Higher entropic uncertainty relations for anti-commuting observables

Stephanie Wehner' and Andreas Winter'

Citation: Journal of Mathematical Physics **49**, 062105 (2008); doi: 10.1063/1.2943685
View online: http://dx.doi.org/10.1063/1.2943685
View Table of Contents: http://aip.scitation.org/toc/jmp/49/6
Published by the American Institute of Physics

Higher entropic uncertainty relations for anti-commuting observables

Stephanie Wehner[1,a)] and Andreas Winter[2,3,b)]
[1]*Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*
[2]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
[3]*Quantum Information Technology Laboratory, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore*

(Received 18 April 2008; accepted 22 May 2008; published online 20 June 2008)

Uncertainty relations provide one of the most powerful formulations of the quantum mechanical principle of complementarity. Yet, very little is known about such uncertainty relations for more than two measurements. Here, we show that sufficient unbiasedness for a set of binary observables, in the sense of mutual anticommutation, is good enough to obtain maximally strong uncertainty relations in terms of the Shannon entropy. We also prove nearly optimal relations for the collision entropy. This is the first systematic and explicit approach to finding an arbitrary number of measurements for which we obtain maximally strong uncertainty relations. Our results have immediate applications to quantum cryptography. © *2008 American Institute of Physics.* [DOI: 10.1063/1.2943685]

I. INTRODUCTION

Uncertainty relations lie at the very core of quantum mechanics. For any observable, it only has sharp values (in the sense that the measurement outcome is deterministic) for its own eigenstates. However, for any other state, the distribution of measurement outcomes is more or less smeared out, or more conveniently expressed: its entropy is strictly positive. Hence, if two or more observables have no eigenstates in common, the sum of these respective entropies is strictly greater than 0 for any state we may measure. We thereby say that a set of observables is more "incompatible" than another, if this sum takes on a larger value. But what makes observables more incompatible? Or rather, what characterizes maximally incompatible observables? Here, we show how to obtain maximally strong uncertainty relations for a large number of binary observables that exhibit simple geometrical properties.

Uncertainty relations are most well known in the form proposed by Heisenberg[1] and generalized by Robertson.[2] Entropic uncertainty relations are an alternative way to state Heisenberg's uncertainty principle. They are frequently a more useful characterization because the "uncertainty" is lower bounded by a quantity that only depends on the eigenstates of the observables, and not on the actual physical quantity to be measured,[3,4] as in Heisenberg's formulation with standard deviations—see also the more recent paper.[5] Following a conjecture by Kraus,[6] Maassen and Uffink[7] proven an entropic uncertainty relation for *two* observables. In particular, they showed that if we measure any state $\rho \in \mathcal{H}$ with $\dim \mathcal{H}=d$ using observables with eigenbases $\mathcal{A}=\{|a_1\rangle,\ldots,|a_d\rangle\}$ and $\mathcal{B}=\{|b_1\rangle,\ldots,|b_d\rangle\}$ respectively, we have

a)Electronic mail: s.d.c.wehner@cwi.nl.
b)Electronic mail: a.j.winter@bris.ac.uk.

$$\tfrac{1}{2}(H(\mathcal{A}|\rho) + H(\mathcal{B}|\rho)) \geq -\log c(\mathcal{A},\mathcal{B}),$$

where $c(\mathcal{A},\mathcal{B}) = \max\{|\langle a|b\rangle| : |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}\}$ and $H(\mathcal{A}|\rho) = -\Sigma_{i=1}^{d} \langle a_i|\rho|a_i\rangle \log\langle a_i|\rho|a_i\rangle$ is the Shannon entropy arising from measuring the state ρ in basis $\mathcal{A}$. Here, the most incompatible measurements arise from choosing $\mathcal{A}$ and $\mathcal{B}$ to be *mutually unbiased bases* (MUBs). That is, for any $|a\rangle \in \mathcal{A}$ and any $|b\rangle \in \mathcal{B}$ we have $|\langle a|b\rangle| = 1/\sqrt{d}$, giving us a lower bound of $\frac{1}{2}\log d$. Clearly, this bound is tight: Choosing $\rho = |a_i\rangle\langle a_i|$ for $|a_i\rangle \in \mathcal{A}$ gives us exactly $\frac{1}{2}\log d$, with maximum uncertainty for one of the two observables and none for the other.

But how about more than two observables? Sadly, very little is known about this case so far. Yet, this question not only eludes our current understanding of quantum mechanics but also has practical consequences for quantum cryptography in the bounded storage model, where proving the security of protocols ultimately reduces to finding such relations.[8] Proving new entropic uncertainty relations could thus give rise to new protocols. Furthermore, uncertainty relations for more than two measurements could also be useful to understand other quantum effects that are derived from such relations, such as locking classical information in quantum states.[9] Sanchez-Ruiz[10–12] has shown that for a full set of $d+1$ MUBs $\mathcal{A}_1, \ldots, \mathcal{A}_{d+1}$, we have

