delta = \max \{\|\pi_{L^*} - \pi_L\|_2, \|\pi_R - \pi_R\|_2\}$.

Because $q \leq 2n$, there is some $\delta_p \geq (0.01\varepsilon_0)^{2n}\delta$ such that $\delta_{p-1}/\delta_p \leq 0.01\varepsilon_0$, where we define $\delta_0 := 0$. Let $S$ denote the sets of indices where $\delta_i$ came from $L$. Without loss of generality assume $\delta$ belongs to $L_i$, i.e. $q \in S$. Set $t = \delta_p^{-1/2}$.

For $i \in S$, write the $i$th singular vector $v_i \in L$ as $v_i = \sqrt{1 - \delta_i^2}x_i + \delta_iy_i$ for unit vectors $x_i \in L^*$, $y_i \in (L^*)^\perp$. Note that $v_i \in L$ is the $i$th principal vector, and $x_i \in L^*$ and $y_i \in (L^*)^\perp$ are corresponding the principal vectors of $L^*$ and $(L^*)^\perp$, respectively. Moreover, because they are right singular vectors, $y_i$ are orthogonal for $i \in S$ and hence $x_i$ are as well. Then $L$ will be spanned by the vectors

$$w_i = X(t)^{-1}v_i = t^{-1}\sqrt{1 - \delta_i^2}x_i + t\delta_iy_i.$$ 

The $w_i$ will remain orthogonal for all $t \in (0, \infty)$, and normalizing each to a unit vector yields

$$\hat{w}_i = \frac{t^{-1}\sqrt{1 - \delta_i^2}x_i + t\delta_iy_i}{\sqrt{(1 - \delta_i^2)t^{-2} + \delta_i^2t^2}}.$$ 

Note that the second coefficient is a monotone increasing function of $t \in (0, \infty)$ and $\delta_i \in (0, 1)$ and vice versa for the first. Take

$$H = \langle \hat{w}_i : i \geq p, i \in S \rangle, \quad H' = \langle \hat{w}_i : i < p, i \in S \rangle$$

$$K = \langle \hat{w}_i : i \geq p, i \not\in S \rangle, \quad K' = \langle \hat{w}_i : i < p, i \not\in S \rangle.$$ 

Obviously, we have $L = H \oplus H'$ and $R = K \oplus K'$. The inner product between $\hat{w}_i \in H$ and any unit vector in $L^*$ is at most

$$\frac{\delta_i^{1/2}\sqrt{1 - \delta_i^2}}{\sqrt{(1 - \delta_i^2)\delta_p + \delta_p}} \leq \frac{1}{\sqrt{2}}. \quad (6.1)$$ 

by our choice of $t$ and $H$. In particular, this implies $L^* \cap H = \{0\}$. On the other hand, for any unit vector in $H'$, the inner product with any unit vector in $L^*$ is at most

$$\frac{\delta_p^{-1/2}\delta_i}{\sqrt{(1 - \delta_i^2)\delta_p + \delta_i^2\delta_p^{-1}}} \leq \frac{0.01\delta_i^{1/2}\varepsilon_0}{\sqrt{5}\delta_p + 0.01\varepsilon_0\delta_p} \leq 0.03\varepsilon_0. \quad (6.2)$$

The analogous inequalities hold for $K, K'$. Now we can check the quality of our independent sets. We prove it for $(L^* + H, K')$; the proof for $(H', R^* + K)$ follows mutatis mutandis. Let $v \in L^*, h \in H$ and let $w + z \in K'$ be a unit vector with $w \in R^*$ and $\|z\| \leq 0.03\varepsilon_0$ as guaranteed by the upper bound (6.2) of inner product between $K'$ and $R^*$. Then

$$(v + h)^\dagger\hat{A}_i(w + z) = v^\dagger\hat{A}_iw + h^\dagger\hat{A}_i(w + z) + v^\dagger\hat{A}_iz \leq 0 + \delta_p^{-1}\varepsilon_0\|h\| + 0.03\varepsilon_0\|v\| \leq (\delta^{-1}\varepsilon_0^{-2n}\varepsilon + 0.03\varepsilon_0)(\|h\| + \|v\|)\|w + z\|.$$
The first inequality used that \((L^*, R^*)\) is \(\epsilon\)-independent for \(\Phi\). It remains to bound \(\|h\| + \|v\|\) by \(\|h + v\|\). But by our upper bound \((6.1)\) of inner product,
\[
\|h + v\|^2 \geq \|h\|^2 + \|v\|^2 - 2\langle h, v \rangle \geq \|h\|^2 + \|v\|^2 - \sqrt{2}\|h\||\|v\|\| \\
\geq 2 \left( \frac{1}{2}(\|h\| + \|v\|) \right)^2 - \sqrt{2} \left( \frac{1}{2}(\|h\| + \|v\|) \right)^2 \geq \frac{1}{4}(2 - \sqrt{2})(\|h\| + \|v\|)^2
\]
by two applications of Jensen’s inequality.

Putting this all together, we find that \((L^* + H, K')\) and \((H', R^* + K)\) are \((10\delta^{-1}\varepsilon_0^{-2n}\varepsilon + .5\varepsilon_0)\)-independent sets of size \(q\). Because \(H\) was nonempty and \(L^* \cap H = \{0\}\), we have \(\dim(L^* + H) > \dim L^*\). Thus, by Theorem 6.9, we must have \(10\delta^{-1}\varepsilon_0^{-2n}\varepsilon \geq .5\varepsilon_0\), or else there is some \(< \varepsilon_0\)-independent set \((L', R')\) with size strictly bigger than \(q\) or of size \(q\) with \(\dim R' < \dim R^*\).

**Lemma 6.11.** If \(\Phi\) has Kraus operators with block decomposition
\[
A_i = \begin{bmatrix} B_i & C_i \\ D_i & 0 \end{bmatrix}
\]
where \(E_i\) is \(\ell \times r\) for \(\ell + r = m + n - k\), and \(\tilde{\Phi}\) has Kraus operators
\[
\tilde{A}_i = \begin{bmatrix} t^{-2}B_i & C_i \\ D_i & 0 \end{bmatrix},
\]
for \(t > 0\) then \(\text{cap}_{k,r}\tilde{\Phi} = \text{cap}_{k,r}\Phi\).

**Proof.** We show that a family of \(\varepsilon\)-minimizers to both objective functions asymptotically achieves the same function value. Let \(X(\gamma) := e^{\gamma \text{diag} A_{m-r}}, Y(\gamma) := e^{\gamma \text{diag} A_{m-t}}\). We have seen (Lemma 5.5) that there are \(X_1, X_2, Y_1, Y_2\) such that \((X, Y, z) := X(2\gamma) \cdot (X_1 \oplus X_2), Y(2\gamma) \cdot (Y_1 \oplus Y_2), 2\gamma\) achieves \(f_{k,r}(X, Y, z) \leq \text{cap}_{k,r}\Phi + \varepsilon\) as \(\gamma \to \infty\). We also have \(f_{k,r} \geq \text{cap}_{k,r}(\Phi)\) because \((X, Y, z)\) is feasible. Note that \(X, Y\) are Hermitian because the block diagonal matrices commute with \(X(\gamma), Y(\gamma)\) resp.

One checks that for any \(\gamma\),
\[
f_{k,r}(X, Y, z) = \text{Tr}(Y_1 \oplus Y_2)^{-1}\Phi_{e^{\gamma X(\gamma)}, e^{\gamma Y(\gamma)}}((X_1 \oplus X_2)^{-1}) \\
+ \alpha_r \cdot \lambda \log X(2\gamma) + \alpha_r \cdot \lambda (X_1 \oplus X_2) \\
+ \log \det(Y(2\gamma)) + \log \det(Y_1 \oplus Y_2) - 2k\gamma.
\]
Here we have used that \(X(\gamma), (X_1 \oplus X_2)\) commute. Some terms cancel:
\[
\alpha_r \cdot \lambda \log X(2\gamma) + \log \det(Y(2\gamma)) - 2k\gamma = 2\gamma(n - r + m - \ell - k) = 0.
\]
Therefore
\[
f_{k,r}(X, Y, z) = \text{Tr}(Y_1 \oplus Y_2)^{-1}\Phi_{e^{\gamma X(\gamma)}, e^{\gamma Y(\gamma)}}((X_1 \oplus X_2)^{-1}) + \alpha_r \cdot \lambda (X_1 \oplus X_2) + \log \det(Y_1 \oplus Y_2).
\]
By Lemma 5.5, the same \((X, Y, z)\) are also \(\varepsilon\)-minimizers for the objective function for \(\tilde{\Phi}\), with the expression
\[
\text{Tr}(Y_1 \oplus Y_2)^{-1}\tilde{\Phi}_{e^{\gamma X(\gamma)}, e^{\gamma Y(\gamma)}}((X_1 \oplus X_2)^{-1}) + \alpha_r \cdot \lambda (X_1 \oplus X_2) + \log \det(Y_1 \oplus Y_2).
\]
But $\Phi e^{\gamma X(-\gamma)} Y(-\gamma)$ and $\tilde{\Phi} e^{\gamma X(-\gamma)} Y(-\gamma)$ tend to the same operator as $\gamma \to \infty$ - namely the one with Kraus operators

$$
\begin{bmatrix}
0 & C_i \\
D_i & 0
\end{bmatrix}.
$$

Thus the function values are asymptotically the same. Letting $\varepsilon \to 0$ completes the proof. \hfill $\square$

### 6.4 Proof of correctness of RoundSubspaces

**Proof of Theorem 3.15.** Theorem 3.11 implies each call to DECISIONSINKHORN produces correct results and takes $O((m+n)^2(m+n+p)(k(n+m)^2 \log(m+n) + n \log M))$ operations. The number of operations taken for the calls to DECISIONSINKHORN is dominated by the calls in the binary search for $r^*$, and there are $O(\log n)$ such calls. Hence the total arithmetic operations here is at most $O((m+n)^2(m+n+p)(k(n+m)^2 \log^2(m+n) + \log M \log n))$.

