

## PROJECTIVE LINE OVER THE FINITE QUOTIENT RING $GF(2)[x]/\langle x^3 - x \rangle$ AND QUANTUM ENTANGLEMENT: THEORETICAL BACKGROUND

M. Saniga\* and M. Planat†

We consider the projective line over the finite quotient ring  $R_\diamond \equiv GF(2)[x]/\langle x^3 - x \rangle$ . The line is endowed with 18 points, spanning the neighborhoods of three pairwise distant points. Because  $R_\diamond$  is not a local ring, the neighbor (or parallel) relation is not an equivalence relation, and the sets of neighbors for two distant points hence overlap. There are nine neighbors of any point on the line, forming three disjoint families under the reduction modulo either of the two maximal ideals of the ring. Two of the families contain four points each, and they swap their roles when switching from one ideal to the other, the points in one family merging with (the image of) the point in question and the points in the other family passing in pairs into the remaining two points of the associated ordinary projective line of order two. The single point in the remaining family passes to the reference point under both maps, and its existence stems from a nontrivial character of the Jacobson radical  $\mathcal{J}_\diamond$  of the ring. The quotient ring  $\tilde{R}_\diamond \equiv R_\diamond/\mathcal{J}_\diamond$  is isomorphic to  $GF(2) \otimes GF(2)$ . The projective line over  $\tilde{R}_\diamond$  features nine points, each of them surrounded by four neighbors and four distant points, and any two distant points share two neighbors. We surmise that these remarkable ring geometries are relevant for modeling entangled qubit states, which we will discuss in detail in Part II of this paper.

**Keywords:** projective ring line, finite quotient ring, neighbor/distant relation, quantum entanglement

### 1. Introduction

Geometries over rings instead of fields have long been investigated by numerous authors [1], but they have only recently been used in physics [2] and have also found potential applications in other natural sciences [3]. The most prominent, and at first sight rather counterintuitive, feature of ring geometries (of dimension two and higher) is that two distinct points or lines need not have a respective unique connecting line or intersection [4], [5]. Perhaps the most elementary, best-known, and most thoroughly studied ring geometry is the finite projective Hjelmslev plane [2], [6].

Various ring geometries differ essentially in the properties imposed on the underlying coordinate ring. In this paper, we study the structure of the projective line defined over the finite quotient ring  $R_\diamond \equiv GF(2)[x]/\langle x^3 - x \rangle$ . Such a ring, like those used in [2] and [3], is sufficiently close to a field to be handled effectively but sufficiently rich in its structure of zero divisors for the corresponding geometry to have a nontrivial structure compared with that of field geometries and to yield interesting and important applications in quantum physics, dovetailing nicely with those discussed in [2] and [3].

---

\*Astronomical Institute, Slovak Academy of Sciences, Tatranská Lomnica, Slovak Republic,  
e-mail: msaniga@astro.sk.

†Institut FEMTO-ST, CNRS, Département LPMO, Besançon, France, e-mail: planat@lpmo.edu.

---

Translated from Teoreticheskaya i Matematicheskaya Fizika, Vol. 151, No. 1, pp. 44–53, April, 2007. Original article submitted July 21, 2006.

## 2. Basics of ring theory

In this section, we recall some basic definitions and properties of rings that are used in what follows; consequently, even the reader not well versed in ring theory should be able to follow the discussion without an urgent need to consult additional relevant literature (e.g., [7]).

A *ring* is a set  $R$  and two binary operations on it (more precisely,  $(R, +, *)$ ), usually called addition (+) and multiplication (\*), such that  $R$  is an Abelian group under addition and a semigroup under multiplication, with multiplication being both left and right distributive over addition.<sup>1</sup> A ring in which the multiplication is commutative is a commutative ring. A ring  $R$  with a multiplicative identity  $1$  such that  $1r = r1 = r$  for all  $r \in R$  is a ring with unity. A ring containing a finite number of elements is a finite ring. In what follows, the word ring always means a commutative ring with unity.

