



HAL
open science

Qudits of composite dimension, mutually unbiased bases and projective ring geometry

Michel R. P. Planat, Anne-Céline Baboin

► **To cite this version:**

Michel R. P. Planat, Anne-Céline Baboin. Qudits of composite dimension, mutually unbiased bases and projective ring geometry. 2007. hal-00172596v1

HAL Id: hal-00172596

<https://hal.science/hal-00172596v1>

Preprint submitted on 17 Sep 2007 (v1), last revised 10 Oct 2007 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Qudits of composite dimension, mutually unbiased bases and projective ring geometry

Michel Planat and Anne-Céline Baboin

Institut FEMTO-ST, CNRS, Département LPMO, 32 Avenue de l'Observatoire
F-25044 Besançon, France

E-mail: michel.planat@femto-st.fr

Abstract. The d^2 Pauli operators attached to a composite qudit in dimension d may be mapped to the vectors of the symplectic module \mathcal{Z}_d^2 (\mathcal{Z}_d the modular ring). As a result, perpendicular vectors correspond to commuting operators, a free cyclic submodule to a maximal commuting set, and disjoint such sets to mutually unbiased bases. For dimensions $d = 6, 10, 15, 12$, and 18 , the fine structure and the incidence between maximal commuting sets is found to reproduce the projective line over the rings $\mathcal{Z}_6, \mathcal{Z}_{10}, \mathcal{Z}_{15}, \mathcal{Z}_6 \times \mathbf{F}_4$ and $\mathcal{Z}_6 \times \mathcal{Z}_3$, respectively.

PACS numbers: 03.67.-a, 03.65.Fd, 02.10.Ox, 02.40.Dr

Summary

The structure of commutation relations between (generalized) Pauli operators provides the skeleton of mutually unbiased bases and quantum entanglement[1, 2]. However an extensive study of them is recent and has mainly been tackled in power of prime dimensions $d = p^N$ [1]-[4], except for the case of the smallest composite dimension $d = 6$ [5]. Commutation relations of two-qubit operators, and dually the incidence relations between maximal commuting sets of them, have been shown to fit the (symplectic) generalized quadrangle of order two, and several projective embeddings have been proposed[2, 6]. For higher dimensions $N > 2$, and for composite dimensions, the duality is lost: the geometrical space of points/observables exhibits several lines/sets passing through n -tuples of distinguished points[5].

Remarkably the incidence between the twelve lines of the sextit system has been shown to fit the grid like structure of the projective line $P_1(\mathcal{Z}_6)$ over the modular ring \mathcal{Z}_6 , but the multiline projective structure of the $d^2 = 36$ Pauli observables (including the unity matrix) has remained elusive[5]. In the higher composite dimensions explored so far $d = 2 \times 5 = 10$, $d = 3 \times 5 = 15$, $d = 2 \times 3^2 = 18$ and $d = 2^2 \times 3 = 12$, the incidence of the maximal commuting sets is found to reproduce the projective line $P_1(\mathcal{R})$ over rings $\mathcal{R} = \mathcal{Z}_{10}$, $\mathcal{R} = \mathcal{Z}_{15}$, $\mathcal{R} = \mathcal{Z}_6 \times \mathcal{Z}_3$ and $\mathcal{R} = \mathcal{Z}_6 \times \mathbf{F}_4$, respectively. The unexpected irruption of the Galois field of four elements \mathbf{F}_4 , within the projective model of the two-qubit/qutrit system, seems to forbid an easy generalization to an arbitrary dimension d .

These numerical findings prompted the authors of [7] to develop a geometrical analysis of the Pauli group G of (generalized) Pauli operators written in normal form $\omega^a X^b Z^c$, where $\omega = \exp(2i\pi/d)$, X and Z are the shift and clock operators, and a , b and c are in the modular ring \mathcal{Z}_d . Another representation of the Pauli group is from tensor products of shift and clock actions in prime dimension [8, 9]. Removing the phase factor ω^a of modulus one, one arrives at the d^2 (including unity matrix) Pauli operators useful in the theory of mutually unbiased bases [9, 10] and used in our previous papers devoted to commutation relations [1]-[5]. This reduction may also be achieved by taking the quotient of G by its center G' (the set of all operators which commute with every other one).

