Qudits and Geometry over Rings

Berlin, March 3rd, 2008

joint work with
Metod Saniga
Astronomical Institute
Slovak Academy of Sciences
Tatranská Lomnica, Slovakia

Supported by *Aktion Slowakei-Österreich*, project 58s2

TECHNISCHE UNIVERSITÄT WIEN
VIENNA UNIVERSITY OF TECHNOLOGY
DIFFERENTIALGEOMETRIE UND GEOMETRISCHE STRUKTUREN

HANS HAVLICEK
FORSCHUNGSGRUPPE
DIFFERENTIALGEOMETRIE UND
GEOMETRISCHE STRUKTUREN
INSTITUT FÜR DISKRETE MATHEMATIK UND GEOMETRIE
TECHNISCHE UNIVERSITÄT WIEN
havlicek@geometrie.tuwien.ac.at

The Generalised Pauli Group

We consider the d-dimensional complex Hilbert space $\mathbb{C}^d$, $d > 1$. A qudit is a unit vector of this space ($d = 2$: qubit, $d = 3$: qutrit).

Let ω be a fixed primitive d-th root of unity, e. g., $\omega = \exp(2\pi i/d)$.

The unitary shift and clock operators on $\mathbb{C}^d$ are defined via their matrices w.r.t. the standard basis:

$$X = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \omega & 0 & \dots & 0 \\ 0 & 0 & \omega^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \omega^{d-1} \end{pmatrix}.$$

The generalised Pauli group G is the multiplicative group generated by X and Z.

(For $d = 2$ another group is known in physics under the name Pauli group.)

The Generalised Pauli Group

The basic relation in G reads

$$\omega XZ = ZX. \tag{1}$$

Each element of G can be written in the unique normal form

$$\omega^a X^b Z^c \quad \text{for some integers} \quad a, b, c \in \mathbb{Z}_d := \{0, 1, \ldots, d-1\}.$$

From (1) it is readily seen that

$$(\omega^a X^b Z^c)(\omega^{a'} X^{b'} Z^{c'}) = \omega^{b'c+a+a'} X^{b+b'} Z^{c+c'},$$

where addition and multiplication of exponents can be understood modulo d.

Non-Commutativity

G is a non-commutative group of order d^3. The commutator of two operators W and W' is

$$[W, W'] := WW'W^{-1}W'^{-1}$$

which in our case acquires the form

$$[\omega^a X^b Z^c, \omega^{a'} X^{b'} Z^{c'}] = \omega^{cb'-c'b} I.$$

There are two important normal subgroups of G: its centre $Z(G)$ and its commutator subgroup G', the two being identical

$$Z(G) = G' = \{\omega^a I : a \in \mathbb{Z}_d\}.$$

Main Result

We characterise and enumerate the generalised Pauli operators commuting with a given one in terms of the projective line over the ring of integers modulo d.

Bridging the Gap

The bijective mappings

$$\psi : \mathbb{Z}_d \to G' : a \mapsto \omega^a I,$$

$$\varphi : \mathbb{Z}_d^2 \to G/G' : (b, c) \mapsto G' X^b Z^c.$$

bridge the gap between the generalised Pauli group and the free $\mathbb{Z}_d$-module $\mathbb{Z}_d^2$.

Furthermore, they yield the symplectic bilinear form

$$[\cdot, \cdot] : \mathbb{Z}_d^2 \times \mathbb{Z}_d^2 \to \mathbb{Z}_d : \big((b, c), (b', c')\big) \mapsto cb' - c'b \tag{2}$$

which just describes the commutator of two operators $\omega^a X^b Z^c$ and $\omega^{a'} X^{b'} Z^{c'}$ in terms of our $\mathbb{Z}_d$-module. These operators commute if, and only if, the form value in (2) vanishes or, said differently, if (b, c) and (b', c') are orthogonal.

The Projective Line

Any vector $(b, c) \in \mathbb{Z}_d^2$ generates the cyclic submodule

$$\mathbb{Z}_d(b, c) = \{(ub, uc) : u \in \mathbb{Z}_d\}.$$

Such a cyclic submodule is called a point, if (b, c) is unimodular, i.e., there exist elements $x, y \in \mathbb{Z}_d$ with $bx + cy = 1$. The point set

$$\mathbb{P}(\mathbb{Z}_d) := \{\mathbb{Z}_d(c, d) : (c, d) \text{ is unimodular}\}$$

is the projective line over the ring $\mathbb{Z}_d$.

According to this definition a point is a set of vectors!

