On the orbit space of unitary actions for mixed quantum states

Vladimir Gerdt, Arsen Khvedelidze and Yuri Palii

Group of Algebraic and Quantum computation
Laboratory of Information Technologies
Joint Institute for Nuclear Research

ACA 2015, Kalamata, Greece, July 20-23, 2015

Contents

The problem statement

Generic question:

“CLASSICALITY OR QUANTUMNESS” ?

Mathematical problem:

DESCRIPTION OF THE ENTANGLEMENT SPACE

Space of states

- A complete information on a generic N-dimensional quantum system is accumulated in $N \times N$ density matrix ϱ .
  1. self-adjoint: $\varrho = \varrho^{+}$,
  2. positive semi-definite: $\varrho \geq 0$,
  3. Unit trace: $\mathrm{Tr}\varrho = 1$,
- The set $\mathfrak{P}_+$, of all possible density matrices, is the space of (*mixed*) quantum states.
- Equivalence relation on $\mathfrak{P}_+$, due to the adjoint action of $SU(N)$ group

$$(\mathrm{Ad}\, g\,)\varrho = g\,\varrho\, g^{-1}\,, \qquad g \in SU(N)\,,$$

defines the orbit space $\mathfrak{P}_+ \,|SU(N)$ that comprises a physically relevant knowledge.

Density matrix for binary composites

- Composition of two subsystems represented by the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ defines tensor product space

$$\mathcal{H}_{A\cup B} = \mathcal{H}_A \otimes \mathcal{H}_B \,.$$

- The density matrix of joint system ϱ acts on $\mathcal{H}_A \otimes \mathcal{H}_B$
- For a binary system, $N_1 \otimes N_2$, the Local Unitary (LU) equivalence, $\varrho \sim \varrho'$, means

$$\varrho' = SU(N_1) \times SU(N_2)\, \varrho\, (SU(N_1) \times SU(N_2))^\dagger \;.$$

- The LU equivalence decomposes $\mathfrak{P}_+$ into the local orbits. The union of these classes is customary to call as the “entanglement space” $\mathcal{E}_n$.

Entanglement

A bipartite quantum system is separable if its density matrix can be written in the form

$$\rho = \sum_{j=1}^{M} q_j\, \rho_j^A \otimes \rho_j^B, \qquad q_j \geq 0 \qquad \sum_{j=1}^{M} q_j = 1.$$

where ρ_j^A and ρ_j^B are density matrices of the constituent systems.

Otherwise the bipartite system is entangled.

The property to be entangled (resp. separated) as well as the measure of entanglement is preserved by local unitary transformations.

"The entanglement of a two-qubit system is a non-local property so that measures of entanglement should be independent of all local transformations of the two qubits separately. Since a mixed two-qubit system is described by its density matrix, its nonlocal entangling properties must be described by local invariants of the density matrix."

King & Welsh. Qubits and invariant theory. J. Phys: Conf. Series **30**, 1-8, 2006.

$\mathfrak{P}_+$ as semialgebraic variety

- The set of all $N \times N$ Hermitian matrices with unit trace is a manifold in hyperplane $P \subset \mathbb{R}^{N^2}$
- The positive semi-definiteness

$$\varrho \geq 0\,,$$

restricts manifold further to a convex $(N^2 - 1)$-dimensional body

- Since all roots of the characteristic equation

$$\det|\lambda \mathrm{I} - \varrho| = \lambda^N - S_1\lambda^{N-1} + \cdots + (-1)^N S_N = 0\,,$$

are real, for their non-negativity it is necessary and sufficient that

$$S_k \geq 0\,, \qquad \forall\, k.$$

Example: Pairs of 2-qubits

- The unit trace condition and semipositivity of ϱ define semialgebraic set

$$0 \leq S_k \leq 1\,, \qquad k = 1, 2, \ldots, N\,.$$

- For 2 qubit case , S_k are polynomials up to fourth order in 15 variables, e.g., in Fano parameters

$$\varrho = \frac{1}{4}\left(\mathrm{I}_2 \otimes \mathrm{I}_2 + \vec{a}\cdot\vec{\sigma} \otimes \mathrm{I}_2 + \mathrm{I}_2 \otimes \vec{b}\cdot\vec{\sigma} + c_{ij}\,\sigma_i \otimes \sigma_j\right)\,.$$

