Block-modified random matrices, operator-valued free probability, and applications to entanglement theory

Ion Nechita

TU München and CNRS

joint work with Octavio Arizmendi and Carlos Vargas (Guanajuato)

Paris, October 20th 2015

Entanglement in Quantum Information Theory

- Quantum states with n degrees of freedom are described by density matrices
$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0$$
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$
- A state ρ_{12} is called separable if it can be written as a convex combination of product states
$$\rho_{12} \in \mathcal{SEP} \iff \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i),$$
where $t_i \geq 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathbb{M}_m^{1,+}$, $\rho_2(i) \in \mathbb{M}_n^{1,+}$
- Equivalently, $\mathcal{SEP} = \mathrm{conv}\left[\mathbb{M}_m^{1,+} \otimes \mathbb{M}_n^{1,+}\right]$
- Non-separable states are called entangled

More on entanglement - pure states

- Separable rank one (pure) states $\rho_{12} = P_{e \otimes f} = P_e \otimes P_f$.
- Bell state or maximally entangled state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2) \neq x \otimes y.$$

- For rank one quantum states, entanglement can be detected and quantified by the entropy of entanglement

$$E_{\text{ent}}(P_x) = H(s(x)) = -\sum_{i=1}^{\min(m,n)} s_i(x) \log s_i(x),$$

where $x \in \mathbb{C}^m \otimes \mathbb{C}^n \cong \mathbb{M}_{m \times n}(\mathbb{C})$ is seen as a $m \times n$ matrix and $s_i(x)$ are its singular values.

- A pure state $x \in \mathbb{C}^m \otimes \mathbb{C}^n$ is separable $\iff$ $E_{\text{ent}}(P_x) = 0$.

Separability criteria

- Let $\mathcal{A}$ be a C^* algebra. A map $f : \mathbb{M}_n \to \mathcal{A}$ is called
  - positive if $A \geq 0 \implies f(A) \geq 0$;
  - completely positive (CP) if $\mathrm{id}_k \otimes f$ is positive for all $k \geq 1$ ($k = n$ is enough).
- Let $f : \mathbb{M}_n \to \mathcal{A}$ be a completely positive map. Then, for every state $\rho_{12} \in \mathbb{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
- Let $f : \mathbb{M}_n \to \mathcal{A}$ be a positive map. Then, for every separable state $\rho_{12} \in \mathbb{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
  - ρ_{12} separable $\implies \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i)$.
  - $[\mathrm{id}_m \otimes f](\rho_{12}) = \sum_i t_i \rho_1(i) \otimes f(\rho_2(i))$.
  - For all i, $([\rho_2(i)) \geq 0$, so $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
- Hence, positive, but not CP maps f provide sufficient entanglement criteria: if $[\mathrm{id}_m \otimes f](\rho_{12}) \not\geq 0$, then ρ_{12} is entangled.
- Moreover, if $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$ for all positive, but not CP maps $f : \mathbb{M}_n \to \mathbb{M}_m$, then ρ_{12} is separable.
- Actually, for the exact converse to hold, uncountably many positive maps are needed [Skowronek], and for a very rough approximation of $\mathcal{SEP}$, exponentially many positive maps are needed [Aubrun, Szarek].

Positive Partial Transpose matrices

- The transposition map $\mathrm{t} : A \mapsto A^t$ is positive, but not CP. Define the convex set

$$\mathcal{PPT} = \{\rho_{12} \in \mathbb{M}_{mn}^{1,+} \mid [\mathrm{id}_m \otimes \mathrm{t}_n](\rho_{12}) \geq 0\}.$$

- For $(m, n) \in \{(2, 2), (2, 3)\}$ we have $\mathcal{SEP} = \mathcal{PPT}$. In other dimensions, the inclusion $\mathcal{SEP} \subset \mathcal{PPT}$ is strict.
- Low dimensions are special because every positive map $f : \mathbb{M}_2 \to \mathbb{M}_{2/3}$ is decomposable:

$$f = g_1 + g_2 \circ \mathrm{t},$$

with $g_{1,2}$ completely positive. Among all decomposable maps, the transposition criterion is the strongest.
$\rightsquigarrow$ see Staszek's talk for a simple proof