Orthogonality

The symplectic form $[\cdot,\cdot]$ remains invariant, to within invertible elements of $\mathbb{Z}_d$, under the natural action of the general linear group $\mathrm{GL}_2(\mathbb{Z}_d)$ on $\mathbb{Z}_d^2$. Hence the orthogonality relation $\perp$ w.r.t. $[\cdot,\cdot]$ is a $\mathrm{GL}_2(\mathbb{Z}_d)$-invariant notion.

Moreover, the projective line $\mathbb{P}(\mathbb{Z}_d)$ equals the orbit of $\mathbb{Z}_d(1,0)$ this action of $\mathrm{GL}_2(\mathbb{Z}_d)$.

Theorem 1. *Let $(b,c)\in\mathbb{Z}_d^2$ be any vector and let $\mathbb{Z}_d(b',c')$ be any point of the projective line $\mathbb{P}(\mathbb{Z}_d)$ which contains the vector (b,c). Then the following assertions hold:*

1. *The point $\mathbb{Z}_d(b',c')$ is a subset of the perp-set $(b,c)^\perp$.*

2. *Under the additional assumption that $\mathbb{Z}_d(b,c)$ is also a point, we have*

$$(b,c)^\perp = \mathbb{Z}_d(b,c) = \mathbb{Z}_d(b',c').$$

Case 1: d is Square-Free

We adopt the assumption that

$$d = p_1 p_2 \cdots p_r,$$

where $p_1, p_2, \ldots, p_r$ are $r \geq 1$ distinct prime numbers. The ring $\mathbb{Z}_d$ can be identified with the direct product

$$\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r}$$

of r finite fields. Any element $y \in \mathbb{Z}_d$ can be written uniquely in the form

$$y = \left(y^{(1)}, y^{(2)}, \ldots, y^{(r)}\right) \quad \text{with} \quad y^{(k)} \in \mathbb{Z}_{p_k}.$$

We refer to the elements $y^{(k)}$ as the components of y.

Case 1: d is Square-Free

Theorem 2. *Let $(b,c) \in \mathbb{Z}_d^2$. We denote by K the set of those indices $k \in \{1,2,\ldots,r\}$ such that $(b^{(k)}, c^{(k)}) = (0,0)$. Then the following assertions hold:*

