Number theory in Pauli type quantum commutation structures

Michel Planat

Institut FEMTO-ST, CNRS, 15 B Avenue des Montboucons, F-25044 Besançon
(michel.planat@femto-st.fr)

SEAMS School, Kuala Lampur: 3 November 2015

Abstract [1]

* **Single qudits**: qubit, qutrit, quartit, quintit, sextit, heptit, octit, 9-dit, 10-dit, 11-dit, 12-dit, 13-dit, ...

- Commutation relations between observables of a single q-dit: maximal commuting sets and the **Pauli** group/graph/geometry,
- a bijection between the Pauli group observables (modulo the center) and the modular lattice $\mathbb{Z}_q^2$,
- number/modular theory on $\mathbb{Z}_q^2$: the **Dedekind psi function** and the projective line $\mathbb{P}_1(\mathbb{Z}_q)$.

* **Multiple qudits**: 2-qubit, 3-qubit, 2-qutrit...

- genralized quadrangle $GQ(2,2)$, symplectic polar space $W_5(2)$, $GQ(3,3)$...

* **Mixture of qudits**: qubit/quartit, qubit/octit...

- three copies of $GQ(2,2)'$, six copies of $GQ(2,2)'$...

[1] M. Planat, Pauli graphs when the Hilbert space dimension contains a square: why the Dedekind psi function? J. Phys. A: Math. Theor. **44**, 045301 (2011).

A few multiplicative number theoretical functions

- The **sum of divisor** function

$$\text{for} \quad q = \prod_i p_i^{s_i} \quad \text{one} \quad \text{gets} \quad \sigma(q) = \prod_i \frac{p_i^{s_i+1} - 1}{p_i - 1}.$$

- The **Dedekind psi** function

$$\psi(q) = q \prod_{p|q, p \in \mathcal{P}} (1 + \frac{1}{p}).$$

One has $\psi(q) \leq \sigma(q)$ where the equality holds if q is square free.

- The **Euler totient** function

$$\phi(q) = q \prod_{p|q, p \in \mathcal{P}} (1 - \frac{1}{p}).$$

The Pauli group $\mathcal{P}_q$ of a single qudit and the n-fold product of them.

- A **Weyl pair** (X, Z) of *shift* and *clock* operators

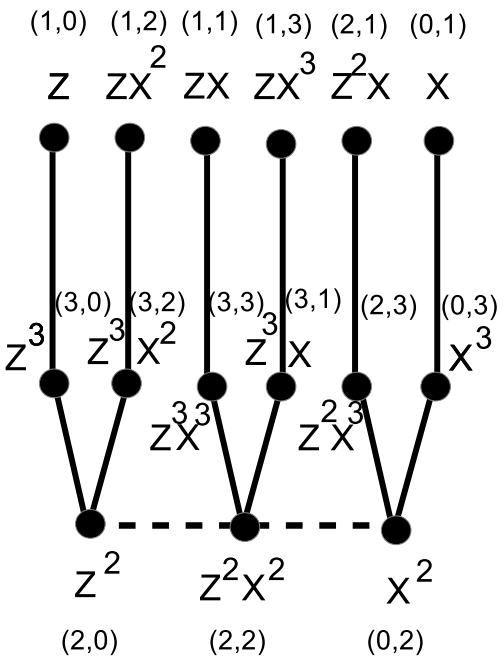
$$Z^q = X^q = I_q, \quad ZX - \omega XZ = 0,$$

where $\omega = \exp(\frac{2i\pi}{q})$ is a primitive q-th root of unity.

