Quantum Computation and Information Seminar

University of California, Berkeley

Entanglement and Invariant Theory

Markus Grassl

joint work with Thomas Beth, Martin Rötteler, Yuriy Makhlin

November 19, 2002

Arbeitsgruppe *Quantum Computing*
Prof. Dr. Thomas Beth
Institut für Algorithmen und Kognitive Systeme
Universität Karlsruhe, Germany

Main Problem

Characterize the non-local properties of quantum states.

Various approaches

- entanglement measures:
  (real) functions on the state space, that
  - are zero for states without entanglement (product states/separable states)
  - are constant under local unitary operations
  - do not increase under local operations and classical communication

  Problem: a single entanglement measure implies a total order on quantum states, but the structure of multi-particle states is complicated

- local orbits:
  Given two quantum states

  $$|\psi\rangle \text{ and } |\phi\rangle \qquad (\rho \text{ and } \rho')$$

  on n particles (qudits), is there a local unitary transformation $U = U_1 \otimes U_2 \otimes \ldots \otimes U_n$ with

  $$U|\psi\rangle = |\phi\rangle \qquad (U\rho U^{-1} = \rho')?$$

Our Approach

Use the polynomial invariants of the groups

- $SU(d) \otimes \ldots \otimes SU(d)$
- $U(d) \otimes \ldots \otimes U(d)$

operating on

- pure states $|\psi\rangle$
- mixed states ρ

to describe multi-particle entanglement.

This gives a *complete* description:

Theorem 3:
The orbits of a compact linear group acting in a real vector space are separated by the (polynomial) invariants.

(A. L. Onishchik, *Lie groups and algebraic groups*, Springer, 1990, Ch. 3, §4)

Operation of $GL(N, \mathbb{F})$

Linear operation

on polynomials $f \in \mathbb{F}[x_1, \ldots, x_N] =: \mathbb{F}[\boldsymbol{x}]$

$$f(\boldsymbol{x})^g := f(\boldsymbol{x}^g) \qquad \text{where } \boldsymbol{x}^g = (x_1, \ldots, x_N) \cdot g \text{ and } g \in GL(N, \mathbb{F})$$

$\Longrightarrow$ pure quantum states

Operation by conjugation

on polynomials $f \in \mathbb{F}[x_{11}, \ldots, x_{NN}] =: \mathbb{F}[X]$

$$f(X)^g := f(X^g) \quad \text{where}$$

$$X^g = g^{-1} \cdot \begin{pmatrix} x_{11} & \cdots & x_{1N} \\ \vdots & \ddots & \vdots \\ x_{N1} & \cdots & x_{NN} \end{pmatrix} \cdot g$$

$\Longrightarrow$ mixed quantum states

Polynomial Invariants

Basic problem

Given a subgroup $G \leq GL(N, \mathbb{F})$, which polynomials
in N (or N^2) variables are invariant under linear operation (or operation by conjugation)?
Notation: $$\mathbb{F}[\boldsymbol{x}]^G := \{f(\boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}] | \forall g \in G : f(\boldsymbol{x})^g = f(\boldsymbol{x})\}$$

Properties of $\mathbb{F}[\boldsymbol{x}]^G$

- Homogeneous polynomials remain homogeneous ($\Longrightarrow$ homogeneous generators).
- Any linear combination of invariants is an invariant.
- The product of invariants is an invariant.
- For reductive groups $\mathbb{F}[\boldsymbol{x}]^G$ is finitely generated.
- Some invariants are algebraically independent (primary invariants).
- The other invariants obey some polynomial relations.
- In special cases: the invariant ring can be decomposed as a free module (generated by the secondary invariants) over the primary invariants.

Example: Invariants of S_4

$$S_4 = \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle \cong \langle (1\,2\,3\,4), (1\,2) \rangle$$

Power sums

$$p_1 := x_1 + x_2 + x_3 + x_4$$
$$p_2 := x_1^2 + x_2^2 + x_3^2 + x4^2$$
$$p_3 := x_1^3 + x_2^3 + x_3^3 + x_4^3$$
$$p_4 := x_1^4 + x_2^4 + x_3^4 + x_4^4$$

Elementary symmetric polynomials

$$s_1 := x_1 + x_2 + x_3 + x_4$$
$$s_2 := x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$
$$s_3 := x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$
$$s_4 := x_1x_2x_3x_4$$

Any polynomial invariant of S_4 can be expressed uniquely as a polynomial in p_1, p_2, p_3, and p_4 (or s_1, s_2, s_3, and s_4).