An element  $r$  of the ring  $R$  is a *unit* (or an invertible element) if there exists an element  $r^{-1}$  such that  $rr^{-1} = r^{-1}r = 1$ . This element, uniquely determined by  $r$ , is called the multiplicative inverse of  $r$ . The set of units forms a group under multiplication. A (nonzero) element  $r$  of  $R$  is said to be a (nontrivial) *zero divisor* if there exists  $s \neq 0$  such that  $sr = rs = 0$ . An element of a finite ring is either a unit or a zero divisor. A ring in which every nonzero element is a unit is a *field*; finite (or Galois) fields, often denoted by  $GF(q)$ , have  $q$  elements and exist only for  $q = p^n$ , where  $p$  is a prime and  $n$  a positive integer. The smallest positive integer  $s$  such that  $s1 = 0$ , where  $s1$  denotes  $1 + 1 + 1 + \dots + 1$  ( $s$  terms), is called the *characteristic* of  $R$ ; if  $s1$  is never zero, then  $R$  is said to have the characteristic zero.

An *ideal*  $\mathcal{I}$  of  $R$  is a subgroup of  $(R, +)$  such that  $a\mathcal{I} = \mathcal{I}a \subseteq \mathcal{I}$  for all  $a \in R$ . An ideal of the ring  $R$  that is not contained in any other ideal except  $R$  itself is called a *maximal* ideal. If an ideal has the form  $Ra$  for some element  $a$  in  $R$ , then it is called a *principal* ideal, usually denoted by  $\langle a \rangle$ . A ring with a unique maximal ideal is a *local* ring. Let  $R$  be a ring and  $\mathcal{I}$  be one of its ideals. Then  $\overline{R} \equiv R/\mathcal{I} = \{a + \mathcal{I} \mid a \in R\}$  together with addition  $(a + \mathcal{I}) + (b + \mathcal{I}) = a + b + \mathcal{I}$  and multiplication  $(a + \mathcal{I})(b + \mathcal{I}) = ab + \mathcal{I}$  is a ring, called the *quotient* (or *factor*) *ring of  $R$  with respect to  $\mathcal{I}$* ; if  $\mathcal{I}$  is maximal, then  $\overline{R}$  is a field. A very important ideal of a ring is that represented by the intersection of all maximal ideals; this ideal is called the *Jacobson radical*.

A map  $\pi: R \mapsto S$  between two rings  $(R, +, *)$  and  $(S, \oplus, \otimes)$  is a ring *homomorphism* if it satisfies the following conditions:  $\pi(a + b) = \pi(a) \oplus \pi(b)$ ,  $\pi(a * b) = \pi(a) \otimes \pi(b)$ , and  $\pi(1) = 1$  for any two elements  $a$  and  $b$  in  $R$ . From this definition, it can be easily seen that  $\pi(0) = 0$ ,  $\pi(-a) = -\pi(a)$ , a unit of  $R$  is sent into a unit of  $S$ , and the set of elements  $\{a \in R \mid \pi(a) = 0\}$ , called the *kernel* of  $\pi$ , is an ideal of  $R$ . A *canonical* (or *natural*) map  $\overline{\pi}: R \rightarrow \overline{R} \equiv R/\mathcal{I}$  defined by  $\overline{\pi}(r) = r + \mathcal{I}$  is clearly a ring homomorphism with the kernel  $\mathcal{I}$ . A bijective ring homomorphism is called a ring *isomorphism*; two rings  $R$  and  $S$  are said to be isomorphic, denoted by  $R \cong S$ , if there exists a ring isomorphism between them.

Finally, we mention two relevant examples of rings: the polynomial ring  $R[x]$ , i.e., the set of all polynomials in one variable  $x$  with coefficients in a ring  $R$ , and the ring  $R_{\otimes}$ , i.e., the (finite) direct product of rings  $R_{\otimes} \equiv R_1 \otimes R_2 \otimes \dots \otimes R_n$ , where both addition and multiplication are performed componentwise and where the component rings need not be the same.

## 3. The ring $R_{\diamond}$ and its canonical homomorphisms

The ring  $R_{\diamond} \equiv GF(2)[x]/\langle x^3 - x \rangle$ , like  $GF(2)$  itself, has the characteristic two and contains the  $\#_t=8$  elements

$$R_{\diamond} = \{0, 1, x, x + 1, x^2, x^2 + 1 = (x + 1)^2, x^2 + x, x^2 + x + 1\}, \quad (1)$$

<sup>1</sup>It is customary to denote multiplication in a ring simply by juxtaposition, using  $ab$  instead of  $a * b$ , and we use this convention.

which include the  $\#_u=2$  units

$$R_\diamond^* = \{1, x^2 + x + 1\} \tag{2}$$

and the  $\#_z=\#_t-\#_u=6$  zero divisors

$$R_\diamond \setminus R_\diamond^* = \{0, x, x + 1, x^2, x^2 + 1, x^2 + x\}. \tag{3}$$

