Norm convergence of unitary random matrices and quantum information theory

Benoît Collins
uOttawa and Lyon 1

JMM, San Diego 2013
Plan

▶ Convergence theorem for the output set of random quantum channels.
▶ Norm convergence for unitary random matrices.
▶ Examples.
▶ Joint works with S. Belinschi, C. Male, M. Fukuda, I. Nechita.
Plan

- Convergence theorem for the output set of random quantum channels.
Plan

- Convergence theorem for the output set of random quantum channels.
- Norm convergence for unitary random matrices.
- Examples.
- Joint works with S. Belinschi, C. Male, M. Fukuda, I. Nechita.
Plan

▶ Convergence theorem for the output set of random quantum channels.
▶ Norm convergence for unitary random matrices.
▶ Examples.

Joint works with S. Belinschi, C. Male, M. Fukuda, I. Nechita.
Plan

- Convergence theorem for the output set of random quantum channels.
- Norm convergence for unitary random matrices.
- Examples.
- Joint works with S. Belinschi, C. Male, M. Fukuda, I. Nechita.
Quantum channels

- A quantum channel $\Phi$ is a map $\mathbb{M}_n(\mathbb{C}) \rightarrow \mathbb{M}_k(\mathbb{C})$
Quantum channels

A quantum channel \( \Phi \) is a map \( \mathbb{M}_n(\mathbb{C}) \rightarrow \mathbb{M}_k(\mathbb{C}) \)
It is linear, completely positive and trace preserving.
A quantum channel $\Phi$ is a map $\mathbb{M}_n(\mathbb{C}) \rightarrow \mathbb{M}_k(\mathbb{C})$
It is linear, completely positive and trace preserving.
Its Choi map is the matrix

$$C_\Phi = \sum_{i,j \in \{1,\ldots,n\}} E_{ij} \otimes \Phi(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_k$$
Quantum channels

- A quantum channel $\Phi$ is a map $\mathbb{M}_n(\mathbb{C}) \rightarrow \mathbb{M}_k(\mathbb{C})$. It is linear, completely positive and trace preserving.
- Its Choi map is the matrix
  \[
  C_\Phi = \sum_{i,j \in \{1,\ldots,n\}} E_{ij} \otimes \Phi(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_k
  \]

$\Phi$ is CP iff $C_\Phi$ is positive.
Our problem

Notation: let $S_n$ be the collection of 'states' on $M_n$, i.e. trace 1 positive operators. This is a convex set whose extremal points are the rank one projections (denoted by $S_{e,n}$).

We want to study the following sets: $\Phi(S_n)$ and $\Phi(S_{e,n})$. The first one is compact convex and the second one is compact. They are subsets of $S_k$. 
Our problem

- Notation: let $S_n$ be the collection of ‘states’ on $\mathbb{M}_n$, i.e. trace 1 positive operators.
Notation: let $S_n$ be the collection of ‘states’ on $\mathbb{M}_n$, i.e. trace 1 positive operators. This is a convex set whose extremal points are the rank one projections (denoted by $S_n^e$).
Notation: let $S_n$ be the collection of ‘states’ on $\mathbb{M}_n$, i.e. trace 1 positive operators. This is a convex set whose extremal points are the rank one projections (denoted by $S_{n}^{e}$).

We want to study the following sets: $\Phi(S_n)$ and $\Phi(S_{n}^{e})$. 
Notation: let $S_n$ be the collection of ‘states’ on $\mathbb{M}_n$, i.e. trace 1 positive operators. This is a convex set whose extremal points are the rank one projections (denoted by $S_n^e$).

We want to study the following sets: $\Phi(S_n)$ and $\Phi(S_n^e)$. The first one is compact convex and the second one is compact. They are subsets of $S_k$. 
Stinespring representation

Given a quantum channel $\Phi : M_n \to M_k$, there exists $N$ and a nonunital rank-preserving embedding $i : M_n \subset M_N \otimes M_k$ such that for all $x$,

$$\Phi(x) = (\text{Tr}_N \otimes \text{id}_k)(x).$$

$\Phi_n(S_n)$ and $\Phi_n(S_e_n)$ depend only on $i(1_n) =: P_n$. 


Stinespring representation

Given a quantum channel $\Phi : \mathcal{M}_n \to \mathcal{M}_k$, there exists $N$ and a nonunital rank-preserving embedding $i : \mathcal{M}_n \subset \mathcal{M}_N \otimes \mathcal{M}_k$. 