Ref [7] describes the commutation relations between operators in G , and thus in G/G' , using vectors $(b, c) \in \mathcal{Z}_d^2$, their attached cyclic submodule

$$\mathcal{Z}_d(b, c) = \{(ub, uc) : u \in \mathcal{Z}_d\}, \quad (1)$$

and the ‘‘points’’ of the projective line

$$\mathcal{P}_1(\mathcal{Z}_d) = \{\mathcal{Z}_d(b, c) : (b, c) \text{ is admissible}\}. \quad (2)$$

An admissible vector (b, c) is such that there exists another vector (x, y) for which the

matrix $\begin{pmatrix} b & c \\ x & y \end{pmatrix}$ is invertible, which for a commutative ring is equivalent to have a determinant equal to a unit of the ring. The equivalence class of (b, c) is a free cyclic submodule $\mathcal{Z}_d(b, c)$, of order d , and also a “point” of the projective line $\mathcal{P}_1(\mathcal{Z}_d)$.

A crucial tool is the concept of a perpendicular set $(b, c)^\perp$ which is defined as

$$(b, c)^\perp = \{(u, v) \in \mathcal{Z}_d^2 : (b, c) \perp (u, v)\}, \quad (3)$$

in which two vectors (b, c) and (u, v) are perpendicular if $\det \begin{pmatrix} b & c \\ u & v \end{pmatrix} = 0$. Note that two vectors within a cyclic submodule are mutually perpendicular. According to [7], operators in G which commute with a fixed operator correspond to a perpendicular set \ddagger . Using this analogy, it seems natural to identify the elements of a free cyclic submodule, which are mutually perpendicular, with the maximal commuting sets of Pauli operators, as we already did it implicitly in [5]. A posteriori one should not be surprised that the projective line $\mathcal{P}_1(\mathcal{Z}_6)$ fits the incidence relations between the maximal commuting sets of the sextit system. To complete the geometrical picture of commutation relations, one needs to identify the (not necessarily admissible) vectors of \mathcal{Z}_d^2 with the d^2 Pauli operators.

Let us summarize main results of [7]:

Theorem 1 asserts that a free cyclic module $\mathcal{Z}_d(b', c')$ containing a vector (b, c) is contained in the perpendicular set $(b, c)^\perp$. Only if (b, c) is admissible the corresponding module equals $(b, c)^\perp$.

It confornts our interpretation that the maximal sets of mutually commuting operators [corresponding to $\mathcal{Z}_d(b, c)$] also define a base of operators [corresponding to $(b, c)^\perp$]. One immediate consequence concerns the application to mutually unbiased bases. Any two vectors in one base should be perpendicular, while any two vectors from distinct mutually unbiased bases should not. Using two non-zero distinct vectors (b, c) and (b', c') , the two vector sets $\mathcal{Z}_d(b, c)/(0, 0) = \{(ub, uc) : u \in \mathcal{Z}_d^*\}$ and $\mathcal{Z}_d(b', c')/(0, 0) = \{(vb', vc') : v \in \mathcal{Z}_d^*\}$ are disjoint only if $uv(bc' - cb') \neq 0$, i.e. $uv \neq 0$ and (b, c) , (b', c') are not perpendicular. This cannot happen maximally since \mathcal{Z}_d is a ring so that u or v may be zero divisors. The maximal number of mutually unbiased bases in composite dimension may thus be reformulated as being the maximal number of such disjoint vector sets in the relevant ring.

If the dimension d is the power of distinct primes p_k , theorem 2 in [7] provides quantitative results about (a) the number of points n_d in which any vector (b, c) lies, (b) the partitioning of $(b, c)^\perp$ as the corresponding set theoretic union of points $\mathcal{Z}_d(b, c)$ and (c) the cardinality of $(b, c)^\perp$. One gets

$$n_d = \prod_{k \in K} (p_k + 1) \quad \text{and} \quad |(b, c)^\perp| = d \prod_{k \in K} p_k, \quad (4)$$

in which K is a subset of the indices related to the decomposition of the entries of (b, c) into their principal ideals.