1. *The vector (b,c) is contained in precisely*

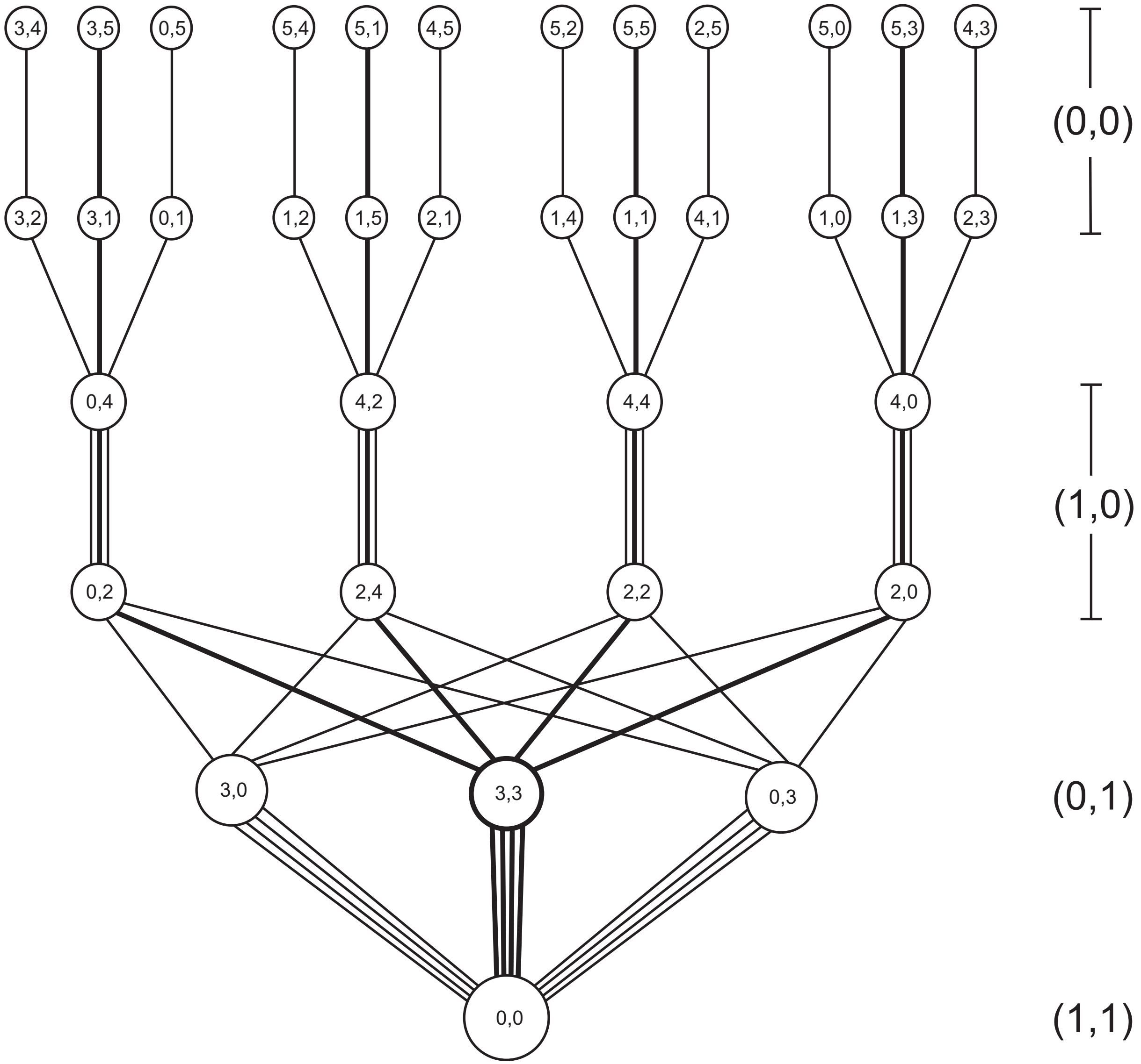
$$\prod_{k \in K} (p_k + 1)$$

   points of the projective line $\mathbb{P}(\mathbb{Z}_d)$.

2. *The set-theoretic union of these points equals $(b,c)^\perp$.*
3. *The perpendicular set of the vector (b,c) satisfies*

$$|(b,c)^\perp| = d \prod_{k \in K} p_k.$$

An Example



The projective line over $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

Case 2: d is a Prime Power

Let $d = p^\varepsilon$, where p is a prime and $\varepsilon \geq 1$ is an integer. The ring $\mathbb{Z}_d$ is local, and its ideals form the chain

$$\mathbb{Z}_d = \mathbb{Z}_d \cdot p^0 \supset \mathbb{Z}_d \cdot p^1 \supset \cdots \supset \mathbb{Z}_d \cdot p^\varepsilon = \{0\}.$$

Let (b, c) be a vector of the $\mathbb{Z}_d$-module $\mathbb{Z}_d^2$. The degree of (b, c) is defined to be

$$\delta \in \{0, 1, \ldots, \varepsilon\}$$

if the ideal of $\mathbb{Z}_d$ generated by $\{b, c\}$ equals $\mathbb{Z}_d \cdot p^\delta$.

Case 2: d is a Prime Power

Theorem 2. *Let (b, c) be a vector of $\mathbb{Z}_d^2$ with degree δ. Then the following hold:*

1. *The number of points of the projective line $\mathbb{P}(\mathbb{Z}_d)$ which contain the vector (b, c) equals*
$$p^{\varepsilon} + p^{\varepsilon-1} \text{ if } \delta = \varepsilon, \quad \text{and} \quad p^{\delta} \text{ if } \delta < \varepsilon.$$
2. *We denote by $U(b, c) \subset \mathbb{Z}_d^2$ the set-theoretic union of all points containing the vector (b, c). Then $U(b, c)$ is a generating set for the submodule $(b, c)^{\perp} \subset \mathbb{Z}_d^2$. Furthermore, the equality*
$$U(b, c) = (b, c)^{\perp}$$
holds if, and only if, one of the following conditions is satisfied:
   - $(b, c) = (0, 0)$.
   - *(b, c) is an admissible pair.*
3. *The perpendicular set of the vector (b, c) satisfies*
$$|(b, c)^{\perp}| = p^{\varepsilon+\delta}.$$