The PPT criterion at work

- Recall the Bell state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2).$$

- Written as a matrix in $\mathbb{M}_{2\cdot 2}^{1,+}$

$$\rho_{12} = \frac{1}{2} \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array} \right) = \frac{1}{2} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

- Partial transposition: transpose each block B_{ij}:

$$\rho_{12}^{\Gamma} = [\mathrm{id}_2 \otimes \mathrm{t}_2](\rho_{12}) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- This matrix is no longer positive $\implies$ the state is entangled.

The Choi matrix of a map

- For any n, recall that the maximally entangled state is the orthogonal projection onto

$$\mathbb{C}^n \otimes \mathbb{C}^n \ni \mathrm{Bell} = \frac{1}{\sqrt{n}} \sum_{i=1}^n e_i \otimes e_i.$$

- To any map $f : \mathbb{M}_n \to \mathcal{A}$, associate its Choi matrix

$$C_f = [\mathrm{id}_n \otimes f](P_{\mathrm{Bell}}) \in \mathbb{M}_n \otimes \mathcal{A}.$$

- Equivalently, if E_{ij} are the matrix units in $\mathbb{M}_n$, then

$$C_f = \sum_{i,j=1}^n E_{ij} \otimes f(E_{ij}).$$

Theorem (Choi '72)

A map $f : \mathbb{M}_n \to \mathcal{A}$ is CP iff its Choi matrix C_f is positive.

The Choi-Jamiołkowski isomorphism

- Recall (from now on $\mathcal{A} = \mathbb{M}_d$)
$$C_f = [\mathrm{id}_n \otimes f](P_{\mathrm{Bell}}) = \sum_{i,j=1}^{n} E_{ij} \otimes f(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_d.$$
- The map $f \mapsto C_f$ is called the Choi-Jamiołkowski isomorphism.
- It sends:
    1. All linear maps to all operators;
    2. Hermicity preserving maps to hermitian operators;
    3. Entanglement breaking maps to separable quantum states;
    4. Unital maps to operators with unit left partial trace ($[\mathrm{Tr} \otimes \mathrm{id}]C_f = \mathrm{I}_d$);
    5. Trace preserving maps to operators with unit left partial trace ($[\mathrm{id} \otimes \mathrm{Tr}]C_f = \mathrm{I}_n$).

Two questions

1. How to construct positive, but not CP maps?

Theorem (Collins, Hayden, N. '15)

Let n be a fixed integer, and consider a compactly supported probability measure μ having the following properties

- $\operatorname{supp}(\mu) \cap (-\infty, 0) \neq \emptyset$;
- $\operatorname{supp}(\mu^{\boxplus n}) \subset (0, \infty)$.

Let $f_d : \mathbb{M}_n \to \mathbb{M}_d$ be a sequence of maps having Choi matrices C_d. Assume that the random matrices C_d are unitarily invariant and that they converge in distribution to μ. Then, almost surely as $d \to \infty$, the map f_d is positive, but not CP.

2. Given a (positive, nut not CP) linear map f, how strong is the entanglement criterion induced by f?

Question 2: How powerful are the entanglement criteria?

