Perimeter Institute Quantum Discussions

Perimeter Institute for Theoretical Physics

Waterloo, ON, Canada

Algebraic Characterization of Entanglement Classes

Markus Grassl

Markus.Grassl@mpl.mpg.de

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
NATURWISSENSCHAFTLICHE FAKULTÄT

MAX PLANCK INSTITUTE for the science of light

September 19, 2014

Overview

- The main tool: polynomial invariants
- Computing polynomial invariants
  - Reynolds operator
  - commuting matrices
  - tensor contractions
- Hilbert-Poincaré series/Molien series
- Derksen's degree bound
- SAGBI bases
- more examples

Prelude: Polynomial Invariants

A matrix group G acts on multivariate polynomials via linear transformation of the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$: $f(\boldsymbol{x}) \mapsto f(\boldsymbol{x})^g = f(\boldsymbol{x} \cdot g)$.

properties of the invariant ring
$\mathbb{K}[\boldsymbol{x}]^G := \{f(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] | \forall g \in G\colon f(\boldsymbol{x})^g = f(\boldsymbol{x})\}$

- 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 $\mathbb{K}[\boldsymbol{x}]^G$ is finitely generated
- some invariants are algebraically independent (primary invariants)
- the other invariants obey some polynomial relations

Main Problem

Characterize the non-local properties of quantum states & systems.

Various approaches

- entanglement measures/monotones:
  (real) functions on the state space, *e. g.* distance to product/separable states

- local equivalence:
  Given two quantum states

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

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

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

[a] We do not consider SLOCC here.

Our Approach

Consider the polynomial invariants of the groups $SU(d)^n$ or $U(d)^n$ acting on pure or mixed quantum states.

This gives a *complete* description:

Theorem:
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)

- pure states: identify $\mathbb{C}^m$ and $\mathbb{R}^{2m}$
- mixed states: Hermitian matrices form a real vector space

but: incomplete for SLOCC (related to $SL(d)^n$)

Entanglement "Coordinates"

Let $f_1, \ldots, f_m$ be a generating set for all polynomial invariants. the first μ being an independent set of maximal size.

entanglement "coordinates":

$$|\psi\rangle \mapsto \big(\underbrace{f_1(|\psi\rangle), \ldots, f_\mu(|\psi\rangle)}_{\text{algebraic independent}}, \underbrace{f_{\mu+1}(|\psi\rangle), \ldots, f_m(|\psi\rangle)}_{\text{finitely many subclasses}}\big) \in \mathbb{C}^m$$

states in the same entanglement class have the same entanglement coordinates

Reynolds Operator

finite groups

$$\begin{array}{rcl} R_G\colon \quad \mathbb{K}[\boldsymbol{x}] & \to & \mathbb{K}[\boldsymbol{x}]^G \\ f(\boldsymbol{x}) & \mapsto & \displaystyle\frac{1}{|G|}\sum_{g\in G} f(\boldsymbol{x})^g \end{array}$$

R_G is a linear projection operator

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

compact groups

$$\begin{array}{rcl} R_G\colon \quad \mathbb{K}[\boldsymbol{x}] & \to & \mathbb{K}[\boldsymbol{x}]^G \\ f(\boldsymbol{x}) & \mapsto & \displaystyle\int_{g\in G} f(\boldsymbol{x})^g \mathrm{d}\mu_G(g) \end{array}$$

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

Problem: computing the integral is very difficult

Invariant Polynomials and Commuting Matrices

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

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

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

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

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

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

Invariant Polynomials and Commuting Matrices

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

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

transformed question

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

R. Brauer (1937):

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

Computing Invariants

(see E. Rains, quant-ph/9704042[a]; Grassl et al., quant-ph/9712040[b])

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

$$f_{\pi_1,\ldots,\pi_n}(\rho_{ij}) := \operatorname{tr}\left(T_{d,k}^{(n)}(\pi) \cdot \rho^{\otimes k}\right)$$

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

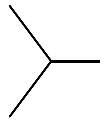
[a] E. Rains, IEEE Transactions on Information Theory, vol. 46, no. 1, pp. 54–59 (2000)
[b] M. Grassl, M. Roetteler & Th. Beth, Physical Review A 58, 1833–1839 (1998)

Invariant Tensors

- use local basis for the 4×4 two-qubit density matrix:

$$\rho = \frac{1}{4} I + \sum_{\ell = x,y,z} s_\ell (\sigma_\ell \otimes I) + \sum_{r = x,y,z} p_r (I \otimes \sigma_r) + \sum_{\ell, r = x,y,z} \beta_{\ell r} (\sigma_\ell \otimes \sigma_r)$$

- $SU(2) \otimes SU(2)$ 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. $SO(3) \times SO(3)$

