# PROJECTIVE RING LINE ENCOMPASSING TWO-QUBITS 

M. Saniga, ${ }^{*}$ M. Planat, ${ }^{\dagger}$ and P. Pracna ${ }^{\ddagger}$


#### Abstract

We find that the projective line over the (noncommutative) ring of $2 \times 2$ matrices with coefficients in $G F(2)$ fully accommodates the algebra of 15 operators (generalized Pauli matrices) characterizing twoqubit systems. The relevant subconfiguration consists of 15 points, each of which is either simultaneously distant or simultaneously neighbor to (any) two given distant points of the line. The operators can be identified one-to-one with the points such that their commutation relations are exactly reproduced by the underlying geometry of the points with the ring geometric notions of neighbor and distant corresponding to the respective operational notions of commuting and noncommuting. This remarkable configuration can be viewed in two principally different ways accounting for the basic corresponding $9+6$ and $10+5$ factorizations of the algebra of observables: first, as a disjoint union of the projective line over $G F(2) \times G F(2)$ (the "Mermin" part) and two lines over GF(4) passing through the two selected points that are omitted; second, as the generalized quadrangle of order two with its ovoids and/or spreads corresponding to (maximum) sets of five mutually noncommuting operators and/or groups of five maximally commuting subsets of three operators each. These findings open unexpected possibilities for an algebro-geometric modeling of finite-dimensional quantum systems and completely new prospects for their numerous applications.


Keywords: projective ring line, generalized quadrangle of order two, two-qubit
Projective lines defined over finite associative rings with unity (identity transformation) [1]-[7] have recently been recognized as an important new tool for obtaining a deeper insight into the underlying algebrogeometric structure of finite-dimensional quantum systems [8]-[10]. In the two-qubit case, i.e., the set of 15 operators or generalized $4 \times 4$ Pauli spin matrices, we find that the lines defined over the direct product of the simplest Galois fields, $G F(2) \times G F(2) \times \cdots \times G F(2)$, are particularly important. In this case, the line defined over $G F(2) \times G F(2)$ plays a prominent role in qualitatively understanding the basic structure of the so-called Mermin's squares [9], [10], i.e., three-by-three arrays in certain remarkable $9+6$ factorizations of the algebra of operators, while the line over $G F(2) \times G F(2) \times G F(2)$ reflects some of the basic features of a specific $8+7$ ("cube and kernel") factorization of the set [10]. Motivated by these partial findings, we began to seek a ring line that would provide a complete picture of the algebra of all 15 operators (matrices). Examining a sufficiently large number of lines defined over commutative rings [6], [7], we gradually realized that a proper candidate is likely to be found in the noncommutative domain, and this indeed turned out to be correct. As we demonstrate in sufficient detail, the sought line is the projective line defined over the full $(2 \times 2)$-matrix ring with entries in $G F(2)$, the unique simple noncommutative ring of order 16 with six units (invertible elements) and ten zero divisors [11]. Preferring the conceptual to the formal side of the

[^0]Translated from Teoreticheskaya i Matematicheskaya Fizika, Vol. 155, No. 3, pp. 463-473, June, 2008. Original article submitted December 12, 2006; revised March 20, 2007.
task, we try to reduce the technicalities of the exposition to a minimum, instead referring the interested reader to the relevant literature.

We first recall the concept of a projective ring line [1]-[7]. Given an associative ring $R$ with unity [12][14], we consider the group $G L(2, R)$, the general linear group of invertible $2 \times 2$ matrices with entries in $R$. A pair $(a, b) \in R^{2}$ is said to be admissible over $R$ if there exist $c, d \in R$ such that

$$
\left(\begin{array}{ll}
a & b  \tag{1}\\
c & d
\end{array}\right) \in G L(2, R)
$$

The projective line over $R$, usually denoted by $P_{1}(R)$, is the set of equivalence classes of ordered pairs $(\varrho a, \varrho b)$, where $\varrho$ 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 said to be respectively distant or neighbor if

$$
\left(\begin{array}{ll}
a & b  \tag{2}\\
c & d
\end{array}\right) \in G L(2, R) \quad \text { or } \quad\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right) \notin G L(2, R)
$$

The group $G L(2, R)$ has an important property of acting transitively on a set of three pairwise-distant points, i.e., for any two triples of mutually distant points, there exists an element of $G L(2, R)$ transforming one triple into the other.

