Pipage Rounding, Pessimistic Estimators and Matrix Concentration

Nicholas J. A. Harvey* Neil Olver†

Abstract

Pipage rounding is a dependent random sampling technique that has several interesting properties and diverse applications. One property that has been useful in applications is negative correlation of the resulting vector. There are some further properties that would be interesting to derive, but do not seem to follow from negative correlation. In particular, recent concentration results for sums of independent random matrices are not known to extend to a negatively dependent setting.

We introduce a simple but useful technique called *concavity of pessimistic estimators*. This technique allows us to show concentration of submodular functions and concentration of matrix sums under pipage rounding. The former result answers a question of Chekuri et al. (2009). To prove the latter result, we derive a new variant of Lieb's celebrated concavity theorem in matrix analysis.

We provide numerous applications of these results. One is to *spectrally-thin trees*, a spectral analog of the *thin trees* that played a crucial role in the recent breakthrough on the asymmetric traveling salesman problem. We show a polynomial time algorithm that, given a graph where every edge has effective conductance at least κ, returns an $O(\kappa^{-1} \cdot \log n / \log \log n)$-spectrally-thin tree. There are further applications to rounding of semidefinite programs and to a geometric question of extracting a nearly-orthonormal basis from an isotropic distribution.

1 Introduction

Rounding is a crucial step in the design of many approximation algorithms. Given a fractional vector satisfying some constraints, a rounding method produces an integer vector that satisfies those constraints, either exactly or approximately. *Randomized rounding* [38] [54, Chapter 5], in which the coordinates of the fractional vector are rounded randomly and independently, produces good integer vectors for many applications. *Dependent rounding* methods, in which the resulting integer vector does not have independent coordinates, are important in many scenarios where naive randomized rounding does poorly. Various techniques exist for designing dependent rounding methods (see, e.g., the surveys [45, 4]).

It is common for a rounding scenario to involve two types of constraints: hard constraints, which must be satisfied exactly by the integer solution, and soft constraints, which must be approximately satisfied by the integer solution. Low-congestion multi-path routing [46], max cut with given sizes of parts [1], thin spanning trees [3], and submodular maximization under a matroid constraint [14, 18] are examples of problems whose solutions involve such a rounding scenario. The hard constraint is often membership in an integer polytope that is defined using combinatorial objects (e.g., matchings or matroids). The soft constraints are usually simple linear inequalities.

With randomized rounding, the independent choices lead to concentration phenomena that are useful for handling soft constraints. For example, Chernoff bounds are commonly used to show that linear inequalities are approximately satisfied [38]. The past decade has seen various uses of *matrix* concentration bounds (e.g., [2, 41, 49]) to show that linear matrix inequalities are approximately satisfied by random sampling or rounding. Such uses have arisen in many areas: graph sparsification [43], compressed sensing [51], statistics [19], machine learning [39] and numerical linear algebra [31].

With dependent rounding, concentration phenomena can also occur. *Pipage rounding*, *swap rounding* and *maximum entropy sampling* are dependent rounding techniques that have seen many important uses over the past decade [46, 1, 23, 14, 3, 18]. An important feature in some scenarios is that any Chernoff bound that is valid under independent randomized rounding remains valid under these dependent rounding techniques. This fact is proven by showing that the rounded solution has a *negatively correlated distribution*, then appealing to

*Department of Computer Science, UBC, Vancouver, Canada. Email: nickhar@cs.ubc.ca. Supported by an NSERC Discovery Grant and a Sloan Foundation Fellowship.

†Work done while at the Department of Mathematics, MIT. Current affiliation: Department of Econometrics & Operations Research, VU Amsterdam, The Netherlands; and CWI, The Netherlands. Email: n.olver@vu.nl. Supported by NSF grant CCF-1115849.

the fact that Chernoff bounds remain valid under such distributions [36]. Unfortunately, commutativity plays a key role in proving that fact, and these arguments do not seem to extend to known matrix concentration bounds [2, 34, 41, 49]. Consequently, these matrix inequalities have so far not been combined with dependent rounding.

We prove the first result showing that matrix concentration bounds are usable in a dependent rounding scenario. Our technique is not based on negative correlation, but rather the fortuitous interaction between pipage rounding and various pessimistic estimators. In particular, we show that Tropp's matrix Chernoff bound [49] has a pessimistic estimator that decreases monotonically under pipage rounding. As a consequence, we can extend the reach of pipage rounding from soft constraints that are linear inequalities to soft constraints that are linear matrix inequalities. Our proof uses nontrivial techniques from matrix analysis and complex analysis; in particular, we prove a new variant of Lieb's concavity theorem.

1.1 Motivation and Results. One key area where our techniques yield new results is for *thin spanning trees*. These are intriguing objects in graph theory that relate to foundational topics, such as nowhere-zero flows [25], and the asymmetric traveling salesman problem [3]. Given a graph G on n nodes, a spanning tree T of G is *α-thin* if, for every cut, the number of edges of T crossing the cut is at most α times the number of edges of G crossing the cut. It has been conjectured that any graph with connectivity k has an $f(k)$-thin spanning tree where $f(k) = O(1/k)$. This would imply a constant factor approximation algorithm for the asymmetric traveling salesman problem [35]. Asadpour et al. [3] give a randomized algorithm to find a spanning tree that is $O(\frac{\log n}{k \log\log n})$-thin. Later Chekuri et al. [17, 18] gave a simpler algorithm using randomized pipage rounding or swap rounding.

A *spectrally-thin* spanning tree is a stronger notion that is naturally motivated by work on spectral sparsification [43, 5]. A spanning tree T is α-spectrally-thin if $L_T \preceq \alpha L_G$, where L_G refers to the Laplacian of G, and $\preceq$ to the Löwner ordering of Hermitian matrices. In Section 4.3, we show a result on spectrally thin trees that strongly mirrors the result of Asadpour et al.

Theorem 1.1. *There is a deterministic, polynomial-time algorithm that given any graph on n nodes where every edge has effective conductance at least κ, constructs a $O(\frac{\log n}{\kappa \log\log n})$-spectrally-thin spanning subtree.*

Our definition of spectral-thinness seems increasingly relevant due to the recent breakthrough of Marcus et al. [32], which implies that $O(1/\kappa)$-spectrally-thin trees exist. Details of this connection are given in Appendix E. It is unknown if similar techniques can show that $O(1/k)$-thin trees exist. The best known algorithmic construction of spectrally-thin trees is still Theorem 1.1.

This result is a special case of a result in a more abstract geometric setting. Suppose $V = \{v_1, \ldots, v_m\}$ are unit vectors in ℓ_2^n for which $\sum_{i=1}^m v_i v_i^\mathsf{T}$ is a multiple of the identity. Does there exist a subset $V_B = \{\, v_i : i \in B \,\}$ that is a *basis* of $\mathbb{R}^n$ and for which the maximum eigenvalue of $\sum_{i\in B} v_i v_i^\mathsf{T}$ is small? The maximum eigenvalue is 1 if and only if V_B is orthonormal, but an arbitrary V need not contain an orthonormal basis. Again, the breakthrough of Marcus et al. [32] yields a non-constructive proof of a basis with maximum eigenvalue $O(1)$; see Appendix E. In Section 4.2, we show how to find in polynomial time a basis $V_B \subseteq V$ for which the maximum eigenvalue of $\sum_{i\in B} v_i v_i^\mathsf{T}$ is $O(\log n/\log\log n)$, whereas previous constructive techniques [2, 34, 41, 49] only provide a bound of $O(\log n)$.

1.2 Techniques. Our results are based on the pipage rounding technique [1, 46, 23, 14], which has had several interesting uses in the recent literature. Our result applies to both the deterministic and randomized forms of pipage rounding, as well as to swap rounding.

We now give a brief overview of pipage rounding; further discussion is in Section 3.1.

- Given any point in a matroid base polytope, pipage rounding produces a sequence of new points within the polytope. Each new point is chosen to lie on a lower-dimensional face than the previous one, ensuring convergence to an extreme point. To get from one point to the next, only two coordinates are modified: one is increased, and the other is decreased by the same amount. The existence of such a sequence of points is a consequence of the basis exchange properties of matroids.
- One approach to ensure useful properties of the final extreme point is to define a potential function that is concave (resp., convex) in directions that increase one coordinate and decrease another by the same amount. Deterministic pipage rounding ensures that each new point does not increase (resp., decrease) the value of this function, whereas randomized pipage rounding ensures this only in expectation. Examples of such functions include the ad hoc functions used in [1], or the multilinear extension of a submodular function [14].
- Randomized pipage rounding [46, 23, 18] outputs an extreme point whose coordinates are negatively

correlated (more precisely, negative cylinder dependent). This, together with existing theorems, implies that linear functions of that point satisfy the same Chernoff-type concentration bounds that are satisfied under independent rounding.

The goal of this paper is to show that, for various concentration bounds, the extreme point produced by pipage rounding satisfies the same bounds that would be achieved by independent randomized rounding. For Chernoff bounds this follows from negative correlation, but for other bounds such a result was not previously known.

- Let f be a monotone submodular function defined on the ground set of the matroid. When using randomized pipage rounding, does the value of f at the final extreme point satisfy the same lower tail bound as when using independent rounding? Chekuri et al. [17] conjectured this to be true, and they proved such a result when using swap rounding.
- Let f be a linear function mapping points in the matroid base polytope to symmetric matrices. When using pipage rounding, can the value of f at the final extreme point be guaranteed to satisfy the same eigenvalue bounds as when using independent rounding?

It does not seem easy to answer these questions using negative correlation properties. We present a new approach that leads to a positive answer to both of these questions.

Our approach is based on pessimistic estimators [37], which we now briefly define; a more detailed discussion is in Section 3.2. Given a distribution and an event $\mathcal{E}$ on the Boolean cube, a pessimistic estimator is an upper bound on the probability of $\mathcal{E}$ that satisfies some additional properties. The key property is that one can repeatedly condition on coordinates being either zero or one, without increasing the estimator. For both of the aforementioned questions, we will define a pessimistic estimator for the event that independent randomized rounding fails to achieve the desired concentration. We then show that these pessimistic estimators are concave when one element's sampling probability is increased and another's is decreased by the same amount. Due to that concavity property, the base output by randomized pipage rounding satisfies the same concentration bounds that would be satisfied under independent randomized rounding. For the second question (matrix concentration), the pessimistic estimator can be efficiently evaluated, so deterministic pipage rounding can also be used.

The concavity property of our pessimistic estimator for matrix concentration is a non-trivial fact. We establish that fact by proving a new variant of Lieb's concavity theorem [30]. Although there is much interest in the mathematical physics community on extensions and variants of Lieb's theorem, our particular variant does not seem to appear in the literature.

2 Preliminaries

Let $[m] = \{1, \ldots, m\}$. For a set $S \subseteq [m]$, the vector $\chi(S) \in \mathbb{R}^m$ is the characteristic vector of S. For a vector $x \in \mathbb{R}^m$ and a set $S \subseteq [m]$, the notation $x(S)$ denotes $\sum_{i \in S} x_i$. The vector e_i denotes the i^{th} standard basis vector of the finite dimensional vector space that is apparent from context. The vector $\vec{1}$ denotes a vector whose components are all ones and whose dimension is apparent from context. We will use $\mathbb{R}_+$ and $\mathbb{Z}_+$ to denote the nonnegative and positive reals respectively.

Let $\mathbb{S}^n$ denote the space of symmetric, real matrices of size $n \times n$. Let $\mathbb{S}^n_+, \mathbb{S}^n_{++} \subset \mathbb{S}^n$ respectively denote the cones of positive semidefinite and positive definite matrices. Let $\mathbb{D}^n \subseteq \mathbb{S}^n$ denote the space of $n \times n$ diagonal matrices. Let $\preceq$ denote the Löwner partial order on symmetric matrices, i.e., $A \preceq B$ iff $B - A \in \mathbb{S}^n_+$. Similarly, $A \prec B$ iff $B - A \in \mathbb{S}^n_{++}$. For $A \in \mathbb{S}^n$, let $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ respectively denote the largest and smallest eigenvalues of A. For $B \in \mathbb{S}^n$, let B^+ denote its Moore-Penrose pseudoinverse. For $B \in \mathbb{S}^n_+$, let $B^{+/2} \in \mathbb{S}^n_+$ denote the positive semidefinite square root of B^+. The image of B is $\operatorname{im} B$ and the orthogonal projection onto $\operatorname{im} B$ is $I_{\operatorname{im} B}$.

The notation $\|\cdot\|$ denotes the ℓ_2 norm for vectors and the ℓ_2 operator norm for matrices.

If $\mathcal{D}$ is a distribution, $X \sim \mathcal{D}$ means that the random variable X has distribution $\mathcal{D}$.

3 Concavity of Pessimistic Estimators

In this section we state the known results on pipage rounding, then state our concavity of pessimistic estimators technique. We then apply this technique in three scenarios: (1) Chernoff bounds, (2) submodular functions, and (3) matrix concentration. The latter two results are new, and in particular are not known to follow using negative correlation. This pessimistic estimator for matrix concentration underlies all applications in Section 4.

3.1 Pipage Rounding. Pipage rounding is a dependent rounding process originating in works of Ageev, Srinivasan and Sviridenko [1, 46]. Calinescu et al. [14] generalized it to a matroid setting. We now state the main results of randomized and deterministic pipage rounding.

