Asymptotic entropic uncertainty relations

Radosław Adamczak and Rafał Łatała
Institute of Mathematics, University of Warsaw, ul. Banacha 2, PL-02-097 Warsaw, Poland

Zbigniew Puchała
Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, ul. Batycka 5, 44-100 Gliwice, Poland and
Institute of Physics, Jagiellonian University, ul. Lojasiewicza 11, 30-059 Kraków, Poland

Karol Życzkowski
Institute of Physics, Jagiellonian University, ul. Lojasiewicza 11, 30-059 Kraków, Poland and
Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, PL-02-668 Warsaw, Poland

(Dated: December 22, 2014)

Entropic uncertainty relations are analyzed for the case of $N$-dimensional Hilbert space and two orthogonal measurements performed in two generic bases, related by a Haar random unitary matrix $U$. We derive estimations for the average norms of truncations of $U$ of a given size, which allow us to study state-independent lower bounds for the sum of two entropies describing the measurements outcomes. In particular, we show that the Maassen-Unflik bound asymptotically behaves as $\ln N - \ln \ln N - \ln 2$, while the strong entropic majorization relation yields a nearly optimal bound, $\ln N - \text{const}$. Analogous results are also obtained for a more general case of several orthogonal measurements performed in generic bases.

I. INTRODUCTION

Uncertainty relations belong to the key features of quantum theory. In the original approach of Heisenberg [1] and Robertson [2] one considers the product of variances characterizing measurements of two non-commuting observables. In a later complementary approach one studies entropies of probability vectors associated with both measurements and derives lower bounds for the sum of the two entropies [3].

State independent bounds for any two orthogonal measurements performed on a state described in a Hilbert space $\mathcal{H}_N$ of a finite dimension $N$ where obtained first by Deutsch [4] and later improved by Maassen and Unflik [5]. The problem is entirely specified by a given unitary matrix $U \in U(N)$, which defines the transition between one measurement basis to the other one, and both bounds rely on the modulus of the largest entry of $U$. More information on entropic uncertainty relations can be found in review articles [6,7], while some of their numerous applications in the theory of quantum information are discussed in [8-11]. Certain improvements with respect to the result of Maassen and Unflik were recently obtained in [12-15].

Usually one aims to obtain concrete bounds for two measurements in bases related by a concrete unitary matrix $U$. Alternatively one may benchmark quality of a given bound by averaging it over the set of all unitaries with respect to the Haar measure on the unitary group. Such an approach was advocated in the papers of Hayden, et. al [10] and of Wehner and Winter [9], in which the authors considered the special case, where the number $L$ of measurements taken was a function of the dimension $N$ of the Hilbert space.

The goal of this work is three-fold. Firstly, we analyze submatrices of random unitary matrices, of a fixed order $N$ generated according to the Haar measure on $U(N)$ and establish bounds on their norms. Secondly, making use of these results we analyze in detail the case of $L = 2$ orthogonal measurements of a pure quantum state in $\mathcal{H}_N$ and find asymptotic behavior for various entropic uncertainty relations. In particular we show that for a large system size $N$ the Maassen-Unflik relation typically dominates the majorization bounds [12,13] and is only marginally weaker than the bounds of Coles and Piani [14]. The strong majorization relation, derived in [15] appears to be asymptotically the strongest and differs by a constant to the upper limit for the lower bound. Thirdly, we study asymptotic behavior of the bounds obtained for an arbitrary number $L$ of orthogonal measurements performed in $N$ dimensional Hilbert space and show that they also yield uncertainty relations optimal up to an additive constants.

This work is organized as follows. In section II we briefly recall the Maassen-Unflik relations and their improvements. Bounds for the norms of submatrices of random unitary matrices, also called their truncations [17], are established in Section III. Asymptotic entropic uncertainty relations are obtained in section IV for the case of two measurements, while the case of several measurements is discussed in section V. The paper is concluded in Sec. VI and the proofs of some theorems are presented in the Appendices.
II. ENTROPIC UNCERTAINTY RELATIONS

Consider a normalized vector $| \psi \rangle$ belonging to an $N$ dimensional Hilbert space $\mathcal{H}_N$ and a non-degenerate observable $A$, whose eigenstates $| a_i \rangle$ determine an orthonormal basis of $\mathcal{H}_N$. The probability that this observable measured in the state $| \psi \rangle$ gives the $i$-th outcome reads $p_i^\psi = |(a_i|\psi\rangle|^2$. Usually we will omit the top index, and derive state independent bounds. The vector $p$ defines a probability distribution $\{p_i\}$ and its properties can be described by the Shannon entropy, $H(p) = -\sum_i p_i \ln p_i$.

Let $H(q)$ denote the Shannon entropy corresponding to the probability vector $q^\psi = |(b_j|\psi\rangle|^2$ associated with another observable $B$. In sections II and IV we are going to consider the case of $L = 2$ observables. If both observables do not commute the sum of both entropies for any state $| \psi \rangle$ is bounded from below, and the bound depends only on the unitary rotation matrix $U_{ij} = \langle a_i|b_j \rangle$. The first lower bound:

$$H(p) + H(q) \geq -2 \ln \frac{1 + c}{2} \equiv B_D,$$

(1)

where $c = \max_{ij} |U_{ij}|$ was derived by Deutsch in 1983 with the help of variational calculus [4]. This bound is state independent, as we implicitly consider the minimization over the set of pure quantum states $| \psi \rangle \in \mathcal{H}_N$. In 1988 Maassen and Unk [5] obtained a stronger result of the form

$$H(p) + H(q) \geq -\ln c^2 \equiv B_{MU} \geq B_D.$$

(2)

Maassen-Unk bound has been improved in the whole range of the parameter $c$. Coles and Piani [14] have provided a state independent bound

$$H(p) + H(q) \geq -\ln c^2 + \left(\frac{1}{2} - \frac{c}{2}\right) \ln \frac{c^2}{c_2^2} \equiv B_{CP},$$

(3)

with $c_2$ being the second largest value among $|U_{ij}|$. Since $c_2 \leq c$ the second term in (3) is a non-negative correction to (2). The above example shows that the improvements of (2) shall rely on more overlaps between the bases.

A. Majorization Entropic uncertainty relations

We find it convenient to introduce the following notation. Let $U \in U(N)$ denote a unitary matrix, while $U_{ij}$ denote its entry. Let $U^{(n,m)}$ be an arbitrary submatrix of $U$ with $n$ rows and $m$ columns. Therefore one can write $U^{(N,N)} = U \in U(N)$. Expression $\|U^{(n,m)}\|$ denotes the norm of sub matrix $U^{(n,m)}$, equal to its largest singular value, $\sigma_{\text{max}}(U^{(n,m)})$, and $\|\hat{U}^{(n,m)}\| = \max\|U^{(n,m)}\|$ represents the maximal norm of a submatrix of $U$ of size $n \times m$.

For any fixed matrix $U$ we shall introduce a set of $N$ coefficients

$$s_k := \max \left\{ \|\hat{U}^{(1,k)}\|, \|\hat{U}^{(2,k-1)}\|, \ldots, \|\hat{U}^{(k,1)}\| \right\},$$

(4)

where the maximum is taken over all submatrices with the same semiperimeter, $m + n = k + 1$. By construction we have $c = s_1 \leq s_2 \leq \cdots \leq s_N = 1$, so that $s_k$ is equal to the modulus of the largest element of $U$. Furthermore, $s_k$ is equal to the maximum of the Euclidean norm of any two-component part of any column or any row of $U$.

$$s_2 = \max \left\{ \max_{i,j_1,j_2} \sqrt{|U_{ij_1}|^2 + |U_{ij_2}|^2}, \max_{i_1,i_2,j} \sqrt{|U_{i_1j}|^2 + |U_{i_2j}|^2} \right\},$$

(5)

hence it depends only on the moduli of $U$. In the case of $s_3$ one needs to find the maximum among Euclidean norms of any $3 \times 1$ and $1 \times 3$ vectors and spectral norms of any $2 \times 2$ submatrix of $U$ belonging to the set $U^{(2,2)}$. In the latter case not only the moduli but also the phases of entries of $U$ become important.

In the next step we define coefficients

$$R_k = \left(\frac{1 + s_k}{2}\right)^2, \quad k = 1, \ldots, N,$$

(6)

so that $\left(\frac{1+c}{2}\right)^2 = R_1 \leq R_2 \leq \cdots \leq R_N = 1$.

Recall also that if $x, y \in \mathbb{R}^N$ have nonnegative coordinates then we say that $x$ is majorized by $y$ (which we denote by $x \prec y$) if for $k = 1, \ldots, N$, $\sum_{i=1}^k x_i^k \leq \sum_{i=1}^k y_i^k$ and $\sum_{i=1}^N x_i^k = \sum_{i=1}^N y_i^k$, where $x_i^k$ is the non-increasing rearrangement
Theorem 3. Define the numbers \( s_i \), where we additionally set \( s_0 = 0 \). As a consequence,
\[
p \oplus q = \{1\} \oplus \{s_1, s_2 - s_1, s_3 - s_2, \ldots, s_N - s_{N-1}\}.  \tag{11}
\]
Majorization relation implies the following uncertainty relation
\[
H(p) + H(q) \geq H\left(\{s_1, s_2 - s_1, s_3 - s_2, \ldots, s_N - s_{N-1}\}\right).  \tag{12}
\]

Note that in this case we apply majorization techniques working with positive vectors which are not normalized to unity. In paper [15] it has been shown, that the bound (12) based on the direct sum is not weaker, than the bound (9) based on the tensor product of probability vectors.

