GEOMETRY OF TWO-QUBITS*

(ICS Praha, January 25, 2007)

METOD SANIGA

Astronomical Institute of the Slovak Academy of Sciences
SK-05960 Tatranská Lomnica, Slovak Republic
(msaniga@astro.sk)

AN OVERVIEW OF THE TALK

1. Introduction

2. Projective Line Over $P_1(M_2(GF(2)))$

- Recalling the Concept of a Projective Ring Line
- Full Matrix Ring $M_2(GF(2)))$ and Its Subrings
- $P_1(M_2(GF(2)))$
- Specific Subconfiguration of $P_1(M_2(GF(2)))$

3. Geometry of Two-Qubits

- "9+6" and "10+5" Factorizations of the Algebra of Pauli Operators
- The Two Factorizations in Terms of Sublines of $P_1(M_2(GF(2)))$
- Generalized Quadrangle of Order Two, $W(2)$
- The Two Factorizations in Terms of Geometric Hyperplanes of $W(2)$
- Correspondence Between the Two Pictures
- Generalizations for N-qubits

4. Conclusion/References

---

*Joint work with **Michel Planat** (FEMTO-ST, Besançon, FR) and **Petr Pracna** (JH-Inst, Prague, CZ)

1. Introduction

- Projective lines defined over finite associative rings with unity/identity have recently been recognized to be an important novel tool for getting a deeper insight into the underlying algebraic geometrical structure of finite dimensional quantum systems.
- As per the two-qubit case, i.e., the set of 15 operators/generalized four-by-four Pauli spin matrices, of particular importance turned out to be the lines defined over the direct product of the simplest Galois fields, $GF(2) \times GF(2) \times \ldots \times GF(2)$.
- Here, the line defined over $GF(2) \times GF(2)$ plays a prominent role in grasping qualitatively the basic structure of so-called Mermin squares, i. e., three-by-three arrays in certain remarkable $9 + 6$ split-ups of the algebra of operators (quant-ph/0603051, quant-ph/0603206), whereas the line over $GF(2) \times GF(2) \times GF(2)$ reflects some of the basic features of a specific $8 + 7$ ("cube-and-kernel") factorization of the set (quant-ph/0605239).
- Motivated by these partial findings, we started our quest for such a ring line that would provide us with a complete picture of the algebra of all the 15 operators/matrices.
- After examining a large number of lines defined over commutative rings (math.AG/0605301, math.AG/0606500), we gradually realized that a proper candidate is likely to be found in the non-commutative domain and this, indeed, turned out to be a right move.
- It is, as we shall demonstrate in what follows, the projective line defined over the full two-by-two matrix ring with entries in $GF(2)$, $M_2(GF(2))$ — the unique simple non-commutative ring of order 16 featuring six units (invertible elements) and ten zero-divisors.

2. Projective Line Over $P_1(M_2(GF(2)))$

Recalling the Concept of a Projective Ring Line

Given

- an associative ring R with unity/identity and
- $GL(2, R)$, the general linear group of invertible two-by-two matrices with entries in R,

a pair $(a, b) \in R^2$ is called admissible over R if there exist $c, d \in R$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, R). \tag{1}$$

The projective line over R, usually denoted as $P_1(R)$, is the set of equivalence classes of ordered pairs $(\varrho a, \varrho b)$, where ϱ is a unit of R and (a, b) is admissible. Two points $X := (\varrho a, \varrho b)$ and $Y := (\varrho c, \varrho d)$ of the line are called *distant* or *neighbor* according as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, R) \quad \text{or} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin GL(2, R), \tag{2}$$

respectively. $GL(2, R)$ has an important property of acting transitively on a set of three pairwise distant points; that is, given any two triples of mutually distant points there exists an element of $GL(2, R)$ transforming one triple into the other.

