Dvoretzky’s theorem and the complexity of entanglement detection

Guillaume Aubrun and Stanislaw Szarek*

U. Lyon 1 and Case Western Reserve U./U. Paris 6

Eprint arxiv:1510.00578, 17p.
We present a lower bound for complexity of entanglement detection which (ultimately) relies on the 1961 Dvoretzky’s theorem, a fundamental result from Asymptotic Geometric Analysis asserting that high-dimensional convex sets typically look round when we observe only their section with a randomly chosen subspaces of smaller dimension.
We present a lower bound for complexity of entanglement detection which (ultimately) relies on the 1961 Dvoretzky’s theorem, a fundamental result from Asymptotic Geometric Analysis asserting that high-dimensional convex sets typically look round when we observe only their section with a randomly chosen subspaces of smaller dimension.

More on the interface between Asymptotic Geometric Analysis and Quantum Information Theory can be found in the forthcoming book

G. Aubrun and S. Szarek, *Alice and Bob meet Banach*

of which a preliminary version is available via Aubrun’s web page.
Outline

- Notation
- Background: Gurvits, Horodecki, Størmer, Skowronek
- The main result
- Strategy behind the proof:
  - Tangible version of Dvoretzky’s theorem (Milman 1971)
  - Face/vertex counting (Figiel–Lindenstrauss–Milman 1977)
  - Bounds on vertical and facial complexity of sets of quantum states
- Sketch of the proof
- Conclusions
Before we proceed... an announcement

Fall 2017 (Sep. 4 - Dec. 15): Trimester on
ANALYSIS IN QUANTUM INFORMATION THEORY
at the Institut Henri Poincaré in Paris
Pre-school, September 4-8, Cargèse, Corsica
Organizers: G. Aubrun, B. Collins, I. Nechita, S. Szarek
Don’t be shy and let one of us know if you are interested!
A quantum state on a finite-dimensional complex Hilbert space $\mathcal{H}$ is a positive operator of trace 1. Denote by $D = D(\mathcal{H})$ the set of states on $\mathcal{H}$. Note that

$$D(\mathcal{H}) = \text{conv}\{ |\psi\rangle\langle\psi| : \psi \in \mathcal{H}, |\psi| = 1 \}.$$
A quantum state on a finite-dimensional complex Hilbert space $\mathcal{H}$ is a positive operator of trace 1. Denote by $D = D(\mathcal{H})$ the set of states on $\mathcal{H}$. Note that

$$D(\mathcal{H}) = \text{conv}\{ |\psi\rangle\langle\psi| : \psi \in \mathcal{H}, |\psi| = 1 \}.$$

When $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is a bipartite Hilbert space, the set of separable states is the subset $\text{Sep}(\mathcal{H}) \subset D(\mathcal{H})$ defined as

$$\text{Sep} = \text{Sep}(\mathcal{H}) := \text{conv}\{ |\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| : \psi_i \in \mathcal{H}_i, |\psi_i| = 1 \}.$$

Elements of $D \setminus \text{Sep}$ are called entangled states.
A quantum state on a finite-dimensional complex Hilbert space $\mathcal{H}$ is a positive operator of trace 1. Denote by $D = D(\mathcal{H})$ the set of states on $\mathcal{H}$. Note that

$$D(\mathcal{H}) = \text{conv}\{ |\psi\rangle\langle\psi| : \psi \in \mathcal{H}, |\psi| = 1 \}.$$ 

When $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is a bipartite Hilbert space, the set of separable states is the subset $\text{Sep}(\mathcal{H}) \subset D(\mathcal{H})$ defined as

$$\text{Sep} = \text{Sep}(\mathcal{H}) := \text{conv}\{ |\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| : \psi_i \in \mathcal{H}_i, |\psi_i| = 1 \}.$$ 

Elements of $D \setminus \text{Sep}$ are called entangled states.

The dichotomy between entanglement vs. separability is fundamental in quantum theory. Entanglement is indispensable for most protocols of quantum information theory/cryptography/computing/teleportation...
Since entanglement is defined as non-membership in a (closed) convex set, it follows from the Hahn–Banach separation theorem that for every entangled state \( \rho \), there is a linear form \( f \) such that \( f \leq a \) on \( \text{Sep} \) and \( f(\rho) > a \). Such \( f \) certifies, or witnesses, the entanglement of \( \rho \).
Certifying/witnessing entanglement

Since entanglement is defined as non-membership in a (closed) convex set, it follows from the Hahn–Banach separation theorem that for every entangled state $\rho$, there is a linear form $f$ such that $f \leq a$ on $\text{Sep}$ and $f(\rho) > a$. Such $f$ certifies, or witnesses, the entanglement of $\rho$.