Another result proved in [13] is an uncertainty relation for many measurements, which we now recall. For \( L \geq 2 \) consider \( N \times N \) unitary matrices \( U_1, \ldots, U_L \) and let \( |u_j^{(i)}\rangle \) be the \( j \)-th column of \( U_i \). Consider the probability distributions \( p_i^{(i)}, i = 1, \ldots, L \) given by \( p_i^{(i)} = |\langle u_j^{(i)} | \psi \rangle|^2, i = 1, \ldots, L, j = 1, \ldots, N \). Let finally \( U \) be the concatenation of matrices \( U_1, \ldots, U_L \) and for a set \( I \subset \{1, \ldots, LN\} \) with \( |I| = k \), let \( U_I \) be the \( N \times k \) matrix obtained from \( U \) by selecting the columns of \( U \) corresponding to the set \( I \). Define for \( k = 0, \ldots, NL - 1, \)
\[
S_k = \max\{|U_I|^2 : I \subset \{1, \ldots, LN\}, |I| = k + 1\}.  \tag{13}
\]
Note that \( S_0 = 1 \), independently of the choice of unitary matrices \( U_i \).

The following theorem was proved in [13].

Theorem 4. In the setting described above, define the coefficients \( x_1, \ldots, x_{NL} \) by the equality
\[
p^{(1)} \otimes \cdots \otimes p^{(L)} = (x_1, \ldots, x_{NL}).  \tag{14}
\]
Then for \( k \leq NL, \)
\[
\sum_{i=1}^k x_i \leq S_{k-1}.  \tag{15}
\]

B. Strong majorization entropic uncertainty relations

A stronger version of majorization entropic uncertainty relations was derived in [13]. Recall the definition 4 of the numbers \( s_k \).

Theorem 3. Define the numbers \( x_i, i = 1, \ldots, 2N \) by the equality \( p \oplus q = (x_1, \ldots, x_{2N}) \). Then for \( k = 1, \ldots, 2N, \)
\[
\sum_{i=1}^k x_i \leq 1 + s_{k-1},  \tag{10}
\]
where we additionally set \( s_0 = 0 \).
As a consequence,
\[ p^{(1)} \otimes \cdots \otimes p^{(L)} \prec (S_0, S_1 - S_0, S_2 - S_1, \ldots, S_{LN} - S_{LN-1}) \] (16)
and
\[ \sum_{i=1}^{L} H(p^{(i)}) \geq -\sum_{i=1}^{LN} (S_i - S_{i-1}) \ln(S_i - S_{i-1}). \] (17)

We note that for \( L > 2 \) deterministic matrices \( U_1, \ldots, U_L \) such that
\[ \sum_{i=1}^{L} H(p^{(i)}) \geq (L - 1) \ln N - C, \] (18)
where \( C \) is a constant are known only in the case \( L = N + 1 \). It was proved by Ivanovic and Sánchez-Ruiz that such a bound holds for a maximal set of mutually unbiased basis. On the other hand, as shown in [19] if \( N \) is an even power of a prime number and \( L \leq \sqrt{N} + 1 \), then there exist \( L \) mutually unbiased basis such that for some state \( |\psi\rangle \),
\[ \sum_{i=1}^{L} H(p^{(i)}) = \frac{1}{2} L \ln N. \] (19)

To the best of our knowledge, for a ‘small’ number of measurements the only available constructions of bases satisfying (18) are given by the random choice of bases and work for \( L \geq \ln^4 N \) [16]. We will discuss them in Section V, where we show that random bases provide strong uncertainty relations also for a smaller number of measurements.

III. NORMS OF TRUNCATIONS OF RANDOM UNITARIES

Motivated by the result of Maassen and Uffink we denote
\[ c(U) = \max_{ij} |U_{ij}|. \] (20)

The behaviour of \( c(U) \) for random unitaries was studied by Jiang [20], who obtained

**Theorem 5.** Let \( U \) be a Haar random unitary matrix of order \( N \), then for all \( \varepsilon > 0 \),
\[ \mathbb{P}\left( (1 - \varepsilon) \sqrt{\frac{2}{N} \ln N} \leq c(U) \leq (1 + \varepsilon) \sqrt{\frac{2}{N} \ln N} \right) \to 1 \text{ as } N \to \infty. \] (21)

The next theorem is a generalization of the result obtained by Jiang to the maximal norm of submatrices \( U^{(n,m)} \) of a random unitary matrix.

**Theorem 6.** For any fixed positive integers \( n, m \) and any \( \varepsilon > 0 \),
\[ \mathbb{P}\left( (1 - \varepsilon) \sqrt{\frac{n + m}{N} \ln N} \leq \|\hat{U}^{(n,m)}\| \leq (1 + \varepsilon) \sqrt{\frac{n + m}{N} \ln N} \right) \to 1 \text{ as } N \to \infty. \] (22)

The above theorem works for fixed \( n, m \), independent of the dimension \( N \). Its proof is based on the following result, which provides an estimate on the maximal norm \( \|\hat{U}^{(n,m)}\| \) for arbitrary \( n, m \leq N \).

**Theorem 7.** Let \( U \) be a random unitary matrix distributed according to the Haar measure on \( U(N) \). Then
\[ \mathbb{P}\left( \|\hat{U}^{(n,m)}\| - \mathbb{E}\|\hat{U}^{(n,m)}\| \geq t \right) \leq 2 \exp \left( -\frac{N t^2}{12} \right) \text{ for } t \geq 0. \] (23)

Moreover, for any \( 0 < \varepsilon < 1/3 \),
\[ \mathbb{E}\|\hat{U}^{(n,m)}\| \leq \frac{1}{1 - 2\varepsilon - \varepsilon^2} \left( \frac{2}{2N - 1} \left( \frac{m \ln eN}{m} + \frac{n \ln eN}{n} + 2(n + m) \ln(1 + \frac{2}{\varepsilon}) \right) \right)^{1/2}. \] (24)

In particular for any fixed \( n, m \) and \( N \to \infty \),
\[ \mathbb{E}\|\hat{U}^{(n,m)}\| \leq (1 + o(1)) \sqrt{\frac{m + n}{N} \ln N}. \] (25)
In the special case, when one of the parameters \( n, m \) equals to one, more precise estimates are provided by the next theorems.

**Theorem 8.** Let \( U \) be a random unitary matrix of size \( N \), then for all \( \varepsilon > 0 \) and

\[
\mathbb{P}\left( \frac{n}{N}(1 + H_N - H_n) - \varepsilon \leq \| \hat{U}^{(n,1)} \|_2^2 \leq \frac{n}{N}(1 + H_N - H_n) + \varepsilon \right) \to 1 \text{ as } N \to \infty,
\]

where \( H_N = \sum_{j=1}^{N} \frac{1}{j} \) denotes the \( N \)-th harmonic number.

The next theorem provides complete characterization of the behaviour of \( \| \hat{U}^{(n,1)} \| \) for large random unitary matrices.

**Theorem 9.** Let \( U \) be a random unitary matrix of size \( N \). For all \( \varepsilon > 0 \), with probability tending to one as \( N \to \infty \), for all \( n = 1, \ldots, N \),

\[
(1 - \varepsilon) \sqrt{\frac{n+1}{N}(1 + \ln \left( \frac{N}{n} \right))} \leq \| \hat{U}^{(n,1)} \| \leq (1 + \varepsilon) \sqrt{\frac{n+1}{N}(1 + \ln \left( \frac{N}{n} \right))}.
\]

Observe, that this result works for any \( n = 1, 2, \ldots, N - 1 \), while setting \( m = 1 \) in Theorem 7 one obtains non-trivial bounds for the norm only for \( n \leq N/\ln N - 1 \).

### IV. ASYMPTOTIC ENTR OPIC UNCERTAINTY RELATIONS

In this section we assume that \( N \gg 1 \) and analyze asymptotic behaviour of the entropic uncertainty relations. We consider two orthogonal von Neumann measurements, with respect to two bases, related by a random unitary matrix \( U \) distributed according to the Haar measure on the unitary group.

The first proposition utilizes the Maassen-Unkentropic uncertainty relation and a result concerning the asymptotic behaviour of the largest element of random unitary matrix.

**Proposition 10.** For sufficiently large \( N \) and for almost any pair of orthogonal von Neumann measurements we have

\[
H(p) + H(q) \geq \ln N - \ln \ln N - \ln 2 - o(1),
\]

which can be written as

\[
\lim_{N \to \infty} \mathbb{P}\left( H(p) + H(q) \geq \ln N - \ln \ln N - \ln 2 - \varepsilon \right) = 1,
\]

for every \( \varepsilon > 0 \).

**Proof of Proposition 10** Plugging the estimation from Theorem 5 to the Maassen-Uffink relation, we obtain asymptotic behaviour

\[
H(p) + H(q) \geq -\ln c^2 \simeq -\ln \left( \frac{2}{N} \ln N \right) = \ln N - \ln \ln N - \ln 2.
\]

The usage of Coles and Piani relation (3) will not give us a notable improvement, since for large \( N \) we have \( c \simeq c_2 \). We can state the following proposition which bounds the relation (3).