Let $\mathbf{M}$ be a matroid on $[m]$ and let $P \subset \mathbb{R}^m$ be its base polytope. For all algorithmic applications in this paper, $\mathbf{M}$ can be presented to the algorithm via an independence oracle. A function $g : P \to \mathbb{R}$ is said to be *concave under swaps* if

(3.1)
$$\forall p \in P,\ \forall a, b \in [m], \quad z \mapsto g\big(p + z(e_a - e_b)\big) \text{ is concave.}$$

Theorem 3.1. (Ageev et al. [1, 46, 14])

(i) Randomized Pipage Rounding. *There is a randomized, polynomial-time algorithm that, given $x \in P$, outputs an extreme point $\hat{x}$ of P with $\mathbb{E}[\,\hat{x}\,] = x$ and such that, for any g concave under swaps, $\mathbb{E}[\,g(\hat{x})\,] \leq g(x)$.*

(ii) Deterministic Pipage Rounding. *There is a deterministic, polynomial-time algorithm that, given $x \in P$ and a value oracle for a function g that is concave under swaps, outputs an extreme point $\hat{x}$ of P with $g(\hat{x}) \leq g(x)$.*

Proof. Let p be a point in the matroid polytope P and assume that g satisfies (3.1). Delete all coordinates of p that are equal to zero and consider the residual problem. It is well-known that, for any such point p, there exists a chain of sets $\emptyset = C_0 \subseteq C_1 \subseteq \cdots C_k \subseteq [m]$ whose corresponding constraints of P span the constraints that are tight at p. If $|C_i \setminus C_{i-1}| = 1$ for every i then these give m linearly independent tight constraints, so the point p is an extreme point. Otherwise there is some set C_i, $i \geq 1$, for which $|C_i \setminus C_{i-1}| > 1$. In this case p is not an extreme point. To see this, let a and b be distinct elements of $C_i \setminus C_{i-1}$. Note that the point $p + z(e_a - e_b)$ satisfies all the constraints that are tight at p. So, for all z in some open neighborhood of 0, the point $p + z(e_a - e_b)$ is still feasible for P.

Define

$$\begin{aligned} &\ell = \min\{\, z \in \mathbb{R} \,:\, p + z(e_a - e_b) \in P \,\} \\ \text{and} \quad &u = \max\{\, z \in \mathbb{R} \,:\, p + z(e_a - e_b) \in P \,\}. \end{aligned}$$

Define

$$p^\ell = p + \ell(e_a - e_b) \qquad \text{and} \qquad p^u = p + u(e_a - e_b).$$

Since $g\big(p + z(e_a - e_b)\big)$ is concave, we must have either

$$g\big(p^\ell\big) \leq g(p) \qquad \text{or} \qquad g\big(p^u\big) \leq g(p).$$

Furthermore, both p^ℓ and p^u lie on a lower-dimensional face than p does. So starting from some initial $p^0 \in P$, m iterations suffice to find an extreme point $\hat{p}$ of P with $g(\hat{p}) \leq g(p^0)$.

The randomized version of pipage rounding does not even need access to the function g. Instead, it simply chooses the next point p' to be p^ℓ with probability $\frac{u}{u-\ell}$, or p^u with probability $\frac{-\ell}{u-\ell}$. This ensures that $\mathbb{E}[\,p'\,] = p$, and the concavity of g yields $\mathbb{E}[\,g(p')\,] \leq g(p)$ by Jensen's inequality. Apply this procedure to some initial point $p_0 \in P$ until an extreme point $\hat{p}$ is obtained. Then $\hat{p}$ satisfies $\mathbb{E}[\,\hat{p}\,] = p_0$ and $\mathbb{E}[\,g(\hat{p})\,] \leq g(p^0)$. ☐

The swap rounding procedure of Chekuri et al. [17, 18] also proves Theorem 3.1.

3.2 Pessimistic estimators. For $x \in [0,1]^m$, let $\mathcal{D}(x)$ be the product distribution on $\{0,1\}^m$ with marginals given by x, i.e., $\mathbb{P}_{X \sim \mathcal{D}(x)}[\,X_i = 1\,] = x_i$. Let $\mathcal{E} \subseteq \{0,1\}^m$. A *pessimistic estimator* [37, 47] for $\mathcal{E}$ is a function $g : [0,1]^m \to \mathbb{R}$ that satisfies

$$\begin{aligned} \text{(3.2)} \qquad \mathbb{P}_{X \sim \mathcal{D}(x)}[\,X \in \mathcal{E}\,] \ &\leq\ g(x) \qquad \forall x \in [0,1]^m \\ \min\{g(x - x_i e_i), g(x + (1 - x_i)e_i)\}& \\ &\leq\ g(x) \quad \forall x \in [0,1]^m, i \in [m]. \end{aligned}$$

For uses of pessimistic estimators in derandomization, the function g is also required to be efficiently computable. Given any point $x^0 \in [0,1]^m$, the method of conditional expectations can then be used to efficiently find $\hat{x} \in \{0,1\}^m$ with $g(\hat{x}) \leq g(x^0)$. In randomized pipage rounding g need not be efficiently computable as g is not even provided as input to the algorithm.

Claim 3.2. (Concavity of Pessimistic Estimators) *Let $\mathcal{E} \subseteq \{0,1\}^m$. Let g be a function that satisfies inequality (3.2) and is concave under swaps.*

Suppose randomized pipage rounding is started at an initial point $x_0 \in P$, and let $\hat{x}$ be the (random) extreme point of P that is output. If $g(x_0) \leq \epsilon$ then $\mathbb{P}[\,\hat{x} \in \mathcal{E}\,] \leq \epsilon$.

Suppose deterministic pipage rounding is given oracle access to g and an initial point $x_0 \in P$ with $g(x_0) < 1$. Then the extreme point $\hat{x}$ of P that is output satisfies $\hat{x} \notin \mathcal{E}$.

We omit the proof of Claim 3.2 as it is an easy consequence of Theorem 3.1.

3.3 Chernoff bound. Let us start with a simple result to illustrate the technique. First we state the Chernoff bound in convenient notation. We discuss only the right tail; an analogous result holds for the left tail. Fix any vector $w \in [0,1]^m$. For $t \in \mathbb{R}$ and $\theta > 0$, define $g_{t,\theta} : [0,1]^m \to \mathbb{R}$ by

$$g_{t,\theta}(x) \ :=\ e^{-\theta t} \cdot \mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, e^{\theta w^\mathsf{T} X} \,\right].$$

Let $\mu = w^{\mathsf{T}} x$ and $\delta \geq 0$. Then

$$\mathbb{P}_{X \sim \mathcal{D}(x)}\left[\, w^{\mathsf{T}} X \geq t \,\right] \;\leq\; \inf_{\theta>0}\, g_{t,\theta}(x)$$

$$\text{and} \quad g_{(1+\delta)\mu,\, \ln(1+\delta)}(x) \;\leq\; \Big(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\Big)^{\mu}. \tag{3.3}$$

CLAIM 3.3. *$g_{t,\theta}$ is concave under swaps.*

Proof. We can rewrite

$$g(x) \;=\; e^{-\theta t} \cdot \textstyle\prod_i \big(1 + x_i(e^{\theta w_i} - 1)\big).$$

Rewriting $g\big(x + z(e_a - e_b)\big)$ in this way, all factors are non-negative and only two of them depend on z, so for some $c \geq 0$,

$$\begin{aligned}
&\frac{d^2}{dz^2} g\big(x + z(e_a - e_b)\big)\\
&= c \frac{d^2}{dz^2}\Big(\big(1 + (x_a + z)(e^{\theta w_a} - 1)\big)\big(1 + (x_b - z)(e^{\theta w_b} - 1)\big)\Big)\\
&= c\big(-2\big(e^{\theta w_a} - 1\big)\big(e^{\theta w_b} - 1\big)\big).
\end{aligned}$$

This is non-positive so g is concave under swaps. □

Consequently, Claim 3.2 implies the following result.

COROLLARY 3.4. *If randomized pipage rounding starts at $x_0 \in P$ and outputs the extreme point $\hat{x}$ of P, then for all $w \in [0,1]^m$ and $\delta \geq 0$,*

$$\mathbb{P}\left[\, w^{\mathsf{T}} \hat{x} \geq (1+\delta)\mu \,\right] \;\leq\; \Big(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\Big)^{\mu} \tag{3.4}$$

where $\mu = w^{\mathsf{T}} x_0$. Furthermore, if this right-hand side is strictly less than 1, then deterministic pipage rounding outputs an extreme point $\hat{x}$ of P with $w^{\mathsf{T}}\hat{x} < (1+\delta)\mu$.

The key point is that the right-hand sides of (3.3) and (3.4) are the same. Chekuri et al. [17] proved this fact using negative correlation of $\hat{x}$, generalizing a result of Srinivasan [46].

3.4 Submodular functions. Chekuri et al. [17, Theorem 1.3] prove an analog of the Chernoff bound for concentration of submodular functions under independent rounding. They show that the same bound remains true under swap rounding [17, Theorem 1.4] and ask whether it remains true under pipage rounding.

Formally, let $f : \{0,1\}^m \to \mathbb{R}$ be a non-negative, monotone, submodular function with marginals in $[0,1]$. The *multilinear extension* of f is $F : [0,1]^m \to \mathbb{R}$ with $F(x) := \mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, f(X) \,\right]$. For $t \in \mathbb{R}$ and $\theta < 0$, define $g_{t,\theta} : [0,1]^m \to \mathbb{R}$ by

$$g_{t,\theta}(x) \;:=\; e^{-\theta t} \cdot \mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, e^{\theta f(X)} \,\right].$$

The left tail bound of Chekuri et al. is: with $\mu = F(x)$, $\delta \in [0,1)$,

$$\mathbb{P}_{X \sim \mathcal{D}(x)}\left[\, f(X) \leq t \,\right] \;\leq\; \inf_{\theta<0}\, g_{t,\theta}(x)$$

$$\text{and} \quad g_{(1-\delta)\mu,\, \ln(1-\delta)}(x) \;\leq\; \exp(-\delta^2\mu/2).$$

CLAIM 3.5. *$g_{t,\theta}$ is concave under swaps.*

Proof. Recall that $\theta < 0$. Define $h : \{0,1\}^m \to \mathbb{R}$ by $h(X) = e^{\theta f(X)}$. Then since $x \mapsto \exp(\theta x)$ is convex and non-increasing, and f is supermodular and non-decreasing, it follows that h is supermodular; see Appendix A for the proof of this fact. The multilinear extension of h is

$$H(x) \;=\; \mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, h(X) \,\right].$$

It follows from results of Calinescu et al. [14], applied to the submodular function $-h$ and its multilinear extension $-H$, that $\frac{\partial^2 H}{\partial x_i \partial x_j} \geq 0$ for any $i, j \in [m]$. Since $g(x) = e^{-\theta t} \cdot H(x)$, the second derivative of

$$z \;\mapsto\; g\big(x + z(e_i - e_j)\big)$$

is non-positive. Thus g is concave under swaps. □

Claim 3.2 implies the following result, answering a question of Chekuri et al. [17, p. 3].

COROLLARY 3.6. *If randomized pipage rounding starts at $x_0 \in P$ and outputs the extreme point $\hat{x}$ of P then, letting $\mu = F(x_0)$, we have $\mathbb{P}\left[\, f(\hat{x}) \leq (1-\delta)\mu \,\right] \leq \exp(-\delta^2\mu/2)$.*

Chekuri et al. [18, p. 583] state that this fact does not follow from negative correlation of $\hat{x}$.

3.5 Matrix Concentration. Tropp [49], improving on Ahlswede-Winter [2] and Oliviera [34], proves a beautiful analog of the Chernoff bound for sums of independent random matrices. We state a simplified form here.

THEOREM 3.7. *Let $M_1, \ldots, M_m \in \mathbb{S}^n_+$ satisfy $M_i \preceq R \cdot I$. For $t \in \mathbb{R}$ and $\theta > 0$, define $g_{t,\theta} : [0,1]^m \to \mathbb{R}$ by*

$$g_{t,\theta}(x) \;:=\; e^{-\theta t} \cdot \operatorname{tr}\exp\Big(\sum_{i=1}^{m} \log \mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, e^{\theta X_i M_i} \,\right]\Big).$$

Then, for $\mu \geq \big\|\mathbb{E}_{X \sim \mathcal{D}(x)}\left[\, \sum_i X_i M_i \,\right]\big\|$ and $\delta \geq 0$,

$$\mathbb{P}_{X \sim \mathcal{D}(x)}\left[\, \|\textstyle\sum_i X_i M_i\| \geq t \,\right] \;\leq\; \inf_{\theta>0}\, g_{t,\theta}(x)$$

$$\textit{and} \quad g_{(1+\delta)\mu,\, \ln(1+\delta)}(x) \;\leq\; n \cdot \Big(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\Big)^{\mu/R}.$$

The following is our main lemma on pessimistic estimators; we delay the proof until later in this section.

LEMMA 3.8. *$g_{t,\theta}$ is concave under swaps.*

Consequently, Claim 3.2 implies the following result.

COROLLARY 3.9. *Let P be a matroid base polytope and let $x_0 \in P$. Let $M_1, \ldots, M_m \in \mathbb{S}^n_+$ satisfy $M_i \preceq R \cdot I$. Let $\mu \geq \left\| \mathbb{E}_{X \sim \mathcal{D}(x_0)} \left[\sum_i X_i M_i \right] \right\|$. If randomized pipage rounding starts at x_0 and outputs the extreme point $\hat{x} = \chi(S)$ of P then we have*

$$\mathbb{P}\left[\left\| \textstyle\sum_{i \in S} M_i \right\| \geq (1+\delta)\mu \right] \;\leq\; n \cdot \left(\frac{e^\delta}{(1+\delta)^{1+\delta}} \right)^{\mu/R}. \tag{3.5}$$

Furthermore, if this right-hand side is strictly less than 1, then deterministic pipage rounding outputs an extreme point $\hat{x} = \chi(S)$ of P with $\left\| \sum_{i \in S} M_i \right\| < (1+\delta)\mu$.

The inequalities in Theorem 3.7 involve non-trivial matrix analysis, such as operator concavity of log and Lieb's celebrated concavity theorem [30]. It seems that even those results do not suffice to prove Lemma 3.8. To prove it, we derive a new variant of Lieb's theorem. Lieb [30] actually proved several related concavity theorems; for us, the most relevant form is as follows.