Equivalently, $\text{Sep}$ is the intersection of half-spaces, which leads to a natural scheme for approximating $\text{Sep}$ by polytopes.
Certifying/witnessing entanglement

Since entanglement is defined as non-membership in a (closed) convex set, it follows from the Hahn–Banach separation theorem that for every entangled state $\rho$, there is a linear form $f$ such that $f \leq a$ on $\text{Sep}$ and $f(\rho) > a$. Such $f$ certifies, or witnesses, the entanglement of $\rho$.

Equivalently, $\text{Sep}$ is the intersection of half-spaces, which leads to a natural scheme for approximating $\text{Sep}$ by polytopes.

A naive – but meaningful – way of measuring complexity of entanglement detection would be determining how well $\text{Sep}$ can be approximated by a polytope with $\leq N$ faces.
Certifying/witnessing entanglement

Since entanglement is defined as non-membership in a (closed) convex set, it follows from the Hahn–Banach separation theorem that for every entangled state \( \rho \), there is a linear form \( f \) such that \( f \leq a \) on \( \text{Sep} \) and \( f(\rho) > a \). Such \( f \) certifies, or witnesses, the entanglement of \( \rho \).

Equivalently, \( \text{Sep} \) is the intersection of half-spaces, which leads to a natural scheme for approximating \( \text{Sep} \) by polytopes.

A naive – but meaningful – way of measuring complexity of entanglement detection would be determining how well \( \text{Sep} \) can be approximated by a polytope with \( \leq N \) faces.

More generally, it is known (Gurvits 2003) that deciding whether a state is entangled or separable is, in general, \textbf{NP-hard}. Later refinements have been due to Ioannou (2007), Gharibian (2010) and others; in particular some upper bounds were supplied by Brandão et al (2011).
The Horodecki criterion

A more structured scheme of witnessing entanglement is given by the following ($M_d$ stands for the space of $n \times n$ complex matrices).

**Theorem (The Horodecki criterion 1996)**

A state $\rho \in \text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is entangled if and only if there is a positive map $\Phi : M_d \rightarrow M_d$ such that the operator $\text{(Id} \otimes \Phi)\rho$ is not positive semi-definite (one says that $\Phi$ witnesses the entanglement of $\rho$).
A more structured scheme of witnessing entanglement is given by the following ($M_d$ stands for the space of $n \times n$ complex matrices).

**Theorem (The Horodecki criterion 1996)**

A state $\rho \in \text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is **entangled** if and only if there is a **positive** map $\Phi : M_d \to M_d$ such that the operator $(\text{Id} \otimes \Phi)\rho$ is not **positive semi-definite** (one says that $\Phi$ witnesses the entanglement of $\rho$).

A linear map $\Phi$ is **positive** if $\Phi(\text{PSD}) \subseteq \text{PSD}$ where $\text{PSD}$ denotes the positive semi-definite cone, more naturally contained in $M_{sa}$. 
A more structured scheme of witnessing entanglement is given by the following (\(M_d\) stands for the space of \(n \times n\) complex matrices).

**Theorem (The Horodecki criterion 1996)**

A state \(\rho \in \text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)\) is **entangled** if and only if there is a **positive** map \(\Phi : M_d \rightarrow M_d\) such that the operator \((\text{Id} \otimes \Phi)\rho\) is **not** positive semi-definite (one says that \(\Phi\) **witnesses** the entanglement of \(\rho\)).

A linear map \(\Phi\) is **positive** if \(\Phi(\text{PSD}) \subseteq \text{PSD}\) where PSD denotes the positive semi-definite cone, more naturally contained in \(M_{sa}^d\).

A map \(M_d \rightarrow M_d\) is completely positive (CP) if it is a positive linear combination of maps of the form \(\Phi_A : X \mapsto AXA^\dagger\). CP maps cannot be witnesses since \(\text{Id} \otimes \Phi_A = \Phi_{I \otimes A}\) is also positive.
Størmer’s theorem

In dimension 2 the cone of positive maps has a rather simple structure.

**Theorem (Størmer 1963)**

Any positive map $\Phi : M_2 \rightarrow M_2$ can be written as $\Phi = \Phi_1 + \Phi_2 \circ T$, where $\Phi_1, \Phi_2$ are CP maps and $T$ is the transposition on $M_2$.

It follows that a state $\rho$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$ is separable if and only if $(\text{Id} \otimes T)(\rho)$ is positive. The transposition is a universal witness.
Størmer’s theorem

In dimension 2 the cone of positive maps has a rather simple structure.

**Theorem (Størmer 1963)**

Any positive map $\Phi : M_2 \to M_2$ can be written as $\Phi = \Phi_1 + \Phi_2 \circ T$, where $\Phi_1, \Phi_2$ are CP maps and $T$ is the transposition on $M_2$.

It follows that a state $\rho$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$ is separable if and only if $(\text{Id} \otimes T)(\rho)$ is positive. The transposition is a universal witness.

This is specific to dimension 2.