We here study only the projective line defined over the full $(2 \times 2)$-matrix ring with $G F(2)$-valued coefficients, i.e.,

$$
R=M_{2}(G F(2)) \equiv\left\{\left.\left(\begin{array}{cc}
\alpha & \beta  \tag{3}\\
\gamma & \delta
\end{array}\right) \right\rvert\, \alpha, \beta, \gamma, \delta \in G F(2)\right\}
$$

Labeling these matrices as

$$
\begin{array}{llll}
1 \equiv\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right), & 2 \equiv\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right), & 3 \equiv\left(\begin{array}{ll}
1 & 1 \\
1 & 1
\end{array}\right), & 4 \equiv\left(\begin{array}{ll}
0 & 0 \\
1 & 1
\end{array}\right) \\
5 \equiv\left(\begin{array}{ll}
1 & 0 \\
1 & 0
\end{array}\right), & 6 \equiv\left(\begin{array}{ll}
0 & 1 \\
0 & 1
\end{array}\right), & 7 \equiv\left(\begin{array}{ll}
1 & 1 \\
0 & 0
\end{array}\right), & 8 \equiv\left(\begin{array}{ll}
0 & 1 \\
0 & 0
\end{array}\right) \\
9 \equiv\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right), & 10 \equiv\left(\begin{array}{ll}
0 & 0 \\
1 & 0
\end{array}\right), & 11 \equiv\left(\begin{array}{ll}
1 & 0 \\
1 & 1
\end{array}\right), & 12 \equiv\left(\begin{array}{ll}
0 & 1 \\
1 & 1
\end{array}\right)  \tag{4}\\
13 \equiv\left(\begin{array}{ll}
1 & 1 \\
1 & 0
\end{array}\right), & 14 \equiv\left(\begin{array}{ll}
0 & 0 \\
0 & 1
\end{array}\right), & 15 \equiv\left(\begin{array}{ll}
1 & 0 \\
0 & 0
\end{array}\right), & 0 \equiv\left(\begin{array}{ll}
0 & 0 \\
0 & 0
\end{array}\right)
\end{array}
$$

we can explicitly verify that addition and multiplication in $M_{2}(G F(2))$ is performed as shown in Table 1 (see pp. 433,531 in [15]). First checking admissibility (1) and then grouping the admissible pairs left-proportional by a unit into equivalence classes (of cardinality six each), we find that the line ${ }^{1} P_{1}\left(M_{2}(G F(2))\right)$ has 35 points altogether, with the following representatives of each equivalence class (see [6]-[8] for more details about this methodology and a number of illustrative examples of a projective ring line):

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

[^1]It can be easily seen from the multiplication table that the representatives in the first row of (5) contain two units ( 1 itself is obviously unity), the representations in the second and third rows contain one unit and one zero divisor, and the representatives in the last row contain two zero divisors.