The latter form two principal (and also maximal) ideals,

$$\begin{aligned} \mathcal{I}_{\langle x \rangle} &\equiv \langle x \rangle = \{0, x, x^2, x^2 + x\}, \\ \mathcal{I}_{\langle x+1 \rangle} &\equiv \langle x + 1 \rangle = \{0, x + 1, x^2 + 1, x^2 + x\}. \end{aligned} \tag{4}$$

Because these two ideals are the only maximal ideals of the ring, its Jacobson radical  $\mathcal{J}_\diamond$  is

$$\mathcal{J}_\diamond = \langle x \rangle \cap \langle x + 1 \rangle = \{0, x^2 + x\}. \tag{5}$$

Recalling that  $2 \equiv 0$  and hence  $+1 = -1$  in  $GF(2)$  and also taking into account that  $x^3 = x$ , the multiplication between the elements of  $R_\diamond$  is easily found to be subject to the rules in Table 1.

**Table 1**

$\otimes$	0	1	$x$	$x^2$	$x + 1$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
0	0	0	0	0	0	0	0	0
1	0	1	$x$	$x^2$	$x + 1$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
$x$	0	$x$	$x^2$	$x$	$x^2 + x$	0	$x^2 + x$	$x^2$
$x^2$	0	$x^2$	$x$	$x^2$	$x^2 + x$	0	$x^2 + x$	$x$
$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + x$	$x^2 + 1$	$x^2 + 1$	0	$x + 1$
$x^2 + 1$	0	$x^2 + 1$	0	0	$x^2 + 1$	$x^2 + 1$	0	$x^2 + 1$
$x^2 + x$	0	$x^2 + x$	$x^2 + x$	$x^2 + x$	0	0	0	$x^2 + x$
$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2$	$x$	$x + 1$	$x^2 + 1$	$x^2 + x$	1

The three ideals yield three fundamental quotient rings, all of characteristic two, namely,  $\widehat{R}_\diamond \equiv R_\diamond/\mathcal{I}_{\langle x \rangle} = \{0, 1\}$ ,  $\overline{R}_\diamond \equiv R_\diamond/\mathcal{I}_{\langle x+1 \rangle} = \{0, 1\}$ , and

$$\widetilde{R}_\diamond \equiv R_\diamond/\mathcal{J}_\diamond = \{0, 1, x, x + 1\}. \tag{6}$$

The first two rings are obviously isomorphic to  $GF(2)$ , and the last one is isomorphic to  $GF(2)[x]/\langle x^2 - x \rangle \cong GF(2) \otimes GF(2)$  with componentwise addition and multiplication (see, e.g., [3]), as follows from its multiplication rules in Table 2.

**Table 2**

$\otimes$	0	1	$x$	$x + 1$
0	0	0	0	0
1	0	1	$x$	$x + 1$
$x$	0	$x$	$x$	0
$x + 1$	0	$x + 1$	0	$x + 1$

These quotient rings lead to the three canonical homomorphisms  $\widehat{\pi}: R_{\diamond} \rightarrow \widehat{R}_{\diamond}$ ,  $\overline{\pi}: R_{\diamond} \rightarrow \overline{R}_{\diamond}$ , and  $\widetilde{\pi}: R_{\diamond} \rightarrow \widetilde{R}_{\diamond}$  with the explicit forms

$$\begin{aligned}\widehat{\pi}: \{0, x, x^2, x^2 + x\} &\rightarrow \{0\}, & \{1, x + 1, x^2 + 1, x^2 + x + 1\} &\rightarrow \{1\}, \\ \overline{\pi}: \{0, x + 1, x^2 + 1, x^2 + x\} &\rightarrow \{0\}, & \{1, x, x^2, x^2 + x + 1\} &\rightarrow \{1\}, \\ \widetilde{\pi}: \{0, x^2 + x\} &\rightarrow \{0\}, & \{x, x^2\} &\rightarrow \{x\}, & \{x + 1, x^2 + 1\} &\rightarrow \{x + 1\}, & \{1, x^2 + x + 1\} &\rightarrow \{1\}.\end{aligned}\tag{7}$$

#### 4. The projective line over $R_{\diamond}$ and the associated ring-induced homomorphisms

Given a ring  $R$  and  $GL_2(R)$ , 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 [8]

