Pure and Applied Mathematics Quarterly
Volume 2, Number 4
(*Special Issue: In honor of
Robert MacPherson, Part 2 of 3*)
943—961, 2006

Approximating Orthogonal Matrices by Permutation Matrices

Alexander Barvinok

Abstract: Motivated in part by a problem of combinatorial optimization and in part by analogies with quantum computations, we consider approximations of orthogonal matrices U by "non-commutative convex combinations" A of permutation matrices of the type $A = \sum A_\sigma \sigma$, where σ are permutation matrices and A_σ are positive semidefinite $n \times n$ matrices summing up to the identity matrix. We prove that for every $n \times n$ orthogonal matrix U there is a non-commutative convex combination A of permutation matrices which approximates U entry-wise within an error of $cn^{-\frac{1}{2}} \ln n$ and in the Frobenius norm within an error of $c \ln n$. The proof uses a certain procedure of randomized rounding of an orthogonal matrix to a permutation matrix.

1. Introduction and main results

Let O_n be the orthogonal group and let S_n be the symmetric group. As is well known, S_n embeds in O_n by means of permutation matrices: with a permutation σ of $\{1, \ldots, n\}$ we associate the $n \times n$ *permutation matrix* $\pi(\sigma)$,

$$\pi_{ij}(\sigma) = \begin{cases} 1 & \text{if} \quad \sigma(j) = i \\ 0 & \text{otherwise.} \end{cases}$$

To simplify notation, we write σ instead of $\pi(\sigma)$, thus identifying a permutation with its permutation matrix and considering S_n as a subgroup of O_n. In this paper, we are interested in the following general question:

Received November 1, 2005.
1991 Mathematics subject Classification. 05A05, 52A20, 52A21, 46B09, 15A48, 15A60.
This research was partially supported by NSF Grant DMS 0400617. The author is grateful to Microsoft (Redmond) for hospitality during his work on this paper.
keywords and phrases orthogonal matrices, permutation matrices, positive semidefinite matrices, order statistics, measure concentration, Gaussian measure.

• How well are orthogonal matrices approximated by permutation matrices?

A related question is:

• Is there a reasonable way to "round" an orthogonal matrix to a permutation matrix, just like real numbers are rounded to integers?

To answer the second question, we suggest a simple procedure of *randomized rounding*, which, given an orthogonal matrix U produces not a single permutation matrix σ but rather a probability distribution on the symmetric group S_n. Using that procedure, we show that asymptotically, as $n \longrightarrow +\infty$, any orthogonal matrix U is approximated by a certain non-commutative convex combination, defined below, of the permutation matrices.

1.1. **Non-commutative convex hull.** Let $v_1, \ldots, v_m \in V$ be vectors, where V is a real vector space. A vector

$$v = \sum_{i=1}^{m} \lambda_i v_i \quad \text{where}$$

$$\sum_{i=1}^{m} \lambda_i = 1 \quad \text{and} \quad \lambda_i \geq 0 \quad \text{for} \quad i = 1, \ldots, m \tag{1.1}$$

is called a *convex combination* of $v_1, \ldots, v_m$. The set of all convex combinations of vectors from a given set $X \subset V$ is called the *convex hull* of X and denoted $\operatorname{conv}(X)$. We introduce the following extension of the convex hull, which we call the non-commutative convex hull.

Let V be a Hilbert space with the scalar product $\langle \cdot, \cdot \rangle$. Recall that a self-conjugate linear operator A on V is called *positive semidefinite* provided $\langle Av, v \rangle \geq 0$ for all $v \in V$. To denote that A is positive semidefinite, we write $A \succeq 0$. Let I denote the identity operator on V.

We say that v is a *non-commutative convex combination* of $v_1, \ldots, v_m$ if

$$v = \sum_{i=1}^{m} A_i v_i \quad \text{where}$$

$$\sum_{i=1}^{m} A_i = I \quad \text{and} \quad A_i \succeq 0 \quad \text{for} \quad i = 1, \ldots, m. \tag{1.2}$$

The set of all non-commutative convex combinations of vectors from a given set $X \subset V$ we call the *non-commutative convex hull* of X and denote $\operatorname{nconv}(X)$.

A result of M. Naimark [Na43] describes a general way to construct operators $A_i \succeq 0$ such that $A_1 + \ldots + A_m = I$. Namely, let $T : V \longrightarrow W$ be an embedding of Hilbert spaces and let $T^* : W \longrightarrow V$ be the corresponding projection. Let

$W = \bigoplus_{i=1}^{m} L_i$ be a decomposition of W into a direct sum of pairwise orthogonal subspaces and let $P_i : W \longrightarrow L_i$ be the orthogonal projections. We let $A_i = T^* P_i T$.

A set of non-negative numbers $\lambda_1, \ldots, \lambda_m$ summing up to 1 can be thought of as a probability distribution on the set $\{1, \ldots, m\}$. Similarly, a set of positive semidefinite operators A_i summing up to the identity matrix can be thought of as a measurement in a quantum system, see, for example, [Kr05]. While we can think of a convex combination of vectors as the expected value of a vector sampled from some set according to some probability distribution, we can think of a non-commutative convex combination as the expected measurement of a vector from the set.

It is clear that $\mathrm{nconv}(X)$ is a convex set and that

$$\mathrm{conv}(X) \subset \mathrm{nconv}(X)$$

since we get a regular convex combination (1.1) if we choose A_i in (1.2) to be the scalar operator of multiplication by λ_i.

