Two proofs of Størmer's theorem

Stanislaw Szarek

Case Western Reserve/Paris 6

Paris, October 20, 2015

With G. Aubrun, to appear in the book:
Alice and Bob Meet Banach, or the Interface of Asymptotic Geometric Analysis and Quantum Information Theory

Abstract

The structure of the set of positivity-preserving maps between matrix algebras is notoriously difficult to describe. The notable exceptions are the low dimensional cases settled by Størmer and Woronowicz, which are equivalent to the Peres-Horodecki positive partial transpose criterion being able to determine whether a state in a 2×2 or 2×3 quantum system is entangled or separable. However, even in these cases the existing arguments (known to the speaker) were based on seemingly ad hoc and long computations. We show a simple proof – based on Brouwer's fixed point theorem – for the 2×2 case (Størmer's theorem), and sketch another argument – following the classical outline, but highly streamlined – based on characterization of extreme self-maps of the Lorentz cone.

Terminology and notation

M_n : $n \times n$ complex matrices; M_n^{sa} : $n \times n$ Hermitian matrices

$\mathcal{PSD} = \mathcal{PSD}(\mathbb{C}^n)$: the cone of *positive semi-definite* matrices

$\mathbf{P} = \mathbf{P}(\mathbb{C}^n)$: the cone of *positivity-preserving* maps $\mathrm{M}_n^{sa} \to \mathrm{M}_n^{sa}$

$\Phi \in \mathbf{P} \iff \Phi(\mathcal{PSD}) \subset \mathcal{PSD}$

$\mathbf{CP} = \mathbf{CP}(\mathbb{C}^n)$: the cone of *completely positive* maps

Official definition: $\Phi \in \mathbf{CP} \iff \Phi \otimes \mathrm{Id}_{\mathrm{M}_m^{sa}} \in \mathbf{P}$ for *all* $m \in \mathbb{N}$

For us, $\Phi \in \mathbf{CP} \iff \Phi(\rho) = \sum_j A_j \rho A_j^\dagger$ for some $\{A_j\} \subset \mathrm{M}_n$

The cone of *co-completely positive* maps:

$\Phi \in \text{co-}\mathbf{CP} \iff \Phi \circ T \in \mathbf{CP}$, where T is the *transpose* map

In other words, if $\Phi(\rho) = \sum_k B_k \rho^T B_k^\dagger$ for some $\{B_k\} \subset \mathrm{M}_n$

Størmer's theorem (1963)

$\Phi \in \mathbf{P}(\mathbb{C}^2) \iff \Phi = \Phi_1 + \Phi_2 \circ T$, where $\Phi_1, \Phi_2 \in \mathbf{CP}(\mathbb{C}^2)$

$\iff \Phi(\rho) = \sum_j A_j \rho A_j^\dagger + \sum_k B_k \rho^T B_k^\dagger$ for some $\{A_j, B_k\} \subset \mathrm{M}_n$

In other words, $\mathbf{P}(\mathbb{C}^2) = \mathbf{CP}(\mathbb{C}^2) + \text{co-}\mathbf{CP}(\mathbb{C}^2) =: \mathbf{DEC}(\mathbb{C}^2)$, the cone of *decomposable* maps.

Woronowicz (1976): Same for $\Phi : \mathrm{M}_2^{sa} \to \mathrm{M}_3^{sa}$ or $\mathrm{M}_3^{sa} \to \mathrm{M}_2^{sa}$, but not for higher dimensions

Corollary Let $\rho \in \mathcal{PSD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. Then ρ is *separable* if and only if its *partial transpose* is positive semi-definite. The same is true for $\rho \in \mathcal{PSD}(\mathbb{C}^3 \otimes \mathbb{C}^2)$

In search of compactness: bases of cones and sets of states

$\mathrm{D}(\mathbb{C}^n) := \mathcal{PSD}(\mathbb{C}^n) \cap H_1$, where $H_1 := \{\mathrm{tr}(\cdot) = 1\} \subset \mathrm{M}_n^{sa}$

We say that D is a *base* of the cone $\mathcal{PSD}$, or $\mathrm{D} = \mathcal{PSD}^{\mathrm{b}}$.