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R).\tag{8}$$

The projective line over  $R$ , hereafter denoted by  $PR(1)$ , is defined as the set of classes of ordered pairs  $(\varrho a, \varrho b)$ , where  $\varrho$  is a unit and  $(a, b)$  is admissible [8]–[11]. In the case of  $R_{\diamond}$ , admissibility condition (8) can be rewritten in simpler terms as

$$\Delta \equiv \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in R_{\diamond}^*,\tag{9}$$

whence it follows that  $PR_{\diamond}(1)$  contains two algebraically distinct kinds of points: (1) the points represented by pairs where at least one entry is a unit and (2) those where both the entries are zero divisors, not of the same ideal. It is then straightforward to see that there are altogether

$$\#^{(I)} = \frac{\#_t^2 - \#_z^2}{\#_u} = \#_t + \#_z = 8 + 6 = 14\tag{10}$$

points of the first type, namely,

$$\begin{aligned}(1, 0), & (1, x), & (1, x^2), & (1, x + 1), & (1, x^2 + 1), & (1, x^2 + x), & (1, 1), & (1, x^2 + x + 1), \\ (0, 1), & (x, 1), & (x^2, 1), & (x + 1, 1), & (x^2 + 1, 1), & (x^2 + x, 1), & & \end{aligned}$$

and

$$\#^{(II)} = \frac{\#_z^2 - \#_s}{\#_u} = \frac{6^2 - (2 \times 4^2 - 2^2)}{2} = 4\tag{11}$$

points of the second type, namely,

$$\begin{aligned}(x, x + 1) &\sim (x^2, x + 1), & (x, x^2 + 1) &\sim (x^2, x^2 + 1), \\ (x + 1, x) &\sim (x + 1, x^2), & (x^2 + 1, x) &\sim (x^2 + 1, x^2),\end{aligned}$$

where  $\#_s$  denotes the number of distinct pairs of zero divisors with both entries in the same ideal. Hence,  $PR_{\diamond}(1)$  contains  $\#^{(I)} + \#^{(II)} = 14 + 4 = 18$  points in total.

The points of  $PR_{\diamond}(1)$  are characterized by two crucial relations, neighbor and distant. In particular, two distinct points  $X: (\varrho a, \varrho b)$  and  $Y: (\varrho c, \varrho d)$  are called *neighbors* (or *parallel*) if  $\Delta$  is a *zero divisor* and *distant* otherwise, i.e., if  $\Delta$  is a *unit*. The neighbor relation is reflexive (every point is obviously a neighbor to itself) and symmetric (i.e., if  $X$  is neighbor to  $Y$ , then also  $Y$  is a neighbor to  $X$ ) but, as is seen below, not transitive (i.e.,  $X$  being a neighbor to  $Y$  and  $Y$  being a neighbor to  $Z$  does not necessarily mean that  $X$  is a neighbor to  $Z$ ), because  $R_{\diamond}$  is *not* a local ring (see, e.g., [5], [11]). Given a point of  $PR_{\diamond}(1)$ , the set of all its neighbor points is called its *neighborhood*.<sup>2</sup> We find the cardinality and “intersection” properties of this remarkable set. For this, we pick three distinguished pairwise distant points of the line,  $U: (1, 0)$ ,  $V: (0, 1)$ , and  $W: (1, 1)$ , for which we can easily find the neighborhoods:

$$\begin{aligned} U: \quad & U_1: (1, x), \quad U_2: (1, x^2), \quad U_3: (1, x+1), \quad U_4: (1, x^2+1), \quad U_0: (1, x^2+x), \\ & U_5: (x, x+1), \quad U_6: (x, x^2+1), \quad U_7: (x+1, x), \quad U_8: (x^2+1, x), \end{aligned} \quad (12)$$

$$\begin{aligned} V: \quad & V_1: (x, 1), \quad V_2: (x^2, 1), \quad V_3: (x+1, 1), \quad V_4: (x^2+1, 1), \quad V_0: (x^2+x, 1), \\ & V_5: (x, x+1), \quad V_6: (x, x^2+1), \quad V_7: (x+1, x), \quad V_8: (x^2+1, x), \end{aligned} \quad (13)$$

$$\begin{aligned} W: \quad & W_1: (1, x), \quad W_2: (1, x^2), \quad W_3: (1, x+1), \quad W_4: (1, x^2+1), \quad W_0: (1, x^2+x+1), \\ & W_5: (x, 1), \quad W_6: (x^2, 1), \quad W_7: (x+1, 1), \quad W_8: (x^2+1, 1). \end{aligned} \quad (14)$$