Full Matrix Ring $M_2(GF(2))$ and Its Subrings

The projective line we are exclusively interested in here is the one defined over the full two-by-two matrix ring with $GF(2)$-valued coefficients, i. e.,

$$R = M_2(GF(2)) \equiv \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha, \beta, \gamma, \delta \in GF(2) \right\}. \tag{3}$$

In an explicit form:

UNITS: Invertible matrices (i. e., matrices with non-zero determinant). They are of two distinct kinds: those which square to 1,

$$1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 2 \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 9 \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad 11 \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{4}$$

and those which square to each other,

$$12 \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad 13 \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{5}$$

ZERO-DIVISORS: Matrices with vanishing determinant. These are also of two different types: *nil*potent, i. e. those which square to zero,

$$3 \equiv \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad 8 \equiv \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad 10 \equiv \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad 0 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \tag{6}$$

and *idem*potent, i. e. those which square to themselves,

$$4 \equiv \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad 5 \equiv \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad 6 \equiv \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad 7 \equiv \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \tag{7}$$

$$14 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad 15 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{8}$$

The structure of this full matrix ring can be well understood from the accompanying colour figure featuring its most important subrings, namely those isomorphic to

- $GF(4)$ (yellow),
- $GF(2)[x]/\langle x^2 \rangle$ (red),
- $GF(2) \otimes GF(2)$ (pink) and to
- the non-commutative ring of 8/6 type (green).

Irrespectively of colour, the dashed/dotted lines join elements represented by upper/lower triangular matrices, while the solid lines link elements represented by "diagonal parity preserving" matrices.

It is worth mentioning a very interesting symmetry of the picture. Namely, the "dpp" ring of 8/6 type (solid green) incorporates both the upper and lower triangular matrix rings isomorphic to $GF(2) \otimes GF(2)$, while, in turn, the "dpp" $GF(2) \otimes GF(2)$ ring (solid pink) is the intersection of the upper and lower triangular matrix rings of 8/6 type.

It is also to be noted that $GF(4)$ has only one representative, the "dpp" set, whereas each of the remaining types have *three* distinct (namely upper and lower triangular, and "dpp") representatives. The shaded circles denote non-trivial idempotents.