Can similarly consider bases of cones of maps.

It is (somewhat) important that all those cones are closed, convex, and *nondegenerate*, so that their bases – and those of the dual cones – are compact, and we have, for example,

$$\mathcal{C} = \mathbb{R}_+ \mathcal{C}^{\mathrm{b}}, \quad \left(\mathcal{C}_1 + \mathcal{C}_2\right)^{\mathrm{b}} = \mathrm{conv}\left(\mathcal{C}_1^{\mathrm{b}} \cup \mathcal{C}_2^{\mathrm{b}}\right).$$

In particular, no closures are needed anywhere.

Duality and composition rules

If $\Phi : \mathrm{M}_m^{sa} \to \mathrm{M}_n^{sa}$, can consider $\Phi^* : \mathrm{M}_n^{sa} \to \mathrm{M}_m^{sa}$.

This is the usual functional analytic adjoint, based on identifying M_n^{sa} with its dual via $\langle \rho, \sigma \rangle_{\mathrm{HS}} := \mathrm{tr}(\rho\sigma)$.

If $B \in \mathrm{M}_n$ (or $B \in \mathrm{M}_{n\times m}$, as appropriate), we set $\Phi_B(\rho) := B\rho B^\dagger$

Easy: $\Phi \in \mathbf{P} \iff \Phi^* \in \mathbf{P}$, and similarly for **CP**, co-**CP**

Φ is *unital* $\iff$ Φ^* is *trace-preserving*

$\Phi_A^* = \Phi_{A^\dagger}$

If A is invertible, then so is Φ_A and $\Phi_A^{-1} = \Phi_{A^{-1}}$

$\Phi, \Psi \in \mathbf{CP}$ or $\Phi, \Psi \in$ co-$\mathbf{CP} \Rightarrow \Phi \circ \Psi \in \mathbf{CP}$

$\Phi \in \mathbf{CP}, \Psi \in$ co-$\mathbf{CP} \Rightarrow \Phi \circ \Psi, \Psi \circ \Phi \in$ co-$\mathbf{CP}$

Pecularity of (complex) dimension 2

$\mathrm{D}(\mathbb{C}^2)$ is (isometric to) a 3-dimensional *Euclidean ball* and $\mathcal{PSD}(\mathbb{C}^2)$ is isomorphic to the *Lorentz cone* $\mathcal{L}_4$, where

$$\mathcal{L}_m = \left\{x = (x_0, x_1, \ldots, x_{m-1}) : x_0 \geq 0,\ q(x) \geq 0\right\},$$

where $q(x) := x_0^2 - \sum_{k=1}^{m-1} x_k^2$.
The center of the ball is the *maximally mixed state* $\rho_* := \frac{\mathbf{I}}{2}$.

This allows to nicely represent all unital trace-preserving maps $\Phi \in \mathbf{P}(\mathbb{C}^2)$: every such Φ can be associated with a linear map $S = S_\Phi : \mathbb{R}^3 \to \mathbb{R}^3$ with $\|S\|_{\mathrm{op}} \leq 1$, and vice versa. Consequently, every such Φ can be written as a convex combination of maps corresponding to $S \in \mathrm{O}(3)$ (isometries).

The unital trace-preserving case and the *spinor map*

If $U \in \mathrm{U}(n)$, then $\Phi_U(\rho) = U\rho U^\dagger$ is a unital, trace-preserving isometry of $\mathcal{PSD}(\mathbb{C}^n)$. If $n = 2$, more is true:

$\mathrm{SU}(2) \ni U \mapsto S_{\Phi_U} \in \mathrm{SO}(3)$ is a two-to-one surjection, and so is

$\mathrm{SU}(2) \ni U \mapsto S_{\Phi_U \circ T} \in \mathrm{O}(3) \setminus \mathrm{SO}(3)$

Since $\Phi_U \in \mathbf{CP}$ and $\Phi_U \circ T \in \mathrm{co}\text{-}\mathbf{CP}$, this implies that every unital trace-preserving $\Phi \in \mathbf{P}(\mathbb{C}^2)$ is decomposable: it can be written as a convex combination of Φ_{U_j}'s and $\Phi_{V_k} \circ T$'s.