THEOREM 3.10. (LIEB [30]) *Let $L, K \in \mathbb{S}^n$ and $C \in \mathbb{S}^n_{++}$. Then $z \mapsto \operatorname{tr}\exp\big(L + \log(C + zK)\big)$ is concave in a neighborhood of 0.*

The main technical result of this paper is:

THEOREM 3.11. *Let $L \in \mathbb{S}^n$, $C_1, C_2 \in \mathbb{S}^n_{++}$ and $K_1, K_2 \in \mathbb{S}^n_+$. Then the univariate function*

$$z \;\mapsto\; \operatorname{tr}\exp\Big(L + \log(C_1 + zK_1) + \log(C_2 - zK_2)\Big) \tag{3.6}$$

is concave in a neighborhood of 0.

There are several known approaches to proving Lieb's theorem. The simplest is Tropp's approach [50]; however, his proof is based on joint convexity of quantum entropy, which is itself usually proven using Lieb's theorem. We were unable to prove Theorem 3.11 using Tropp's approach. Lieb's original proof [30], which proves concavity by directly analyzing the second derivative, involves numerous delicate steps of matrix analysis. We were able to adapt this approach to prove a weaker form of Theorem 3.11 that requires some additional commutativity assumptions; details are in Appendix D. This weaker result suffices to prove Lemma 3.8. Epstein [21] gives an elegant approach to proving Lieb's theorem using complex analysis, and in particular powerful results concerning Herglotz functions. Our proof of Theorem 3.11, which appears in Appendix C, is an adaptation of Epstein's approach.

Proof of Lemma 3.8. We will show that for all $x \in (0,1)^m$ and $a, b \in [m]$, the map

$$z \;\mapsto\; g_{t,\theta}\big(x + z(e_a - e_b)\big)$$

is concave. The boundary of $[0,1]^m$ is handled by continuity.

To begin, note that

$$\begin{aligned} \mathbb{E}_{X \sim \mathcal{D}(x)}\left[e^{\theta X_i M_i} \right] \;&=\; x_i \cdot e^{\theta M_i} \;+\; (1 - x_i) \cdot I \\ &=:\; C_i. \end{aligned} \tag{3.7}$$

Adding z (with $|z|$ sufficiently small) to the sampling probability of coordinate i, the expectation becomes

$$\begin{aligned} &\mathbb{E}_{X \sim \mathcal{D}(x + z e_i)}\left[e^{\theta X_i M_i} \right] \\ &\qquad=\; (x_i + z) \cdot e^{\theta M_i} \;+\; (1 - x_i - z) \cdot I \\ &\qquad=\; C_i + z \underbrace{\left(e^{\theta M_i} \;-\; I \right)}_{=: \, K_i}. \end{aligned} \tag{3.8}$$

Note that $C_i \succeq I$ and $K_i \succeq 0$ because $M_i \succeq 0$ and $\theta > 0$. Furthermore, the matrices C_i and K_i commute since any eigenbasis for M_i is also an eigenbasis of C_i and K_i.

Let us return to the main statement of the lemma. We must show that, for distinct $a, b \in [m]$, and for z in a neighborhood of zero, the following univariate function is concave.

$$\begin{aligned} z \;\mapsto\; & g_{t,\theta}\big(x + z(e_a - e_b)\big) \\ =\;& \operatorname{tr}\exp\Big(\log \mathbb{E}_{X \sim \mathcal{D}(x + z e_a)}\left[e^{\theta X_a M_a} \right] \\ & \quad + \log \mathbb{E}_{X \sim \mathcal{D}(x - z e_b)}\left[e^{\theta X_b M_b} \right] \\ & \quad + \textstyle\sum_{i \notin \{a,b\}} \log \mathbb{E}_{X \sim \mathcal{D}(x)}\left[e^{\theta X_i M_i} \right] \Big) \\ =\;& \operatorname{tr}\exp\Big(\log\left(C_a + z K_a \right) + \log\left(C_b - z K_b \right) \\ & \quad + \textstyle\sum_{i \notin \{a,b\}} \log C_i \Big) \end{aligned}$$

The last equality follows from (3.7) and (3.8). Letting $L = \sum_{i \notin \{a,b\}} \log C_i$, the desired concavity follows from Theorem 3.11. $\square$

REMARK. Another well-known matrix concentration inequality is the Ahlswede-Winter [2] inequality, for which pessimistic estimators were studied by Wigderson and Xiao [53]. It is natural to wonder whether we could have used their pessimistic estimators instead. Unfortunately they do not seem applicable for our scenario. The issue is that the Ahlswede-Winter inequality is most effective for analyzing sums of i.i.d. random matrices, due to some inequalities that arise in their analysis. In our scenario, due to the way that pipage rounding works, we require non-i.i.d. product distributions, so it is much more convenient to base our approach on Theorem 3.7.

4 Applications

4.1 Rounding of semidefinite programs. Let $\mathbf{M}$ be a matroid and let $P \subset \mathbb{R}^n$ be its base polytope. Consider the spectrahedron

$$Q \;:=\; P \,\cap\, \Big\{\, x \in \mathbb{R}^m \,:\, \sum_{i=1}^m x_i A_i \preceq I \,\Big\}, \tag{4.9}$$

where each $A_1, \ldots, A_m \in \mathbb{S}_+^n$. We think of P as specifying "hard" constraints and the semidefinite constraint as being "soft".

THEOREM 4.1. *Suppose that $A_i \preceq I$ for all i. If randomized pipage rounding starts at $x_0 \in Q$ and outputs the extreme point $\chi(S)$ of P, then $\mathbb{P}\big[\sum_{i\in S} A_i \preceq \alpha\big] \geq 1 - 1/n$, for some $\alpha = O(\log n/\log\log n)$. Furthermore, if deterministic pipage rounding starts at $x_0 \in Q$, then it outputs an extreme point $\chi(S)$ of P with $\sum_{i\in S} A_i \preceq \alpha$.*

This theorem is optimal with respect to α, as discussed below. The hypothesis that $A_i \preceq I$ is a "width" condition that commonly arises in optimization and rounding. Variations of this theorem involving events of the form $\sum_{i\in S} A_i \preceq \alpha B$ for some $B \in \mathbb{S}_+^n$ can be obtained by an appropriate change of basis.

Proof. Apply Corollary 3.9 with $M_i = A_i$, $\delta = 4\log n/\log\log n$, $\mu = 1$ and $R = 1$. A standard calculation shows that the right-hand side of (3.5) is less than $1/n$. $\square$

Chekuri, Vondrák and Zenklusen [17, 18] considered the problem of rounding a point in a matroid polytope to an extreme point, subject to additional packing constraints. Their result generalizes the low-congestion multi-path routing problem studied earlier by Srinivasan et al. [46, 23], but it is itself a special case of Theorem 4.1 where the matrices A_i are diagonal. The factor $\alpha = O(\log n/\log\log n)$ is optimal in Theorem 4.1 because it is optimal for rounding this low-congestion multi-path routing problem, and even for the congestion minimization problem [29].

4.2 Rounding an isotropic distribution to a nearly orthonormal basis. Let $w_1, \ldots, w_m \in \mathbb{R}^n$ satisfy $\|w_i\| = 1$ for all i. Let $p_1, \ldots, p_m$ be a probability distribution on these vectors such that $\sum_i p_i w_i w_i^\mathsf{T} = I/n$. (This is the covariance matrix of the distribution, if we assume that $\sum_i p_i w_i = 0$.) A random vector drawn from that distribution is said to be in *isotropic position*.

THEOREM 4.2. *There is a polynomial time algorithm (either randomized or deterministic) to compute a subset $S \subseteq [m]$ such that $\{\, w_i : i \in S \,\}$ forms a* basis *of $\mathbb{R}^n$, and for which $\big\|\sum_{i\in S} w_i w_i^\mathsf{T}\big\| \leq \alpha$, where $\alpha = O(\log n/\log\log n)$.*

As is discussed in Appendix E, the recent breakthrough on the Kadison-Singer problem [32] implies the following existential result:

THEOREM 4.3. *There exists $S \subseteq [m]$ such that $\{\, w_i : i \in S \,\}$ forms a basis of $\mathbb{R}^n$, and for which $\big\|\sum_{i\in S} w_i w_i^\mathsf{T}\big\| = O(1)$.*

We now prove Theorem 4.2 using Theorem 4.1. Let $\mathbf{M}$ be the linear matroid corresponding to the vectors $\{w_1, \ldots, w_m\}$. Let P be the base polytope of that linear matroid. Let $r : 2^{[m]} \to \mathbb{Z}_+$ be the rank function of that matroid, i.e., $r(S) = \dim\big(\operatorname{span}\{\, w_i \,:\, i \in S \,\}\big)$. Then

$$\begin{aligned} P \;:=\; \big\{ x \in \mathbb{R}_+^n \,:\, x(J) \leq r(J) \quad \forall J \subseteq [m] \\ \text{and} \;\; x([m]) = r([m]) \big\}. \end{aligned}$$

Define $A_i = w_i w_i^\mathsf{T}$, and

$$Q \;=\; P \,\cap\, \Big\{\, x \in \mathbb{R}^m \,:\, \sum_i x_i A_i \preceq I \,\Big\}.$$

Let $x = n \cdot p$. Then the following claim and the hypothesis that $\sum_i p_i w_i w_i^\mathsf{T} = I/n$ show that $x \in Q$.

CLAIM 4.4. *$x \in P$.*

Since $\|w_i\| = 1$, we have $A_i = w_i w_i^\mathsf{T} \preceq I$. Theorem 4.1 gives an algorithm to construct an extreme point $\chi(S)$ of P for which $\sum_{i\in S} A_i \preceq \alpha$, with $\alpha = O(\log n/\log\log n)$. Since P is the base polytope of $\mathbf{M}$, $\{\, w_i \,:\, i \in S \,\}$ forms a basis of $\mathbb{R}^n$. Finally, $\sum_{i\in S} w_i w_i^\mathsf{T} \preceq \alpha \cdot I$. This completes the proof of Theorem 4.2, modulo the proof of Claim 4.4.

Proof of Claim 4.4. By the assumption $\sum_i p_i w_i w_i^\mathsf{T} = I/n$ we have $r([m]) = n$ and

$$\sum_i x_i \;=\; n \sum_i p_i \;=\; \operatorname{tr}\Big(n \sum_i p_i w_i w_i^\mathsf{T} \Big) \;=\; \operatorname{tr}(I) \;=\; n.$$

So x satisfies the last constraint in the definition of P.

It remains to show that $\sum_{i\in J} x_i \leq r(J)$ for all J. For any positive semidefinite matrix, the average of the non-zero eigenvalues is a lower bound on the maximum eigenvalue, so

$$\frac{\operatorname{tr}(\sum_{i\in J} p_i w_i w_i^{\mathsf{T}})}{\operatorname{rank}(\sum_{i\in J} p_i w_i w_i^{\mathsf{T}})} \;\leq\; \Big\|\sum_{i\in J} p_i w_i w_i^{\mathsf{T}}\Big\| \;\leq\; \Big\|\sum_{i=1}^{m} p_i w_i w_i^{\mathsf{T}}\Big\| \;=\; 1/n.$$

Thus

$$\sum_{i\in J} x_i \;=\; n\sum_{i\in J} p_i \;=\; n\cdot \operatorname{tr}(\textstyle\sum_{i\in J} p_i w_i w_i^{\mathsf{T}}) \;\leq\; \operatorname{rank}(\textstyle\sum_{i\in J} p_i w_i w_i^{\mathsf{T}}) \;=\; r(J).$$

This proves that $x \in P$. □

In Appendix B.1, we show that Theorem 4.2 can be generalized from a decomposition of the identity into rank-one matrices $w_i w_i^{\mathsf{T}}$ to a decomposition into matrices of arbitrary rank. We remark that Theorem 4.3 is not known to have a generalization to matrices of arbitrary rank.

Column-subset selection. Column-subset selection is a topic of recent interest in numerical linear algebra [12, 48, 20, 11] that relates to important questions in operator theory [9, 10, 44, 48, 55]. The following theorem generalizes Theorem 4.2 to this setting. We remove the hypothesis that the vectors are isotropic, and allow the set S to be somewhat smaller. Formally, we ensure that $|S|$ is at least the *stable rank* of $\{w_1,\ldots,w_m\}$, which is

$$\operatorname{st.rank}(w_1,\ldots,w_m) \;:=\; \operatorname{tr}(\textstyle\sum_i w_i w_i^{\mathsf{T}})/\|\sum_i w_i w_i^{\mathsf{T}}\|.$$

The stable rank is a lower bound on $\operatorname{rank}(\{w_1,\ldots,w_m\})$ that de-emphasizes the contribution of small singular values; it has been used as a more tractable proxy for rank in previous work on column-subset selection.

THEOREM 4.5. *Let $w_1,\ldots,w_m \in \mathbb{R}^n$ satisfy $\|w_i\| = 1$ for all i. Then there is a deterministic, polynomial time algorithm to compute $S \subseteq [m]$ of size*

$$|S| \;\geq\; \lfloor \operatorname{st.rank}(w_1,\ldots,w_m)\rfloor$$

such that $\{\, w_i : i \in S \,\}$ is linearly independent, and $\|\sum_{i\in S} w_i w_i^{\mathsf{T}}\| \leq O(\log n/\log\log n)$.

The proof of Theorem 4.5 is essentially the same as the proof of Theorem 4.2, except that the matroid $\mathbf{M}$ is truncated to have rank equal to $\lfloor \operatorname{st.rank}(w_1,\ldots,w_m)\rfloor$.

4.3 Thin trees. Let $G = (V,E)$ be a graph. For convenience we assume that $V = [n]$. The *cut* defined by $U \subseteq V$ is

$$\delta_G(U) \;=\; \{\, uv \in E : \text{ exactly one of } u \text{ and } v \text{ is in } U \,\}.$$

For a subgraph T of G, let $\delta_T(U)$ denote all edges of T with exactly one endpoint in U.

DEFINITION 4.6. A subgraph T of G is called *ϵ-thin* if $|\delta_T(U)| \leq \epsilon \cdot |\delta_G(U)|$ for all $U \subseteq V$.