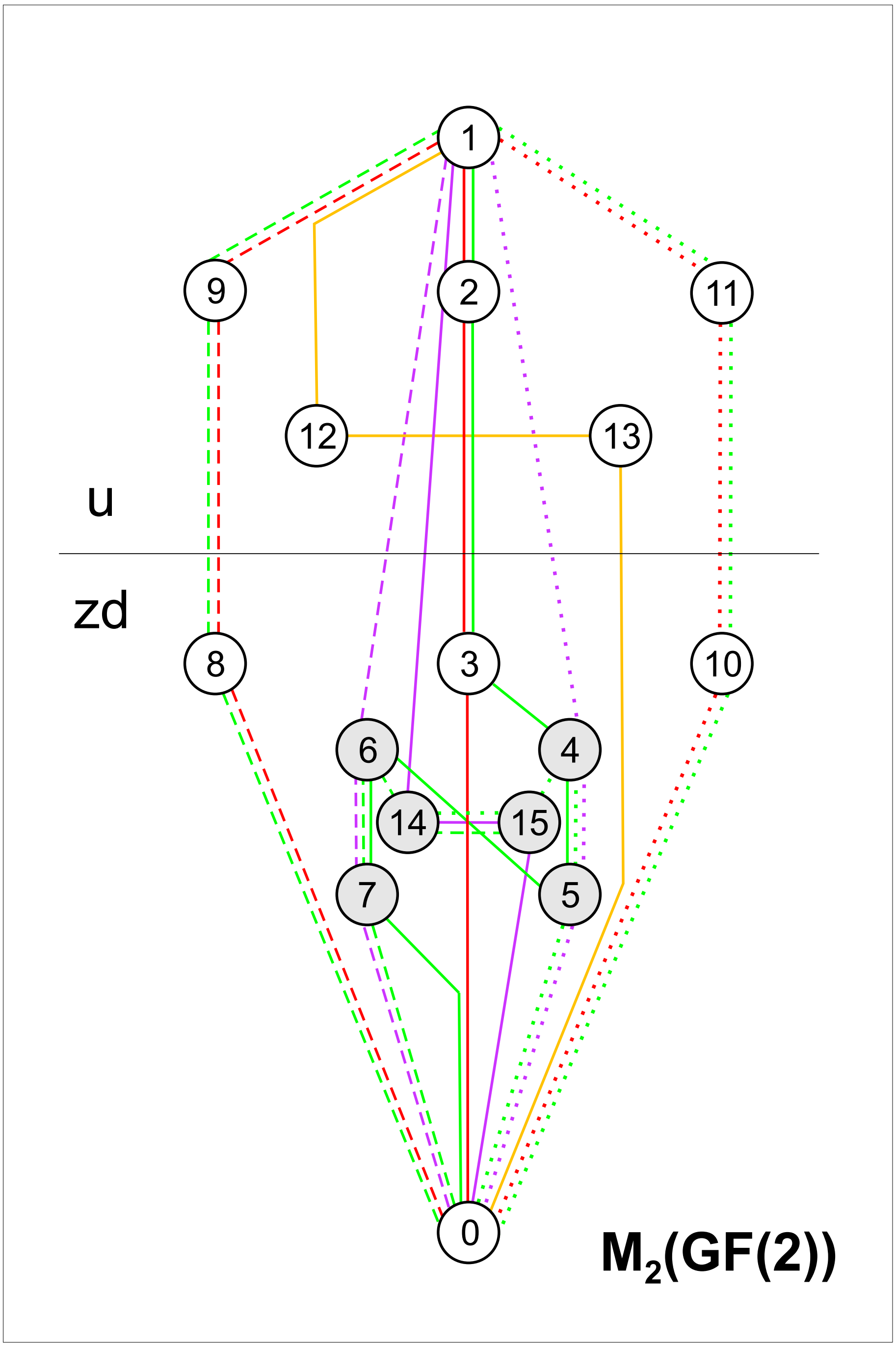

Figure 1: The subrings of $M_2(GF(2))$.

$P_1(M_2(GF(2)))$

Checking first for admissibility (Eq. (1)) and then grouping the admissible pairs left-proportional by a unit into equivalence classes (of cardinality six each), we find that $P_1(M_2(GF(2)))$ possesses altogether 35 points, with the following representatives of each equivalence class:

$$\begin{array}{l}
(1,1),\ (1,2),\ (1,9),\ (1,11),\ (1,12),(1,13),\\
(1,0),\ (1,3),\ (1,4),\ (1,5),\ (1,6),\ (1,7),\ (1,8),\ (1,10),\ (1,14),\ (1,15),\\
(0,1),\ (3,1),\ (4,1),\ (5,1),\ (6,1),\ (7,1),\ (8,1),\ (10,1),\ (14,1),\ (15,1),\\
(3,4),\ (3,10),\ (3,14),\ (5,4),\ (5,10),\ (5,14),\ (6,4),\ (6,10),\ (6,14).
\end{array} \quad (9)$$

From Eqs. (4)–(8) one can easily recognize that the representatives in the first row of the last equation have both entries units (1 being, obviously, unity/multiplicative identity), those of the second and third row have one entry unit(y) and the other a zero-divisor, whilst all pairs in the last row feature zero-divisors in both the entries. At this point we are ready to shown which "portion" of $P_1(M_2(GF(2)))$ is the proper algebraic geometrical setting of two-qubits.

Specific Subconfiguration of $P_1(M_2(GF(2)))$

To this end, we consider two distant points of the line. Taking into account the above-mentioned three-distant-transitivity of $GL(2, R)$, we can take these, without any loss of generality, to be the points $U := (1, 0)$ and $V := (0, 1)$. Next we pick up all those points of the line which are

- either simultaneously distant or
- simultaneously neighbor

to U and V. Employing the left part of Eq. (2), we find the following six points

$$\begin{aligned}
&C_1 = (1, 1),\ C_2 = (1, 2),\ C_3 = (1, 9),\\
&C_4 = (1, 11),\ C_5 = (1, 12),\ C_6 = (1, 13),
\end{aligned} \tag{10}$$

to belong to the first family, whereas the right part of Eq. (2) tells us that the second family comprises the following nine points

$$\begin{aligned}
&C_7 = (3, 4),\ C_8 = (3, 10),\ C_9 = (3, 14),\\
&C_{10} = (5, 4),\ C_{11} = (5, 10),\ C_{12} = (5, 14),\\
&C_{13} = (6, 4),\ C_{14} = (6, 10),\ C_{15} = (6, 14).
\end{aligned} \tag{11}$$

Making again use of Eq. (2), one finds that the points of our special subset of $P_1(M_2(GF(2)))$ are related with each other as shown in Table 2; from this table it can readily be discerned that

- to every point of the configuration there are six neighbor and eight distant points, and that
- the maximum number of pairwise neighbor points is three.

