International Journal of Modern Physics B
Vol. 20, Nos. 11, 12 & 13 (2006) 1885–1892

World Scientific
www.worldscientific.com

FINITE GEOMETRIES IN QUANTUM THEORY: FROM GALOIS (FIELDS) TO HJELMSLEV (RINGS)

METOD SANIGA

Astronomical Institute, Slovak Academy of Sciences,
05960 Tatranská Lomnica, Slovak Republic
msaniga@astro.sk

MICHEL PLANAT

Institut FEMTO-ST, Departement LPMO,
32 Avenue de l'Observatoire, 25044 Besançon Cedex, France
planat@lpmo.edu

Received 28 February 2006

Geometries over Galois *fields* (and related finite combinatorial structures/algebras) have recently been recognized to play an ever-increasing role in quantum theory, especially when addressing properties of mutually unbiased bases (MUBs). The purpose of this contribution is to show that completely new vistas open up if we consider a generalized class of finite (projective) geometries, viz. those defined over Galois *rings* and/or other finite Hjelmslev *rings*. The case is illustrated by demonstrating that the basic combinatorial properties of a complete set of MUBs of a q-dimensional Hilbert space $\mathcal{H}_q$, $q = p^r$ with p being a prime and r a positive integer, are qualitatively mimicked by the configuration of points lying on a proper conic in a projective Hjelmslev plane defined over a Galois ring of characteristic p^2 and rank r. The q vectors of a basis of $\mathcal{H}_q$ correspond to the q points of a (so-called) neighbour class and the $q+1$ MUBs answer to the total number of (pairwise disjoint) neighbour classes on the conic. Although this remarkable analogy is still established at the level of cardinalities only, we currently work on constructing an explicit mapping by associating a MUB to each neighbour class of the points of the conic and a state vector of this MUB to a particular point of the class. Further research in this direction may prove to be of great relevance for many areas of quantum information theory, in particular for quantum information processing.

Keywords: Galois rings; projective Hjelmslev planes; conics; mutually unbiased bases.

1. Introduction

History offers us numerous examples when the solution of a tough physical problem was found to be intimately linked with one or several long-standing problems of purely mathematical nature. We believe that such a situation is currently encountered in quantum mechanics where we try to understand the "problem of quantum measurement" in terms of so-called mutually unbiased bases of a finite-dimensional Hilbert space. Here we are referring to our recent conjecture[1] that the question of the existence of the maximum, or complete, sets of mutually unbiased bases in a q-dimensional Hilbert space if q differs from a prime power (i.e., it is a "composite" integer) is intricately connected with the formidable geometrical combinatorics problem of whether there exist projective planes of a "composite" order q.

Two distinct orthonormal bases of a q-dimensional Hilbert space, $\mathcal{H}_q$, are said to be mutually unbiased if all inner products between any element of the first basis and any element of the second basis are of the same value $1/\sqrt{q}$. This concept plays a key role in a search for a rigorous formulation of quantum complementarity and lends itself to numerous applications in quantum information theory. It is a well-known fact (see, e.g., Refs. 2–9 and references therein) that $\mathcal{H}_q$ supports at most $q+1$ pairwise mutually unbiased bases (MUBs) and various algebraic geometrical constructions of such $q+1$, or *complete*, sets of MUBs have been found when $q = p^r$, with p being a prime and r a positive integer. In our recent paper[10] we have demonstrated that the bases of such a set can be viewed as points of a proper conic (or, more generally, of an oval) in an ordinary (Galois) projective plane of order q. In this article we extend and qualitatively finalize this picture by showing that also individual vectors of every such a basis can be represented by points, although these points are of a different nature and require a more general projective setting, that of a projective *Hjelmslev* plane. [11–14]