- Parameters c_{ij} determine the correlation matrix $c_{ij} = ||C||_{ij}$

Coefficients S_k for two qubits

$$
\begin{aligned}
S_2 &= 1 - \frac{1}{3}\left(\boldsymbol{a}^2 + \boldsymbol{b}^2 + \boldsymbol{c}^2\right) \\
S_3 &= 1 - \left(\boldsymbol{a}^2 + \boldsymbol{b}^2 + \boldsymbol{c}^2\right) - 2\left(c_1 c_2 c_3 - \sum_{i=1}^{3} a_i b_i c_i\right), \\
S_4 &= \left(1 - \left(\boldsymbol{a}^2 + \boldsymbol{b}^2 + \boldsymbol{c}^2\right)\right)^2 + 8\left(c_1 c_2 c_3 - \sum_{i=1}^{3} a_i b_i c_i\right) \\
&- 2\left[2\left(\boldsymbol{a}^2 \boldsymbol{b}^2 + (a_i^2 + b_i^2) c_i^2 - \sum_{cyclic} a_i b_i c_j c_k\right) + (\boldsymbol{c}^2)^2 - c_i^4\right].
\end{aligned}
$$

c_1, c_2, c_3- singular numbers of correlation matrix C

Peres–Horodecki separability criterion

- Peres–Horodecki separability criterion:
  The system is in a separable state iff partially transposed density matrix

$$\varrho^{T_B} = I \otimes T\varrho\,, \qquad T - \text{transposition operator}$$

  satisfies the conditions for a density operator.
- Coefficients of the characteristic equation for ϱ^{T_B}:

$$S_2^{T_B} = S_2\,,$$
$$S_3^{T_B} = S_3 - \frac{1}{4}\det(C)\,,$$
$$S_4^{T_B} = S_4 + \frac{1}{16}\det(M)\,,$$

- $M = \varrho - \varrho_A \otimes \varrho_B$ −Schlienz & Mahler matrix,
  $\varrho_A = \mathrm{tr}_B\varrho$ and $\varrho_B = \mathrm{tr}_A\varrho$ - density matrices of subsystems A, and B.

3-parameter family of 2-qubits states

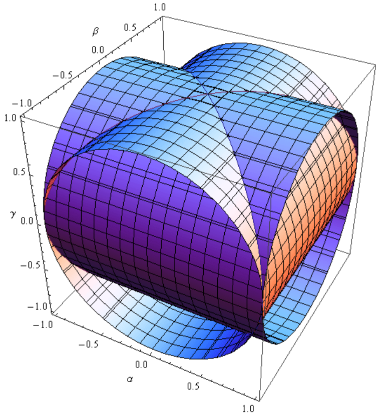
- A sample density matrix (GKP, Phys. Atom. Nucl. 74(6),893-900,2011)

$$\rho = \frac{1}{4}\begin{pmatrix} 1+\alpha & 0 & 0 & 0 \\ 0 & 1-\beta & i\gamma & 0 \\ 0 & -i\gamma & 1+\beta & 0 \\ 0 & 0 & 0 & 1-\alpha \end{pmatrix}$$

- Its partially transposed

$$\rho^{T_B} = \frac{1}{4}\begin{pmatrix} 1+\alpha & 0 & 0 & i\gamma \\ 0 & 1-\beta & 0 & 0 \\ 0 & 0 & 1+\beta & 0 \\ -i\gamma & 0 & 0 & 1-\alpha \end{pmatrix}$$