By Theorem 3.12, APPROXINDEP is correct and takes $O(\alpha^2 n^3(m+n)^3(m+n+p) \log(n \varepsilon)) = O(n^5(m+n)^3(m+n+p) \log(n \varepsilon))$ operations, where $\varepsilon = 1/2M_0 M_1^2 = e^{-O((mn^2 + n^3) \log(m+n) + n^3 \log(Mnp))}$. Hence the total number of operations is $O(n^7(m+n)^3(m+n+p)((m+n) \log(m+n) + n^3 \log(Mnp)))$.

The application of APPROXINDEP produces an $\varepsilon$-independent pair $(L,R)$ violating $(k^*, r^* + 1)$ for $\varepsilon = 1/2M_0 M_1^3$. It remains to show that our rounding procedure is correct, i.e. that after rounding $\pi_R$ we obtain $\pi_{R^*}$. By Theorem 3.14, there is some number $0 < q \leq M_1 = e^{O(n^3 \log(Mn))}$ such that every entry of $\pi_{R^*}$ takes the form $p/q$ for $p \in \mathbb{Z}$. On the other hand, by Theorem 3.13 we know that $\|\pi_R - \pi_{R^*}\|_2 \leq M_0 \varepsilon$, so by Lemma 6.12 every entry $\alpha$ of $\pi_R$ differs from the corresponding entry $p/q$ of $\pi_{R^*}$ by at most $M_0 \varepsilon$. By our choice of $\varepsilon$, $M_0 \varepsilon \leq 1/2M_1^3$. If we round $\alpha$ to the nearest rational number $a/b$ satisfying $b \leq M_1$, we must have $|a/b - \alpha| \leq M_0 \varepsilon$. But by our choice of $\varepsilon$ we have $M_0 \varepsilon < 1/2M_1^3$, and so $|a/b - p/q| < 1/M_1^3$. Hence we must have $a/b = p/q$. The rounding takes time $O(\log M_1) = O(n^9 \log(Mn))$, which is dominated by the other steps. \hfill $\square$

**Lemma 6.12.** Let $A \in \mathbb{C}^{n \times n}$ be a Hermitian matrix. Then $\|A\|_2 \geq \sup_{i,j \in [n]} |A_{ij}|$.

**Proof.** By interlacing it is enough to prove this for $2 \times 2$ matrices. For the diagonal entries it is true by $\|A\|_2 \geq e_i^\dagger A e_i$. For the off-diagonal entries, note that $\lambda_1(A)^2 + \lambda_2(A)^2 = A_{11}^2 + A_{22}^2 + 2|A_{12}|^2$. The larger of $\lambda_1(A)^2$, $\lambda_2(A)^2$ is at least half this expression, which is at least $|A_{12}|^2 = |A_{21}|^2$. \hfill $\square$

### 7 Application to fractional linear matroid matching and rank-2 Brascamp-Lieb polytope

In this section, we describe applications of our algorithms to fractional linear matroid matching and rank-2 BL polytope.

#### 7.1 Fractional linear matroid matching and rank-2 Brascamp-Lieb polytope

Let us recall the definition of fractional matching polytope [Van92]. Let $M = (E,I)$ be a matroid. Note that the size of the ground set $E$ may be infinite but $M$ must have a finite rank. A subset of $E$ of rank one or two is called a line. Note that a line need not to be a flat in general. Given a matroid $M$ and a set of lines $L (p = |L|)$, the fractional matroid polytope is given by

$$
a(F) \cdot x \leq r(F), \quad (F: \text{flat of } M)
$$

$$
x \geq 0,
$$

(7.1)
where \( a(F) \in \{0, 1, 2\}^L \) is defined as

\[
a(F)_\ell = \begin{cases} 
0 & (F \cap \ell = \emptyset) \\
2 & (F \supseteq \ell) \\
1 & \text{(otherwise)}
\end{cases}
\]

and \( r \) is the rank function of \( M \). A vector in this polytope is called a fractional matroid matching. A fractional matroid matching \( x \) is said to be \textit{perfect} if \( 2 \sum_{i \in L} x_i = n \).

In particular, we are interested in the case that the matroid is defined by the linear independence in \( \mathbb{C}^n \) and each line is a two-dimensional subspace in \( \mathbb{C}^n \). We call it the \textit{fractional linear matroid matching polytope}. Assume that each line \( \ell_i \) is given by the row space of \( B_i \in \mathbb{C}^{2 \times n} \). Then, the perfect fractional matching polytope is given by

\[
\sum_{i=1}^{p} x_i \dim(\text{row } B_i \cap V) \leq \dim V, \quad (V: \text{subspace of } \mathbb{C}^n)
\]

\[
2 \sum_{i=1}^{p} x_i = n, \\
x_i \geq 0 \quad (i = 1, \ldots, p)
\]

If all \( B_i \) are real matrices of rank-2, the perfect fractional linear matroid matching polytope coincides with the BL polytope of a tuple of operators \( B = (B_1, \ldots, B_p) \). Recall that the BL polytope for full row-rank operators \( B_i \in \mathbb{R}^{n_i \times n} \) is given by (1.1).

\textbf{Lemma 7.1.} If \( n_i = 2 \) for all \( i \), (7.2) and (1.1) define the same polytope.

\textit{Proof.} For \( V \subseteq \mathbb{C}^n \), let \( W = V^\perp \). Then \( \dim(\text{row } B_i \cap V) = n_i - \dim(B_i W) \). So (7.2) implies (1.1). The other direction is analogous. \qed

Thus, linear optimization on rank-2 BL polytopes can be reduced to the algorithms on fractional matroid matching polytopes [CLV01a, GP13]. However, the algorithms of [CLV01a, GP13] are polynomial only in the arithmetic model, i.e., the bit complexity of the intermediate numbers may explode. Furthermore, the algorithm of [CLV01a] is fairly complicated. We might hope to use the following “scaling” characterization of the BL polytope to find a simpler algorithm.

\textbf{Theorem 7.2} ([BCCT08, GGOW18]). Suppose each \( B_i \) has rank \( n_i \) and \( x \in \mathbb{R}_{\geq 0}^p \). The following are equivalent:

1. \( x \in \text{BL}(B) \).

2. For every \( \varepsilon > 0 \) there is an invertible matrix \( g \in \mathbb{R}^{n \times n} \) and invertible matrices \( h_i \in \mathbb{R}^{n_i \times n_i} \) such that \( \tilde{B}_i := h_i B g^T \) satisfies

\[
(1 - \varepsilon) I_n \preceq \sum_{i=1}^{p} x_i \tilde{B}_i \tilde{B}_i^\dagger \preceq (1 + \varepsilon) I_n
\]

and \( \tilde{B}_i \tilde{B}_i^\dagger = I_{n_i} \forall i \in [p] \).

3. The following quantity is finite:

\[
\text{cap}_x B := \inf_{X > 0, Z_i > 0} \sum_{i=1}^{n} \text{Tr } B_i X^{-1} B_i^\dagger Z_i^{-1} + x_i \log \det Z_i + \log \det X.
\]
Moreover, suppose $x = c/d$ for $c \in \mathbb{Z}_{\geq 0}$, $d \in \mathbb{Z}_{>0}$, and that the entries of $B$ are Gaussian integers with absolute value at most $\log M$. Then it is possible to decide if $x \in BL(B)$ in time $\text{poly}(k, d, n, \log M)$ where $k = \sum_i c_i n_i$.

The third item looks different from the optimization problem considered in [BCCT08], but it is easily shown that the conditions are equivalent. In the following, we provide a simple Sinkhorn-style algorithm for finding a maximum fractional linear matroid matching.

### 7.2 Algorithm for finding maximum fractional linear matroid matching

We are to solve the following linear program.

$$\begin{aligned}
\text{maximize} & \quad \sum_{i=1}^{p} x_i \\
\text{subject to} & \quad \sum_{i=1}^{p} x_i \dim(\text{row } B_i \cap V) \leq \dim V, \quad (V: \text{subspace of } \mathbb{C}^n) \\
& \quad x_i \geq 0 \quad (i = 1, \ldots, p)
\end{aligned}$$

Denote the feasible region of this program by $P(B)$. The dual problem is the *minimum 2-cover problem*. A pair $(S, T)$ of flats in $M$ is called a 2-cover if $a_i(S) + a_i(T) \geq 2$ for each $i$. A 2-cover $(S, T)$ is said to be nested if $S \subseteq T$ and minimum if $r(S) + r(T)$ is minimized. [CLV01b] showed that the size of maximum fractional matroid matching is equal to the size of a minimum 2-cover.

While we could define a Sinkhorn-style algorithm directly using the $B_i$’s, we instead relate 2-covers for fractional linear matroid matching with shrunk subspaces of a matrix space in order to re-use the algorithms we have already defined.

Let $a_i, b_i$ be arbitrary basis of line $\ell_i = \text{row } B_i$ and let $A_i = a_i \wedge b_i := a_i b_i^T - b_i a_i^T \in \mathbb{C}^{n \times n}$ for each $i \in [p]$. Let $\mathcal{A}$ be the matrix space spanned by $A_1, \ldots, A_p$. Then, it is easy to see that $(S, T)$ is a nested minimum 2-cover if and only if $(S^\perp, T^\perp)$ is a maximum independent set; see [OS22]. The lattice structure of maximum independent sets implies the existence of minimum 2-cover $(S^*, T^*)$ such that $S^* \subseteq S$ and $T \subseteq T^*$ for any nested minimum 2-cover $(S, T)$. This special minimum 2-cover is called the dominant 2-cover [CLV01b]. Thus, if $(L, R)$ is the dominant independent set, then $(L^\perp, R^\perp)$ is the dominant 2-cover. So we can find the dominant 2-cover with Algorithm 4.