**Theorem (Skowronek, unpublished)**

Let $d \geq 3$. Let $\mathcal{F}$ be a family of positive maps $M_d \to M_d$ such that any entangled state $\rho$ on $\mathbb{C}^d \otimes \mathbb{C}^d$ is witnessed by an element of $\mathcal{F}$. Then $\mathcal{F}$ is infinite.

In fact, any closed universal family of witnesses must be uncountable.
Our main result

Denote by \( \bullet \) homotheties with respect to \( \rho_* := \frac{I_{\mathcal{H}}}{\dim \mathcal{H}} \):

\[
t \bullet \rho := t \rho + (1 - t) \rho_*.
\]

Say that a state \( \rho \) is **robustly entangled** if \( \frac{1}{2} \bullet \rho \) is entangled. Robustly entangled states remain entangled in the presence of randomizing noise.
Our main result

Denote by \( \bullet \) homotheties with respect to \( \rho_* := \frac{I_H}{\dim H} \):

\[
t \bullet \rho := t \rho + (1 - t) \rho_*.
\]

Say that a state \( \rho \) is \textit{robustly entangled} if \( \frac{1}{2} \bullet \rho \) is entangled. Robustly entangled states remain entangled in the presence of randomizing noise.

\begin{tcolorbox}[colback=blue!5!white,colframe=blue!75!black]
Theorem (Aubrun–Szarek)

\textit{Suppose that} \( \Phi_1, \ldots, \Phi_N \) \textit{are positive maps on} \( \mathbb{M}_d \) \textit{such that, for any robustly entangled state} \( \rho \) \textit{on} \( \mathbb{C}^d \otimes \mathbb{C}^d \), \textit{there is an index} \( i \) \text{ such that} \( (\text{Id} \otimes \Phi_i)(\rho) \) \textit{is not positive semi-definite. Then} \( N \geq \exp(cd^3 / \log d) \) \textit{for some universal constant} \( c > 0 \).}
\end{tcolorbox}
Our main result

Denote by $\bullet$ homotheties with respect to $\rho_\bullet := \frac{I_H}{\dim H}$:

$$t \cdot \rho := t \rho + (1 - t)\rho_* .$$

Say that a state $\rho$ is robustly entangled if $\frac{1}{2} \cdot \rho$ is entangled. Robustly entangled states remain entangled in the presence of randomizing noise.

**Theorem (Aubrun–Szarek)**

Suppose that $\Phi_1, \ldots, \Phi_N$ are positive maps on $M_d$ such that, for any robustly entangled state $\rho$ on $\mathbb{C}^d \otimes \mathbb{C}^d$, there is an index $i$ such that $(\text{Id} \otimes \Phi_i)(\rho)$ is not positive semi-definite. Then $N \geq \exp(cd^3/\log d)$ for some universal constant $c > 0$.

This shows that the set of separable states is complex, and not because of some fine features of its boundary.
Our main result

Denote by $\bullet$ homotheties with respect to $\rho_* := \frac{1_H}{\dim \mathcal{H}}$:

$$t \bullet \rho := t \rho + (1 - t) \rho_*.$$

Say that a state $\rho$ is robustly entangled if $\frac{1}{2} \bullet \rho$ is entangled. Robustly entangled states remain entangled in the presence of randomizing noise.

**Theorem (Aubrun–Szarek)**

Suppose that $\Phi_1, \ldots, \Phi_N$ are positive maps on $\mathbb{M}_d$ such that, for any robustly entangled state $\rho$ on $\mathbb{C}^d \otimes \mathbb{C}^d$, there is an index $i$ such that $(\text{Id} \otimes \Phi_i)(\rho)$ is not positive semi-definite. Then $N \geq \exp(cd^3 / \log d)$ for some universal constant $c > 0$.

This shows that the set of separable states is complex, and not because of some fine features of its boundary. Results about NP-hardness of entanglement detection have usually focused on boundary effects.
Let $K \subset \mathbb{R}^n$ be a convex compact set with 0 in the interior. Define the verticial and facial dimensions of $K$ as

$$\dim_V(K) := \log \inf \{ \#\text{vertices}(P) : K \subset P \subset 4K \}$$

$$\dim_F(K) := \log \inf \{ \#\text{facets}(P) : K \subset P \subset 4K \}$$

where the infima run over all polytopes $P \subset \mathbb{R}^n$.

The affine invariants $\dim_F$ and $\dim_V$ are measures of complexity.
Let $K \subset \mathbb{R}^n$ be a convex compact set with 0 in the interior. Define the vertical and facial dimensions of $K$ as

$$\dim_V(K) := \log \inf \{ \# \text{vertices}(P) : K \subset P \subset 4K \}$$

$$\dim_F(K) := \log \inf \{ \# \text{facets}(P) : K \subset P \subset 4K \}$$

where the infima run over all polytopes $P \subset \mathbb{R}^n$.