- Let $f : \mathbb{M}_m \to \mathbb{M}_n$ be a given linear map (f positive, but not CP).
- If $[f \otimes \mathrm{id}](\rho) \not\geq 0$, then $\rho \in \mathbb{M}_m \otimes \mathbb{M}_d$ is entangled.
- If $[f \otimes \mathrm{id}](\rho) \geq 0$, then ... we do not know.
- Define

$$\mathcal{K}_f := \{\rho \,:\, [f \otimes \mathrm{id}](\rho) \geq 0\} \supseteq \mathcal{SEP}.$$

- We would like to compare (e.g. using the volume) the sets $\mathcal{K}_f$ and $\mathcal{SEP}$.
- Several probability measures on the set $\mathbb{M}_{md}^{1,+}$: for any parameter $s \geq md$, let W be a Wishart matrix of parameters (md, s):

$$W = XX^*, \text{ with } X \in \mathbb{M}_{md \times s} \text{ a Ginibre random matrix.}$$

- Let $\mathbb{P}_s$ be the probability measure obtained by pushing forward the Wishart measure by the map $W \mapsto W/\mathrm{Tr}(W)$.
- To compute $\mathbb{P}_s(\mathcal{K}_f)$, one needs to decide whether the spectrum of the random matrix $[f \otimes \mathrm{id}](W)$ is positive (here, d is large, m, n are fixed) $\rightsquigarrow$ block modified matrices.

Block-modified random matrices - previous results

Many cases studied independently, using the method of moments; no unified approach, each case requires a separate analysis:

- [Aubrun '12]: the asymptotic spectrum of $W^\Gamma := [\mathrm{id} \otimes \mathrm{t}](W)$ is a shifted semicircular, for $W \in \mathbb{M}_d \otimes \mathbb{M}_d$, $d \to \infty$
- [Banica, N. '13]: the asymptotic spectrum of $W^\Gamma := [\mathrm{id} \otimes \mathrm{t}](W)$ is a free difference of free Poisson distributions, for $W \in \mathbb{M}_m \otimes \mathbb{M}_d$, $d \to \infty$, m fixed
- [Jivulescu, Lupa, N. '14,'15]: the asymptotic spectrum of $W^{red} := W - [\mathrm{Tr} \otimes \mathrm{id}](W) \otimes I$ is a compound free Poisson distribution, for $W \in \mathbb{M}_m \otimes \mathbb{M}_d$, $d \to \infty$, m fixed (here, $f(X) = X - \mathrm{Tr}(X) \cdot I$)
- etc...

$\rightsquigarrow$ we propose a general, unified framework for such problems

The problem

- Consider a sequence of unitarily invariant random matrices $X_d \in \mathbb{M}_n \otimes \mathbb{M}_d$, having limiting spectral distribution μ.
- Define the modified version of X_d:

$$X_d^f = [f \otimes \mathrm{id}_d](X_d).$$

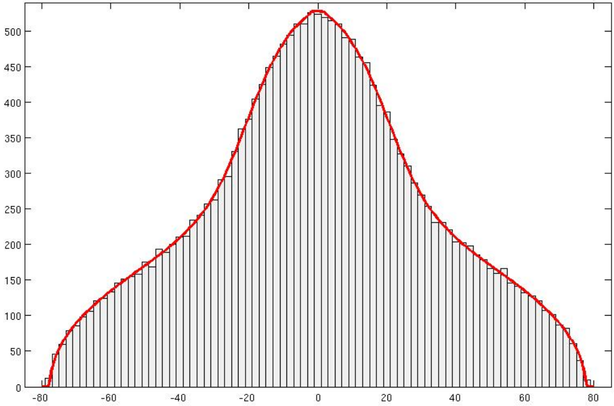
- Our goal: compute μ^f, the limiting spectral distribution of $\hat{X}_d$, as a function of
  1. The initial distribution μ
  2. The function f.

- Results: achieved this for all μ and a fairly large class of f.
- Tools: operator-valued free probability theory.