Table 1: The distant and neighbor ("+" and "−", respectively) relation between the points of the configuration. The points are arranged in such a way that the last nine of them (i. e., C_7 to C_{15}) form the projective line over $GF(2) \times GF(2)$.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
C_1	−	−	−	−	+	+	−	+	+	+	−	+	+	+	−
C_2	−	−	+	+	−	−	−	+	+	+	+	−	+	−	+
C_3	−	+	−	+	−	−	+	−	+	−	+	+	+	+	−
C_4	−	+	+	−	−	−	+	+	−	+	−	+	−	+	+
C_5	+	−	−	−	−	+	+	−	+	+	+	−	−	+	+
C_6	+	−	−	−	+	−	+	+	−	−	+	+	+	−	+
C_7	−	−	+	+	+	+	−	−	−	−	+	+	−	+	+
C_8	+	+	−	+	−	+	−	−	−	+	−	+	+	−	+
C_9	+	+	+	−	+	−	−	−	−	+	+	−	+	+	−
C_{10}	+	+	−	+	+	−	−	+	+	−	−	−	−	+	+
C_{11}	−	+	+	−	+	+	+	−	+	−	−	−	+	−	+
C_{12}	+	−	+	+	−	+	+	+	−	−	−	−	+	+	−
C_{13}	+	+	+	−	−	+	−	+	+	−	+	+	−	−	−
C_{14}	+	−	+	+	+	−	+	−	+	+	−	+	−	−	−
C_{15}	−	+	−	+	+	+	+	+	−	+	+	−	−	−	−

The final step is to identify these 15 points with the 15 generalized Pauli matrices/operators of two-qubits in the following way

$$
\begin{aligned}
&C_1 = \sigma_z \otimes \sigma_x,\ C_2 = \sigma_y \otimes \sigma_y,\ C_3 = 1_2 \otimes \sigma_x,\\
&C_4 = \sigma_y \otimes \sigma_z,\ C_5 = \sigma_y \otimes 1_2,\ C_6 = \sigma_x \otimes \sigma_x,\\
&C_7 = \sigma_x \otimes \sigma_z,\ C_8 = \sigma_y \otimes \sigma_x,\ C_9 = \sigma_z \otimes \sigma_y,\\
&C_{10} = \sigma_x \otimes 1_2,\ C_{11} = \sigma_x \otimes \sigma_y,\ C_{12} = 1_2 \otimes \sigma_y,\\
&C_{13} = 1_2 \otimes \sigma_z,\ C_{14} = \sigma_z \otimes \sigma_z,\ C_{15} = \sigma_z \otimes 1_2,
\end{aligned}
\tag{12}
$$

where 1_2 is the 2×2 unit matrix, σ_x, σ_y and σ_z are the classical Pauli matrices and the symbol "$\otimes$" stands for the tensorial product of matrices, in order to readily verify that **Table 2 gives the correct commutation relations between these operators with the symbols "+" and "−" now having the meaning of "non-commuting" and "commuting", respectively.**