Table 1

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 | 9 | 8 | 11 | 10 | 13 | 12 | 15 | 14 |
| 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | 10 | 11 | 8 | 9 | 14 | 15 | 12 | 13 |
| 3 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 11 | 10 | 9 | 8 | 15 | 14 | 13 | 12 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 12 | 13 | 14 | 15 | 8 | 9 | 10 | 11 |
| 5 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 | 13 | 12 | 15 | 14 | 9 | 8 | 11 | 10 |
| 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | 14 | 15 | 12 | 13 | 10 | 11 | 8 | 9 |
| 7 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 |
| 8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 8 | 11 | 10 | 13 | 12 | 15 | 14 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| 10 | 10 | 11 | 8 | 9 | 14 | 15 | 12 | 13 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 11 | 11 | 10 | 9 | 8 | 15 | 14 | 13 | 12 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| 12 | 12 | 13 | 14 | 15 | 8 | 9 | 10 | 11 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 13 | 13 | 12 | 15 | 14 | 9 | 8 | 11 | 10 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| 14 | 14 | 15 | 12 | 13 | 10 | 11 | 8 | 9 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| 15 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| $\times$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 | 0 | 2 | 1 | 3 | 7 | 5 | 6 | 4 | 14 | 12 | 15 | 13 | 9 | 11 | 8 | 10 |
| 3 | 0 | 3 | 3 | 0 | 3 | 0 | 0 | 3 | 6 | 5 | 5 | 6 | 5 | 6 | 6 | 5 |
| 4 | 0 | 4 | 4 | 0 | 4 | 0 | 0 | 4 | 14 | 10 | 10 | 14 | 10 | 14 | 14 | 10 |
| 5 | 0 | 5 | 6 | 3 | 0 | 5 | 6 | 3 | 6 | 3 | 0 | 5 | 6 | 3 | 0 | 5 |
| 6 | 0 | 6 | 5 | 3 | 3 | 5 | 6 | 0 | 0 | 6 | 5 | 3 | 3 | 5 | 6 | 0 |
| 7 | 0 | 7 | 7 | 0 | 7 | 0 | 0 | 7 | 8 | 15 | 15 | 8 | 15 | 8 | 8 | 15 |
| 8 | 0 | 8 | 15 | 7 | 7 | 15 | 8 | 0 | 0 | 8 | 15 | 7 | 7 | 15 | 8 | 0 |
| 9 | 0 | 9 | 13 | 4 | 3 | 10 | 14 | 7 | 8 | 1 | 5 | 12 | 11 | 2 | 6 | 15 |
| 10 | 0 | 10 | 14 | 4 | 0 | 10 | 14 | 4 | 14 | 4 | 0 | 10 | 14 | 4 | 0 | 10 |
| 11 | 0 | 11 | 12 | 7 | 4 | 15 | 8 | 3 | 6 | 13 | 10 | 1 | 2 | 9 | 14 | 5 |
| 12 | 0 | 12 | 11 | 7 | 3 | 15 | 8 | 4 | 14 | 2 | 5 | 9 | 13 | 1 | 6 | 10 |
| 13 | 0 | 13 | 9 | 4 | 7 | 10 | 14 | 3 | 6 | 11 | 15 | 2 | 1 | 12 | 8 | 5 |
| 14 | 0 | 14 | 10 | 4 | 4 | 10 | 14 | 0 | 0 | 14 | 10 | 4 | 4 | 10 | 14 | 0 |
| 15 | 0 | 15 | 8 | 7 | 0 | 15 | 8 | 7 | 8 | 7 | 0 | 15 | 8 | 7 | 0 | 15 |
| $A d$ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Addition (top) and multiplication (bottom) in $M_{2}(G F(2))$.
Already at this stage, we can show which "portion" of $P_{1}\left(M_{2}(G F(2))\right)$ is the proper algebro-geometric setting for two-qubits. We consider two distant points on the line. Taking the abovementioned three-distant-transitivity of $G L(2, R)$ into account, we can choose the points $U:=(1,0)$ and $V:=(0,1)$ without loss of generality. We next gather all those points on the line that are either simultaneously distant or simultaneously neighbor to $U$ and $V$. From the first condition in (2), we find that the six points

$$
\begin{array}{lll}
C_{1}=(1,1), & C_{2}=(1,2), & C_{3}=(1,9), \\
C_{4}=(1,11), & C_{5}=(1,12), & C_{6}=(1,13) \tag{6}
\end{array}
$$

belong to the first family, and from the second condition in (2), we find that the nine points

$$
\begin{array}{lll}
C_{7}=(3,4), & C_{8}=(3,10), & C_{9}=(3,14) \\
C_{10}=(5,4), & C_{11}=(5,10), & C_{12}=(5,14)  \tag{7}\\
C_{13}=(6,4), & C_{14}=(6,10), & C_{15}=(6,14)
\end{array}
$$

belong to the second family. Again using (2), we find that the points of our special subset of $P_{1}\left(M_{2}(G F(2))\right)$ are related to each other as shown in Table 2. It can easily seen from this table that each point of the configuration has six neighbor and eight distant points and that the maximum number of pairwise-neighbor points is three.