$\Phi_n(S_n)$ and $\Phi_n(S_e_n)$ depend only on $i(1_n) =: P_n$. 

$\mathcal{M}_n$ and $\mathcal{M}_k$.
Stinespring representation

Given a quantum channel $\Phi : \mathcal{M}_n \to \mathcal{M}_k$, there exists $N$ and a nonunital rank-preserving embedding $i : \mathcal{M}_n \subset \mathcal{M}_N \otimes \mathcal{M}_k$ such that for all $x$,

$$\Phi(x) = (Tr_N \otimes id_k)x.$$
Given a quantum channel $\Phi : \mathbb{M}_n \to \mathbb{M}_k$, there exists $N$ and a nonunital rank-preserving embedding $i : \mathbb{M}_n \subset \mathbb{M}_N \otimes \mathbb{M}_k$ such that for all $x$,

$$\Phi(x) = (\text{Tr}_N \otimes id_k)x.$$ 

$\Phi_n(S_n)$ and $\Phi_n(S_n^e)$ depend only on $i(1_n) =: P_n$. 

Stinespring representation
Random quantum channels

We are interested in sequences $\Phi_n$ of such quantum channels ($k$ is fixed).

Working with the Stinespring picture, for each $n$ we fix an $N = N(n)$ and we choose $i: M_n \subset M_N \otimes M_k$ at random according to various distributions.

Since $\Phi_n(S_n)$ and $\Phi_n(S_{en})$ depend only on $i(1_n) = P_n$, it is enough for our purposes to study a random projection $P_n$ of rank $n$ in $M_N \otimes M_k$. 
Random quantum channels

- A random quantum channel is a quantum channel... chosen at random.
A random quantum channel is a quantum channel... chosen at random. We are interested in sequences \( \Phi_n \) of such quantum channels (\( k \) is fixed).
Random quantum channels

- A random quantum channel is a quantum channel... chosen at random. We are interested in sequences $\Phi_n$ of such quantum channels ($k$ is fixed).
- Working with the Stinespring picture, for each $n$ we fix an $N = N(n)$ and we choose $i : M_n \subset M_N \otimes M_k$ at random according to various distributions.
Random quantum channels

- A random quantum channel is a quantum channel... chosen at random. We are interested in sequences $\Phi_n$ of such quantum channels ($k$ is fixed).
- Working with the Stinespring picture, for each $n$ we fix an $N = N(n)$ and we choose $i : \mathbb{M}_n \subset \mathbb{M}_N \otimes \mathbb{M}_k$ at random according to various distributions.
- Since $\Phi_n(S_n)$ and $\Phi_n(S^e_n)$ depend only on $i(1_n) = P_n$, it is enough for our purposes to study a random projection $P_n$ of rank $n$ in $\mathbb{M}_N \otimes \mathbb{M}_k$. 
Convergence result

- Our key assumption on the law of $P_n$ is:
Our key assumption on the law of $P_n$ is:
For any projection $B \in \mathbb{M}_k$, $\|B \otimes 1_N \cdot P_n\|_\infty$ converges with probability one to $\sqrt{f(B)}$ as $n \to \infty$. 
Convergence result

- Our key assumption on the law of $P_n$ is:
  For any projection $B \in \mathbb{M}_k$, $\|B \otimes 1_N \cdot P_n\|_\infty$ converges with probability one to $\sqrt{f(B)}$ as $n \to \infty$.

- Theorem (C, Fukuda, Nechita, 2013)
  There exists a convex compact set $K$ such that $\Phi_n(S_n) \to K$ and $\partial \Phi_n(S_n) \to \partial K$ (Hausdorff distance between sets).
Convergence result

- Our key assumption on the law of $P_n$ is:
  For any projection $B \in \mathbb{M}_k$, $\|B \otimes 1_N \cdot P_n\|_{\infty}$ converges with probability one to $\sqrt{f(B)}$ as $n \to \infty$.

- Theorem (C, Fukuda, Nechita, 2013)

  There exists a convex compact set $K$ such that $\Phi_n(S_n) \to K$ and $\partial \Phi_n(S_n) \to \partial K$ (Hausdorff distance between sets).

  $K = \{A \in S_k, \forall B \in S_k, Tr_k(AB) \leq f(B)\}$
Convergence result

- Our key assumption on the law of $P_n$ is:
  For any projection $B \in \mathbb{M}_k$, $\|B \otimes 1_N \cdot P_n\|_\infty$ converges with probability one to $\sqrt{f(B)}$ as $n \to \infty$.