Example: Invariants of $Z_4 \leq S_4$

$$Z_4 \cong \langle (1\,2\,3\,4) \rangle$$

Elementary symmetric polynomials:

$$\begin{aligned} s_1 &:= x_1 + x_2 + x_3 + x_4 \\ s_2 &:= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ s_3 &:= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ s_4 &:= x_1x_2x_3x_4 \end{aligned}$$

and additional invariants:

$$\begin{aligned} f_1 &:= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 \\ f_2 &:= x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2 \\ f_3 &:= x_1x_2^3 + x_2x_3^3 + x_3x_4^3 + x_4x_1^3 \end{aligned}$$

Relations:

$$f_1^3 = 2s_2f_1^2 + (4s_4 - s_1s_3 - s_2^2)f_1 + s_1s_2s_3 - s_1^2s_4 - s_3^2$$

$$f_2^2 = (s_1f_1 - 2s_3)f_2 - f_1^3 + (4s_2 - s_1^2)f_1^2 + (s_1^2s_2 + s_1s_3 - 4s_2^2)f_1 + 4s_1s_2s_3 - s_1^3s_3 - 5s_3^2$$

$$f_3^2 = p_1(s_1, s_2, s_3, s_4, f_1)f_3 + p_0(s_1, s_2, s_3, s_4, f_1)$$

Example: Invariants of $Z_4 \leq S_4$ (continued)

None of the invariants f_1, f_2, and f_3 is redundant:

	$(1\,3\,4\,2)$		$(2\,4)$		$(1\,4)(2\,3)$	
x_1	-1	α	-1	-1	3	6
x_2	α	$-2\alpha^2-4\alpha-1$	1	2	-2	1
x_3	1	-1	3	3	1	-2
x_4	$-2\alpha^2-4\alpha-1$	1	2	1	6	3
s_1	$-2\alpha^2-3\alpha-1$	$-2\alpha^2-3\alpha-1$	5	5	8	8
s_2	$2\alpha^2+3\alpha$	$2\alpha^2+3\alpha$	5	5	7	7
s_3	$2\alpha^2+3\alpha+1$	$2\alpha^2+3\alpha+1$	-5	-5	-36	-36
s_4	$-2\alpha^2-3\alpha-1$	$-2\alpha^2-3\alpha-1$	-6	-6	-36	-36
f_1	$\mathbf{0}$	$\mathbf{4\alpha^2+8\alpha+1}$	6	6	16	16
f_2	$-3\alpha^2-5\alpha-2$	$-3\alpha^2-5\alpha-2$	**22**	**18**	100	100
f_3	$3\alpha^2+5\alpha+1/2$	$3\alpha^2+5\alpha+1/2$	48	48	**352**	**592**

(where $\alpha^3+3\alpha^2+2\alpha+1/2=0$)

Invariants for "Generic States"

(see e. g. N. Linden, S. Popescu, and A. Sudbery, PRL 83, 243–247 (1999), quant-ph/9801076)

- express the state ρ in terms of a local basis:

$$\rho = \frac{1}{D} I \otimes \ldots \otimes I + \sum_{r=1}^{n} \alpha_{i_r}^{(r)} I \otimes \ldots \otimes T_{i_r}^{(r)} \otimes \ldots \otimes I + \ldots + R_{i_1 \ldots i_n} T_{i_1}^{(1)} \otimes \ldots \otimes T_{i_n}^{(n)}$$

- investigate the infinitesimal action of $SU(d_1) \otimes \ldots \otimes SU(d_n)$ on ρ
  $\Longrightarrow$ invariants are solutions of the PDE given by the resulting vector field
  (Cayley's omega-process[a])

- "generic states":
  maximal linear independent vector fields ($\hat{=}$ algebraically independent invariants)
  $\Longrightarrow$ e. g., invariants that depend only on $\alpha_i^{(r)}$ and the tensor R

- this does not apply to all states, e. g., for QECC $\alpha_i^{(r)} = 0$.

[a] see e. .g. B. Sturmfels, Algorithms in Invariant Theory, Springer, 1993

"Generic Invariants": Two Qubits

$$\rho = \frac{1}{4} I \otimes I + \sum_{j=x,y,z} \alpha_j^{(1)} \sigma_j \otimes I + \sum_{k=x,y,z} \alpha_k^{(2)} I \otimes \sigma_k + \sum_{j,k=x,y,z} \beta_{j,k} \sigma_j \otimes \sigma_k$$

Generic invariants (see, e. g., S. Lomonaco, "An Entangled Tale of Quantum Entanglement")

$Tr(\beta\beta^t)$	$Tr((\beta\beta^t)^2)$	$\det(\beta)$
$(\alpha^{(1)}, \alpha^{(1)})$	$(\alpha^{(1)}\beta, \alpha^{(1)}\beta)$	$(\alpha^{(1)}\beta\beta^t, \alpha^{(1)}\beta\beta^t)$
$\alpha^{(1)}\beta\alpha^{(2)}$	$\alpha^{(1)}\beta\beta^t\beta\alpha^{(2)}$	$\alpha^{(1)}(\beta\beta^t)^2\beta\alpha^{(2)}$

$\Longrightarrow$ for almost all states, these are algebraically independent invariants

additional invariant:

$$(\alpha^{(1)}, \alpha^{(1)}\beta\beta^t \times \alpha^{(1)}(\beta\beta^t)^2)$$

"to fix the signs"