**Proposition 11.** For sufficiently large \( N \) and for almost all von Neumann measurements the bound (3) is not stronger than

\[
B_{\text{CP}} \leq \ln N - \ln \ln N - \frac{1}{2} \ln 2 + o(1).
\]

To see the above fact, first we note that for large \( N \),

\[
B_{\text{CP}} = -\ln c^2 + \left( \frac{1}{2} - \frac{c}{2} \right) \ln \frac{c^2}{c_2} = -\frac{1}{2} (\ln c^2 + \ln c_2^2) + o(1).
\]
Moreover, one can easily note that $c_1^2 + c_2^2 \geq \|\hat{U}^{(1.2)}\|^2$ and from Theorem 6 we obtain that for all $\varepsilon > 0$

$$P\left(c_2^2 \geq (1 - \varepsilon)\frac{\ln N}{N}\right) \to 1 \text{ as } N \to \infty,$$  \hspace{1cm} (33)

which translates into relation (31).

Majorization-entropic uncertainty relation introduced in [13] in many cases provides a tighter bound than the Maassen-Uffink relation (2), but in the case of large random matrices we have the following

**Proposition 12.** For sufficiently large $N$ and for almost any von Neumann measurements the bound for majorization relation (9) is not stronger than

$$H(Q) \leq \frac{3}{4} \ln(N - 1),$$  \hspace{1cm} (34)

where the vector $Q$ is defined in equation (8).

The above proposition follows from Lemma 21 presented in Appendix D.

Now we consider the strong majorization-entropic uncertainty relation formulated in Theorem 3. This relation is stronger than the result (9) and in many cases gives a better bound than the relation of Maassen and Uffink.

It is then instructive to compare asymptotic behaviour of both bounds. The following theorem, proved in Appendix E, demonstrates an advantage of the majorization techniques.

**Theorem 13.** For sufficiently large $N$ and for almost any unitary matrix $U$ drawn according to the Haar measure, we have

$$\min_\psi \left( H(p^\psi) + H(q^\psi) \right) \geq \ln N - C_1,$$ \hspace{1cm} (35)

for $C_1 = 3.49$. This fact can be written as

$$\lim_{N \to \infty} P\left(H(p) + H(q) \geq \ln N - C_1\right) = 1.$$

An estimation for the mean entropy of a random state follows from a work [21] by Jones. Let $|\psi\rangle$ and $|\phi\rangle$ be $N$-dimensional normalised vectors in $\mathbb{C}^N$ and $d\Omega_\phi$ be the unique, normalized unitary invariant measure $d\Omega_\phi$, upon the set of pure quantum states. Jones analyzed mean value of the following entropy

$$H(1,1) = -N \int (|(\langle \psi | \phi \rangle|^2) \ln(\langle \psi | \phi \rangle|^2) d\Omega_\phi,$$

and derived its asymptotic behaviour

$$H(1,1) = \Psi(N + 1) - \Psi(2) \sim_N \ln(N) - \Psi(2) + o(1).$$ \hspace{1cm} (38)

Here $\Psi(z)$ denotes the digamma function, and $\Psi(2) = 1 - \gamma \simeq 0.42$, where $\gamma$ is the Euler constant. Note, that $H(1,1)$ is also the mean value of the entropy of a probability vector $p_i = |\langle \psi | U | i \rangle|^2$, $i = 1, 2, \ldots, N$ describing von Neumann measurement of a fixed pure state $|\psi\rangle$ with respect to a basis related to a random unitary matrix $U$ or equivalently entropy of a pure random state with respect to a fixed basis. Since it is known that Shannon’s entropy of a pure random state concentrates strongly around the expectation (see Appendix B.2. of [16]), by combining the above result with Theorem 13 we arrive at a sandwich relation described by the following theorem.

**Theorem 14.** With probability tending to 1 as $N \to \infty$, we have

$$\ln N - C_0 \geq \min_\psi[H(p^\psi) + H(q^\psi)] \geq \ln N - C_1,$$ \hspace{1cm} (39)

for any $C_0 < 1 - \gamma \simeq 0.42$ and $C_1 = 3.49$. 
V. SEVERAL MEASUREMENTS

As explained in Section IVB strong entropic uncertainty relations for several measurements given by deterministic matrices are known only when the number of measurements is large. Here we will consider the case of measurements given by independent random unitary matrices.

For $N \geq 2$ let $L = L_N \geq 1$ and let $U_1, \ldots, U_L$ be independent random matrices distributed according to the Haar measure on $U_N$. For a state $|\psi\rangle$, let $p^{(i)} = p^{(i)}(\psi) = (p_1^{(i)}, \ldots, p_N^{(i)})$, with $p_j^{(i)} = |\langle u_j^{(i)} | \psi \rangle|^2$, where $u_j^{(i)}$ is the $j$-th column of $U_i$.

The following uncertainty relation for random unitaries was proved in [16]. It considers a number of $L$ measurements growing with the dimension $N$.

**Theorem 15.** There exists a universal constants $C_2$ such that if $L = L_N > C_2 \ln^4 N$ then with probability tending to 1 as $N \to \infty$,

$$
\min_{\psi} \frac{1}{L} \sum_{i=1}^L H(p^{(i)} \psi) \geq \ln N - C_2.
$$

The main result of this section shows that uniform unitaries satisfy strong uncertainty relations for an arbitrary number of measurements.

**Theorem 16.** There exists a universal constant $C_3$ such that with probability tending to 1 as $N \to \infty$ (uniformly in $L \geq 2$),

$$
\min_{\psi} \frac{1}{L} \sum_{i=1}^L H(p^{(i)} \psi) \geq \frac{L-1}{L} \ln N - C_3.
$$

We remark that clearly the lower bound on $\min_{\psi} \frac{1}{L} \sum_{i=1}^L H(p^{(i)} \psi)$ cannot be larger then $\frac{L-1}{L} \ln N$. Note also that in the above theorem we do not assume any relation between $L$ and $N$. In particular, in contrast to [16], our result covers the case of a fixed (independent of dimension) number of measurements and proves that for sufficiently high dimension $N$ and for any $L$ there indeed exist matrices satisfying almost optimal entropic uncertainty principles. Providing a constructive proof of their existence remains a challenge. Theorem [16] is proved in Appendix [C].

VI. CONCLUDING REMARKS

In this work we analyzed truncations of random unitary matrices of order $N$ and obtained estimations (25), (26), and (27) for their norms. These results allowed us to study various entropic uncertainty relations describing the bounds for the sum of entropies describing information gained in two orthogonal measurements of any $N$-dimensional pure quantum state.

For instance, the Maassen-Uffink bound [3] averaged with the Haar measure over the unitary group behaves asymptotically as $\ln N - \ln \ln N - \ln 2$. As the largest element of a random orthogonal matrix is typically larger by a factor of $\sqrt{2}$ [20], the same bound averaged over the orthogonal group gives in $N - \ln \ln N - 2 \ln 2$. These results can be compared with implications of the strong entropic uncertainty relation which, averaged over the unitary group behaves as in $N - C_2$, so it is close to the optimal. Although the exact value of the optimal constant $C_2$ is still unknown, the sandwich form [29] implies that $C_2 \in (0.42, 3.49)$.

It is natural to conjecture that if $U$ is drawn from the Haar measure on the unitary group $U_N$ and $D_N = \min_{\psi} (H(p^\psi) + H(q^\psi))$ then there exists a limit

$$
\lim_{N \to \infty} (\ln N - \mathbb{E}D_N).
$$

Strong majorization entropic uncertainty relations can be also formulated for $L$ orthogonal measurements, determined by a collection of $L$ unitary matrices of order $N$. Making use of bounds for the norms of their submatrices we established an estimate (41), which implies that the sum of $L$ entropies behaves asymptotically as $(L-1) \ln N - \text{const}$. This result, holding for an arbitrary number $L$ of measurements, is up to an additive constant compatible with the estimate [29] valid for $L = 2$.

A natural open question is to find more precise estimations for these additive constants determining the typical behavior of entropic uncertainty relations. To get tighter bounds for the averaged relation [12] one would need to improve the bounds for the average norms of the leading truncations of random unitaries. Note that the bounds [26]
and derived in this work can be considered as complementary: The former one holds for $m = 1$ and an arbitrary $n \in [1, N]$, while the latter one works for any sizes $n$ and $m$ of the submatrix, but provides non-trivial estimates if $n$ is small with respect to the matrix size $N$. Therefore, it is tempting to believe that establishing a new family of bounds for the norms $||\hat{U}(n,m)||$, which share advantages of both known results, would allow one to improve the quality of the asymptotic entropic uncertainty relations.

It is a pleasure to thank Patrick Coles and Łukasz Rudnicki for fruitful discussions and helpful remarks. This work was supported by the Grants number 2012/05/B/ST1/00412 (RA and RL), DEC-2012/04/S/ST6/00400 (ZP) and DEC-2011/02/A/ST1/00119 (KŻ) of the Polish National Science Centre NCN and in part by the Transregio-12 project C4 of the Deutsche Forschungsgemeinschaft.

**Appendix A: PROOFS OF ESTIMATES FOR NORMS OF SUBMATRICES**

1. **Proof of Theorem 7**

Recall that a probability measure $\mu$ on a metric space $(X, d)$ satisfies a log-Sobolev inequality with constant $C$ if for any locally Lipschitz function $f$

$$\int f^2 \ln f^2 \, dp - \int f^2 \, dp \ln \int f^2 \, dp \leq 2C \int |\nabla f|^2 \, d\mu,$$

(A1)

where $|\nabla f|$ is the length of gradient with respect to the metric $d$ (see e.g. Chapter 3.1. of [22] or the Appendix of [23]). For any such measure and any $L$-Lipschitz function $F$ we then have (cf. [22] Section 5.1)]

$$\int \exp \left( \lambda \left( F - \int F \, d\mu \right) \right) \, d\mu \leq \exp \left( \frac{CL^2}{2} \lambda^2 \right) \quad \text{for all } \lambda \in \mathbb{R}$$

(A2)

and

$$\mu \left( F \geq \int F \, d\mu + t \right) \leq \exp \left( - \frac{t^2}{2CL^2} \right) \quad \text{for } t \geq 0.$$  

(A3)

We will use the following estimate of the log-Sobolev constant for the unitary group (cf. [23] Theorem 15]).