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H(\mathcal{A}_j|\rho) \geq \log\left(\frac{d+1}{2}\right),$$

and for $d=2$ gave a lower bound of 2/3. Indeed, strong uncertainty relations for a smaller number of bases do exist. If we choose a set $\mathcal{T}$ of $(\log d)^4$ bases uniformly at random, then (with high probability) we have that for all states ρ: $1/|\mathcal{T}|\Sigma_{\mathcal{B}\in\mathcal{T}} H(\mathcal{B}|\rho) \geq \log d - 3$.[13] This means that there exist $(\log d)^4$ bases for which the sum of entropies is very large, i.e., measurements in such bases are very incompatible. However, no explicit constructions are known. It may be tempting to conjecture that simply choosing our measurements to be mutually unbiased leads to strong uncertainty relations, in general. In fact, when choosing bases at random they will be almost mutually unbiased. In this case, we might expect the entropy average to be quite large: if the state to be measured is an eigenstate of one of the bases, the corresponding entropy average will be $(1 - 1/|\mathcal{T}|)\log d$. This value is thus clearly an upper bound on the minimum entropy average $\min_\rho 1/|\mathcal{T}|\Sigma_{\mathcal{B}\in\mathcal{T}} H(\mathcal{B}|\rho)$ for any set of bases, mutually unbiased or not. Perhaps surprisingly, however, choosing the bases to be mutually unbiased is not the right property: there exists up to $|\mathcal{T}| \leq \sqrt{d}$ MUBs for which $\min_\rho 1/|\mathcal{T}|\Sigma_{\mathcal{B}\in\mathcal{T}} H(\mathcal{B}|\rho) = 1/2 \log d$.[14] Note that the right hand side is a lower bound for any set of MUBs, since it is the average of pairs of entropies to which we can apply the uncertainty relation by Maassen and Uffink.[7] Hence we call this the trivial lower bound. When considering entropic uncertainty relations as a measure of "incompatibility," we must thus look for different properties to obtain strong uncertainty relations. But, what properties lead to strong entropic uncertainty relations for more than two observables?

Here, we show that for binary observables we obtain maximally strong uncertainty relations for the Shannon entropy if they satisfy the property that they *anticommute*. We also obtain a nearly optimal uncertainty relation for the collision entropy (Rényi entropy of order of 2) $H_2(X) = -\log \Sigma_x P_X(x)^2$ that is of particular relevance to cryptography. As we will see, we can take the anticommuting observables to have a particularly simple form that in principle allows us to apply our result to quantum cryptography using present-day technology.

II. CLIFFORD ALGEBRA

For our result we will make use of the structure of Clifford algebra,[15–17] which has many beautiful geometrical properties of which we shall use a few. For any integer n, the free real associative algebra generated by $\Gamma_1, \ldots, \Gamma_{2n}$, subject to the anticommutation relations

$$\{\Gamma_j, \Gamma_k\} = \Gamma_j\Gamma_k + \Gamma_k\Gamma_j = 2\delta_{jk}\mathbb{1}, \tag{1}$$

is called *Clifford algebra*. We briefly recall its most essential properties that we will use in this

text. The Clifford algebra has a unique representation by Hermitian matrices on n qubits (up to unitary equivalence) which we fix henceforth. This representation can be obtained via the famous Jordan–Wigner transformation,[18]

$$\Gamma_{2j-1} = Z^{\otimes(j-1)} \otimes X \otimes \mathbb{1}^{\otimes(n-j)},$$

$$\Gamma_{2j} = Z^{\otimes(j-1)} \otimes Y \otimes \mathbb{1}^{\otimes(n-j)},$$

for $j=1,\ldots,n$, where we use X, Y, and Z to denote the Pauli matrices.

Let us first consider these operators themselves. Evidently, each operator Γ_i has exactly two eigenvalues ± 1: Let $|\eta\rangle$ be an eigenvector of Γ_i with eigenvalue λ. From $\Gamma_i^2=\mathbb{1}$ we have that $\lambda^2=1$. Furthermore, we have $\Gamma_i(\Gamma_j|\eta\rangle)=-\lambda\Gamma_j|\eta\rangle$. We can therefore express each Γ_i as

$$\Gamma_i = \Gamma_i^0 - \Gamma_i^1,$$

where Γ_i^0 and Γ_i^1 are projectors onto the positive and negative eigenspaces of Γ_i, respectively. Furthermore, note that we have for $i \neq j$

$$\mathrm{Tr}(\Gamma_i\Gamma_j) = \tfrac{1}{2}\mathrm{Tr}(\Gamma_i\Gamma_j + \Gamma_j\Gamma_i) = 0.$$

That is, all such operators are orthogonal. Hence, the positive and negative eigenspaces of such operators are similarly mutually unbiased than bases can be: we have that for all $i \neq j$

$$\mathrm{Tr}(\Gamma_i\Gamma_j^0) = \mathrm{Tr}(\Gamma_i\Gamma_j^1).$$

The crucial aspect of the Clifford algebra that makes it so useful in geometry is that we can view the operators $\Gamma_1,\ldots,\Gamma_{2n}$ as $2n$ orthogonal vectors forming a basis for $\mathbb{R}^{2n}$. Each vector $a=(a_1,\ldots,a_{2n})\in\mathbb{R}^{2n}$ can then be written as $a=\Sigma_j a_j\Gamma_j$. Note that the inner product of two vectors obeys $a\cdot b=\Sigma_j a_j b_j\mathbb{1}=\{a,b\}/2$, where ab is the Clifford product which here is just equal to the matrix product. Hence, anticommutation takes a geometric meaning within the algebra: two vectors anticommute if and only if they are orthogonal. Evidently, if we now transform the generating set of Γ_j linearly to obtain the new operators

$$\Gamma_k' = \sum_j T_{jk}\Gamma_j,$$

then the set $\{\Gamma_1',\ldots,\Gamma_{2n}'\}$ satisfies the anticommutation relations if and only if $(T_{jk})_{jk}$ is an orthogonal matrix: these are exactly the operations which preserve the inner product. Because of the uniqueness of representation, there exists a matching unitary $U(T)$ of $\mathcal{H}$ which transforms the operator basis on the Hilbert space level, by conjugation

$$\Gamma_j' = U(T)\Gamma_j U(T)^\dagger.$$

Essentially, we can think of the positive and negative eigenspaces of such operators as the positive and negative directions of the basis vectors.