A maximum fractional matching can be also found by $\text{MajSinkhorn}$ for a CP map $\Phi : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}$ with the Kraus operator $A_i$. Note that $\Phi(X) = \Phi^*(X)$ because $A_i^T = -A_i$. This implies that $f_k(X, \overline{Y}, z) = f_k(Y, X, z)$ (see (3.6) for the definition of $f_k$). Let $\tilde{\Phi} = \Phi_{g,k}$ be a $k$-scaling of $\Phi$ to $(\mathbf{1}_n, \mathbf{1}_n)$. First observe that we can take $h = \overline{g}$. This follows from the g-convexity

$$\frac{f_k(X, \overline{Y}, z) + f_k(Y, \overline{X}, z)}{2} \geq f_k((X \# Y, \overline{Y} \# \overline{X}, z) = f_k((X \# Y, \overline{X} \# \overline{Y}, z))$$

where $X \# Y$ denotes the mid point of the geodesic between $X$ and $Y$, i.e., the matrix geometric mean of $X$ and $Y$.

By the scaling condition of $\Phi$, for any $\varepsilon > 0$, there exists $g$ such that

$$\sum_{i=1}^{p} \tilde{A}_i \tilde{A}_i^T \preceq (1 + \varepsilon)I_n, \quad \sum_{i=1}^{p} \text{Tr}(\tilde{A}_i \tilde{A}_i^T) \geq k, \quad (7.3)$$
where $\tilde{A}_i = gA_i g^T = g(a_i \land b_i) g^T$. Denote $\tilde{a}_i = ga_i$ and $\tilde{b}_i = gb_i$ so that $\tilde{A}_i = \tilde{a}_i \land \tilde{b}_i$. Apply the Gram-Schmidt orthogonalization to $\tilde{a}_i, \tilde{b}_i$ and obtain an orthonormal basis $u_i, v_i$ of $\text{Im}(\tilde{A}_i)$. This is equivalent to the thin QR-decomposition:

$$
[\tilde{a}_i \quad \tilde{b}_i] = [u_i \quad v_i] \begin{bmatrix}
    r_{11}^{(i)} & r_{12}^{(i)} \\
    0 & r_{22}^{(i)}
\end{bmatrix} := Q_i R_i.
$$

By $\tilde{a}_i = r_{11}^{(i)} u_i$ and $\tilde{b}_i = r_{12}^{(i)} u_i + r_{22}^{(i)} v_i$, we have $\tilde{a}_i \land \tilde{b}_i = (r_{11}^{(i)} u_i) \land (r_{12}^{(i)} u_i + r_{22}^{(i)} v_i) = r_{11}^{(i)} r_{22}^{(i)} u_i \land v_i = \det R_i u_i \land v_i$ since $u_i \land v_i = 0$. Plugging this back, we have

$$
\sum_{i=1}^p |\det R_i|^2 (u_i \land v_i) (u_i \land v_i) \leq (1 + \varepsilon) I_n, \quad \sum_{i=1}^p |\det R_i|^2 \text{Tr}((u_i \land v_i) (u_i \land v_i) \dagger) \geq k.
$$

Now observe that $(u_i \land v_i) (u_i \land v_i) \dagger$ is the orthogonal projection onto $\text{Im}(\tilde{A}_i)$. This follows from $(u_i \land v_i) (u_i \land v_i) \dagger = (u_i u_i^T - v_i v_i^T)(v_i u_i^T - u_i v_i^T) = u_i u_i^T + v_i v_i^T = Q_i Q_i^T$ by the orthonormality of $u_i, v_i$. So $\text{Tr}((u_i \land v_i) (u_i \land v_i) \dagger) = \dim \text{Im}(\tilde{A}_i) = 2$. Letting $x_i := |\det R_i|^2$, we have

$$
\sum_{i=1}^p x_i 1_{\text{Im}(\tilde{A}_i)} \leq (1 + \varepsilon) I_n, \quad (7.4)
$$

and $\sum_{i=1}^p x_i \geq k/2$. We can show that $x$ satisfies the constraints of fractional linear matroid matching up to $(1 + \varepsilon)$ multiplicative error. Here is a useful lemma for obtaining the linear inequalities for all subspaces from a matrix inequality.

**Lemma 7.3.** Let $\pi_V$ be the orthogonal projection onto a subspace $V_i$ and $x_i \geq 0 (i = 1, \ldots, m)$, and $\alpha \geq 0$. If $\sum_{i=1}^m x_i \pi_V \leq \alpha I_n$, then $\sum_{i=1}^m x_i \dim(V_i \cap V) \leq \alpha \dim V$ for any subspace $V$.

**Proof.** For any subspace $V$, multiplying the orthogonal projection $\pi_V$ onto $V$, we obtain $\sum_{i=1}^m x_i \pi_V \pi_V \leq \alpha \pi_V$. Taking the trace of both sides, $\sum_{i=1}^m x_i \text{Tr}(\pi_V \pi_V) \leq \alpha \dim V$. Now the claim follows from $\text{Tr}(\pi_V \pi_V) \geq \dim(V_i \cap V)$ and $x_i \geq 0$ for each $i$. □

For any subspace $V$, the subspace $\tilde{V} = gV$ satisfies $\text{Im}(A_i) \cap V = \text{Im}(\tilde{A}_i) \cap \tilde{V}$. By Lemma 7.3 and (7.4), we have

$$
\sum_{i=1}^p x_i \dim(\text{Im}(\tilde{A}_i) \cap \tilde{V}) \leq (1 + \varepsilon) \dim \tilde{V} = (1 + \varepsilon) \dim V,
$$

so $x/(1 + \varepsilon)$ is a fractional linear matroid matching of size $k/(2(1+\varepsilon))$. Summarizing this argument, we obtain Algorithm 6.

We obtain the following theorem from Theorems 4.9 and 3.11.

**Theorem 7.4.** For any $\varepsilon > 0$, Algorithm 6 finds a $(1 - \varepsilon)$-maximum fractional linear matroid matching in $O(n^3(n + p)(n^2 \log^2 n + \log n \log M + \frac{1}{\varepsilon}(n \log n + \log Mp)))$ arithmetic operations. Furthermore, the bit complexity of intermediate numbers is $\text{poly}(n, p, \log M)$.

For a constant $\varepsilon > 0$, Algorithm 6 runs in $\tilde{O}(n^3(n + p))$ time, where the $\tilde{O}$ notation hides the $\text{poly}(\log n, \log M, 1/\varepsilon)$ factor, which improves $O(n^3p^4)$ time of [CLV01a] for fractional linear matroid matching. Furthermore, we can also bound the bit complexity of intermediate numbers, whereas [CLV01a] did not analyze the bit complexity.
Algorithm FracLinearMatroidMatching($B_1,\ldots,B_p$):

**Input:** Lines $\{a_i,b_i\} \subseteq \mathbb{C}^n$ ($i = 1,\ldots,p$), a parameter $\varepsilon > 0$.

**Output:** A $(1 - \varepsilon)$-maximum fractional linear matroid matching $x$.

**Algorithm:**

1. Compute $A_i = a_i \land b_i$ for each $i$. Let $\mathcal{A}$ be the matrix space spanned by $A_i$.
2. Determine the noncommutative rank $k$ of $\mathcal{A}$ with DecisionSinkhorn (Algorithm 3) and binary search.
3. Find a matrix $g$ that satisfies the scaling condition (7.3) with Algorithm 2.
4. For each $i$, let $\tilde{A}_i = gA_ig^T$ and $x_i = \frac{|\det R_i|^2}{1+\varepsilon}$, where $R_i$ is the upper-triangular factor of the thin QR-decomposition of $\tilde{A}_i$.
5. **output** $x$.

**Algorithm 6:** Deterministic algorithm for finding an approximate maximum fractional linear matorid matching.

### 7.3 Scaling characterization of the fractional linear matroid matching polytope

We show a scaling characterization of $P(B)$ analogously to Theorem 7.2. The characterization is identical to that of Theorem 7.2 apart from the lower bound by $(1 - \varepsilon)I_n$ in the second item and the constraint $X \succeq I_n$ in the third item.

**Theorem 7.5.** Suppose each $B_i$ has rank $n_i$ and $x \in \mathbb{R}_{\geq 0}^p$. The following are equivalent:

1. $x \in P(B)$.
2. For every $\varepsilon > 0$ there is an invertible matrix $g \in \mathbb{R}^{n \times n}$ and invertible matrices $h_i \in \mathbb{R}^{n_i \times n_i}$ such that $\tilde{B}_i := h_iBg^T$ satisfies
   \[
   \sum x_i \tilde{B}_i \tilde{B}_i^\dagger \preceq (1 + \varepsilon)I_n
   \]
   and $\tilde{B}_i \tilde{B}_i^\dagger = I_{n_i}$ $\forall i \in [p]$.
3. The following quantity is finite:
   \[
   \text{cap}_x B := \inf_{X \succeq I_n, Z_i > 0} \sum_{i=1}^n \text{Tr} B_i X^{-1} B_i^\dagger Z_i^{-1} + x_i \log \det Z_i + \log \det X.
   \]

Moreover, suppose $x = c/d$ for $c \in \mathbb{Z}_{\geq 0}^p$, $d \in \mathbb{Z}_{>0}$, and that the entries of $B$ are Gaussian integers with absolute value at most $\log M$. Then it is possible to decide if $x \in P(B)$ in time $\text{poly}(k,d,n,\log M)$ where $k = \sum_i c_i n_i$. 47
Proof. Let $S$ be the set of $x \geq 0$ for which the desired $g_i, h_i$ exist, and let $C$ be the set of $x \geq 0$ for which $\text{cap}_x B$ is finite. It is straightforward from calculus $C \subseteq S$, i.e. (3) implies (2), because if the capacity is finite then we may take $g^\dagger g = X$ and $h^\dagger h_i = Z_i$ from $X, Z$ with subgradients of the objective function of norm $\varepsilon$. Furthermore, $S$ is convex by the log-convexity of $\text{cap}_x \Phi_B$ in $x$.