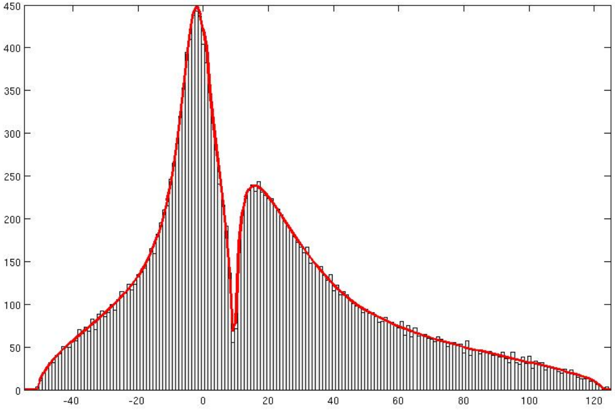
An example

$$f\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\right) = \begin{bmatrix} 11a_{11} + 15a_{22} - 25a_{12} - 25a_{21} & 36a_{21} \\ 36a_{12} & 11a_{11} - 4a_{22} \end{bmatrix}$$

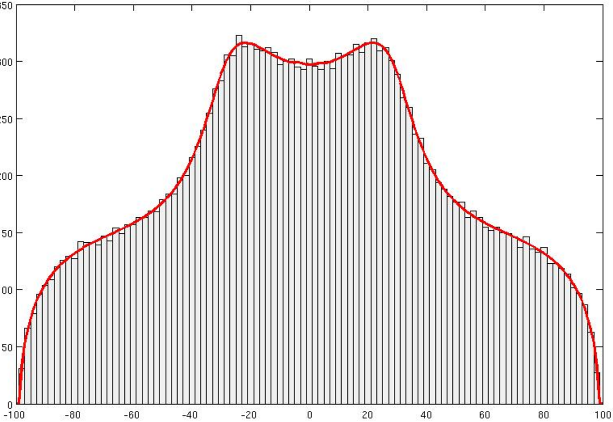
Wigner distribution



Wishart distribution



Arcsine distribution



Taking the limit

- We can write

$$X_d^f = [f \otimes \mathrm{id}](X_d) = \sum_{i,j,k,l=1}^{n} c_{ijkl}(E_{ij} \otimes I_d)X_d(\otimes E_{kl} \otimes I_d) \in \mathbb{M}_n \otimes \mathbb{M}_d,$$

  for some coefficients $c_{ijkl} \in \mathbb{C}$, which are actually the entries of the Choi matrix of f.

- At the limit:

$$x^f = \sum_{i,j,k,l=1}^{n} c_{ijkl} e_{i,j} x e_{k,l},$$

  for some random variable x having the same distribution as the limit of X_d and some (abstract) matrix units e_{ij}.

$\rightsquigarrow$ In the rectangular case $m \neq n$, one needs to use the techniques of Benaych-Georges; we will have freeness with amalgamation on $\langle p_m, p_m \rangle$.

Operator valued freeness

Definition

(1) Let $\mathcal{A}$ be a unital $*$-algebra and let $\mathbb{C} \subseteq \mathcal{B} \subseteq \mathcal{A}$ be a $*$-subalgebra. A $\mathcal{B}$-probability space is a pair $(\mathcal{A}, \mathbb{E})$, where $\mathbb{E} : \mathcal{A} \to \mathcal{B}$ is a conditional expectation, that is, a linear map satisfying:

$$\begin{aligned} \mathbb{E}\left(bab'\right) &= b\mathbb{E}(a)b', \qquad \forall b, b' \in \mathcal{B}, a \in \mathcal{A} \\ \mathbb{E}\left(1\right) &= 1. \end{aligned}$$

(2) Let $(\mathcal{A}, \mathbb{E})$ be a $\mathcal{B}$-probability space and let $\bar{a} := a - \mathbb{E}(a)1_{\mathcal{A}}$ for any $a \in \mathcal{A}$. The $*$-subalgebras $\mathcal{B} \subseteq A_1, \ldots, A_k \subseteq \mathcal{A}$ are $\mathcal{B}$-free (or free over $\mathcal{B}$, or free with amalgamation over $\mathcal{B}$) (with respect to $\mathbb{E}$) iff

$$\mathbb{E}(\bar{a}_1 \bar{a}_2 \cdots \bar{a}_r) = 0,$$

for all $r \geq 1$ and all tuples $a_1, \ldots, a_r \in \mathcal{A}$ such that $a_i \in A_{j(i)}$ with $j(1) \neq j(2) \neq \cdots \neq j(r)$.
(3) Subsets $S_1, \ldots, S_k \subset \mathcal{A}$ are $\mathcal{B}$-free if so are the $*$-subalgebras $\langle S_1, \mathcal{B} \rangle, \ldots, \langle S_k, \mathcal{B} \rangle$.