1.2. **Convex hulls of the symmetric group and of the orthogonal group.** The convex hull of the permutation matrices $\sigma \in S_n$, described by the Birkhoff-von Neumann Theorem, consists of the $n \times n$ doubly stochastic matrices A, that is, non-negative matrices with all row and column sums equal to 1, see, for example, Section II.5 of [Ba02].

The convex hull of the orthogonal matrices $U \in O_n$ consists of all the operators of norm at most 1, that is, of the operators $A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ such that $\|Ax\| \leq \|x\|$ for all $x \in \mathbb{R}^n$, where $\|\cdot\|$ is the Euclidean norm on $\mathbb{R}^n$, see, for example, [Ha82].

In this paper, we consider the non-commutative convex hull $\mathrm{nconv}\,(S_n)$ of the symmetric group and show that asymptotically, as $n \longrightarrow +\infty$, it approximates all the orthogonal matrices. To state our main result, we consider the following two norms on matrices: the ℓ^∞ norm

$$\|B\|_\infty = \max_{i,j} |\beta_{ij}|$$

and the Frobenius or ℓ^2 norm

$$\|B\|_F = \left(\sum_{i,j=1}^{n} \beta_{ij}^2 \right)^{1/2},$$

where $B = (\beta_{ij})$.

We prove the following result.

Theorem 1.3. *For every orthogonal $n \times n$ matrix U there exist positive semi-definite $n \times n$ matrices $A_\sigma \succeq 0$, $\sigma \in S_n$, such that*

$$\sum_{\sigma \in S_n} A_\sigma = I,$$

where I is the $n \times n$ identity matrix, and such that for the non-commutative convex combination

$$A = \sum_{\sigma \in S_n} A_\sigma \sigma$$

we have

$$\|U - A\|_\infty \leq c \frac{\ln n}{\sqrt{n}}$$

and

$$\|U - A\|_F \leq c \ln n,$$

where c is an absolute constant.

1.4. **Discussion.** We consider $A_\sigma \sigma$ as the usual product of $n \times n$ matrices. Thus the matrix A_σ acts as a linear operator

$$X \longmapsto A_\sigma X$$

on the space Mat_n of $n \times n$ matrices X. Identifying

$$\text{Mat}_n = \underbrace{\mathbb{R}^n \oplus \cdots \oplus \mathbb{R}^n}_{n \text{ times}}$$

by slicing a matrix onto its columns, we identify the action of A_σ with the block-diagonal operator

$$\begin{pmatrix} A_\sigma & 0 & \ldots\ldots\ldots & 0 & 0 \\ 0 & A_\sigma & \ldots\ldots\ldots & 0 & 0 \\ \ldots & \ldots & \ldots\ldots\ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots\ldots\ldots & \ldots & \ldots \\ 0 & 0 & \ldots\ldots\ldots & A_\sigma & 0 \\ 0 & 0 & \ldots\ldots\ldots & 0 & A_\sigma \end{pmatrix}$$

on $\mathbb{R}^n \oplus \ldots \oplus \mathbb{R}^n$.

Hence the combination $\sum_\sigma A_\sigma \sigma$ indeed fits the definition of Section 1.1 of a non-commutative convex combination.

Let $v = (1, \ldots, 1)$ interpreted as a column vector. Then, for any $A = \sum_\sigma A_\sigma \sigma$ where $\sum_\sigma A_\sigma = I$, we have $Av = v$. In particular, if U is a matrix such that $Uv \neq v$ then U cannot be exactly equal to A, so the asymptotic character of Theorem 1.3 is unavoidable. Taking $U = -I$ we note that one cannot approximate U entry-wise better than within $1/n$ error, say. If U is a "typical" orthogonal matrix, then we have $\|U\|_\infty \approx c_1 \sqrt{n^{-1} \ln n}$ for some absolute constant c_1, cf., for example, Chapter 5 of [MS86]. It follows from our proof that for such a typical U we will have $\|U - A\|_\infty \leq c_2 n^{-1} \ln n$ for some other absolute constant c_2.

We also note that $\|U\|_F = \sqrt{n}$ for every $U \in O_n$, so the error in the Frobenius norm is exponentially small compared to the norm of the matrix.

It is a legitimate question whether the bounds in Theorem 1.3 can be sharpened.

One can ask what kind of matrices one can expect to get via non-commutative convex combinations

$$A = \sum_{\sigma \in S_n} A_\sigma \sigma$$

of permutation matrices. It is easy to notice that the resulting matrices A can be quite far away from the (usual) convex hull of the orthogonal matrices. Consider, for example, the following situation: for the identity permutation σ, let A_σ be the projection onto the first coordinate, for every transposition $\sigma = (1k)$, $k = 2, \ldots, n$, let A_σ to be the projection onto the kth coordinate, and for all other σ, let $A_\sigma = 0$. Then, for $A = (\alpha_{ij})$ we have $\alpha_{1i} = 1$ for all i and all other entries of A are 0. Thus the operator norm of A is $\sqrt{n}$.