We may also easily check that $S \subseteq P(B)$, i.e. (2) implies (1), by checking that $x \in S$ implies the inequalities for $P(B)$. Let $\varepsilon > 0$ to be determined, and let $\tilde{B}_i$ be as in the theorem statement. For any subspace $V$, the subspace $\tilde{V} = g^\dagger V$ satisfies row $B_i \cap V = row \tilde{B}_i \cap \tilde{V}$. Consider the orthogonal projection $\pi_{\tilde{V}}$ onto $\tilde{V}$. By the condition on the $\tilde{B}_i$’s and Lemma 7.3, we have that

$$\sum x_i \dim \text{row } B_i \cap V \leq (1 + \varepsilon) \dim V.$$ 

Taking $\varepsilon \to 0$, we have $x \in P(B)$.

In summary, so we have

$$C \subseteq S \subseteq P(B)$$

or equivalently (3) $\implies$ (2) $\implies$ (1). To show that these containments are in fact equalities, and so (1) $\implies$ (3), it suffices to show that every extreme point of $P(B)$ is contained in $C$. To do this, observe that every extreme point $x$ of $P(B)$ may be written as $c/d$ where $d \in \mathbb{Z}$ and $c \in \mathbb{Z}^P$. We may assume all $x_i > 0$, and let $k = \sum c_i n_i$. For contradiction, assume $\text{cap}_x \Phi_B = -\infty$. Construct a CP map $\Psi$ as in [GGOW18] with $k \times nd$ Kraus operators with a block structure having $p$ groups of rows with $c_i n_i$ consecutive rows each, broken into $c_i$ groups of $n_i$ consecutive rows and columns broken into into consecutive groups of $n$ columns. Each of the $d \cdot \prod c_i$ many Kraus operators has exactly one of these $n_i \times n$ blocks filled with $B_i$ and the rest equal to zero. It is straightforward to check that $\text{cap}_k \tilde{\Psi} = d \text{cap}_x cB = -\infty$ where $cB = (c_1 B_1, \ldots, c_p B_p)$. By Theorem 3.9, there is an independent set $L, R$ for $\Psi$ such that $\dim L + \dim R \geq k + nd - k = nd$. We only increase the dimension of $L$ and $R$ by assuming $R = \oplus_{i=1}^d V$ for $V \subseteq \mathbb{R}^n$ and $L = \oplus_{i=1}^p \oplus_{j=1}^{n_i} (B_i V)^\perp$. Thus

$$\sum_i c_i \dim (B_i V)^\perp + d \dim V > nd.$$ 

Using $\dim (B_i V)^\perp = \dim V^\perp \cap \text{row } B_i$ for $B_i$ full row rank and $x_i = c_i/d$, we have $\sum_i x_i \dim \text{row } B_i \cap V^\perp > d \dim V^\perp$, contradicting $x \in P(B)$.

The construction of $\Psi$ yields an algorithm for deciding membership in $P(B)$: simply construct $\Psi$ from $B, c, d$ and check if $\text{cap}_k \Psi > -\infty$ for $k = \sum c_i n_i$. By the argument above, this is the case if and only if $x \in P(B)$. The runtime follows from Theorem 3.11 applied to $\Psi$. A pseudocode is shown in Algorithm 7.

We now outline why this algorithm works. We keep it brief because it is so similar to the proof of Corollary 4.18.

Proof outline of Theorem 1.4. The proof follows a similar structure to typical analyses of Sinkhorn-type algorithms. We use the objective function $f(X, Y) := \sum_{i=1}^n \text{Tr } B_i X^{-1} B_i Y_i^{-1} + x_i \log \det Y_i + \log \det X$ from Theorem 7.5.

First suppose that $x \in P(B)$. The capacity lower bound independent of $x_i$ is similar to the proof of 4.16. It follows by using the reduction in the proof of Theorem 7.5 on the vertices of $P(B)$ and applying concavity of $\text{cap}_x (B)$ in $x$. The progress bound is very similar to the proof of Theorem 4.9. This time the generalized KL projections are to the point $\oplus_i x_i 1_{n_i}$ (the $Y_i$ update) and the
violated by $x$

An integral vector can be checked in polynomial time by the result of [GGOW18] because the common coefficients form a certificate with polynomial bit-complexity. Note that the membership of a half-integral vector $x$ there exists a facet-defining valid inequality

\[ \sum_{\alpha} \alpha \in \text{polytope} \{ \mu : \mu \leq 1_n \} \text{ (the } X \text{ update). The former makes progress because it is an alternating minimization step, and the latter was already analyzed Theorem 4.9.}

Finally, Lemma 4.10 shows that the output $y$ is in $P(B)$, and it is equal to $e^{-\varepsilon} x$, hence the distance bound. On the other hand, if $x$ is at least $\varepsilon$-far from $P(B)$, then the Sinkhorn steps will not terminate and hence the algorithm will correctly output that $x$ is not in the polytope.

**Proof of Theorem 1.2.** As mentioned earlier, an NP certificate for $x^* \in BL(B)$ can be obtained by decomposing $x^*$ as a convex combination of half-integral vertices. These vertices and convex coefficients form a certificate with polynomial bit-complexity. Note that the membership of a half-integral vector can be checked in polynomial time by the result of [GGOW18] because the common denominator is a constant.

For an NP certificate for $x^* \notin BL(B)$, we can proceed as follows. Wlog, we can assume that $\sum_i n_i x_i^* = n$, and therefore we need to certify that $x^* \notin P(B)$. Not being in $P(B)$ means that there exists a facet-defining valid inequality $\alpha^T x \leq \beta$ for $P(B)$ with $\alpha \in \{0,1,2\}^p$ and $\beta \in \mathbb{Z}_+$ violated by $x^*$. The certificate consists of $p$ affinely independent half-integral points (or vertices) $x(i) \in \frac{1}{2}\mathbb{Z}^p \cap BL(B)$ for $i = 1, \cdots, p$ satisfying $\alpha^T x(i) = \beta$ for all $i$. Either $\alpha \in \{0,1,2\}^p$ and $\beta \in \mathbb{Z}_+$ are also part of the certificate, or the verifier first computes them (by solving a system of linear equations), and the verifier then checks that $\alpha^T x^* > \beta$. The next task for the verifier is to check that $\alpha$ and $\beta$ indeed defines a valid inequality for $P(B)$. For this purpose, the verifier computes

\[ y^* = \frac{1}{p} \sum_{i=1}^p x(i) + \frac{1}{4p^2} 1. \]

We claim that the validity of $\alpha^T x \leq \beta$ over $P(B)$ can be checked by verifying that $x(i) \in P(B)$ for every $i$ and that $y^* \notin P(B)$. This would complete the proof as these tasks can be done in
polynomial time using the result of [GGOW18] since the common denominator of these points is either 2 (for the $x^{(l)}$’s) or $4p^2$ (for $y^*$).

To prove the claim, consider any facet-defining valid inequality $\gamma^T x \leq \delta$ for $P(B)$ with $\gamma \in \{0,1,2\}^p$ and $\delta \in \mathbb{Z}_+$ for which $\gamma^T y^* > \delta$. Such inequality must exist. If this inequality is not $\alpha^T x \leq \beta$ then one of the $x^{(i)}$’s would satisfy $\gamma^T x^{(i)} \leq \delta - \frac{1}{2}$ by half-integrality, and therefore

$$
\gamma^T y^* = \frac{1}{p} \sum_{i=1}^{p} \gamma^T x^{(i)} + \frac{1}{4p^2} \gamma^T 1 \leq \delta - \frac{1}{2p} + \frac{1}{2p} = \delta,
$$

a contradiction. Thus, the unique $\{0,1,2\}$ facet-defining inequality separating the $x^{(i)}$’s from $y^*$ must be $\alpha^T x \leq \beta$, proving its validity.

\[\blacksquare\]

### 7.4 Pseudopolynomial weighted optimization algorithm

In this section we describe algorithm \textsc{WeightedSinkhorn} (Algorithm 8) to find the optimum value $OPT$ of the linear program

\[
\begin{align*}
\text{maximize} & \quad w^T x \\
\text{subject to} & \quad \sum_{i=1}^{p} x_i \dim(\text{row } B_i \cap V) \leq \dim V, \quad (V: \text{subspace of } \mathbb{C}^n) \\
& \quad x_i \geq 0 \quad (i = 1, \ldots, p),
\end{align*}
\]

i.e. $OPT = \max \{w^T x : x \in P(B)\}$, in time $\text{poly}(\|w\|_1, m, n)$. We will find a feasible point $x$ such that $w^T x > OPT - 1/2$, which if all $n_i = 2$ implies $OPT = [2x]/2$ by half-integrality of the feasible region. Let $H_{w,k} = \{x : w^T x \geq k\}$, and let $D(H_{w,k} \| \alpha)$ denote the generalized KL distance from $\alpha$ to $H_{w,k}$. We assume that $B_i$ have full row rank, and so $\|x\|_\infty \leq 1$ for all $x \in P(B)$ and $e_i \in P(B)$ for all $i$. Thus $\|w\|_\infty \leq OPT \leq \|w\|_1$. We also assume $w \geq 0$ because the negative coordinates will be optimized at $x_i = 0$.