We can easily see that  $U_i \equiv W_i$  for  $i = 1, 2, 3, 4$ ,  $U_j \equiv V_j$  for  $j = 5, 6, 7, 8$ , and  $V_k \equiv W_{k+4}$  for  $k = 1, 2, 3, 4$ . Now, because the coordinate system on this line can *always* be chosen such that the coordinates of *any* three pairwise distant points are identical to those of  $U$ ,  $V$ , and  $W$ , we see from the last three expressions that the neighborhood of any point on the line contains nine distinct points, the neighborhoods of any two distant points have four points in common (this property implies the previously stated nontransitivity of the neighbor relation), and the neighborhoods of any three pairwise distant points have no element in common, as illustrated in Fig. 1.

A deeper insight into the structure and properties of neighborhoods is obtained if we consider the three canonical homomorphisms given by Eqs. (7). The first two induce the homomorphisms from  $PR_{\diamond}(1)$  to  $PG(1, 2)$ , the ordinary projective line of order two, and the third induces  $PR_{\diamond}(1) \rightarrow P\tilde{R}_{\diamond}(1)$ . Because  $PG(1, 2)$  contains three points, namely,  $U: (1, 0)$ ,  $V: (0, 1)$ , and  $W: (1, 1)$ , we find that the first homomorphism,  $PR_{\diamond}(1) \rightarrow P\hat{R}_{\diamond}(1)$ , acts on a neighborhood, taken to be that of  $U$  without loss of generality, as

$$U_1, U_2, U_7, U_8, U_0 \rightarrow \hat{U}, \quad U_5, U_6 \rightarrow \hat{V}, \quad U_3, U_4 \rightarrow \hat{W}, \quad (15)$$

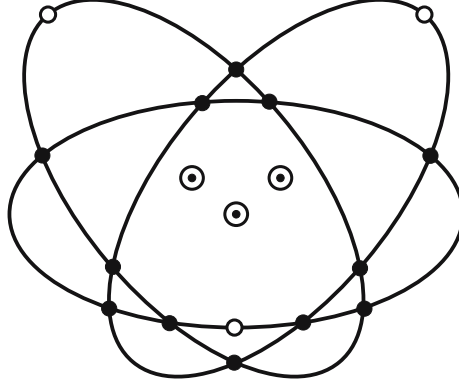
while the second,  $PR_{\diamond}(1) \rightarrow P\bar{R}_{\diamond}(1)$ , shows an almost complementary behavior,

$$U_3, U_4, U_5, U_6, U_0 \rightarrow \bar{U}, \quad U_7, U_8 \rightarrow \bar{V}, \quad U_1, U_2 \rightarrow \bar{W}. \quad (16)$$

But the third homomorphism,  $PR_{\diamond}(1) \rightarrow P\tilde{R}_{\diamond}(1)$ , is more intricate. To fully grasp its meaning, we must first understand the structure of the line  $P\tilde{R}_{\diamond}(1)$ . For this, we follow the same chain of reasoning as for  $PR_{\diamond}(1)$ . Using Eq. (6) and Table 2, we find that  $P\tilde{R}_{\diamond}(1)$  has nine points: there are seven of the first kind  $((1, 0), (1, x), (1, x+1), (1, 1), (0, 1), (x, 1), \text{ and } (x+1, 1))$  and two of the second kind  $((x, x+1) \text{ and } (x+1, x))$ .

---

<sup>2</sup>To avoid any confusion, we here warn that some authors (see, e.g., [10], [11]) use this term for the set of *distant* points instead.



**Fig. 1.** A schematic sketch of the structure of the projective line  $PR_{\diamond}(1)$ . Given any three pairwise distant points (represented by the three circled dots), the remaining points of the line are all located in the neighborhoods of the three points (three sets of points located on three different ellipses centered on the points in question). Two neighborhoods share four points, and because the three neighborhoods have no common intersection, we thus obtain twelve points; the existence of the remaining three points (open circles) is intimately connected with the ring  $R_{\diamond}$  having a nontrivial Jacobson radical.