1.5. **Rounding an orthogonal matrix to a permutation matrix.** The key construction used in the proof of Theorem 1.3 is that of a randomized rounding of an orthogonal matrix to a permutation matrix. By now, the idea of randomized rounding (be it the rounding of a real number to an integer or the rounding of a positive semidefinite matrix to a vector) proved itself to be extremely useful in optimization and other areas; see, for example, [MR95]. Let U be an $n \times n$ orthogonal matrix and let $x \in \mathbb{R}^n$ be a vector. Let $y = Ux$, so

$$x = (\xi_1, \ldots, \xi_n) \quad \text{and} \quad y = (\eta_1, \ldots, \eta_n).$$

Suppose that the coordinates ξ_i of x are distinct and that the coordinates η_i of y are distinct. Let $\phi, \psi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ be the orderings of the coordinates of x and y respectively:

$$\xi_{\phi(1)} < \xi_{\phi(2)} < \ldots < \xi_{\phi(n)} \quad \text{and} \quad \eta_{\psi(1)} < \eta_{\psi(2)} < \ldots < \eta_{\psi(n)}.$$

We define the *rounding of U at x* as the permutation $\sigma = \sigma(U, x)$, $\sigma \in S_n$, such that

$$\sigma\big(\phi(k)\big) = \psi(k) \quad \text{for} \quad k = 1, \ldots, n.$$

In words: $\sigma = \sigma(U, x)$ matches the kth smallest coordinate of x with the kth smallest coordinate of $y = Ux$ for $k = 1, \ldots, n$.

Let μ_n be the standard Gaussian measure on $\mathbb{R}^n$ with the density

$$(2\pi)^{-n/2} e^{-\|x\|^2/2} \quad \text{where} \quad \|x\|^2 = \xi_1^2 + \ldots + \xi_n^2 \quad \text{for} \quad x = (\xi_1, \ldots, \xi_n).$$

If we sample $x \in \mathbb{R}^n$ at random with respect to μ_n then with probability 1 the coordinates of x are distinct and the coordinates of $y = Ux$ are distinct. Thus the rounding $\sigma(U, x)$ is defined with probability 1. Fixing U and choosing x at random, we obtain a certain probability distribution on the symmetric group S_n.

The crucial observation is that for a typical x, the vector $y = Ux$ is very close to the vector σx for $\sigma = \sigma(U, x)$. In other words, the action of a given orthogonal matrix on a random vector x with high probability is very close to a permutation of the coordinates. However, the permutation varies as x varies.

We prove the following result.

Theorem 1.6. *Let U be an $n \times n$ orthogonal matrix. For $x \in \mathbb{R}^n$, let $\sigma(U, x) \in S_n$ be the rounding of U at x. Let $z(x) = x - \sigma(U, x)x$ and let $\zeta_i(x)$ be the ith coordinate of $z(x)$. Then*

$$\int_{\mathbb{R}^n} \zeta_i^2(x) \; d\mu_n(x) \leq c \frac{\ln^2 n}{n}$$

for some absolute constant c and $i = 1, \ldots, n$.

1.7. **Discussion.** It follows from Theorem 1.6 that

$$\int_{\mathbb{R}^n} \|z(x)\|^2 \; d\mu_n(x) \leq c \ln^2 n.$$

Thus, for a typical $x \in \mathbb{R}^n$, we should have

$$\|Ux - \sigma(U, x)x\| = O\left(\ln n\right).$$

This should be contrasted with the fact that for a typical $x \in \mathbb{R}^n$ we have

$$\|x\| \approx n^{1/2}.$$

Indeed, for any $0 < \epsilon < 1$, we have

$$\mu_n\Big\{x \in \mathbb{R}^n : \quad \|x\|^2 > \tfrac{n}{1-\epsilon}\Big\} \leq \exp\left\{-\tfrac{\epsilon^2 n}{4}\right\} \quad \text{and}$$
$$\mu_n\Big\{x \in \mathbb{R}^n : \quad \|x\|^2 \leq (1-\epsilon)n\Big\} \leq \exp\left\{-\tfrac{\epsilon^2 n}{4}\right\},$$

see, for example, Section V.5 of [Ba02].

Thus, for on a typical x, the action of operator U and the permutation $\sigma(U, x)$ do not differ much. The paper is structured as follows.

In Section 2, we discuss some general properties of the proposed randomized rounding and its possible application in the Quadratic Assignment Problem, a hard problem of combinatorial optimization.

In Section 3, we establish concentration inequalities for the order statistics of the Gaussian distribution on which the proof of Theorem 1.6 is based.

In Section 4, we prove Theorem 1.6.

In Section 5, we deduce Theorem 1.3 from Theorem 1.6.

In Section 6, we conclude with some general remarks.

2. Randomized rounding

The procedure described in Section 1.5 satisfies some straightforward properties that one expects a rounding procedure to satisfy. Given a matrix $U \in O_n$, the rounding $\sigma(U,x) \in S_n$ for $x \in \mathbb{R}^n$ is well-defined with probability 1. Thus as x ranges over $\mathbb{R}^n$, with every orthogonal matrix U we associate a probability distribution p_U on S_n:

$$p_U(\sigma) = \mu_n \Big\{ x \in \mathbb{R}^n : \quad \sigma(U,x) = \sigma \Big\}.$$

In other words, $p_U(\sigma)$ tells us how often do we get a particular permutation $\sigma \in S_n$ as a rounding of U. For example, if $U = -I$ then p_U is uniform on the permutations σ that are the products of $\lfloor n/2 \rfloor$ commuting transpositions: $\sigma(-I,x)$ is the permutation matching the kth smallest coordinate of x to its $(n-k)$th smallest coordinate.

We note that if U is a permutation matrix itself, then $\sigma(U,x) = U$ with probability 1, so permutation matrices are rounded to themselves. By continuity, if U is close to a permutation matrix, one can expect that the distribution p_U concentrates around that permutation matrix. One can also show that if U is "local", that is, acts on some set J of $k \ll n$ coordinates of x then $\sigma(U,x)$ is also "local" with high probability, that is, acts on some $s \ll n$ coordinates containing J.