3. Geometry of Two-Qubits

"9+6" and "10+5" Factorizations of the Algebra of Pauli Operators

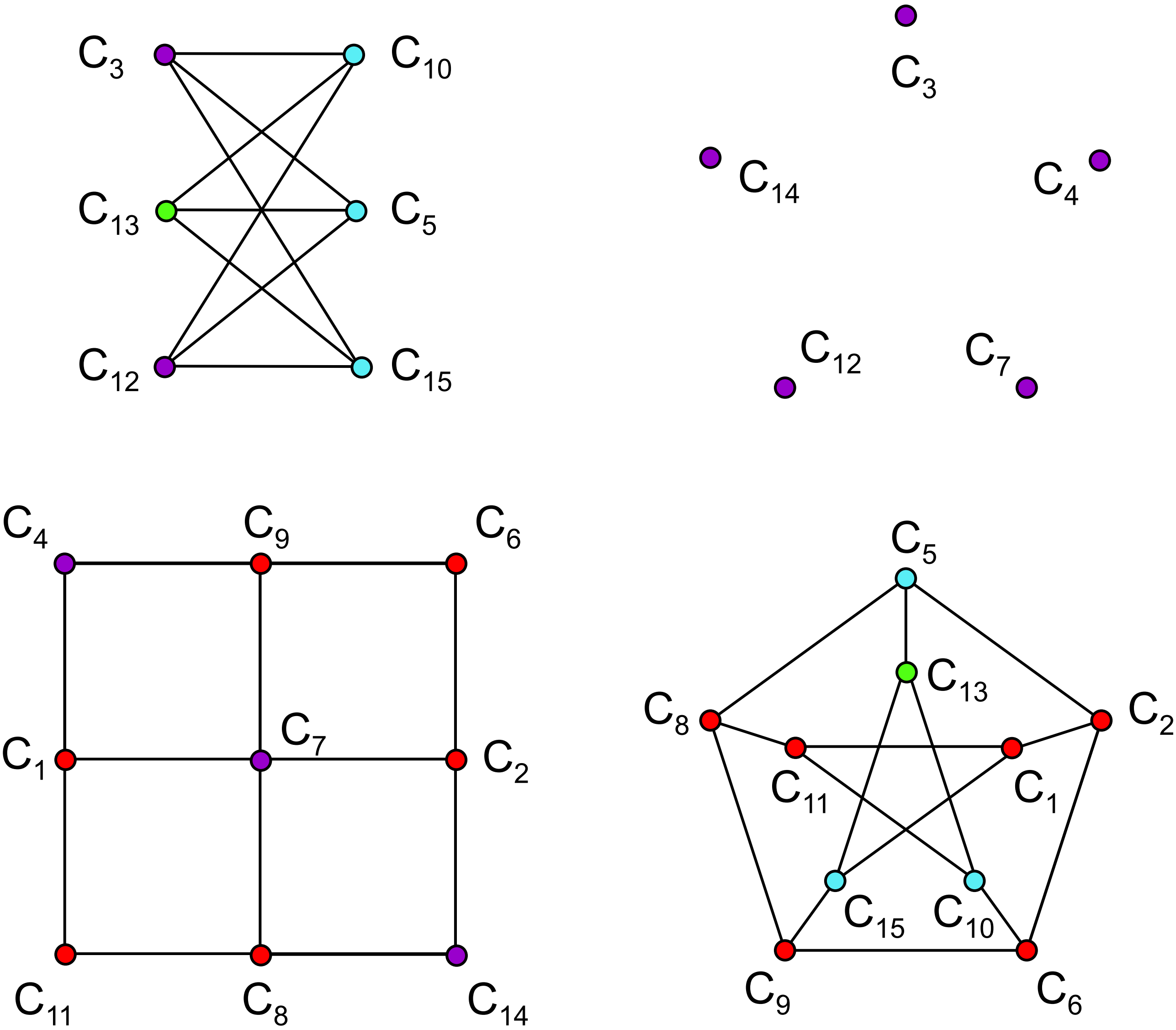

Figure 2:

The two basic factorizations of the algebra of the 15 operators of a two-qubit system. In both the cases, two operators are joined by a line-segment only if they are commute and the color is used to illustrate how the two factorizations relate to each other.

The Two Factorizations in Terms of Sublines of $P_1(M_2(GF(2)))$

The 9+6 factorization (*left*) corresponds geometrically to the split-up of our sub-configuration of $P_1(M_2(GF(2)))$ into

- the projective line over $GF(2) \times GF(2)$ (*bottom*) and
- a couple of projective lines over $GF(4)$ sharing two points (*top*).

The 10+5 one (*right*) corresponds to the partition of the sub-configuration into

- the projective line over $GF(4)$ (*top*) and
- a set of five lines over $GF(2)[x]/\langle x^2 \rangle$ intersecting pairwise in the line over $GF(2)$ (*bottom*).