It will be particularly useful that the collection of operators

$$\mathbb{1}$$

$$\Gamma_j (1 \leq j \leq 2n),$$

$$\Gamma_{jk} = i\Gamma_j\Gamma_k (1 \leq j < k \leq 2n),$$

$$\Gamma_{jk\ell} = \Gamma_j\Gamma_k\Gamma_\ell (1 \leq j < k < \ell \leq 2n),$$

$$\vdots$$

$$\Gamma_{12\ldots(2n)} = i\Gamma_1\Gamma_2\cdots\Gamma_{2n} =: \Gamma_0$$

form an orthogonal basis for the $d\times d$ complex matrices for $d=2^n$, again by the anticommutation relations. By counting, the above operators form a complete operator basis with respect to the Hilbert–Schmidt inner product. Notice that the products with an odd number of factors are Hermitian, while the ones with an even number of factors are skew-Hermitian, so in the definition of the above operators we introduce a factor of i to all with an even number of indices to make the whole set a real basis for the Hermitian operators. Working out the above terms using the representation from above, we can see that this gives us the familiar Pauli basis consisting of elements $B_j^1\otimes\ldots\otimes B_j^n$ with $B_j^i\in\{\mathbb{1},X,Y,Z\}$.

Hence we can write every state ρ on $\mathcal{H}$ as

$$\rho = \frac{1}{d}\left(\mathbb{1} + \sum_j g_j\Gamma_j + \sum_{j<k} g_{jk}\Gamma_{jk} + \cdots + g_0\Gamma_0\right). \tag{2}$$

This expansion has been used before in quantum information theory, see, e.g., Ref. 17. The (real valued) coefficients $(g_1,\ldots,g_{2n})$ in this expansion are called "vector" components and the ones belonging to degree $k>1$ products of Γ's are "tensor" or k-vector components. k-vectors also have very nice geometric interpretation within the algebra: they represent oriented plane and higher volume elements. The—unique—coordinate Γ_0 of degree $2n$ also plays special role (it corresponds to the volume element in $\mathbb{R}^{2n}$), and is called the "pseudoscalar" component. Note that it anticommutes with all the Γ_j, which has another important consequence: Substituting Γ_0 for any of the Γ_j again yields a generating set of the Clifford algebra, hence there exists a unitary on $\mathcal{H}$ taking the original to the new basis by conjugation.

The vector and pseudoscalar components of the Clifford algebra span a $(2n+1)$-dimensional space isomorphic to $\mathbb{R}^{2n+1}$: indeed, extending the $\mathrm{O}(2n)$ symmetry of $\mathrm{span}\{\Gamma_1,\ldots,\Gamma_{2n}\}$, the extended $\mathrm{span}\{\Gamma_0,\Gamma_1,\ldots,\Gamma_{2n}\}$ has the symmetry of $\mathrm{SO}(2n+1)$: for every special-orthogonal $(2n+1)\times(2n+1)$ matrix $\tilde{T}$, we can write transformed Clifford operators $\Gamma'_k=\Sigma_{j=0}^{2n}\tilde{T}_{jk}\Gamma_j$ obeying the anticommutation relations. As before (but now this requires an additional proof that we provide in the Appendix using the condition $\det\tilde{T}=1$), there exists a unitary $U(\tilde{T})$ of the underlying Hilbert space $\mathcal{H}$ such that for all $j=0,\ldots,2n$, $\Gamma'_j=U(\tilde{T})\Gamma_jU(\tilde{T})^\dagger$.

Using the orthogonal group symmetry of the Clifford algebra, we show the following lemma in the Appendix.

Lemma 1: The linear map $\mathbb{P}$ *taking* ρ *as in Eq. (2) to*

$$\mathbb{P}(\rho) := \frac{1}{d}\left(\mathbb{1} + \sum_{j=0}^{2n} g_j\Gamma_j\right) \tag{3}$$

is positive. That is, if ρ *is a state, then so is* $\mathbb{P}(\rho)$, *and in this case* $\Sigma_{j=0}^{2n}g_j^2\leq 1$. *Conversely, if* $\Sigma_{j=0}^{2n}g_j^2\leq 1$, *then*

$$\sigma = \frac{1}{d}\left(\mathbb{1} + \sum_{j=0}^{2n} g_j\Gamma_j\right)$$

is positive semidefinite, hence a state.

It is interesting to note that the map $\mathbb{P}$ is positive, but not *completely positive*, for any $n>1$, as one can see straightforwardly by looking at its Choi–Jamiołkowski operator.

III. APPLICATIONS

We now first use the tools from above to prove a "meta-uncertainty" relation, from which we will then derive two new entropic uncertainty relations. Evidently, we have immediately from the above the following.