CONJECTURE 4.7. (GODDYN [25]) *Every graph with connectivity at least k has an $f(k)$-thin spanning subtree, for some function f that vanishes as k tends to infinity.*

The crucial detail in this conjecture is that the function f should not depend on the size of the graph. The best progress on this conjecture for general graphs is as follows.

THEOREM 4.8. (ASADPOUR ET AL. [3]) *Let G be a graph with n vertices and connectivity k. Then G has a $O\big(\frac{\log n}{k\log\log n}\big)$-thin spanning subtree. Moreover, there is a randomized, polynomial time algorithm to construct such a tree.*

Now we define spectrally-thin trees and prove an analog of this theorem. The Laplacian of G is the symmetric matrix L_G with rows and columns indexed by V defined by

$$L_G \;:=\; \sum_{uv\in E} (e_u - e_v)(e_u - e_v)^{\mathsf{T}}.$$

DEFINITION 4.9. Let T be a spanning subtree of G and let L_T be the Laplacian of T. The tree T is *ϵ-spectrally-thin* if $L_T \preceq \epsilon L_G$.

Any tree that is ϵ-spectrally-thin is also ϵ-thin, because

$$\begin{aligned} |\delta_T(U)| \;&=\; \chi(U)^{\mathsf{T}} L_T\, \chi(U) \\ &\leq\; \epsilon\cdot \chi(U)^{\mathsf{T}} L_G\, \chi(U) \\ &=\; \epsilon\cdot|\delta_G(U)|. \end{aligned}$$

The converse is not true. Moreover, the connectivity hypothesis in Theorem 4.8 does not suffice[1] to obtain a good spectrally-thin tree. The proof is in Appendix B.2.1.

THEOREM 4.10. *For every $n,k \geq 1$, there exists a weighted graph with n vertices and connectivity k that does not have an $o(\sqrt{n}/k)$-spectrally-thin spanning subtree.*

[1] This result was independently observed by M. de Carli Silva, N. Harvey and C. Sato, and by M. Goemans [26], using slightly different examples.

Nevertheless, if we strengthen the connectivity lower bound to a lower bound on the effective conductances, then we have the following construction of spectrally-thin trees. For an edge $e = uv \in E$, the *effective resistance* in G between u and v is $R_e := (e_u - e_v)^\intercal L_G^+(e_u - e_v)$. The *effective conductance* in G between u and v is $C_e := 1/R_e$.

THEOREM 4.11. *Let G be a graph with n vertices such that $\kappa \leq C_e$ for every edge e. Then there is a polynomial time algorithm (either randomized or deterministic) to construct a $O\big(\frac{\log n}{\kappa \log\log n}\big)$-spectrally-thin spanning subtree of G.*

Theorem 4.11 follows directly from Theorem 4.1, letting $\mathbf{M}$ be the graphic matroid corresponding to G. It also follows from Theorem 4.2, as we show in Appendix B.2. That viewpoint is advantageous, since Theorem 4.3 then immediately implies

THEOREM 4.12. *Let G be a graph with n vertices such that $\kappa \leq C_e$ for every edge e. Then G has a $O(1/\kappa)$-spectrally-thin spanning subtree.*

We are not aware of any formal connection between Theorem 4.12 and Conjecture 4.7 or the traveling salesman problem.

Although Theorem 4.8 and Theorem 4.11 are formally incomparable, it is worth understanding their similarities and differences. Both results have a seemingly suboptimal factor of $\log n/\log\log n$. Theorem 4.8 requires only a connectivity lower bound, which is important in applications [25, 3], but the resulting tree is thin, not spectrally-thin; also, their algorithm is randomized. Theorem 4.11 requires a conductance lower bound (which is stronger than a connectivity lower bound), but the resulting tree is spectrally-thin (which is stronger than being thin); also, our algorithm can be made deterministic. The use of randomization seems quite inherent in the algorithms [3, 18] for Theorem 4.8, as the thinness condition involves controlling exponentially many cuts, which seems difficult to accomplish by a deterministic, polynomial-time algorithm.

The quantities k and κ can be related in certain classes of graphs. We say that a family of graphs has *nearly equal resistances* if there is a constant c (independent of the number of vertices) such that $R_e \leq cR_f$ for all edges e, f. For example, any Ramanujan graph has nearly equal resistances. Edge-transitive graphs, such as hypercubes, have nearly equal (in fact, exactly equal) resistances.

COROLLARY 4.13. *Let G be a graph with n vertices, nearly equal resistances, and connectivity k. Then there is a deterministic, polynomial time algorithm to construct a $O\big(\frac{\log n}{k \log\log n}\big)$-spectrally-thin tree of G.*

The proof is in Appendix B.2.

Acknowledgements

N. Harvey thanks Joel Friedman and Mohit Singh for numerous enlightening discussions. We thank Isaac Fung for collaborating at a preliminary stage of this work. We also thank Christos Boutsidis, Joseph Cheriyan, Satoru Fujishige, Michel Goemans, Mary Beth Ruskai, Nikhil Srivastava, Joel Tropp, Roman Vershynin and Jan Vondrák for helpful discussions and suggestions. We are also grateful to the anonymous referees for their detailed comments and suggestions.

References

[1] A. A. Ageev and M. Sviridenko. Pipage rounding: A new method of constructing algorithms with proven performance guarantee. *Journal of Combinatorial Optimization*, 8, 2004.

[2] R. Ahlswede and A. Winter. Strong converse for identification via quantum channels. *IEEE Transactions on Information Theory*, 48(3):569–579, Mar. 2002.

[3] A. Asadpour, M. X. Goemans, A. Madry, S. Oveis Gharan, and A. Saberi. An $O(\log n/\log\log n)$-approximation algorithm for the asymmetric traveling salesman problem. In *SODA*, 2010.

[4] N. Bansal. Refinements of randomized rounding. Invited lecture at the Landelijk Netwerk Mathematische Beslikunde Lunteren Conference, 2012.

[5] J. Batson, D. A. Spielman, and N. Srivastava. Twice-Ramanujan sparsifiers. In *STOC*, 2009.

[6] R. Bhatia. *Matrix Analysis*. Springer, 1996.

[7] R. Bhatia. The logarithmic mean. *Resonance*, 13, 2008.

[8] B. Bollobás. *Modern Graph Theory*. Springer, 1998.

[9] J. Bourgain and L. Tzafriri. Invertibility of "large" submatrices with applications to the geometry of Banach spaces and harmonic analysis. *Israel J. Math*, 57, 1987.

[10] J. Bourgain and L. Tzafriri. On a problem of Kadison and Singer. *J. Reine. Angew. Math.*, 420:1–43, 1991.

[11] C. Boutsidis, P. Drineas, and M. Magdon-Ismail. Near optimal column-based matrix reconstruction. In *FOCS*, 2011.

[12] C. Boutsidis, M. W. Mahoney, and P. Drineas. An improved approximation algorithm for the column subset selection problem. In *SODA*, 2009.

[13] S. C. Boyd and W. R. Pulleyblank. Optimizing over the subtour polytope of the travelling salesman problem. *Mathematical Programming*, 49:163–187, 1991.

[14] G. Calinescu, C. Chekuri, M. Pál, and J. Vondrák. Maximizing a monotone submodular function subject to a matroid constraint. *SIAM Journal on Computing*, 40, 2011.

[15] B. C. Carlson. The logarithmic mean. *The American Mathematical Monthly*, 79(6):615–618, 1972.

[16] P. G. Casazza and J. C. Tremain. The Kadison-Singer problem in mathematics and engineering. *Proceedings of the National Academy of Sciences*, 103(7):2032–2039, 2006.

[17] C. Chekuri, J. Vondrák, and R. Zenklusen. Dependent randomized rounding for matroid polytopes and applications, 2009. arXiv:0909.4348.

[18] C. Chekuri, J. Vondrák, and R. Zenklusen. Dependent randomized rounding via exchange properties of combinatorial structures. In *FOCS*, pages 575–584, 2010.

[19] R. Y. Chen, A. Gittens, and J. A. Tropp. The masked sample covariance estimator: an analysis using matrix concentration inequalities. *Information and Inference*, 2012.

[20] A. Deshpande and L. Rademacher. Efficient volume sampling for row/column subset selection. In *FOCS*, 2010.

[21] H. Epstein. Remarks on Two Theorems of E. Lieb. *Communications in Mathematical Physics*, 31, 1973.

[22] S. Fujishige. *Submodular Functions and Optimization*. Elsevier, second edition, 2005.

[23] R. Gandhi, S. Khuller, S. Parthasarathy, and A. Srinivasan. Dependent rounding and its applications to approximation algorithms. *Journal of the ACM*, 53(3):324–360, 2006.

[24] F. Gesztesy and E. Tsekanovskii. On matrix-valued Herglotz functions. *Math. Nachrichten*, 218:61–138, 2000.

[25] L. A. Goddyn. Some open problems I like. Available at http://math.sfu.ca/~goddyn/Problems/problems.html.

[26] M. Goemans. Thin spanning trees. Lecture at "Graph Theory @ Georgia Tech: Conference Honoring the 50th Birthday of Robin Thomas", 2012.

[27] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991.

[28] R. V. Kadison and J. R. Ringrose. *Fundamentals of the Theory of Operator Algebras*. American Mathematical Society, 1983.

[29] T. Leighton, S. Rao, and A. Srinivasan. Multicommodity flow and circuit switching. In *Proc. Hawaii International Conference on System Sciences (HICSS)*, 1998.

[30] E. H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Advances in Mathematics*, 11:267–288, 1973.

[31] M. W. Mahoney. Randomized algorithms for matrices and data. arXiv:1104.5557.

[32] A. Marcus, D. A. Spielman, and N. Srivastava. Interlacing families II: Mixed characteristic polynomials and the Kadison-Singer problem, June 2013. arXiv:1306.3969.

[33] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, 1993.

[34] R. I. Oliveira. Concentration of the adjacency matrix and of the Laplacian in random graphs with independent edges, 2010. arXiv:0911.0600.

[35] S. Oveis Gharan and A. Saberi. Asymmetric traveling salesman problem on graphs with bounded genus. In *SODA*, 2011.

[36] A. Panconesi and A. Srinivasan. Randomized distributed edge coloring via an extension of the Chernoff-Hoeffding bounds. *SIAM Journal on Computing*, 26(2):350–368, 1997.

[37] P. Raghavan. Probabilistic construction of deterministic algorithms: Approximating packing integer programs. *Journal of Computer and System Sciences*, 37, 1988.

[38] P. Raghavan and C. D. Thompson. Randomized rounding: a technique for provably good algorithms and algorithmic proofs. *Combinatorica*, 7:365–374, 1987.

[39] B. Recht. A simpler approach to matrix completion. *Journal of Machine Learning Research*, 12, 2011.

[40] M. Rudelson. Almost orthogonal submatrices of an orthogonal matrix. *Israel J. Math.*, 111(1):143–155, 1999.

[41] M. Rudelson and R. Vershynin. Sampling from large matrices: An approach through geometric functional analysis. *Journal of the ACM*, 54(4), 2007.

[42] W. Rudin. *Real and Complex Analysis*. McGraw-Hill, third edition, May 1986.

[43] D. A. Spielman and N. Srivastava. Graph sparsification by effective resistances. In *STOC*, 2008.

[44] D. A. Spielman and N. Srivastava. An elementary proof of the restricted invertibility theorem. *Israel J. Math*, 190(1):83–91, Aug. 2012.

[45] A. Srinivasan. Approximation algorithms via randomized rounding: a survey. In M. Karonski and H. J. Promel, editors, *Lectures on Approximation and Randomized Algorithms*, pages 9–71. Polish Scientific Publishers PWN, 1999.

[46] A. Srinivasan. Distributions on level-sets with applications to approximation algorithms. In *FOCS*, 2001.

[47] A. Srinivasan. Pessimistic estimators, 2003. Lecture notes for CMSC858T "Randomized Algorithms".

[48] J. A. Tropp. Column subset selection, matrix factorization, and eigenvalue optimization. In *SODA*, 2009.

[49] J. A. Tropp. User-friendly tail bounds for sums of random matrices. *Foundations of Computational Mathematics*, 2011.

[50] J. A. Tropp. From the joint convexity of quantum relative entropy to a concavity theorem of Lieb. *Proc. Amer. Math. Soc.*, 140(5):1757–1760, 2012.

[51] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. In Y. Eldar and G. Kutyniok, editors, *Compressed Sensing: Theory and Applications*, chapter 5, pages 210–268. Cambridge University Press, 2012.

[52] N. Weaver. The Kadison-Singer problem in discrepancy theory. *Discrete Mathematics*, 278:227–239, 2004.

[53] A. Wigderson and D. Xiao. Derandomizing the Ahlswede-Winter matrix-valued Chernoff bound using pessimistic estimators and applications. *Theory of Computing*, 4(3), 2008.

[54] D. P. Williamson and D. B. Shmoys. *The Design of Approximation Algorithms*. Cambridge University Press, 2011.

[55] P. Youssef. Restricted invertibility and the Banach-Mazur distance to the cube, 2012. arXiv:1206.0654v1.

A A fact about submodularity and convexity

The following simple fact is needed in the proof of Claim 3.5.