If $\rho \in S_n$ is a permutation then $\sigma(\rho U, x) = \rho\sigma(U,x)$. Therefore, if we fix $x \in \mathbb{R}^n$ with distinct coordinates and sample U at random from the Haar probability measure on O_n, we get a probability distribution on S_n which is invariant under left multiplication by S_n and hence is the uniform distribution. Thus, for any fixed $x \in \mathbb{R}^n$ with distinct coordinates, the rounding of a random matrix $U \in O_n$ is a random permutation $\sigma \in S_n$. Geometrically, every such an x produces a partition of O_n onto $n!$ isometric regions, each consisting of the matrices rounded at x to a given permutation $\sigma \in S_n$.

We also note that $\sigma(U,x) = \sigma(U,-x)$.

2.1. **Rounding in the Quadratic Assignment Problem.** Let us define the scalar product on the space Mat_n of real $n \times n$ matrices by

$$\big\langle A, B \big\rangle = \sum_{i,j} a_{ij} b_{ij} \quad \text{for} \quad A = (a_{ij}) \quad \text{and} \quad B = (b_{ij}) \,.$$

Given two $n \times n$ matrices A and B, let us consider the function $f : S_n \longrightarrow \mathbb{R}$ defined by

$$f(\sigma) = \langle A,\ \sigma B \sigma^{-1} \rangle$$

(recall that we identify σ with its permutation matrix). The problem of minimizing f over S_n, known as the *Quadratic Assignment Problem*, is one of the hardest combinatorial optimization problems, see [Çe98]. It has long been known that if one of the matrices is symmetric (in which case the other can be replaced by its symmetric part, so we may assume that both A and B are symmetric), then an easily computable "eigenvalue bound" is available. Namely, let

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$$

be the eigenvalues of A and let

$$\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n$$

be the eigenvalues of B. Then the minimum value of f is at least

$$\sum_{i=1}^{n} \lambda_i \mu_{n-i}. \tag{2.1}$$

The bound (2.1) comes from extending the function $f : S_n \longrightarrow \mathbb{R}$ to the function $f : O_n \longrightarrow \mathbb{R}$ defined by

$$f(U) = \langle A,\ UBU^* \rangle.$$

It is then easy to compute the minimum of f on O_n.

First, we compute U_1 such that $U_1 B U_1^* = \operatorname{diag}(\mu_1, \ldots, \mu_n)$ is the diagonal matrix. Next, we notice that

$$\begin{aligned} f(U) &= \langle A,\ UBU^* \rangle = \langle A,\ (UU_1^*)U_1BU_1^*(U_1U^*) \rangle \\ &= \langle U_1U^*AUU_1^*,\ U_1BU_1^* \rangle. \end{aligned}$$

It is then easy to see that the minimum of $f(U)$ is achieved when $U_1U^* = U_2$ such that $U_2AU_2^* = \operatorname{diag}(\lambda_n, \ldots, \lambda_1)$. Then we compute $U = U_2^*U_1$.

The eigenvalue bound (2.1) may be far off the minimum of f on S_n, in which case one would expect the optimal matrix $U \in O_n$ to be far away from a single permutation matrix. Suppose, for example, that $n = 2m$ is even. Let J be the $m \times m$ matrix of all 1's and let

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes J \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes J.$$

Then $f(\sigma) \equiv 0$ on S_n while the values of f on O_n range from $-n^2/2$ to $n^2/2$.

However, if U is close to a particular permutation matrix, that matrix may be recovered by rounding.

3. Concentration for order statistics

Let $\xi_1, \ldots, \xi_n$ be independent identically distributed real valued random variables. We define their *order statistics* as the random variables $\omega_1, \ldots, \omega_n$, $\omega_k = \omega_k(\xi_1, \ldots, \xi_n)$ such that

$$\omega_k(\xi_1, \ldots, \xi_n) = \quad \text{the } k\text{th smallest among} \quad \xi_1, \ldots, \xi_n.$$

Thus ω_1 is the smallest among $\xi_1, \ldots, \xi_n$ and ω_n is the largest among $\xi_1, \ldots, \xi_n$. We have

$$\omega_1 \leq \omega_2 \leq \ldots \leq \omega_n.$$

We need some concentration inequalities for order statistics.

Lemma 3.1. *Suppose that the cumulative distribution function F of ξ_i is continuous and strictly increasing. Let k be an integer, $1 \leq k \leq n$.*

(1) Let α be a number such that $F(\alpha) < k/n < 2F(\alpha)$. Then

$$\mathbf{P}\big\{\omega_k < \alpha\big\} \leq \exp\left\{-\frac{n}{3F(\alpha)}\left(\frac{k}{n} - F(\alpha)\right)^2\right\}.$$

(2) Let α be a number such that $F(\alpha) > k/n$. Then

$$\mathbf{P}\big\{\omega_k > \alpha\big\} \leq \exp\left\{-\frac{n}{2F(\alpha)}\left(\frac{k}{n} - F(\alpha)\right)^2\right\}.$$

Proof. Let us define random variables $\chi_1, \ldots, \chi_n$ by

$$\chi_i = \begin{cases} 1 & \text{if} \quad \xi_i < \alpha \\ 0 & \quad \text{otherwise} \end{cases}$$

and let $\chi = \chi_1 + \ldots + \chi_n$.

Thus χ_i are independent random variables and

$$\mathbf{P}\Big\{\chi_i = 1\Big\} = F(\alpha) = p.$$

We note that $\omega_k < \alpha$ if and only if $\chi \geq k$. By Chernoff's inequality (see, for example, [Mc89] or [Bo91]) we get for $0 < \epsilon < 1$

$$\mathbf{P}\Big\{\chi \geq pn(1+\epsilon)\Big\} \leq \exp\left\{-\frac{\epsilon^2 pn}{3}\right\}.$$

Choosing

$$\epsilon = \frac{k}{pn} - 1 = \frac{k}{F(\alpha)n} - 1$$

we complete the proof in Part (1).