Lemma 2: Let $\rho \in \mathcal{H}$ *with* $\dim \mathcal{H}=2^n$ *be a quantum state and consider* $K \leq 2n+1$ *anticommuting observables* Γ_j *as defined above. Then*,

$$\sum_{j=0}^{K-1} (\mathrm{Tr}(\rho\Gamma_j))^2 \leq \sum_{j=0}^{2n} (\mathrm{Tr}(\rho\Gamma_j))^2 \leq 1.$$

□

Our result is essentially a generalization of the Bloch sphere picture to higher dimensions (see also Ref. 17): For $n=1$ ($d=2$) the state is parametrized by $\rho=\frac{1}{2}(\mathbb{1}+g_1\Gamma_1+g_2\Gamma_2+g_0\Gamma_0)$, where $\Gamma_1=X$, $\Gamma_2=Z$, and $\Gamma_0=Y$ are the familiar Pauli matrices. Lemma 2 tells us that $g_0^2+g_1^2+g_2^2 \leq 1$, i.e., the state must lie inside the Bloch sphere. Our result may be of independent interest, since it is often hard to find conditions on the coefficients $g_1, g_2, \ldots$, such that ρ is a state.

Notice that the $g_j=\mathrm{Tr}(\rho\Gamma_j)$ are directly interpreted as the expectations of the observables Γ_j. Indeed, g_j is precisely the bias of the ± 1-variable Γ_j

$$\Pr\{\Gamma_j = 1|\rho\} = \frac{1+g_j}{2}.$$

Hence, we can interpret Lemma 2 as a form of uncertainty relation between the observables Γ_j: if one or more of the observables have a large bias (i.e., they are more precisely defined), this limits the bias of the other observables (i.e., they are closer to uniformly distributed).

Indeed, Lemma 2 has strong consequences for the Rényi and von Neumann entropic averages,

$$\frac{1}{K}\sum_{j=0}^{K-1} H_\alpha(\Gamma_j|\rho),$$

where $H_\alpha(\Gamma_j|\rho)$ is the Rényi entropy at α of the probability distribution arising from measuring the state ρ with observable Γ_j. The minima of such expressions can be interpreted as giving entropic uncertainty relations, as we shall now do for $\alpha=2$ (the collision entropy) and $\alpha=1$ (the Shannon entropy).

Theorem 3: *Let* $\dim \mathcal{H}=2^n$, *and consider* $K \leq 2n+1$ *anticommuting observables as defined above. Then*,

$$\min_\rho \frac{1}{K}\sum_{j=0}^{K-1} H_2(\Gamma_j|\rho) = 1 - \log\left(1+\frac{1}{K}\right) \sim 1 - \frac{\log e}{K},$$

where $H_2(\Gamma_j|\rho)=-\log \Sigma_{b\in\{0,1\}}\mathrm{Tr}(\Gamma_j^b\rho)^2$, *and the minimization is taken over all states* ρ. *The latter holds asymptotically for large* K.

Proof: Using the fact that $\Gamma_j^b=(\mathbb{1}+(-1)^b\Gamma_j)/2$ we can first rewrite

$$\frac{1}{K}\sum_{j=0}^{K-1} H_2(\Gamma_j|\rho) = -\frac{1}{K}\sum_{j=0}^{K-1} \log\left[\frac{1}{2}(1+\mathrm{Tr}(\rho\Gamma_j)^2)\right] \geq -\log\left(\frac{1}{2K}\sum_{j=0}^{K-1}(1+g_j^2)\right) \geq 1-\log\left(1+\frac{1}{K}\right),$$

where the first inequality follows from Jensen's inequality and the concavity of the log, and the second from Lemma 2. Clearly, the minimum is attained if all $g_j=\mathrm{Tr}(\rho\Gamma_j)=\sqrt{1/K}$. It follows from Lemma 1 that our inequality is tight. Via the Taylor expansion of $\log(1+1/K)$ we obtain the asymptotic result for large K. □

For the Shannon entropy ($\alpha=1$) we obtain something even nicer.

Theorem 4: *Let* $\dim \mathcal{H}=2^n$ *and consider* $K\leq 2n+1$ *anticommuting observables as defined above. Then*,

$$\min_{\rho}\frac{1}{K}\sum_{j=0}^{K-1} H(\Gamma_j|\rho)=1-\frac{1}{K},$$

where $H(\Gamma_j|\rho)=-\Sigma_{b\in\{0,1\}}\mathrm{Tr}(\Gamma_j^b\rho)\log \mathrm{Tr}(\Gamma_j^b\rho)$, *and the minimization is taken over all states* ρ.

Proof: To see this, note that by rewriting our objective as above, we observe that we need to minimize the expression

$$\frac{1}{K}\sum_{j=0}^{K-1} H\left(\frac{1\pm\sqrt{t_j}}{2}\right),$$

subject to $\Sigma_j t_j\leq 1$ and $t_j\geq 0$, via the identification $t_j=(\mathrm{Tr}(\rho\Gamma_j))^2$. An elementary calculation (included in the Appendix for completeness) shows that the function $f(t)=H(1\pm\sqrt{t}/2)$ is concave in $t\in[0;1]$. Hence, by Jensen's inequality (read in the opposite direction), the minimum is attained with all the t_j being extremal, i.e., one of the t_j is 1 and the others are 0, giving just the lower bound of $1-1/K$. □

It is clear that based on Lemma 1 one can derive similar uncertainty relations for other Rényi entropies ($\alpha\neq 1,2$) by performing the analogous optimization. We stuck to the two values above as they are the most relevant in view of the existing literature; for example, using the same convexity arguments as for $\alpha=2$, we obtain for $\alpha=\infty$

$$\frac{1}{K}\sum_{j=0}^{K-1} H_\infty(\Gamma_j|\rho)\geq 1-\log\left(1+\frac{1}{\sqrt{K}}\right).$$

This should be compared to Deutsch's inequality[4] for the case of two MUBs of a qubit because the latter really is about H_∞.