Similar to independence, freeness allows to compute mixed moments free random variables in terms of their individual moments.

Matrix-valued probability spaces

Let $\mathcal{A}$ be a unital C^*-algebra and let $\tau : \mathcal{A} \to \mathbb{C}$ be a state. Consider the algebra $\mathbb{M}_n(\mathcal{A}) \cong \mathbb{M}_n \otimes \mathcal{A}$ of $n \times n$ matrices with entries in $\mathcal{A}$. The maps

$$\mathbb{E}_3 : (a_{ij})_{ij} \mapsto (\tau(a_{ij}))_{ij} \in \mathbb{M}_n,$$

$$\mathbb{E}_2 : (a_{ij})_{ij} \mapsto (\delta_{ij}\tau(a_{ij}))_{ij} \in \mathbb{D}_n,$$

and

$$\mathbb{E}_1 : (a_{ij})_{ij} \mapsto \sum_{i=1}^{n} \frac{1}{n}\tau(a_{ii}) I_n \in \mathbb{C} \cdot I_n$$

are respectively, conditional expectations onto the algebras $\mathbb{M}_n \supset \mathbb{D}_n \supset \mathbb{C} \cdot I_n$ of constant matrices, diagonal matrices and multiples of the identity.

Proposition

If $A_1, \ldots, A_k$ are free in $(\mathcal{A}, \tau)$, then the algebras $M_n(A_1), \ldots, M_n(A_k)$ of matrices with entries in $A_1, \ldots, A_k$ respectively are in general not free over $\mathbb{C}$ (with respect to $\mathbb{E}_1$). They are, however, $\mathbb{M}_n$-free (with respect to $\mathbb{E}_3$).

Restricting cumulants

Proposition (Nica, Shlyakhtenko, Speicher)

Let $1 \in \mathcal{D} \subset \mathcal{B} \subset \mathcal{A}$ be algebras such that $(\mathcal{A}, \mathbb{F})$ and $(\mathcal{B}, \mathbb{E})$ are respectively $\mathcal{B}$-valued and $\mathcal{D}$-valued probability spaces and let $a_1, \ldots, a_k \in \mathcal{A}$. Assume that the $\mathcal{B}$-cumulants of $a_1, \ldots, a_k \in \mathcal{A}$ satisfy

$$R^{\mathcal{B};a_1,\ldots,a_k}_{i_1,\ldots,i_n}(d_1, \ldots, d_{n-1}) \in \mathcal{D},$$

for all $n \in \mathbb{N}$, $1 \leq i_1, \ldots, i_n \leq k$, $d_1, \ldots, d_{n-1} \in \mathcal{D}$.
Then the $\mathcal{D}$-cumulants of $a_1, \ldots, a_k$ are exactly the restrictions of the $\mathcal{B}$-cumulants of $a_1, \ldots, a_k$, namely for all $n \in \mathbb{N}$, $1 \leq i_1, \ldots, i_n \leq k$, $d_1, \ldots, d_{n-1} \in \mathcal{D}$:

$$R^{\mathcal{B};a_1,\ldots,a_k}_{i_1,\ldots,i_n}(d_1, \ldots, d_{n-1}) = R^{\mathcal{D};a_1,\ldots,a_k}_{i_1,\ldots,i_n}(d_1, \ldots, d_{n-1}),$$