Generalized Quadrangle of Order Two, $W(2)$

The second interpretation involves a *generalized quadrangle*, a rank two point-line incidence geometry where two points share at most one line and where for any point X and a line $\mathcal{L}$, $X \notin \mathcal{L}$, there exists exactly one line through X which intersect $\mathcal{L}$. The generalized quadrangle associated with our observables is of order two, i. e., the one where every line contains three points and every point is on three lines. Such a quadrangle has, indeed, 15 points (and, because of its self-duality, the same number of lines), each of which is joined by a line with other six — as easily discernible from the following figure:

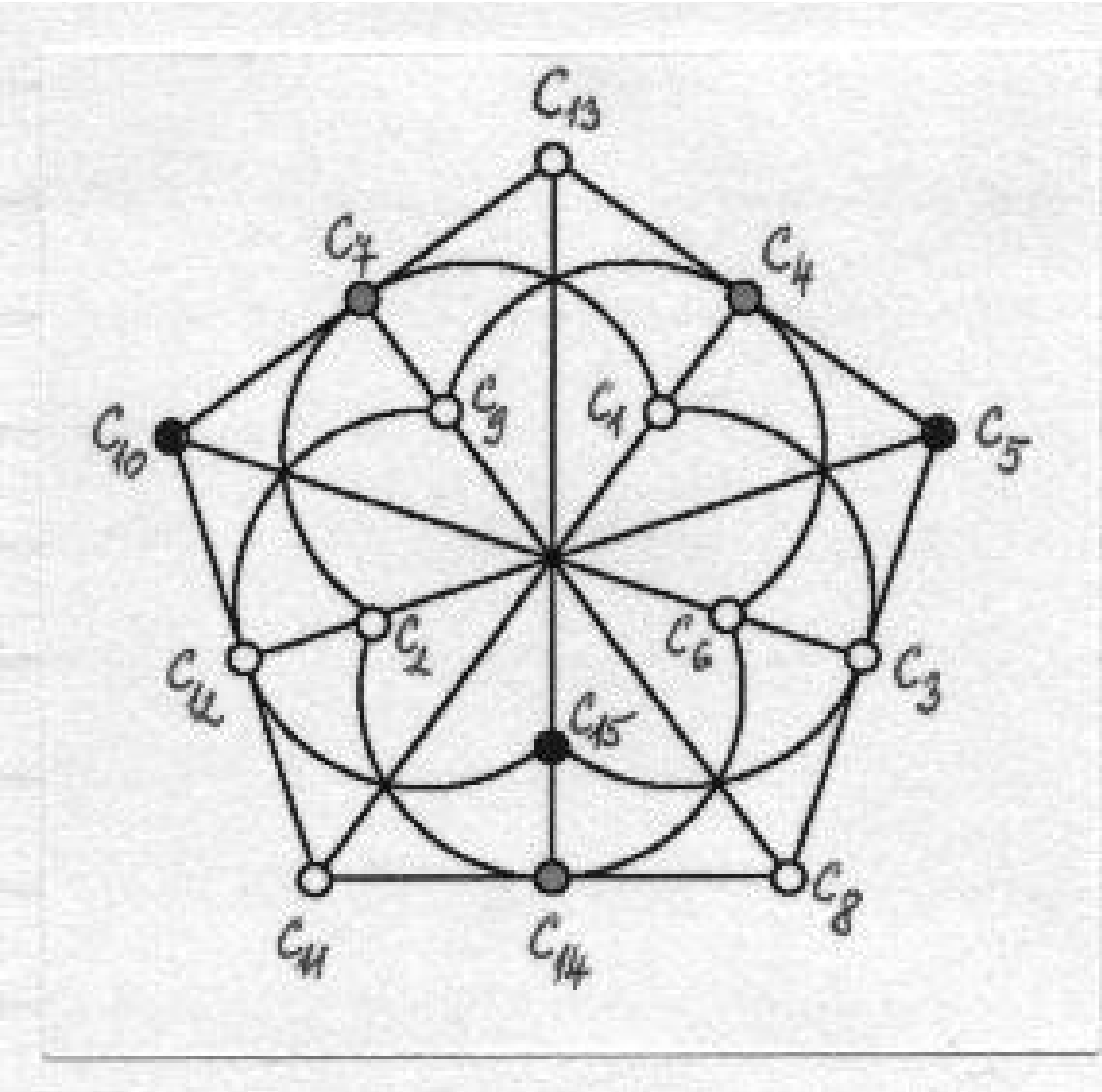

Figure 3:

The Two Factorizations in Terms of Geometric Hyperplanes of $W(2)$

The 9+6 factorization of operators (*left*) now corresponds geometrically to the split-up of the quadrangle of into

- its grid, i.e., a *slim* generalized quadrangle of order $(2, 1)$ (*bottom*) and
- its dual (*top*).