Table 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 distant and neighbor relations (respectively + and - ) between the points of the configuration. The points are arranged such that the last nine of them (i.e., $C_{7}$ to $C_{15}$ ) form the projective line over $G F(2) \times G F(2)$ (see [8]-[10]).

The final step is to identify these 15 points with the 15 generalized Pauli matrices (operators of twoqubits; see, e.g., Eq. (1) in [10]) by

$$
\begin{array}{lll}
C_{1}=\sigma_{z} \otimes \sigma_{x}, & C_{2}=\sigma_{y} \otimes \sigma_{y}, & C_{3}=1_{2} \otimes \sigma_{x} \\
C_{4}=\sigma_{y} \otimes \sigma_{z}, & C_{5}=\sigma_{y} \otimes 1_{2}, & C_{6}=\sigma_{x} \otimes \sigma_{x} \\
C_{7}=\sigma_{x} \otimes \sigma_{z}, & C_{8}=\sigma_{y} \otimes \sigma_{x}, & C_{9}=\sigma_{z} \otimes \sigma_{y}  \tag{8}\\
C_{10}=\sigma_{x} \otimes 1_{2}, & C_{11}=\sigma_{x} \otimes \sigma_{y}, & C_{12}=1_{2} \otimes \sigma_{y} \\
C_{13}=1_{2} \otimes \sigma_{z}, & C_{14}=\sigma_{z} \otimes \sigma_{z}, & C_{15}=\sigma_{z} \otimes 1_{2}
\end{array}
$$

where $1_{2}$ is the $2 \times 2$ unit matrix, $\sigma_{x}, \sigma_{y}$, and $\sigma_{z}$ are the classical Pauli matrices, and the symbol $\otimes$ denotes the tensor product of matrices. We can now easily verify that Table 2 gives the correct commutation relations


Fig. 1. The two basic factorizations of the algebra of the 15 observables (operators) of a two-qubit system. A $9+6$ factorization ( $a, c$ ) corresponds geometrically to the disjunction of our subconfiguration of $P_{1}\left(M_{2}(G F(2))\right)$ into (c) the projective line over $G F(2) \times G F(2)$ and (a) a couple of projective lines over $G F(4)$ with two points in common. A $10+5$ factorization $(b, d)$, as is also shown differently in Fig. 2, corresponds to the partition of the generalized quadrangle into (b) one of its ovoids and (d) the Petersen graph. In both the cases, two points (observables) are joined by a line segment only if they are neighbor (commute); but to avoid crowding the figure, we omit the edges between the points (observables) of two distinct factors. Color (see the on-line version) is used to illustrate how the two factorizations relate to each other.
between these operators with the symbols + and - now having the respective meanings "noncommuting" and "commuting." In other words, the same "incidence matrix" (given in Table 2) pertains to two distinct configurations of completely different origins: a set of points of the projective line over a particular finite ring with the symbols + and - having the algebro-geometric meanings distant and neighbor and also a set of operators in four-dimensional Hilbert space with the same symbols acquiring the respective operatorial meanings "noncommuting" and "commuting."

