Reflection groups for quantum computing

Michel Planat

Institut FEMTO-ST, 32 Avenue de l'Observatoire, F-25044 Besançon
(michel.planat@femto-st.fr)

Seminar in Bristol, 8 October 2008

Introduction

- Pauli and Clifford groups
- (Unitary) Reflection groups
- Automorphisms of Pauli groups
- Topology and geometry of Clifford groups
- Perspectives: Invariant theory

Clifford gates are group operations stabilizing Pauli operations[1]

- Action $g \in \mathcal{P}_n$ on an n-qubit state $|\psi\rangle$ is $g|\psi\rangle$, evolves as $Ug|\psi\rangle$, and can be stabilized by U such that $(UgU^\dagger)U|\psi\rangle = U|\psi\rangle$, with $UgU^\dagger \in \mathcal{P}_n$

$$\mathcal{C}_n = \left\{ U \in U(2^n) | U\mathcal{P}_n U^\dagger = \mathcal{P}_n \right\}.$$

  In view of $U^\dagger = U^{-1}$, any normal subgroup $\mathcal{Q}_n = \left\{ UgU^{-1}, g \in \mathcal{Q}_n, \forall U \in \mathcal{C}_n \right\}$ of $\mathcal{C}_n$ may be relevant.
- A group extension $1 \rightarrow \mathcal{Q}_n \rightarrow \mathcal{C}_n \rightarrow \mathcal{C}_n/\mathcal{Q}_n \rightarrow 1$ carries some information about the structure of the error group $\mathcal{P}_n$ and its normalizer $\mathcal{C}_n$ in $U(2^n)$.

[1] Clark S, Jozsa R and Linden N 2008 *Quantum Inf. Comp.* **8** 106.

Given the *short exact sequence*

$$1 \to N \to G \to H \to 1,$$

i.e. $N \cong$ normal subgroup[2] of G, $H \cong G/N$,
in a splitting sequence $G = NH$ and $N \cap H = \{1\}$.

- non-split extension $G = N.H$
- split extension: the *semi-direct product* $G = N \rtimes H$
- *wreath product* $M \wr H$: semidirect product of M^n with the permutation group H acting on n copies of M
- *direct product* $G = N \times H$
- *central product* $G = N * H$

[2]a) The center $Z(G)$. The central quotient is $\tilde{G} = G/Z(G)$.
b) The subgroup G' of commutators $ghg^{-1}h^{-1}$.

Group of automorphisms

- Given the group operation $*$ of a group G, a *group endomorphism* is a function ϕ from G to itself such that $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$, for all $g_1, g_2 \in G$. If it is bijective it is called an **automorphism**.
- An automorphism of G that is induced by conjugation of some $g \in G$ is called inner. Otherwise it is called an outer automorphism. Under composition the set of all automorphisms defines a group denoted $\mathrm{Aut}(G)$. The **inner automorphisms** form a *normal subgroup* $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$, that is isomorphic to the cental quotient of G. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the **outer** automorphism group.

Reflections 1

- $\mathbb{E} = \mathbb{R}^l$: the l-dimensional (real) Euclidean space
- $O(\mathbb{E})$: the orthogonal group of linear transformations of $\mathbb{E}$ [3]
- $H_\alpha \subset \mathbb{E}$: *the hyperplane*

$$H_\alpha = \{x \in \mathbb{E} | (x, \alpha) = 0\}, \text{ given } \alpha \in \mathbb{E}.$$

- then a *reflection* $s_\alpha : \mathbb{E} \to \mathbb{E}$ is defined as

$$s_\alpha(x) = x \text{ if } x \in H_\alpha \text{ and } s_\alpha(\alpha) = -\alpha.$$

[3] endowed with a product $(.,.)$ such that $\forall a, b \in \mathbb{R}$ and $\forall x, y \in \mathbb{E}$, we have $(x, y) = (y, x)$ (symmetry), $(ax + by, z) = a(x, z) + b(y, z)$ (linearity), $(x, x) \geq 0$ and $(x, x) = 0 \Rightarrow x = 0$ (a positive definite form).