Non-Generic States

Consider the states

$$\rho := \frac{1}{256}\begin{pmatrix} 66 & 0 & 32-4i & 1 \\ 0 & 62 & 3 & 32-4i \\ 32+4i & 3 & 66 & 0 \\ 1 & 32+4i & 0 & 62 \end{pmatrix} \quad \rho' := \frac{1}{256}\begin{pmatrix} 66 & 0 & 32+4i & 1 \\ 0 & 62 & 3 & 32+4i \\ 32-4i & 3 & 66 & 0 \\ 1 & 32-4i & 0 & 62 \end{pmatrix}$$

$$\rho = \frac{1}{4}I\otimes I + \frac{1}{8}\sigma_x\otimes I + \frac{1}{64}\sigma_y\otimes I + \frac{1}{128}I\otimes\sigma_z + \frac{1}{128}\sigma_x\otimes\sigma_x + \frac{1}{256}\sigma_y\otimes\sigma_y$$

$$\rho' = \frac{1}{4}I\otimes I + \frac{1}{8}\sigma_x\otimes I - \frac{1}{64}\sigma_y\otimes I + \frac{1}{128}I\otimes\sigma_z + \frac{1}{128}\sigma_x\otimes\sigma_x + \frac{1}{256}\sigma_y\otimes\sigma_y$$

$$\alpha^{(1)} = (\frac{1}{8}, \pm\frac{1}{64}, 0), \quad \alpha^{(2)} = (0, 0, \frac{1}{128})^t, \quad \beta := \frac{1}{256}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\Longrightarrow$ the values of the previous invariants are equal for ρ and ρ', but $\rho \ncong \rho'$

Invariant Tensors

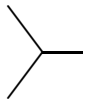
(Y. Makhlin, quant-ph/0002045 and private communication)

- use local basis for the density matrix:

$$\rho = \frac{1}{4} I + \sum_{i=x,y,z} s_i \sigma_i \otimes I + \sum_{j=x,y,z} p_j I \otimes \sigma_j + \sum_{i,j=x,y,z} \beta_{ij} \sigma_i \otimes \sigma_j$$

- $SU(2) \otimes SU(2)$ acts as $SO(3) \times SO(3)$ on the coefficient vectors s, p and the coefficient matrix β
- contract copies of the coefficient tensors with tensors that are invariant under $SO(3)$ resp. $SO(3) \times SO(3)$

δ_{ij} inner product

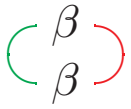
ϵ_{ijk} determinant 

- create all possible contractions modulo the relations of the tensors

for two qubits, there is only a finite number of such contractions

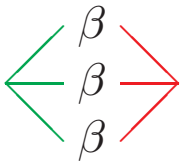
$\Longrightarrow$ complete set of invariants, resp. a set of generators for all invariants ("fundamental invariants")

Fundamental Invariants (I)