The affine invariants $\dim_F$ and $\dim_V$ are measures of complexity. These are dual concepts since $\dim_F(K) = \dim_V(K^\circ)$, where $K^\circ := \{ x \in \mathbb{R}^n : \langle x, y \rangle \leq 1, \forall y \in K \}$ is the polar of $K$. 
Let $K \subset \mathbb{R}^n$ be a convex compact set with 0 in the interior. Define the \textit{vertical} and \textit{facial dimensions} of $K$ as

$$\dim_V(K) := \log \inf \{ \# \text{vertices}(P) : K \subset P \subset 4K \}$$

$$\dim_F(K) := \log \inf \{ \# \text{facets}(P) : K \subset P \subset 4K \}$$

where the infima run over all polytopes $P \subset \mathbb{R}^n$.

The \textit{affine invariants} $\dim_F$ and $\dim_V$ are measures of complexity.

These are \textit{dual} concepts since $\dim_F(K) = \dim_V(K^\circ)$, where $K^\circ := \{ x \in \mathbb{R}^n : \langle x, y \rangle \leq 1, \forall y \in K \}$ is the \textit{polar} of $K$.

One has $\dim_F(K) = O(n)$ and $\dim_V(K) = O(n)$ if (say) the origin is the center of mass of $K$.

If $E \subset \mathbb{R}^n$ is a linear subspace, then $\dim_F(K \cap E) \leq \dim_F(K)$.
Let $K \subset \mathbb{R}^n$ be a convex compact set with 0 in the interior. Define the **vertical** and **facial dimensions** of $K$ as
dim_V(K) := \log \inf \{ \#\text{vertices}(P) : K \subset P \subset 4K \}
dim_F(K) := \log \inf \{ \#\text{facets}(P) : K \subset P \subset 4K \}
where the infima run over all polytopes $P \subset \mathbb{R}^n$.
The **affine invariants** $\dim_F$ and $\dim_V$ are measures of complexity. These are **dual** concepts since $\dim_F(K) = \dim_V(K^\circ)$, where $K^\circ := \{ x \in \mathbb{R}^n : \langle x, y \rangle \leq 1, \forall y \in K \}$ is the **polar** of $K$.

One has $\dim_F(K) = O(n)$ and $\dim_V(K) = O(n)$ if (say) the origin is the center of mass of $K$.

If $E \subset \mathbb{R}^n$ is a linear subspace, then $\dim_F(K \cap E) \leq \dim_F(K)$.
We have $\dim_F(B_2^n) = \dim_V(B_2^n) = \Theta(n)$ (B_2^n is the Euclidean ball).
Vertical and facial dimensions of convex bodies

Let $K \subset \mathbb{R}^n$ be a convex compact set with 0 in the interior. Define the vertical and facial dimensions of $K$ as

$$\dim_V(K) := \log \inf \{ \#\text{vertices}(P) : K \subset P \subset 4K \}$$

$$\dim_F(K) := \log \inf \{ \#\text{facets}(P) : K \subset P \subset 4K \}$$

where the infima run over all polytopes $P \subset \mathbb{R}^n$.

The affine invariants $\dim_F$ and $\dim_V$ are measures of complexity. These are dual concepts since $\dim_F(K) = \dim_V(K^\circ)$, where $K^\circ := \{ x \in \mathbb{R}^n : \langle x, y \rangle \leq 1, \forall y \in K \}$ is the polar of $K$.

One has $\dim_F(K) = O(n)$ and $\dim_V(K) = O(n)$ if (say) the origin is the center of mass of $K$.

If $E \subset \mathbb{R}^n$ is a linear subspace, then $\dim_F(K \cap E) \leq \dim_F(K)$.

We have $\dim_F(B_2^n) = \dim_V(B_2^n) = \Theta(n)$ (where $B_2^n$ is the Euclidean ball).

Another parameter is the asphericity of $K$ defined as

$$a(K) := \inf \{ R/r : rB_2^n \subset K \subset RB_2^n \}.$$
The Figiel–Lindenstrauss–Milman bound

A fundamental property ("complexity must lie somewhere") of convex sets is the following.

Theorem (Figiel–Lindenstrauss–Milman 1977)
For any convex body $K \subset \mathbb{R}^n$ containing the origin in the interior we have

$$\dim F(K) \cdot \dim V(K) \cdot a(K)^2 = \Omega(n^2).$$

This result is a consequence of the tangible version of Dvoretzky’s theorem due to Milman, which gives a sharp formula for the dimension of almost Euclidean sections of convex bodies.

If $K \subset \mathbb{R}^n$ is a convex body such that $rB_n^2 \subset K$ and $M = M(K)$ denotes the average of the "norm" $\|\cdot\|_K$ over the sphere, then $K$ has lots of almost Euclidean sections of dimension $k = \Omega(nr^2M^2)$.

Thus the facial dimension of $K$ exceeds $ck$.