To analyze the algorithm, we define another capacity.

$$
f_{w,k}(X,Y,z) = \sum_{i=1}^{p} e^{w_i z/n_i} \text{Tr } B_i X^{-1} B_i^T Y_i^{-1} - k z + \log \det X. \quad (7.5)
$$

Consider the geodesically convex domain $\mathcal{D}' = \{(X,Y,z) : X \succ I_n, \det Y_i = 1, z \geq 0\}$, and define

$$
\text{cap}_{w,k} B := \inf_{Y \in \mathcal{D}'} f_{w,k}(Y). \quad (7.6)
$$

We will show that our modified capacity characterizes the optimum over the BL polytope. First, we show that it acts as a Lyapunov function much as in Theorem 4.9.

\textbf{Theorem 7.6.} Suppose $w \in \mathbb{R}_{\geq 0}^p$, $k \geq \|w\|_\infty$, and $0 \leq \varepsilon \leq 1$.

- \textit{If} \textsc{WeightedSinkhorn} terminates before step $T$, then the output is a feasible point $x$ with $w^T x \geq (1 - \varepsilon)k$.
- \textit{If} $\text{cap}_{w,k} B$ is finite and $\sum_i \|B_i\|_F^2 \leq 1$, \textsc{WeightedSinkhorn} terminates before step

$$
T = 2 \cdot \frac{1 - \text{cap}_{w,k} B}{\varepsilon^2}.
$$

50
Algorithm \text{WeightedSinkhorn}(B_1, \ldots, B_p):

\textbf{Input:} A $p$-tuple of $n_i \times n$ complex matrices $B = (B_1, \ldots, B_p)$, a vector $w \in \mathbb{R}^p_{\geq 0}$, a number $k \in \mathbb{Z}_{>0}$, a running time $T$, and a parameter $0 < \varepsilon$.

\textbf{Output:} A feasible point $x$ such that $w^T x > (1 - \varepsilon)k$ if $OPT \geq k$, and that $OPT < k$ otherwise.

\textbf{Algorithm:} Set $X = I_n, Y_i = I_{n_i}, z = 0$, and $\delta := \varepsilon/(2\sqrt{n})$. Define $\tilde{w}_i := w_i/n_i$. For $t = 1, \ldots, T$:

1. Update $Y$: Set $Y_i = e^{\tilde{w}_i z} B_i X^{-1} B_i^\dagger$ and then set $Y_i = Y_i / \det(Y_i)^{1/n_i}$.

2. Update $X, z$:
   - Let $\mu = \lambda(\sum_i e^{\tilde{w}_i z} X^{-1/2} B_i^\dagger Y_i^{-1} B_i X^{-1/2})$. Set $\varepsilon_X = \sum_{i \in 1} \mu_i - 1 - \log \mu_i$.
   - For $i \in [p]$ set $\nu_i = \text{Tr} e^{\tilde{w}_i z} B_i^\dagger Y_i^{-1} B_i X^{-1}$ and $\varepsilon_Z = D(H_{\tilde{w}, \mu} || \nu)$.

   If: $\varepsilon_X, \varepsilon_Z \leq \frac{\varepsilon^2}{T}$: Output $x_i = e^{-\delta \nu_i}/n_i$.

   Else:
     - If: $\varepsilon_Z$ is larger: set $\alpha_i = \text{Tr} B_i^\dagger Y_i^{-1} B_i X^{-1}$ and choose $z$ to be the minimum value such that $\sum_i \tilde{w}_i \alpha_i \geq k$.
     - If: $\varepsilon_X$ is larger: choose $X$ in the same eigenbasis as $\sum_i e^{\tilde{w}_i z} B_i^\dagger Y_i^{-1} B_i$ with eigenvalues $\lambda_i(X) = \max\{1, \mu_i\}$.

\textbf{Output} that $OPT < k$.

\textbf{Algorithm 8:} Algorithm for optimizing a linear functional over the Brascamp-Lieb polytope.

The proof is so similar to that of Theorem 4.9 that we omit many of the details, but we include a sketch below. We’ll use a standard convex duality lemma for generalized KL projections.

\textbf{Lemma 7.7.} Let $0 \neq \alpha \in \mathbb{R}^p_{>0}$, $w \in \mathbb{R}^p_{\geq 0}$, and $k \geq 0$. Then

$$D(H_{w,k} \| \alpha) = \sum_{i=1}^p \alpha_i - \min_{z \geq 0} \left( \sum_{i=1}^p e^{w_i z} \alpha_i - k z \right),$$

where $D(H_{w,k} \| \alpha)$ is the generalized Kullback-Leibler distance from $\alpha$ to the half-space $H_{w,k} = \{ x : w^T x \geq k \}$. Furthermore, $\arg \min_{z \geq 0} \left( \sum_{i=1}^p e^{w_i z} \alpha_i - k z \right) = \{ z : \sum_i w_i e^{w_i z} \alpha_i \geq k \} \cup \{0\}$.

In particular this lemma shows that the $z$-update step minimizes $f_{w,k}$ in $z$ while holding the other variables fixed. If $w^T \alpha \geq k$, then $\inf_{z \geq 0} \sum_{i=1}^p e^{w_i z} \alpha_i - k z$ is simply $\sum_i \alpha_i$ because $D(\alpha \| \alpha) = 0$. We also have an analogue of Lemma 4.8 for the $z$ update.

\textbf{Corollary 7.8} (z-update progress bound). Let $z \geq 0$, $\alpha_i \in \mathbb{R}^p_{>0}$ and $w \in \mathbb{R}^p$. Let $\nu_i = e^{w_i z} \alpha_i$. Then

$$\sum_{i=1}^p e^{w_i z} \alpha_i - k z \geq D(H_{w,k} \| \nu) + \sum_{i=1}^p \alpha_i - D(H_{w,k} \| \alpha).$$

In particular, the progress made in the $z$ update of \text{WeightedSinkhorn} is at least $D(H_{w,k} \| \nu) \geq \delta^2/2$.  

51
Proof. Like Lemma 4.8, the proof is a change of variables. By Lemma 7.7,

\[ \sum_i \alpha_i - D(H_{w,k}||\alpha) = \min_{z' \geq 0} \left( \sum_{i=1}^p e^{w_i z'} \alpha_i - k z' \right) \leq \min_{z' \geq 0} \left( \sum_{i=1}^p e^{w_i (z' + z)} \alpha_i - k(z' + z) \right) = -kz + \min_{z' \geq 0} \left( \sum_{i=1}^p e^{w_i z'} \nu_i - k z' \right) = -kz + \sum_{i=1}^p e^{w_i z} \alpha_i - D(H_{w,k}||\nu). \]

Rearranging the terms yields the inequality. The progress bound follows from Lemma 7.7, because the terms that depend on \( z \) change from \( \sum_{i=1}^p e^{w_i z} \alpha_i - kz \) to \( \min_{z' \geq 0} \left( \sum_{i=1}^p e^{w_i z'} \alpha_i - k z' \right) = \sum_i \alpha_i - D(H_{w,k}||\alpha). \]

Proof of Theorem 7.6. We first verify that, assuming the algorithm terminates, the output is a feasible point. We claim that \( \tilde{B}_i = \sqrt{\hat{m}/\nu_i} e^{w_i z/n} Y_i^{-1/2} \tilde{B}_i X^{-1/2} \) and \( x \) satisfy the conditions in Theorem 7.5 for feasibility of \( x \). As in the algorithm, let \( \tilde{w}_i = w_i/n_i \). By the \( Y \) update step previously, \( \tilde{B}_i \tilde{B}_i^\dagger = I_{n_i} \). Hence \( \tilde{B}_i \tilde{B}_i^\dagger/\nu_i = I_{n_i} \). On the other hand, \( \sum_i x_i \tilde{B}_i \tilde{B}_i^\dagger = e^{-\delta} \sum_i e^{w_i z} X^{-1/2} B_i^\dagger Y_i^{-1} B_i X^{-1/2} \), which has spectrum \( e^{-\delta} \mu \) for \( \mu \) as in the \( X, Y \) update step of the algorithm. Note that \( D(P_n||\mu) = \sum_{i=1}^p e^{w_i z} \nu_i - 1 - \log \mu_i \), so Lemma 4.10 implies \( e^{-\delta} \mu \leq 1 \). This implies \( x \) is feasible.

Next we verify that \( w^T x \) is at least \( (1 - \varepsilon)k \). By the termination condition, we know there is some \( \beta \in \mathbb{R}_{\geq 0}^p \) such that \( \tilde{w}^T \beta \geq k \) and \( D(\beta||\nu) \leq \delta^2/2 \). Then we have \( w^T x = e^{-\delta} \tilde{w}^T \nu, \) and

\[ \tilde{w}^T \nu = e^{-\delta} \tilde{w}^T (\nu - \beta) + e^{-\delta} \tilde{w}^T \beta \geq k - \| \tilde{w} \| \| \nu - \beta \|_1. \]

By Lemma 5.2, \( D(\beta||\nu) \geq \min \left\{ \frac{1}{\| \nu \|_1} \| \nu - \beta \|_1, (1 - \ln 2) \| \alpha - \beta \|_1 \right\} \). Because \( e^{-\delta} \mu \leq 1 \), we know that \( \| \nu \|_1 \leq \sum_i \nu_i n_i \leq e^{\delta} n \). Thus \( \| \nu - \beta \|_1 \leq \max \left\{ \frac{\delta^2}{(1 - \ln 2)} \sqrt{2ne^{\delta}/2} \right\} \). For \( \varepsilon \leq 1 \), the latter argument dominates. Combining the inequalities we have \( w^T x \geq e^{-\delta} (k - \| w \|_\infty \sqrt{2ne^{\delta}/2}) \geq (1 - (\sqrt{2n} + 1))k \geq (1 - \varepsilon)k \).