Reflections 2

- Explicit definition [4]

$$\forall x \in \mathbb{E} : s_\alpha(x) = x - \langle x, \alpha \rangle \alpha.$$

- Invariance under $t \in O(\mathbb{E})$

$$t(H_\alpha) = H_{t(\alpha)},$$

- Invariance under conjugation

$$t s_\alpha t^{-1} = s_{t(\alpha)}.$$

- The group of reflections

$$W = \{s_\alpha\} \subset O(\mathbb{E}).$$

irreducibility if $W \neq W_1 W_2$.

[4] in the Cartan notation $\langle x, y \rangle = 2\frac{(x,y)}{(x,x)}$.

The *root system* $\Delta \subset \mathbb{E}$ is obtained by replacing each hyperplane by its two orthogonal vectors of unit length:

- If $\alpha \in \Delta$, then $\lambda\alpha \in \Delta$ iff $\lambda = \pm 1$.
- The set Δ is permuted under the action of W: If $\alpha, \beta \in \Delta$, then $s_\alpha(\beta) \in \Delta$.
  Any element of Δ is a *root*, and Δ is named a *root system*.
- (*) Crystallographic property: W as a Weyl group.
  For any $\alpha, \beta \in \Delta$, one has $\langle \alpha, \beta \rangle := 2\frac{(\alpha,\beta)}{(\alpha,\alpha)} \in \mathbb{Z}$.

Finite reflection groups: the Coxeter presentation 1

- A group W is a **Coxeter group** if it is finitely generated by a subset $S \subset W$ of involutions and pairwise relations

$$W = \left\langle s \in S | (ss')^{m_{ss'}} = 1 \right\rangle , \quad (1)$$

where $m_{ss} = 1$ and $m_{ss'} \in \{2, 3, \ldots\} \cup \{\infty\}$ if $s \neq s'$. The pair (W, S) is a Coxeter system, of rank $|S|$ equal to the number of generators.

Finite reflection groups: the Coxeter presentation 2

- A (unique) *fundamental system* of $\Sigma \subset \Delta$:
  (i) Σ is linearly independent, (ii) every element of Δ is a linear combination of elements of Σ where the coefficients are all non-negative or all non-positive.
- *Fundamental root* $\alpha \in \Sigma \Rightarrow$ a fundamental reflection s_α.
  Given the fundamental system Σ of Δ, then $W(\Delta) = W$ is generated by fundamental reflections s_α.
  Define the (positive definite) bilinear form $\mathcal{B} : \Sigma \times \Sigma \rightarrow \mathbb{R}$ by

  $$\mathcal{B}(\alpha_s, \alpha_{s'}) = -\cos(\frac{\pi}{m_{ss'}}).$$

  $\mathcal{B}(\alpha_s, \alpha_s) = 1$ and $\mathcal{B}(\alpha_s, \alpha_{s'}) = 0$ when $m_{ss'} = 2$.
  It may be identified with the original inner product in $\mathbb{E}$.

A dihedral group

- Symmetries of the hexagon[5] $Out(\mathcal{P}_1) \cong W(G_2) = \text{Dih}_6$

$$\text{Dih}_6 = \left\langle x_1, x_2 | (x_1)^2 = (x_2)^2 = (x_1 x_2)^6 = 1 \right\rangle .$$

- Coxeter Diagram $\quad x_1 \;-\; -_6 \;-\; x_2$
- Cartan matrix
$$C = \left(\begin{array}{cc} 2 & -1 \\ -3 & 2 \end{array} \right)$$
- Dynkin Diagram $\quad x_1 \;=\; <_3 \;=\; x_2$

[5] $\mathcal{P}_1$ is the single qubit Pauli group

An entangling group

- The Coxeter system[6] of type D_5

$$\langle x_1 \dots x_5 | x_1^2 = \dots = x_5^2 = (x_1x_4)^2 = (x_2x_4)^2 = (x_1x_5)^2 = (x_2x_5)^2 = (x_4x_5)^2 = (x_2x_1)^3 = (x_3x_2)^3 = (x_4x_3)^3 = (x_5x_3)^3 = 1\rangle. \tag{2}$$

- Coxeter Diagram

$x_1 - - - x_2 - - - x_3 - - - x_5$ $- - - x_4$

- Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & -1 \\ 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 2 \end{pmatrix}$$

[6] The Weyl group $W(D_5)$ is the central quotient of the two-qubit Bell group.