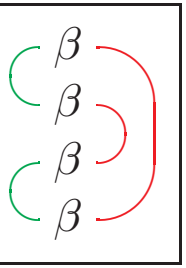
$\mathrm{Tr}(\beta\beta^t) =$ 

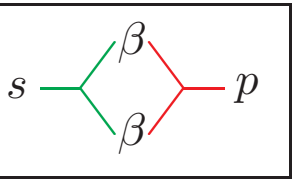
$s^t\, s = s$ — s

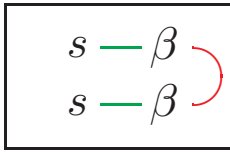
$p\, p^t = p$ — p

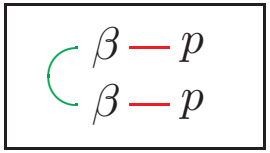
$\det\beta =$ 

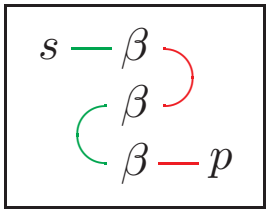
$s^t\, \beta\, p = s$ — β — p

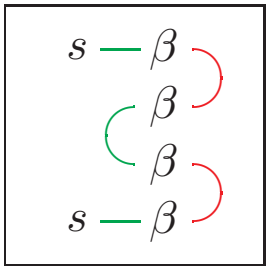


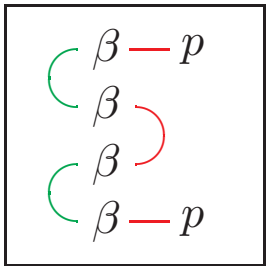


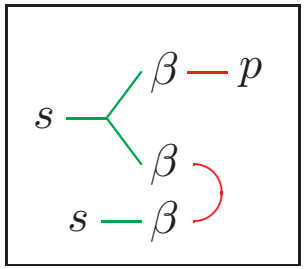


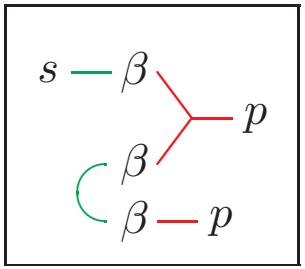




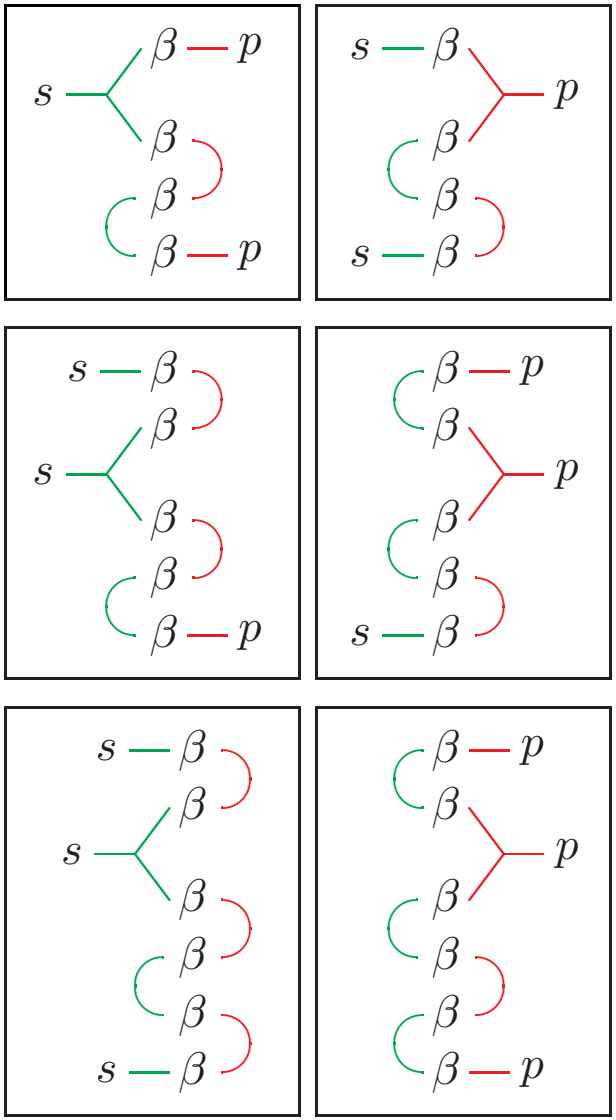








Fundamental Invariants (II)



Reynolds Operator

finite groups

$$\begin{aligned} R_G: \quad \mathbb{F}[\boldsymbol{x}] &\rightarrow \mathbb{F}[\boldsymbol{x}]^G \\ f(\boldsymbol{x}) &\mapsto \frac{1}{|G|}\sum_{g\in G} f(\boldsymbol{x})^g \end{aligned}$$

R_G is a linear projection operator

$\Rightarrow$ compute $R_G(\boldsymbol{m})$ for all monomials $\boldsymbol{m} \in \mathbb{F}[\boldsymbol{x}]$ of degree $d = 1, 2, \ldots$

compact groups

$$\begin{aligned} R_G: \quad \mathbb{F}[\boldsymbol{x}] &\rightarrow \mathbb{F}[\boldsymbol{x}]^G \\ f(\boldsymbol{x}) &\mapsto \int_{g\in G} f(\boldsymbol{x})^g d\mu_G(g) \end{aligned}$$

where $\mu_G(g)$ is the normalized Haar measure of G

Problem computing the integral is very difficult

Invariant Polynomials and Commuting Matrices (I)

Every homogeneous polynomial $f(X) \in \mathbb{F}[x_{11}, \ldots, x_{NN}]$ of degree k can be expressed as

$$f_F(X) := \mathrm{Tr}(F \cdot X^{\otimes k}) \quad \text{where } F \in \mathbb{F}^{kN \times kN}$$

(since $X^{\otimes k}$ contains all monomials of degree k).

Example ($N = 2$, $k = 2$):

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$

$$X^{\otimes 2} = \begin{pmatrix} x_{11}^2 & x_{11}x_{12} & x_{12}x_{11} & x_{12}^2 \\ x_{11}x_{21} & x_{11}x_{22} & x_{12}x_{21} & x_{12}x_{22} \\ x_{21}x_{11} & x_{21}x_{12} & x_{22}x_{11} & x_{22}x_{12} \\ x_{21}^2 & x_{21}x_{22} & x_{22}x_{21} & x_{22}^2 \end{pmatrix}$$

Invariant Polynomials and Commuting Matrices (II)

$$\begin{aligned} f_F(X)^g &= \mathrm{Tr}(F \cdot (g^{-1} \cdot X \cdot g)^{\otimes k}) \\ &= \mathrm{Tr}(F \cdot (g^{-1})^{\otimes k} \cdot X^{\otimes k} \cdot g^{\otimes k}) \\ &= \mathrm{Tr}(g^{\otimes k} \cdot F \cdot (g^{-1})^{\otimes k} \cdot X^{\otimes k}) \\ &= \mathrm{Tr}(F^{(g^{-1})^{\otimes k}} \cdot X^{\otimes k}) \end{aligned}$$

$$f_F(X)^g = f_F(X) \Longleftrightarrow f_F(X) = f_{F'}(X) \quad \text{and} \quad F' \cdot g^{\otimes k} = g^{\otimes k} \cdot F'$$

transformed question

Which matrices commute with each $g^{\otimes k}$ for $g \in G$?

R. Brauer (1937):

The algebra $\mathcal{A}_{n,k}$ of matrices that commute with each $U^{\otimes k}$ for $U \in U(n)$ is generated by a certain representation of S_k.