**Theorem 17.** The Haar measure on the unitary group $U(N)$ satisfies a log-Sobolev inequality with constant $6/\sqrt{N}$ with respect to the Hilbert-Schmidt distance.

We recall, that for a $N \times N$ matrix $U = (U_{i,j})_{i,j \leq N}$ by $||\hat{U}(n,m)||$ we denote the maximal norm of its $n \times m$ submatrices, i.e.

$$||\hat{U}(n,m)|| := \max_{|I| = n, |J| = m} \|U(I,J)\|_{1 \rightarrow 2}^m,$$

where $U(I,J) := (U_{i,j})_{i \in I, j \in J}$.

**Proof of Theorem 7.** The function $U \mapsto ||\hat{U}(m,n)||$ is 1-Lipschitz with respect to the Hilbert-Schmidt norm. Therefore estimate (23) immediately follows by (A3) and Theorem 17.

Observe that for any $x \in \mathbb{C}^N$ with $|x| = 1$, the random variable $Ux$ is uniformly distributed on $S(\mathbb{C}^N) \simeq S^{2N-1}$. Uniform distribution on $S^1$ satisfies log-Sobolev inequality with constant $1/l$ (cf. formula (5.7) in [22]). For any $y \in \mathbb{C}^N$ the function $z \mapsto \text{Re}(z | y)$ is $|y|$-Lipschitz on $S^{2N-1}$. Therefore, using the fact that $E(Ux | y) = 0$, we get

$$E e^{\lambda \text{Re}(Ux | y)} \leq \exp \left( \frac{1}{2(2N-1)} \lambda^2 \right) \quad \text{for all } \lambda \in \mathbb{R}, \ x, y \in S(\mathbb{C}^N).$$

(A4)

Now suppose that we have a finite set $E \subset S^{N-1} \times S^{N-1}$. Then

$$E \max_{(x,y) \in E} \text{Re}(Ux | y) \leq \sqrt{\frac{2 \ln |E|}{2N-1}}.$$  

(A5)
Indeed we have for $\lambda > 0$,

$$E\exp\left(\lambda \max_{(x,y)\in E} \text{Re}(Ux|y)\right) \leq E \sum_{(x,y)\in E} e^{\lambda \text{Re}(Ux|y)} \leq |E| \exp\left(\frac{1}{2(2N-1)}\lambda^2\right). \quad (A6)$$

Jensen’s inequality gives

$$E\exp\left(\lambda \max_{(x,y)\in E} \text{Re}(Ux|y)\right) \geq \exp\left(\lambda E \max_{(x,y)\in E} \text{Re}(Ux|y)\right), \quad (A7)$$

hence

$$E \max_{(x,y)\in E} \text{Re}(Ux|y) \leq \inf_{\lambda > 0} \frac{1}{\lambda} \left(\ln |E| + \frac{1}{2(2N-1)}\lambda^2\right) = \sqrt{\frac{2\ln |E|}{2N-1}}. \quad (A8)$$

To bound $E\|\hat{U}^{(m,n)}\|$ let us choose for any $\emptyset \neq I \subset \{1, \ldots, N\}$ an $\varepsilon$-net $E_I$ in the unit sphere $S_I := \{x \in \mathbb{C}^N: |x| = 1, \text{supp}(x) \subset I\}$ of cardinality at most $(1 + 2/\varepsilon)^{|I|}$ (it exists by standard volumetric estimates, see e.g. [24]). Let $E_l := \bigcup_{|I|=l} E_I$, then for any $1 \leq l \leq N$,

$$|E_l| \leq \left(\frac{N}{l}\right)^{\frac{2}{\varepsilon^2}} \leq \left(\frac{eN}{l}\right)^{\frac{2}{\varepsilon^2}} \leq \left(\frac{2}{\varepsilon^2}\right)^{|I|}. \quad (A9)$$

Estimate (A3) gives

$$E \max_{x \in E_n, y \in E_m} \text{Re}(Ux|y) \leq \sqrt{\frac{2\ln |E_n|}{2N-1} + \ln |E_m|}. \quad (A10)$$

Finally it is not hard to see that

$$\|\hat{U}^{(m,n)}\| \leq \frac{1}{1 - 2\varepsilon - \varepsilon^2} \max_{x \in E_n, y \in E_m} \text{Re}(Ux|y). \quad (A11)$$

\[\square\]

2. **Proof of Theorem 6**

Note that the upper bound on $\|\hat{U}^{(m,n)}\|$ follows from the already proven Theorem 7. We will show that for all fixed positive integers $n, m$ and $\varepsilon > 0$,

$$\mathbb{P}\left(\|\hat{U}^{(m,n)}\| \leq (1 - \varepsilon)\sqrt{(n + m)\ln N/N}\right) \to 0, \quad (A12)$$

as $N \to \infty$.

Let $\Gamma = (\Gamma_{ij})_{i,j \leq N}$ be an $N \times N$ matrix whose entries are i.i.d. standard complex Gaussian variables (i.e. their real and imaginary parts are independent, with distribution $N(0,1/2)$).

Set $M = M_N = N/\ln^2 N$. By Theorem 6 in [20] (applied with $m = M_N$, $r = 1/\ln N$, $s = \ln N/(\ln \ln N)^{1/2}$, $t = \sqrt{\ln N/\ln \ln N}$, cf. formula (2.10) in [20]) we can assume that

$$\max_{1 \leq i,j \leq m} |\sqrt{N}U_{ij} - \Gamma_{ij}| \leq 3\sqrt{\ln N/\ln \ln N},$$

with probability at least $1 - O(1/\ln^3 N)$.

Thus when $N \to \infty$, we have with probability tending to 1

$$\max_{i,j \leq M_N} |U_{ij}^2 - 1/N| \Gamma_{ij}^2 \leq C_\varepsilon \frac{\ln N}{N \sqrt{\ln \ln N}}, \quad (A14)$$

where we used the fact that with probability tending to 1 as $N \to \infty$

$$\max_{i,j \leq N} |U_{ij}| + \frac{1}{\sqrt{N}} |\Gamma_{ij}| \leq C_\varepsilon \frac{\ln N}{N} \quad (A15)$$
and the identity $|a^2 - b^2| = |(a - b)(a + b)|$.

By (A14) it is enough to show that with probability tending to 1,

$$\|\hat{\Gamma}^{(n,m)}\| \geq (1 - \varepsilon)\sqrt{(n + m)\ln N},$$

(A16)

where $\Gamma'$ is the $M_N \times M_N$ principal submatrix of $\Gamma$.

Since $\ln M_N \to 1$ as $N \to \infty$, (A12) will follow if we prove

**Proposition 18.** For any positive integers $n, m$ and any $\varepsilon > 0$,

$$\mathbb{P}\left(\|\hat{\Gamma}^{(n,m)}\| \leq (1 - \varepsilon)\sqrt{(n + m)\ln N}\right) \to 0.$$  

(A17)

**Proof.** First note that by the concentration property of Gaussian measures (see e.g. [22]) and the fact that $\|\hat{\Gamma}^{(n,m)}\|$ is 1-Lipschitz with respect to the Hilbert-Schmidt norm, we have

$$\mathbb{P}\left(\|\hat{\Gamma}^{(n,m)}\| - \mathbb{E}[\|\hat{\Gamma}^{(n,m)}\|] \geq t\right) \leq 2\exp(-t^2).$$

(A18)

Thus to prove the proposition it is enough to show that for every $\varepsilon > 0$, and $N$ large enough $\mathbb{E}[\|\hat{\Gamma}^{(n,m)}\|] \geq (1 - \varepsilon)\sqrt{(n + m)\ln N}$. Assume that $\mathbb{E}[\|\hat{\Gamma}^{(n,m)}\|] < (1 - \varepsilon)\sqrt{(n + m)\ln N}$. Then, again by concentration $\mathbb{P}(\|\hat{\Gamma}^{(n,m)}\| \geq (1 - \varepsilon/2)\sqrt{(n + m)\ln N}) \leq 1/N^{(n+m)/2} \to 0$ as $N \to \infty$. Therefore, to prove (A17) it is enough to show that for every $\varepsilon > 0$, there exists $d > 0$ such that for $N$ large enough, we have

$$\mathbb{P}\left(\|\hat{\Gamma}^{(n,m)}\| \geq (1 - \varepsilon)\sqrt{(n + m)\ln N}\right) > d.$$  

(A19)

It is well known that $|\Gamma_{ij}|^2$ are standard exponential variables, therefore

$$\mathbb{P}\left(|\Gamma_{ij}|^2 \geq \frac{n + m}{nm} \ln N\right) = \frac{1}{N^{n+m}}.$$ 

(A20)

Moreover $\Gamma_{ij}$ are rotationally invariant, so for any $\delta \in (0,1)$,

$$\mathbb{P}\left(|\Gamma_{ij}|^2 \geq \frac{n + m}{nm} \ln N, \text{Arg} \Gamma_{ij} \in [0, 2\pi \delta]\right) = \frac{\delta}{N^{n+m}}.$$  

(A21)

Consider any $I, J \subset \{1, \ldots, N\}$ with $|I| = n, |J| = m$ and define the event

$$\mathcal{E}(I, J) = \left\{\forall i \in I, j \in J |\Gamma_{ij}|^2 \geq \frac{n + m}{nm} \ln N, \text{Arg} \Gamma_{ij} \in [0, 2\pi \delta]\right\}.$$ 

(A22)

Note that for $\delta$ small enough, depending on $\varepsilon$, on the event $\mathcal{E}(I, J)$ we have

$$\|\Gamma(I,J)\| \geq (1 - \varepsilon)\sqrt{(n + m)\ln N},$$

(A23)

where $\Gamma(I,J) = (\Gamma_{ij})_{i \in I, j \in J}$.