\ddagger This notion of perpendicularity related to the commutativity of the operators was already used within the context of symplectic polar spaces as models of N -qubit systems (see [3] and Sec 4.1 of [2]).

Commutation relations of the sextit system

The sextit system ($d = 2 \times 3 = 6$) was investigated in our recent paper [5]. In this dimension, the (generalized) Pauli operators are defined as

$$\sigma_i \otimes \sigma_j, \quad i \in \{0, \dots, 3\}, \quad j \in \{0, \dots, 8\}, \quad (i, j) \neq (0, 0). \quad (5)$$

The orthonormal set of the qubits comprises the standard Pauli matrices $\sigma_i = (I_2, \sigma_x, \sigma_y, \sigma_z)$, where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\sigma_y = i\sigma_x\sigma_z$, while the orthonormal set of the qutrits is taken as

$$\sigma_j = \{I_3, Z, X, Y, V, Z^2, X^2, Y^2, V^2\}, \quad \text{where } I_3 \text{ is the } 3 \times 3 \text{ unit matrix, } Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, Y = XZ, V = XZ^2 \text{ and } \omega = \exp(2i\pi/3).$$

The sextit operators can be conveniently labelled as follows: $1 = I_2 \otimes \sigma_1$, $2 = I_2 \otimes \sigma_2$, \dots , $8 = I_2 \otimes \sigma_8$, $a_0 = \sigma_z \otimes I_2$, $9 = \sigma_z \otimes \sigma_1, \dots$, $b_0 = \sigma_x \otimes I_2$, $17 = \sigma_x \otimes \sigma_1, \dots$, $c_0 = \sigma_y \otimes I_2, \dots$, $32 = \sigma_y \otimes \sigma_8$, in which we singled out the three reference points a_0 , b_0 and c_0 .

Then one can use the strategy already described in [2] for N -qudit systems. The Pauli operators are identified with the vertices of a (Pauli) graph and the mutually commuting operators are identified with the edges. The maximal cliques of the graph correspond to the maximal sets of mutually commuting operators. For the sextit system one gets the twelve sets

$$\begin{aligned} L_1 &= \{1, 5, a_0, 9, 13\}, & L_2 &= \{2, 6, a_0, 10, 14\}, & L_3 &= \{3, 7, a_0, 11, 15\}, & L_4 &= \{4, 8, a_0, 12, 16\}, \\ M_1 &= \{1, 5, b_0, 17, 21\}, & M_2 &= \{2, 6, b_0, 18, 22\}, & M_3 &= \{3, 7, b_0, 19, 23\}, & M_4 &= \{4, 8, b_0, 19, 24\}, \\ N_1 &= \{1, 5, c_0, 25, 29\}, & N_2 &= \{2, 6, c_0, 26, 30\}, & N_3 &= \{3, 7, c_0, 27, 31\}, & N_4 &= \{4, 8, c_0, 28, 32\}. \end{aligned}$$

As emphasized in [5] the incidence between the maximal commuting sets leads to a 3×4 grid-like structure isomorphic to the projective line $P_1(\mathcal{Z}_6)$ over the ring $\mathcal{Z}_6 = \mathcal{Z}_2 \times \mathcal{Z}_3$. A subset of the commutation structure of the operators is illustrated in Fig 1. Let us comment about the relationship between this geometrical representation and the projective one described in the summary. Operators x belonging to the maximal sets are of three distinct types§ (see also Fig 1)

- (i) x is one of the reference points a_0 , b_0 or c_0 , lies in four sets and the number of points commuting with x is $|x^\perp| = 18$,
- (ii) $x \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ lies in three sets and $|x^\perp| = 12$,
- (iii) otherwise x lies in a single set and $|x^\perp| = 6$.

These results clearly fits (4) with $d = 6$, $p_1 = 2$ and $p_3 = 3$.

Analogous results are indeed obtained for square free dimensions $d = 2 \times 5 = 10$ and $d = 3 \times 5 = 15$, so far explored.