We next verify that \( f_{w,k} \) is monotone decreasing. For \( X \) and \( Y \) one can easily verify that each update step minimizes \( f_{w,k} \) in the corresponding variable while holding the others fixed. In fact, the \( X \) update is the same as the update in \textsc{MajSinkhorn} for \( \alpha = 1 \). For \( z \) update this follows from Lemma 7.7. It remains to check that the progress made each iteration is at least \( \delta^2/2 \) whenever the termination condition is not met. If the \( X \) variable is updated, this follows from Lemma 4.8, and if \( z \) is updated it follows from Corollary 7.8. \( \square \)

Theorem 7.9. \( \text{cap}_{w,k} B > -\infty \) if and only if \( \text{OPT} := \max \{ w^T x : x \in BL(B) \} \geq k \). Moreover, if \( B \) has Gaussian integer entries then \( \text{OPT} \geq k \) implies \( \text{cap}_{w,k} B = O(k(n + m) \log(m + n)) \).

We first prove a lemma relating \( \text{cap}_{w,k} \) to the capacity for majorization scaling.

Lemma 7.10. Suppose \( x \in \mathbb{R}_{\geq 0}^p \) is such that \( w^T x \geq k \). Then \( \text{cap}_{w,k} B \geq \text{cap}_x B \).
Proof. We have

\[
\text{cap}_{w,k} B = \inf_{(X,Y,z) \in \mathcal{D}'} \sum_{i=1}^{P} e^{w_i z / n_i} \text{Tr} B_i X^{-1} B_i^T Y_i^{-1} - k z + \log \det X
\]

\[
= \inf_{(X,Y,z) \in \mathcal{D}'} \sum_{i=1}^{P} (\text{Tr} B_i X^{-1} B_i^T (e^{w_i z / n_i} Y_i)^{-1} + x_i \log \det (e^{-w_i z / n_i} Y_i) + w_i x_i) - k z + \log \det X
\]

\[
\geq \inf_{x \geq l_n, z_i > 0} \sum_{i=1}^{P} (\text{Tr} B_i X^{-1} B_i^T Z_i^{-1} + x_i \log \det Z_i) + \log \det X.
\]

In the last inequality we used that \(w^T x \geq k\) and \(z \geq 0\).

We can now easily prove Theorem 7.9.

Proof of Theorem 7.9. For the forward direction, if \(\text{cap}_{w,k} B > -\infty\) then for any \(\varepsilon > 0\) our algorithm produces a point with \(P(B) \) with \(w^T x \geq (1 - \varepsilon) k\) by Theorem 7.6; hence \(\text{OPT} \geq k\). Now suppose that \(\text{OPT} \geq k\). Then there is a point \(x \in P(B)\) with \(w^T x \geq k\). By Theorem 7.5, \(\text{cap}_{x} B \geq -\infty\). By a similar argument to the proof of Theorem 4.16 (which we omit to avoid redundancy), if \(B\) has Gaussian integer entries then \(-\text{cap}_{x} B = O(k(n + m) \log(m + n) + k \log p) = O(k(m + n) \log(m + n))\).

Theorem 7.11. Suppose \(B\) has Gaussian integer entries of absolute value at most \(M\), that all \(n_i \in \{1, 2\}\), and that \(k \geq \|w\|_\infty\) and \(w \in \mathbb{Z}_{\geq 0}^P\). Then \(\text{WeightedSinkhorn}\) run on \(B/\sqrt{mnM}\) terminates before step

\[T = O((k(m + n) \log(m + n) + n \log M)/\varepsilon^2)\]

if \(\text{OPT} \geq k\) and outputs a feasible point \(x \in P(B)\) with \(w^T x \geq k - \varepsilon\), and does not terminate if \(\text{OPT} \leq k - \varepsilon\). As \(\text{OPT} \leq \|w\|_1\), we may find \(\text{OPT}\) to precision \(2\varepsilon\) by binary search over values of \(k\) in \(O(|\log(\|w\|_1/\varepsilon)|)\) calls to the algorithm and hence

\[O((\|w\|_1(m + n) \log(m + n) + n \log M)(m_1 n^2 + n^3 + m_2 n + m_3) \log(\|w\|_1/\varepsilon)/\varepsilon^2)\]

arithmetic operations, where \(m_1 := \sum_{i=1}^{P} n_i\), \(m_2 := \sum_{i=1}^{P} n_i^2\), and \(m_3 := \sum_{i=1}^{P} n_i^3\). If all \(n_i \leq 2\) and \(\varepsilon = 1/4k\) then the algorithm correctly computes \(\text{OPT} = \max\{w^T x : x \in P(B)\}\) in

\[O((\|w\|_1(m + n) \log(m + n) + n \log M)\|w\|_1^2 \log \|w\|_1)\]

iterations and

\[O((\|w\|_1(m + n) \log(m + n) + n \log M)(m_1 n^2 + n^3 + m_2 n + m_3)\|w\|_1^2 \log \|w\|_1)\]

arithmetic operations.

We can check if \(BL(B)\) is empty by computing the value for \(w = (n_1, \ldots, n_p)\). If \(BL(B) \neq \emptyset\), optimizing \(w^T x\) over \(BL(B)\) reduces to optimizing \(2\|w\|_1(n_1, \ldots, n_p) + w\) over \(P(B)\).
Proof. First assume $OPT \geq k$. Note that $B/\sqrt{mnM}$ has size at most 1. By the same proof as Lemma 4.17, $\cap_{w,k} B/\sqrt{mnM} \geq \cap_{w,k} B - n \log mnM$, which is $-O(k(m+n) \log(m+n)+n \log M)$ by Theorem 7.9. By Theorem 7.6, if $OPT \geq k$ WeightedSinkhorn terminates before step $T = O((k(m+n) \log(m+n)+n \log M)/\varepsilon^2) = O(k^3(m+n) \log(m+n)+k^2n \log M)$ and outputs a feasible point $x \in P(B)$ with $w^T x \geq k - \varepsilon$. If $OPT \leq k - \varepsilon$, the algorithm cannot terminate before step $T$ or else it outputs a feasible point with value $\geq k - \varepsilon$, a contradiction. The case of $n_i \leq 2$ follows by half-integrality. □

Remark 7.12. If we do not have all $n_i = 2$, the algorithm still runs in time $O((k(m+n) \log(m+n)+n \log M)/\varepsilon^2)$ - only we may need to take $\varepsilon$ exponentially small to certify $OPT \geq k$, because $OPT$ need not be half-integral. The number of arithmetic operations per step is $O(mn^2 + n^3 + \sum_i n_i^2n + \sum_i n_i^3)$.

We now give another proof of Theorem 1.2.

Another Proof of Theorem 1.2. It suffices to prove the statement for $P(B)$; the claim for $BL(B)$ follows immediately because $BL(B) = P(B) \cap \{x : \sum_i n_ix_i = n\}$.

Suppose $x \in P(B)$. Then $x$ is in the convex hull of at most $p+1$ vertices of $P(B)$, which are half-integral. By Theorem 7.5, there is a polynomial time algorithm to decide if a half-integral vector is in $P(B)$, so the $p+1$ vertices are a polynomial length certificate that $x \in P(B)$.

Next suppose $x \notin P(B)$. Then there is some subspace $V \subseteq \mathbb{C}^n$ such that $\sum_i x_i \dim \text{row } B_i \cap V > \dim V$. If we let $w_i = \dim \text{row } B_i \cap V$, then we have $OPT = \max \{w^T x' : x' \in P(B)\} < w^T x$. We can verify this in polynomial time using Theorem 7.11, so $w$ is a certificate that $x \notin P(B)$. □

Acknowledgements

CF acknowledges helpful conversations with Akshay Ramachandran and Harold Nieuwboer. The authors thank Nikhil Srivastava for references to eigendecomposition algorithms. The authors also thank Koyo Hayashi and Hiroshi Hirai for references [Aas14, GR13] and sharing a draft of [HH22].

References

[Aas14] Erik Aas. Limit points of the iterative scaling procedure. Annals of Operations Research, 215(1):15–23, 2014.

[AKRS21] Carlos Améndola, Kathlén Kohn, Philipp Reichenbach, and Anna Seigal. Invariant theory and scaling algorithms for maximum likelihood estimation. SIAM Journal on Applied Algebra and Geometry, 5(2):304–337, 2021.

[Bar98] Franck Barthe. On a reverse form of the Brascamp-Lieb inequality. Inventiones Mathematicae, 134(2):335–361, 1998.

[BCCT08] Jonathan Bennett, Anthony Carbery, Michael Christ, and Terence Tao. The Brascamp-Lieb inequalities: Finiteness, structure and extremals. Geometric and Functional Analysis, 17(5):1343–1415, 2008.
[BD06] Matthias Bürgin and Jan Draisma. The hilbert null-cone on tuples of matrices and bilinear forms. *Mathematische Zeitschrift*, 254(4):785–809, 2006.

[BFG+19] Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Oliveira, Michael Walter, and Avi Wigderson. Towards a theory of non-commutative optimization: Geodesic 1st and 2nd order methods for moment maps and polytopes. In *Proceedings of the IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 845–861. IEEE, 2019.

[BGVKS20] Jess Banks, Jorge Garza-Vargas, Archit Kulkarni, and Nikhil Srivastava. Pseudospectral shattering, the sign function, and diagonalization in nearly matrix multiplication time. In *The proceedings of the IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 529–540. IEEE, 2020.

[Bha09] Rajendra Bhatia. *Positive Definite Matrices*. Princeton university press, 2009.

[Bha13] Rajendra Bhatia. *Matrix analysis*, volume 169. Springer Science & Business Media, 2013.