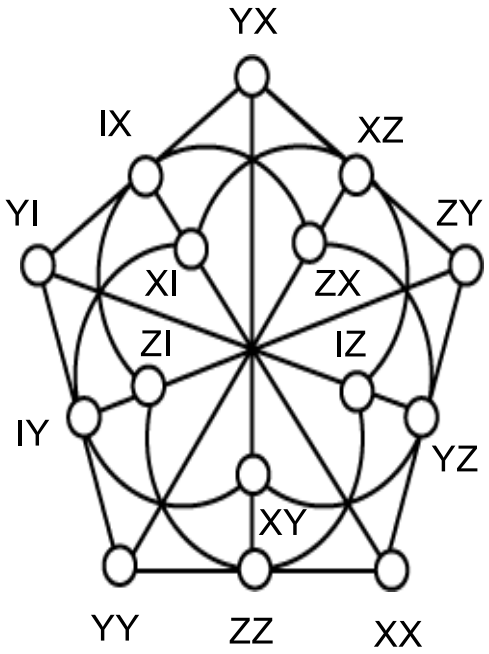
$$X = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ . & . & \dots & . & . \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad Z = \mathrm{diag}(1, \omega, \omega^2, \dots, \omega^{q-1}).$$

- In the single qudit **Pauli group** $\mathcal{P}_q = \langle X, Z \rangle$ of order q^3, each element may be written as $\omega^a X^b Z^c$, with $a, b, c \in \mathbb{Z}_q$.
- The multiple qudit **Pauli group** $\mathcal{P}_q (q = p^n)$ is the n-fold tensor product between single p-dit Pauli operators with $\omega = \exp(\frac{2i\pi}{p})$, i.e. $IX = I \otimes X$, $IY = I \otimes Y$...

Quantum commutation in dimension four: $4 \neq 2^2$



$P_1(Z_4)$



GQ(2,2)

- left: commutation geometry for a quartit, $\sigma(4) = 7 = 1 + \psi(4)$.
- right: commutation geometry for a two-qubit system, $IX = I \otimes X, YZ = Y \otimes Z \cdots$.

The bijection between the (central quotient) of the Pauli group $\mathcal{P}_q$ and the modular lattice $\mathbb{Z}_q^2$

- The **group commutator** is $[X, Z] = XZX^{-1}Z^{-1} = \omega^{-1} I_q$ so that
$$\left[\omega^a X^b Z^c, \omega^{a'} X^{b'} Z^{c'}\right] = \omega^{cb'-c'b} I_q,$$
meaning that two elements of $\mathcal{P}_q$ commute iff $\Delta = \det \begin{pmatrix} b' & b \\ c' & c \end{pmatrix}$ vanishes.
- For **perpendicular vectors**, the symplectic inner product $[(b', c').(b, c)] = \Delta = b'c - bc' = 0$. *One transfers the study of commutation relations within the group $\mathcal{P}_q$ to that of perpendicularity of vectors in the ring $\mathbb{Z}_q^2$.*
- Thus, since $\mathcal{P}_q' \cong Center(\mathcal{P}_q)$
$$(\mathcal{P}_q / Center(\mathcal{P}_q), \times) \cong (\mathbb{Z}_q^2, +).$$

Isotropic lines of the lattice $\mathbb{Z}_q^2$

- Isotropic line[2]: as a set of q points on the lattice $\mathbb{Z}_q^2$ such that the symplectic product of any two of them is $0 (\mathrm{mod}\ q)$. It corresponds a maximal commuting set in $\mathcal{P}_q/Z(\mathcal{P}_q)$.
  Taking the the Hilbert space dimension as $q = \prod_i p_i^{s_i}$, the number of isotropic lines of the lattice $\mathbb{Z}_q^2$ reads

$$\eta(q) = \prod_i \frac{p_i^{s_i+1} - 1}{p_i - 1} \equiv \sigma(q).$$

- Isotropic line though a given point x

$$\eta(q; x) = \prod_i \frac{p_i^{t_i+1} - 1}{p_i - 1} \equiv \sigma(\tilde{q}(x))$$

  where $t_i = v_{p_i}(x)$ the p_i-valuation of x and $\tilde{q}(x) = \prod_i p_i^{t_i} \leq q$ is a *local* dimension defined at the selected point x.

[2] Albouy O. The isotropic lines of $\mathbb{Z}_d^2$ *J. Phys. A: Math. Theor.* **42** 072001 (2009).