§ The perpendicular set x^\perp includes the operator x itself and the unity operator[7]. But for maximal commuting sets one usually ignores the unity operator which commutes with every other operator[2, 9]

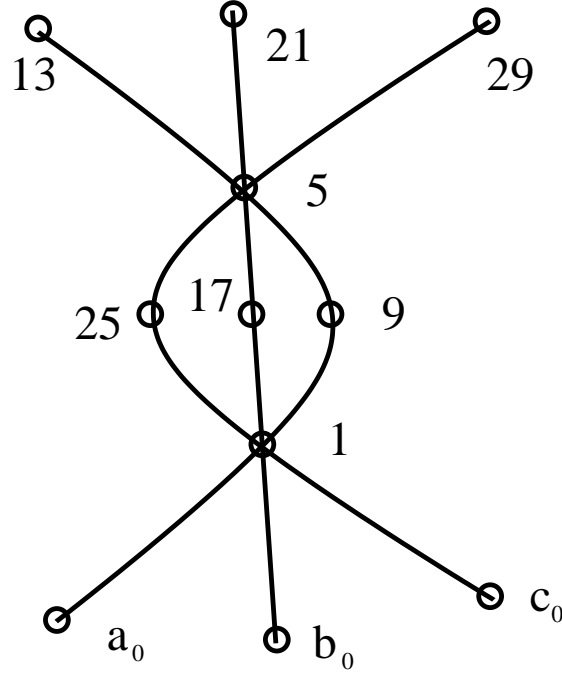


Figure 1. A sketch of a perpendicular set x^\perp attached to a point of type (ii) (see the text for a definition). The whole structure comprises four similar sets having the operators a_0 , b_0 and c_0 in common.

Commutation relations for qudits in dimension twelve

The qudit system in dimension $d = 2^2 \times 3 = 12$ contains the even square 2^2 . In this dimension, the (generalized) Pauli operators are defined as

$$\sigma_i \otimes \sigma_j \otimes \sigma_k, \quad i, j \in \{0, \dots, 3\}, \quad k \in \{0, \dots, 8\}, \quad (i, j, k) \neq (0, 0, 0). \quad (6)$$

One proceeds as for the sextit system, one determines the Pauli graph of the 12-dit and one extracts the maximal cliques. The incidence between the corresponding maximal commuting sets is found to reproduce the projective line over the ring $\mathcal{R} = \mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2} \times \mathbf{F}_{q^2}$, of order $|\mathcal{R}| = (p_1 + 1)(p_2 + 1)(q^2 + 1)$ with $p_1 = q = 2$ and $p_2 = 3$.

Operators x belonging to the maximal sets still are found to be of three distinct types

(i) x is one of the reference points (it includes I_3 in its tensor product), then one finds that x lies in $(p_1 + 1)(p_2 + 1) = 12$ sets and $|x^\perp| = dp_1p_2 = 72$.

(ii) x includes $I_2 \otimes I_2$ in its tensor product, lies in $(p_1 + 1)(q^2 + 1) = 15$ sets and $|x^\perp| = dp_1q = 48$,

(iii) otherwise x lies in $p_1 + 1 = 3$ sets and $|x^\perp| = p_1d = 24$.

The commutation relations within a perpendicular set x^\perp of type (i) are illustrated in Fig 2. It comprises three bundles of four lines each, organized in a parachute like

|| For a classification of projective lines over small commutative rings see Ref [11].