[CLV01a] Shiow-yun Chang, Donna C. Llewellyn, and John H. Vande Vate. Matching 2-lattice polyhedra: finding a maximum vector. *Discrete Mathematics*, 237(1):29–61, 2001.

[CLV01b] Shiow-yun Chang, Donna C. Llewellyn, and John H. Vande Vate. Two-lattice polyhedra: duality and extreme points. *Discrete Mathematics*, 237(1):63–95, 2001.

[DM17] Harm Derksen and Visu Makam. Polynomial degree bounds for matrix semi-invariants. *Advances in Mathematics*, 310:44–63, 2017.

[FR04] Marc Fortin and Christophe Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Séminaire Lotharingien de Combinatoire*, 52:B52f, 2004.

[Fra18] Cole Franks. Operator scaling with specified marginals. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 190–203, 2018.

[FW20] Cole Franks and Michael Walter. Minimal length in an orbit closure as a semiclassical limit. *arXiv preprint arXiv:2004.14872*, 2020.

[GGOW16] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *Proceedings of the IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 109–117. IEEE, 2016.

[GGOW18] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. Algorithmic and optimization aspects of Brascamp–Lieb inequalities, via operator scaling. *Geometric and Functional Analysis*, 28(1):100–145, 2018.

[GGOW19] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. Operator scaling: Theory and applications. *Foundations of Computational Mathematics*, 20:223–290, 2019.
[GLS12] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2. Springer Science & Business Media, 2012.

[GP13] Dion Gijswijt and Gyula Pap. An algorithm for weighted fractional matroid matching. *Journal of Combinatorial Theory, Series B*, 103(4):509–520, 2013.

[GR13] Christoph Gietl and Fabian P. Reffel. Accumulation points of the iterative proportional fitting procedure. *Metrika*, 76(6):783–798, 2013.

[Gur04] Leonid Gurvits. Classical complexity and quantum entanglement. *Journal of Computer and System Sciences*, 69(3):448–484, 2004.

[HH21] Masaki Hamada and Hiroshi Hirai. Computing the nc-rank via discrete convex optimization on CAT(0) spaces. *SIAM Journal on Applied Algebra and Geometry*, 5(3):455–478, 2021.

[HH22] Koyo Hayashi and Hiroshi Hirai. Finding hall blockers by matrix scaling. *arXiv preprint arXiv:2204.07425*, 2022.

[Ide16] Martin Idel. A review of matrix scaling and Sinkhorn’s normal form for matrices and positive maps. *arXiv preprint arXiv:1609.06349v1*, 2016.

[IKQS15] Gábor Ivanyos, Marek Karpinski, Youming Qiao, and Miklos Santha. Generalized Wong sequences and their applications to Edmonds’ problems. *Journal of Computer and System Sciences*, 81(7):1373–1386, 2015.

[IQS17] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative Edmonds’ problem and matrix semi-invariants. *Computational Complexity*, 26(3):717–763, 2017.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Computational Complexity*, 27(4):561–593, 2018.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1):1–46, 2004.

[Kin94] Alastair D. King. Moduli of representations of finite dimensional algebras. *The Quarterly Journal of Mathematics*, 45(4):515–530, 1994.

[LSV18] Yin Tat Lee, Aaron Sidford, and Santosh S Vempala. Efficient convex optimization with membership oracles. In *Proceedings of the 31st Conference On Learning Theory (COLT)*, pages 1292–1294. PMLR, 2018.

[LW16] Cong Han Lim and Stephen J. Wright. Efficient bregman projections onto the permutohedron and related polytopes. In *Proceedings of the 19th International Conference on Artificial Intelligence and Statistics (AISTATS)*, volume 51, pages 1205–1213, 2016.

[Mah64] Kurt Mahler. An inequality for the discriminant of a polynomial. *Michigan Mathematical Journal*, 11(3):257–262, 1964.
[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric Invariant Theory*, volume 34. Springer Science & Business Media, 1994.

[MS22] Takeru Matsuda and Tasuku Soma. Information geometry of operator scaling. *Linear Algebra and its Applications*, 649:240–267, 2022.

[Mur09] Kazuo Murota. *Matrices and Matroids for System Analysis*. Springer-Verlag, Berlin, 2nd edition, 2009.

[OS22] Taihei Oki and Tasuku Soma. Algebraic algorithms for fractional linear matroid parity via non-commutative rank. *arxiv*, 2022.

[Par98] Beresford N. Parlett. *The symmetric eigenvalue problem*. SIAM, 1998.

[SHK+12] Daiki Suehiro, Kohei Hatano, Shuji Kijima, Eiji Takimoto, and Kiyohito Nagano. Online prediction under submodular constraints. In *Proceedings of the 23rd International Conference on Algorithmic Learning Theory (ALT)*, pages 260–274, 2012.

[Sin64] Richard Sinkhorn. A relationship between arbitrary positive matrices and doubly stochastic matrices. *The Annals of Mathematical Statistics*, 35(2):876–879, 1964.

[vAGL+20] Joran van Apeldoorn, Sander Gribling, Yinan Li, Harold Nieuwboer, Michael Walter, and Ronald de Wolf. Quantum algorithms for matrix scaling and matrix balancing. *arXiv preprint arXiv:2011.12823*, 2020.

[Val79] Leslie G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.

[Van92] John H. Vande Vate. Fractional matroid matchings. *Journal of Combinatorial Theory, Series B*, 55(1):133–145, 1992.
A Bit complexity of linear algebra operations

A.1 Models of computations

We need two models of computations of rational numbers, which we formalize below.

**Rational Arithmetic.** A rational number $r$ is represented as $r = p/q$, where $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$. This model of arithmetic is suitable to represent rational numbers exactly such as results of Gaussian elimination and Gram-Schmidt orthogonalization. A caveat of this model is that careless implementation of an algorithm may explode the bit length to represent integers $p, q$, even if it makes only polynomially many arithmetic operations.

**Finite Precision Arithmetic.** A rational number $r$ is rounded to a fixed length of bits, where the length may depend on the size of the problem and desired accuracy. We call the length of bits the *precision*. This model of arithmetic is more suitable to numerical computations such as eigendecompositions.

A.2 Gaussian elimination and pseudoinverse

The following is a well-known theorem for Gaussian elimination.

**Theorem A.1 ([GLS12]).** For $A \in \mathbb{Q}[\sqrt{-1}]^{n \times n}$, the Gaussian elimination algorithm runs in $O(n^3)$ arithmetic operations. If $A$ have Gaussian integer entries with magnitude at most $M$, the output as well as intermediate numbers are rationals with numerator and denominator at most $e^{O(n \log(nM))}$.

A nonsingular matrix $A^+$ is called a *pseudoinverse* of $A$ if $A^+A$ is the identity map restricted on $\text{Im}(A)$. It is easy to construct $A^+$ by the result of Gaussian elimination. More specifically, let $A = P \left[ \begin{array}{cc} I_r & O_{r,n-r} \\ O_{n-r,r} & O_{n-r,n-r} \end{array} \right] Q^{-1}$ be a rank normal form obtained by Gaussian elimination, where $P,Q$ are nonsingular and $r = \text{rank}(A)$. The first $r$ columns of $Q$ spans $\text{Im}(A)$. We can see that $QP^{-1}$ is a pseudoinverse of $A$.

A.3 Gram-Schmidt orthogonalization

Given an ordered basis $(a_1, \ldots, a_n) \subseteq \mathbb{Q}[\sqrt{-1}]^m$ of a subspace $U$, the Gram-Schmidt orthogonalization computes orthogonal ordered basis $(b_1, \ldots, b_n)$ of $U$. The Gram-Schmidt algorithm can be carried out in the same time and bit complexity as Gaussian elimination [GLS12].

Once we compute $(b_1, \ldots, b_n)$, the orthogonal projection onto $U$ is given by $\pi_U = \sum_{i=1}^n \frac{b_i b_i^\dagger}{\|b_i\|^2}$. The orthogonal projection onto $U^\perp$ is simply $I - \pi_U$.

**Theorem A.2.** Given a basis $a_1, \ldots, a_n \in \mathbb{Q}[\sqrt{-1}]^m$ of a subspace $U$, the orthogonal projections onto $U$ and its orthogonal complements can be found in $O(mn^2)$ arithmetic operations. If $a_1, \ldots, a_n$ have Gaussian integer entries with magnitude at most $M$, the output as well as intermediate numbers are rationals with numerator and denominator at most $e^{O(m \log(mM))}$. 


A.4 Eigendecomposition of Hermitian matrices

Given a Hermitian matrix $A \in \mathbb{Q}[\sqrt{-1}]^{n \times n}$, we are to find all pairs of eigenvalues and eigenvectors. Since eigenvalues can be irrational, the best we can hope for is to approximate them in desired accuracy. The following result is essentially achieved by the QR algorithm with Wilkinson’s shift and the standard $O(n^3)$-time matrix multiplication. For more recent improvements, see [BGVKS20] and references therein.

**Theorem A.3 ([Par98]).** Let $A \in \mathbb{Q}[\sqrt{-1}]^{n \times n}$ be a Hermitian matrix with distinct eigenvalues $\lambda_i$ and (normalized) eigenvector $v_i$ ($i = 1, \ldots, n$).

There exists an algorithm that for $\delta > 0$, outputs pairs $(\hat{\lambda}_i, \hat{v}_i)$ such that

$$|\lambda_i - \hat{\lambda}_i| \leq \delta \|A\|, \quad \|v_i - \hat{v}_i\| \leq \delta \|A\|,$$

by making $O(n^3 + n^2 \log(1/\delta))$ arithmetic operations with $O(\log(n/\delta))$ precision.