- Theorem (C, Fukuda, Nechita, 2013)
  There exists a convex compact set $K$ such that $\Phi_n(S_n) \to K$ and $\partial \Phi_n(S_n) \to \partial K$ (Hausdorff distance between sets).
  $K = \{A \in S_k, \forall B \in S_k, \text{Tr}_k(AB) \leq f(B)\}$

- Replacing $\Phi_n(S_n)$ by $\Phi_n(S^e_n)$ (much smaller set) is possible if one makes a slightly stronger assumption
Convergence result

- Our key assumption on the law of $P_n$ is:
  For any projection $B \in \mathbb{M}_k$, $\|B \otimes 1_N \cdot P_n\|_\infty$ converges with probability one to $\sqrt{f(B)}$ as $n \to \infty$.

- Theorem (C, Fukuda, Nechita, 2013)

There exists a convex compact set $K$ such that $\Phi_n(S_n) \to K$ and $\partial \Phi_n(S_n) \to \partial K$ (Hausdorff distance between sets).

$K = \{A \in S_k, \forall B \in S_k, \text{Tr}_k(AB) \leq f(B)\}$

- Replacing $\Phi_n(S_n)$ by $\Phi_n(S_n^e)$ (much smaller set) is possible if one makes a slightly stronger assumption (no gap between the first few largest eigenvalues).
First example

- In [BCN 2012] we proved the convergence in the particular case where $P_n$ is a uniform random projection of rank $n \sim tNk$ ($t$ in $(0, 1)$ is fixed).
In [BCN 2012] we proved the convergence in the particular case where $P_n$ is a uniform random projection of rank $n \sim tNk$ ($t$ in $(0, 1)$ is fixed). Here, the convergence works for $\Phi_n(S_n^e)$ too.
First example

- In [BCN 2012] we proved the convergence in the particular case where $P_n$ is a uniform random projection of rank $n \sim tNk$ ($t$ in $(0, 1)$ is fixed). Here, the convergence works for $\Phi_n(S^e_n)$ too.

- In this case, $f(B) = \|pBp\|_\infty$ where $p$ is a rank $t$ projection free of $B$. We denote it $\|B\|_t$ and call it the t-norm (free compression norm).
First example

- In [BCN 2012] we proved the convergence in the particular case where $P_n$ is a uniform random projection of rank $n \sim tN_k$ ($t$ in $(0, 1)$ is fixed). Here, the convergence works for $\Phi_n(S^e_n)$ too.

- In this case, $f(B) = \|pBp\|_\infty$ where $p$ is a rank $t$ projection free of $B$. We denote it $\|B\|_{(t)}$ and call it the t-norm (free compression norm). $K$ is a convex body with smooth boundary under mild assumptions.
First example

- In [BCN 2012] we proved the convergence in the particular case where $P_n$ is a uniform random projection of rank $n \sim tN_k$ ($t$ in $(0,1)$ is fixed). Here, the convergence works for $\Phi_n(S^e_n)$ too.

- In this case, $f(B) = ||pBp||_\infty$ where $p$ is a rank $t$ projection free of $B$. We denote it $||B||_{(t)}$ and call it the t-norm (free compression norm). $K$ is a convex body with smooth boundary under mild assumptions.

- We need new tools in RMT to construct more examples.
Asymptotic freeness for RMT

In 1992, Voiculescu proved that iid GUEs $X_1(\ldots, X_k(\ldots)$ are asymptotically free as $n \to \infty$.

In 1998 he proved the following stronger result: if $(A_1(\ldots, A_k(\ldots))$ is a family of $n \times n$ random matrices with an asymptotic distribution and $U_n$ is a Haar distributed unitary random matrix, then $(A_1(\ldots, A_k, U_n)$ has also an asymptotic distribution (and there is asymptotic freeness).
Asymptotic freeness for RMT

- In 1992, Voiculescu proved that iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ are asymptotically free as $n \to \infty$. 

- In 1998 he proved the following stronger result: if $(A_1^{(n)}, \ldots, A_k^{(n)})$ is a family of $n \times n$ random matrices with an asymptotic $\ast$-distribution and $U_n$ is a Haar distributed unitary random matrix, then $(A_1^{(n)}, \ldots, A_k^{(n)}, U_n)$ has also an asymptotic $\ast$-distribution (and there is asymptotic freeness).
Asymptotic freeness for RMT

In 1992, Voiculescu proved that iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ are asymptotically free as $n \to \infty$. (i.e. the normalized trace of any word in the matrices converges almost surely to a quantity that can be computed with free probability).
Asymptotic freeness for RMT

- In 1992, Voiculescu proved that iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ are asymptotically free as $n \to \infty$. (i.e. the normalized trace of any word in the matrices converges almost surely to a quantity that can be computed with free probability).