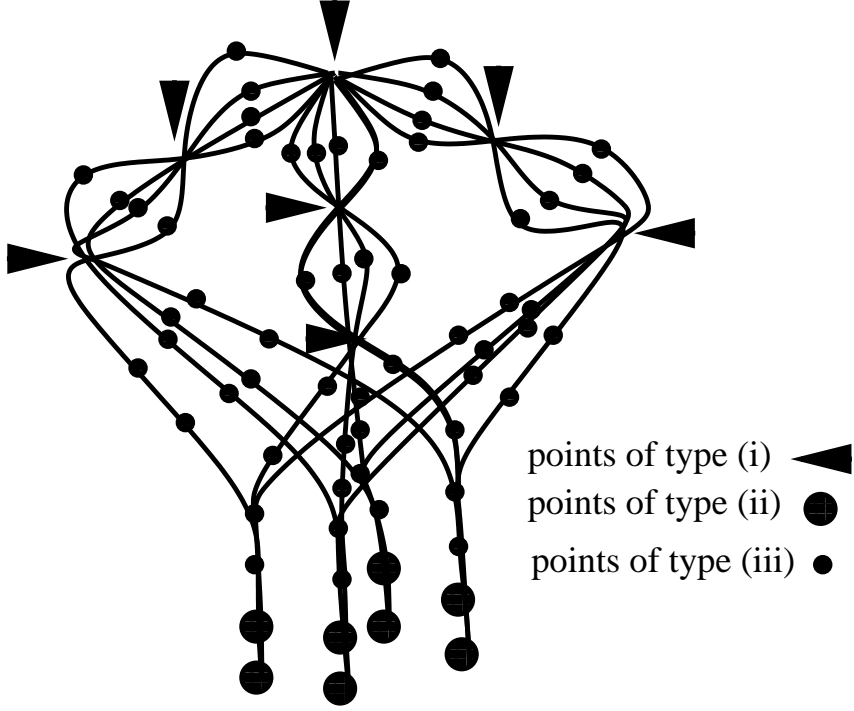


Figure 2. A sketch of a perpendicular set x^\perp (x is the reference point at the top of the parachute like structure. It comprises twelve maximal commuting sets, each one having eleven points (the unity operator is omitted). The three types of points (i), (ii) and (iii) are described in the text.

structure. The lines of a specific bundle intersects at three distinguished points, each one of type (i).

Commutation relations for qudits in dimension eighteen

The qudit system in dimension $d = 2 \times 3^2 = 18$ contains the odd square 3^2 . In this dimension, the (generalized) Pauli operators are defined as

$$\sigma_i \otimes \sigma_j \otimes \sigma_k, \quad i \in \{0, \dots, 3\}, \quad j, k \in \{0, \dots, 8\}, \quad (i, j, k) \neq (0, 0, 0). \quad (7)$$

Again one determines the Pauli graph of the 18-dit and one computes the maximal cliques. The incidence between the corresponding maximal commuting sets is found to reproduce the projective line $P_1(\mathcal{R})$ over the ring $\mathcal{R} = \mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, of order $|\mathcal{R}| = (p_1 + 1)(p_2 + 1)^2$ with $p_1 = 2$ and $p_2 = 3$.

Operators x belonging to the maximal sets are found to be of five distinct types

- (i) x is one of the three reference points containing $I_3 \otimes I_3$ in the tensor decomposition, it lies in $(p_2 + 1)^2 = 16$ sets and $|x^\perp| = dp_2^2 = 162$,
- (ii) x lies in $(p_1 + 1)(p_2 + 1) = 12$ sets and $|x^\perp| = dp_1 p_2 = 108$,
- (iii) x lies in $p_2 + 1 = 4$ sets and $|x^\perp| = dp_2 = 54$,
- (iv) x lies in $p_1 + 1 = 3$ sets and $|x^\perp| = dp_1 p_2 = 108$,