This remarkable configuration can be interpreted in two principally different ways, which respectively account for the basic $9+6$ and $10+5$ factorizations of the algebra of observables (Figs. $1 a, 1 c$ and $1 b, 1 d$ ). The first factorization is simply a disjoint union of the projective line over $G F(2) \times G F(2)$ and two lines over $G F(4)$ passing through the two selected points $U$ and $V$, which are omitted. As shown in detail in [9], [10], the line over $G F(2) \times G F(2)$ underlies the qualitative structure of Mermin's magic squares, i.e., $3 \times 3$ arrays of nine observables commuting pairwise in each row and column and arranged such that their product properties contradict those of the assigned eigenvalues. The two lines over $G F(4)$ represent


Fig. 2. The generalized quadrangle of order two (left) and its factorization into an ovoid (middle) and the "Petersen" part (right). The lines of the quadrangle are illustrated by straight segments and also arcs of circles. We note that not every intersection of two segments counts for a point of the quadrangle.
the remaining, bipartite part of the disjunction, where three points (observables) on each of the lines are mutually distant (noncommuting) and every point (observable) on one line is neighbor to (commutes with) any point (observable) on the other line (see Fig. 1a).

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 $X$ that intersects $\mathcal{L}$ [16]-[20]. 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 indeed has 15 points (and the same number of lines because of its self-duality), each of which is joined by lines to six others (Fig. 2, left). If we remove one of the ovoids from this quadrangle, i.e., remove a set of (five) points that has exactly one point in common with every line (Fig. 2, middle), then ten points remain forming the famous Petersen graph (Fig. 2, right) [19], [20]. The five points of an ovoid correspond to the five mutually distant points of $P_{1}(G F(4))$ and correspondingly to the five (i.e., the maximum number of) mutually noncommuting observables of two-qubits. If we remove a spread from the quadrangle, i.e., remove the dual set of (five) pairwise disjoint lines that partition the point set, then we obtain the dual of the Petersen graph (Fig. 3). The five lines of a spread correspond to just the five maximum subsets of three mutually commuting operators each. As we will show in a separate paper, the five lines of any such spread carry maximally commuting subsets of operators whose associated bases are mutually unbiased [10], [21]. This means that the existence and cardinality of a spread in the generalized quadrangle is synonymous with the existence and cardinality of the maximum set of mutually unbiased bases in the associated Hilbert space.

Hence, this geometric approach, when it is properly generalized to higher-order qubits and qudits, provides a unique new tool for addressing the question of the maximum number of mutually unbiased bases in a finite-dimensional Hilbert space, which is still a difficult open problem in the case where this dimension is not a power of a prime. It is a straightforward exercise to associate the points of the quadrangle with the operators (observables) $C_{i}$ (see (8)) such that Table 2 is recovered after substituting the - or + symbol for any two points of the quadrangle that are or are not on a common line.

To complete this interesting algebro-geometric picture of two-qubits, one more important geometric object remains to be introduced. The attentive reader might have noticed that we have already used two different kinds of the projective lines defined over rings of order four and characteristic two, i.e., the line defined over the field $G F(4)$ and the line defined over the direct product ring $G F(2) \times G F(2)$. The former was seen to correspond to an ovoid of the generalized quadrangle and also to a set of five mutually noncommuting operators (Fig. 1b), while the latter corresponds to a grid of nine points on six lines ${ }^{2}$ and

[^2]

Fig. 3. A dual view of the generalized quadrangle of order two (left) as a disjoint union of one of its spreads (middle) and a dual of the Petersen graph or a two-spread (right).
also to a Mermin's square of operators (Fig. 1c). But there is one more associative ring with unity of order four and characteristic two, namely, the (local) factor ring of polynomials $G F(2)[x] /\left\langle x^{2}\right\rangle[12]-[14]$. This ring is also a subring of $M_{2}(G F(2))$, and the corresponding projective line is also expected to play a role in our model. And this is indeed the case. As demonstrated, for example, in Table 3 in [6], the projective line $P_{1}\left(G F(2)[x] /\left\langle x^{2}\right\rangle\right)$ has six points any of which is neighbor to one and distant to the remaining four points, thus comprising three pairs of neighbors. In the set of Pauli operators, this configuration is present as the sextuple of operators commuting with a given operator. If $C_{13}$, for example, is taken as the given operator, then the six operators in question, as can be easily seen from Table 2 , are $\left\{C_{4}, C_{5} ; C_{7}, C_{10} ; C_{14}, C_{15}\right\}$, which indeed form three pairs of commuting members (these pairs are separated by semicolons). In the generalized quadrangle, any such configuration is a sextuple of points collinear with a given point.