The 10+5 one (*right*) corresponds to the partition of the quadrangle into

- one of its *ovoids*, i. e., a set of (five) points that has exactly one point in common with every line (*top*) and
- the set of ten points that form the famous Petersen graph (*bottom*)

as illustrated in Figure 4:

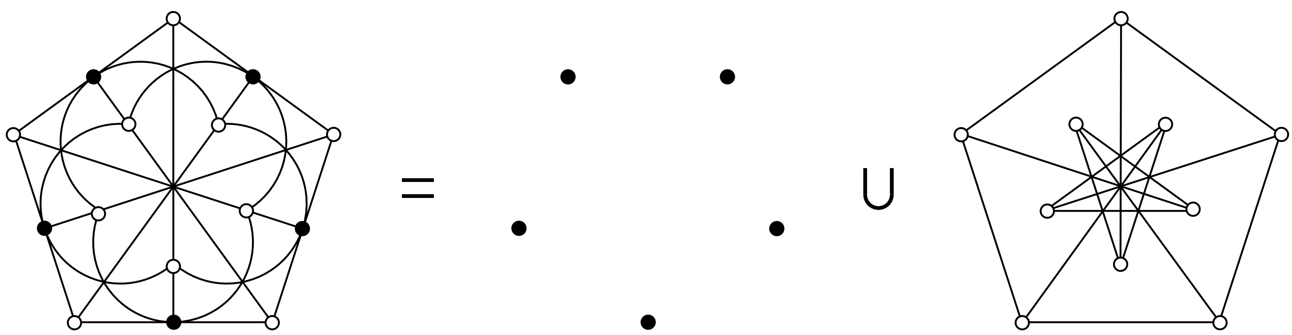

Figure 4:

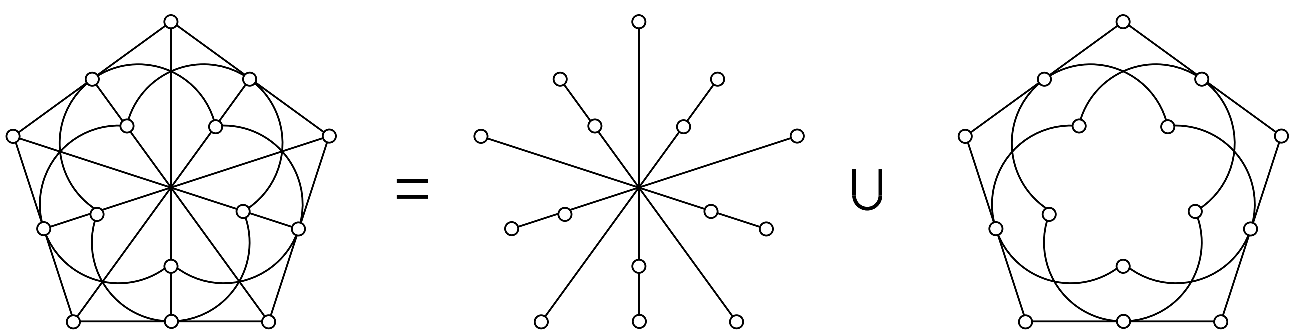

Figure 5:

If, dually, one removes from the quadrangle a *spread*, i. e., a set of (five) pairwise disjoint lines that partition the point set (Fig. 5), one gets the dual of the Petersen graph; five lines of a spread represent nothing but the five maximum subsets of three mutually commuting operators each, whose associated bases are *mutually unbiased*.

Correspondence Between the Two Pictures

A geometric hyperplane H of a finite geometry is a set of points such that every line of the geometry either contains exactly one point of H, or is completely contained in H. It is easy to verify that for the generalized quadrangle of order two H is of one of the following *three* kinds:

- $H_{\rm ov}$, an ovoid (there are six such hyperplanes);
- $H_{\rm cl}(X)$, a set of points collinear with a given point X, the point itself *in*clusive (there are 15 such hyperplanes); and
- $H_{\rm gr}$, a grid as defined above (there are 10 such hyperplanes).