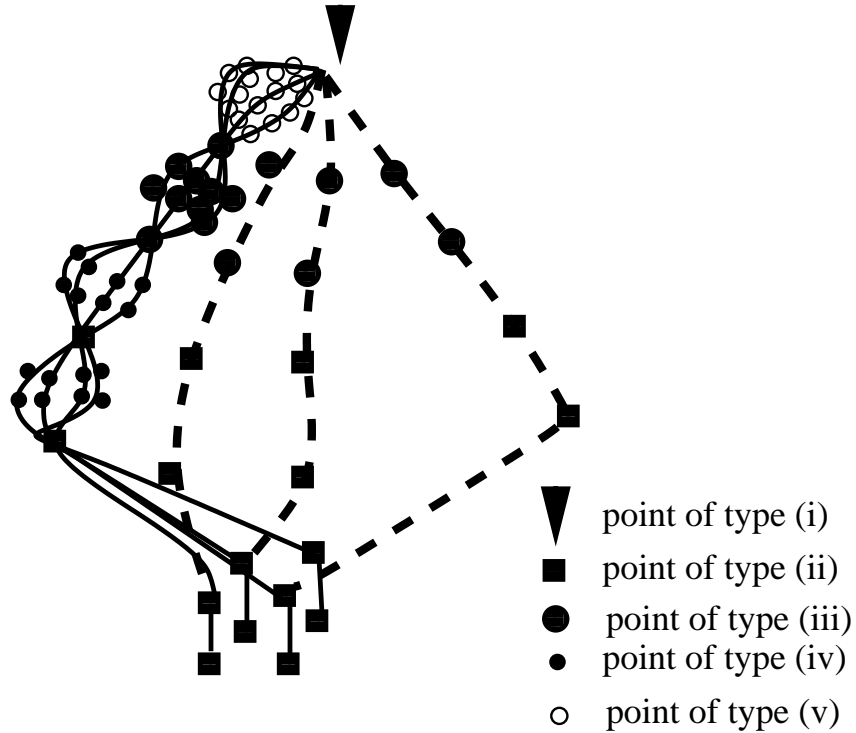


Figure 3. A sketch of a perpendicular set x^\perp (x is the reference point [of type (i)] at the top of the parachute like structure. It comprises sixteen maximal commuting sets, each one having seventeen points (the unity operator is omitted). Only one bundle is represented in detail. The five types of points (i) to (v) are described in the text.

(v) otherwise x lies in a single set and $|x^\perp| = dp_2 = 54$.

The perpendicular set attached to a point of type (i) is illustrated in Fig 3. The fine structure of the bundles increases in complexity compared to Fig 2, each one comprising four lines intersecting at five points, one of type (i), two of type (ii) and the remaining two of type (iii).

Discussion and conclusion

It has been found that commuting operators associated to composite qudits in dimension d correspond to perpendicular vectors within the symplectic module \mathcal{Z}_d^2 . Moreover the maximal commuting sets reflect the set-theoretic structure of free cyclic submodules defined over some commutative ring \mathcal{R} , distinct from the modular ring \mathcal{Z}_d as soon as d contains squares in the prime number decomposition. An admissible vector, which defines such a submodule, is of two types[11] (a) either one (at least) of its entries is a unit of the ring \mathcal{R} , or (b) both of its entries are zero divisors, not in the same maximal ideal of \mathcal{R} . Thus the maximal ideals predermine the projective line[11] and the commutation structure of qudit operators.

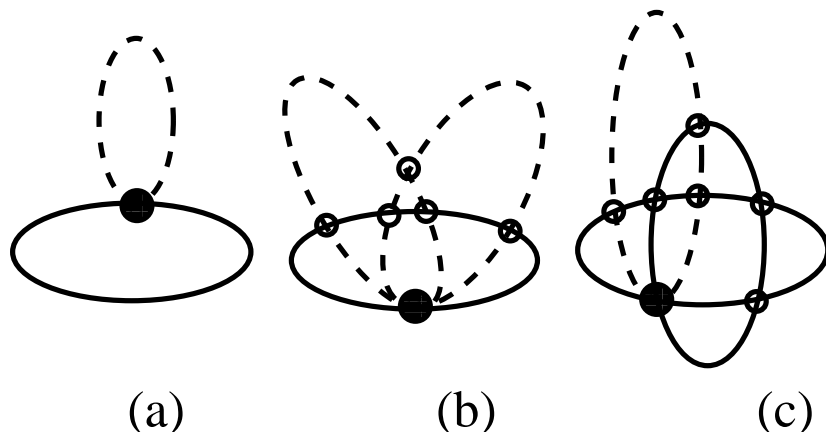


Figure 4. A sketch of the maximal ideals of rings $\mathcal{Z}_2 \times \mathcal{Z}_3$ (illustrating the qubit/qutrit)(a), $\mathcal{Z}_2 \times \mathcal{Z}_3 \times \mathcal{Z}_3$ (illustrating the two-qutrit/qubit) (b) and $\mathcal{Z}_2 \times \mathcal{Z}_3 \times \mathbf{F}_4$ (illustrating the two-qubit/qutrit)(c). The ellipses feature maximal ideals, and their intersection is marked by a small circle; the filled black circle is the zero element of the ring (compare Fig 5 in [1]).