Finite Coxeter groups

Type	*Group*	*Order*	*Rank*	*Related polytope*	*Coxeter diagram*
A_n	S_{n+1}	$(n+1)!$	n	n-simplex	$x_1 - x_2 \dots x_{n-1} - x_n$
B_n	$\mathbb{Z}_2^n \rtimes S_n$	$2^n n!$	n	n-hypercube	$x_1 -_4 x_2 \dots x_{n-1} - x_n$
D_n	$\mathbb{Z}_2^{n-1} \rtimes S_n$	$2^{n-1} n!$	n	demihypercube	$x_1 - {}^{-x_2}\ x_3 \dots x_{n-2} - x_{n-1}$
$I_2(p)$	Dih_p	$2p$	2	p-gon	$x_1 -_p x_2$
H_3	**	120	3	icosahedron/dodecahedron	$x_1 -_5 x_2 - x_3$
F_4	**	1152	4	24-cell	$x_1 - x_2 -_4 x_3 - x_4$
G_4	**	1440	4	120-cell/600-cell	$x_1 -_5 x_2 - x_3 - x_4$
E_6	**	51840	6	E_6 polytope	$x_1 - x_2 - x_3{}^{-x_4} - x_5 - x_6$
E_7	**	2 903 040	7	E_7 polytope	$x_1 - x_2 - x_3{}^{-x_4} - x_5 - x_6 - x_7$
E_8	**	696 729 600	8	E_8 polytope	$x_1 - x_2 - x_3{}^{-x_4} - x_5 - x_6 - x_7 - x_8$

Complex reflection groups 1

- V a complex vector space over $\mathbb{C}$.
- Every reflection $s: V \to V$ of order n over $\mathbb{C}$ satisfies the reflection property

$$s(x) = x + (\xi - 1)\frac{(\alpha, x)}{(\alpha, \alpha)}\alpha,$$

for all $x \in V$, where ξ is a primitive n-th root of unity.
- The eigenvector α is such that $s(\alpha) = \xi\alpha$ and (x, y) is a positive definite Hermitian form satisfying $(s(x), s(y)) = (x, y)$.

Complex reflection groups: classification[7]

- Three infinite families $\{\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}\}$, $\{S_n\}$, $\{G(m,p,n)\}$, and exceptional cases $\mathcal{U}_l$, $l = 1..34$.
- The *imprimitive unitary reflection groups*:
  There exists a decomposition $V = V_1 \otimes \ldots \otimes V_k$ $(k \geq 2)$, where the subspaces V_i are permuted transitively by G.
  If $p|m$, we can define the semidirect group

$$G(m,p,n) = A(m,p,n) \rtimes S_n,$$

$$A(m,p,n) = \left\{\mathrm{Diag}(\omega_1,\omega_2,\ldots,\omega_{n-1},\omega_n)|\omega_i^m = 1 \text{ and } (\omega_1\ldots\omega_n)^{m/p} = 1\right\}$$

- Special cases: $G(1,1,n) := S_n := W(A_{n-1})$, $G(m,m,2) := \mathrm{Dih}_m = W(G_2(m))$, $G(2,2,n) := W(D_n)$.

[7] Shephard G C and Todd J A 1954 *Canadian J Math* **6** 274.