2. Galois Rings and Projective Hjelmslev Planes

To this end in view, we shall first introduce the basics of the Galois ring theory (see e.g., Ref. 15 for the symbols, notation and further details). Let, as above, p be a prime number and r a positive integer, and let $f(x) \in \mathcal{Z}_{p^2}[x]$ be a monic polynomial of degree r whose image in $\mathcal{Z}_p[x]$ is irreducible. Then $GR(p^2, r) \equiv \mathcal{Z}_{p^2}[x]/(f)$ is a ring, called a *Galois ring*, of characteristic p^2 and rank r, whose maximal ideal is $p\,GR(p^2, r)$. In this ring there exists a non-zero element ζ of order $p^r - 1$ that is a root of $f(x)$ over $\mathcal{Z}_{p^2}$, with $f(x)$ dividing $x^{p^r-1} - 1$ in $\mathcal{Z}_{p^2}[x]$. Then any element of $GR(p^2, r)$ can uniquely be written in the form

$$g = a + pb, \tag{1}$$

where both a and b belong to the so-called Teichmüller set $\mathcal{T}_r$,

$$\mathcal{T}_r \equiv \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^r-2}\right\}, \tag{2}$$

having

$$q = p^r \tag{3}$$

elements. From Eq. (1) it is obvious that g is a unit (i.e., an invertible element) of $GR(p^2, r)$ iff $a \neq 0$ and a zero-divisor iff $a = 0$. It then follows that $GR(p^2, r)$ has $\#_{\rm t} = q^2$ elements in total, out of which there are $\#_{\rm z} = q$ zero-divisors and $\#_{\rm u} = q^2 - q = q(q-1)$ units. Next, let "—" denote reduction modulo p; then $\overline{\mathcal{T}}_r = GF(q)$, the Galois *field* of order q, and $\overline{\zeta}$ is a primitive element of $GF(q)$.

Finally, one notes that any two Galois rings of the same characteristic and rank are isomorphic.

Now we have a sufficient algebraic background to introduce the concept of a projective Hjelmslev plane over $GR(p^2, r)$, henceforth referred to as $PH(2,q)$.[a] $PH(2,q)$ is an incidence structure whose points are classes of ordered triples $(\varrho\breve{x}_1, \varrho\breve{x}_2, \varrho\breve{x}_3)$, where both ϱ and at least one $\breve{x}_i$ $(i = 1, 2, 3)$ are units, whose lines are classes of ordered triples $(\sigma\breve{l}_1, \sigma\breve{l}_2, \sigma\breve{l}_3)$, where both σ and at least one $\breve{l}_i$ $(i = 1, 2, 3)$ are units, and the incidence relation is given by

$$\sum_{i=1}^{3} \breve{l}_i\breve{x}_i \equiv \breve{l}_1\breve{x}_1 + \breve{l}_2\breve{x}_2 + \breve{l}_3\breve{x}_3 = 0. \tag{4}$$

¿From this definintion it follows that in $PH(2,q)$ — as in any *ordinary* projective plane — there is a perfect duality between points and lines; that is, instead viewing the points of the plane as the fundamental entities, and the lines as ranges (loci) of points, we may equally well take the lines as primary geometric constituents and define points in terms of lines, characterizing a point by the complete set of lines passing through it. It is also straightforward to see that this plane contains

$$\#_{\mathrm{trip}} = \frac{\#_{\mathrm{t}}^3 - \#_{\mathrm{z}}^3}{\#_{\mathrm{u}}} = \frac{(q^2)^3 - q^3}{q(q-1)} = \frac{q^3(q^3-1)}{q(q-1)} = q^2\left(q^2+q+1\right) \tag{5}$$

points/lines and that the number of points/lines incident with a given line/point is, in light of Eq. (4), equal to the number of non-equivalent couples $(\varrho\breve{x}_1, \varrho\breve{x}_2)/(\sigma\breve{l}_1, \sigma\breve{l}_2)$, i.e.,

$$\#_{\mathrm{coup}} = \frac{\#_{\mathrm{t}}^2 - \#_{\mathrm{z}}^2}{\#_{\mathrm{u}}} = \frac{(q^2)^2 - q^2}{q(q-1)} = \frac{q^2(q^2-1)}{q(q-1)} = q\,(q+1)\,. \tag{6}$$

These figures should be compared with those characterizing ordinary finite planes of order q, which read $\overline{\#}_{\mathrm{trip}} = q^2 + q + 1$ and $\overline{\#}_{\mathrm{coup}} = q + 1$, respectively (e.g., Ref. 16).