Indeed for the unit vector $z = m^{-1/2}(1, \ldots, 1) \in \ell_2^n$ we have

$$\|\Gamma(I,J)z\|^2 = \sum_{i \in I} \frac{1}{m} \left|\sum_{j \in J} \Gamma_{ij}\right|^2.$$ 

(A24)

Now for $\delta$ small enough,

$$\left|\sum_{j \in J} \Gamma_{ij}\right|^2 \geq \sum_{j,j' \in J} |\Gamma_{ij}| |\Gamma_{ij'}| \cos \text{Arg} \Gamma_{ij} \Gamma_{ij'}$$

$$\geq \sum_{j,j' \in J} |\Gamma_{ij}| |\Gamma_{ij'}| \cos 2\pi \delta \geq (1 - \varepsilon)^2 m^2 \frac{n + m}{nm} \ln N$$  

(A25)

and thus

$$\|\Gamma(I,J)z\|^2 \geq (1 - \varepsilon)^2 (n + m) \ln N,$$ 

(A26)
which proves (A23).

Thus to prove the proposition it is enough to show that for $N$ large enough,

$$\mathbb{P}\left( \bigcup_{|I|=n, |J|=m} \mathcal{E}(I,J) \right) \geq d. \quad (A27)$$

By the Bonferroni inequality we have

$$\mathbb{P}\left( \bigcup_{|I|=n, |J|=m} \mathcal{E}(I,J) \right) \geq \sum_{|I|=n, |J|=m} \mathbb{P}(\mathcal{E}(I,J)) - \sum_{|I|=n, |J|=m} \mathbb{P}(\mathcal{E}(I,J) \cap \mathcal{E}(I',J')) \quad (A28)$$

$$=: A - B.$$ 

By (A21) and independence of entries,

$$A = \binom{N}{m} \binom{N}{n} \frac{\delta_{nm}}{N^{n+m}} \rightarrow \frac{\delta_{nm}}{n!m!}, \quad (A29)$$

as $N \rightarrow \infty$.

Now we group the summands in $B$, depending on the cardinality of $I \cup I'$ and $J \cup J'$ and obtain

$$B = \sum_{n \leq r \leq 2n, m \leq s \leq 2m} \sum_{|I|=|I'|=n, |J|=|J'|=m, (I,J) \neq (I',J')} \mathbb{P}(\mathcal{E}(I,J) \cap \mathcal{E}(I',J')). \quad (A30)$$

For fixed $r, s$ there are at most $C_{rs}N^{r+s}$ pairs $(I,J), (I',J')$ such that $|I| = |I'| = n, |J| = |J'| = m, |I \cup I'| = r, |J \cup J'| = s$ where $C_{rs}$ is a constant depending only on $r$ and $s$. For each such pair the event $\mathcal{E}(I,J) \cap \mathcal{E}(I',J')$ is the intersection of $rs - 2(r-n)(s-m)$ independent events of the form (A21). Therefore,

$$\mathbb{P}(\mathcal{E}(I,J) \cap \mathcal{E}(I',J')) = \delta_{rs}^{2(r-n)(s-m)}N^{-(rs-2(r-n)(s-m))}(n+m)/(nm) \quad (A31)$$

and as a consequence

$$\sum_{|I|=|I'|=n, |J|=|J'|=m, (I,J) \neq (I',J')} \mathbb{P}(\mathcal{E}(I,J) \cap \mathcal{E}(I',J')) \leq C_{rs}\delta_{rs}^{2(r-n)(s-m)}N^{r+s-(rs-2(r-n)(s-m))(n+m)/(nm)} \quad (A32)$$

$$= C_{rs}\delta_{rs}^{2(r-n)(s-m)}N^{(s-2m)(r-n)}/m(r-2n)(s-m).$$

One can see that if $r \neq 2n$ or $s \neq 2m$ then $\frac{(s-2m)(r-n)}{m} + \frac{(r-2n)(s-m)}{m} < 0$ and so the contribution to (A30) from such pairs converges to 0 as $N \rightarrow \infty$. Therefore, for $\delta$ small enough and large $N$,

$$\mathbb{P}\left( \bigcup_{|I|=n, |J|=m} \mathcal{E}(I,J) \right) \geq \frac{\delta_{nm}}{2n!m!} - C_{2n,2m}\delta_{2nm}^{2n} \geq \frac{\delta_{nm}}{4n!m!}. \quad (A33)$$

Thus (A27) holds with $d = \frac{\delta_{nm}}{4n!m!}$, which ends the proof of the proposition. \hfill \Box

3. Proof of Theorems 8 and 9

Proof of Theorem 8 Let $U$ be a random unitary matrix distributed according to the Haar measure on the unitary group $U(N)$. Then its first column $(U_{1j})_{j \leq N}$ (or any other column or row) is uniformly distributed on $S(\mathbb{C}^N) \approx S^{2N-1}$. Hence squares of its moduli $q_i = |U_{1j}|^2$ for $i = 1, \ldots, N$ form a random probability vector uniformly distributed on the simplex $\Delta_{N-1} \subset \mathbb{R}^N$ (this observation seems to be a part of the folklore, it can be easily obtained by 1) expressing the uniform measure on $S(\mathbb{C}^N)$ in terms of normalized complex Gaussian vectors, 2) using the fact that the square of the absolute value of a standard complex Gaussian variable has standard exponential distribution, 3) invoking the well known fact that a self normalized vector with i.i.d. standard exponential coordinates is distributed uniformly on $\Delta_{N-1}$, see e.g. [25]).

To look for the largest component of the vector we order $q_1, \ldots, q_N$ in a weakly decreasing order, $q_1^+ \geq q_2^+ \geq \cdots \geq q_N^+$. It is not hard to notice that random vector $q^+ = (q_1^+, q_2^+, \ldots, q_N^+)$ is uniformly distributed on the simplex $\Delta_{N-1}$ with vertices $(1, 0, \ldots, 0), \frac{1}{n}(1, 1, 0, \ldots, 0), \ldots, \frac{1}{n}(1, 1, \ldots, 1)$.
Figure 1: Probability simplex $\Delta_2$ for $N = 3$ a) and its asymmetric part $\tilde{\Delta}_2$ with vertices $A, B, C$ and the barycenter $X = (A + B + C)/3 = (11,5,2)/18$, the components of which represent the averaged ordered vector $EQ^\downarrow$.

Thus the mean value of $q^\downarrow$ is the barycenter of $\tilde{\Delta}_{N-1}$. Its coordinates can be expressed by the harmonic numbers $H_m := \sum_{j=1}^m 1/j$, which asymptotically behave as $\ln m + \gamma$, where $\gamma \approx 0.5772$ denotes the Euler constant. Namely,

$$E q_m^\downarrow = x_m = \frac{1}{N} \sum_{j=m}^N \frac{1}{j} = [H_N - H_{m-1}]/N. \tag{A34}$$

Denote by $X_{n,i}$ ($i = 1, \ldots, N$) the maximum norm of a subvector of dimension $n \leq N$ of the $i$-th column of $U$. The average of $X_{n,i}^2$ is equal to the sum of first $n$ components of the ordered vector $q^\downarrow$, averaged over the simplex $\tilde{\Delta}_{N-1}$,

$$EX_{n,i}^2 = \sum_{m=1}^n x_m = \frac{1}{N} \sum_{m=1}^n \sum_{j=m}^N \frac{1}{j}. \tag{A35}$$

To evaluate this sum we divide the summation region in the $(m,j)$ plane into a triangle and a rectangle and change the summation order,

$$\sum_{m=1}^n x_m = \frac{1}{N} \sum_{j=1}^n \sum_{m=1}^j \sum_{j=n+1}^N \frac{1}{j} \sum_{m=1}^j \frac{1}{1} = \frac{n}{N} \left[ 1 + \sum_{j=n+1}^N \frac{1}{j} \right] = \frac{n}{N} [1 + H_N - H_n]. \tag{A36}$$

We have

$$\|\hat{U}^{(n,1)}\|^2 = \max_{i \leq N} X_{n,i}^2,$$

and (36) follows by the concentration of measure since the uniform distribution on $S(C^N)$ satisfies the log-Sobolev inequality with constant $1/(2N - 1)$.