One Particle

- Hilbert space $\mathcal{H}$ of dimension n
- $G = U(n)$
- representation of S_k:
  S_k operates on a tensor product of k Hilbert spaces $\mathcal{H}_i$ of dimension n by permuting the spaces:
  $$T_{n,k}(\pi) \cdot (\mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_k) = \mathcal{H}_{\pi(1)} \otimes \ldots \otimes \mathcal{H}_{\pi(k)}$$
- "permuting k copies of $\mathcal{H}$"

N Particles

- Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_N$
- $G = U(n)^{\otimes N}$, $g = U_1 \otimes \ldots \otimes U_N$, $g^{\otimes k} = (U_1 \otimes \ldots \otimes U_N) \otimes \ldots \otimes (U_1 \otimes \ldots \otimes U_N)$
- N permutations $\pi_\nu \in S_k$
- representation of $(S_k)^N$:
  $\pi = (\pi_1, \ldots, \pi_N)$, π_ν permutes the copies of the ν^{th} particle:

$$T_{n,k}^{(N)}(\pi) \cdot \big((\mathcal{H}_{1,1} \otimes \ldots \otimes \mathcal{H}_{N,1}) \otimes \ldots \otimes (\mathcal{H}_{1,k} \otimes \ldots \otimes \mathcal{H}_{N,k})\big) =$$

$$(\mathcal{H}_{1,\pi_1(1)} \otimes \ldots \otimes \mathcal{H}_{N,\pi_N(1)}) \otimes \ldots \otimes (\mathcal{H}_{1,\pi_1(k)} \otimes \ldots \otimes \mathcal{H}_{N,\pi_N(k)})\big)$$

Computing Invariants

(see E. Rains, quant-ph/9704042[a]; Grassl et al. PRA 58, 1833-1839 (1998), quant-ph/9712040)

Computing the homogeneous polynomial invariants of degree k for an N particle system with density operator ρ:

for each N tuple $\pi = (\pi_1, \ldots, \pi_N)$ of permutations $\pi_\nu \in S_k$ compute

$$f_{\pi_1,\ldots,\pi_N}(\rho_{ij}) := \mathrm{Tr}\left(T^{(N)}_{n,k}(\pi) \cdot \rho^{\otimes k}\right)$$

- all homogeneous polynomial invariant of degree k
- in general, $(k!)^N$ invariants to compute
- not necessarily distinct
- not linearly independent
- it is sufficient to consider certain tuples of permutations

[a] IEEE Transactions on Information Theory, vol. 46, no. 1, pp. 54–59 (2000)

Molien Series

- Formal power series with non–negative integer coefficients
- Encodes the vector space dimension d_k of the homogeneous invariants of degree k:

$$M(z) := \sum_{k \geq 0} d_k z^k \in \mathbb{Z}[\![z]\!].$$

- A rational function (for finitely generated algebras)
- General formula (for linear operation)

$$M(z) = \int_{g \in G} \mathrm{d}\mu_G(g) \frac{1}{\det(id - z \cdot g)}$$

Problems:

1. Applies only to the case of linear operation
   $\Longrightarrow$ "linearize" the operation by conjugation using the adjoint representation
2. Integral is very difficult to compute

Pure States: Two Particles

Pure State

$|\psi\rangle = \sum_{i=1}^{d^2} x_i |b_i\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$

with a (global) orthonormal basis $|b_i\rangle$.

Schmidt decomposition

$$|\psi\rangle = \sum_{j=1}^{d} \alpha_j |b_j^{(1)}\rangle |b_j^{(2)}\rangle$$

with local orthonormal bases $|b_j^{(1)}\rangle$, and $|b_j^{(2)}\rangle$.

Invariants The (real) coefficients α_j are the local invariants.

Problem The invariants α_j are no polynomial function in the coefficients x_i, but α_j are eigenvalues of $\rho_i := \mathrm{Tr}_i(|\psi\rangle\langle\psi|)$

$\Longrightarrow$ Use the coeffiecients of the characteristic polynomial of ρ_i (elementary symmetric polynomials or power sums).

Example: Two Qubits

Pure State

$$|\psi\rangle = x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$$

Invariants

$$\begin{aligned}
\mathrm{Tr}(|\psi\rangle\langle\psi|) &= x_{00}\overline{x}_{00} + x_{01}\overline{x}_{01} + x_{10}\overline{x}_{10} + x_{11}\overline{x}_{11} \\
\mathrm{Tr}\left((\mathrm{Tr}_i\,|\psi\rangle\langle\psi|)^2\right) &= x_{00}^2\overline{x}_{00}^2 + x_{01}^2\overline{x}_{01}^2 + x_{10}^2\overline{x}_{10}^2 + x_{11}^2\overline{x}_{11}^2 \\
&\quad + 2x_{00}x_{01}\overline{x}_{00}\overline{x}_{01} + 2x_{00}x_{10}\overline{x}_{00}\overline{x}_{10} + 2x_{00}x_{11}\overline{x}_{01}\overline{x}_{10} \\
&\quad + 2x_{01}x_{10}\overline{x}_{00}\overline{x}_{11} + 2x_{01}x_{11}\overline{x}_{01}\overline{x}_{11} + 2x_{10}x_{11}\overline{x}_{10}\overline{x}_{11}
\end{aligned}$$

Problem

We have to introduce new variables which are the "complex conjugated variables".

Note

Algebraically, the roots i and $-i$ of $f(x) = x^2 + 1$ cannot be distinguished.