A deeper understanding and a fuller appreciation of this observation is acquired after introducing the concept of a geometric hyperplane. 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 $H$ [20], [22]. It is easy to verify that for the generalized quadrangle of order two, $H$ is one of the following three kinds [22]:

1. $H_{\mathrm{ov}}$, an ovoid (there are six such hyperplanes);
2. $H_{\mathrm{cl}}(X)$, a set of points collinear with a given point $X$ including the point itself (there are 15 such hyperplanes); and
3. $H_{\mathrm{gr}}$, a grid as defined above (there are 10 such hyperplanes).

A superlative match is thus revealed between the three kinds of geometric hyperplanes of the generalized quadrangle of order two and the three kinds of projective lines over the rings of four elements and characteristic two embedded in our subconfiguration of $P_{1}\left(M_{2}(G F(2))\right)$, which yields three kinds of distinguished subsets of the Pauli operators of two-qubits, as summarized in Table 3.

Table 3

| GQ | $H_{\mathrm{ov}}$ | $H_{\mathrm{cl}}(X) \backslash\{X\}$ | $H_{\mathrm{gr}}$ |
| :--- | :--- | :--- | :--- |
| PL | $P_{1}(G F(4))$ | $P_{1}\left(G F(2)[x] /\left\langle x^{2}\right\rangle\right)$ | $P_{1}(G F(2) \times G F(2))$ |
| TQ | set of five mutually <br> noncommuting operators | set of six operators <br> commuting with a given one | nine operators of a <br> Mermin's square |

Three kinds of distinguished subsets of the generalized Pauli operators of two-qubits (TQ) viewed as geometric hyperplanes in the generalized quadrangle of order two (GQ) and as projective lines over the rings of order four and characteristic two in the projective line $P_{1}\left(M_{2}(G F(2))\right)(\mathrm{PL})$.

In conclusion, we note that the generalized quadrangle of order two is also contained in $P_{1}\left(M_{2}(G F(2))\right)$ as the projective line over the so-called Jordan system of symmetric $2 \times 2$ matrices over $G F(2)$ [23] or, equivalently, as a generic hyperplane section of the Klein quadric in the five-dimensional projective space over $G F(2)$ (see [22]).

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 that, as we found, is equivalent to the generalized quadrangle of order two. Because such systems are the simplest ones exhibiting phenomena like quantum entanglement and quantum nonlocality, they have a leading place in numerous applications, of which the most popular are quantum cryptography, quantum coding, quantum cloning (teleportation), and quantum computing. Our discovery not only offers a principally new geometrically enriched insight into the intrinsic nature of these phenomena but also opens completely new prospects for their applications and rather unexpected opportunities for an algebro-geometric modeling of their higher-dimensional analogues [24], [25].

Acknowledgments. One of the authors (M. S.) thanks Professor H. Havlicek (Vienna University of Technology) for directing our attention to the description of the generalized quadrangle of order two as the projective line over the Jordan system of the ring in question.

This work was supported in part by the Science and Technology Assistance Agency of the Slovak Republic (Contract No. APVT-51-012704), VEGA of the Slovak Republic (Project No. 2/6070/26), the transnational ECO-NET of France (Project No. 12651NJ, Geometries over finite rings and the properties of mutually unbiased bases), and the Academy of Sciences of the Czech Republic (Project No. 1ET400400410).