Applying the same argument to $K^\circ$ and using the inequality $M(K) \leq M(K^\circ)$ yields the FLM bound.
The Figiel–Lindenstrauss–Milman bound

A fundamental property ("complexity must lie somewhere") of convex sets is the following.

**Theorem (Figiel–Lindenstrauss–Milman 1977)**

For any convex body $K \subset \mathbb{R}^n$ containing the origin in the interior we have

$$\dim_F(K) \cdot \dim_V(K) \cdot a(K)^2 = \Omega(n^2).$$
The Figiel–Lindenstrauss–Milman bound

A fundamental property ("complexity must lie somewhere") of convex sets is the following.

**Theorem (Figiel–Lindenstrauss–Milman 1977)**

For any convex body \( K \subset \mathbb{R}^n \) containing the origin in the interior we have

\[
\dim_F(K) \cdot \dim_V(K) \cdot a(K)^2 = \Omega(n^2).
\]

This result is a consequence of the tangible version of Dvoretzky’s theorem due to Milman, which gives a sharp formula for the dimension of almost Euclidean sections of convex bodies.

If \( K \subset \mathbb{R}^n \) is a convex body such that \( rB_2^n \subset K \) and \( M = M(K) \) denotes the average of the "norm" \( \| \cdot \|_K \) over the sphere, then \( K \) has lots of almost Euclidean sections of dimension \( k = \Omega(nr^2M^2) \).
A fundamental property ("complexity must lie somewhere") of convex sets is the following.

**Theorem (Figiel–Lindenstrauss–Milman 1977)**

For any convex body $K \subset \mathbb{R}^n$ containing the origin in the interior we have

$$\dim F(K) \cdot \dim V(K) \cdot a(K)^2 = \Omega(n^2).$$

This result is a consequence of the tangible version of Dvoretzky’s theorem due to Milman, which gives a sharp formula for the dimension of almost Euclidean sections of convex bodies.

*If $K \subset \mathbb{R}^n$ is a convex body such that $rB_2^n \subset K$ and $M = M(K)$ denotes the average of the “norm” $\| \cdot \|_K$ over the sphere, then $K$ has lots of almost Euclidean sections of dimension $k = \Omega(nr^2M^2)$. Thus the facial dimension of $K$ exceeds $ck$.***
A fundamental property ("complexity must lie somewhere") of convex sets is the following.

**Theorem (Figiel–Lindenstrauss–Milman 1977)**

For any convex body $K \subset \mathbb{R}^n$ containing the origin in the interior we have

$$\dim_F(K) \cdot \dim_V(K) \cdot a(K)^2 = \Omega(n^2).$$

This result is a consequence of the **tangible** version of Dvoretzky’s theorem due to Milman, which gives a sharp formula for the dimension of almost Euclidean sections of convex bodies.

*If $K \subset \mathbb{R}^n$ is a convex body such that $rB_2^n \subset K$ and $M = M(K)$ denotes the average of the “norm” $\|\cdot\|_K$ over the sphere, then $K$ has lots of almost Euclidean sections of dimension $k = \Omega(nr^2M^2)$.***

Thus the facial dimension of $K$ exceeds $ck$. Applying the same argument to $K^\circ$ and using the inequality $M(K)M(K^\circ) \geq 1$ yields the FLM bound.
We illustrate the FLM bound on some examples where it is sharp up to polylog factors

\[ \dim_V(K) \cdot \dim_F(K) \geq c \left( \frac{n}{a(K)} \right)^2 \]

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$B_2^n$</td>
<td>$n$</td>
<td>1</td>
<td>$\Theta(n)$</td>
<td>$\Theta(n)$</td>
</tr>
<tr>
<td>$[-1,1]^n$</td>
<td>$n$</td>
<td>$\sqrt{n}$</td>
<td>$\Theta(n)$</td>
<td>$\Theta(\log n)$</td>
</tr>
<tr>
<td>$\Delta_n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$\Theta(\log n)$</td>
<td>$\Theta(\log n)$</td>
</tr>
</tbody>
</table>

Recall that $B_2^n$ is the $n$-dimensional Euclidean ball, while $\Delta_n$ is the $n$-dimensional simplex.
Quantum-related examples

And here are some more examples related to entanglement detection.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\text{dim}_V(K)$</th>
<th>$\text{dim}_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{D} (\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{Sep} (\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The value of $a(\text{D})$ is elementary to compute; the value of $a(\text{Sep})$ is due to Gurvits–Barnum (2002).
Quantum-related examples

And here are some more examples related to entanglement detection.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\text{dim}_V(K)$</th>
<th>$\text{dim}_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td></td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td></td>
</tr>
</tbody>
</table>

The value of $a(D)$ is elementary to compute; the value of $a(\text{Sep})$ is due to Gurvits–Barnum (2002).