Generalized Molien Series

Bi-degree of polynomials f in variables x_i and $\overline{x}_i$:

$$(\deg_{x_1,\ldots,x_n} f,\ \deg_{\overline{x}_1,\ldots,\overline{x}_n} f)$$

F-Series:[a]

- Formal power series with non–negative integer coefficients
- Encodes the vector space dimension $d_{k,\ell}$ of the homogeneous invariants of bi-degree (k,ℓ):

$$F(z,\overline{z}) := \sum_{k,\ell\geq 0} d_{k,\ell}\, z^k\, \overline{z}^{\ell} \in \mathbb{Z}[\![z,\overline{z}]\!].$$

- General formula (for linear operation)

$$F(z,\overline{z}) = \int_G \mathrm{d}\mu_G(g) \frac{1}{\det(id - z\cdot g)} \frac{1}{\det(id - \overline{z}\cdot \overline{g})}$$

[a] Michael Forger, J. Math. Phys. 39, pp. 1107–1141 (1998)

Three Qubits: Ansatz F-Series of $SU(2)^{\otimes 3}$

$$F(\overline{z}, z) = \int_{U \in G} \mathrm{d}\mu_G(U) \frac{1}{\det(id - z \cdot U)} \frac{1}{\det(id - \overline{z} \cdot U^t)}$$

$$= \frac{1}{(2\pi i)^3} \oint_{\Gamma_v} \oint_{\Gamma_w} \oint_{\Gamma_x} \frac{(1-v^2)(1-w^2)(1-x^2)}{\prod_{a,b,c \in \{1,-1\}} (1 - z \cdot v^a w^b x^c)\,(1 - \overline{z} \cdot v^a w^b x^c)} \frac{\mathrm{d}v}{v} \frac{\mathrm{d}w}{w} \frac{\mathrm{d}x}{x}$$

$(G = SU(2)^{\otimes 3},\ U = U_1 \otimes U_2 \otimes U_3,\ \Gamma =$complex unit circle$)$

Computation of the integral using the theorem of residues

- symbolic computation of singularities and residues
- data type: factored rational functions implemented in MAGMA
  (Maple fails: "object too large")

Three Qubits: F- and M-Series of $SU(2)^{\otimes 3}$

$$F(z,\overline{z}) = \frac{z^5\overline{z}^5 + z^3\overline{z}^3 + z^2\overline{z}^2 + 1}{(1-z\overline{z})(1-z^4)(1-\overline{z}^4)(1-z^2\overline{z}^2)^2(1-z\overline{z}^3)(1-z^3\overline{z})}$$

$$\begin{aligned}
&= 1 + z\overline{z} + z^4 + z^3\overline{z} + 4z^2\overline{z}^2 + z\overline{z}^3 + \overline{z}^4 + z^5\overline{z} + z^4\overline{z}^2 + 5z^3\overline{z}^3 + z^2\overline{z}^4 + z\overline{z}^5 \\
&\quad + z^8 + z^7\overline{z} + 5z^6\overline{z}^2 + 5z^5\overline{z}^3 + 12z^4\overline{z}^4 + 5z^3\overline{z}^5 + 5z^2\overline{z}^6 + z\overline{z}^7 + \overline{z}^8 \\
&\quad + z^9\overline{z} + z^8\overline{z}^2 + 6z^7\overline{z}^3 + 6z^6\overline{z}^4 + 15z^5\overline{z}^5 + z\overline{z}^9 + z^2\overline{z}^8 + 6z^3\overline{z}^7 + 6z^4\overline{z}^6 \\
&\quad + z^{12} + z^{11}\overline{z} + 5z^{10}\overline{z}^2 + 6z^9\overline{z}^3 + 16z^8\overline{z}^4 + 16z^7\overline{z}^5 + 30z^6\overline{z}^6 \\
&\qquad + \overline{z}^{12} + z\overline{z}^{11} + 5z^2\overline{z}^{10} + 6z^3\overline{z}^9 + 16z^4\overline{z}^8 + 16z^5\overline{z}^7 \\
&\quad + \ldots
\end{aligned}$$

$$M(z) = \frac{z^{12}+1}{(1-z^2)(1-z^4)^3(1-z^6)(1-z^8)}$$

$$\begin{aligned}
&= 1 + z^2 + 4z^4 + 5z^6 + 12z^8 + 15z^{10} + 30z^{12} + 37z^{14} + 65z^{16} + 80z^{18} \\
&\quad + 128z^{20} + 156z^{22} + 234z^{24} + 282z^{26} + 402z^{28} + 480z^{30} + \ldots
\end{aligned}$$

Three Qubits: Invariant Ring of $SU(2)^{\otimes 3}$

Coefficient vector:

$$\boldsymbol{x} = \Big(\underbrace{x_{000}, x_{001}}_{00}, \underbrace{x_{010}, x_{011}}_{01}, \underbrace{x_{100}, x_{101}}_{10}, \underbrace{x_{110}, x_{111}}_{11} \Big)$$

Invariants of $I_4 \otimes SU(2)$:

brackets	$[i,j]$	$:=$	$x_{i0}x_{j1} - x_{i1}x_{j0}$
inner products	$\langle i,j \rangle$	$:=$	$x_{i0}\overline{x}_{j0} + x_{i1}\overline{x}_{j1}$