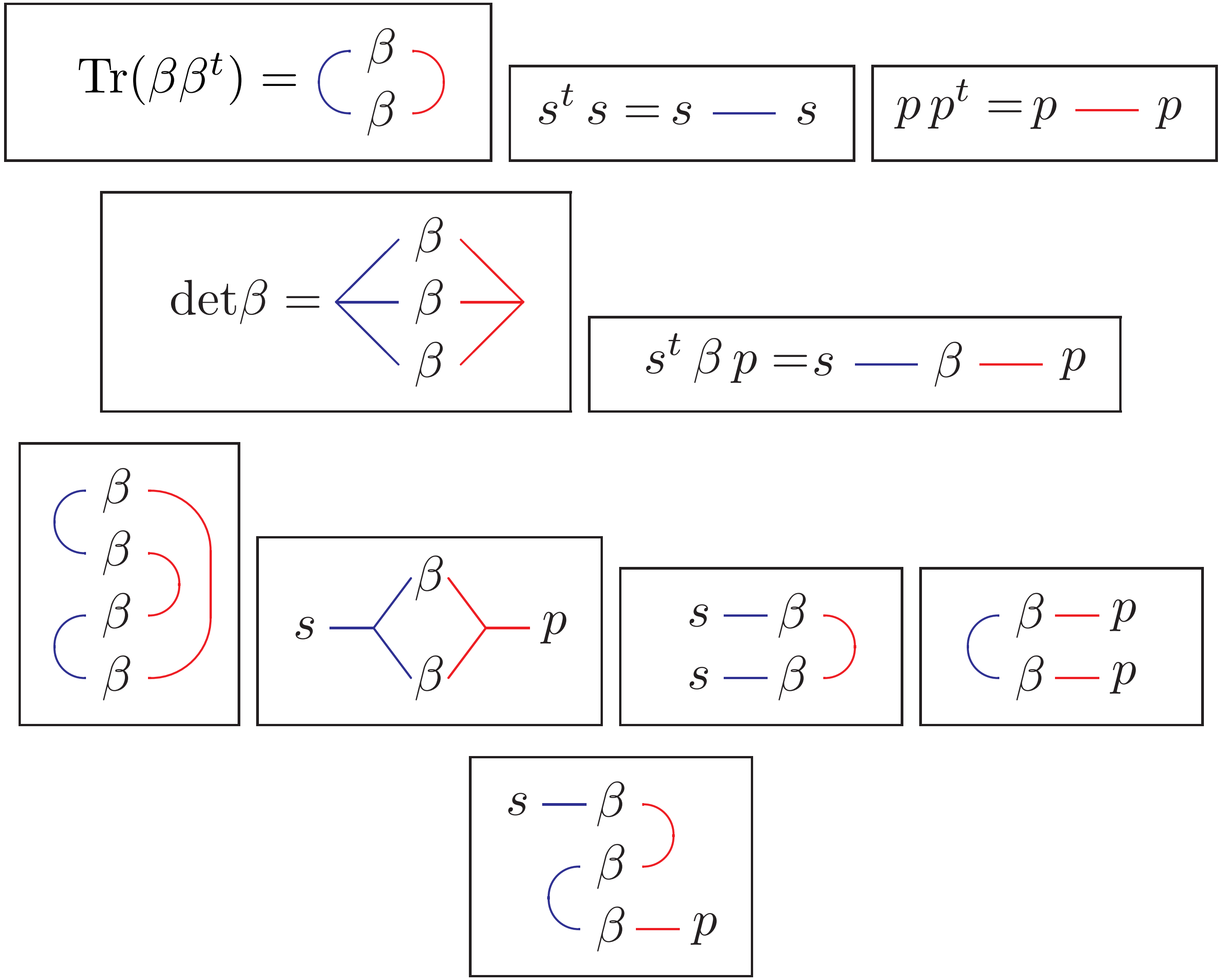
δ_{ij}	inner product	
ϵ_{ijk}	determinant	