Similarly in Part (2), we have $\omega_k \geq \alpha$ if and only if $\chi \leq k-1$. By Chernoff's inequality we get for $0 < \epsilon < 1$

$$\mathbf{P}\Big\{\chi \leq pn(1-\epsilon)\Big\} \leq \exp\left\{-\frac{\epsilon^2 pn}{2}\right\}.$$

Choosing

$$\epsilon = 1 - \frac{k}{pn} = 1 - \frac{k}{F(\alpha)n},$$

we complete the proof of Part (2). $\square$

3.2. **Corollary.**

(1) Let k be an integer, $1 \leq k \leq n$. For $0 < \epsilon < 1/2$, let us define the number $\alpha^- = \alpha^-(k, \epsilon)$ from the equation

$$F\left(\alpha^-\right) = \frac{(1-\epsilon)k}{n}.$$

Then

$$\mathbf{P}\big\{\omega_k < \alpha^-\big\} \leq \exp\left\{-\frac{\epsilon^2 k}{3(1-\epsilon)}\right\}.$$

(2) Let $1 \leq k \leq n/2$ be an integer. For $0 < \epsilon < 1$, let us define the number $\alpha^+ = \alpha^+(k, \epsilon)$ from the equation

$$F\left(\alpha^+\right) = \frac{(1+\epsilon)k}{n}.$$

Then

$$\mathbf{P}\big\{\omega_k > \alpha^+\big\} \leq \exp\left\{-\frac{\epsilon^2 k}{2(1+\epsilon)}\right\}.$$

Next, we consider the case of the identically distributed standard Gaussian random variables with the density

$$\phi(t) = \frac{1}{\sqrt{2\pi}} e^{-t^2/2}$$

and the cumulative distribution function

$$F(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\tau^2/2}\, d\tau.$$

Lemma 3.3. *Let $\xi_1, \ldots, \xi_n$ be independent standard Gaussian random variables. Let $1 \leq k \leq n/2$ be an integer. Let $0 < \epsilon < 1/2$ be a number and let us define numbers $\alpha^+ = \alpha^+(k, \epsilon)$ and $\alpha^- = \alpha^-(k, \epsilon)$ from the equations*

$$F\left(\alpha^+\right) = \frac{(1+\epsilon)k}{n} \quad \text{and} \quad F\left(\alpha^-\right) = \frac{(1-\epsilon)k}{n}.$$

Then

(1)

$$\mathbf{P}\Big\{\omega_k < \alpha^-\Big\} \leq \exp\left\{-\frac{\epsilon^2 k}{3}\right\} \quad \textit{and} \quad \mathbf{P}\Big\{\omega_k > \alpha^+\Big\} \leq \exp\left\{-\frac{\epsilon^2 k}{3}\right\};$$

(2)

$$0 \leq \alpha^+ - \alpha^- \leq \frac{\epsilon\sqrt{8\pi}}{1-\epsilon}.$$

Proof. Part (1) is immediate from Corollary 3.2. Clearly, $\alpha^+ - \alpha^- \geq 0$. Applying Rolle's Theorem we get

$$\frac{2k\epsilon}{n} = F\left(\alpha^+\right) - F\left(\alpha^-\right) = \left(\alpha^+ - \alpha^-\right)\phi(t^*) \quad \text{for some} \quad \alpha^- < t^* < \alpha^+.$$

Using the inequality

$$F(\alpha) < e^{-\alpha^2/2} = \sqrt{2\pi}\phi(\alpha) \quad \text{for} \quad \alpha \leq 0$$

(cf. also formula (4.2) below), we get

$$\phi(t) \geq \frac{F(t)}{\sqrt{2\pi}} \geq \frac{1}{\sqrt{2\pi}} \frac{(1-\epsilon)k}{n} \quad \text{for} \quad \alpha^- < t \leq 0.$$

By symmetry,

$$\phi(t) \geq \frac{1}{\sqrt{2\pi}} \frac{(1-\epsilon)k}{n} \quad \text{for} \quad 0 \leq t < \alpha^+.$$

Summarizing,

$$\alpha^+ - \alpha^- = \frac{2k\epsilon}{n\phi(t^*)} \leq \frac{\epsilon\sqrt{8\pi}}{1-\epsilon}$$

and the proof of Part (2) follows. □

4. Proof of Theorem 1.6

We need a technical (non-optimal) estimate.

Lemma 4.1. *Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a function such that $f(\lambda x) = \lambda f(x)$ for all $x \in \mathbb{R}^n$ and all $\lambda \geq 0$. Let*

$$B = \Big\{x \in \mathbb{R}^n : \quad \|x\| \leq n\Big\}$$

be a ball of radius n and let μ_n be the standard Gaussian measure on $\mathbb{R}^n$. Then there exists a constant c such that

$$\int_{\mathbb{R}^n} f^2 \, d\mu_n \leq c \int_B f^2 \, d\mu_n$$

for all n.