Invariants of $SU(2) \otimes SU(2) \otimes SU(2)$:

correspond to permutations (π_1, π_2, π_3):

$$f_{\pi_1,\pi_2,\pi_3} = \sum_{i,j,\ldots} x_{i_1,i_2,i_3} \overline{x}_{\pi_1(i_1),\pi_2(i_2),\pi_3(i_3)} \cdot x_{j_1,j_2,j_3} \overline{x}_{\pi_1(j_1),\pi_2(j_2),\pi_3(j_3)} \cdot \ldots$$

Three Qubits: Invariant Ring of $SU(2)^{\otimes 3}$

Generators:

	bi-degree	permutations (π_1, π_2, π_3), brackets, inner products	#terms
f_1	$(1,1)$	(id, id, id)	8
f_2	$(2,2)$	$((1,2),(1,2), id)$	36
f_3	$(2,2)$	$((1,2), id, (1,2))$	36
s_1	$(4,0)$	$[1,2]^2 - 2[0,1][2,3] - 2[0,2][1,3] + [0,3]^2$	12
$\overline{s_1}$	$(0,4)$	$\overline{[1,2]}^2 - 2\overline{[0,1]}\ \overline{[2,3]} - 2\overline{[0,2]}\ \overline{[1,3]} + \overline{[0,3]}^2$	12
s_2	$(3,1)$	$[3,0]\langle 0,0\rangle - [3,0]\langle 3,3\rangle + [3,1]\langle 0,1\rangle + [3,2]\langle 0,2\rangle$ $+2[3,2]\langle 1,3\rangle - 2[1,0]\langle 2,0\rangle - [1,0]\langle 3,1\rangle - [2,0]\langle 3,2\rangle$ $-[2,1]\langle 0,0\rangle - [2,1]\langle 1,1\rangle + [2,1]\langle 2,2\rangle + [2,1]\langle 3,3\rangle$	40
$\overline{s_2}$	$(1,3)$		40
f_4	$(2,2)$	$(id, (1,2), (1,2))$	36
f_5	$(3,3)$	$((1,2),(2,3),(1,3))$	176
$f_4 f_5$	$(5,5)$		3760

Three Qubits: Invariant Ring of $U(2)^{\otimes 3}$

Generators of the invariant ring:

	degree	permutations (π_1, π_2, π_3)	#terms
f_1	2	(id, id, id)	8
f_2	4	$((1,2), (1,2), id)$	36
f_3	4	$((1,2), id, (1,2))$	36
f_4	4	$(id, (1,2), (1,2))$	36
f_5	6	$((1,2), (2,3), (1,3))$	176
f_6	8	$s_1 \overline{s}_1$	144
f_7	12	$\overline{s}_1 s_2^2$	5988

$f_1, \ldots, f_6$ are algebraic independent. Relation for f_7:

$$f_7^2 + c_1(f_1, \ldots, f_6) f_7 + c_0(f_1, \ldots, f_6) \qquad \text{where } c_0, c_1 \in \mathbb{Q}[f_1, \ldots, f_6].$$

Four Qubits: Ansatz F-Series of $SU(2)^{\otimes 4}$

$$F(\overline{z},z)=\int_{U\in G}\mathrm{d}\mu_G(U)\frac{1}{\det(id-z\cdot U)}\frac{1}{\det(id-\overline{z}\cdot U^t)}$$

$$=\alpha\oint_{\Gamma_u}\oint_{\Gamma_v}\oint_{\Gamma_w}\oint_{\Gamma_x}\frac{(1-u^2)(1-v^2)(1-w^2)(1-x^2)}{\prod_{a,b,c,d\in\{1,-1\}}(1-z\cdot u^av^bw^cx^d)\,(1-\overline{z}\cdot u^av^bw^cx^d)}\frac{\mathrm{d}u}{u}\frac{\mathrm{d}v}{v}\frac{\mathrm{d}w}{w}\frac{\mathrm{d}x}{x}$$

$$=\big((z^{36}\overline{z}^{36}-z^{35}\overline{z}^{33}+2z^{34}\overline{z}^{34}+6z^{34}\overline{z}^{32}+9z^{34}\overline{z}^{30}+4z^{34}\overline{z}^{28}+3z^{34}\overline{z}^{26}-z^{33}\overline{z}^{35}+7z^{33}\overline{z}^{33}+$$
$$12z^{33}\overline{z}^{31}+\ldots+12z^3\overline{z}^5+7z^3\overline{z}^3-z^3\overline{z}+3z^2\overline{z}^{10}+4z^2\overline{z}^8+9z^2\overline{z}^6+6z^2\overline{z}^4+2z^2\overline{z}^2-z\overline{z}^3+1\big)\Big/$$
$$\big((1-\overline{z}^6)(1-\overline{z}^4)(1-\overline{z}^4)(1-\overline{z}^2)(1-z^6)(1-z^4)(1-z^4)(1-z^2)(1-z^3\overline{z}^3)(1-z^2\overline{z}^2)^4$$
$$(1-z\overline{z})(1-z^5\overline{z})(1-z^3\overline{z})^3(1-z^4\overline{z}^2)(1-\overline{z}^5z)(1-\overline{z}^3z)^3(1-\overline{z}^4z^2)\big)$$