Now for the hard part.

The general case: two possible strategies

1. Focus on maps Φ generating *extreme rays* of $\mathbf{P}(\mathbb{C}^2)$, and conclude via the Krein-Milman theorem.

2. Focus on maps Φ belonging to the *interior* of $\mathbf{P}(\mathbb{C}^2)$, and conclude by passing to the closure (remember we have enough compactness).

The usual approach, starting with Størmer's proof, was to use the first strategy. We will try the second one.

A reduction to the unital trace-preserving case

Proposition Let $\Phi : \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_n^{\mathrm{sa}}$ be a linear map which belongs to the *interior* of $\mathbf{P}(\mathbb{C}^n)$. Then there exist *positive-definite* operators $A, B \in \mathcal{PSD}(\mathbb{C}^n)$ such that

$$\tilde{\Phi}(\rho) = A\Phi(B\rho B)A$$

is *simultaneously* unital and trace-preserving (and necessarily positivity-preserving). In other words,

$$\tilde{\Phi} = \Phi_A \circ \Phi \circ \Phi_B \quad \text{and} \quad \Phi = \Phi_{A^{-1}} \circ \tilde{\Phi} \circ \Phi_{B^{-1}}$$

Once we prove the Proposition, Størmer's theorem follows immediately from the composition rules and the already solved unital trace-preserving case.

Proof of the Proposition

We need to find A, B so that the maps $\tilde{\Phi}(\rho) = A\Phi(B\rho B)A$ and $\tilde{\Phi}^*(\sigma) = B\Phi^*(B\sigma B)A$ are unital, i.e.,

$$\tilde{\Phi}(\mathbf{I}) = A\Phi(B^2)A = \mathbf{I} \quad \text{and} \quad \tilde{\Phi}^*(\mathbf{I}) = B\Phi^*(A^2)B = \mathbf{I}.$$

Since the hypotheses on Φ ensure invertibility, this resolves to

$$A^2 = \Phi(B^2)^{-1} \text{ and } B^2 = \Phi^*(A^2)^{-1} \Rightarrow \Phi(\Phi^*(A^2)^{-1})^{-1} = A^2.$$

In other words, $X = A^2$ is to be a fixed point of the nonlinear map

$$f(X) = \Phi(\Phi^*(X)^{-1})^{-1},$$

and letting $A = X^{1/2}$ and $B = \Phi^*(X)^{-1/2}$ will yield what we need.

Now, f acts on $\mathcal{PSD} \setminus \{0\}$, which is convex, but not compact. To be able to use Brouwer's fixed-point theorem we consider instead

$$f_1 : \mathrm{D}(\mathbb{C}^n) \to \mathrm{D}(\mathbb{C}^n) \quad \text{given by} \quad f_1(X) = \frac{f(X)}{\operatorname{tr} f(X)}.$$

If $X_0 \in D(\mathbb{C}^n)$ is such that $f_1(X_0) = X_0$, then $f(X_0) = tX_0$, where $t = \operatorname{tr} f(X_0) > 0$. However, if we choose – as before – $A = X_0^{1/2}$ and $B = \Phi^*(A^2)^{-1/2}$, then the resulting $\tilde{\Phi}$ is trace-preserving and satisfies $\tilde{\Phi}(\mathrm{Id}) = t^{-1}\,\mathrm{Id}$, which is only possible if $t = 1$, as needed.

Similar fixed point argument was used in a similar context by L. Gurvits, and likely others.

The other strategy

Since $\mathcal{PSD}(\mathbb{C}^2)$ is isomorphic to the Lorentz cone $\mathcal{L}_4$, it is enough to put our hands on extreme rays of the cone of maps preserving the latter. We will call such maps *Lorentz-positive* and denote the cone by $\mathbf{P}(\mathcal{L}_m)$ (for general $m \geq 2$, not just for $m = 4$). We have

Proposition (R. Loewy, H. Schneider 1975) Let $\Phi : \mathbb{R}^m \to \mathbb{R}^m$ be a linear map which generates an extreme ray of $\mathbf{P}(\mathcal{L}_m)$. Then either Φ is an *automorphism* of $\mathcal{L}_m$ or Φ is of *rank one*, in which case $\Phi = |u\rangle\langle v|$ for some $u, v \in \partial\mathcal{L}_m \setminus \{0\}$. If $n > 2$, the converse implication also holds.