Projective line $\mathbb{P}_1(\mathbb{Z}_q)$ of the lattice $\mathbb{Z}_q^2$

- A isotropic line of $\mathbb{Z}_q^2$ corresponds to a *Lagrangian submodule*, i.e. a maximal module such that the perpendicular module $M^\perp = M$. For free cyclic submodules[3]

$$\mathbb{Z}_q(b,c) = \{(ub, uc) | u \in \mathbb{Z}_q\},$$

  the application $u \to (ub, uc)$ is injective.
- A point $x = (b,c)$ such that $\mathbb{Z}_q(b,c)$ is free is called an **admissible point**, and the set of admissible points is called the **projective line**

$$\mathbb{P}_1(\mathbb{Z}_q) = \{\mathbb{Z}_q(b,c) | (b,c) \text{ is admissible}\}.$$

  Its cardinality is the **Dedekind psi function**

$$|\mathbb{P}_1(\mathbb{Z}_q)| = \prod_i (p_i^{s_i} + p_i^{s_i - 1}) \equiv \psi(q).$$

[3] Havlicek H ans Saniga M 2007 Projective line of a specific qudit *J. Phys. A: Math. Theor.* **40** F943-F952.

Admissible vectors of the lattice $\mathbb{Z}_q^2$

- If $q = p^s$, there are $p^{2s} - p^{2(s-1)}$ **admissible vectors** $x = (b, c)$ and, for arbitrary dimensions $q = \prod_i p_i^{s_i}$, the number of admissible vectors is the **Jordan totient function**

$$q^2 \prod_i (1 - \frac{1}{p^2}) = \phi(q)\psi(q) = J_2(q).$$

- Locally: $J_2(\tilde{q}(x))$, with $\tilde{q}(x) = \prod_i p_i^{t_i} \leq q$ is the local dimension.
- **The symplectic group** $\mathrm{Sp}(2, \mathbb{Z}_q)$ is built from all matrices $\begin{pmatrix} b' & b \\ c' & c \end{pmatrix}$ such that (b, c) is an admissible vector and the symplectic inner product, i.e. the determinant $\Delta = b'c - bc' = 1$. One gets [4] $|\mathrm{Sp}(2, \mathbb{Z}_q)| = qJ_2(q)$.

[4] Vourdas A and Banderier C 2010 Symplectic transformations and quantum tomography in finite quantum systems *J. Phys. A: Math. Theor.* **43** 042001-10.

The Pauli graph of a qudit

- The Pauli graph $\mathcal{G}_q$: observables as vertices and a edge joining two commuting observables.
- a point/line incidence geometry with observables as points and maximum cliques of $\mathcal{G}_q$ (maximal sets of mutually commuting observables) as lines.
  $\Rightarrow$ a dual graph $\mathcal{G}_q^*$ such that the vertices are the cliques and a edge joins two non-intersecting cliques.
  The **connected component** of $\mathcal{G}_q^*$ corresponds to the graph of the projective line $\mathbb{P}_1(\mathbb{Z}_q)$.

Structure of a few single qudit systems

q	name	# cliques	geometry	aut. group
4	quartit	$6+1$	$P_1(\mathbb{Z}_4)$	$G_{48} = \mathbb{Z}_2 \times S_4$
8	octit	$12+3$	$P_1(\mathbb{Z}_8)$	$\mathbb{Z}_2^6 \rtimes (\mathbb{Z}_3^3 \rtimes G_{48})$
9	9-dit	$12+1$	$P_1(\mathbb{Z}_9)$	$G_{648} \rtimes G_{48}$
12	12-dit	$24+4$	$P_1(\mathbb{Z}_{12})$	$\mathbb{Z}_2^{12} \rtimes G_{144}$
16	16-dit	$24+7$	$P_1(\mathbb{Z}_{16})$	$A_8^3 \rtimes G_{48}$
18	18-dit	$36+3$	$P_1(\mathbb{Z}_{18})$	$\mathbb{Z}_3^{12} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$
24	24-dit	$48+12$	$P_1(\mathbb{Z}_{24})$	$G_{2^{24}3^{12}} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$

- e.g. $q = 12 = 2^2 \times 3$, there are $12^2 - 1 = 143$ observables in $\mathcal{G}_{12}$, $\sigma(12) = 28$ max. cliques in $\mathcal{G}_{12}$ and $|P_1(\mathbb{Z}_{12})| = \psi(12) = 24$. $(aut)(|P_1(\mathbb{Z}_{12})) = \mathbb{Z}_{12} \rtimes G_{144}$ with $G_{144} = A_4 \rtimes D_6$.