Semipositivity domains



- $\rho \geq 0$:

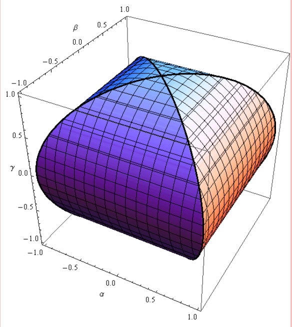
$$\alpha^2 \leq 1$$
$$\beta^2 + \gamma^2 \leq 1$$

- $\rho^{T_B} \geq 0$:

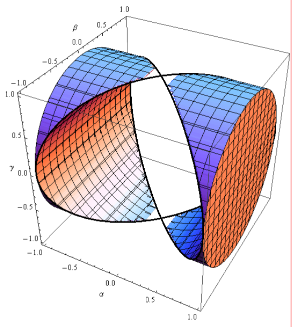
$$\beta^2 \leq 1$$
$$\alpha^2 + \gamma^2 \leq 1$$

Domains of Separability vs. Entanglement

Separability domain



Entanglement domain



Bipartite ($r \times s-$dimensional) quantum system

$$\rho = \frac{1}{r \cdot s}\left(\mathbb{I}_{r \cdot s} + \sum_{i=1}^{r^2-1} a_i\,\lambda_i \otimes \mathbb{I}_s + \sum_{i=1}^{s^2-1} b_i\,\mathbb{I}_r \otimes \mu_i + \sum_{i=1}^{r^2-1}\sum_{j=1}^{s^2-1} c_{ij}\lambda_i \otimes \mu_j\right)$$

ρ is an element in the universal enveloping algebra of $\mathfrak{su}(r \cdot s)$.

Matrix $C := ||c_{ij}||$

$$c_{ij} = \mathrm{Tr}(\rho \cdot \lambda_i \otimes \mu_j)$$

accounts for correlations of parts.

Local unitary transformations:

$$\rho \quad \mapsto \quad (U_1 \times U_2) \cdot \rho \cdot (U_1 \times U_2)^{\dagger}\,, \qquad U_1 \in \mathrm{SU}(r), \qquad U_2 \in \mathrm{SU}(s)$$

It is natural to describe the orbit space in terms of elements in the invariant ring $K[X]^G$

$$X := \{a_i, b_j, c_{ij} \mid 1 \le i \le r^2 - 1,\ 1 \le j \le s^2 - 1\} \subset R^{(r^2-1)(s^2-1)}$$

Elements of Invariant Theory I

Let G be a compact Lie group. Then,

- The invariant ring

$$\mathbb{R}[X]^G := \{\, p \in \mathbb{R}[X] \mid p(v) = p(g \circ v)\ \forall v \in V,\ g \in G \,\}$$

  is finitely generated (Hilbert's finiteness theorem).
- There exist algorithms to construct generators of $\mathbb{R}[X]^G$.
- There exist a set of algebraically independent homogeneous primary invariants

$$\mathcal{P} := \{p_1, \ldots, p_q\} \subset \mathbb{R}[X]^G$$

  such that $\mathbb{R}[X]^G$ is integral over $\mathbb{R}[\mathcal{P}]$ (Noether normalization lemma).
  Criterion: the variety in C^q given by $\mathcal{P}$ is $\{0\}$.
- There exist a set $\mathcal{S} := \{s_1, \ldots, s_m\}$ of secondary invariants, homogeneous generators of $\mathbb{R}[X]^G$ as a module over $\mathbb{R}[\mathcal{P}]$.

  Together, primary and secondary invariants (integrity basis) generate $\mathbb{R}[X]^G$.