The neighborhoods of the three distinguished pairwise distant points  $\tilde{U}: (1, 0)$ ,  $\tilde{V}: (0, 1)$ , and  $\tilde{W}: (1, 1)$  here are

$$\begin{aligned}
 \tilde{U}: \quad & \tilde{U}_1: (1, x), \quad \tilde{U}_2: (1, x+1), \quad \tilde{U}_3: (x, x+1), \quad \tilde{U}_4: (x+1, x), \\
 \tilde{V}: \quad & \tilde{V}_1: (x, 1), \quad \tilde{V}_2: (x+1, 1), \quad \tilde{V}_3: (x, x+1), \quad \tilde{V}_4: (x+1, x), \\
 \tilde{W}: \quad & \tilde{W}_1: (1, x), \quad \tilde{W}_2: (1, x+1), \quad \tilde{W}_3: (x, 1), \quad \tilde{W}_4: (x+1, 1).
 \end{aligned} \tag{17}$$

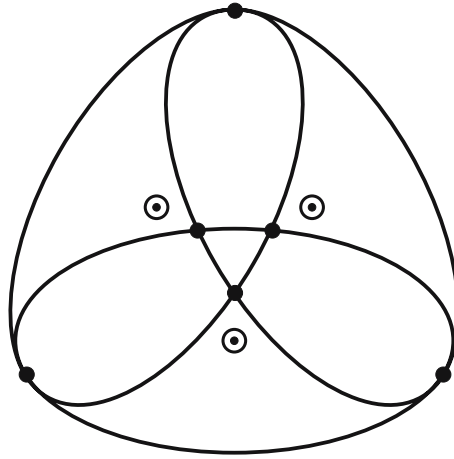
From these expressions, because the coordinates of any three pairwise distant points can again be made identical to those of  $\tilde{U}$ ,  $\tilde{V}$ , and  $\tilde{W}$ , we find that the neighborhood of any point on this line contains four distinct points, the neighborhoods of any two distant points have two points in common (which again implies the nontransitivity of the neighbor relation), and the neighborhoods of any three pairwise distant points are disjoint, as illustrated in Fig. 2. We note that in this case, there are no “Jacobson” points, i.e., points belonging solely to a single neighborhood, because the Jacobson radical is trivial,  $\tilde{\mathcal{J}}_{\diamond} = \{0\}$ . At this point, we can write an explicit expression for  $PR_{\diamond}(1) \rightarrow P\tilde{R}_{\diamond}(1)$ :

$$\begin{aligned}
 U_1/W_1, U_2/W_2 &\rightarrow \tilde{U}_1/\tilde{W}_1, & U_3/W_3, U_4/W_4 &\rightarrow \tilde{U}_2/\tilde{W}_2, \\
 U_5/V_5, U_6/V_6 &\rightarrow \tilde{U}_3/\tilde{V}_3, & U_7/V_7, U_8/V_8 &\rightarrow \tilde{U}_4/\tilde{V}_4, \\
 V_1/W_5, V_2/W_6 &\rightarrow \tilde{V}_1/\tilde{W}_3, & V_3/W_7, V_4/W_8 &\rightarrow \tilde{V}_2/\tilde{W}_4, \\
 U, U_0 &\rightarrow \tilde{U}, & V, V_0 &\rightarrow \tilde{V}, & W, W_0 &\rightarrow \tilde{W}.
 \end{aligned} \tag{18}$$

This map plays an especially important role in the physical applications of the theory.

## 5. Envisioned applications of the two geometries

We assume that  $P\tilde{R}_{\diamond}(1)$  and  $PR_{\diamond}(1)$  provide a suitable algebraic geometric setting for properly understanding two- and three-qubit states as embodied in the respective structures of the so-called Peres–Mermin magic square and pentagram [12]. The Peres–Mermin square is a  $3 \times 3$  “lattice” of nine four-dimensional operators (or matrices) with the degenerate eigenvalues  $\pm 1$ . The three operators in each line



**Fig. 2.** A schematic sketch of the structure of the projective line  $P\tilde{R}_\diamond(1)$ . As in the previous case, given any three pairwise distant points (represented by the three circled dots), the remaining points of the line (solid circles) are all located in the neighborhoods of the three points (three sets of points located on three different ellipses centered on the points in question).