On the other hand, there are, respectively, *three* kinds of the projective lines over the rings of order four and characteristic two living in the projective line $P_1(M_2(GF(2)))$:

- $P_1(GF(4))$;
- $P_1(GF(2)[x]/\langle x^2\rangle)$; and
- $P_1(GF(2) \times GF(2))$.

One thus reveals a perfect parity between the three kinds of the geometric hyperplanes of the generalized quadrangle of order two and the three kinds of the projective lines over the rings of four elements and characteristic two embedded in our sub-configuration of $P_1(M_2(GF(2)))$, giving rise to the three kinds of the distinguished subsets of the Pauli operators of two-qubits, as summarized in Table 2.

Table 2:

GQ	$H_{\rm ov}$	$H_{\rm cl}(X) \setminus \{X\}$	$H_{\rm gr}$
PL	$P_1(GF(4))$	$P_1(GF(2)[x]/\langle x^2\rangle)$	$P_1(GF(2) \times GF(2))$
TQ	set of five mutually non-commuting operators	set of six operators commuting with a given one	nine operators of a Mermin's square

Generalizations for N-qubits

It is surmised (quant-ph/0612179) that the algebra of the Pauli operators on the Hilbert space of N-qubits is embodied in the geometry of the **symplectic polar space of rank N and order two,** $W_{2N-1}(2)$:

- the operators (discarding the identity) answer to the points of $W_{2N-1}(2)$,
- their partitionings into maximally commuting subsets correspond to spreads of the space,
- a maximally commuting subset has its representative in a maximal totally isotropic subspace of $W_{2N-1}(2)$ and, finally,
- "commuting" translates into "collinear" (or "perpendicular").

4. Conclusion

We have demonstrated that the basic properties of a system of two interacting spin-1/2 particles are uniquely embodied in the (sub)geometry of a particular projective line, found to be equivalent to the generalized quadrangle of order two.

As such systems are the simplest ones exhibiting phenomena like quantum entanglement and quantum non-locality and play, therefore, a crucial role in numerous applications like quantum cryptography, quantum coding, quantum cloning/teleportation and/or quantum computing to mention the most salient ones, our discovery thus

- not only offers a principally new geometrically-underlined insight into their intrinsic nature,
- but also gives their applications a wholly new perspective
- and opens up rather unexpected vistas for an algebraic geometrical modelling of their higher-dimensional counterparts.

References

[1] Saniga, M., Planat, M., and Pracna, "Projective Ring Line Encompassing Two-Qubits," Theoretical and Mathematical Physics, submitted, quant-ph/0611063.

[2] Saniga, M., Planat, M., Kibler, M. R., and Pracna, P., "A classification of the projective lines over small rings," Chaos, Solitons & Fractals, accepted, math.AG/0605301.

[3] Saniga, M., and Planat, M., "On the fine structure of the projective line over GF(2) $\otimes$ GF(2) $\otimes$ GF(2)," Chaos, Solitons & Fractals, in press, math.AG/0604307.

[4] Saniga, M., and Planat, M., "The projective line over the finite quotient ring GF(2)$[x]/\langle x^3 - x\rangle$ and quantum entanglement. Theoretical background," Theoretical and Mathematical Physics, accepted, quant-ph/0603051.

[5] Saniga, M., Planat, M., and Minarovjech, M., "The projective line over the finite quotient ring GF(2)$[x]/\langle x^3 - x\rangle$ and quantum entanglement. The Mermin "magic" square/pentagram," Theoretical and Mathematical Physics, accepted, quant-ph/0603206.

[6] Planat, M., Saniga, M., and Kibler, M. R., "Quantum entanglement and finite ring geometry," *SIGMA* **2**, Paper 066 (2006), quant-ph/0605239.

[7] Saniga, M., Planat, M., and Pracna, P., "A classification of the projective lines over small rings II. Non-commutative case," math.AG/0606500.

[8] Polster, B., *A Geometrical Picture Book* (Springer, New York, 1998).

[9] Polster, B., "Pretty pictures of geometries," Bull. Belg. Math. Soc. **5**, 417–425 (1998).

[10] Polster, B., Schroth, A. E., and Van Maldeghem, H., "Generalized flatland," Math. Intelligencer **23**, 33–47 (2001).

[11] Saniga, M., and Planat, M., "Multiple qubits as symplectic polar spaces of order two," quant-ph/0612179.