Proof. Let $S \subset \mathbb{R}^n$ be the unit sphere. Passing to the polar coordinates, we get

$$\int_{\mathbb{R}^n} f^2 \ d\mu_n = (2\pi)^{-n/2} \left(\int_S f^2 \ dx \right) \int_0^{+\infty} t^{n+1} e^{-t^2/2} \ dt$$

and, similarly,

$$\int_B f^2 \ d\mu_n = (2\pi)^{-n/2} \left(\int_S f^2 \ dx \right) \int_0^{n} t^{n+1} e^{-t^2/2} \ dt.$$

Furthermore, we have

$$\int_0^{+\infty} t^{n+1} e^{-t^2/2} \ dt = 2^{n/2} \Gamma \left(\frac{n+2}{2} \right).$$

For all sufficiently large n, we have

$$t^{n+1} e^{-t^2/2} \leq e^{-t^2/4} \quad \text{for all} \quad t > n,$$

so we have

$$\int_n^{+\infty} t^{n+1} e^{-t^2/2} \ dt \leq c$$

for some constant c and all n. The proof now follows. □

Apart from Lemma 4.1, we need the estimate:

$$\mu_n \Big\{ x = (\xi_1, \ldots, \xi_n) : \quad |\xi_i| > t \Big\} \leq 2 e^{-t^2/2} \tag{4.2}$$

for any $t \geq 0$ and any $i = 1, \ldots, n$, see, for example, Section V.5 of [Ba02]. Now we can prove Theorem 1.6.

Proof of Theorem 1.6 Let B be the ball of radius n in $\mathbb{R}^n$ centered at the origin. By Lemma 4.1 it suffices to prove the estimate for the integral

$$\int_B \zeta_i^2(x) \ d\mu_n(x).$$

Without loss of generality, we may assume that $i = 1$ so that $\zeta(x) = \zeta_1(x)$ is the first coordinate of $Ux - \sigma(U, x)x$.

Let $V_k \subset B$ be the subset of $x \in B$ such the first coordinate of Ux is the kth smallest among the coordinates of Ux. Geometrically, each V_k is the intersection of B with a union of some $(n-1)!$ cones from the collection of the $n!$ non-overlapping polyhedral cones corresponding to the possible orderings of the coordinates of Ux. The sets V_k cover B and intersect only at boundary points and since B is O_n-invariant, we have

$$\mu_n(V_1) = \ldots = \mu_n(V_n) = \frac{\mu_n(B)}{n} < \frac{1}{n}.$$

Thus we have

$$\int_B \zeta^2(x)\ d\mu_n(x) = \sum_{k=1}^n \int_{V_k} \zeta^2(x)\ d\mu_n(x).$$

In what follows, c_i for $i = 1, 2, \ldots$ denote various absolute constants.

We note that for any $x \in B$ we have $|\zeta(x)| \leq 2n$. Moreover, by (4.2)

$$\mu_n\Big\{x \in V_k : \quad |\zeta(x)| \geq c_1\sqrt{\ln n}\Big\} \leq n^{-3} \quad \text{for all} \quad n.$$

Therefore,

$$\int_{V_k} \zeta^2(x)\ d\mu_n(x) \leq c_2\frac{\ln n}{n} \quad \text{for all} \quad k. \tag{4.3}$$

For

$$36\ln n < k \leq n/2$$

and all n we get a better estimate via Lemma 3.3. Namely, let us choose $\epsilon = \epsilon_k = 3k^{-1/2}\sqrt{\ln n}$ in Lemma 3.3 and let α_k^+ and α_k^- be the corresponding bounds. It follows that for $36\ln n < k \leq n/2$ and all sufficiently large n we have

$$\mu_n\Big\{x \in \mathbb{R}^n : \quad \omega_k(x) \notin [\alpha_k^-, \alpha_k^+]\Big\} \leq n^{-3}$$

and, similarly,

$$\mu_n\Big\{x \in \mathbb{R}^n : \quad \omega_k(Ux) \notin [\alpha_k^-, \alpha_k^+]\Big\} \leq n^{-3},$$

where

$$0 \leq \alpha_k^+ - \alpha_k^- \leq c_3 k^{-\frac{1}{2}}\sqrt{\ln n}.$$

Hence

$$\mu_n\Big\{x \in \mathbb{R}^n : \quad |\omega_k(Ux) - \omega_k(x)| > c_3 k^{-\frac{1}{2}}\sqrt{\ln n}\Big\} \leq 2n^{-3}.$$

Since for $x \in V_k$ we have $\zeta(x) = \omega_k(Ux) - \omega_k(x)$, we conclude

$$\mu_n\Big\{x \in V_k : \quad |\zeta(x)| > c_3 k^{-\frac{1}{2}}\sqrt{\ln n}\Big\} \leq 2n^{-3}$$

and

$$\int_{V_k} \zeta^2(x)\ d\mu_n(x) \leq c_4\frac{\ln n}{kn} \quad \text{for} \quad 36\ln n < k \leq n/2 \tag{4.4}$$

and all n.

Summarizing (4.3) and (4.4), we get

$$\begin{aligned}&\sum_{1\le k\le n/2}\int_{V_k}\zeta^2(x)\ d\mu_n(x)\\ =&\sum_{1\le k\le 36\ln n}\int_{V_k}\zeta^2(x)\ d\mu_n(x)+\sum_{36\ln n<k\le n/2}\int_{V_k}\zeta^2(x)\ d\mu_n(x)\\ \le&\ c_5\frac{\ln^2 n}{n}.\end{aligned}$$

Since by the symmetry $x\leftrightarrow -x$ we have

$$\int_{V_k}\zeta^2(x)\ d\mu_n(x)=\int_{V_{n-k}}\zeta^2(x)\ d\mu_n(x),$$

the proof follows. □

5. Proof of Theorem 1.3

First, we introduce some notation.