or column are mutually commuting, and each operator is the product of the two others in the same line or column except the last column, where a minus sign appears. The algebraic rule for the eigenvalues contradicts that for the operators, which is the heart of the Kochen–Specker theorem [13] for this particular case. The explanation of this puzzling behavior is that three lines and two columns have joint orthogonal bases of *nonentangled* eigenstates, while the operators in the third column share a base of *maximally entangled* states. We can establish a one-to-one correspondence between the observables in the Peres–Mermin square and the points of the projective line  $P\tilde{R}_\diamond(1)$ . A closely related phenomenon occurs in the three-qubit case with the square replaced with a pentagram involving ten operators, and the geometric explanation here can be based on the properties of the neighborhood of a point of the projective line  $PR_\diamond(1)$ . These and some other closely related quantum mechanical issues will be examined in detail in Part II of this paper [14].

**Acknowledgments.** One of the authors (M. S.) thanks Dr. Milan Minarovjech for the insightful remarks and suggestions, Mr. Pavol Bendík for carefully drawing the figures, and Dr. Richard Komžík for the computer-related assistance.

This work was supported in part by the Science and Technology Assistance Agency, Slovak Republic (Contract No. APVT-51-012704), the VEGA, Slovak Republic (Project No. 2/6070/26), and the ECONE, France (Project No. 12651NJ “Geometries over Finite Rings and the Properties of Mutually Unbiased Bases”).

## REFERENCES

1. G. Törner and F. D. Veldkamp, *J. Geom.*, **42**, 180–200 (1991).
2. M. Saniga and M. Planat, *J. Phys. A*, **39**, 435–440 (2006); math-ph/0506057 (2005).
3. M. Saniga and M. Planat, *Chaos Solitons Fractals* (in press); math.NT/0601261 (2006).
4. F. D. Veldkamp, *Geom. Dedicata*, **11**, 285–308 (1981); “Projective ring planes and their homomorphisms,” in: *Rings and Geometry* (NATO ASI Ser. C Math. Phys. Sci., Vol. 160, R. Kaya, P. Plaumann, and K. Strambach, eds.), Reidel, Dordrecht (1985), pp. 289–350; “Projective ring planes: Some special cases,” in: *Proc. Conf.*

- Combinatorial and Incidence Geometry: Principles and Applications* (La Mendola, 1982, Rend. Sem. Mat. Brescia, Vol. 7), Vita e Pensiero, Milan (1984), pp. 609–615.
5. F. D. Veldkamp, “Geometry over rings,” in: *Handbook of Incidence Geometry* (F. Buekenhout, ed.), North-Holland, Amsterdam (1995), pp. 1033–1084.
  6. J. Hjelmslev, *Abh. Math. Sem. Univ. Hamburg*, **2**, 1–36 (1923); W. Klingenberg, *Math. Z.*, **60**, 384–406 (1954); E. Kleinfeld, *Illinois J. Math.*, **3**, 403–407 (1959); P. Dembowski, *Finite Geometries*, Springer, Berlin (1968); D. A. Drake and D. Jungnickel, “Finite Hjelmslev planes and Klingenberg epimorphism,” in: *Rings and Geometry* (NATO ASI Ser. C Math. Phys. Sci., Vol. 160, R. Kaya, P. Plaumann, and K. Strambach, eds.), Reidel, Dordrecht (1985), pp. 153–231.
  7. J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, Reading, Mass. (1994); B. R. McDonald, *Finite Rings with Identity* (Pure Appl. Math., Vol. 28), Marcel Dekker, New York (1974); R. Raghavendran, *Compositio Math.*, **21**, 195–229 (1969).
  8. A. Herzer, “Chain geometries,” in: *Handbook of Incidence Geometry* (F. Buekenhout, ed.), North-Holland, Amsterdam (1995), pp. 781–842.
  9. A. Blunck and H. Havlicek, *Abh. Math. Sem. Univ. Hamburg*, **70**, 287–299 (2000).
  10. A. Blunck and H. Havlicek, *Math. Pannon.*, **14**, 113–127 (2003).
  11. H. Havlicek, *Quad. Sem. Mat. Brescia*, **11**, 1–63 (2006); <http://www.geometrie.tuwien.ac.at/havlicek/dd-laguerre.pdf>.
  12. N. D. Mermin, *Rev. Modern Phys.*, **65**, 803–815 (1993).
  13. S. Kochen and E. Specker, *J. Math. Mech.*, **17**, 59–87 (1967).
  14. M. Saniga and M. Planat, *Theor. Math. Phys.*, **151**, No. 2 (2007).