Any projective Hjelmslev plane, $PH(2,q)$ in particular, is endowed with a very important, and of crucial relevance when it comes to MUBs, property that has no analogue in an ordinary projective plane — the so-called *neighbour* (or, as occasionally referred to, non-remoteness) relation. Namely (see, e.g., Refs. 12–14), we say that two points A and B are neighbour, and write $A \odot B$, if either $A = B$, or $A \neq B$ and there exist two different lines incident with both; otherwise, they are called nonneighbour, or remote. The same symbol and the dual definition is used for neighbour lines. Let us find the cardinality of the set of neighbours of a given point/line of $PH(2,q)$. Algebraically speaking, given a point $\varrho\breve{x}_i$, $i = 1, 2, 3$, the points that are its neighbours must be of the form $\varrho\,(\breve{x}_i + p\breve{y}_i)$, with $\breve{y}_i \in \mathcal{T}_r$; for two points are neighbour iff their corresponding coordinates differ by a zero

[a]This is, of course, a very specific, and rather elementary, kind of projective Hjelmslev plane; its most general, axiomatic definition can be found, for example, in Refs. 12–14.

divisor.[12–14] Although there are q^3 different choices for the triple $(\breve{y}_1, \breve{y}_2, \breve{y}_3)$, only $q^3/q = q^2$ of the classes $\varrho\,(\breve{x}_i + p\breve{y}_i)$ represent distinct points because $\varrho\,(\breve{x}_i + p\breve{y}_i)$ and $\varrho\,(\breve{x}_i + p(\breve{y}_i + \kappa\breve{x}_i))$ represent one and the same point as κ runs through all the q elements of $\mathcal{T}_r$. Hence, every point/line of $PH(2,q)$ has q^2 neighbours, the point/line in question inclusive. Following the same line of reasoning, but restricting only to couples of coordinates, we find that given a point P and a line $\mathcal{L}$, P incident with $\mathcal{L}$, there exist exactly $\left(q^2/q =\right) q$ points on $\mathcal{L}$ that are neighbour to P and, dually, q lines through P that are neighbour to $\mathcal{L}$.

Clearly, as $A \odot A$ (reflexivity), $A \odot B$ implies $B \odot A$ (symmetry) and $A \odot B$ and $B \odot C$ implies $A \odot C$ (transitivity), the neighbour relation is an *equivalence* relation. Given "$\odot$" and a point P/line $\mathcal{L}$, we call the subset of all points Q/lines $\mathcal{K}$ of $PH(2,q)$ satisfying $P \odot Q/\mathcal{L} \odot \mathcal{K}$ the neighbour class of $P/\mathcal{L}$. And since "$\odot$" is an equivalence relation, the aggregate of neighbour classes *partitions* the plane, i.e. the plane consists of a *dis*joint union of neighbour classes of points/lines. The modulo-p-mapping then "induces" a so-called canonical epimorphism of $PH(2,q)$ into $PG(2,q)$, the ordinary projective plane defined over $GF(q)$, with the neighbour classes being the cosets of this epimorphism.[14] Loosely rephrased, $PH(2,q)$ comprises $q^2 + q + 1$ "clusters" of neighbour points/lines, each of cardinality q^2, such that its restriction modulo the neighbour relation is the ordinary projective plane $PG(2,q)$ every single point/line of which encompasses the whole "cluster" of these neighbour points/lines. Analogously, each line of $PH(2,q)$ consists of $q+1$ neighbour classes, each of cardinality q, such that its "—" image is the ordinary projective line in the $PG(2,q)$ whose points are exactly these neighbour classes.

Let us illustrate these remarkable properties on the simplest possible example that is furnished by $PH(2,q=2)$, i.e. the plane defined over $GR(4,1)$ whose epimorphic "shadow" is the simplest projective plane $PG(2,2)$ — the Fano plane. As partially depicted in Fig. 1, this plane consists of seven classes of quadruples of neighbour points/lines, each point/line featuring three classes of couples of neighbour lines/points. When modulo-two-projected, each quadruple of neighbour points/lines goes into a single point/line of the associated Fano plane.