Multiple qudits as symplectic polar spaces [5]

- The multiple qudit **Pauli group** $\mathcal{P}_q(q = p^n)$ is the n-fold tensor product between single p-dit Pauli operators with $\omega = \exp(\frac{2i\pi}{p})$, i.e. $IX = I \otimes X$, $IY = I \otimes Y$...

  Observables of $\mathcal{P}_q/\text{Center}(\mathcal{P}_q)$ are seen as the elements of the $2n$-dim. Vector space $V(2n, p)$ defined over $\mathbb{F}_p$. The **commutator** $[.,.]: \ V(2n,p) \times V(2n,p) \to \mathcal{P}'_q$ induces a non-singular alternating bilinear form on $V(2n, p)$, and simultaneously a symplectic form on the projective space $PG(2n-1, p)$ over $\mathbb{F}_p$.

- The $|V(2n, q)| = p^{2n}$ observables of $\mathcal{P}_q/\text{Center}(\mathcal{P}_q)$ are **mapped to the points of the symplectic polar space** $W_{2n-1}(p)$ of cardinality

$$|W_{2n-1}(p)| = \frac{p^{2n}-1}{p-1} \equiv \sigma(p^{2n-1}),$$

  and two elements of $[\mathcal{P}_q/\text{Center}(\mathcal{P}_q), \times]$ commute iff the corresponding points of the polar space $W_{2n-1}(p)$ are collinear.

[5] Saniga M and Planat M 2007 *Adv. Stud. Theor. Phys.* **1** 1-4.

Generators of symplectic polar spaces

- A subspace of $V(2n, p)$ is called **totally isotropic** if the symplectic form vanishes identically on it. The number of such totally isotropic subspaces/generators G (of dimension $p^n - 1$ is

$$|\Sigma(W_{2n-1}(p))| = \prod_{i=1}^{n}(1 + p^i).$$

- A **spread** S of a vector space a set of generators partitioning its points. $|S| = p^n + 1$ and one has $|V(2n, p)| - 1 = |S| \times |G| = (p^n + 1) \times (p^n - 1) = p^{2n} - 1$.

  A **generator** G corresponds to a **maximal commuting set** and a spread S corresponds to a maximum (and complete) set of disjoint maximal commuting sets.

  Two generators in a spread are mutually disjoint and the corresponding maximal commuting sets are **mutually unbiased**.

Punctured symplectic polar spaces

- Let us define the punctured polar space $W_{2n-1}(p)'$ as the polar space $W_{2n-1}(p)$ **minus a point u and all the totally isotropic spaces passing though it**. Then, one gets

$$|W_{2n-1}(p)'| = \sigma(p^{2n-1}) - \sigma(p^{2n-3}) = \psi(p^{2n-1}),$$

where $\sigma(p^{2n-3})$ is the size of the removed part and $\psi(q)$ is the Dedekind psi function.

Pauli graphs of multiple qudits

- The Pauli graph $\mathcal{G}_{p^n}$: observables as vertices and a edge joining two commuting observables.
- A dual graph $\mathcal{G}^*_{p^n}$ such that the vertices are the cliques and a edge joins two non-intersecting cliques.
- Another dual graph $\mathcal{G}'^*_{p^n}$ obtained by removing a perp-set in the symplectic polar space.