In Fig 4 we give a sketch of the interaction between maximal ideals of the rings $\mathcal{Z}_2 \times \mathcal{Z}_3$ (corresponding to the qubit/qutrit system), $\mathcal{Z}_2 \times \mathcal{Z}_3 \times \mathcal{Z}_3$ (corresponding to the qubit/two-qutrit system) and $\mathcal{Z}_2 \times \mathcal{Z}_3 \times \mathbf{F}_4$ (corresponding to the two-qubit/qutrit system). To some extent one can identify the factors of the qudit system with the maximal ideals, and the peculiar set theoretic union/intersection of them governs the whole commutation structure. The ideals themselves have a ring structure. For example the three ideals in (c) are subsets isomorphic to $\mathcal{Z}_2 \times \mathcal{Z}_3$, $\mathcal{Z}_2 \times \mathbf{F}_4$ and $\mathcal{Z}_3 \times \mathbf{F}_4$ respectively. The corresponding projective lines are 3×4 , 3×5 and 4×5 grids. The last grid exhibits a maximum number of four distant points, corresponding to the maximum number of mutually unbiased bases in dimension twelve.

Further work should clarify whether a ring \mathcal{R} is attached to any composite qubit. This could have application to quantum chemistry[12], quantum channels [13] and the non abelian hidden subgroup problem [14].

Acknowledgments

The authors acknowledge Hans Havlicek, Metod Saniga, Peter Pracna and Maurice Kibler for helpful interactions during the workshop “Finite projective geometries in quantum theory” [<http://www.ta3.sk/msaniga/QuantGeom.htm>], held in Tatranska-Lomnica in august 2007. The work was supported under the ECO-NET project 12651NJ “Geometries over finite rings and the properties of mutually unbiased bases” and the CNRS-SAV project 20246 “Projective and related geometries for quantum information”.

References

- [1] M Planat, M Saniga and M Kibler. Quantum entanglement and projective ring geometry. SIGMA 2006;2:Paper 066.
- [2] M Planat and M Saniga. On the Pauli graphs of N -qudits. Quantum Information and Computation 2008;8:127-146.
- [3] M Saniga and M Planat. Multiple qubits as symplectic polar spaces of order two. Adv Studies Theor Phys 2007;1:1-4.
- [4] H. Havlicek, *A mathematician's insight into the Saniga-Planat theorem*, available on-line from <http://www.geometrie.tuwien.ac.at/havlicek/talks.html>.
- [5] M Planat, A-C Baboin and M Saniga. Multi-line geometry of qubit/qutrit and higher order Pauli operators. Int J Theor Phys 2008; accepted, 0705.2538[quant-ph].
- [6] M Saniga, M Planat, P Pracna and H Havlicek. The Veldkamp space of two-qubits. SIGMA 2007;3:Paper 075.
- [7] H Havlicek and M Saniga. Projective ring line of a specific qudit. Preprint 0708.4333 (quant-ph).
- [8] D Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. Lecture Notes in Computer Science 1998;1509:302-313.
- [9] S Bandyopadhyay, P O Boykin, V Roychowdhury and F. Vatan. A new proof for the existence of MUBs. Algorithmica 2002;34:512-.
- [10] M Planat and H C Rosu. Mutually unbiased phase states, phase uncertainties and Gauss sums. Eur Phys J D 2005;36:133-139.
- [11] M Saniga, M Planat, M R Kibler and P Pracna. A classification of the projective lines over small rings. Chaos, Solitons and Fractals 2007;33:1095-1102.
- [12] O Albouy and M Kibler. SU_2 non standard bases: the case of mutually unbiased bases. SIGMA 2007;3:Paper076.
- [13] M Nathanson and M B Ruskai. Pauli diagonal channels constant on axes. J Phys A: Math Theor 2007;40:8171-8204.
- [14] J Radhakrishnan, M Rötteler and P Sen. On the power of random bases in Fourier sampling: hidden subgroup problem in the Heisenberg group. Lecture Notes in Computer Science 2005;3580:1399-1411.