For vectors $x=(\xi_1,\ldots,\xi_n)$ and $y=(\eta_1,\ldots,\eta_n)$ let $x\otimes y$ be the $n\times n$ matrix with the (i,j)th entry equal to $\xi_i\eta_j$.

We observe that for any $n\times n$ matrix A we have

$$A(x\otimes y)=(Ax)\otimes y,$$

where the product in the left hand side we interpret as the product of matrices and the product Ax in the right hand side we interpret as a product of a matrix and a column vector.

Let

$$\langle x,y\rangle=\sum_{i=1}^n\xi_i\eta_i\quad\text{for}\quad x=(\xi_1,\ldots,\xi_n)\quad\text{and}\quad y=(\eta_1,\ldots,\eta_n)$$

be the standard scalar product in $\mathbb{R}^n$. Then for all $x,y,a\in\mathbb{R}^n$, we have

$$(x\otimes y)\,a=\langle a,y\rangle x. \tag{5.1}$$

Let

$$\|x\|=\sqrt{\langle x,x\rangle}\quad\text{for}\quad x\in\mathbb{R}^n$$

be the usual Euclidean norm of a vector.

We need a couple of technical results.

Lemma 5.2. *Let L be an $n\times n$ matrix. Then*

$$\|L\|_F^2=\int_{\mathbb{R}^n}\|La\|^2\ d\mu_n(a).$$

Proof. Let $a = (\alpha_1, \ldots, \alpha_n)$, where α_i are independent standard Gaussian random variables. Then

$$\|La\|^2 = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} l_{ij}\alpha_j \right)^2 .$$

Since $\mathbf{E}\, \alpha_i \alpha_j = 0$ for $i \neq j$ and $\mathbf{E}\, \alpha_j^2 = 1$, taking the expectation we get

$$\mathbf{E}\, \|La\|^2 = \sum_{i,j=1}^{n} l_{ij}^2.$$

□

Lemma 5.3. *For every* $f \in L^2(\mathbb{R}^n, \mu_n)$ *we have*

$$\int_{\mathbb{R}^n} \left(\int_{\mathbb{R}^n} \langle a, x\rangle f(x)\ d\mu_n(x) \right)^2\ d\mu_n(a) \leq \int_{\mathbb{R}^n} f^2(x)\ d\mu_n(x).$$

Proof. Let $\mathcal{L} \subset L^2(\mathbb{R}^n, \mu_n)$ be the subspace consisting of the linear functions and let $\mathcal{L}^\perp$ be its orthogonal complement. We write

$$f(x) = \langle b, x\rangle + h(x),$$

where $b \in \mathbb{R}^n$ and $h \in \mathcal{L}^\perp$.

Hence we have

$$\int_{\mathbb{R}^n} f^2(x)\ d\mu_n(x) \geq \int_{\mathbb{R}^n} \langle b, x\rangle^2\ d\mu_n(x) = \langle b, b\rangle$$

and

$$\int_{\mathbb{R}^n} \langle a, x\rangle f(x)\ d\mu_n(x) = \int_{\mathbb{R}^n} \langle a, x\rangle \langle b, x\rangle\ d\mu_n(x) = \langle a, b\rangle.$$

Therefore,

$$\int_{\mathbb{R}^n} \left(\int_{\mathbb{R}^n} \langle a, x\rangle f(x)\ d\mu_n(x) \right)^2\ d\mu_n(a) = \int_{\mathbb{R}^n} \langle a, b\rangle^2\ d\mu_n(a)$$
$$= \langle b, b\rangle \leq \int_{\mathbb{R}^n} f^2(x)\ d\mu_n(x)$$

as claimed. □

Now we are ready prove Theorem 1.3.

Proof of Theorem 1.3. Given an orthogonal matrix U, we will construct a matrix A approximating U as desired in the form

$$A = \sum_{\sigma \in S_n} \sigma A_\sigma, \quad \text{where} \quad \sum_{\sigma \in S_n} A_\sigma = I \quad \text{and} \quad A_\sigma \succeq 0.$$

To get the approximation of the type

$$A = \sum_{\sigma \in S_n} A_\sigma \sigma$$

claimed in the Theorem, one should apply the construction to U^*.

Let $\sigma(U, x)$ be the rounding of U at x and let us define

$$X_\sigma = \Big\{ x \in \mathbb{R}^n : \quad \sigma(U, x) = \sigma \Big\} \quad \text{for} \quad \sigma \in S_n$$

and

$$A_\sigma = \int_{X_\sigma} x \otimes x \; d\mu_n(x).$$

Clearly, A_σ are positive semidefinite and

$$\sum_{\sigma \in S_n} A_\sigma = \int_{\mathbb{R}^n} x \otimes x \; d\mu_n(x) = I.$$

On the other hand,

$$\begin{aligned} U - \sum_\sigma \sigma A_\sigma &= \int_{\mathbb{R}^n} (Ux) \otimes x \; d\mu_n(x) - \sum_{\sigma \in S_n} \sigma \int_{X_\sigma} x \otimes x \; d\mu_n(x) \\ &= \int_{\mathbb{R}^n} (Ux) \otimes x \; d\mu_n(x) - \sum_{\sigma \in S_n} \int_{X_\sigma} \sigma(x) \otimes x \; d\mu_n(x) \\ &= \int_{\mathbb{R}^n} (Ux - \sigma(U, x)x) \otimes x \; d\mu_n(x). \end{aligned}$$