IV. DISCUSSION

We have shown that anticommuting Clifford observables obey the strongest possible uncertainty relation for the von Neumann entropy. It is interesting that in the process of the proof, however, we have found three uncertainty type inequalities (the sum of squares bound, the bound on H_2, and finally the bound on H_1), and all three have a different structure of attaining the limit. The sum of squares bound can be achieved in every direction (meaning for every tuple satisfying the bound we get one attaining it by multiplying all components by some appropriate factor), the H_2 expression requires all components to be equal, while the H_1 expression demands exactly the opposite.

Our result for the collision entropy is slightly suboptimal but strong enough for all cryptographic purposes. Indeed, one could use our entropic uncertainty relation in the bounded quantum storage setting to construct, for instance, one-out-of-K oblivious transfer protocols analogous to Ref. 8. Here, instead of encoding a single bit into either the computational or Hadamard basis, which gives us a one-out-of-two oblivious transfer, we now encode a single bit into the positive or negative eigenspace of each of these K operators. It is clear from the representation of such operators discussed earlier that such an encoding can be done experimentally as easily as encoding a single bit into three MUBs given by the Pauli operators X, Y, and Z. Indeed, our construction can be seen as a direct extension of such an encoding: we obtain the uncertainty relations for these three MUBs used in Ref. 8, previously proven by Sanchez-Ruiz,[10,11] as a special case of our analysis for $K=3$ ($d=2$).

Alas, strong uncertainty relations for measurements with more than two outcomes remain inaccessible to us. It has been shown[19] that uncertainty relations for more outcomes can be obtained via a coding argument from uncertainty relations as we construct them here. Yet, these seem far from optimal. A natural choice would be to consider the generators of a generalized

Clifford algebra,[20,21] yet this algebra does not have the nice symmetry properties which enabled us to implement operations on the vector components above. It remains an exciting open question, whether such operators form a good generalization or whether we must continue our search for new properties.

ACKNOWLEDGMENTS

The authors acknowledge support by the EC project "QAP" (Grant No. IST-2005-015848). S.W. was additionally supported by the NWO vici project 2004–2009. A.W. was additionally supported by the EPSRC-GB via the "IRC QIP" and an Advanced Research Fellowship. S.W. thanks Andrew Doherty for an explanation of the Jordan–Wigner transform.

APPENDIX

$SO(2n+1)$ structure. While the orthogonal group symmetry of the vector component of the Clifford algebra, spanned by the generators $\{\Gamma_1,\ldots,\Gamma_{2n}\}$, is usually covered in textbook accounts, the symmetry of the extended set $\{\Gamma_0,\Gamma_1,\ldots,\Gamma_{2n}\}$, including the pseudoscalar element, seems much less well known. It is quite natural to consider this set as all its elements mutually anticommute, so any family $\mathcal{K}=(k_1,\ldots,k_{2n})$ of $2n$ pairwise distinct elements will generate the full Clifford algebra. Hence there exists a unitary $U(\mathcal{K})$ mapping the original generators Γ_j to the Γ_{k_j}:

$$\Gamma_{k_j}=U(\mathcal{K})\Gamma_j U(\mathcal{K})^\dagger.$$

The initial observation is that indeed an orthogonal transformation T of the $2n$ generators extends to a special-orthogonal transformation $\tilde{T}=(\det T)\oplus T$ of the extended set, since

$$\Gamma_0'=U(T)\Gamma_0 U(T)^\dagger=i\Gamma_1'\cdots\Gamma_{2n}'=(\det T)\Gamma_0.$$

A nice and easy geometrical way of seeing this is via the higher-dimensional analog of the well-known Euler angle parametrization of orthogonal matrices (see Ref. 22).

Euler angle decomposition.[23] *Let* T be an $N\times N$ orthogonal matrix. Then there exist angles $\theta_{jk}\in[0;2\pi)$ for $1\leq j<k\leq N$, such that

$$T=E_1^{\det T}\prod_{j<k}R_{jk}(\theta_{jk}),$$

where $E_1^\epsilon=\epsilon|1\rangle\langle 1|+\Sigma_{i>1}|j\rangle\langle j|$ is either the identity or the reflection along the first coordinate axis and $R_{jk}(\theta)$ is the rotation by angle θ in the plane spanned by the jth and kth coordinate axes, i.e.,

$$R_{jk}(\theta)=\cos\theta|j\rangle\langle j|+\sin\theta|k\rangle\langle j|-\sin\theta|j\rangle\langle k|+\cos\theta|k\rangle\langle k|+\sum_{i\neq j,k}|i\rangle\langle i|.$$

(The product is to be taken in some fixed order of the indices, say, lexicographically.) □

With this, we only have to understand how Γ_0 transforms under the action of the elementary transformations E_1^ϵ and $R_{jk}(\theta)$. Clearly, under the former,

$$\Gamma_0'=\epsilon\Gamma_0,$$

while for the latter (using the abbreviations $c=\cos\theta$ and $s=\sin\theta$),

$$\begin{aligned}\Gamma_0'&=i\Gamma_1'\cdots\Gamma_{2n}'=i\Gamma_1\cdots\Gamma_{j-1}\cdot(c\Gamma_j+s\Gamma_k)\Gamma_{j+1}\cdots\Gamma_{k-1}(-s\Gamma_j+c\Gamma_k)\cdot\Gamma_{k+1}\cdots\Gamma_{2n}\\&=i(c^2+s^2)\Gamma_1\cdots\Gamma_{2n}+i(-cs+sc)\Gamma_1\cdots\Gamma_{j-1}\Gamma_{j+1}\cdots\Gamma_{k-1}\Gamma_{k+1}\cdots\Gamma_{2n}\\&=\Gamma_0.\end{aligned}$$