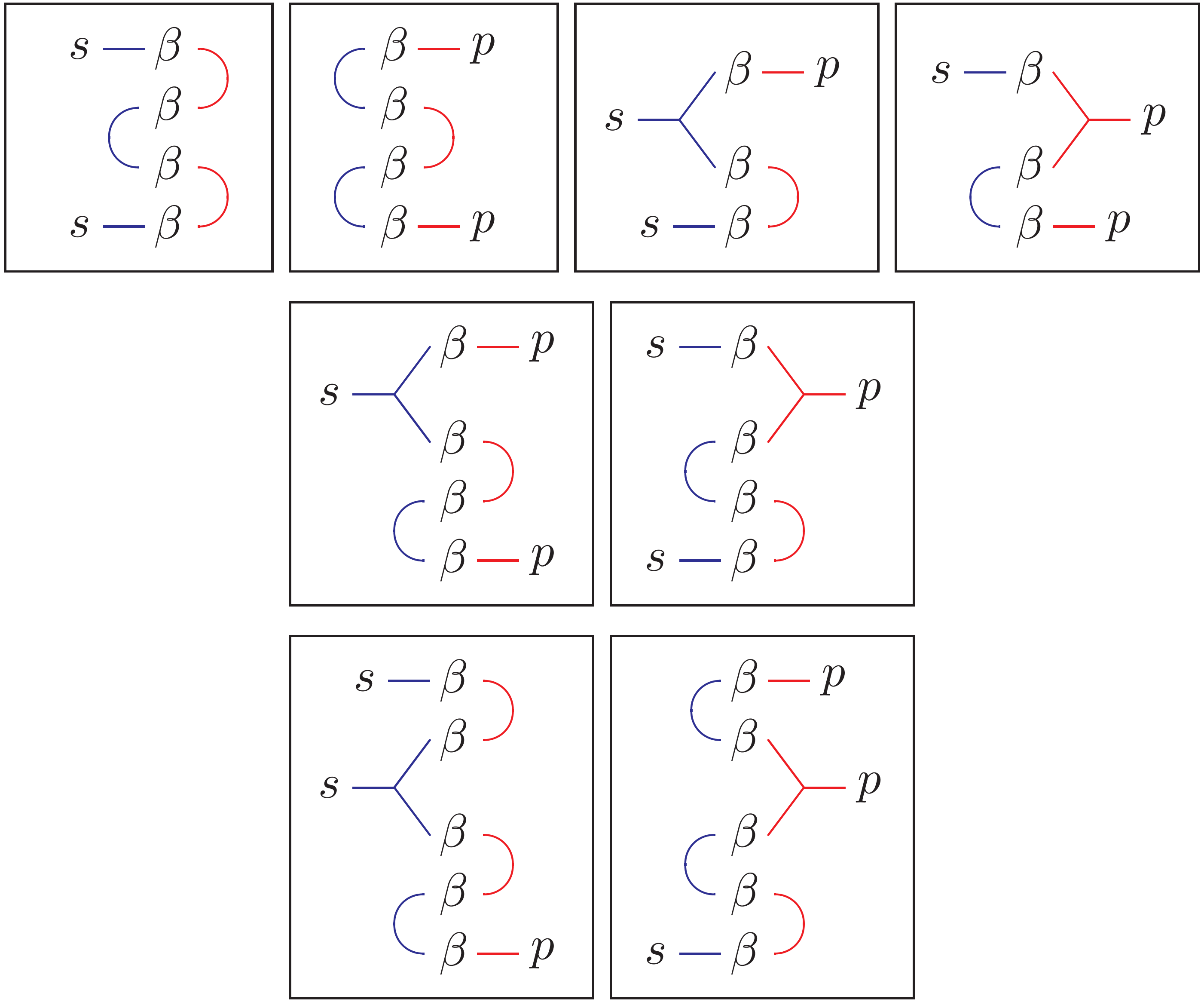
- create all possible contractions modulo the relations of the tensors

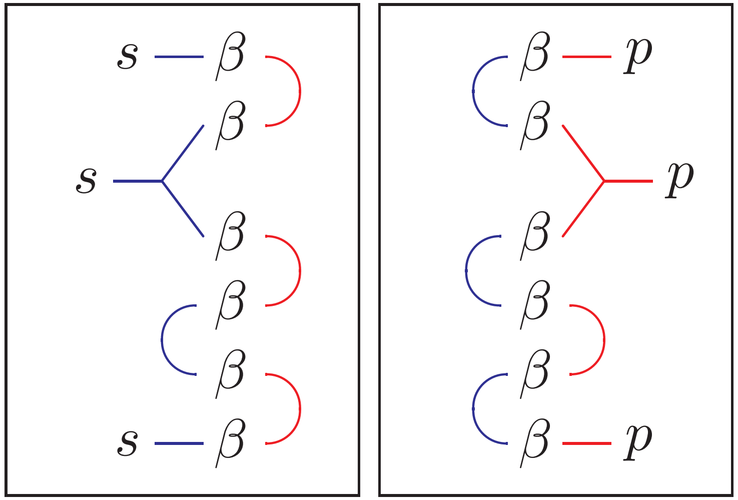
for two qubits, there is only a finite number of such contractions

$\Longrightarrow$ complete set of invariants, resp. a set of generators for all invariants

Fundamental Invariants (I)







References

Makhlin, Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations, Quantum Info. Proc. 1, 243–252, (2000).