Pauli graphs of multiple qudits

p^n	name	$\mathrm{aut}(\mathcal{G}_{p^n})$	$\mathrm{aut}(\mathcal{G}^*_{p^n})$	$\mathrm{aut}(\mathcal{G}'^*_{p^n})$	$c = \frac{\lvert\mathrm{aut}(\mathcal{G}^*_{p^n})\rvert}{\lvert\mathrm{aut}(\mathcal{G}'^*_{p^n})\rvert}$
2	qubit	S_3	S_3	S_2	$3 \equiv \sigma(2)$
2^2	2-qubit	S_6	S_6	$G_{48} = \mathbb{Z}_2 \times S_4$	$15 \equiv \sigma(2^3)$
2^3	3-qubit	$Sp(6,2)$	$O^+(8,2)$	$\mathbb{Z}_2^6 \rtimes A_8$	$2 \times 135 \neq 63$
2^4	4-qubit	$Sp(8,2)$	$Sp(8,2)$	$\mathbb{Z}_2^7 \rtimes Sp(6,2)$	$255 = \sigma(2^7)$
3	qutrit	$\mathbb{Z}_2^4 \rtimes S_4$	S_4	S_3	$4 \equiv \sigma(3)$
3^2	2-qutrit	$\mathbb{Z}_2^{40}.W(E_6)$	$W(E_6)$	$G_{648} \rtimes \mathbb{Z}_2$	$40 \equiv \sigma(3^3)$
3^3	3-qutrit	$\mathbb{Z}_2^{364}.Sp(6,3)$	$Sp(6,3)$	$(E_{243} \rtimes \mathbb{Z}_2).W(E_6)$	$364 \equiv \sigma(3^5)$
5	quintit	$\mathbb{Z}_2^{12} \rtimes (\mathbb{Z}_3^6 \rtimes (\mathbb{Z}_2 \wr S_6))$	S_6	S_5	$6 \equiv \sigma(5)$

- Comparison of the automorphism group of the **dual Pauli graph** $\mathcal{G}^*_{p^n}$ and that of its **building block** $\mathcal{G}'^*_{p^n}$. The ratio of sizes of both groups turns out to be the size $|W_{2n-1}(p)| = \sigma(p^{2n-1})$ of the corresponding symplectic polar space space, except for the case of the 3-qubit system where it is twice the number 135 of maximum cliques in the Pauli graph $\mathcal{G}_{2^3}$.

Multiple qudit mixtures

q	name	# cliques	geometry	aut. group
4	quartit	$6+1$	$P_1(\mathbb{Z}_4)$	$G_{48} = \mathbb{Z}_2 \times S_4$
2^2	2-qubit	15	$GQ(2,2)$	S_6
8	octit	$12+3$	$P_1(\mathbb{Z}_8)$	$\mathbb{Z}_2^6 \rtimes (\mathbb{Z}_3^3 \rtimes G_{48})$
2×2^2	qubit/quartit	$36+3$	$3 \times GQ(2,2)'$	$G_{48}^3 \rtimes S_3$
2^3	3-qubit	135	$W_5(2)$	$\mathrm{Sp}(6,2)$
9	9-dit	$12+1$	$P_1(\mathbb{Z}_9)$	$G_{648} \rtimes G_{48}$
3^2	2-qutrit	40	$GQ(3,3)$	$\mathbb{Z}_2^{40}.W(E_6)$
12	12-dit	$24+4$	$P_1(\mathbb{Z}_{12})$	$\mathbb{Z}_2^{12} \rtimes G_{144}$
$2^2 \times 3$	2-qubit/qutrit	60	$4 \times GQ(2,2)$	$S_6^4 \rtimes S_4$
16	16-dit	$24+7$	$P_1(\mathbb{Z}_{16})$	$A_8^3 \rtimes G_{48}$
2×8	qubit/octit	$72+15$	$6 \times GQ(2,2)'$	$G_{48}^6 \rtimes S_6$
4×4	2-quartit	$120+30+1$	15-cube	$G_{48}^{15} \rtimes S_{15}$
$2^2 \times 4$	2-qubit/quartit	$360+15$	$3 \times W_5(2)'$	$(\mathbb{Z}_2^5 \rtimes S_6)^3 \rtimes S_3$
2^4	4-qubit	2295	$W_7(2)$	$\mathrm{Sp}(8,2)$
18	18-dit	$36+3$	$P_1(\mathbb{Z}_{18})$	$\mathbb{Z}_3^{12} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$
2×3^2	2-qutrit/qubit	120	$3 \times GQ(3,3)$	$W'(E_6)^3.G_{48}$
24	24-dit	$48+12$	$P_1(\mathbb{Z}_{24})$	$G_{2^{24}3^{12}} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$
$2^3 \times 3$	3-qubit/qutrit	540	$4 \times W_5(2)$	$\mathrm{Sp}(6,2)^4.S_4$