LEMMA A.1. *Let $f : 2^{[m]} \to \mathbb{R}$ be non-decreasing and submodular. Let $g : \mathbb{R} \to \mathbb{R}$ be non-increasing and convex. Then $g \circ f$ is supermodular.*

Proof. We require the following property of convex functions. Suppose a, b, c, d satisfy

$$\text{(A.1)} \qquad a \;\leq\; \min\{b, c\} \;\leq\; \max\{b, c\} \;\leq\; d.$$

Then any function g that is convex on $[a, d]$ satisfies

$$\text{(A.2)} \qquad \frac{g(d) - g(c)}{d - c} \;\geq\; \frac{g(b) - g(a)}{b - a}.$$

Fix any $A \subseteq B \subseteq [m]$, and an element $x \in [m] \setminus B$. Define

$$\begin{aligned} &a := f(A), \quad b := f(A + x), \qquad c := f(B), \\ &d := f(B) + f(A + x) - f(A), \quad e := f(B + x). \end{aligned}$$

Since f is non-decreasing, (A.1) holds. Since f is submodular, $e \leq d$ holds. Since g is non-increasing, $g(e) \geq g(d)$. Combining that with (A.2) and the observation that $d - c = b - a$, we obtain

$$g(e) - g(c) \;\geq\; g(d) - g(c) \;\geq\; g(b) - g(a).$$

That is,

$$g\big(f(B + x)\big) - g\big(f(B)\big) \;\geq\; g\big(f(A + x)\big) - g\big(f(A)\big),$$

so $g \circ f$ is supermodular. □

B Proofs of Applications

B.1 Rounding decompositions of the identity.

Here, we give a generalization of Theorem 4.2 to a decomposition of the identity into matrices of arbitrary rank.

THEOREM B.1. *Let $X_1, \ldots, X_m \in \mathbb{S}^n_+$ satisfy $\sum_{i=1}^m X_i = I$. Then there exists a subset $S \subseteq [m]$ with $|S| \leq n$ such that $\sum_{i \in S} X_i / \operatorname{tr} X_i$ has full rank and maximum eigenvalue at most $\alpha = O(\log n / \log \log n)$.*

Proof. Let V_i be a matrix such that $X_i = V_i V_i^{\mathsf{T}}$. Define the function $r : 2^{[m]} \to \mathbb{Z}_+$ by

$$r(J) \;=\; \operatorname{rank}\Big(\sum_{j \in J} V_j V_j^{\mathsf{T}}\Big) \;=\; \operatorname{rank} V_J,$$

where V_J is the matrix obtained by concatenating in any order all columns from the matrices $\{\, V_j \,:\, j \in J \,\}$. It is well-known that such a function r is:

- *Normalized:* $r(\emptyset) = 0$,
- *Monotone:* $r(I) \leq r(J)$ whenever $I \subseteq J$, and
- *Submodular:* $r(I) + r(J) \geq r(I \cup J) + r(I \cap J)$ for all $I, J \subseteq [m]$.

For any normalized, monotone, submodular function $f : 2^{[m]} \to \mathbb{R}$, its *base polytope* is defined to be

$$\begin{aligned} B(f) \;:=\; \Big\{\, x \in \mathbb{R}^m_+ \,:\, & x(J) \leq f(J) \;\; \forall J \subseteq [m], \\ & \text{and} \;\; x([m]) = f([m]) \,\Big\}. \end{aligned}$$

Define the vector $p \in \mathbb{R}^m$ by $p_i = \operatorname{tr} X_i$. Note that $p \geq 0$ and $\sum_i p_i = \operatorname{tr}(\sum_i X_i) = n$, so we can think of p as defining a "fractional multiset" of n matrices. Intuitively, we want to "round" the coordinates of p to integers. To that end, define the polytope

$$P' \;:=\; B(r) \cap \{\, x \,:\, \lfloor p \rfloor \leq x \leq \lceil p \rceil \,\},$$

where $\lfloor p \rfloor$ and $\lceil p \rceil$ respectively denote the componentwise floor and ceiling of the vector $p \in \mathbb{R}^m$. The polytope P' is not necessarily a matroid polytope; for example, a vector in P' could have a coordinate strictly greater than 1.

CLAIM B.2. *$p \in P'$.*

CLAIM B.3. *$P := \{\, x - \lfloor p \rfloor \,:\, x \in P' \,\}$ is a matroid base polytope.*

Claim B.2 is proven below. Claim B.3 is a "folklore result", known to experts in the area, that can be derived using reductions and contractions of submodular functions [22, §3.1(b)]; see also Fujishige's remarks on crossing submodular functions [22, Eq. (3.97)].

Define $A_i = X_i / \operatorname{tr} X_i$ and

$$Q \;:=\; P \cap \Big\{\, x \in \mathbb{R}^m \,:\, \sum_i x_i A_i \preceq I \,\Big\}.$$

Setting $x = p - \lfloor p \rfloor$, we have $x \in P$ by Claim B.2 and

$$\sum_i x_i A_i \;\preceq\; \sum_i p_i \frac{X_i}{\operatorname{tr} X_i} \;=\; \sum_i X_i \;=\; I,$$

so $x \in Q$.

Since $\operatorname{tr} A_i = 1$, we have $A_i \preceq I$. Applying Theorem 4.1, we obtain a vector $\hat{x} \in \{0, 1\}^n$ that is an extreme point of P, and for which $\sum_i \hat{x}_i A_i \preceq \alpha$. Let S be the support of $\hat{x}$. Note that $\hat{x} + \lfloor p \rfloor \in P'$. So

$$|S| \;=\; \sum_{i=1}^m \hat{x}_i \;\leq\; \sum_{i=1}^m (\hat{x}_i + \lfloor p_i \rfloor) \;\leq\; r([m]) \;=\; n$$

and $\sum_{i \in S} X_i / \operatorname{tr} X_i \preceq \alpha$ as required. □

Proof of Claim B.2. The box constraint $\lfloor p \rfloor \leq p \leq \lceil p \rceil$ is trivially satisfied. We have noted above that $\sum_i p_i = n$, so the constraint $p([m]) \leq r([m]) = n$ is also satisfied.

It remains to show that $\sum_{i \in I} p_i \leq r(I)$ for all I. For any positive semidefinite matrix, the average of the non-zero eigenvalues is a lower bound on the maximum eigenvalue, so

$$\frac{\operatorname{tr}(\sum_{i \in I} X_i)}{\operatorname{rank}(\sum_{i \in I} X_i)} \;\leq\; \Big\| \sum_{i \in I} X_i \Big\| \;\leq\; \Big\| \sum_{i=1}^{m} X_i \Big\| \;=\; 1.$$

Thus $\sum_{i \in I} p_i = \operatorname{tr}(\sum_{i \in I} X_i) \leq \operatorname{rank}(\sum_{i \in I} X_i) = r(I)$. This proves that $p \in P$. ☐

B.2 Thin trees. *Proof of Theorem 4.11.* Recall the notation defined in Section 2. For $e = uv \in E$, define vectors $x_e = L_G^{+/2}(e_u - e_v)$ and $w_e = x_e / \|x_e\|$. Then $R_e = \|x_e\|^2$; let $p_e = R_e/(n-1)$. It is well-known [8] that the vector of effective resistances describes the edge marginals of the uniform spanning tree, and hence that $\sum_e p_e = 1$. Then, following the argument of Spielman and Srivastava [43],

$$\begin{aligned} \sum_{e \in E} p_e w_e w_e^{\mathsf{T}} &= \frac{1}{n-1} \sum_{e \in E} x_e x_e^{\mathsf{T}} \\ &= \frac{1}{n-1} L_G^{+/2} \Big(\sum_{e \in E} (e_u - e_v)(e_u - e_v)^{\mathsf{T}} \Big) L_G^{+/2} \\ &= \frac{1}{n-1} I_{\operatorname{im} L_G}. \end{aligned}$$

We view the vectors $\{ w_e \,:\, e \in E \}$ as $(n-1)$-dimensional vectors in their linear span and apply Theorem 4.2. This gives a set $T \subseteq E$ of size $n-1$ such that $\{ w_e \,:\, e \in T \}$ is linearly independent and

$$\sum_{e \in T} w_e w_e^{\mathsf{T}} \;\preceq\; O(\log n / \log\log n) \cdot I_{\operatorname{im} L_G}.$$

The first two conditions imply that the edges in T form a spanning tree on the vertex set V. Then since $R_e = \|x_e\|^2$, we have

$$\sum_{e \in T} \frac{x_e x_e^{\mathsf{T}}}{R_e} \;\preceq\; O(\log n / \log\log n) \cdot I_{\operatorname{im} L_G}.$$

Equivalently,

$$\sum_{uv \in T} \frac{(e_u - e_v)(e_u - e_v)^{\mathsf{T}}}{R_{uv}} \;\preceq\; O(\log n / \log\log n) \cdot L_G.$$

Since we assume that $\kappa \leq C_e = 1/R_e$ for every edge e, we obtain

$$L_T \;=\; \sum_{uv \in T} (e_u - e_v)(e_u - e_v)^{\mathsf{T}} \;\preceq\; O\Big(\frac{\log n}{\kappa \log\log n} \Big) \cdot L_G.$$

So T is $O\big(\frac{\log n}{\kappa \log\log n}\big)$-spectrally-thin. ☐

Proof of Corollary 4.13. By the nearly equal resistances assumption, $R_e = O(\frac{n-1}{|E|})$ for every edge e. On the other hand, the connectivity k is at most the average degree, which is $2|E|/n$. Thus $R_e = O(1/k)$ for every edge e. The result now follows from Theorem 4.11. ☐

B.2.1 Proof of Theorem 4.10 Assume n is a multiple of 4. We define a graph that is related to an example of Boyd and Pulleyblank [13, p. 180]. There are two disjoint cycles, each of length $n/2$. Let us number the vertices in the first cycle as $1, \ldots, n/2$ and the vertices in the second cycle as $n/2+1, \ldots, n$. Add a matching where the i^{th} edge connects the i^{th} vertex in the first cycle and the i^{th} vertex in the second cycle. The edges in the cycles each have weight $w_c := k/2$ and the edges in the matching each have weight $w_m := 2k/n$. Obviously this weighted graph has connectivity at least k.

Let T be any subtree of G, without any weights on the edges of T. The first claim proves the theorem in the case when T uses exactly one matching edge, and the second claim handles the case when T uses several matching edges.

Claim B.4. *Suppose that T uses only a single matching edge. There exists a vector z such that*

$$\frac{z^{\mathsf{T}} L_T z}{z^{\mathsf{T}} L_G z} \;=\; \Omega\Big(\frac{\sqrt{n}}{k} \Big).$$

Proof. Without loss of generality, $\{n/4, 3n/4\}$ be the matching edge used by T. Let $\alpha = n^{-0.5}$ and $c = 1 - \alpha$. Define the vector z where

$$z_i \;=\; \begin{cases} c^{|n/4 - i|} & (i \leq n/2) \\ 0 & (i > n/2). \end{cases}$$

Numerator: The numerator is $z^{\mathsf{T}} L_T z = \sum_{uv \in E} (z_u - z_v)^2 \geq (z_{n/4} - z_{3n/4})^2 = 1$.

Denominator: To evaluate $z^{\mathsf{T}} L_G z$, we separately consider the cycle edges and matching edges. The contribution from the matching edges is

$$\begin{aligned} C_m \;&:=\; w_m \cdot \sum_{i=1}^{n/2} (z_i - z_{n/2+i})^2 \\ &<\; 2 w_m \cdot \sum_{i \geq 0} c^{2i} \\ &<\; \frac{2 w_m}{1-c} \\ &=\; \frac{2 w_m}{\alpha}. \end{aligned}$$

The contribution from the cycle edges is

$$\begin{aligned} C_c &:= w_c \sum_{i=2}^{n/2} (z_{i-1} - z_i)^2 \; + \; w_c (z_1 - z_{n/2})^2 \\ &< 2w_c \sum_{i \geq 1} (c^{i-1} - c^i)^2 \\ &= 2w_c (1-c)^2 \sum_{i \geq 0} c^{2i} \\ &= 2w_c \frac{(1-c)^2}{1-c^2} \\ &< 2w_c \frac{(1-c)^2}{1-c} \\ &= 2w_c \alpha. \end{aligned}$$

Since $\alpha = n^{-0.5}$, we get $C_m = O(k/\sqrt{n})$ and $C_c = O(k/\sqrt{n})$, so $z^\mathsf{T} L_G z = O(k/\sqrt{n})$. □

CLAIM B.5. *Suppose that T uses $m > 1$ matching edges. There exists a vector z such that*

$$\frac{z^\mathsf{T} L_T z}{z^\mathsf{T} L_G z} \; = \; \Omega\Big(\frac{\sqrt{n}}{k}\Big).$$

Proof. Let the matching edges used by T be $\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_m, b_m\}$. Define the vector z by

$$z_i \; = \; \begin{cases} c^{\min_{j \in [m]} d_1(i, a_j)} & (i \leq n/2) \\ 0 & (i > n/2) \end{cases}$$

where d_1 denotes distance in the first cycle.

Numerator: As in Claim B.4, every matching edge used by T contributes at least 1, so $z^\mathsf{T} L_T z \geq m$.

Denominator: Obviously $z^\mathsf{T} L_G z$ is no more than m times what it would be if T used exactly one matching edge. That is, $z^\mathsf{T} L_G z \leq O(mk/\sqrt{n})$. □

C Proof of Theorem 3.11

The outline of this proof follows a proof of Lieb's theorem presented by Epstein [21]. Epstein's proof proceeds via complex analytic techniques, and in particular makes use of some powerful results involving Herglotz functions (see, e.g., [6, 24]). While an effort has been made to make the treatment here accessible, a modicum of complex analysis will be assumed; a standard reference is [42].

For a complex number z, let $\Re z$ and $\Im z$ respectively denote the real and imaginary parts of z. Let $\mathbb{C}_{++} = \{z \in \mathbb{C} \mid \Im z > 0\}$ denote the open upper half-plane, and $\mathbb{C}_+$ the closed upper half-plane. Define $\mathbb{C}_{--}$ and $\mathbb{C}_-$ in the obvious corresponding way.

DEFINITION C.1. A function $g : \mathbb{C}_{++} \to \mathbb{C}$ is called a *Herglotz function* (or *Pick function*) if it is analytic on $\mathbb{C}_{++}$ and $g(\mathbb{C}_{++}) \subseteq \mathbb{C}_{++}$.

For example the map $z \mapsto az+b$ is Herglotz if $a \in \mathbb{R}_+$ and $b \in \mathbb{C}_+$. The maps $z \mapsto -1/z$ and $z \mapsto \log z$ are also Herglotz.