Grassl, Entanglement and Invariant Theory, Quantum Computation and Information Seminar, UC Berkeley, 19.11.2002.

King, Welsh & Jarvis, The mixed two-qubit system and the structure of its ring of local invariants, J. Phys. A. 40, 10083–10108 (2007).

Hilbert-Poincaré/Molien Series

- encodes the vector space dimension d_k of the homogeneous invariants of degree k as a formal power series with non–negative integer coefficients:

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

- a rational function (for finitely generated algebras)
- general formula (for linear operation)

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

1. applies only to the case of linear operation
   $\Longrightarrow$ "linearize" the operation by conjugation via the adjoint representation
2. integral is very difficult to compute

Pure State of Two Qubits

pure state

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

Invariants

$$\mathrm{tr}(|\psi\rangle\langle\psi|) = x_{00}\overline{x}_{00} + x_{01}\overline{x}_{01} + x_{10}\overline{x}_{10} + x_{11}\overline{x}_{11}$$

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

Remark

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

Multivariate Hilbert Series

- operation on polynomials $f(\boldsymbol{x}, \overline{\boldsymbol{x}})$ in variables x_i and $\overline{x}_i$ with the representation $g \oplus \overline{g}$
- bi-degree

$$(\deg_{x_1,\ldots,x_m} f,\ \deg_{\overline{x}_1,\ldots,\overline{x}_m} f)$$

- invariant ring admits bi-graduation with Hilbert series

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

- general formula (for linear operation)

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

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

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

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

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

- uses Weyl's integral formula and the residue theorem
- symbolic computation of singularities and residues
- data type: factored rational functions implemented in MAGMA

Three Pure Qubits: Series for $SU(2)^{\otimes 3}$ and $U(2)^{\otimes 3}$

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

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

$$\begin{aligned}
M_U(z) &= \frac{z^{12}+1}{(1-z^2)(1-z^4)^3(1-z^6)(1-z^8)} \\
&= 1 + z^2 + 4z^4 + 5z^6 + 12z^8 + 15z^{10} + 30z^{12} + 37z^{14} + 65z^{16} + 80z^{18} \\
&\quad + 128z^{20} + 156z^{22} + 234z^{24} + 282z^{26} + 402z^{28} + 480z^{30} + \ldots
\end{aligned}$$

Three Pure 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 Pure 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,. . . ,f_6 are algebraic independent; relation for f_7:

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

completeness can be shown using the fact that there is only one algebraic relation

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

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

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

Four Pure Qubits: Hilbert Series of $SU(2)^{\otimes 4}$

$$
\begin{aligned}
M_{SU}(z,\overline{z}) = \; & (z^{36}\overline{z}^{36} - z^{35}\overline{z}^{33} + 2z^{34}\overline{z}^{34} + 6z^{34}\overline{z}^{32} + 9z^{34}\overline{z}^{30} + 4z^{34}\overline{z}^{28} + \\
& 3z^{34}\overline{z}^{26} - z^{33}\overline{z}^{35} + 7z^{33}\overline{z}^{33} + 12z^{33}\overline{z}^{31} + \ldots + 12z^{3}\overline{z}^{5} + 7z^{3}\overline{z}^{3} - \\
& z^{3}\overline{z} + 3z^{2}\overline{z}^{10} + 4z^{2}\overline{z}^{8} + 9z^{2}\overline{z}^{6} + 6z^{2}\overline{z}^{4} + 2z^{2}\overline{z}^{2} - z\overline{z}^{3} + 1) \Big/ \\
& ((1-\overline{z}^{6})(1-\overline{z}^{4})(1-\overline{z}^{4})(1-\overline{z}^{2})(1-z^{6})(1-z^{4})(1-z^{4})(1-z^{2}) \\
& (1-z^{3}\overline{z}^{3})(1-z^{2}\overline{z}^{2})^{4}(1-z\overline{z})(1-z^{5}\overline{z})(1-z^{3}\overline{z})^{3}(1-z^{4}\overline{z}^{2}) \\
& (1-\overline{z}^{5}z)(1-\overline{z}^{3}z)^{3}(1-\overline{z}^{4}z^{2})) \\
= \; & 1+z^{2}+z\overline{z}+\overline{z}^{2}+3z^{4}+3z^{3}\overline{z}+8z^{2}\overline{z}^{2}+3z\overline{z}^{3}+3\overline{z}^{4}+4z^{6}+6z^{5}\overline{z}+19z^{4}\overline{z}^{2} \\
& +20z^{3}\overline{z}^{3}+19z^{2}\overline{z}^{4}+6z\overline{z}^{5}+4\overline{z}^{6}+7z^{8}+11z^{7}\overline{z}+47z^{6}\overline{z}^{2}+62z^{5}\overline{z}^{3}+98z^{4}\overline{z}^{4} \\
& +62z^{3}\overline{z}^{5}+47z^{2}\overline{z}^{6}+11z\overline{z}^{7}+7\overline{z}^{8}+9z^{10}+18z^{9}\overline{z}+81z^{8}\overline{z}^{2}+150z^{7}\overline{z}^{3} \\
& +278z^{6}\overline{z}^{4}+293z^{5}\overline{z}^{5}+278z^{4}\overline{z}^{6}+150z^{3}\overline{z}^{7}+81z^{2}\overline{z}^{8}+18z\overline{z}^{9}+9\overline{z}^{10} \\
& +14z^{12}+27z^{11}\overline{z}+143z^{10}\overline{z}^{2}+299z^{9}\overline{z}^{3}+669z^{8}\overline{z}^{4}+900z^{7}\overline{z}^{5}+1128z^{6}\overline{z}^{6} \\
& +900z^{5}\overline{z}^{7}+669z^{4}\overline{z}^{8}+299z^{3}\overline{z}^{9}+143z^{2}\overline{z}^{10}+27z\overline{z}^{11}+14\overline{z}^{12} + \ldots
\end{aligned}
$$