The most relevant geometrical object for our model[10] is, of course, a *conic*, that is a curve $\mathcal{Q}$ of $PH(2,q)$ whose points obey the equation

$$\mathcal{Q}: \quad \sum_{i \leq j} c_{ij}\breve{x}_i\breve{x}_j \equiv c_{11}\breve{x}_1^2 + c_{22}\breve{x}_2^2 + c_{33}\breve{x}_3^2 + c_{12}\breve{x}_1\breve{x}_2 + c_{13}\breve{x}_1\breve{x}_3 + c_{23}\breve{x}_2\breve{x}_3 = 0, \quad (7)$$

with at least one of the c_{ij} 's being a unit of $GR(p^2,r)$. In particular, we are interested in a *proper* conic, which is a conic whose equation cannot be reduced into a form featuring fewer variables whatever coordinate transformation one would employ. It is known (see, e.g., Ref. 17) that the equation of a proper conic of $PH(2,q)$ can always be brought into a "canonical" form

$$\mathcal{Q}^\star: \quad \breve{x}_1\breve{x}_3 - \breve{x}_2^2 = 0 \quad (8)$$

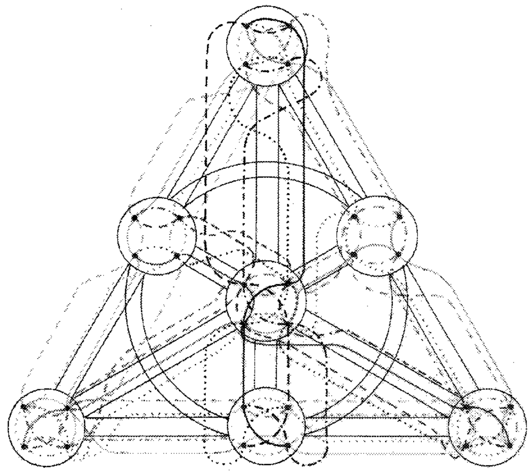

Fig. 1. A schematic sketch of the structure of the simplest projective Hjelmslev plane, $PH(2,2)$. Shown are all the 28 of its points (represented by small filled circles), grouped into seven pairwise disjoint sets (neighbour classes), each of cardinality four, as well as 24 of its lines (drawn as solid, dashed, dotted and dot-dashed curves), forming six different neighbour classes. In order to make the sketch more illustrative, different neighbour classes of lines have different colour. Also shown is the associated Fano plane, $PG(2,2)$, whose points are represented by seven big circles, six of its lines are drawn as pairs of line segments and the remaining line as a pair of concentric circles. Notice the intricate character of pairwise intersection of the lines of $PH(2,2)$; two lines from distinct neighbour classes have just one point in common, while any two lines within a neighbour class share ($q=$)2 points, both of the same neighbour class.

from which it readily follows that any such conic is endowed, like a line, with $q^2+q=q(q+1)$ points; q^2 of them are of the form

$$\varrho\breve{x}_i=(1,\sigma,\sigma^2), \tag{9}$$

where the parameter σ runs through all the elements of $GR(p^2,r)$, whilst the remaining q are represented by

$$\varrho\breve{x}_i=(0,\delta,1), \tag{10}$$

with δ running through all the zero-divisors of $GR(p^2,r)$. And each point of a proper conic, like that of a line, has q neighbours; for the neighbours of a particular point $\sigma=\sigma_0$ of (9) are of the form

$$\varrho\breve{x}_i=(1,\sigma_0+p\kappa,(\sigma_0+p\kappa)^2)=(1,\sigma_0+p\kappa,\sigma_0^2+p2\kappa) \tag{11}$$

and there are q of them (the point in question inclusive) as κ runs through $\mathcal{T}_r$, and all the q points of (10) are the neighbours of any of them. All in all, a proper conic, like a line, of $PH(2,q)$ features $q+1$ pairwise disjoint classes of neighbour points, each having q elements, these classes being the single points of its modular image in $PG(2,q)$.