The vertical dimensions of $D$ and $\text{Sep}$ are easier to compute since these sets are defined by convex hulls. However, there are some surprises.
Quantum-related examples

And here are some more examples related to entanglement detection.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(C^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td></td>
</tr>
<tr>
<td>$\text{Sep}(C^d \otimes C^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td></td>
</tr>
</tbody>
</table>

The value of $a(D)$ is elementary to compute; the value of $a(\text{Sep})$ is due to Gurvits–Barnum (2002).

The vertical dimensions of $D$ and $\text{Sep}$ are easier to compute since these sets are defined by convex hulls. However, there are some surprises.

- There are $\varepsilon$-nets in the sphere of $C^d$ with $(2/\varepsilon)^{2d} = e^{\Theta(d \log(2/\varepsilon))}$ elements.
Quantum-related examples

And here are some more examples related to entanglement detection.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td></td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td></td>
</tr>
</tbody>
</table>

The value of $a(D)$ is elementary to compute; the value of $a(\text{Sep})$ is due to Gurvits–Barnum (2002).

The vertical dimensions of $D$ and $\text{Sep}$ are easier to compute since these sets are defined by convex hulls. However, there are some surprises.

- There are $\varepsilon$-nets in the sphere of $\mathbb{C}^d$ with $(2/\varepsilon)^{2d} = e^{\Theta(d \log(2/\varepsilon))}$ elements.
- For a well chosen (e.g., random) $\frac{1}{10}$-net $\mathcal{N}$ in the unit sphere of $\mathbb{C}^m$ and $P = \text{conv}\{\ketbra{\psi}{\psi} : \psi \in \mathcal{N}\}$, we have $\frac{1}{4} \bullet D \subset P \subset D$. 
Quantum-related examples

And here are some more examples related to entanglement detection.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td></td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td></td>
</tr>
</tbody>
</table>

The value of $a(D)$ is elementary to compute; the value of $a(\text{Sep})$ is due to Gurvits–Barnum (2002).

The vertical dimensions of $D$ and $\text{Sep}$ are easier to compute since these sets are defined by convex hulls. However, there are some surprises.

- There are $\varepsilon$-nets in the sphere of $\mathbb{C}^d$ with $(2/\varepsilon)^{2d} = e^{\Theta(d \log(2/\varepsilon))}$ elements.
- For a well chosen (e.g., random) $\frac{1}{10}$-net $\mathcal{N}$ in the unit sphere of $\mathbb{C}^m$ and $P = \text{conv}\{|\psi\rangle\langle\psi| : \psi \in \mathcal{N}\}$, we have $\frac{1}{4} \bullet D \subset P \subset D$.
- Similarly, for any $\frac{1}{10d}$-net $\mathcal{N}'$ in the unit sphere of $\mathbb{C}^d$ and $P' = \text{conv}\{|\psi \otimes \varphi\rangle\langle\psi \otimes \varphi| : \psi, \varphi \in \mathcal{N}'\}$, we have $\frac{1}{4} \bullet \text{Sep} \subset P' \subset \text{Sep}$.
Quantum-related examples, II

We now complete the table.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td>$\Theta(m)$</td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td>$\Omega(d^3 / \log d)$</td>
</tr>
</tbody>
</table>

The set $D$ is self-dual (or, more precisely, $D^\circ = (-m) \bullet D$), so its facial dimension equals its vertical dimension.
Quantum-related examples, II

We now complete the table.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>$\dim_V(K)$</th>
<th>$\dim_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td>$\Theta(m)$</td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td>$\Omega(d^3 / \log d)$</td>
</tr>
</tbody>
</table>

The set $D$ is self-dual (or, more precisely, $D^\circ = (-m) \cdot D$), so its facial dimension equals its vertical dimension.

The lower bound on the facial dimension of $\text{Sep}$ follows from the Figiel–Lindenstrauss–Milman inequality

$$\dim_V(\text{Sep}) \cdot \dim_F(\text{Sep}) \geq c \left( \frac{d^4 - 1}{d^2 - 1} \right)^2 > cd^4$$
We now complete the table.

<table>
<thead>
<tr>
<th>$K$</th>
<th>dimension</th>
<th>$a(K)$</th>
<th>dim$_V(K)$</th>
<th>dim$_F(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D(\mathbb{C}^m)$</td>
<td>$m^2 - 1$</td>
<td>$m - 1$</td>
<td>$\Theta(m)$</td>
<td>$\Theta(m)$</td>
</tr>
<tr>
<td>$\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$</td>
<td>$d^4 - 1$</td>
<td>$d^2 - 1$</td>
<td>$\Theta(d \log d)$</td>
<td>$\Omega(d^3 / \log d)$</td>
</tr>
</tbody>
</table>

The set $D$ is self-dual (or, more precisely, $D^\circ = (-m) \bullet D$), so its facial dimension equals its verticial dimension.