A key reason that Herglotz functions will be useful is the following classical theorem (see, e.g., [6, Eq. V.42] or [27, p. 542]).

THEOREM C.2. (HERGLOTZ-NEVANLINNA-RIESZ REPRESENTATION THEOREM) *For any Herglotz function g, there exists $a \in \mathbb{R}$, $b \in \mathbb{R}_+$ and a positive Borel measure μ on $\mathbb{R}$, with $\int_\mathbb{R} \frac{1}{t^2+1} d\mu(t) < \infty$, such that*
(C.3)

$$g(z) \; = \; a + bz + \int_\mathbb{R} \Big(\frac{1}{t-z} - \frac{t}{1+t^2}\Big)\, d\mu(t) \quad \forall z \in \mathbb{C}_{++}.$$

Roughly speaking, this provides a description of a Herglotz function through its boundary (the real line); since the function may diverge as it approaches the real line, the generality of a measure (which may have atoms) is needed.

The relevance of this theorem to our purposes comes from the following:

LEMMA C.3. (IMPLICIT IN [21]) *Let D be a domain[2] in $\mathbb{C}$ containing $\mathbb{C}_{--} \cup \{0\}$. Suppose $f : D \to \mathbb{C}$ is analytic, its restriction to $D \cap \mathbb{R}$ is real-valued, and moreover the function g on $\mathbb{C}_{++}$ defined by $g(z) = zf(1/z)$ is a Herglotz function. Then the restriction of f to $D \cap \mathbb{R}$ is concave in some neighborhood of the origin.*

Proof. Since $0 \in D$ and D is open, there exists some $\tau > 0$ so that the interval $[-\tau, \tau] \subset D$. Let D' be the image of D under the map $z \mapsto 1/z$; so D' contains $\mathbb{C}_{++} \cup [\tau^{-1}, \infty) \cup (-\infty, -\tau^{-1}]$. We may think of g as being defined on all of D'. Let μ be the positive Borel measure associated with g by Theorem C.2. This measure can be thought of as the limit of $\Im g(z)$ as z approaches the real line, in the appropriate distributional sense: this is known as the Stieltjes inversion formula; see, e.g., [6, Thm. V.4.12], [24, Thm. 2.2]. We will use only the following consequence:

> If for some open interval $I \subseteq \mathbb{R}$,
>
> $$\lim_{\epsilon \downarrow 0} \Im g(w + i\epsilon) = 0 \quad \text{for all } w \in I,$$
>
> then $\mu(I) = 0$.

We deduce that μ is supported on $[-\tau^{-1}, \tau^{-1}]$, since $\lim_{\epsilon \downarrow 0} \Im g(w + i\epsilon) = \Im g(w) = 0$ for all $w \in D' \cap \mathbb{R}$.

[2] Recall that, in analysis, a domain is defined to be an open, connected set.

Expressing f in terms of the Herglotz-Nevanlinna-Riesz representation of g, we have that

$$f(z) \;=\; az + b + \int_{-\tau^{-1}}^{\tau^{-1}} \frac{z^2}{zt-1}\, d\mu(t).$$

(Note that the final term of (C.3) can be folded into the constant a — since μ is Borel and has bounded support, it is finite.) Now calculate the second derivative of f, considered as a real-valued function on $D \cap \mathbb{R}$:

$$\begin{aligned} f''(x) \;&=\; \int_{-\tau^{-1}}^{\tau^{-1}} \frac{d^2}{dx^2}\left(\frac{x^2}{xt-1}\right) d\mu(t) \\ &=\; \int_{-\tau^{-1}}^{\tau^{-1}} \frac{2}{(xt-1)^3}\, d\mu(t). \end{aligned}$$

So for all $x \in (-\tau, \tau)$, $f''(x) < 0$, and so f (as a real-valued function on $D \cap \mathbb{R}$) is concave in the neighborhood of 0. □

We will apply Lemma C.3 with f as in the statement of Theorem 3.11:

$$f(z) = \operatorname{tr}\exp\Big(L + \log(C_1 + zK_1) + \log(C_2 - zK_2)\Big).$$

In order to extend our definition of log beyond symmetric matrices, we use (again following [21]) the Cauchy integral description

$$\log C = \int_0^\infty \frac{1}{t+1} - (t+C)^{-1}\, dt;$$

this is well-defined as long as C has no nonpositive eigenvalues. As our domain D, we take $\mathbb{C}_{--} \cup B_\epsilon$, where B_ϵ is an open ball around the origin of radius $\epsilon := \frac{1}{2}\min\{\lambda_{min}(C_1)\|K_1\|^{-1}, \lambda_{min}(C_2)\|K_2\|^{-1}\}$. This ensures that

Lemma C.4. *The function f is well-defined and analytic on D.*

For convenience, we withhold the proof until the end of this section.

To deduce that f is concave by Lemma C.3, we must show that g defined by $g(z) = zf(1/z)$ is Herglotz. We have

$$\begin{aligned} g(z) &= z \cdot f(1/z) \\ &= z \operatorname{tr}\exp\Big(L + \log(C_1 + K_1/z) + \log(C_2 - K_2/z)\Big) \\ &= \operatorname{tr}\exp\Big(\log(zI) + L + \log(C_1 + K_1/z) \\ &\qquad + \log(C_2 - K_2/z)\Big) \\ &= \operatorname{tr}\exp\Big(L + \log(C_1 z + K_1) + \log(C_2 + (-1/z)K_2)\Big). \end{aligned}$$

We will work with complex matrices for the remainder of this section, so let $M_n(\mathbb{C})$ denote the space of $n \times n$ complex matrices, and $\mathbb{H}^n$ the space of $n \times n$ Hermitian matrices. We will make use of operator formalism on occasion; in particular, the identity I will generally be omitted, and so for a scalar $w \in \mathbb{C}$, wI will be written as simply w.

An arbitrary matrix $C \in M_n(\mathbb{C})$ has a unique decomposition $C = P + iQ$ with $P, Q \in \mathbb{H}^n$, by taking $P = \frac{1}{2}(C + C^*)$ and $Q = \frac{1}{2i}(C - C^*)$, where * denotes adjoint (conjugate transpose). The standard terminology [28, pp. 237] is that P is the "real part" of C, denoted by $\Re C$, and that Q is the "imaginary part" of C, denoted by $\Im C$. This terminology is consistent with the scalar $(n=1)$ case, and has nothing to do with the entry-wise real and imaginary parts of the matrix.

This analogy to the scalar case provides a lot of helpful intuition, and so at this point we will sketch a version of the proof for $n = 1$. The full argument will follow the same essential steps, though the generalization is not completely straightforward. The scalar analog of a Hermitian matrix is a real number, and the scalar analog of a positive definite matrix is a positive number; so we consider the function $h : \mathbb{C} \to \mathbb{C}$ defined by

$$h(z) \;=\; \exp\big(l + \log(c_1 z + k_1) + \log(c_2 + (-1/z)k_2)\big),$$

with real parameters $l \in \mathbb{R}$, $k_1, k_2 \geq 0$ and $c_1, c_2 > 0$. Then

$$\Im \log(c_1 z + k_1) \;=\; \arg(c_1 z + k_1) \;\in\; (0, \arg z].$$

Similarly,

$$\begin{aligned} &\Im \log(c_2 + (-1/z)k_2) \;= \\ &\qquad \arg(c_2 + (-1/z)k_2) \;\in\; [0, \arg(-1/z)). \end{aligned}$$

Since $\arg(-1/z) = \pi - \arg z$, we obtain

$$\Im(l + \log(c_1 z + k_1) + \log(c_2 + (-1/z)k_2)) \;\in\; (0, \pi).$$

Since $\Im e^{a+ib} = e^a \sin b$ for $a, b \in \mathbb{R}$, we deduce that $\Im h(z) > 0$, as required.

We now resume the argument for the case $n > 1$. Define

$$\begin{aligned} \mathcal{I}_{++} \;&=\; \{\, C \in M_n(\mathbb{C}) \,:\, \Im C \succ 0 \,\} \\ \mathcal{I}_{+} \;&=\; \{\, C \in M_n(\mathbb{C}) \,:\, \Im C \succeq 0 \,\}. \end{aligned}$$

Much of the argument revolves around noting that $\mathcal{I}_{++}$ is closed under various operations. For example, if $C, A \in \mathcal{I}_{++}$ then clearly $A + C \in \mathcal{I}_{++}$. The following is less straightforward:

Lemma C.5. ([21, pp. 318–319]) *For any $C \in \mathcal{I}_{++}$,* *(i)* $-C^{-1} \in \mathcal{I}_{++}$, *and*

(ii) $0 \prec \Im \log C \prec \pi$.

We refer to [21] for the proofs, but we again note the intuition by analogy with the $n = 1$ case, where C is just an element of $\mathbb{C}_{++}$. Then $C = re^{i\theta}$ for some $r > 0$ and $0 < \theta < \pi$; so $-C^{-1} = r^{-1}e^{i(\pi-\theta)} \in \mathbb{C}_{++}$ and $\log C = \log r + i\theta$.

A crucial lemma will be the following:

Lemma C.6. *Let $A, B \in \mathbb{H}^n$ satisfy $A, B \succeq 0$, where in addition at least one of A and B are strictly positive definite. Then for any $z \in \mathbb{C}_{++}$, $\log(A + Bz)$ is defined and*

$$0 \ \preceq \ \Im \log(A + Bz) \ \preceq \ \arg z.$$

Moreover, if $A \succ 0$, then the left inequality is strict, and if $B \succ 0$, the right inequality is strict.

Proof. We first observe that the conditions imply that $A + Bz$ has no nonpositive real eigenvalues, and hence that the logarithm is well defined. It suffices to show that $A + Bz$ is nonsingular, since we can apply the same argument to $A' + Bz$, where $A' = A + t$ for any $t \geq 0$.

If $B \succ 0$, then $B^{1/2}$ exists and is positive definite. Thus

$$A + Bz = B^{1/2}(\underbrace{B^{-1/2}AB^{-1/2}}_{=:Q} + z)B^{1/2}.$$

But Q is Hermitian (as can be seen since $B^{-1/2}$ and A are Hermitian) and so it has real spectrum; thus since $\Im z > 0$, 0 is not in the spectrum of $Q + z$. Hence $Q + z$ and so also $A + Bz$ are invertible.

If instead $A \succ 0$, then

$$A + Bz = zA^{1/2}(1/z + A^{-1/2}BA^{-1/2})A^{1/2},$$

and similar reasoning applies.

Suppose first that $B \succ 0$. Then $A + Bz \in \mathcal{I}_{++}$, and so by Lemma C.5 (ii) we immediately have that $\Im \log(A + Bz) \succ 0$. Now if $B \succeq 0$ but is not positive definite, then $B + \epsilon \succ 0$ for any $\epsilon > 0$, and so $\Im \log(A + (B + \epsilon)z) \succ 0$. Since $\log(A + Bz)$ is well defined, we have by continuity that

$$\Im \log(A + Bz) = \lim_{\epsilon \downarrow 0} \Im \log(A + (B + \epsilon)z) \succeq 0.$$

This completes the proof of the left inequality.

For the right inequality, suppose first that $A \succ 0$. Since $\arg z = \Im \log z$, our goal is to show that

$$\Im(\log z - \log(A + Bz)) \succ 0,$$

or equivalently (using that $A + Bz$ is nonsingular)

$$\Im \log((A/z + B)^{-1}) \succ 0.$$

Now since $-1/z \in \mathbb{C}_{++}$, it follows that $\Im(-A/z) \succ 0$. Since $\Im B = 0$, we obtain that $-A/z - B \in \mathcal{I}_{++}$. Thus $(A/z + B)^{-1} \in \mathcal{I}_{++}$ by Lemma C.5 (i), and so the result follows by Lemma C.5 (ii). If $A \succeq 0$ but A is not positive definite, we apply a limiting argument as before to deduce that $\Im \log(A + Bz) \succeq 0$. □

We will also need the following result:

Lemma C.7. ([21]) *If $0 \prec \Im C \prec \pi$, then* $\operatorname{tr} \exp C \in \mathbb{C}_{++}$.

We omit the proof, which proceeds by first showing that the spectrum of C is contained in the strip $\{\, z \in \mathbb{C} : 0 < \Im z < \pi \,\}$, and then using the spectral mapping theorem to deduce that the spectrum of $\exp C$ lies in $\mathbb{C}_{++}$.

Lemma C.8. *The function g is Herglotz.*

Proof. Take any $z \in \mathbb{C}_{++}$. By Lemma C.6, we have that

$$\begin{aligned} & 0 \preceq \Im \log(C_1 z + K_1) \prec \arg z \\ \text{and} \qquad & 0 \prec \Im \log(C_2 + (-1/z)K_2) \preceq \arg(-1/z). \end{aligned}$$

Since $\arg(-1/z) = \pi - \arg z$, we obtain that

$$0 \prec \Im\big(L + \log(C_1 z + K_1) + \log(C_2 + (-1/z)K_2)\big) \prec \pi.$$

Thus by Lemma C.7, $g(z) \in \mathbb{C}_{++}$. Hence g is indeed Herglotz. □

Applying Lemma C.3, and observing the proof of Lemma C.4 below, Theorem 3.11 has been proved.

Proof of Lemma C.4. Firstly, if $z \notin \mathbb{R}$, then either $C_1 + zK_1 \in \mathcal{I}_{++}$, or $-(C_1 + zK_1) \in \mathcal{I}_{++}$. Thus, as observed by Epstein, $\log(C_1 + zK_1)$ is defined; indeed, we already proved more in Lemma C.6. The same is true for $\log(C_2 - zK_2)$.

Now suppose $z \in (-\epsilon, \epsilon)$. Then

$$C_1 + zK_1 \succeq C_1 - \epsilon\|K_1\| \succeq C_1 - \tfrac{1}{2}\lambda_{min}(C_1) \succ 0.$$

Similarly $C_2 - zK_2 \succ 0$. □

D Weaker Proof of Theorem 3.11

In this appendix we prove Theorem 3.11, under the additional hypothesis that C_i & K_i commute. This suffices to prove Lemma 3.8. The argument builds on Lieb's original proof [30] of Theorem 3.10.