Now, for a general special-orthogonal transformation $\tilde{T}$ of the $2n+1$ coordinates of the extended set, the Euler angle decomposition gives

$$\tilde{T} = \prod_{0 \le j < k \le 2n} R_{jk}(\theta_{jk}).$$

Then, the unitary representation $U(\tilde{T})$ clearly has to be the product of terms $U(R_{jk}(\theta))$. For $1 \le j < k \le 2n$ we know already what these are, as the transformation is only one of the generating set $\{\Gamma_1, \ldots, \Gamma_{2n}\}$ (and by the above observation the pseudoscalar Γ_0 is indeed left alone, as required); for $0 = j < k \le 2n$ on the other hand, we first map the generating set $\mathcal{K} = \{\Gamma_0, \Gamma_k \ldots\}$ to $\{\Gamma_1, \ldots, \Gamma_{2n}\}$ by the unitary $U(\mathcal{K})^\dagger$, then apply the unitary belonging to $R_{12}(\theta)$ and then map the generators back via $U(\mathcal{K})$. This clearly implements

$$U(R_{jk}(\theta)) = U(\mathcal{K}) U(R_{12}(\theta)) U(\mathcal{K})^\dagger,$$

and we are done. □

Proof of Lemma 1: First, we show that there exists a unitary U such that $\rho' = U\rho U^\dagger$ has no pseudoscalar and only one nonzero vector component, say, at Γ_1, which we can choose to be $g_1' = \sqrt{\Sigma_{j=0}^{2n} g_j^2}$. Indeed, there is a special-orthogonal transformation T^{-1} of the coefficient vector $(g_0, g_1, \ldots, g_{2n})$ to a vector whose zeroth as well as second until last components are all 0: since the length is preserved, this is consistent with the first component becoming $\sqrt{\Sigma_j g_j^2}$.

Now, let $U = U(T)$ be the corresponding unitary of the Hilbert space. By the above-mentioned representation of $\mathrm{SO}(2n+1)$ on $\mathcal{H}$, we arrive at a new, simpler looking state,

$$\rho' = U(T)\rho U(T)^\dagger = \frac{1}{d}\left(\mathbb{1} + g_1'\Gamma_1 + \sum_{j<k} g_{jk}'\Gamma_{jk} + \cdots + 0\Gamma_0\right),$$

for some g_{jk}', etc.

There exist of course orthogonal transformations F_j that take Γ_k to $(-1)^{\delta_{jk}}\Gamma_k$. Such transformations flip the sign of a chosen Clifford generator. They can be extended to a special-orthogonal transformation of $\mathrm{span}\{\Gamma_0, \ldots, \Gamma_{2n}\}$ by also flipping the sign of Γ_0: $F_j\Gamma_0 = -\Gamma_0$. (Using the geometry of the Clifford algebra it is easy to see that $U(F_j) = \Gamma_0\Gamma_j$ fulfills this task.) Now, consider

$$\rho'' = \tfrac{1}{2}\rho' + \tfrac{1}{2}U(F_j)\rho' U(F_j)^\dagger,$$

for $j > 1$.

Clearly, if ρ' were a state, then the new operator ρ'' would also be a state. We claim that ρ' has no terms with an index j in its Clifford basis expansion: Note that if we flip the sign of precisely those terms that have an index j (i.e., they have a factor Γ_j in the definition of the operator basis), and then the coefficients cancel with those of ρ'.

We now iterate this map through $j = 2, 3, \ldots, 2n$, and we are left with a final state $\hat{\rho}$, which hence must be of the form

$$\hat{\rho} = \frac{1}{d}(\mathbb{1} + g_1'\Gamma_1).$$

By applying $U(T)^\dagger$ from above, we now transform $\hat{\rho}$ to $U(T)^\dagger\hat{\rho}U(T) = \mathbb{P}(\rho)$, which is the first part of the lemma.

Looking at $\hat{\rho}$ once more, we see that this can be positive semidefinite only if $g_1' \le 1$, i.e., $\Sigma_{j=0}^{2n} g_j^2 \le 1$.

Conversely, if $\Sigma_{j=0}^{2n} g_j^2 \le 1$, then the (Hermitian) operator $A = \Sigma_j g_j \Gamma_j$ has the property

$$A^2 = \sum_{jk} g_j g_k \Gamma_j \Gamma_k = \sum_j g_j^2 \mathbb{1} \le \mathbb{1},$$

i.e., $-\mathbb{1} \le A \le \mathbb{1}$, so $\sigma = 1/d(\mathbb{1} + A) \ge 0$. □

Concavity of $f(t) = H(1 \pm \sqrt{t}/2)$. Straightforward calculation shows that

$$f'(t) = \frac{1}{4\ln 2}\frac{1}{\sqrt{t}}(\ln(1-\sqrt{t}) - \ln(1+\sqrt{t})),$$

and so

$$f''(t) = \frac{1}{8\ln 2}\frac{1}{t^{3/2}}\left(\ln\frac{1+\sqrt{t}}{1-\sqrt{t}} - \frac{2\sqrt{t}}{1-t}\right).$$