The lower bound on the facial dimension of $\text{Sep}$ follows from the Figiel–Lindenstrauss–Milman inequality

$$\dim_V(\text{Sep}) \cdot \dim_F(\text{Sep}) \geq c \left( \frac{d^4 - 1}{d^2 - 1} \right)^2 > cd^4$$

However, it is conceivable that we actually have $\dim_F(\text{Sep}) = \Theta(d^4)$. 
Sketch of the proof of the theorem

Let $\Phi_1, \ldots, \Phi_N$ be $N$ positive maps on $M_d$ with the property that for every robustly entangled state $\rho$, there exists an index $i$ such that $(\Phi_i \otimes \text{Id})(\rho)$ is not positive. This hypothesis is equivalent to the following inclusion

$$\bigcap_{i=1}^N \{ \rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d) : (\text{Id} \otimes \Phi_i)(\rho) \text{ is PSD} \} \subset 2 \cdot \text{Sep}. $$
Let $\Phi_1, \ldots, \Phi_N$ be $N$ positive maps on $M_d$ with the property that for every robustly entangled state $\rho$, there exists an index $i$ such that $(\Phi_i \otimes \text{Id})(\rho)$ is not positive. This hypothesis is equivalent to the following inclusion

$$\bigcap_{i=1}^N \{ \rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d) : (\text{Id} \otimes \Phi_i)(\rho) \text{ is PSD} \} \subset 2 \cdot \text{Sep}.$$ 

By considering $X \mapsto \Phi_i(I)^{-1/2} \Phi_i(X) \Phi_i(I)^{-1/2}$, we may assume that $\Phi_i(I) = I$ for all $i = 1, \ldots, N$. 
Sketch of the proof of the theorem

Let $\Phi_1, \ldots, \Phi_N$ be $N$ positive maps on $M_d$ with the property that for every robustly entangled state $\rho$, there exists an index $i$ such that $(\Phi_i \otimes \text{Id})(\rho)$ is not positive. This hypothesis is equivalent to the following inclusion

$$\bigcap_{i=1}^{N} \{ \rho \in D(C^d \otimes C^d) : (\text{Id} \otimes \Phi_i)(\rho) \text{ is PSD} \} \subset 2 \cdot \text{Sep}. $$

By considering $X \mapsto \Phi_i(I)^{-1/2}\Phi_i(X)\Phi_i(I)^{-1/2}$, we may assume that $\Phi_i(I) = I$ for all $i = 1, \ldots, N$.

Next, for simplicity, let us assume first that each $\Phi_i$ is trace-preserving, i.e., $\Phi_i(\rho_*) = \rho_*$. Consider the convex body

$$K = D \cap \bigcap_{i=1}^{N} (\text{Id} \otimes \Phi_i)^{-1}(D)$$

which satisfies $\text{Sep} \subset K \subset 2 \cdot \text{Sep}$.
Sketch of the proof of the theorem

Let $\Phi_1, \ldots, \Phi_N$ be $N$ positive maps on $M_d$ with the property that for every robustly entangled state $\rho$, there exists an index $i$ such that $(\Phi_i \otimes \text{Id})(\rho)$ is not positive. This hypothesis is equivalent to the following inclusion

$$\bigcap_{i=1}^{N} \{ \rho \in D(C^d \otimes C^d) : (\text{Id} \otimes \Phi_i)(\rho) \text{ is PSD} \} \subset 2 \cdot \text{Sep}. $$

By considering $X \mapsto \Phi_i(I)^{-1/2} \Phi_i(X) \Phi_i(I)^{-1/2}$, we may assume that $\Phi_i(I) = I$ for all $i = 1, \ldots, N$.

Next, for simplicity, let us assume first that each $\Phi_i$ is trace-preserving, i.e., $\Phi_i(\rho_*) = \rho_*$. Consider the convex body

$$K = D \cap \bigcap_{i=1}^{N} (\text{Id} \otimes \Phi_i)^{-1}(D)$$

which satisfies $\text{Sep} \subset K \subset 2 \cdot \text{Sep}$. Note the trace-preserving condition assures that for all $i$’s we are $\bullet$-dilating with respect to the same point.
Since the facial dimension of $D(\mathbb{C}^d \otimes \mathbb{C}^d)$ is of order $d^2$, there exists a polytope $P$ with at most $\exp(Cd^2)$ facets such that $\frac{1}{2} \bullet D \subset P \subset D$. Then the polytope

$$Q = P \cap \bigcap_{i=1}^{N} (\text{Id} \otimes \Phi_i)^{-1}(P)$$

satisfies $\frac{1}{2} \bullet \text{Sep} \subset \frac{1}{2} \bullet K \subset Q \subset K \subset 2 \bullet \text{Sep}$. Since

$$\#\text{facets}(P_1 \cap P_2) \leq \#\text{facets}(P_1) + \#\text{facets}(P_2),$$

the polytope $Q$ has at most $(N + 1) \exp(Cd^2)$ facets.
Sketch of the proof of the theorem, II