Case 3: d is Arbitrary

Let

$$d = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r},$$

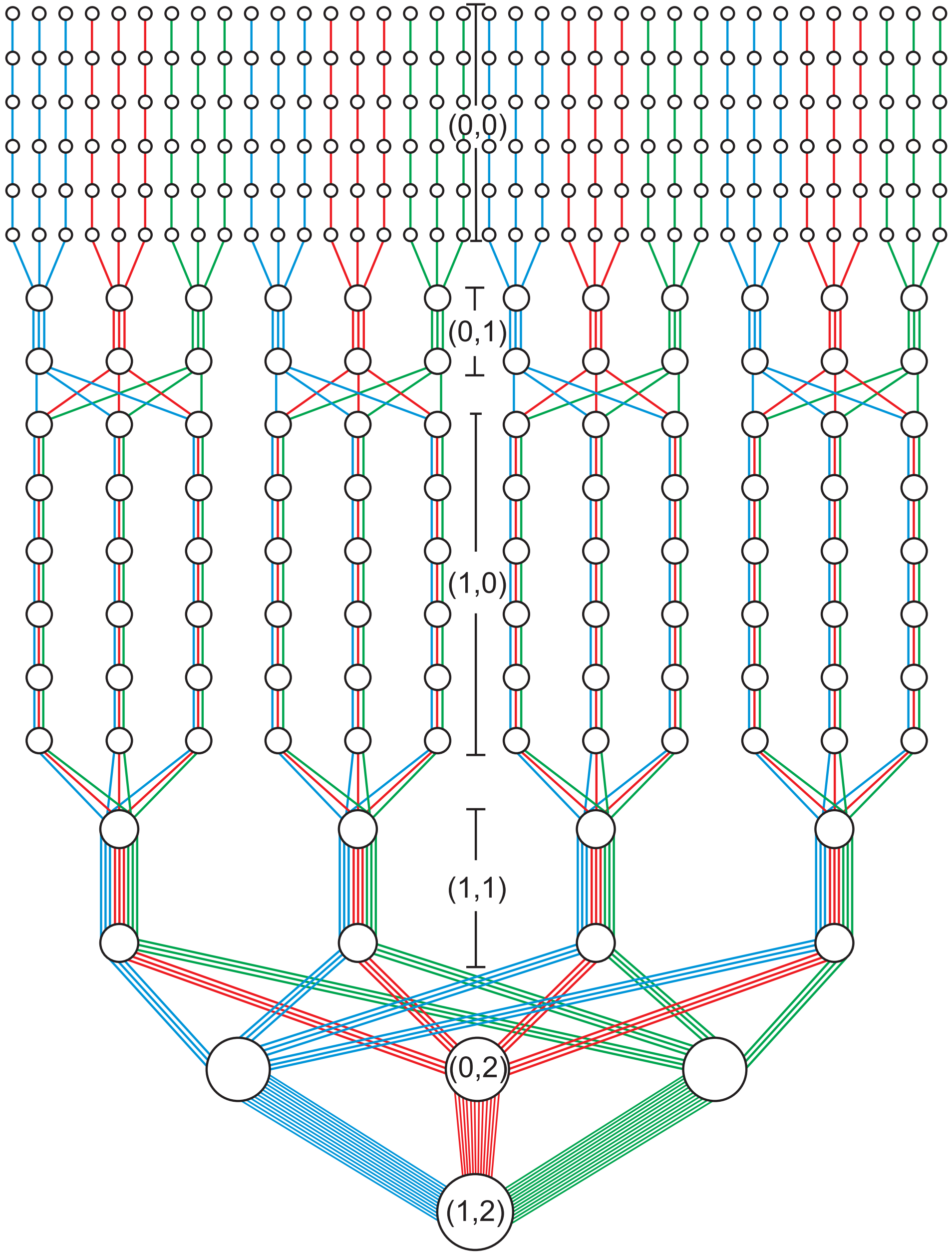
where $p_1, p_2, \ldots, p_r$ are $r \geq 1$ distinct prime numbers, and the exponents $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ are integers ≥ 1.

It is well known that the ring $(\mathbb{Z}_d, +, \cdot)$ is isomorphic to the direct product