Let

$$L = \int_{\mathbb{R}^n} (Ux - \sigma(U, x)x) \otimes x \; d\mu_n(x) = \int_{\mathbb{R}^n} z(x) \otimes x \; d\mu_n(x)$$

in the notation of Theorem 1.3. Thus L is an $n \times n$ matrix, $L = (l_{ij})$ and

$$U - A = L.$$

Using Theorem 1.6, we estimate l_{ij}. Denoting $\xi_j(x)$ the jth coordinate of x, we get from Theorem 1.6

$$
\begin{aligned}
|l_{ij}| &= \Big| \int_{\mathbb{R}^n} \zeta_i(x)\xi_j(x)\ d\mu_n(x) \Big| \\
&\leq \left(\int_{\mathbb{R}^n} \zeta_i^2(x)\ d\mu_n(x) \right)^{1/2} \left(\int_{\mathbb{R}^n} \xi_j^2(x)\ d\mu_n(x) \right)^{1/2} \leq c \frac{\ln n}{\sqrt{n}},
\end{aligned}
$$

from which we get

$$\|U - A\|_\infty \leq c \frac{\ln n}{\sqrt{n}}$$

as desired.

Finally, we estimate

$$\|U - A\|_F = \|L\|_F$$

using Lemma 5.2. By formula (5.1) for $a \in \mathbb{R}^n$ we have

$$La = \int_{\mathbb{R}^n} \langle a, x \rangle \left(Ux - \sigma(U, x)x \right)\ d\mu_n(x) = \int_{\mathbb{R}^n} \langle a, x \rangle z(x)\ d\mu_n(x)$$

in the notation of Theorem 1.6. Let us estimate

$$\int_{\mathbb{R}^n} \|La\|^2\ d\mu_n(a).$$

The ith coordinate $\lambda_i(a)$ of La is

$$\lambda_i(a) = \int_{\mathbb{R}^n} \langle a, x \rangle \zeta_i(x)\ d\mu_n(x).$$

By Lemma 5.3,

$$
\begin{aligned}
\int_{\mathbb{R}^n} \lambda_i^2(a)\ d\mu_n(a) &= \int_{\mathbb{R}^n} \left(\int_{\mathbb{R}^n} \langle a, x \rangle \zeta_i(x)\ d\mu_n(x) \right)^2\ d\mu_n(a) \\
&\leq \int_{\mathbb{R}^n} \zeta_i^2(x)\ d\mu_n(x) \leq c \frac{\ln^2 n}{n}
\end{aligned}
$$

by Theorem 1.3. Therefore,

$$\|L\|_F^2 = \int_{\mathbb{R}^n} \|La\|^2\ d\mu_n(a) = \sum_{i=1}^n \int_{\mathbb{R}^n} \lambda_i^2(a)\ d\mu_n(a) \leq c \ln^2 n$$

as desired. □

6. Concluding remarks

A somewhat stronger estimate follows from our proof of Theorem 1.3. Namely, let $u_1, \ldots, u_n$ be the column vectors of U and let $a_1, \ldots, a_n$ be the column vectors of A. Then

$$\|u_i - a_i\| \leq c\frac{\ln n}{\sqrt{n}} \quad \text{for} \quad i = 1, \ldots, n,$$

where $\| \cdot \|$ is the Euclidean norm in $\mathbb{R}^n$.

It follows from our construction of matrices A_σ in the proof of Theorem 1.3 that the value of $n^{-1}\,(\operatorname{trace} A_\sigma)$ equals to the probability that the matrix U^* is rounded to the permutation σ^{-1}.

One can easily construct small approximate non-commutative convex combinations

$$U \approx \sum_{i=1}^{N} A_i \sigma_i$$

with

$$A_i \succeq 0 \quad \text{and} \quad \sum_{i=1}^{N} A_i \approx I$$

by sampling N points x_i at random from the Gaussian distribution μ_n, computing the rounding $\sigma_i = \sigma^{-1}\,(U^*, x_i)$ and letting $A_i = x_i \otimes x_i$.

References

[Ba] A. Barvinok,*A Course in Convexity*, Graduate Studies in Mathematics, vol. 54, American Mathematical Society, Providence, RI, 2002.

[Bo91] B. Bollobás, Random graphs, Probabilistic combinatorics and its applications (San Francisco, CA, 1991), Proc. Sympos. Appl. Math. vol.44, Amer. Math. Soc., Providence, RI, 1991, PP.1–20.

[Çe98] E. Çela, *The Quadratic Assignment problem.* Theory and Algorithms, Combinatorial Optimization, vol. 1, Kluwer Academic Publishers, Dordrecht, 1998.

[Ha82] P.R. Halmos, *A Hilbert Space Problem Book. Second edition*, Graduate Texts in Mathematics, vol. 19. Encyclopedia of Mathematics and its Applications, vol. 17, Springer-Verlag, New York-Berlin, 1982.

[Kr05] D.W. Kribs, *A quantum computing primer for operator theorists*, Linear Algebra Appl., vol. 400, (2005) 147–167

[Mc89] C. McDiarmid, *On the method of bounded differences*, Surveys in combinatorics 1989 (Norwich, 1989), London Math. Soc. Lecture Note Ser., vol. 141, Cambridge Univ. Press, Cambridge, 1989,PP.148–188.

[MR95] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, Cambridge, 1995.

[MS86] V.D. Milman and G. Schechtman *Asymptotic Theory of Finite-Dimensional Normed Spaces. With an appendix by M. Gromov*, Lecture Notes in Mathematics, vol. 1200, Springer-Verlag , Berlin, 1986.

[Na43] M.A. Naimark, *On a representation of additive operator set functions*, C. R. (Doklady) Acad. Sci. URSS (N.S.), vol. 41(1943), 359–361

Alexander Barvinok
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1043
E-mail: barvinok@umich.edu