- In 1998 he proved the following stronger result: if $(A_1^{(n)}, \ldots, A_k^{(n)})$ is a family of $n \times n$ random matrices with an asymptotic $*$- distribution and $U_n$ is a Haar distributed unitary random matrix, then $(A_1^{(n)}, \ldots, A_k^{(n)}, U_n)$ has also an asymptotic $*$- distribution (and there is asymptotic freeness).
Asymptotic freeness for RMT, ctd

- In 2005, Haagerup and Thorbjørnsen proved that the norm of any NC polynomial in iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ converges with probability one as $n \to \infty$ (towards where it should)
Asymptotic freeness for RMT, ctd

- In 2005, Haagerup and Thorbjørnsen proved that the norm of any NC polynomial in iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ converges with probability one as $n \to \infty$ (towards where it should).

- In 2010, Male proved that if $(A_1^{(n)}, \ldots, A_k^{(n)})$ is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial),
Asymptotic freeness for RMT, ctd

- In 2005, Haagerup and Thorbjørnsen proved that the norm of any NC polynomial in iid GUEs $X_1^{(n)}, \ldots, X_k^{(n)}$ converges with probability one as $n \to \infty$ (towards where it should).

- In 2010, Male proved that if $(A_1^{(n)}, \ldots, A_k^{(n)})$ is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial), then so does $(A_1^{(n)}, \ldots, A_k^{(n)}, X^{(n)})$, where $X^{(n)}$ is an independent GUE.
Norm convergence for random unitaries

Theorem (C, Male, 2011)

If \((A_1^{(n)}, \ldots, A_k^{(n)})\) is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial),
Norm convergence for random unitaries

Theorem (C, Male, 2011)

If \((A_1^{(n)}, \ldots, A_k^{(n)})\) is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial), then so does \((A_1^{(n)}, \ldots, A_k^{(n)}, U_n)\), where \(U_n\) is an independent Haar matrix.
Norm convergence for random unitaries

Theorem (C, Male, 2011)

If $(A_1^{(n)}, \ldots, A_k^{(n)})$ is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial), then so does $(A_1^{(n)}, \ldots, A_k^{(n)}, U_n)$, where $U_n$ is an independent Haar matrix.

Our proof builds on Camille’s proof and uses an ‘unfolding’ trick.
Norm convergence for random unitaries

Theorem (C, Male, 2011)

If \((A_1^{(n)}, \ldots, A_k^{(n)})\) is a family that satisfies strong asymptotic convergence (i.e. asymptotic convergence plus convergence of the operator norm of any NC polynomial), then so does \((A_1^{(n)}, \ldots, A_k^{(n)}, U_n)\), where \(U_n\) is an independent Haar matrix.

Our proof builds on Camille’s proof and uses an ‘unfolding’ trick.

Corollary (C, Male, 2011)

i.i.d copies of \(k\) random \(n \times n\) Haar unitaries converge strongly (in norm) towards generators of the free group factor.
Consequence: new examples

Corollary (C, Fukuda, Nechita)

Let $k \geq 2$ be an integer, $U_n^{(i)}$ be iid $n \times n$ Haar unitaries, and

$$\Phi_n(x) = k^{-1} \sum U_n^{(i)} x U_n^{(i)*}.$$
Consequence: new examples

Corollary (C, Fukuda, Nechita)

Let \( k \geq 2 \) be an integer, \( U_n^{(i)} \) be iid \( n \times n \) Haar unitaries, and

\[
\Phi_n(x) = k^{-1} \sum U_n^{(i)} x U_n^{(i)*}.
\]

Then the collection of nontrivial ordered eigenvalues of output of all pure states converges with probability one to a deterministic set (of \( \mathbb{R}^k \)).
Corollary (C, Fukuda, Nechita)

Let $k \geq 2$ be an integer, $U_n^{(i)}$ be iid $n \times n$ Haar unitaries, and

$$
\Phi_n(x) = k^{-1} \sum U_n^{(i)} x U_n^{(i)*}.
$$

Then the collection of nontrivial ordered eigenvalues of output of all pure states converges with probability one to a deterministic set (of $\mathbb{R}^k$).

In particular, almost surely,

$$
\lim_{n} \| \Phi_n \|_1 = \frac{4(k - 1)}{k^2}.
$$
Consequence: new examples

Thank you!