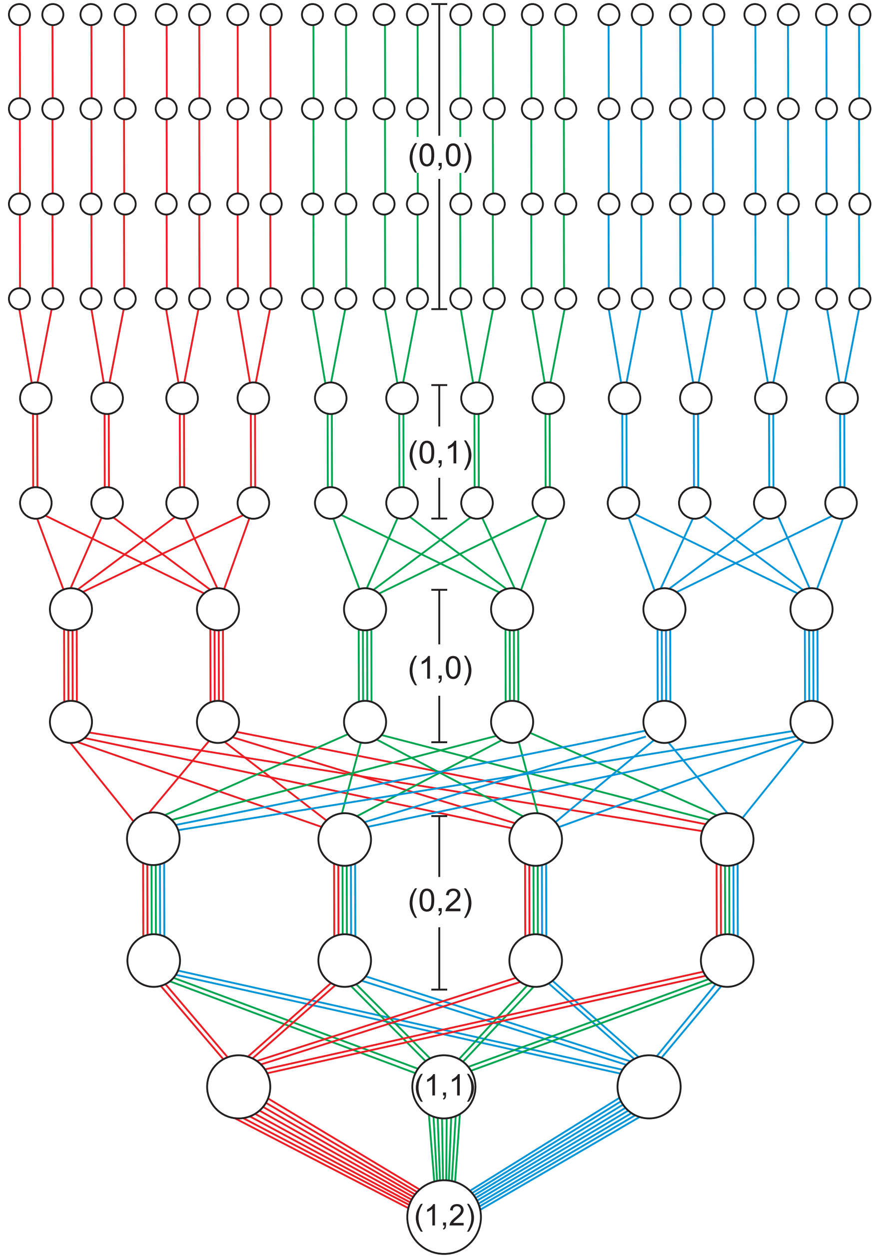
$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \quad \text{where} \quad d_k := p_k^{\varepsilon_k} \quad \text{for all} \quad k \in \{1, 2, \ldots, r\}. \tag{3}$$

This observation allows to apply the results from Case 2 to the components of a vector (b, c), but our explicit formulas turn out to be very technical. In particular, one has to define an r-tuple $(\delta_1, \delta_2, \ldots, \delta_r)$ as the degree of (b, c).

Two Examples



The projective line over $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$



The projective line over $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$

Back to Pauli Operators

Theorem 3. *Let d be arbitrary. The number of operators in the generalised Pauli group G which commute with the operator $\omega^a X^b Z^c \in G$ is equal to*

$$d \cdot |(b, c)^{\perp}| = d^2 \cdot \prod_{k=1}^{r} p_k^{\delta_k}, \tag{4}$$

where $(\delta_1, \delta_2, \ldots, \delta_r)$ is the degree of (b, c).

Final Remarks

We are grateful to Petr Pracna (Prague) for his help in creating the pictures.

References

[1] H. Havlicek and M. Saniga: Projective ring line of a specific qudit, *J. Phys. A* **40** (2007), F943–F952.

[2] H. Havlicek and M. Saniga: Projective ring line of an arbitrary single qudit, *J. Phys. A* **41** (2008), 015302 (12pp).

[3] K. Thas: Pauli operators of N-qubit Hilbert spaces and the Saniga-Planat conjecture, *Chaos, Solitons and Fractals*, in print.

Further references can be found in the cited papers.

[3] contains an important generalisation to multiple qubits.