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

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

later independently computed by:

Nolan R. Wallach, The Hilbert Series of Measures of Entanglement for 4 Qubits, Acta Applicandae Mathematicae 86:203–220 (2005)

Four Pure Qubits: Invariants of $U(2)^{\otimes 4}$

$$
\begin{aligned}
M_U(z) = \; & 1 + z^2 + 8\,z^4 + 20\,z^6 + 98\,z^8 + 293\,z^{10} + 1\,128\,z^{12} + 3\,409\,z^{14} \\
& + 10\,846\,z^{16} + 30\,480\,z^{18} + 84\,652\,z^{20} + 217\,677\,z^{22} + 544\,312\,z^{24} \\
& + 1\,289\,225\,z^{26} + 2\,961\,626\,z^{28} + 6\,528\,284\,z^{30} + 13\,980\,717\,z^{32} \\
& + 28\,963\,980\,z^{34} + 58\,464\,510\,z^{36} + 114\,806\,429\,z^{38} + \ldots
\end{aligned}
$$

intermediate results:

1 invariant of degree 2 7 invariants of degree 4 12 invariants of degree 6 50 invariants of degree 8 111 invariants of degree 10	these 181 invariants generate a (sub)ring with series $1 + z^2 + 8z^4 + 20z^6 + 98z^8 + 293z^{10} + 801z^{12} + \ldots$

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

Derksen's Degree Bound

[H. Derksen, Proc. Am. Math. Soc., 129(4):955–963 (2000)]

Let G be a linearly reductive algebraic group over $\mathbb{K}$, $\mathbb{K}$ algebraically closed, $\mathrm{char}(\mathbb{K}) = 0$.

- G is defined via polynomials $h_i \in \mathbb{K}[Z_1, \ldots, Z_t]$
- representation $\rho\colon G \to GL(V)$ defined via polynomials $a_{i,j} \in \mathbb{K}[Z_1, \ldots, Z_t]$
- $H := \max_i \deg(h_i)$, $A := \max_{i,j} \deg(a_{i,j})$, and $m := \dim(G)$

If ρ has finite kernel, then the degree of primary invariants is bounded by

$$\sigma(V) \leq H^{t-m} A^m.$$

The degree of generators for the invariant ring is bounded by

$$\beta(V) \leq \max\{2, \frac{3}{8} \dim \mathcal{O}(V)^G \sigma^2(V)\}.$$

Derksen's Degree Bound: $SU(2)$

Consider the group $G = SU(2)^{\otimes n}$ acting via conjugation on $2^n \times 2^n$ matrices.

- $\dim SU(2) = 3$, defined via polynomials of degree 2 in 4 variables
  $\Longrightarrow m = 3n$, $H = 2$, $t = 4n$
- action is given by $M \mapsto (g_1 \otimes \ldots \otimes g_n)M(g_1 \otimes \ldots \otimes g_n)^{-1}$
  $\Longrightarrow A = 2n$

degree bound $\sigma(V)$ for the primary invariants:

$$\sigma(V) \leq H^{t-m}A^m = 2^{4n-3n}(2n)^{3n} = 2^{4n}n^{3n}$$

already for $n = 2$, we get $\sigma(V) \leq 2^{14} = 16384$

Relation Ideal

Problem:

Given some invariants $f_1, \ldots, f_m$, do they generate the full invariant ring?