Since we are only interested in the sign of the second derivative, we ignore the (positive) factors in front of the bracket, and are done if we can show that

$$g(t) := \ln\frac{1+\sqrt{t}}{1-\sqrt{t}} - \frac{2\sqrt{t}}{1-t} = \ln(1+\sqrt{t}) + \frac{1}{1+\sqrt{t}} - \ln(1-\sqrt{t}) - \frac{1}{1-\sqrt{t}}$$

is nonpositive for $0 \le t \le 1$. Substituting $s = 1-\sqrt{t}$, which is also between 0 and 1, we rewrite this as

$$h(s) = -\ln s - \frac{1}{s} + \ln(2-s) + \frac{1}{2-s},$$

which has derivative

$$h'(s) = (1-s)\left(\frac{1}{s^2} - \frac{1}{(2-s)^2}\right),$$

and this is clearly positive for $0 < s < 1$. In other words, h increases from its value at $s=0$ [where it is $h(0) = -\infty$] to its value at $s=1$ [where it is $h(1)=0$], so indeed $h(s) \le 0$ for all $0 \le s \le 1$.

Consequently, also $f''(t) \le 0$ for $0 \le t \le 1$, and we are done. □

Constructive proof of Lemma 1: For the interested reader, we now give an explicit construction of the unitaries $U(T)$ and $U(F_j)$, which, however, requires a more intimate knowledge of the Clifford algebra. First of all, recall that we can write two vectors $a, b \in \mathbb{R}^{2n}$ in terms of the generators of the Clifford algebra as $a = \sum_{j=1}^{2n} a_j \Gamma_j$ and $b = \sum_{j=1}^{2n} b_j \Gamma_j$. The Clifford product of the two vectors is defined as $ab = a \cdot b + a \wedge b$, where $a \wedge b$ is the outer product of the two vectors.[15,16] When using the matrix representation of the Clifford algebra given above, this product is simply the matrix product. Second, it is well known that within the Clifford algebra we may write the vector resulting from a reflection of the vector α on the plane perpendicular to the vector b (in 0) as $-bab$. Rotations can then be expressed as successive reflections.[15,16]

We first consider $U(T)$. Here, our goal is to find the transformation $U(T)$ that rotates the vector $g = \sum_{j=0}^{2n} g_j \Gamma_j$ to the vector $b = \sqrt{\ell}\Gamma_1$, where we let $\ell := \sum_{j=0}^{2n} g_j^2$. Finding such a transformation for only the first $2n$ generators can easily be achieved. The challenge is thus to include Γ_0. To this end we perform three individual operations: First, we rotate $g' = \sum_{j=1}^{2n} g_j \Gamma_j$ onto the vector $b' = \sqrt{\ell'}\Gamma_1$ with $\ell' := \sum_{j=1}^{2n} g_j^2$. Second, we exchange Γ_2 and Γ_0. Finally we rotate the vector $g'' = \sqrt{\ell'}\Gamma_1 + g_0\Gamma_2$ onto the vector $b = \sqrt{\ell}\Gamma_1$.

First, we rotate $g' = \sum_{j=1}^{2n} g_j \Gamma_j$ onto the vector $b' = \sqrt{\ell'}\Gamma_1$: Consider the vector $\hat{g} = 1/\sqrt{\ell'}\, g'$. We have $\hat{g}^2 = |\hat{g}|^2 \mathbb{1} = \mathbb{1}$ and thus the vector is of length 1. Let $m = \hat{g} + \Gamma_1$ denote the vector lying in the plane spanned by Γ_1 and $\hat{g}$ located exactly half way between Γ_1 and $\hat{g}$. Let $\hat{m} = c(\hat{g} + \Gamma_1)$ with $c = 1/\sqrt{2(1 + g_1/\sqrt{\ell'})}$. It is easy to verify that $\hat{m}^2 = \mathbb{1}$ and hence the vector $\hat{m}$ has length 1. To rotate the vector g' onto the vector b', we now need to first reflect g' around the plane perpendicular to $\hat{m}$, and then around the plane perpendicular to Γ_1. Hence, we now define $R = \Gamma_1 \hat{m}$. Evidently, R is unitary since $RR^\dagger = R^\dagger R = \mathbb{1}$. First of all, note that

$$Rg' = \Gamma_1 \hat{m} g' = c\Gamma_1 \left(\frac{1}{\sqrt{\ell'}} g' + \Gamma_1 \right) g' = c\left(\Gamma_1 \frac{a^2}{\sqrt{\ell'}} + \Gamma_1^2 g' \right) = c\sqrt{\ell'} \left(\Gamma_1 + \frac{1}{\sqrt{\ell'}} g' \right) = \sqrt{\ell'} \hat{m}.$$

Hence,

$$Rg' R^\dagger = \sqrt{\ell'} \hat{m} \hat{m} \Gamma_1 = \sqrt{\ell'} \Gamma_1 = b',$$

as desired. Using the geometry of the Clifford algebra, one can see that k-vectors remain k-vectors when transformed with the rotation R.[16] Similarly, it is easy to see that Γ_0 is untouched by the operation R,

$$R\Gamma_0 R^\dagger = \Gamma_0 R R^\dagger = \Gamma_0,$$

since $\{\Gamma_0, \Gamma_j\} = 0$ for all $j \in \{1, \ldots, 2n\}$. We can thus conclude that

$$R\rho R^\dagger = \frac{1}{d} \left(\mathbb{1} + \sqrt{\ell'} \Gamma_1 + g_0 \Gamma_0 + \sum_{j<k} g'_{jk} \Gamma_{jk} + \cdots \right),$$

for some coefficients g'_{jk}.