... and the Clifford groups

- $\mathcal{P}_1 = G(4,2,2)$, $\mathcal{C}_1 \cong \mathcal{U}_9 = \mathbb{Z}_8.S_4$ of order 192.

$$\mathcal{U}_9 = \left\langle x_1, x_2 | x_1^2 = x_2^4 = (x_2^{-1}x_1)^3(x_2x_1)^3 = 1 \right\rangle .$$

- $\mathcal{C}_2$ (of order 92160) possesses 3 maximal normal subgroups of order 46080, one of them is $\mathcal{U}_{31} = (\mathbb{Z}_4 * \mathcal{Z}_2^{1+4}).S_6$.

$$\langle x_1 \dots x_5 | x_1^2 = \dots = x_5^2 = (x_1x_4)^2 = (x_2x_4)^2 = (x_2x_5)^2 = (x_4x_3)^3 = (x_5x_4)^3 = (x_3x_2)^3 = x_5x_1x_3x_1x_5x_3 = x_1x_5x_3x_1x_3x_5 = 1\rangle. \tag{3}$$

- $\mathcal{C}_3$ is related to E_7 and E_6.

- Pauli group $\mathcal{P}_1 = \langle \sigma_x, \sigma_y, \sigma_z \rangle \cong (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$
- $\mathrm{Aut}(\mathcal{P}_1) = \mathbb{Z}_2^3 \rtimes S_3 = W(B_3) = \mathbb{Z}_2 \times S_4 = W(A_1 A_3)$

$$x_1 \;-\; -_4 \;-\; x_2 \;-\; - \;-\; x_3$$

- $\mathrm{Out}(\mathcal{P}_1) = \mathrm{Dih}_6 = W(G_2) = \mathbb{Z}_2 \times \mathrm{Dih}_3 = W(A_1 I_2(3))$

$$x_1 \;-\; -_6 \;-\; x_2$$

Two qubits

- $\mathcal{P}_2 = \langle \sigma_0 \otimes \sigma_x, \sigma_x \otimes \sigma_x, \sigma_z \otimes \sigma_z, \sigma_y \otimes \sigma_z, \sigma_z \otimes \sigma_x \rangle \cong \mathbb{Z}_2 \times ((\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_2$
- $\text{Aut}(\mathcal{P}_2) = U_6.\mathbb{Z}_2^2$ with $U_6 = \text{Aut}(\mathcal{P}_2)' = \mathbb{Z}_2^4 \rtimes A_6$
  The group U_6 is a maximal subgroup of the Mathieu group M_{22}. It appears in a subgeometry of M_{22} known as a *hexad*. The group M_{22} stabilizes the Steiner system $S(3, 6, 22)$[8].
- $\text{Out}(\mathcal{P}_2) = \mathbb{Z}_2 \times S_6 = W(A_1 A_5)$.

[8] A Steiner system $S(a, b, c)$ with parameters a, b, c, is a c-element set together with a set of b-element subsets of S (called *blocks*) with the property that each a-element subset of S is contained in exactly one block.

Multiple qubits

- The automorphism group of the central quotient $\tilde{\mathcal{P}}_n \cong \mathbb{Z}_2^{2n}$.
  $\mathrm{Aut}(\tilde{\mathcal{P}}_1) = \mathbb{Z}_6$.
  $\mathrm{Aut}(\tilde{\mathcal{P}}_2) = A_8 \cong PSL(4,2)$ (of order 20160).
  $\mathrm{Aut}(\tilde{\mathcal{P}}_3) = PSL(6,2)$ (of order 20 158 709 760).

$$\mathrm{Aut}(\tilde{\mathcal{P}}_n) = PSL(2n,2) = A_{2n-1}(2).$$

- $PSL(2n,2)$ is the group of Lie type A_{2n-1} over the field $\mathbb{F}_2$. The Weyl group is defined by the Coxeter system of type A_{2n-1}, i.e., the symmetry group S_{2n}.
- Also the automorphism group of the $(n-1)$-qubit CSS (Calderbank-Schor-Steane) *additive* quantum code .