Proof of Theorem 9 Let us fix $\varepsilon > 0$ and let $n_0 = n_0(\varepsilon)$ be a sufficiently large constant depending on $\varepsilon$, to be chosen later on. By Theorem 3 with probability tending to 1 as $N \to \infty$, we have for all $n \leq n_0$

$$(1 - \varepsilon) \frac{n + 1}{N} (1 + \ln \left( \frac{N}{n} \right)) \leq \|\hat{U}^{(n,1)}\| \leq (1 + \varepsilon) \frac{n + 1}{N} (1 + \ln \left( \frac{N}{n} \right)). \tag{A37}$$

(note that in this range of $n$, $(1 + \ln(N/n)) = (1 + o(1)) \ln N$ as $N \to \infty$).

As in the proof of Theorem 8 denote by $X_{n,i}$ ($i = 1, \ldots, N$) the maximum norm of an $n \times 1$ submatrix of the $i$-th column of $U$. Using (A35) we get $E X_{n,i}^2 = H_n/(1 + H_N - H_n)$ and so

$$(1 - \varepsilon/8)^2 \frac{n + 1}{N} (1 + \ln(N/n)) \leq E X_{n,i}^2 \leq (1 + \varepsilon/8)^2 \frac{n + 1}{N} (1 + \ln(N/n)), \tag{A38}$$
(where we used the fact that \( n > n_0 \)). Now, by integration by parts and (A3) it is easy to see that for large \( N \),
\[
\mathbb{E}X_{n,i} \geq \sqrt{\mathbb{E}X_{n,i}^2 - O(1/N)} \geq (1 - \varepsilon/8) \sqrt{\mathbb{E}X_{n,i}^2},
\]
and thus
\[
(1 - \varepsilon/2) \sqrt{\frac{n+1}{N}(1 + \ln(N/n))} \leq \mathbb{E}X_{n,i} \leq (1 + \varepsilon/2) \sqrt{\frac{n+1}{N}(1 + \ln(N/n))}. \tag{A39}
\]

Now, using again (A3) together with the union bound we get
\[
(1 - \varepsilon) \sqrt{\frac{n+1}{N}(1 + \ln(N/n))} \leq X_{n,i} \leq (1 + \varepsilon) \sqrt{\frac{n+1}{N}(1 + \ln(N/n))}, \tag{A40}
\]
for all \( n > n_0 \) and \( i \leq N \), with probability at least
\[
1 - N^2 \exp\left(-\frac{\varepsilon^2}{24}(n+1)\ln(\varepsilon N/n)\right), \tag{A41}
\]
which can be made arbitrarily close to one for \( N \to \infty \) if one chooses \( n_0(\varepsilon) \) sufficiently large (as can be easily seen by considering separately the cases \( n_0 < n < \sqrt{N} \) and \( \sqrt{N} < n \leq N \)). The proof is concluded by combining (A37) and (A40).

Appendix B: PROOF OF THEOREM 13

Recall the definition of the parameters \( s_k \) given in (4). The proof of Theorem 13 will be based on the following

**Proposition 19.** With probability tending to 1 as \( N \to \infty \),
\[
s_k \leq \sqrt{C_0 \frac{k+1}{N} \left(1 + \ln\left(\frac{2N}{k+1}\right)\right)} \quad \text{for } 1 \leq k \leq N, \tag{B1}
\]
where \( C_0 = 4.18 \).

**Proof.** Note, that if for any \( n, m \), such that \( n + m = k + 1 \), we have

\[
\mathbb{E}\|\hat{U}^{(n,m)}\| \leq \sqrt{\frac{Dk+1}{N} \left(1 + \ln\left(\frac{2N}{k+1}\right)\right)}, \tag{B2}
\]
then (B1) will hold with \( C_0 = D + \delta \), for any \( \delta > 0 \), since by Theorem 17 and (A3) we get
\[
\mathbb{P}\left(\exists k \leq N \text{ s.t. } \sqrt{C_0 \frac{k+1}{N} \left(1 + \ln\left(\frac{2N}{k+1}\right)\right)} \leq \sum_{k=1}^{N-1} \sum_{n=1}^{k} \mathbb{P}\left(\|\hat{U}^{(n,k+1-n)}\| \geq \sqrt{C_0 \frac{k+1}{N} \left(1 + \ln\left(\frac{2N}{k+1}\right)\right)}\right) \right.
\leq \sum_{k=1}^{N} k \exp\left(-cD,\delta N \frac{k+1}{N} \left(1 + \ln\left(\frac{2N}{k+1}\right)\right)\right) \to 0 \quad \text{as } N \to \infty.
\]

By Theorem 7 we get
\[
\mathbb{E}\|\hat{U}^{(n,m)}\| \leq \frac{1}{1 - 2\varepsilon - \varepsilon^2} \sqrt{\frac{2}{2N - 1} \left(m \ln\frac{\varepsilon n}{m} + n \ln\frac{\varepsilon n}{n} + 2(n+m) \ln\left(1 + \frac{2}{\varepsilon}\right)\right)^{1/2}}, \tag{B4}
\]
for \( \varepsilon < 1/3 \).

Note that when \( k+1 > N/D \), the right hand side of (B2) exceeds 1, so the inequality is satisfied trivially. We can therefore assume that \( k+1 \leq N/D \). We maximize the above under constrain that \( n + m = k + 1 \) and get
\[
\mathbb{E}\|\hat{U}^{(n,m)}\| \leq \frac{1}{1 - 2\varepsilon - \varepsilon^2} \sqrt{\frac{2}{2N - 1} \left((k+1) \ln\frac{2\varepsilon n}{k+1} + 2(k+1) \ln(1 + \frac{2}{\varepsilon})\right)^{1/2}}
\leq \sqrt{\frac{2}{2N - 1} \left((k+1) \ln\frac{2\varepsilon n}{k+1}\right)^{1/2} \left(\frac{1}{\ln(2eD)}\right)^{1/2}, \tag{B5}
\]
where we used the assumption \(N/(k+1) \geq D\).

Now we set \(D = 4.175\) and perform a minimization with respect to \(\varepsilon \in (0, 1/3)\) of the expression

\[
\frac{1}{(1 - 2\varepsilon - \varepsilon^2)^2} \left(1 + \frac{2\ln(1 + \frac{2}{\varepsilon})}{\ln(2eD)}\right). \tag{B6}
\]

The numerical value of the minimum is approximately \(4.172 \leq 4.175\) (obtained for \(\varepsilon = 0.039\)). This shows \([B2]\) with \(D = 4.175\) and thus for we can take \(C_6 = 4.18\).

**Proof of Theorem [T3]** Recall that \(C_6 = 4.18\). We define vector \(m\), as

\[
m_1 = \sqrt{C_6 \frac{2}{N}(1 + \ln(N))}, \tag{B7}
\]

and for \(i \geq 2\),

\[
m_i = \sqrt{C_6 \frac{i + 1}{N} \left(1 + \ln \left(\frac{2N}{i + 1}\right)\right)} - \sqrt{C_6 \frac{i}{N} \left(1 + \ln \left(\frac{2N}{i}\right)\right)} > 0, \tag{B8}
\]

which for \(2 \leq i < 2eN - 1\) we can rewrite as

\[
m_i = \sqrt{2C_6 \left(f \left(\frac{i + 1}{2N}\right) - f \left(\frac{i}{2N}\right)\right)}, \tag{B9}
\]

where \(f: (0, e) \to \mathbb{R}\) is given by \(f(x) = \sqrt{x(1 - \ln x)}\). The function \(f\) is concave, which can be verified by simple calculations, i.e.

\[
\frac{d}{dx} f(x) = \frac{-\ln x}{2 \sqrt{x(1 - \ln x)}} \tag{B10}
\]

and

\[
\frac{d^2}{dx^2} f(x) = \frac{-(1 - \ln x)^2 - 1}{4(x(1 - \ln x))^{3/2}} < 0. \tag{B11}
\]

From concavity we obtain that for \(i \geq 2\),

\[
m_i \leq \sqrt{2C_6 \frac{1}{2N} \frac{d}{dx} f \left(\frac{i}{2N}\right)} = \frac{1}{\sqrt{2N}} \frac{\sqrt{C_6 \ln \left(\frac{2N}{i}\right)}}{\sqrt{\frac{1}{N} \left(\ln \left(\frac{2N}{i}\right) + 1\right)}} \tag{B12}
\]

Note that

\[
m_1 + \sum_{i=2}^{N} \frac{1}{N} \frac{\sqrt{C_6 \ln \left(\frac{2N}{i}\right)}}{\sqrt{\frac{1}{N} \left(\ln \left(\frac{2N}{i}\right) + 1\right)}} \geq \sum_{i=1}^{N} m_i = \sqrt{C_6 \frac{N + 1}{N} \left(1 + \ln \left(\frac{2N}{N + 1}\right)\right)} > 1. \tag{B13}
\]