evaluation homorphism: $\mathbb{K}[y_1, \ldots, y_m] \to \mathbb{K}[x_1, \ldots, x_n]$

$$g(y_1, \ldots, y_m) \mapsto g(f_1, \ldots, f_m)$$

relation ideal:

$$\operatorname{Rel}(f_1, \ldots, f_m) = \{g(y_1, \ldots, y_m) \colon g(f_1, \ldots, f_m) = 0\} \trianglelefteq \mathbb{K}[y_1, \ldots, y_m]$$

$$\mathcal{A} = \langle f_1, \ldots, f_m \rangle \cong \mathbb{K}[y_1, \ldots, y_m] / \operatorname{Rel}(f_1, \ldots, f_m)$$

Hilbert series: $\operatorname{Hilb}(\mathcal{A}) = \operatorname{Hilb}(\operatorname{Rel})$

computed (in principle) as

$$\operatorname{Rel}(f_1, \ldots, f_m) = \langle f_1 - y_1, \ldots, f_m - y_m \rangle \cap \mathbb{K}[y_1, \ldots, y_m]$$

SAGBI Bases

Subalgebra **A**nalogue to **G**röbner **B**asis for **I**deals[a]

- basis $B = \{g_1, \ldots, g_\ell\}$ of a subalgebra $\mathcal{A} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$
- depends on a term ordering $>$ for polynomials, *e. g.*, lexicographic ordering $x_1 > x_2 > \cdots > x_n$
- the semigroup $\mathrm{LM}(\mathcal{A})$ of leading monomials of $\mathcal{A}$ is generated by $\mathrm{LM}(B)$, *i. e.* $\mathrm{LM}(\mathcal{A}) = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_\ell) \rangle$
- allows membership test for $\mathcal{A}$ via top reduction:

$$h \xrightarrow{B} h - c g_{i_1}^{e_1} \cdots g_{i_k}^{e_k} \quad \text{if } \mathrm{LT}(h) = c\,\mathrm{LT}(g_{i_1})^{e_1} \cdots \mathrm{LT}(g_{i_k})^{e_k}$$

- need not be finite, even if $\mathcal{A}$ is finitely generated

[a] Kapur & Madlener 1989, Robbiano & Sweedler, 1990

Sturmfels' Conjecture

Conjecture: The invariant ring of a connected reductive affine algebraic group has a finite SAGBI basis with respect to some term order.

(see M. Stillman & H. Tsai, Using SAGBI bases to compute invariants, J. Pure and Appl. Algebra 139:285–302 (1999))

Bernd Sturmfels, email on 5 September 2006:

> *I did indeed conjecture, some time ago, that for a connected reductive group over C, the ring of invariants has a finite SAGBI basis. However, I don't [think] this conjecture ever made it into writing. Also, it was based mainly on "wishful thinking." To the best of my knowledge, it's still open.*

Using SAGBI Bases

assume $B = \{g_1, \ldots, g_\ell\}$ is a SAGBI basis of the polynomial algebra $\mathcal{A}$

all relevant information is given by the leading monomials

- $\mathrm{Hilb}(\mathcal{A}) = \mathrm{Hilb}(\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_\ell) \rangle)$
- the Hilbert series can be computed from the ideal

$$\mathrm{Rel}(\mathrm{LM}(B)) = \langle \mathrm{LM}(g_1) - t_1, \ldots, \mathrm{LM}(g_\ell) - t_\ell \rangle \cap \mathbb{K}[t_1, \ldots, t_\ell]$$

- if B has been computed only up to degree d, we can still compare the Hilbert series

$\Longrightarrow$ direct proof of completeness for two-qubit mixed state < 1 min

$\Longrightarrow$ proof of completeness for $SU(2)^{\otimes 3}$
("private communication" in Luque, Thibon & Toumazet (2007))

Three-Qubit Systems

(joint work with Robert Zeier, work in progress)

- action of $U(2)^{\otimes 3}$ on density matrices ρ (or Hamiltonians) via conjugation
- adjoint representation of $SU(2)$ decomposes as $1 \oplus 3$
  $\Longrightarrow (1 \oplus 3)^3 = 1 \oplus (3 \times 3) \oplus (3 \times 3^2) \oplus 3^3$
- corresponds to the action on

$$
\begin{gathered}
I_2 \otimes I_2 \otimes I_2 \\
\oplus \big(\mathfrak{su}(2) \otimes I_2 \otimes I_2\big) \oplus \big(I_2 \otimes \mathfrak{su}(2) \otimes I_2\big) \oplus \big(I_2 \otimes I_2 \otimes \mathfrak{su}(2)\big) \\
\oplus \big(\mathfrak{su}(2) \otimes \mathfrak{su}(2) \otimes I_2\big) \oplus \big(\mathfrak{su}(2) \otimes I_2 \otimes \mathfrak{su}(2)\big) \oplus \big(I_2 \otimes \mathfrak{su}(2) \otimes \mathfrak{su}(2)\big) \\
\oplus \big(\mathfrak{su}(2) \otimes \mathfrak{su}(2) \otimes \mathfrak{su}(2)\big)
\end{gathered}
$$