Corollary

Let $\mathcal{B} \subseteq A_1, A_2 \subseteq \mathcal{A}$ be $\mathcal{B}$-free and let $\mathcal{D} \subseteq M_N(\mathbb{C}) \otimes \mathcal{B}$. Assume that, individually, the $\mathbb{M}_N \otimes \mathcal{B}$-valued moments (or, equivalently, the $\mathbb{M}_N \otimes \mathcal{B}$-cumulants) of both $x \in \mathbb{M}_N \otimes A_1$ and $y \in \mathbb{M}_N \otimes A_2$, when restricted to arguments in $\mathcal{D}$, remain in $\mathcal{D}$. Then x, y are $\mathcal{D}$-free.

A different formulation

Proposition

The block-modified random variable x^f has the following expression in terms of the eigenvalues and of the eigenvectors of the Choi matrix C:

$$x^f = v^*(x \otimes C)v,$$

where

$$v = \sum_{s=1}^{n^2} b_s^* \otimes a_s \in \mathcal{A} \otimes \mathbb{M}_{n^2},$$

a_s are the eigenvectors of C, and the random variables $b_s \in \mathcal{A}$ are defined by $b_s = \sum_{i,j=1}^n \langle E_i \otimes E_j, a_s \rangle e_{i,j}$.

Theorem

Consider a linear map $f : \mathbb{M}_n \to \mathbb{M}_n$ having a Choi matrix $C \in \mathbb{M}_{n^2} \subset \mathcal{A} \otimes \mathbb{M}_{n^2}$ which has tracially well behaved eigenspaces. Then, the random variables $x \otimes C$ and vv^* are free with amalgamation over the (commutative) unital algebra $\mathcal{B} = \langle C \rangle$ generated by the matrix C.

Well behaved functions

Definition

We say that f is well behaved if the eigenspaces of its Choi matrix are *tracially well behaved* if

$$\tau(b_{j_1} b_{j_2}^* Q_{i_1} \ldots Q_{i_k}) = \delta_{j_1 j_2} \tau(b_{j_1} b_{j_1}^* Q_{i_1} \ldots Q_{i_k}),$$

for every $i_1, \ldots, i_k \leq n^2$ and $j_1, j_2 \leq n^2$. We define

$$Q_i = b_i^* b_i.$$

$\rightsquigarrow$ a stronger condition:

Definition

The Choi matrix C is said to satisfy the unitarity condition if, for all t, there is some real constant d_t such that $[\mathrm{id} \otimes \mathrm{Tr}](P_t) = d_t I_n$, where P_t are the eigenprojectors of C.

The limiting distributions of block-modified matrices

Theorem

If the Choi matrix C satisfies the unitarity condition, then the distribution of x^f has the following R-transform:

$$R_{x^f}(z) = \sum_{i=1}^{s} d_i \rho_i R_x \left[\frac{\rho_i}{n} z \right],$$

where ρ_i are the distinct eigenvalues of C and nd_i are ranks of the corresponding eigenprojectors. In other words, if μ, resp. μ^f, are the respective distributions of x and x^f, then

$$\mu^f = \boxplus_{i=1}^{s} (D_{\rho_i/n}\mu)^{\boxplus nd_i}.$$

Range of applications

The following functions are well behaved

1. Unitary conjugations $f(X) = UXU^*$
2. The trace and its dual $f(X) = \mathrm{Tr}(X)$, $f(x) = xI_n$
3. The transposition $f(X) = X^\top$
4. The reduction map $f(X) = I_n \cdot \mathrm{Tr}(X) - X$
5. Linear combinations of the above $f(X) = \alpha X + \beta \mathrm{Tr}(X) I_n + \gamma X^\top$
6. Mixtures of orthogonal automorphisms

$$f(X) = \sum_{i=1}^{n^2} \alpha_i U_i X U_i^*,$$

for orthogonal unitary operators U_i

$$\mathrm{Tr}(U_i U_j^*) = n\delta_{ij}.$$

The End

arXiv:1508.05732