Let \(N_0\) be the greatest integer not exceeding \(N\), such that

\[
m_1 + \sum_{i=2}^{N_0} \frac{1}{N} \frac{\sqrt{C_6 \ln \left(\frac{2N}{i}\right)}}{\sqrt{\frac{1}{N} \left(\ln \left(\frac{2N}{i}\right) + 1\right)}} \leq 1 \tag{B14}
\]

and define a vector \(r \in \mathbb{R}^{N_0+1}\) by specifying its coordinates as \(r_1 = m_1\) and

\[
r_i = \frac{1}{\sqrt{\frac{1}{N} \left(\ln \left(\frac{2N}{i}\right) + 1\right)}} \tag{B15}
\]

for \(i = 2, \ldots, N_0\). As the last coordinate we put \(r_{N_0+1} = 1 - \sum_{i=1}^{N_0} r_i\), so \(r\) is a probabilistic vector. Note that

\[
r_{N_0+1} \leq \frac{1}{\sqrt{\frac{N_0+1}{N} \left(\ln \left(\frac{2N}{N_0+1}\right) + 1\right)}} \leq \sqrt{\frac{C_6 \ln N}{N}}. \tag{B16}
\]
Let $z$ be the non-increasing rearrangement of $p \oplus q$. For $k \leq N_0 + 1$, Theorem\[8\] and Proposition\[19\] give
\[
\begin{align*}
z_1 + \ldots + z_k &\leq 1 + s_{k-1} \leq 1 + \sqrt{C_6 \frac{k}{N} \ln \left( \frac{2N}{k} \right)} \\&= 1 + m_1 + \ldots + m_{k-1} \\&\leq 1 + r_1 + \ldots + r_{k-1}
\end{align*}
\]
and obviously $z_1 + \ldots + z_k \leq 2 = 1 + r_1 + \ldots + r_{N_0+1}$, for $k > N_0 + 1$ so $z < 1 \oplus r$. As a consequence,
\[
H(p) + H(q) \geq H(r).
\]
We will now bound from below the entropy of the vector $r$
\[
H(r) \geq -\sum_{i=2}^{N_0} r_i \ln r_i = -\sum_{i=2}^{N_0} r_i \ln \left( \frac{1}{N} \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \right)
\]
\[
= \sum_{i=2}^{N_0} r_i \ln N - \sum_{i=2}^{N_0} \frac{1}{N} \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \ln \left( \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \right)
\]
\[
= \ln N - (m_1 + r_{N_0+1}) \ln N - A_N = \ln N - O\left( \frac{\ln^{3/2} N}{\sqrt{N}} \right) - A_N,
\]
where
\[
A_N = \sum_{i=2}^{N_0} \frac{1}{N} \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \ln \left( \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \right).
\]
Above we used (B16) and the estimate $m_1 = O\left( \sqrt{\frac{\ln N}{N}} \right)$.

Let us now bound $N_0/N$ from above. Since
\[
m_1 + \sum_{i=2}^{k} \frac{1}{N} \frac{\sqrt{C_6 \ln \left( \frac{2N}{i} \right)}}{2 \sqrt{\frac{i}{N} \ln \left( \frac{2N}{i} \right) + 1}} \geq \sum_{i=1}^{k} m_i = \sqrt{C_6 \frac{k+1}{N} \left( 1 + \ln \left( \frac{2N}{k+1} \right) \right)}.
\]
we have $N_0 \leq N_1$, where $N_1$ is the largest integer smaller than $N$, such that
\[
\sqrt{C_6 \frac{N_1+1}{N} \left( 1 + \ln \left( \frac{2N}{N_1+1} \right) \right)} \leq 1.
\]
We have $N_1/N \to x^*$, where $x^*$ is the unique solution of
\[
C_6 x^* \left( 1 + \ln \left( \frac{2}{x^*} \right) \right) = 1.
\]
Since $C_6 = 4.18$ we can evaluate numerically that $x^* \simeq 0.051$ and so we can write
\[
\limsup A_N \leq \int_{0}^{0.052} \frac{\sqrt{C_6 \ln \left( \frac{3}{2} \right)}}{2 \sqrt{\frac{x}{\ln \left( \frac{2^x}{3} \right)}}} \ln \left( \frac{\sqrt{C_6 \ln \left( \frac{3}{2} \right)}}{2 \sqrt{\frac{x}{\ln \left( \frac{2^x}{3} \right)}}} \right) dx \simeq 3.488,
\]
which ends the proof (note that the integrand above is positive on the interval of integration). \(\square\)

Appendix C: PROOF OF ENTROPIC UNCERTAINTY RELATION FOR SEVERAL RANDOM MEASUREMENTS (THEOREM 10)

Let $U$ be the concatenation of $U_1, \ldots, U_L$. For $I \subset \{1, \ldots, NL\}$ let $U_I$ be the matrix obtained from $U$ by selecting the columns corresponding to the set $I$. Recall also the definition of the parameters $S_k$ given in (13).
Lemma 20. With probability tending to 1 as $N \to \infty$ (uniformly in $L \geq 2$), for all $k \leq LN - 1$,

\[
\sqrt{S_k} = \max_{|I|=k+1} \|U_I\| \leq 1 + \sqrt{C_7 \frac{k+1}{N} \ln \left(\frac{eNL}{k+1}\right)}, \quad \text{(C1)}
\]

where $C_7$ is a universal constant.

Proof of Lemma 20. Let us first note that by the tensorization property of entropy, $U$ satisfies the log-Sobolev inequality with parameter $6/\sqrt{N}$ with respect to the Hilbert-Schmidt metric. In particular, since for any unit vector $x \in C^{NL}$, the map $U \mapsto |Ux|$ is $1$-Lipschitz, we get

\[
P(|Ux| \geq \mathbb{E}|Ux| + t) \leq 2e^{-Nt^2/12}. \quad \text{(C2)}
\]

Denote the columns of $U$ by $Y_i$, $i = 1, \ldots, NL$. We also have

\[
\mathbb{E}|Ux|^2 = \mathbb{E}<Ux,Ux> = \sum_{i=1}^{NL} |x_i|^2 \mathbb{E}|Y_i|^2 + \sum_{i \neq j} x_i x_j \mathbb{E}<Y_i,Y_j> = 1, \quad \text{(C3)}
\]

where we used the fact that for each $i \neq j$, $Y_i$ and $Y_j$ are of mean zero and either independent or orthogonal with probability one. Thus $\mathbb{E}|Ux| \leq 1$. Moreover, by (C2) and integration by parts

\[
1 = \sqrt{\mathbb{E}|Ux|^2} \leq \mathbb{E}|Ux| + \sqrt{\frac{24}{N}}, \quad \text{(C4)}
\]

Consider now fixed $I \subset \{1, \ldots, NL\}$ with $|I| = k+1$ and let $N_I$ be a $1/4$-net in the unit ball of $C^I = \{x \in C^{NL} : x_i = 0$ for $i \notin I\}$ of cardinality $10^2(k+1)$ (it exists by standard volumetric estimates, see [24]). If $C_8$ is a sufficiently large absolute constant, then by the union bound, with probability at least

\[
1 - 10^2(k+1) \left(\frac{LN}{k+1}\right) e^{-C_8 (k+1) \ln(eNL/(k+1))}/13 \geq 1 - e^{-N(k+1) \ln(eNL/(k+1))}, \quad \text{(C5)}
\]

we have

\[
1 - \sqrt{C_8 \frac{k+1}{N} \ln \left(\frac{eNL}{k+1}\right)} \leq |Ux| \leq 1 + \sqrt{C_8 \frac{k+1}{N} \ln \left(\frac{eNL}{k+1}\right)}, \quad \text{(C6)}
\]

for all $I$ with $|I| = k+1$ and $x \in N_I$.

Let $\delta = \sqrt{C_8 \frac{k+1}{N} \ln \left(\frac{eNL}{k+1}\right)}$. If $\delta > 1$, then the second inequality in (C6) implies that

\[
\|U_I\| \leq \frac{4}{3}(1 + \delta) \leq 1 + \sqrt{C_8 \frac{k+1}{N} \ln \left(\frac{eNL}{k+1}\right)}, \quad \text{(C7)}
\]

for $C_9$ sufficiently large (depending only on $C_8$).

If $\delta < 1$, then on the event where (C6) holds, we have for $I$ with $|I| = k+1$ and $x \in N_I$,

\[
1 - 2\delta \leq \langle U_I x, U_I x \rangle \leq 1 + 3\delta, \quad \text{(C8)}
\]

which implies that the operator $A = U_I^* U_I - I$ on $C^I$ satisfies

\[
|\langle Ax, x \rangle| \leq 3\delta, \quad \text{(C9)}
\]

for $x \in N_I$.

Let now $y$ be any unit vector in $C^I$ and $x$ a point in $N_I$ such that $|x - y| < 1/4$. We have

\[
|\langle Ay, y \rangle| \leq |\langle (A(y-x))(y-x) \rangle| + |\langle Ax(y-x) \rangle| + |\langle Ay-y \rangle| + |\langle Ax \rangle| \leq \frac{1}{16} \|A\| + \frac{1}{2} \|A\| + 3\delta. \quad \text{(C10)}
\]

Taking the supremum over $y \in S_{C}^{N-1}$, using the fact that $A$ is Hermitian and performing easy calculations we get

\[
\|A\| \leq 7\delta, \quad \text{(C11)}
\]
which implies that
\[ \|U_I\|^2 \leq 1 + 7\delta \]  
(C12)

and as a consequence
\[ \|U_I\| \leq 1 + \sqrt{C_{10} \frac{k+1}{N} \ln \left( \frac{eNL}{k+1} \right)}. \]  
(C13)

Now it remains to set \( C_7 = \max(C_9, C_{10}) \), take the union bound over all \( k \leq NL - 1 \) and note that
\[ \sum_{k=1}^{NL-1} e^{-(k+1)\ln(eNL/(k+1))} \to 0, \]  
(C14)
as \( N \to \infty \) for \( L \geq 2 \).