g_i	g_2	g_3	g_4	g_5	g_6
G	$\mathbb{Z}_2^2$	$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	$(\mathbb{Z}_2 \times \mathcal{Q}) \rtimes \mathbb{Z}_2$	$\mathbb{Z}_2 \times ((\mathbb{Z}_2 \times \mathcal{Q}) \rtimes \mathbb{Z}_2)$	g_6
$\mathrm{Aut}(G)$	Dih_4	$\mathbb{Z}_2 \times S_4$	$\mathbb{Z}_2 \wr A_5$	$\mathbb{Z}_2^2 \wr A_5$	$\mathbb{Z}_2^3 \wr A_5$
$\lvert\mathrm{Aut}(G)\rvert$	8	48	1920	61440	1966080
$\mathrm{Out}(G)$	$\mathbb{Z}_2$	Dih_6	S_5	$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes M_{20}$	$(\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes M_{20}^{(2)}$

Two-qubits

Let m_i $(i = 1, \ldots, 5)$, the elements of maximal sets of MUBs, $g_2 = \langle m_1, m_2 \rangle, \ldots$ $g_4 = \langle m_1, m_2, m_3, m_4 \rangle$,

More qubits

$\mathrm{Aut}(g_i) = \mathbb{Z}_2^l \wr A_5 = G(2^l, 2, 5)$ with $l = i - 3$ $(i > 3)$,

$\mathrm{Out}(g_i) = G(2^{l-1}, 2, 5)$.

$M_{20}^{(l-1)} = G'(2^l, l, 5)$ such that $M' \neq K(M)$[9].

[9] $M_{20} = G'(2, 2, 5) = \mathbb{Z}_2^4 \rtimes A_5$, $|M_{20}| = 960$.
$M_{20}^{(2)} = G(4, 2, 5) = \mathbb{Z}_2^4 \rtimes M_{20}$, $|M_{20}^{(2)}| = 15360$.

Two-qubit Clifford and Bell groups

- **Clifford groups** $\mathcal{C}_1 = \langle H, P \rangle$, $\mathcal{C}_2 = \langle \mathcal{C}_1 \otimes \mathcal{C}_1, \mathrm{CZ} \rangle$
  H: the Hadamard gate, P the $\pi/4$ phase gate,
  CZ:= Diag(1,1,1,-1).

$$1 \to U_6 \to \tilde{\mathcal{C}}_2 \to \mathbb{Z}_2 \to 1, \quad U_6 = \mathbb{Z}_2^4 \rtimes A_6$$

$$\mathcal{C}_2/\mathcal{P}_2 \cong \mathrm{Out}(\mathcal{P}_2) = \mathbb{Z}_2 \times S_6$$

- **Bell group** $\mathcal{B}_2 = \langle \mathcal{C}_1 \otimes \mathcal{C}_1, R \rangle \subset \mathcal{C}_2$, $\mathbf{R}:= 1/\sqrt{2} \begin{pmatrix} \sigma_0 & i\sigma_y \\ i\sigma_y & \sigma_0 \end{pmatrix}$.

$$1 \to M_{20} \to \tilde{\mathcal{B}}_2 \to \mathbb{Z}_2 \to 1, \quad M_{20} = \mathbb{Z}_2^4 \rtimes A_5 \quad \tilde{\mathcal{B}}_2 = W(D_5)$$

$$\mathcal{B}_2/\mathcal{P}_2 = \mathbb{Z}_2 \times S_5$$

Bell matrix and the Yang-Baxter equation

- One uses pairs $\left|v, v^{-1}\right\rangle$ of magnetic fluxes for the qubits exchanged within a group G

$$\left|v_1, v_2\right\rangle \rightarrow \left|v_2, v_2^{-1} v_1 v_2\right\rangle,$$

a form of Aharonov-Bohm interactions, which is nontrivial in a nonabelian group. This process can be shown to produce universal quantum computation.

- It is intimately related to topological entanglement, the braid group and unitary solutions of the Yang-Baxter equation[10]

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

[10] Kauffman L H and Lomonaco S J 2004 *New J Phys* **6**, 134.