Second, we exchange Γ_2 and Γ_0: To this end, recall that $\Gamma_2, \ldots, \Gamma_{2n}, \Gamma_0$ is also a generating set for the Clifford algebra. Hence, we can now view Γ_0 itself as a vector with respect to the new generators. To exchange Γ_0 and Γ_2, we now simply rotate Γ_0 onto Γ_2. Essentially, this corresponds to a rotation about 90° in the plane spanned by vectors Γ_0 and Γ_2. Consider the vector $n = \Gamma_0 + \Gamma_2$ located exactly in the middle between both vectors. Let $\hat{n} = n/\sqrt{2}$ be the normalized vector. Let $R' = \Gamma_2 \hat{n}$. A small calculation analogous to the above shows that

$$R'\Gamma_0 R'^\dagger = \Gamma_2 \quad \text{and} \quad R'\Gamma_2 R'^\dagger = -\Gamma_0.$$

We also have that $\Gamma_1, \Gamma_3, \ldots, \Gamma_{2n}$ are untouched by the operation: for $j \neq 0$ and $j \neq 2$, we have that

$$R'\Gamma_j R'^\dagger = \Gamma_j,$$

since $\{\Gamma_0, \Gamma_j\} = \{\Gamma_2, \Gamma_j\} = 0$. How does R' affect the k-vectors in terms of the original generators $\Gamma_1, \ldots, \Gamma_{2n}$? Using the anticommutation relations and the definition of Γ_0 it is easy to convince yourself that all k-vectors are mapped to k'-vectors with $k' \geq 2$ (except for Γ_0 itself). Hence, the coefficient of Γ_1 remains untouched. We can thus conclude that

$$R'R\rho R^\dagger R'^\dagger = \frac{1}{d} \left(\mathbb{1} + \sqrt{\ell'} \Gamma_1 + g_0 \Gamma_2 + \sum_{j<k} g''_{jk} \Gamma_{jk} + \cdots \right),$$

for some coefficients g''_{jk}.

Finally, we now rotate the vector $g'' = \sqrt{\ell'}\Gamma_1 + g_0\Gamma_2$ onto the vector b. Note that $(g'')^2 = (\ell + g_0^2)\mathbb{1} = \ell\mathbb{1}$. Let $\hat{g}'' = g''/\sqrt{\ell}$ be the normalized vector. Our rotation is derived exactly analogous to the first step: Let $k = \hat{g}'' + \Gamma_1$, and let $\hat{k} = k/\sqrt{2(1 + \sqrt{\ell'}/\sqrt{\ell})}$. Let $R'' = \Gamma_1 \hat{k}$. A simple calculation analogous to the above shows that

$$R'' g'' R''^\dagger = \sqrt{\ell}\Gamma_1,$$

as desired. Again, we have $R''\Gamma_k R''^\dagger = \Gamma_k$ for $k \neq 1$ and $k \neq 2$. Furthermore, k-vectors remain k-vectors under the actions of R''.[16] Summarizing, we obtain

$$R''R'R\rho R^\dagger R'^\dagger R''^\dagger = \frac{1}{d} \left(\mathbb{1} + \sqrt{\ell}\Gamma_1 + \sum_{j<k} g'''_{jk} \Gamma_{jk} + \cdots \right),$$

for some coefficients g'''_{jk}. Thus, we can take $U(T) = R''R'R$.

The argument for finding $U(F_j)$ is analogous. A simple computation using the fact that $\{\Gamma_0, \Gamma_j\} = 0$ for all j gives us $U(F_j) = \Gamma_0 \Gamma_j$.

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] H. Robertson, Phys. Rev. **34**, 163 (1929).
[3] I. Białynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).
[4] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[5] P. Gibilisco, D. Imparato, and T. Isola, J. Math. Phys. **48**, 072109 (2007).
[6] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[7] H. Maassen and J. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[8] I. Damgard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, Proceedings of the CRYPTO, 2007 (unpublished), pp. 360–378.
[9] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Phys. Rev. Lett. **92**, 067902 (2004); e-print arXiv:quant-ph/0303088.
[10] J. Sanchez, Phys. Lett. A **173**, 233 (1993).
[11] J. Sanchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[12] J. Sanchez-Ruiz, Phys. Lett. A **244**, 189 (1998).
[13] P. Hayden, D. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[14] M. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[15] P. Lounesto, *Clifford Algebras and Spinors* (Cambridge University Press, Cambridge, 2001).
[16] C. Doran and A. Lasenby, *Geometric Algebra for Physicists* (Cambridge University Press, Cambridge, 2003).
[17] K. Dietz, J. Phys. A **39**, 1433 (2006).
[18] P. Jordan and E. Wigner, Z. Phys. **47**, 631 (1928).
[19] S. Fehr (private communication).
[20] A. O. Morris, Q. J. Math. **18**, 7 (1967).
[21] A. O. Morris, Q. J. Math. **19**, 289 (1968).
[22] H. Goldstein, *Classical Mechanics* (Addison-Wesley, Reading, MA, 1980).
[23] D. K. Hoffman, R. C. Raffenetti, and K. Ruedenberg, J. Math. Phys. **13**, 528 (1972).