**Proof of Theorem 16** Let \( C_7 \) be the constant from Lemma 20. Define \( M_1 = \left(1 + \sqrt{C_7 \frac{i}{N} \ln \left( \frac{eLN}{i} \right)} \right)^2 - 1 \) and for \( 2 \leq i \leq NL - 1 \),
\[ M_i = \left(1 + \sqrt{C_7 \frac{i+1}{N} \ln \left( \frac{eLN}{i+1} \right)} \right)^2 - \left(1 + \sqrt{C_7 \frac{i}{N} \ln \left( \frac{eLN}{i} \right)} \right)^2. \]  
(C15)

We have
\[ M_i = 2 \nu \left( \sqrt{C_7 \frac{i+1}{N} \ln \left( \frac{eLN}{i+1} \right)} - \sqrt{C_7 \frac{i}{N} \ln \left( \frac{eLN}{i} \right)} \right) + C_7 \nu \left( g\left( \frac{i+1}{LN} \right) - g\left( \frac{i}{LN} \right) \right), \]  
(C16)
where \( f, g : [0,e] \to \mathbb{R} \) are given by \( f(x) = \sqrt{x \ln(e/x)} \) and \( g(x) = x \ln(e/x) \).

Both \( f \) and \( g \) are concave and thus
\[ M_i \leq 2\nu \sqrt{C_7 L} \frac{1}{LN} \frac{d}{dx} f\left( \frac{i}{LN} \right) + C_7 \nu \frac{1}{LN} \frac{d}{dx} g\left( \frac{i}{LN} \right) = \nu \left( \frac{\sqrt{C_7 \ln\left( \frac{LN}{i} \right)}}{\sqrt{\nu} \ln\left( \frac{eLN}{i} \right)} + \frac{\sqrt{C_7 \ln\left( \frac{LN}{i} \right)}}{\sqrt{\nu} \ln\left( \frac{eLN}{i} \right)} \right) =: \tilde{M}_i. \]  
(C17)

Since
\[ M_1 + \sum_{i=2}^{LN-1} \tilde{M}_i \geq \sum_{i=1}^{LN-1} M_i = \left(1 + \sqrt{C_7 \frac{LN}{N} \ln \left( \frac{eLN}{LN} \right)} \right)^2 - 1 > L - 1, \]  
(C18)
there exists maximum \( N_0 < LN - 1 \) such that
\[ M_1 + \sum_{i=2}^{N_0} \tilde{M}_i \leq L - 1, \]  
(C19)
(note that for \( N \) sufficiently large, independent of \( L \), \( M_1 \leq L - 1 \).

Define a vector \( W \in \mathbb{R}^{N_0+1} \) by \( W_1 = M_1 \),
\[ W_i = \tilde{M}_i, \]  
(C20)
for \( i = 2, \ldots, N_0 \) and \( W_{N_0+1} = L - 1 - \sum_{i=1}^{N_0} W_i \).

Let \( z_i \) be the non-increasing rearrangement of \( p_1 \oplus \cdots \oplus p_L \). Using Theorem 4 and Lemma 20 we get that with probability tending to one as \( N \to \infty \), for \( k \leq N_0 + 1 \),

\[
z_1 + \ldots + z_k \leq S_{k-1}
\]

\[
\leq \left( 1 + \sqrt{C_7 \frac{k}{N} \ln \left( \frac{CNL}{k} \right)} \right)^2 \leq 1 + M_1 + \ldots + M_{k-1} \leq 1 + W_1 + \ldots + W_{k-1}.
\]

Also for \( k > N_0 + 1 \) we have \( z_1 + \ldots + z_k \leq L = 1 + W_1 + \ldots + W_{N_0+1} \), so \( z < 1 + R \) and as a consequence

\[
\sum_{i=1}^{N_0+1} H(p_i) \geq - \sum_{i=1}^{N_0+1} W_i \ln W_i.
\]

Now, using the definition of \( M_1 \) and \( M_i \), it is easy to see that \( M_1 + W_{N_0+1} \leq C_{11} \left( \sqrt{\ln \frac{LN}{N} + \ln \frac{LN}{N}} \right) \). In particular for large \( N \) (uniformly in \( L \geq 2 \)) we have \( M_1 \ln M_1 + W_{N_0+1} 
\ln W_{N_0+1} \leq C_{12} \ln^2 L \) and so

\[
- \sum_{i=1}^{N_0+1} W_i \ln W_i \geq \sum_{i=1}^{N_0} W_i \ln W_i 
\geq - C_{12} \ln^2 L + \left( \sum_{i=1}^{N_0} W_i \right) \ln N
\geq \sum_{i=1}^{N_0} \frac{1}{N} \left( \sqrt{C_7 \frac{\ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}{N}} + C_7 \ln \left( \frac{LN}{i} \right) \right) \ln \left( \sqrt{C_7 \frac{\ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}{N}} + C_7 \ln \left( \frac{LN}{i} \right) \right)
\geq (L - 1) \ln N - (M_1 + W_{N_0+1}) \ln N - C_{12} \ln^2 L - B_N
\geq (L - 1) \ln N - C_{12} \ln^2 L - C_{11} \left( \sqrt{\ln \frac{LN}{N} + \ln \frac{LN}{N}} \right) \ln N - B_N,
\]

where

\[
B_N = \sum_{i=2}^{N_0} \frac{1}{N} \left( \sqrt{C_7 \frac{\ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}{N}} + C_7 \ln \left( \frac{LN}{i} \right) \right) \ln \left( \sqrt{C_7 \frac{\ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}{N}} + C_7 \ln \left( \frac{LN}{i} \right) \right).
\]

Now, the following holds for a sufficiently large absolute constant \( C_{13} \).

If \( i < LN/C_{13} \), then \( \ln \left( \frac{LN}{i} \right) \leq \left( \frac{LN}{i} \right)^{3/4} \) and using the inequality \( L \geq 2 \), we get

\[
\left( \frac{\sqrt{C_7 \ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}}{\sqrt{C_7 \ln \left( \frac{LAN}{i} \right) \ln \left( \frac{eLN}{i} \right)}} + C_7 \ln \left( \frac{LN}{i} \right) \right) \ln \left( \sqrt{C_7 \ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)} + C_7 \ln \left( \frac{LN}{i} \right) \right) \leq C_{14} \left( \frac{LN}{i} \right)^{7/8},
\]

for some absolute constant \( C_{14} \).

On the other hand if \( i > LN/C_{13} \), then

\[
\left( \frac{\sqrt{C_7 \ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)}}{\sqrt{C_7 \ln \left( \frac{LAN}{i} \right) \ln \left( \frac{eLN}{i} \right)}} + C_7 \ln \left( \frac{LN}{i} \right) \right) \ln \left( \sqrt{C_7 \ln \left( \frac{LN}{i} \right) \ln \left( \frac{eLN}{i} \right)} + C_7 \ln \left( \frac{LN}{i} \right) \right) \leq C_{15},
\]

where \( C_{15} \) is another absolute constant.
Thus, using $N_0 \leq LN$, we get
\[
B_N \leq \frac{C_{15}}{N}(N_0 - LN/C_{13}) + \frac{C_{14}(LN)^{7/8}}{N} \sum_{i=2}^{\lfloor LN/C_{13} \rfloor} \frac{1}{i^{7/8}} \quad (C27)
\]
\[
\leq C_{15}L + \frac{C_{14}(LN)^{7/8}}{N}C_{16}(LN/C_{13})^{1/8} \leq C_{17}L.
\]
It remains to bound from above the term $C_{12} \ln^2 L + C_{11} \left( \sqrt{\frac{\ln(LN)}{N}} + \frac{\ln(LN)}{N} \right) \ln N$ appearing in (C23). It is easy to see that for sufficiently large $N$ (uniformly in $L \geq 2$) it is bounded by $C_{18}L$.
Combining this estimate with (C23) and (C27) gives
\[
\sum_{i=1}^{N_0+1} W_i \ln W_i \geq (L - 1) \ln N - C_3 L, \quad (C28)
\]
with $C_3 = C_{17} + C_{18}$.

By (C22) this ends the proof of the theorem.

\begin{appendix}

\section*{Appendix D: SIMPLE MAJORIZATION LEMMA}

\begin{lemma}
Let $p \in \mathbb{R}^N$ be a probability vector and $x = p_1 \geq p_2 \geq \cdots \geq p_N \geq 0$. We define two vectors
\[
r = \left( x, \ldots, x, 1 - x \left\lfloor \frac{1}{x} \right\rfloor \right), \quad q = \left( x, \frac{1 - x}{N - 1}, \ldots, \frac{1 - x}{N - 1} \right), \quad (D1)
\]
we have the following majorization relations
\[
q \prec p \prec r. \quad (D2)
\]
In the case of Shannon entropy we get
\[
H(p) \geq H(r) = H \left( x, \ldots, x, 1 - x \left\lfloor \frac{1}{x} \right\rfloor \right) = -x \left\lfloor \frac{1}{x} \right\rfloor \ln x - \left( 1 - x \left\lfloor \frac{1}{x} \right\rfloor \right) \ln \left( 1 - x \left\lfloor \frac{1}{x} \right\rfloor \right) \quad (D3)
\]
\[
\geq -x \left\lfloor \frac{1}{x} \right\rfloor \ln x \geq -(1 - x) \ln x
\]
and
\[
H(p) \leq H(q) = H \left( x, \frac{1 - x}{N - 1}, \ldots, \frac{1 - x}{N - 1} \right) = -x \ln x - (N - 1) \frac{1 - x}{N - 1} \ln \left( \frac{1 - x}{N - 1} \right) \quad (D4)
\]
\[
= -x \ln x - (1 - x) \ln(1 - x) + (1 - x) \ln(N - 1) = H(x, 1 - x) + (1 - x) \ln(N - 1).
\]
\end{lemma}

\end{appendix}