Three-qubit Clifford and Bell groups

- $\mathcal{C}_3 = \langle H \otimes H \otimes P, H \otimes \mathrm{CZ}, \mathrm{CZ} \otimes H \rangle$ of order 743 178 240

$$\tilde{\mathcal{C}}_3 = \mathbb{Z}_2^6 \rtimes W'(E_7), \quad \text{with } W'(E_7) = \mathrm{Sp}(6,2)$$

$$\mathcal{C}_3/\mathcal{P}_3 \cong \mathrm{Out}(\mathcal{P}_3) = \mathbb{Z}_2 \times \mathrm{Sp}(6,2)$$

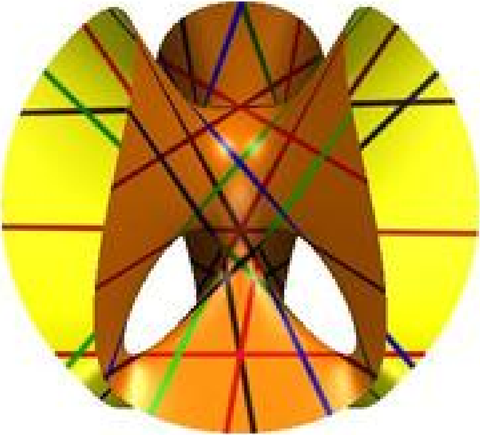
- $\mathcal{B}_3 = \langle H \otimes H \otimes P, H \otimes R, R \otimes H \rangle$ of order 13 271 040

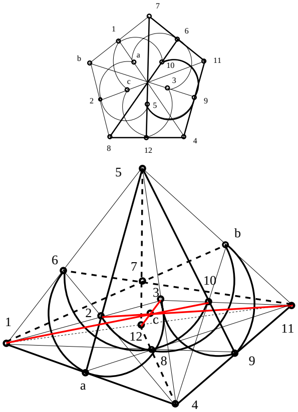
$$\tilde{\mathcal{B}}_3 = \mathbb{Z}_2^6 \rtimes W'(E_6), \quad \text{with } W'(E_6) = \mathrm{SU}(4,2) \cong \mathrm{PSp}(4,3)$$

Geometry of Bell groups: D5, E6 and a cubic surface

- *Among maximal subgroups*[11] of $W(E_6)$
  * $W'(E_6)$ (order 25920 and index 1),
  * $W(D_5)$ (order 1920 and index 27),
  * $W(F_4)$ (order 1152 and index 45)
  * $A_6.\mathcal{Z}_2^2$ (order 1440, index 36)
- *Smooth cubic surface* K_3: A. Cayley, L Cremona... in 19th century
  * $W(E_6)$: group of permutations of the 27 lines of K_3
  * $W(D_5)$: the stabilizing group of a line, $W(E_6)/W(D_5) = 27$
  * 45 tritangent planes stabilized by $W(F_4)$
  * 36 double-sixes with stabilizing group $A_6.\mathcal{Z}_2^2$

[11] Maximal subgroup H of G: $H \neq G$ and no subgroup K of G such that $H < K < G$.





- Embedding of $GQ(2)$ into the projective space $PG(3,2)$ [Planat M and Saniga M 2008 *Quant Inf Comp* **8** 127].

Geometry of the three-qubit system: $A_2(2)$, $G_2(2)$?

- instead of GQ(2) the generalized hexagon $G_2(2)$[12]?
- Lie groups
  $G_2(2)$, $G_2(2)' \cong SU(3,3)$, and $A_2(2) = PSL(2,7) \subset \mathcal{C}_3$
  $|G_2(2)| = 12096$, $|PSL(2,7)|$=168
- Presentation of $PSL(2,7)$ is
  $x_1^2 = x_2^4 = (x_1 x_2^{-1})^7 = (x_2^{-2} x_1)^2 x_2^2 x_1 = 1$

$$x_1 = \frac{1}{2}\begin{pmatrix} \sigma_0 & -\sigma_z & i\sigma_z & -i\sigma_0 \\ -\sigma_z & \sigma_0 & i\sigma_0 & -i\sigma_z \\ -i\sigma_z & -i\sigma_0 & \sigma_0 & \sigma_z \\ i\sigma_0 & i\sigma_z & \sigma_z & \sigma_0 \end{pmatrix},\ x_2^2 = \frac{1}{2}\begin{pmatrix} \sigma_0 & \sigma_y & i\sigma_y & -i\sigma_0 \\ \sigma_y & \sigma_0 & -i\sigma_0 & i\sigma_y \\ -i\sigma_y & i\sigma_0 & \sigma_0 & \sigma_y \\ i\sigma_0 & -i\sigma_y & \sigma_y & \sigma_0 \end{pmatrix}.$$