- invariant ring (excluding the trivial rep.) admits 7-fold grading
- Hilbert series $M(z_1, z_2, z_3,\ z_{12}, z_{13}, z_{23},\ z_{123})$
- consider only some of the irreducible components

Three-Qubit Systems: Partial Results

univariate Hilbert series

$$
\begin{aligned}
M(z) &= (z^{206} + \ldots + 1)/(1 - \ldots - z^{270})\\
&= 1 + z + 8\,z^2 + 24\,z^3 + 148\,z^4 + 649\,z^5 + 3.576\,z^6 + 17.206\,z^7\\
&\quad + 84.320\,z^8 + 386.599\,z^9 + 1.720.880\,z^{10} + 7.302.550\,z^{11} + 29.864.124\,z^{12}\\
&\quad + 117.329.840\,z^{13} + 444.769.448\,z^{14} + 1.627.560.935\,z^{15} + \ldots
\end{aligned}
$$

- in 2009: computed up to degree 8000 in about 4.5 days via two-fold integration and (Laurent) series expansion using `LazySeries` in MAGMA, using 15 GB
- in 2014: verified by direct integration using adapted residue computation in about 2.5 days using 27 GB

Three-Qubit System: Linear Chain $A \overset{\alpha}{\text{---}} B \overset{\beta}{\text{---}} C$

action on two irreducible components of dimension 9

- Hilbert series

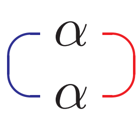
$$
\begin{aligned}
M_{9\oplus 9}(z) &= \frac{1+z^8+z^{16}}{(1-z^2)^2(1-z^3)^2(1-z^4)^3(1-z^6)^2}\\
&= 1+2\,z^2+2\,z^3+6\,z^4+4\,z^5+15\,z^6+12\,z^7+31\,z^8+28\,z^9\\
&\quad +62\,z^{10}+58\,z^{11}+120\,z^{12}+112\,z^{13}+213\,z^{14}+212\,z^{15}\\
&\quad +370\,z^{16}+368\,z^{17}+622\,z^{18}+628\,z^{19}+1006\,z^{20}+\ldots
\end{aligned}
$$

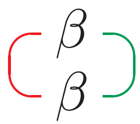
- generated by 9 primary invariants and 1 additional invariant
- completeness follows from the fact that there is only one additional invariant

Three-Qubit System: Linear Chain $A \overset{\alpha}{\text{———}} B \overset{\beta}{\text{———}} C$

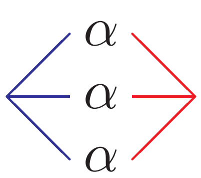
$$H = \sum_{i,j} \alpha_{i,j} \left(\sigma_i^A \otimes \sigma_j^B\right) + \sum_{j,k} \beta_{j,k} \left(\sigma_j^B \otimes \sigma_k^C\right)$$

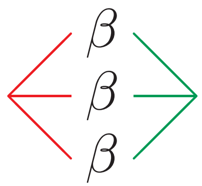
degree 2:

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

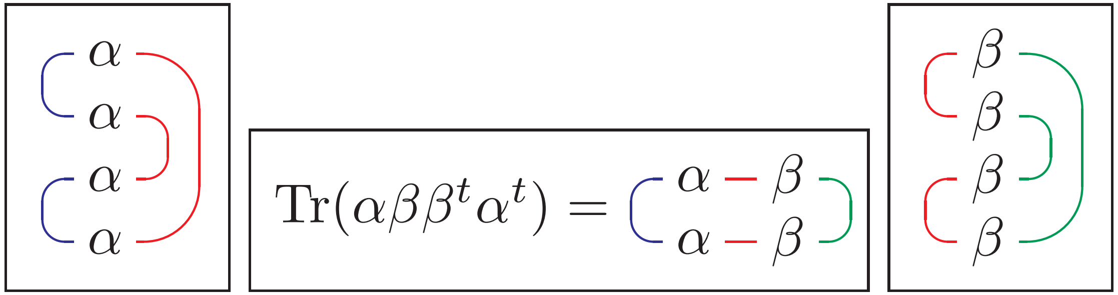
$\mathrm{Tr}(\beta\beta^t) =$ 

degree 3:

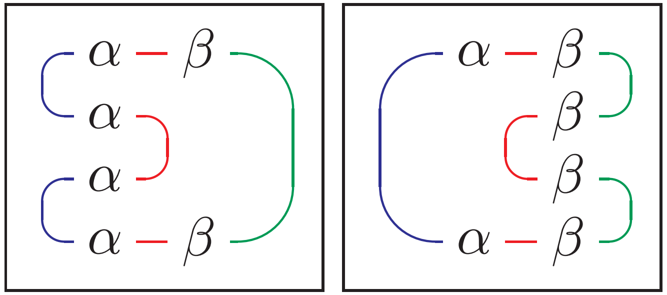
$\det\alpha =$ 

$\det\beta =$ 

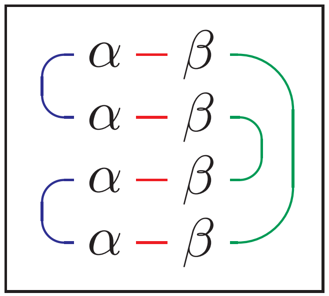
degree 4:



degree 6:



degree 8:



Three Qubits: All Two-body Interactions

action on the three irreducible components of dimension 9

$$M_{3\times 9}(z) = \big(z^{36} - z^{35} - z^{34} + z^{33} + 4\,z^{32} + 6\,z^{30} - 2\,z^{29} + 12\,z^{28} + 12\,z^{27} + 33\,z^{26}$$
$$+ 28\,z^{25} + 69\,z^{24} + 45\,z^{23} + 82\,z^{22} + 73\,z^{21} + 116\,z^{20} + 86\,z^{19} + 134\,z^{18}$$
$$+ 86\,z^{17} + 116\,z^{16} + 73\,z^{15} + 82\,z^{14} + 45\,z^{13} + 69\,z^{12} + 28\,z^{11} + 33\,z^{10}$$
$$+ 12\,z^{9} + 12\,z^{8} - 2\,z^{7} + 6\,z^{6} + 4\,z^{4} + z^{3} - z^{2} - z + 1\big)/$$
$$\big((z-1)^{18}(z+1)^{11}(z^2 - z + 1)^2(z^2+1)^5(z^2+z+1)^6(z^4+z^3+z^2+z+1)^2\big)$$
$$= 1 + 3\,z^2 + 4\,z^3 + 15\,z^4 + 18\,z^5 + 63\,z^6 + 90\,z^7 + 240\,z^8 + 386\,z^9 + 882\,z^{10}$$
$$+ 1.479\,z^{11} + 3.093\,z^{12} + 5.247\,z^{13} + 10.179\,z^{14} + 17.299\,z^{15} + 31.695\,z^{16}$$
$$+ 53.133\,z^{17} + 93.143\,z^{18} + 153.354\,z^{19} + 258.852\,z^{20} + \ldots$$

- computed 178 invariants with max. degree 12
- verified up to degree 20 using triple-grading, max. dimension 6.281

Three Qubits: Three-body Interactions

action on the irreducible component of dimension 27

$$
\begin{aligned}
M_{27}(z) = \big(&z^{79} - z^{75} + 5z^{73} + 3z^{72} + 24z^{71} + 29z^{70} + \ldots \\
&\ldots + 193z^{12} + 100z^{11} + 64z^{10} + 29z^{9} + 24z^{8} + 3z^{7} + 5z^{6} - z^{4} + 1\big)/ \\
&\big((1-z^2)(1-z^4)^5(1-z^5)(1-z^6)^6(1-z^7)(1-z^8)^2(1-z^{10})^2\big) \\
= 1 &+ z^2 + 5z^4 + z^5 + 16z^6 + 5z^7 + 52z^8 + 38z^9 + 168z^{10} + 168z^{11} + 564z^{12} \\
&+ 692z^{13} + 1.773z^{14} + 2.477z^{15} + 5.438z^{16} + 8.032z^{17} + 15.824z^{18} \\
&+ 23.989z^{19} + 43.785z^{20} + \ldots
\end{aligned}
$$

- computed 76 invariants generating all up to degree 9
- estimate on the number of generators:

$$
\begin{aligned}
&z^2 + 4z^4 + z^5 + 11z^6 + 4z^7 + 26z^8 + 29z^9 + 71z^{10} + 103z^{11} \\
&\quad + 202z^{12} + 328z^{13} + 486z^{14} + 794z^{15} + 920z^{16} + 1210z^{17} + 603z^{18}
\end{aligned}
$$

Summary

- invariant theory provides a means to describe all entanglement classes
- information about the invariants via the Hilbert series
- already for small systems, we are facing combinatorial explosion
- proof of completeness via Hilbert series and SAGBI bases

Open Problems/Outlook

- Does Sturmfels' conjecture hold, at least for the representations considered here?
- Is it possible to find fewer invariants separating the orbits?
- Extend the approach to the group $SL(d)^n$, including covariants.
- Coarse-graining of the entanglement classes.