Elements of Invariant Theory II

- $\mathbb{R}[X]^G$ is Cohen-Macaulay and there is a Hironaka decomposition

$$\mathbb{R}[X]^G = \oplus_{k=0}^{m} s_k \mathbb{R}[\mathcal{P}]\,.$$

- Orbit separation: (Onishchik & Vinberg. Lie Groups and Algebraic Groups. Springer, 1990; Th.3, Chap.3, §4)

$$\forall u, v \in V \text{ s.t. } G \circ u \neq G \circ v \;:\; \exists p \in \mathbb{R}[X]^G \text{ s.t. } p(u) \neq p(v)\,.$$

- Syzygy ideal:

$$I_{\mathcal{P}} := \{\, h \in \mathbb{R}[y_1, \ldots, y_q] \mid h(p_1, p_2, \ldots, p_q) = 0 \text{ in } \mathbb{R}[x_1, \ldots, x_d] \,\}\,,$$

$$\mathbb{R}[y_1, \ldots, y_q] \,/\, I_{\mathcal{P}} \simeq \mathbb{R}[X]^G\,.$$

Algorithms to construct invariants of linear algebraic groups

- Hilbert's algorithm, 1893. Based on computing nullcone and then passing from invariants defining the nullcone to the complete set of generators, which amounts to an integral closure computation (Sturmfels. Algorithm in Invariant Theory. 2nd edition, 2008)
- Derksen's algorithm for reductive G, 1999. Implemented in Magma, Singular.
- Gatermann & Guyard, 1999. Hilbert series driven Buchberger algorithm.
- Bayer, 2003. Algorithm for computation of invariants up to a given degree. Implemented in Singular.
- Müller-Quade & Beth, 1999. Implemented in Magma.
- Hubert & Kogan, 2007. Algorithm for computation of rational invariants.
- ....
- Eröcal, Motsak, Schreyer, Steenpass, 2015 (arXiv:1502.01654v1 [math.AC]). Two refined algorithms for computation of syzygies. Implemented in Singular.

Main Theorem

(Procesi & Schwarz. Invent. Math. 81,539-554,1985) (cf. also Abud & Sartori. Phys. Lett. B 104, 147-152,1981)

Let a compact Lie group G acts linearly on $\mathbb{R}[X]$, $\mathcal{B} = \{p_1, \ldots, p_m\}$ be an integrity basis of $\mathbb{R}[X]^G$ where $X = \{x_1, \ldots, x_d\}$ ($\mathbb{R}[X]^G = \mathbb{R}[\mathcal{B}]$) and $V_\mathcal{B} \subseteq \mathbb{R}^m$ be the real irreducible algebraic set (variety) generated by $I_\mathcal{B}$. Then $\mathcal{B}$ defines the polynomial mapping

$$X \to \mathbb{R}[\mathcal{B}] \ : \ (x_1, \ldots, x_d) \stackrel{p}{\longrightarrow} (p_1, \ldots, p_m)\,,$$

such that

- The image $Z \subseteq V_\mathcal{B}$ of p is a semialgebraic set.
- If one gives X and Z their classical topologies, then the mapping p is proper, and it induces a homomorphism

$$\bar{p} : \ X/G \longrightarrow Z.$$

- $Z = \{\, v \in V_\mathcal{B} \mid \mathrm{Grad(v)} \geq 0 \,\}$. where Grad is $m \times m$ matrix

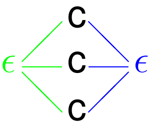
$$||\mathrm{Grad}||_{\alpha\beta} = \partial_i p_\alpha \cdot \partial_i p_\beta\,.$$

The last positivity condition follows from $(p_\alpha \partial_i p_\alpha)(p_\beta \partial_i p_\beta) \geq 0$.