On the n-dimensional Euclidean lattice

- An n-dimensional Euclidean lattice L is a discrete additive subgroup of the real vector space $\mathbb{R}^n$, endowed with the standard Euclidean product, and spanned by a generator matrix M with rows in $\mathbb{R}^n$.
- The automorphism group $\mathrm{Aut}(L)$ is the set of orthogonal matrices B such that under the conjugation action $U = MBM^{-1}$ by the generating matrix M, one has (i) $\det U = \pm 1$ and (ii) U is an integer matrix [6].
- One focuses on **Barnes-Wall lattices** BW_n ($n = 2^m$ and $m > 1$) that generalize the root lattices $BW_4 \cong D_4$ and $BW_8 \cong E_8$ with BW_{16} (the densest known lattices) and higher [7]. Their automorphismgroup group is the so-called **real Clifford group**[8].

[6] J. H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups* (Springer, New York, 1999, p. 90).

[7] M. Planat, Phys. Scr. T147 014025 (2011).

[8] G. Nebe, E. M. Rains and N. J. A Sloane, Self-Dual Codes and Invariant Theory (Springer, Berlin, 2006).

Real rays of the n-qubit Pauli group and BW lattices:1

$n = 2^m$	$\#mcs$	#rays	#real rays	aut group	#aut group
2	3	6	4	D_4	8
4	15	60	24	$\mathbb{Z}_2^4 \rtimes (\mathbb{Z}_3^2 \rtimes D_4)$	1152
8	135	1080	240	$\mathbb{Z}_2^6 \rtimes S_8$	2580480
16	2295	36720	4320	$\cong aut(BW_{16})$	89181388800
32	75735	2423520	146880	$\cong aut(BW_{32})$	$\approx 4.8 \times 10^{15}$

- The relationship between the **Barnes-Wall lattices and the real rays** arising from the n-qubit Pauli group P_n: the total number of states/rays appearing as eigenstates shared by the maximal commuting sets mcs of operators in P_m is nL, where $n = 2^m$ and the number of maximal commuting sets is $L = \prod_{i=1}^{m}(1 + 2^i)$, as shown in column 3 ; the corresponding number of real rays is shown in column 4. The rays form maximal orthogonal bases whose orthogonality graph is defined in columns 5 and 6.

Real rays of the n-qubit Pauli group and BW lattices: 2

- The **number of real rays identifies to the kissing number** $k_n = (2^n + 2)k_{n-1}$ **(with** $k_1 = 1$**) of a Barnes-Wall lattice** BW_n ($n = 2^m$ and $m > 1$), that is isomorphic to $D_4, E_8, \Lambda_{16}, BW_{32} \cdots$.
- The **automorphism group of the orthogonality graph attached to the real rays is that of** BW_n**, that is the real Clifford group** $C_n^+ = 2_+^{1+2m}.\Omega_{2m}^+(2)$, of order $2^{m^2+m+1}(2^m - 1)\prod_{j=1}^{m-1}(4^j - 1)$, with 2_+^{1+2m} the extraspecial group of order 2^{2m+1} and $\Omega_{2m}^+(2)$ the orthogonal group [the derived subgroup of the general orthogonal group $O_{2m}^{\pm}(2)$].

  One concludes that a natural frame for the real rays arising from the multiple qubit Pauli group P_m is the Barnes-Wall lattice BW_{2^m}.