Since the facial dimension of $D(\mathbb{C}^d \otimes \mathbb{C}^d)$ is of order $d^2$, there exists a polytope $P$ with at most $\exp(Cd^2)$ facets such that $\frac{1}{2} \cdot D \subset P \subset D$. Then the polytope

$$Q = P \cap \bigcap_{i=1}^{N} (\text{Id} \otimes \Phi_i)^{-1}(P)$$

satisfies $\frac{1}{2} \cdot \text{Sep} \subset \frac{1}{2} \cdot K \subset Q \subset K \subset 2 \cdot \text{Sep}$. Since

$$\#\text{facets}(P_1 \cap P_2) \leq \#\text{facets}(P_1) + \#\text{facets}(P_2),$$

the polytope $Q$ has at most $(N + 1) \exp(Cd^2)$ facets.

Since the facial dimension of $\text{Sep}$ is $\Omega(d^3/\log d)$, it follows that

$$\log((N + 1) \exp(Cd^2)) \geq cd^3/\log d$$

so that $N \geq \exp(cd^3/\log d)$ as claimed.
Sketch of the proof of the theorem, II

Since the facial dimension of $D(\mathbb{C}^d \otimes \mathbb{C}^d)$ is of order $d^2$, there exists a polytope $P$ with at most $\exp(Cd^2)$ facets such that $\frac{1}{2} \cdot D \subset P \subset D$. Then the polytope

$$Q = P \cap \bigcap_{i=1}^{N} (\text{Id} \otimes \Phi_i)^{-1}(P)$$

satisfies $\frac{1}{2} \cdot \text{Sep} \subset \frac{1}{2} \cdot K \subset Q \subset K \subset 2 \cdot \text{Sep}$. Since

$$\#\text{facets}(P_1 \cap P_2) \leq \#\text{facets}(P_1) + \#\text{facets}(P_2),$$

the polytope $Q$ has at most $(N + 1) \exp(Cd^2)$ facets.

Since the facial dimension of $\text{Sep}$ is $\Omega(d^3 / \log d)$, it follows that

$$\log((N + 1) \exp(Cd^2)) \geq cd^3 / \log d$$

so that $N \geq \exp(cd^3 / \log d)$ as claimed.

The general situation (without the trace-preserving restriction) is handled similarly starting with the assumption that $(1 - \frac{1}{2d}) \cdot D \subset P \subset D$. 

Aubrun & Szarek (Lyon & CWRU/Paris 6)  Dvoretzky's theorem and entanglement  Banff, January 11, 2016 17 / 18
Conclusion

We illustrated the complexity of robust entanglement by showing that super-exponentially many positive maps are needed to detect it – at least if used non-adaptively/without reflection.
Conclusion

We illustrated the complexity of robust entanglement by showing that super-exponentially many positive maps are needed to detect it – at least if used non-adaptively/without reflection.

The proof is via a facet-counting argument (even if the set of separable states is not a polytope itself) and ultimately relies on the bound due to Figiel–Lindenstrauss–Milman which asserts that – between (i) the number of vertices, (ii) the number of facets, and (iii) asphericity – complexity must lie somewhere.

Can this approach be used to handle other problems in complexity theory?

Some other directions in which this work can be continued are:

• Upper bounds; in particular, what is the order of $d_F$(Sep)?

• Less/more robust entanglement, i.e., replacing $\frac{1}{2}$ with $\epsilon \in (0,1)$

• What if we use witnesses $\Phi : M_d \rightarrow M_m$, where $m = \text{poly}(d)$?

• The multipartite or “unbalanced” ($H = C_d \otimes C_m$) setting
Conclusion

We illustrated the complexity of robust entanglement by showing that super-exponentially many positive maps are needed to detect it – at least if used non-adaptively/without reflection.

The proof is via a facet-counting argument (even if the set of separable states is not a polytope itself) and ultimately relies on the bound due to Figiel–Lindenstrauss–Milman which asserts that – between (i) the number of vertices, (ii) the number of facets, and (iii) asphericity – complexity must lie somewhere.

Can this approach be used to handle other problems in complexity theory?
Conclusion

We illustrated the complexity of robust entanglement by showing that super-exponentially many positive maps are needed to detect it – at least if used non-adaptively/without reflection.

The proof is via a facet-counting argument (even if the set of separable states is not a polytope itself) and ultimately relies on the bound due to Figiel–Lindenstrauss–Milman which asserts that – between (i) the number of vertices, (ii) the number of facets, and (iii) asphericity – complexity must lie somewhere.

Can this approach be used to handle other problems in complexity theory?

Some other directions in which this work can be continued are:

• Upper bounds; in particular, what is the order of $d_F(Sep)$?
• Less/more robust entanglement, i.e., replacing $\frac{1}{2}$ with $\varepsilon \in (0, 1)$
• What if we use witnesses $\Phi : M_d \to M_m$, where $m = poly(d)$?
• The multipartite or “unbalanced” ($\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^m$) setting