Theorem D.1. *Let $L \in \mathbb{S}^n$, $C_1, C_2 \in \mathbb{S}^n_{++}$ and $K_1, K_2 \in \mathbb{S}^n_+$ be such that C_1 & K_1 commute, and that C_2 & K_2 commute. Then*

(D.4)
$$f(z) \ := \ \operatorname{tr} \exp\Big(L + \log(C_1 + zK_1) + \log(C_2 - zK_2)\Big)$$

is concave in a neighborhood of 0.

First we need some preliminary definitions. For $x, y \geq 0$, define the logarithmic mean and binomial mean as follows:

$$\mathrm{LM}(x,y) \;=\; \begin{cases} \frac{x-y}{\log x - \log y} & (x \neq y) \\ x & (\text{otherwise}) \end{cases}$$

$$\mathrm{BM}(x,y) \;=\; \Big(\frac{x+y}{2} + \sqrt{xy}\Big)/2 \;=\; \Big(\frac{\sqrt{x}+\sqrt{y}}{2}\Big)^2.$$

THEOREM D.2. (CARLSON [15], BHATIA [7]) *For $x, y \geq 0$,*

$$\sqrt{xy} \;\leq\; \mathrm{LM}(x,y) \;\leq\; \mathrm{BM}(x,y) \;\leq\; (x+y)/2.$$

For any $X \in \mathbb{S}^n_{++}$, define the operators $T_X, R_X : \mathbb{S}^n \to \mathbb{S}^n$ by

$$T_X(Y) := \int_0^\infty (X+tI)^{-1} Y (X+tI)^{-1} dt$$
$$R_X(Y) := 2\int_0^\infty (X+tI)^{-1} Y (X+tI)^{-1} Y (X+tI)^{-1} dt.$$

CLAIM D.3. *Let $X \in \mathbb{S}^n_{++}$ and $Y \in \mathbb{S}^n$.*

- **(P1)**: *If X and Y commute then $T_X(Y) = YX^{-1}$ and $R_X(Y) = Y^2X^{-2}$.*
- **(P2)**: *The inverse of T_X is the operator T_X^{-1} where $T_X^{-1}(Y) = \int_0^1 X^t Y X^{1-t}\, dt$.*
- **(P3)**: *In a basis in which X is diagonal, we have $\big(T_X^{-1}(Y)\big)_{i,j} = Y_{i,j} \cdot \mathrm{LM}(X_{i,i}, X_{j,j})$.*
- **(P4)**: *T_X is a positive map, i.e., $T_X(Y) \in \mathbb{S}^n_+$ whenever $Y \in \mathbb{S}^n_+$.*

Proof. See Lieb [30] p. 277, and Ohya and Petz [33] Eq. (3.7) and p. 49. □

CLAIM D.4. *For any $C \in \mathbb{S}^n_{++}$, $K \in \mathbb{S}^n$ and $x \in \mathbb{R}$,*

$$\log(C + xK) \;=\; \log C + xT_C(K) - \frac{1}{2}x^2 R_C(K) + O(x^3).$$

Proof. See Lieb [30] equations (3.6) and (3.9), and Ohya and Petz [33, p. 53]. □

CLAIM D.5. *Let $L \in \mathbb{S}^n$, $C_1, C_2 \in \mathbb{S}^n_{++}$ and $K_1, K_2 \in \mathbb{S}^n$. Define $M = \exp(L + \log C_1 + \log C_2)$. Then*

$$\begin{aligned}
&\exp\Big(L + \log(C_1 + zK_1) + \log(C_2 - zK_2)\Big) \\
&\quad= M + z\int_0^1 M^{1-s}\Big(T_{C_1}(K_1) - T_{C_2}(K_2)\Big)M^s\, ds \\
&\quad+ z^2\Bigg(-\frac{1}{2}\int_0^1 M^{1-s}\Big(R_{C_1}(K_1) + R_{C_2}(K_2)\Big)M^s\, ds \\
&\quad+ \int_0^1\int_0^s M^{1-s}\Big(T_{C_1}(K_1) - T_{C_2}(K_2)\Big)M^{s-u} \\
&\qquad \Big(T_{C_1}(K_1) - T_{C_2}(K_2)\Big)M^u\; du\, ds\Bigg) \;+\; O(z^3).
\end{aligned}$$

Proof. Similar to Ohya and Petz [33, p. 53]. □

Proof of Theorem D.1. The theorem is equivalent to $0 \leq \frac{d^2f}{dz^2}\big|_{z=0}$ (assuming that this derivative exists). From Claim D.5 we have

(D.5)
$$\begin{aligned}
\frac{d^2f}{dz^2}\bigg|_{z=0}
&= -\operatorname{tr} M\big(R_{C_1}(K_1) + R_{C_2}(K_2)\big) + \\
&\operatorname{tr}\int_0^1 \big(T_{C_1}(K_1) - T_{C_2}(K_2)\big)M^y\big(T_{C_1}(K_1) - T_{C_2}(K_2)\big)M^{1-y}\, dy \\
&= -\operatorname{tr} M\big(R_{C_1}(K_1) + R_{C_2}(K_2)\big) + \\
&\operatorname{tr}\big(T_{C_1}(K_1) - T_{C_2}(K_2)\big)T_M^{-1}\big(T_{C_1}(K_1) - T_{C_2}(K_2)\big).
\end{aligned}$$

From **(P1)** and the assumption that C_i and K_i commute we have $R_{C_i}(K_i) = T_{C_i}(K_i)^2$. So the assertion of the theorem is equivalent to

$$\begin{aligned}
\text{(D.6)}\quad &\operatorname{tr} M\, T_{C_1}(K_1)^2 + \operatorname{tr} M\, T_{C_2}(K_2)^2 \;\geq \\
&\operatorname{tr}\Big(T_{C_1}(K_1) - T_{C_2}(K_2)\Big)T_M^{-1}\Big(T_{C_1}(K_1) - T_{C_2}(K_2)\Big).
\end{aligned}$$

We will prove the more general statement that for all $M \in \mathbb{S}^n_{++}$ and $X, Y \in \mathbb{S}^n_+$,

(D.7)
$$\operatorname{tr} MX^2 \;+\; \operatorname{tr} MY^2 \;\geq\; \operatorname{tr}(X-Y)T_M^{-1}(X-Y).$$

This implies (D.6) by our assumption that $K_1, K_2 \in \mathbb{S}^n_+$ and **(P4)**.

The preceding discussion is basis-independent. It is now convenient to fix a basis in which M is diagonal and to view M, X and Y as matrices in that basis. Let us denote the diagonal entries of M by $\lambda_i = M_{i,i}$; these are positive since we assume $M \in \mathbb{S}^n_{++}$. By **(P3)**, the right-hand side of (D.7) is

$$\begin{aligned}
\operatorname{tr}(X-Y)T_M^{-1}(X-Y) &= \sum_{i,j} \mathrm{LM}(\lambda_i, \lambda_j)\cdot\big(X_{i,j} - Y_{i,j}\big)^2 \\
\text{(D.8)}\qquad &\leq \sum_{i,j} \mathrm{BM}(\lambda_i, \lambda_j)\cdot\big(X_{i,j} - Y_{i,j}\big)^2,
\end{aligned}$$

by Theorem D.2. We may rewrite the right-hand side as

(D.9)
$$\sum_{i,j}\Big(\frac{\lambda_i}{4}+\frac{\lambda_j}{4}+\frac{\sqrt{\lambda_i\lambda_j}}{2}\Big)((X_{i,j})^2+(Y_{i,j})^2-2X_{i,j}Y_{i,j})$$
$$\begin{aligned} &= \frac{\operatorname{tr} MX^2}{2}+\frac{\operatorname{tr} M^{1/2}XM^{1/2}X}{2} \\ &\quad+\frac{\operatorname{tr} MY^2}{2}+\frac{\operatorname{tr} M^{1/2}YM^{1/2}Y}{2} \\ &\quad-\operatorname{tr} MXY-\operatorname{tr} M^{1/2}XM^{1/2}Y \end{aligned}$$

by repeatedly using the observation

$$\sum_{i,j} D_{i,i}P_{i,j}Q_{i,j}E_{j,j} \;=\; \operatorname{tr} DPEQ \;=\; \operatorname{tr} EPDQ$$

for all $D,E\in\mathbb{D}^n$, $P,Q\in\mathbb{S}^n$.

Thus, combining (D.7), (D.8) and (D.9), it suffices to prove

$$\begin{aligned}\operatorname{tr} MX^2-\operatorname{tr} M^{1/2}XM^{1/2}X+\operatorname{tr} MY^2-\operatorname{tr} M^{1/2}YM^{1/2}Y \\ \geq\; -2\operatorname{tr} MXY-2\operatorname{tr} M^{1/2}XM^{1/2}Y\end{aligned}$$

for every $M,X,Y\in\mathbb{S}_+^n$.

Since that inequality is invariant under choice of orthonormal basis, and since $\operatorname{tr} M^{1/2}XM^{1/2}Y\geq 0$, it suffices to prove

(D.10)
$$\begin{aligned}&\operatorname{tr} XD^2X-\operatorname{tr} XDXD+\operatorname{tr} YD^2Y-\operatorname{tr} YDYD \\ &\quad\geq\; -2\operatorname{tr} XD^2Y \qquad \forall D\in\mathbb{D}^n,\ \forall X,Y\in\mathbb{S}_+^n.\end{aligned}$$

Denote the diagonal entries of D by $d_i=D_{i,i}$. Then

$$\begin{aligned}&\operatorname{tr} XD^2X-\operatorname{tr} XDXD \\ &\quad=\; \frac{1}{2}\sum_{i,j}X_{i,j}^2(d_i^2+d_j^2)-\sum_{i,j}X_{i,j}^2 d_i d_j \\ &\quad=\; \frac{1}{2}\sum_{i,j}X_{i,j}^2(d_i-d_j)^2.\end{aligned}$$

So the left-hand side of (D.10) equals

$$\sum_{i,j}\frac{X_{i,j}^2+Y_{i,j}^2}{2}(d_i-d_j)^2 \;\geq\; \sum_{i,j}|X_{i,j}Y_{i,j}|\cdot(d_i-d_j)^2,$$

by the arithmetic-mean geometric-mean (AM-GM) inequality. The right-hand side of (D.10) is

$$\begin{aligned}-2\operatorname{tr}(XD^2Y) \;&=\; -\operatorname{tr}(XD^2Y)-\operatorname{tr}(D^2XY) \\ &=\; -\sum_{i,j}X_{i,j}Y_{i,j}(d_i^2+d_j^2).\end{aligned}$$

So, to prove (D.10), it suffices to prove that

(D.11)
$$\sum_{i,j}|X_{i,j}Y_{i,j}|\cdot(d_i-d_j)^2 \;\geq\; -\sum_{i,j}X_{i,j}Y_{i,j}(d_i^2+d_j^2).$$

We will prove the more general inequality

(D.12)
$$\sum_{i,j}|Z_{i,j}|\cdot(d_i-d_j)^2 \;\geq\; -\sum_{i,j}Z_{i,j}(d_i^2+d_j^2) \qquad \forall d\in\mathbb{R}^n,\ \forall Z\in\mathbb{S}_+^n.$$

This implies (D.11) by letting $Z=X\circ Y$ (the Hadamard product of X and Y), which is positive semidefinite by the Schur product theorem [6, p. 23]. Rearranging, (D.12) becomes

(D.13)
$$\frac{1}{2}\sum_{i,j}(|Z_{i,j}|+Z_{i,j})(d_i^2+d_j^2) \;\geq\; \sum_{i,j}|Z_{i,j}|\,d_i d_j.$$

Since $|Z_{i,j}|+Z_{i,j}\geq 0$, the AM-GM inequality implies that the left-hand side is at least

$$\sum_{i,j}(|Z_{i,j}|+Z_{i,j})d_i d_j \;=\; \sum_{i,j}|Z_{i,j}|\,d_i d_j \;+\; d^{\mathsf{T}}Zd.$$

Since $Z\in\mathbb{S}_+^n$, this implies (D.13). ☐

E Connections to the Kadison-Singer Problen

The Kadison-Singer problem, which dates back to 1959, is an important, and until very recently unsolved, question in operator theory. The importance of this question has become increasingly apparent in recent years as it is now known to be equivalent, or closely related, to numerous conjectures in disparate areas of mathematics [16]. In a very recent breakthrough, Marcus, Spielman and Srivastava [32] positively resolved the Kadison-Singer problem. More precisely, they proved the following strong form of Weaver's conjecture [52, Conjecture KS_2 and Theorem 2]:

Theorem E.1. (Marcus et al. [32]) *Let $\epsilon>0$, and $u_1,\ldots,u_m\in\mathbb{C}^n$ be such that $\|u_i\|\leq\epsilon$ for all i, and $\sum_i u_iu_i^{\mathsf{T}}=I$. Then there exists a partition of $[m]$ into S_1,S_2 such that for each $j\in\{1,2\}$,*

(E.14)
$$\sum_{i\in S_j}u_iu_i^{\mathsf{T}} \;\leq\; \tfrac{1}{2}(1+\sqrt{2\epsilon})^2.$$

It is well-known that, given a strong discrepancy result such as (E.14), an iterative argument yields a "well-conditioned" sparse object. Such an argument was used by Rudelson [40], for example. For the sake of completeness, we include here a detailed argument that Theorem E.1 implies the existence of $O(1/\kappa)$-spectrally-thin trees.

First, the following corollary of Theorem E.1 will be convenient for induction purposes.