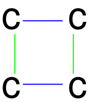
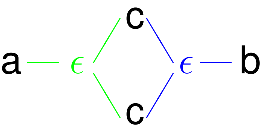
Invariants for $SU(2) \times SU(2)$ I

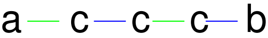
King, Welsh, Jarvis. J. Phys. A: Math. Gen. 40, 10083-110108, 2007

2	a — a	$C_{200} = a_i\, a_i$
	b — b	$C_{020} = b_i\, b_i$
	c = c	$C_{002} = c_{ij}\, c_{ij}$

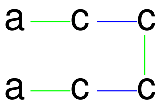
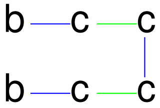
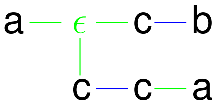
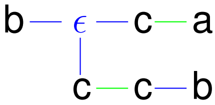
3	a — c — b	$C_{111} = a_i\, b_j\, c_{ij}$
		$C_{003} = \dfrac{1}{3!}\, \epsilon_{ijk}\, \epsilon_{pqr}\, c_{ip}\, c_{jq}\, c_{kr}$

Invariants for $SU(2) \times SU(2)$ II

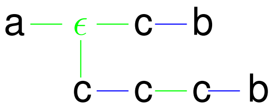
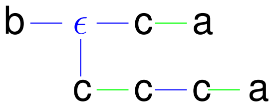
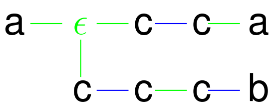
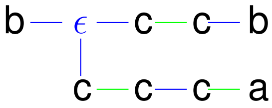
4		$C_{202} = a_i\, a_j\, c_{i,\alpha}\, c_{j,\alpha}$
		$C_{022} = b_\alpha\, b_\beta\, c_{i,\alpha}\, c_{i,\beta}$
		$C_{004} = c_{i,\alpha}\, c_{i,\beta}\, c_{j,\alpha}\, c_{j,\beta}$
		$C_{112} = \frac{1}{2}\, \epsilon_{i,j,k}\, \epsilon_{\alpha,\beta,\gamma}\, a_i\, b_\alpha\, c_{j,\beta}\, c_{k,\gamma}$

5		$C_{113} = a_i\, b_\alpha\, c_{i,j}\, c_{k,j}\, c_{k,\alpha}$

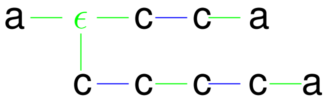
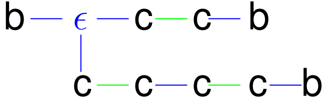
Invariants for $SU(2) \times SU(2)$ III

6		$C_{204} = a_i\, a_\beta\, c_{i,j}\, c_{k,j}\, c_{k,\alpha}\, c_{\beta,\alpha}$
		$C_{024} = b_i\, b_\beta\, c_{j,i}\, c_{j,k}\, c_{\alpha,k}\, c_{\alpha,\beta}$
		$C_{213} = \epsilon_{i,j,k}\, a_i\, a_l\, b_\alpha\, c_{j,\alpha} c_{k,\gamma}\, c_{l,\gamma}$
		$C_{123} = \epsilon_{\alpha,\beta,\gamma}\, a_i\, b_\alpha\, b_\delta\, c_{i,\beta}\, c_{j,\gamma}\, c_{j,\delta}$

Invariants for $SU(2) \times SU(2)$ IV

7		$C_{124} = \epsilon_{i,j,k}\, a_i\, b_\alpha\, b_\delta\, c_{j,\alpha}\, c_{k,\beta}\, c_{\gamma,\beta}\, c_{\gamma,\delta}$
		$C_{214} = \epsilon_{i,j,k}\, a_\alpha\, a_\delta\, b_i\, c_{\alpha,j}\, c_{\beta,k}\, c_{\beta,\gamma}\, c_{\delta,\gamma}$
8		$C_{215} = \epsilon_{i,j,k}\, a_i\, a_\beta\, b_\eta\, c_{j,\alpha}\, c_{k,\gamma}\, c_{\beta,\alpha}\, c_{\delta,\gamma}\, c_{\delta,\eta}$
		$C_{125} = \epsilon_{i,j,k}\, a_\eta\, b_i\, b_\beta\, c_{\alpha,j}\, c_{\gamma,k}\, c_{\alpha,\beta}\, c_{\gamma,\delta}\, c_{\eta,\delta}$