To conclude the argument is again standard: automorphisms Φ of $\mathcal{L}_m$ are (roughly) given by the *Lorentz group* $\mathrm{O}^+(1, m-1)$. For $m = 4$, this translates to $\Phi = \Phi_V$ or $\Phi = \Phi_V \circ T$ for $V \in \mathrm{SL}(2, \mathbb{C})$. If rank $\Phi = 1$, the argument is completely straightforward.

This line of proof seems to have been folklore, arXiv:1503.04283

The S-lemma

The trick – found by R. Hildebrand – is to use the S-lemma, a well-known fact from control theory and quadratic/semi-definite programming.

S-lemma: (V. A. Yakubovich 1971) *Let M, N be $m \times m$ symmetric real matrices. The following two properties are equivalent:*
(i) $\{x \in \mathbb{R}^m : \langle Mx, x\rangle \geq 0\} \cup \{x \in \mathbb{R}^m : \langle Nx, x\rangle \geq 0\} = \mathbb{R}^m$
(ii) there exists $t \in [0, 1]$ *such that the matrix* $(1 - t)M + tN$ *is positive semi-definite.*

Proof of the S-lemma: about half a page, see I. Pólik, T. Terlaky, *A Survey of the S-Lemma.* SIAM Rev. 49 (2007), 371-418.

Proof of "S-lemma $\Rightarrow$ Proposition": again about half a page. Our contribution, if any, consists of streamlining Hildebrand's argument.

S-lemma $\Rightarrow$ Proposition

Let J be the $m \times m$ diagonal matrix with entries $1, -1, \ldots, -1$, then $q(x) = \langle Jx, x\rangle$ and so $\Phi \in \mathbf{P}(\mathcal{L}_m)$ translates to

$$\langle Jx, x\rangle \geq 0 \Rightarrow \langle J\Phi x, \Phi x\rangle \geq 0.$$

So the hypotheses of the S-lemma hold with $M = \Phi^* J\Phi, N = -J$ and hence there is $\mu \geq 0$ and $Q \in \mathcal{PSD}$ such that

$$\Phi^* J\Phi = \mu J + Q.$$

Now, $\mu = 0$ is possible only if rank $\Phi = 1$, while $\mu > 0$ and $Q = 0$ $\Rightarrow \mu^{1/2}\Phi \in \mathrm{O}(1, n-1)$. So it is enough to show that if $\mu > 0$ and $Q \neq 0$, then there is Δ with $\operatorname{rank}\Delta = 1$ such that $\Phi \pm \Delta \in \mathbf{P}(\mathcal{L}_m)$.

Let $v \neq 0$ be such that $Q - |v\rangle\langle v| \in \mathcal{PSD}$. Next, let $u \neq 0$ be such that $\Phi^* J u = \delta v$, where δ is either 1 or 0. Such u exists: if Φ^* is invertible, then $u = J(\Phi^*)^{-1} v$ satisfies $\Phi^* J u = v$, while in the opposite case the nullspace of $\Phi^* J$ is nontrivial. Now set

$$\Delta = s|u\rangle\langle v|.$$

By the choice of u and using $\Phi^* J \Phi = \mu J + Q$ we calculate

$$(\Phi \pm \Delta)^* J(\Phi \pm \Delta) = \mu J + Q + (s^2\langle Ju, u\rangle \pm 2s\delta)|v\rangle\langle v|.$$

Since $s^2\langle Ju, u\rangle \pm 2s\delta \geq -1$ if $|s|$ is sufficiently small, it follows that, for such s, $(\Phi \pm \Delta)^* J(\Phi \pm \Delta) - \mu J$ is positive semidefinite. The S-lemma (the easy direction) shows now that $\Phi \pm \Delta \in \mathbf{P}(\mathcal{L}_m)$, as needed.

THANK YOU