[12] P Levay, M Saniga and P Vrana, 0808.3849 [quant-ph]

Poincaré series

Let M a *graded connected* $\mathbb{F}$ vector space *of finite type* [13], the Poincaré series is

$$P_t(M) = \sum_{i=0}^{\infty} (\dim_{\mathbb{F}} M_i) t^i.$$

- Let $M = \mathbb{F}[x]/(x^{n+1})$, where $\deg(x) = d$. Then

$$P_t(M) = 1 + t^d + t^{2d} + \cdots = \frac{1}{1 - t^d}.$$

[13] $M = \bigotimes_{i \in \mathbb{N}} M_i$. It is of finite type if $\dim_{\mathbb{F}} M_i < \infty$ for all i.

Let V an n-dimensional $\mathbb{F}$ vector space and $G \subset GL(V)$ a finite nonmodular subgroup[14].

- Polynomial algebra

$$S(V) = \mathbb{F}[t_1, \ldots, t_n],$$

- Ring of invariants

$$S(V)^G = \{s \in S(V) | g.s = s \text{ for all } g \in G\},$$

- Molien's theorem

$$P_t(S(V)^G) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)}.$$

[14] Char $\mathbb{F}$ does not divide $|G|$.

Molien's theorem for the shift matrix σ_x

- Let $V = \mathbb{C}x + \mathbb{C}y$ and $G = <\sigma_x> \cong \mathbb{Z}_2 \subset GL(V)$. So σ_x flips "the qubits" x and y.

g	$\det(1-gt)$
$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$(1-t)^2$
$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$1-t^2$

- $P_t(S(V)^G) = \frac{1}{2}\left[\frac{1}{(1-t)^2} + \frac{1}{1-t^2}\right] = \frac{1}{(1-t)(1-t^2)}$.
- Invariants $s_1 = x + y$ and $s_2 = xy$ and $S(V)^G = \mathbb{C}[s_1, s_2]$.

Molien's theorem for single qubit Pauli's and Clifford's

Let $V=\mathbb{C}x+\mathbb{C}y$,

- $G=\mathcal{P}_1=G(4,2,2)=<\sigma_x,\sigma_y,\sigma_z>\subset GL(V)$.
  $P_t(S(V)^G)=\frac{1}{(1-t^4)^2}$
  Invariants $s_1=x^4+y^4$ and $s_2=x^4y^4$ and $S(V)^G=\mathbb{C}[s_1,s_2]$.
- $G=\mathcal{C}_1=\mathcal{U}_9\subset GL(V)$[15].
  $P_t(S(V)^G)=\frac{1}{(1-t^8)(1-t^{24})}$
  Invariants $s_1=x^8+14x^4y^4+y^8$
  and $s_2=x^{24}+759x^{16}y^8+2576x^{12}y^{12}+759x^8y^{16}+y^{24}$,
  $s_3=x^4y^4(x^4-y^4)^4$,
  $S(V)^G=\mathbb{C}[s_1,s_2]$ or $\mathbb{C}[s_1,s_3]$.

[15] Invariants s_1 and s_2 are the weight enumerators of the $[8,4,4]$-Hamming code e_8 and $[24,12,8]$-Golay code G_{24} respectively. By Gleason's theorem any even self-dual code possesses a weight enumerator of the form $\mathbb{C}[s_1,s_3]$ [Mac Williams and Sloane *The theory of error-correcting codes* 1977 North-Holland (Amsterdam)].