Invariants for $SU(2) \times SU(2)$ V

9		$C_{306} = \epsilon_{i,j,k}\, a_i\, a_\beta\, a_\theta\, c_{j,\alpha}\, c_{k,\gamma}\, c_{\beta,\alpha}\, c_{\delta,\gamma}\, c_{\delta,\eta}\, c_{\theta,\eta}$
		$C_{036} = \epsilon_{i,j,k}\, b_i\, b_\beta\, b_\theta\, c_{\alpha,j}\, c_{\gamma,k}\, c_{\alpha,\beta}\, c_{\gamma,\delta}\, c_{\eta,\delta} c_{\eta,\theta}$

Example: 5-parameter density matrix ("X"-matrix)

$$\varrho = \frac{1}{4}\begin{pmatrix} 1+\alpha+\beta+\gamma_3 & 0 & 0 & \gamma_1-\gamma_2 \\ 0 & 1+\alpha-\beta-\gamma_3 & \gamma_1+\gamma_2 & 0 \\ 0 & \gamma_1+\gamma_2 & 1-\alpha+\beta-\gamma_3 & 0 \\ \gamma_1-\gamma_2 & 0 & 0 & 1-\alpha-\beta+\gamma_3 \end{pmatrix}$$

Fano parameters: $a_3 = \alpha,\ b_3 = \beta,\ c_{11} = \gamma_1,\ c_{22} = \gamma_2,\ c_{33} = \gamma_3$

Partial transposition:

$$\varrho^{T_b} = \frac{1}{4}\begin{pmatrix} 1+\alpha+\beta+\gamma_3 & 0 & 0 & \gamma_1+\gamma_2 \\ 0 & 1+\alpha-\beta-\gamma_3 & \gamma_1-\gamma_2 & 0 \\ 0 & \gamma_1-\gamma_2 & 1-\alpha+\beta-\gamma_3 & 0 \\ \gamma_1+\gamma_2 & 0 & 0 & 1-\alpha-\beta+\gamma_3 \end{pmatrix}$$

Peres–Horodecki separability criterion:

The two-qubit the system is in a separable state iff partially transposed density matrix ρ^{T_b} satisfies the conditions for a density operator.

Nonzero fundamental invariants

For our space of 5-parameter matrices there are 12 non-zero local invariants

$$C_{200},\ C_{020},\ C_{002},\ C_{111},\ C_{003},\ C_{202},\ C_{022},\ C_{004},\ C_{112},\ C_{113},\ C_{204},\ C_{024}$$

of the form

$$
\begin{aligned}
\text{Deg 2}: &\ C_{200} = \alpha^2\,, \qquad C_{020} = \beta^2\,, \qquad C_{002} = \gamma_1^2 + \gamma_2^2 + \gamma_3^2 \\
\text{Deg 3}: &\ C_{111} = \alpha\beta\gamma_3\,, \qquad C_{003} = \gamma_1\gamma_2\gamma_3 \\
\text{Deg 4}: &\ C_{202} = \alpha^2\gamma_3^2\,, \qquad C_{022} = \beta^2\gamma_3^2 \\
&\ C_{004} = \gamma_1^4 + \gamma_2^4 + \gamma_3^4\,, \qquad C_{112} = \alpha\beta\gamma_1\gamma_2 \\
\text{Deg 5}: &\ C_{113} = \alpha\beta\gamma_3^3 \\
\text{Deg 6}: &\ C_{204} = \alpha^2\gamma_3^4\,, \qquad C_{024} = \alpha^2\gamma_3^4
\end{aligned}
$$

Primary invariants and syzygies

Primary invariants:

$$C_{200} \equiv a,\ C_{020} \equiv b,\ C_{002} \equiv c,\ C_{111} \equiv x,\ C_{003} \equiv y.$$