$$=\ 1+z^2+z\overline{z}+\overline{z}^2+3z^4+3z^3\overline{z}+8z^2\overline{z}^2+3z\overline{z}^3+3\overline{z}^4+4z^6+6z^5\overline{z}+19z^4\overline{z}^2+20z^3\overline{z}^3+19z^2\overline{z}^4+6z\overline{z}^5$$
$$+4\overline{z}^6+7z^8+11z^7\overline{z}+47z^6\overline{z}^2+62z^5\overline{z}^3+98z^4\overline{z}^4+62z^3\overline{z}^5+47z^2\overline{z}^6+11z\overline{z}^7+7\overline{z}^8+9z^{10}+18z^9\overline{z}$$
$$+81z^8\overline{z}^2+150z^7\overline{z}^3+278z^6\overline{z}^4+293z^5\overline{z}^5+278z^4\overline{z}^6+150z^3\overline{z}^7+81z^2\overline{z}^8+18z\overline{z}^9+9\overline{z}^{10}+14z^{12}$$
$$+27z^{11}\overline{z}+143z^{10}\overline{z}^2+299z^9\overline{z}^3+669z^8\overline{z}^4+900z^7\overline{z}^5+1128z^6\overline{z}^6+900z^5\overline{z}^7+669z^4\overline{z}^8$$
$$+299z^3\overline{z}^9+143z^2\overline{z}^{10}+27z\overline{z}^{11}+14\overline{z}^{12}+\ldots$$

Four Qubits: Molien Series of $U(2)^{\otimes 4}$

$$
\begin{aligned}
M(z) = \big(&z^{76}+6z^{70}+46z^{68}+110z^{66}+344z^{64}+844z^{62}+2154z^{60}+4606z^{58}+9397z^{56}+16848z^{54}\\
&+28747z^{52}+44580z^{50}+65366z^{48}+88036z^{46}+111909z^{44}+131368z^{42}+145676z^{40}\\
&+149860z^{38}+145676z^{36}+131368z^{34}+111909z^{32}+88036z^{30}+65366z^{28}+44580z^{26}\\
&+28747z^{24}+16848z^{221}+9397z^{20}+4606z^{18}+2154z^{16}+844z^{14}+344z^{12}+110z^{10}+46z^{8}\\
&+6z^{6}+1\big) \Big/ \left(\left(1-z^{10}\right)\left(1-z^{8}\right)^{4}\left(1-z^{6}\right)^{6}\left(1-z^{4}\right)^{7}\left(1-z^{2}\right)\right)\\
= \;& 1+z^2+8z^4+20z^6+98z^8+293z^{10}+1\,128z^{12}+3\,409z^{14}+10\,846z^{16}+30\,480z^{18}\\
&+84\,652z^{20}+217\,677z^{22}+544\,312z^{24}+1\,289\,225z^{26}+2\,961\,626z^{28}+6\,528\,284z^{30}\\
&+13\,980\,717z^{32}+28\,963\,980z^{34}+58\,464\,510z^{36}+114\,806\,429z^{38}+\ldots
\end{aligned}
$$

intermediate results:

1 invariant of degree	2
7 invariants of degree	4
12 invariants of degree	6
50 invariants of degree	8
39 invariants of degree	10

these 109 invariants generate a (sub)ring with series
$1+z^2+8z^4+20z^6+98z^8+221z^{10}+\ldots$

$\Longrightarrow$ even more invariants are required to generate the whole invariant ring

"Homework"

Given: pure states $|\psi\rangle, |\phi\rangle \in (\mathbb{C}^2)^{\otimes 4}$ of four qubits such that

$$\text{for all } 1 \leq i < j \leq 4\text{: } \mathrm{Tr}_{i,j}(|\psi\rangle\langle\psi|) \cong \mathrm{Tr}_{i,j}(|\phi\rangle\langle\phi|), \qquad (1)$$

i. e., all reduced two-party density matrices are locally equivalent

Problem: Are the states $|\psi\rangle$ and $|\phi\rangle$ locally equivalent?

Related Work:

- N. Linden, and W. K. Wootters, "High order correlations of generic pure states of finite-dimensional quantum systems are determined by lower order correlations", quant-ph/0208093
- N. Linden, S. Popescu, and W. K. Wootters, "The power of reduced quantum states", quant-ph/0207109

but: these results hold only for generic states

$\Longrightarrow$ Find states $|\psi\rangle$ and $|\phi\rangle$ for which (1) holds, but the states are not locally equivalent, or proof that such states do not exist.

Some Open Problems

- Find a complete set of polynomial invariants for many particles and arbitrary dimension (e. g. using relations for tensors of higher rank).
- Investigate the structure of those invariant rings, e. g. via the Molien series.
- How many invariants are needed to separate the orbits in general?

  Y. Makhlin has shown that a proper subset of the invariants of two qubits is sufficient to separate the orbits under local operations.
- Combine polynomial invariants with semi-algebraic conditions (e. g. a density matrix has non-negative eigenvalues)
- Find a "physical" interpretation of the invariants.
- Find alternative characterizations, e. g.,
  - using the spectral decomposition of a state
  - normal forms for states
  - using representatives for each orbit