**Remark A.4.** If $A$ has a repeated eigenvalue, the above definition of the approximation of eigenvectors must be replaced with the approximation of eigenspaces. The QR algorithm can also find an approximate eigenspace $\tilde{V}$ close to a true eigenspace $V$ with respect to the principal angle distance. More precisely, $\|\pi_\tilde{V} - \pi_V\| \leq O(\kappa_A \delta \|A\|)$, where $\kappa_A$ is the condition number of eigenspaces, i.e., the minimum gap of distinct eigenvalues. If $A$ has Gaussian integer entries with magnitude at most $M$, we have $\kappa_A = e^{-O(n \log M + n \log n)}$ [Mah64]. So this only adds an additional $O(n \log M + n \log n)$ factor to the precision. For simplicity, we assume that matrices have distinct eigenvalues in the following argument.

B Finite precision algorithms

So far we have assumed exact arithmetic for computing each iterate in MAJSINKHORN (our main algorithmic primitive in this work; Algorithm 2). In order to obtain a polynomial time algorithm in the Turing model, we need to show that we can round the numbers in each iterate to finite precision. Morally this should be possible because we are optimizing a (geodesically) convex function, but making the argument rigorous still requires some work.

Algorithm 9 (MAJSINKHORNFinite) is the finite precision version of MAJSINKHORN. Note that we must represent the eigendecomposition of a matrix implicitly, because diagonalizing unitaries of rational matrices are hardly ever rational.

Next we argue that this algorithm has the same time complexity and guarantees as MAJSINKHORN. First we argue that, for sufficient precision, the finite precision steps still make at least half the progress that the infinite precision steps make. Next we argue that MAJSINKHORN only ever results in $\|X\|_2, \|Y\|_2, e^{\epsilon} \leq e^{O(T)}$, and that this remains true even with the finite precision steps. Finally, we show that these radius bounds imply that each step of the finite precision algorithm can be performed in polynomial time with polynomial bit complexity.

**Theorem B.1** (Finite precision progress bound). Suppose $\delta \leq \min\{\alpha_1, \beta_1\} \frac{\epsilon^2}{8}$. Then the amount of progress made by the $X$ or $Y$ update in MAJSINKHORNFinite is at least half the progress made by the corresponding step in MAJSINKHORN. If $\delta q \leq \frac{\epsilon^2}{8}$, where $q$ the updated value, the $q$ update decreases the function value by at least half as much as the infinite precision $\epsilon$ update.
Proof. Consider the $X$ update; the $Y$ update is analogous. The infinite precision version would set $X = \arg\min_{X \in \mathcal{F}}(f_C(X) = \text{Tr} X^{-1} C + \alpha \cdot \lambda (\log X))$. In the finite precision version we rather set $X$ to a minimizer of $f_{\tilde{C}}$ where we have chosen $\tilde{C}$ such that $\|C - \tilde{C}\|_1 \leq \delta$. Note that $|f_{\tilde{C}}(X) - f_C(X)| \leq \delta$ for $X \succeq I_n$. Therefore the optimal value $\text{OPT}$ and $\text{OPT}_f$ of $f_C$ and $f_{\tilde{C}}$ are within $\delta$ of one another and if $X$ is an optimizer of $f_{\tilde{C}}$ we have $f_{\tilde{C}}(X) \leq \text{OPT} + 2\delta$.

In the $q$ update we choose $q \geq 1$ to minimize $\tilde{a}q - k\log q$, but the new function value becomes $\tilde{a}q - k\log q$ where $a = \text{Tr} \Phi(X^{-1})Y^{-1}$.

We now show why the intermediate numbers in each step are only polynomial bit complexity and can be computed in polynomial time. In order to ensure at least half the progress is made, the most
onerous requirement is in the $z$ update. For this we need to take $\delta \leq \varepsilon^2/8q$, but by Theorem B.3 we have $q \leq 3(3S)^T$ which is merely exponential. Therefore it suffices to take $\delta$ inverse exponential in the input size and $\log(1/\varepsilon)$.

We begin with the $X$ update. Given an implicit representation of $Y$ as $(y, B)$ and $e^z \in \mathbb{Q}$, we need to compute $e^z\Phi^*(Y)$ to precision $\delta$ in the trace norm. Let $B = V \text{diag}(b)V^\dagger$. By the particular choice of $B$ ($\Phi(X)e^z$ for the previous $X$), any choice of $V$ diagonalizing $B$ will give rise to $Y$ with the same function value. Therefore it suffices to find a $\tilde{V}$ which is $\delta$-close to some $V$ diagonalizing $B$ and set $\hat{C} = e^z\Phi^*(\tilde{V}\text{diag}(r)\tilde{V}^\dagger)$ for $e^y \approx r \in \mathbb{Q}^m$. Standard eigendecomposition algorithms output $\tilde{V}$ deterministically with $\text{poly}(m, \log 1/\delta, \log \|B\|_2)$ bits in time $\text{poly}(m, \log 1/\delta, \log \|B\|_2)$ (Theorem A.3). We know that $\|B\|_2 \leq M\sqrt{mnp(3S)^T}$ by Theorem B.3, so this takes polynomial time. The $Y$ update is analogous, and the $z$ update is trivial. Approximating $\varepsilon_X, \varepsilon_Y, \varepsilon_q$ is similar. This concludes the argument.

**Calling MajSinkhornFinite as a subroutine**

As MajSinkhornFinite with appropriate $\delta$ makes at least half the progress of MajSinkhorn in every step, it only needs to be run for twice as many iterations. Therefore we can use MajSinkhornFinite as a replacement for MajSinkhorn in all the algorithms in this paper.

The only algorithm that requires further discussion is ApproximateIndep. We are given $X$ and $Y$ implicitly as $(x, A), (y, B)$. We need to check if some pairs $R = \langle u_1, \ldots, u_i \rangle, L = \langle v_1, \ldots, v_j \rangle$ are $\varepsilon$-shrunk subspaces for $\varepsilon$ inverse exponential, where $u_i, v_j$ are some eigenbases of $A, B$ in order of decreasing eigenvalue. We merely need to compute approximations $\tilde{u}_i \approx \delta u_i, \tilde{v}_j \approx \delta v_j$ for some such eigenbases, which again is possible in polynomial time by standard eigendecomposition algorithms (Theorem A.3). Taking $\delta$ inverse exponential will suffice because $\text{Tr} \cdot \Phi(\pi_R)\pi_L$ is sufficiently Lipschitz in $R$ and $L$. 

61
Algorithm MajSinkhornFinite($\Phi, \alpha, \beta, \varepsilon$):

**Input:** A CP map $\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m}$ with Kraus operators in $\mathbb{Q}[\sqrt{-1}]^{m \times n}$, non-increasing vectors $\alpha \in \mathbb{Q}^n, \beta \in \mathbb{Q}^m$, and a parameter $\varepsilon > 0$.

**Output:** $X, Y, q$ such that the scaling $q\Phi_{X^{-1/2}, Y^{-1/2}}$ that is $(\alpha, \beta)$-majorized and has size at least $(1 - \varepsilon)^2 k$.

**Algorithm:**

1. Set $X = I_n, Y = I_m, q = 1$. Implicitly represent $X$ with the pair $x \in \mathbb{Q}^n, 0 \preceq A \in \mathbb{Q}[\sqrt{-1}]^{n \times n}$, where $X = U \text{diag}(x) U^*$ for $U$ diagonalizing $A$. Represent $Y$ with $(y, B)$ analogously.

2. For $t \in \{0, ..., T\}$:
   
   1. Using the implicit representations of $X$ and $Y$, compute rational vectors $\mu \approx_{\delta} \lambda(qX^{-1}\Phi^*(Y^{-1}))$ and $\nu \approx_{\delta} \lambda(qY^{-1}\Phi(X^{-1}))$. Using KLPProject, compute the divergences $\varepsilon_X := D(P_\alpha||\mu)$ and $\varepsilon_Y := D(P_\beta||\nu)$, where $P_\alpha$ and $P_\beta$ are the down-closure of the permutahedron of $\alpha$ and $\beta$, respectively. Compute also $\varepsilon_q \approx_{\delta} qa - k \log q$ where $a = \text{Tr} \Phi(X^{-1})Y^{-1}$.
   
   2. If: $\varepsilon_X, \varepsilon_Y, \varepsilon_q \leq \min\{\alpha_1, \beta_1\} \frac{\varepsilon^2}{2}$, **Output:** $X, Y, (1 - \varepsilon)q$.

   Else: Update either $X, Y$ or $q$ depending on which of $\varepsilon_X, \varepsilon_Y, \varepsilon_q$ is largest:
   
   (a) $X$ update:
   
   i. Using the implicit representation $(y, B)$ of $Y$, compute $0 \preceq \tilde{C} \in \mathbb{Q}^{n \times n}$ such that $\tilde{C} \approx_{\delta} C := e^x \Phi^*(Y^{-1})$ in the trace norm. Compute $\lambda \in \mathbb{Q}^n$ diagonal such that $U \text{diag}(\lambda) U^* \approx_{\delta} \tilde{C}$ in the trace norm, where $U$ diagonalizes $\tilde{C}$.
   
   ii. Compute $x \in \mathbb{Q}^n$ to be a minimizer of $x^{-1} \cdot \lambda + \alpha \cdot (\log x^\downarrow)$ subject to $x \geq 1$ using KLPProject.
   
   iii. Return $X$ represented implicitly as $(x, \tilde{C})$, and set $\tilde{a} = (\lambda \cdot x^{-1})/q$ for use in the next $z$ update.
   
   (b) $Y$ update: analogous to $X$.
   
   (c) $q$ update: take $\tilde{a}$ computed in the $X$ or $Y$ update (or $\tilde{a} = \text{Tr} \Phi(I_n)$ if this is the first step). If $\tilde{a} \geq k$, set $q = e^z = 1$. Else set $q = e^z = k/\tilde{a}$.

**Algorithm 9:** Finite precision algorithm for majorization scaling.