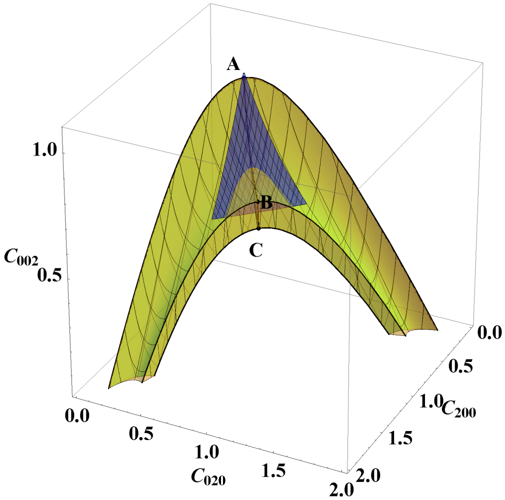
Solution of the syzygies

$$C_{204} = \frac{x^4}{ab^2} \qquad C_{024} = \frac{x^4}{a^2 b} \qquad C_{112} = \frac{aby}{x}$$

$$C_{022} = \frac{x^2}{a} \qquad C_{202} = \frac{x^2}{b} \qquad C_{113} = \frac{x^3}{ab}$$

$$C_{004} = c^2 + 2\frac{x^4}{a^2 b^2} - 2\frac{cx^2}{ab} - 2\frac{aby^2}{x^2}$$

Semipositivity of ϱ and Grad

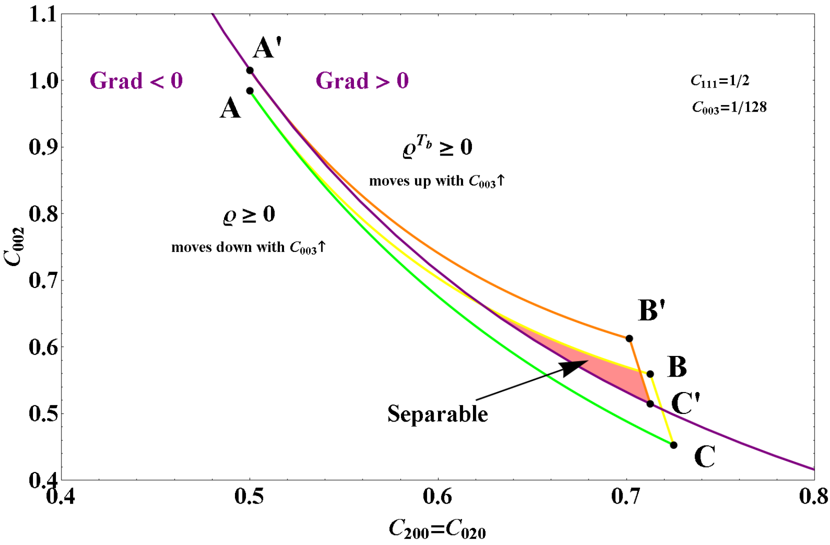


green: $\varrho \geq 0$

blue: Grad≥ 0

$C_{111} = 1/2$,
$C_{003} = 1/128$

Separability area



Conclusions

- It is natural to describe entanglement space of mixed quantum states in terms of local unitary invariants.
- The entanglement space is a semialgebraic variety.
- For 2-qubit the integrity basis of the invariant polynomial ring $\mathbb{R}[X]^{SU(2)\times SU(2)}$ has been constructed. Here X is the set of 15 Fano parameters.
- It is a challenge for computer algebra to recompute algorithmically the integrity basis of $\mathbb{R}[X]^{SU(2)\times SU(2)}$ and to derive the full set of polynomial equations and inequalities defining the 2-qubit entanglement space.
- Recent versions of MAPLE and MATHEMATICA have special built-in routines for (numerical) solving systems of polynomial equations and inequalities.