Corollary E.2. *There exists a constant $C \geq 1$ such that the following is true. Let $v_1, \ldots, v_m \in \mathbb{R}^n$ be such that $\alpha I \preceq \sum_i v_i v_i^\mathsf{T} \preceq \beta I$ and $\|v_i\|^2 = \delta := n/m$ for all i. Suppose that $\alpha \in [1/2, 1]$ and $\beta \in [1, 2]$. Then there exists $S \subseteq [m]$ satisfying*

$$(\alpha - C\sqrt{\delta})I \;\preceq\; 2\sum_{i \in S} v_i v_i^\mathsf{T} \;\preceq\; (\beta + C\sqrt{\delta})I. \tag{E.15}$$

Proof. Let $\alpha, \beta, \delta, v_1, \ldots, v_m$ be as in the statement of Corollary E.2. Note that $\delta \leq 1$, since $m \geq n$. Letting $M = \sum_i v_i v_i^\mathsf{T}$, we see that $\|M^{-1}\| \leq \alpha^{-1}$. Define $u_i = M^{-1/2} v_i$. Then

$$\sum_i u_i u_i^\mathsf{T} \;=\; M^{-1/2}\Big(\sum_i v_i v_i^\mathsf{T}\Big)M^{-1/2} \;=\; I$$

and

$$\|u_i\|^2 \;\leq\; \|M^{-1}\|\,\|v_i\|^2 \;\leq\; \alpha^{-1}\delta \;=:\; \epsilon.$$

Applying Theorem E.1 of Marcus et al. [32], we deduce (E.14), and hence (since $\epsilon \leq 2$)

$$2\sum_{i \in S_j} u_i u_i^\mathsf{T} \;\preceq\; 1 + 4\sqrt{2\epsilon} \qquad \text{for } j \in \{1, 2\}.$$

Consequently,

$$2\sum_{i \in S_1} v_i v_i^\mathsf{T} \;\preceq\; (1{+}4\sqrt{2\epsilon})M \;\preceq\; (1{+}4\sqrt{2\epsilon})\beta \;\preceq\; \beta{+}16\sqrt{\delta}$$

by the hypotheses $\alpha \in [1/2, 1]$ and $\beta \in [1, 2]$.

Observing that

$$2\sum_{i \in S_1} u_i u_i^\mathsf{T} = 2I - 2\sum_{i \in S_2} u_i u_i^\mathsf{T} \succeq 1 - 4\sqrt{2\epsilon},$$

we similarly obtain

$$2\sum_{i \in S_1} v_i v_i^\mathsf{T} \;\succeq\; (1{-}4\sqrt{2\epsilon})M \;\succeq\; (1{-}4\sqrt{2\epsilon})\alpha \;\succeq\; \alpha{-}4\sqrt{2\delta}.$$

Thus taking $S = S_1$, we see that (E.15) holds with $C = 16$. □

Claim E.3. *Let $w_1, \ldots, w_m \in \mathbb{R}^n$ satisfy $\|w_i\| = 1$ for all i. Suppose that $\sum_i w_i w_i^\mathsf{T}/m = I/n$. For any $\epsilon \leq 1/3$, there exists $y \in \{0, 1\}^m$ with*

- $(1 - \epsilon)I \preceq \Theta(\epsilon^2)\sum_i y_i w_i w_i^\mathsf{T} \preceq (1 + \epsilon)I$,
- $|\mathrm{supp}(y)| = \Theta(n/\epsilon^2)$.

Proof. Define $v_i = \sqrt{n/m} \cdot w_i$, so that $\|v_i\|^2 = n/m =: \delta_0$ for all i. We will iteratively construct sets $S_t \subseteq [m]$, with $S_0 = [m]$. Let C be as in Corollary E.2. Define $\alpha_0 = \beta_0 = m$, and then inductively

$$\begin{aligned}\alpha_{t+1} &= \alpha_t - C(2^t n)^{1/2}(\beta_t)^{1/2}\\ \beta_{t+1} &= \beta_t + C(2^t n)^{1/2}(\beta_t)^{1/2}.\end{aligned}$$

Let

$$T = \max\Big\{\, t \,:\, C\sum_{j=0}^{t-1}(2^j n/m)^{1/2} \leq \epsilon/2 \,\Big\}.$$

This choice of T is motivated by the following:

Claim E.4. *For all $t \leq T$, $\beta_t \leq m(1 + \epsilon)$ and $\alpha_t \geq m(1 - \epsilon)$.*

Proof. For $0 \leq t < T$,

$$\beta_{t+1} \;=\; \beta_t(1 + C(2^t n/\beta_t)^{1/2}) \;\leq\; \beta_t(1 + C(2^t n/m)^{1/2}).$$

So

$$\begin{aligned}\beta_t \;&\leq\; m\prod_{j=0}^{t-1}\Big(1 + C(2^j n/m)^{1/2}\Big)\\ &\leq\; m\exp\Big(C\sum_{j=0}^{t-1}(2^j n/m)^{1/2}\Big)\\ &\leq\; m\exp(\epsilon/2)\\ &\leq\; m(1 + \epsilon).\end{aligned}$$

Note that

$$\alpha_0 - \alpha_t \;=\; \beta_t - \beta_0$$

and so since $\beta_t \leq m(1 + \epsilon)$, $\alpha_t \geq m(1 - \epsilon)$. □

Note that since $\sum_{j=0}^{T-1}(2^j n/m)^c = \Theta((2^T n/m)^{1/2})$, we have that

$$2^T = \Theta\left(\frac{m}{n}\epsilon^2\right). \tag{E.16}$$

Our first goal will be to show inductively that for all $t \leq T$, there exists a set $S_t \subseteq [m]$ so that

$$\alpha_t \;\preceq\; m2^t\sum_{i \in S_t} v_i v_i^\mathsf{T} \;\preceq\; \beta_t. \tag{E.17}$$

Note that this is true for $t = 0$ by assumption.

It will be convenient to define $\gamma_t = 2^t|S_t|$. Suppose (E.17) holds for some particular $t < T$. Define

$$v_i^{(t)} \;=\; v_i \cdot \sqrt{m2^t/\gamma_t},$$

so that $\|v_i^{(t)}\|^2 = \frac{n}{|S_t|} =: \delta_t$ for all t. Then just by scaling,

$$\alpha_t/\gamma_t \;\preceq\; \sum_{i \in S_t} v_i^{(t)}(v_i^{(t)})^\mathsf{T} \;\preceq\; \beta_t/\gamma_t.$$

Taking a trace yields $n\alpha_t/\gamma_t \le n \le n\beta_t/\gamma_t$, i.e.,

$$\alpha_t \;\le\; \gamma_t \;\le\; \beta_t. \tag{E.18}$$

By (E.18) and Claim E.4, we have

$$\begin{aligned} 1/2 \;\le\; \frac{1-\epsilon}{1+\epsilon} \;\le\; \frac{\alpha_t}{\beta_t} \;\le\; \frac{\alpha_t}{\gamma_t} \;\le\; 1 \\ 1 \;\le\; \frac{\beta_t}{\gamma_t} \;\le\; \frac{\beta_t}{\alpha_t} \;\le\; \frac{1+\epsilon}{1-\epsilon} \;\le\; 2. \end{aligned}$$

Now apply Corollary E.2 with S_t instead of $[m]$, $v_i^{(t)}$ instead of v_i, α_t/γ_t instead of α, β_t/γ_t instead of β, and δ_t instead of δ. The hypotheses of Corollary E.2 are satisfied, so it follows that there is a set $S_{t+1} \subseteq S_t$ with

$$\alpha_t/\gamma_t - C\delta_t^{1/2} \;\preceq\; 2 \sum_{i \in S_{t+1}} v_i^{(t)} (v_i^{(t)})^{\mathsf{T}} \;\preceq\; \beta_t/\gamma_t + C\delta_t^{1/2}.$$

Rewriting in terms of the original v_i's, we obtain

$$\alpha_t - C\gamma_t\delta_t^{1/2} \;\preceq\; 2^{t+1} m \sum_{i \in S_{t+1}} v_i v_i^{\mathsf{T}} \;\preceq\; \beta_t + C\gamma_t\delta_t^{1/2}.$$

Now

$$\begin{aligned} \gamma_t\delta_t^{1/2} \;&=\; \gamma_t(n/|S_t|)^{1/2} \\ &=\; (2^t n)^{1/2}(\gamma_t)^{1/2} \\ &\le\; (2^t n)^{1/2}(\beta_t)^{1/2}. \end{aligned}$$

Hence

$$\alpha_{t+1} \;\preceq\; 2^{t+1} m \sum_{i \in S_{t+1}} v_i v_i^{\mathsf{T}} \;\preceq\; \beta_{t+1},$$

and the inductive step is achieved.

From the definition of v_i, Claim E.4 and (E.17) for $t = T$, we deduce that

$$m(1-\epsilon) \;\preceq\; 2^T n \sum_{i \in S_T} w_i w_i^{\mathsf{T}} \;\preceq\; m(1+\epsilon).$$

Recalling (E.16), we see that

$$(1-\epsilon)I \;\preceq\; \Theta(\epsilon^2) \sum_{i \in S_T} w_i w_i^{\mathsf{T}} \;\preceq\; (1+\epsilon)I.$$

Taking the trace of these inequalities shows that $|S_T| = \Theta(n/\epsilon^2)$. The proof is completed by taking y to be the characteristic vector of S_T. $\square$

COROLLARY E.5. *Let $w_1, \ldots, w_m \in \mathbb{R}^n$ satisfy $\|w_i\| = 1$ for all i. Let $p_1, \ldots, p_m$ be a probability distribution on these vectors such that the covariance matrix is $\sum_i p_i w_i w_i^{\mathsf{T}} = I/n$. For any $\epsilon \le 1/3$, there exists $z \in \mathbb{Z}_+^m$ with*

- $(1-\epsilon)I \preceq \Theta(\epsilon^2) \sum_i z_i w_i w_i^{\mathsf{T}} \preceq (1+\epsilon)I$,
- $\sum_i z_i = \Theta(n/\epsilon^2)$

Proof. We may assume that $p_1, \ldots, p_m$ are rational numbers of the form q_i/M where $q_1, \ldots, q_m, M$ are nonnegative integers. (If $p_1, \ldots, p_m$ are not rational, we may approximate them by rationals while introducing vanishing error.) Replace each w_i with q_i copies of itself. The uniform distribution on the resulting multiset of vectors still has covariance matrix I/n. Apply Claim E.3 to this multiset of vectors, yielding a vector y. Let z be the vector obtained in the obvious way from y to take multiplicities into account. $\square$

This easily implies a proof of Theorem 4.3.

Proof of Theorem 4.3. Apply Corollary E.5 with $\epsilon = 1/3$. Then $\Theta(1/\epsilon^2)I \preceq \sum_i z_i w_i w_i$, implying that $\{\, w_i \,:\, i \in \operatorname{supp}(z) \,\}$ spans $\mathbb{R}^n$. Choose $S \subseteq \operatorname{supp}(z)$ arbitrarily so that $\{\, w_i \,:\, i \in S \,\}$ is a basis of $\mathbb{R}^n$. Then

$$\sum_{i \in S} w_i w_i^{\mathsf{T}} \;\preceq\; \sum_i z_i w_i w_i^{\mathsf{T}} \;\preceq\; \Theta(1/\epsilon^2)I$$

as required. $\square$

Corollary E.5 implies that every graph has a spectral sparsifier with a linear number of edges. Let $G = (V, E)$ be a connected, unweighted graph with n vertices. As before, let L_G denote its Laplacian matrix, let R_{uv} denote the effective resistance between u and v, and let $C_{uv} = 1/R_{uv}$.

COROLLARY E.6. *For any $\epsilon \le 1/3$, there exists $z \in \mathbb{Z}_+^E$ with $\sum_{e \in E} z_e = \Theta(n/\epsilon^2)$ and*

$$(1-\epsilon)L_G \;\preceq\; \Theta(\epsilon^2)L' \;\preceq\; (1+\epsilon)L_G, \tag{E.19}$$

where

$$L' \;=\; \sum_{uv \in E} z_{uv} C_{uv} (e_u - e_v)(e_u - e_v)^{\mathsf{T}}.$$

Proof. As in the proof of Theorem 4.11, for $e = uv \in E$, let $x_e = L_G^{+/2}(e_u - e_v)$ and $w_e = x_e/\|x_e\|$. Then $p_e = R_e/(n-1)$ is a probability distribution on e and $\sum_e p_e w_e w_e^{\mathsf{T}} = I_{\operatorname{im} L_G}/(n-1)$. Applying Corollary E.5, we obtain a vector $z \in \mathbb{Z}_+^E$ with $\sum_e z_e = \Theta(n/\epsilon^2)$ and

$$(1-\epsilon)I_{\operatorname{im} L_G} \;\preceq\; \Theta(\epsilon^2) \sum_{e \in E} z_e w_e w_e^{\mathsf{T}} \;\preceq\; (1+\epsilon)I_{\operatorname{im} L_G}.$$

Multiply these inequalities on both sides by $L_G^{1/2}$ and use the identity $1/\|x_e\|^2 = C_e$ to obtain the desired conclusion. $\square$

Either Theorem 4.3 or Corollary E.6 can now be used to obtain a proof of Theorem 4.12.

Proof of Theorem 4.12. Apply Corollary E.6 with $\epsilon = 1/3$. The left-hand inequality of (E.19) implies that $\mathrm{supp}(z)$ forms a connected graph. Pick an arbitrary spanning tree T from $\mathrm{supp}(z)$. Then

$$\begin{aligned}
&\sum_{uv \in T} C_{uv}(e_u - e_v)(e_u - e_v)^{\mathsf{T}} \\
&\quad \preceq \sum_{uv \in E} z_{uv} C_{uv}(e_u - e_v)(e_u - e_v)^{\mathsf{T}} \\
&\quad \preceq \Theta(1/\epsilon^2) L_G.
\end{aligned}$$

As $\kappa \leq C_e$ for all edges e, we have $\sum_{uv \in T}(e_u - e_v)(e_u - e_v)^{\mathsf{T}} \preceq \Theta(1/\kappa) L_G$. $\square$