## REFERENCES

1. A. Blunck and H. Havlicek, Abh. Math. Sem. Univ. Hamburg, 70, 287-299 (2000).
2. A. Blunck and H. Havlicek, Math. Pannon., 14, 113-127 (2003).
3. A. Blunck and H. Havlicek, Aequationes Math., 69, 146-163 (2005).
4. H. Havlicek, Quad. Sem. Matem. di Brescia, 11, 1-63 (2006); http://www.geometrie.tuwien.ac.at/havlicek/pdf/ dd-laguerre.pdf (2004).
5. A. Herzer, "Chain geometries," in: Handbook of Incidence Geometry (F. Buekenhout, ed.), Elsevier, Amsterdam (1995), p. 781-842.
6. M. Saniga, M. Planat, M. R. Kibler, and P. Pracna, Chaos Solitons Fractals, 33, 1095-1102 (2007); arXiv:math/0605301v4 [math.AG] (2006).
7. M. Saniga and M. Planat, Chaos Solitons Fractals, 37, 337-345 (2008); arXiv:math/0604307v2 [math.AG] (2006).
8. M. Saniga and M. Planat, Theor. Math. Phys., 151, 474-481 (2007); arXiv:quant-ph/0603051v2 (2006).
9. M. Saniga, M. Planat, and M. Minarovjech, Theor. Math. Phys., 151, 625-631 (2007); arXiv:quant-ph/ 0603206v1 (2006).
10. M. Planat, M. Saniga, and M. R. Kibler, SIGMA, 0602, 066 (2006); arXiv:quant-ph/0605239v4 (2006).
11. M. Saniga, M. Planat, and P. Pracna, "A classification of the projective lines over small rings II: Noncommutative case," arXiv:math.AG/0606500v1 (2006).
12. J. B. Fraleigh, A First Course in Abstract Algebra, Addison-Wesley, Reading, Mass. (1967).
13. B. R. McDonald, Finite Rings with Identity, Dekker, New York (1974).
14. R. Raghavendran, Compos. Math., 21, 195-229 (1969).
15. C. Nöbauer, "The book of the rings: Part I," http://www.algebra.uni-linz.ac.at/~noebsi/pub/rings.ps (2000).
16. H. Van Maldeghem, Generalized Polygons, Birkhäuser, Basel (1998).
17. B. Polster and H. Van Maldeghem, J. Combin. Theory Ser. A, 96, 162-179 (2001).
18. B. Polster, A Geometrical Picture Book, Springer, New York (1998).
19. B. Polster, Bull. Belg. Math. Soc. Simon Stevin, 5, 417-425 (1998).
20. B. Polster, A. E. Schroth, and H. Van Maldeghem, Math. Intelligencer, 23, 33-47 (2001).
21. J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A, 65, 032320 (2002).
22. S. E. Payne and J. A. Thas, Finite Generalized Quadrangles, Pitman, Boston (1984).
23. H. Havlicek, Mitt. Math. Ges. Hamburg, 26, 75-94 (2007); http://www.geometrie.tuwien.ac.at/havlicek/pub/ pentazyklisch.pdf.
24. M. Saniga and M. Planat, Adv. Stud. Theor. Phys., 1, 1-4 (2007); arXiv:quant-ph/0612179v1 (2006).
25. M. Planat and M. Saniga, Quantum Inf. Comput., 8, 127-146 (2008); arXiv:quant-ph/0701211v3 (2007).

[^0]:    *Astronomical Institute, Slovak Academy of Sciences, Tatranská Lomnica, Slovak Republic, e-mail: msaniga@astro.sk.
    ${ }^{\dagger}$ Institut FEMTO-ST, CNRS, Département LPMO, Besançon, France, e-mail: michel.planat@femto-st.fr.
    ${ }^{\ddagger}$ Heyrovský Institute of Physical Chemistry, Academy of Sciences of the Czech Republic, Prague, Czech Republic, e-mail: petr.pracna@jh-inst.cas.cz.

[^1]:    ${ }^{1}$ This line was found to be distinguished among noncommutative ring lines because it differs fundamentally from its two commutative counterparts [11].

[^2]:    ${ }^{2}$ This is also known as the slim generalized quadrangle of order $(2,1)$ (see, e.g., [18] and [20]). In fact, both the configurations depicted in Figs. 1a and $1 c$ are slim generalized quadrangles, one being the dual of the other.