There exists, however, a profound difference between the two geometrical objects when it comes to the *neighbour* relation. For while two distinct neighbour lines

Table 1. The structure/composition of five different neighbour conics of $PH(2,2)$. Every conic comprises ("picks up") a couple of points from each of the three relevant neighbour classes $(\bar{1},\bar{0},\bar{0})$, $(\bar{0},\bar{1},\bar{0})$ and $(\bar{1},\bar{1},\bar{1})$, the points in question being labelled by a bullet ("•"). To save space, we use the abbreviated notation where "100" stands for "$(1,0,0)$", "120" for "$(1,2,0)$", etc.

Type of Conic	(Neighbour Classes of) Points of $PH(2,2)$											
	$(\bar{1},\bar{0},\bar{0})$				$(\bar{0},\bar{1},\bar{0})$				$(\bar{1},\bar{1},\bar{1})$			
	100	120	102	122	010	210	012	212	111	131	113	311
$\mathcal{Q}^{(+)}$	•		•		•		•			•		•
$\mathcal{Q}^{(-)}$	•		•		•		•		•		•	
$\mathcal{Q}^{(1)}$		•		•	•		•			•		•
$\mathcal{Q}^{(2)}$	•		•			•		•		•		•
$\mathcal{Q}^{(3)}$		•		•		•		•	•		•	

always have q points in common, two different neighbour conics (i.e., conics having the same epimorphic image in the corresponding ordinary projective plane) may also share *more than* q points, or, on the other hand, be completely *dis*joint. This property is illustrated by Table 1, which features composition of several neighbour conics of $PH(2,2)$ whose image in $PG(2,2)$ is the conic $\overline{\mathcal{Q}} := \bar{\breve{x}}_1\bar{\breve{x}}_2 + \bar{\breve{x}}_3^2$, namely the conics $\mathcal{Q}^{(+)} := \breve{x}_1\breve{x}_2 + \breve{x}_3^2$, $\mathcal{Q}^{(-)} := \breve{x}_1\breve{x}_2 - \breve{x}_3^2$, $\mathcal{Q}^{(1)} := \breve{x}_1\breve{x}_2 - \breve{x}_3^2 + 2\breve{x}_1^2$, $\mathcal{Q}^{(2)} := \breve{x}_1\breve{x}_2 - \breve{x}_3^2 + 2\breve{x}_2^2$, $\mathcal{Q}^{(3)} := \breve{x}_1\breve{x}_2 - \breve{x}_3^2 + 2\breve{x}_1^2 + 2\breve{x}_2^2$. We see, for example, that $\mathcal{Q}^{(1)}$ and $\mathcal{Q}^{(2)}$ have $2(=q)$ points in common, $\mathcal{Q}^{(+)}$ and $\mathcal{Q}^{(-)}$ overlap in $4(=2q>q)$ points, whilst $\mathcal{Q}^{(+)}$ and $\mathcal{Q}^{(3)}$ do not share any point at all.

3. Hjelmslev Conics and MUBs

At this point our algebraic geometrical machinery is elaborate enough to generalize and qualitatively complete the geometrical picture of MUBs proposed in Ref. 10 where we have argued that a basis of $\mathcal{H}_q$, q given by (3), can be regarded as a point of an arc in $PG(2,q)$, with a complete set of MUBs corresponding to a proper conic (or, in the case of $p=2$, to a more general geometrical object called oval). This model, however, lacks a geometrical interpretation of the individual vectors of a basis, which can be achieved in our extended projective setting *à la* Hjelmslev only. Namely, taking any complete, i.e., of cardinality $q+1$, set of MUBs, its *bases* are now viewed as the *neighbour classes* of points of a proper conic of $PH(2,q)$ and the *vectors* of a given basis have their counterpart in the *points* of the corresponding neighbour class. The property of different vectors of a basis being pairwise *orthogonal* is then geometrically embodied in the fact that the corresponding points are all *neighbour*, whilst the property of two different bases being *mutually unbiased* answers to the fact that the points of any two neighbour classes are *remote* from each other. It is left to the reader as an easy exercise to check that "rephrasing these statements modulo p" one recovers all the conic-related properties of MUBs given in Ref. 10, irrespective of the value of p. The $(p=2)$ case of "non-conic" MUBs is here, however, much more complex and intricate than that in the ordinary projective planes and will properly be dealt with in a separate paper.

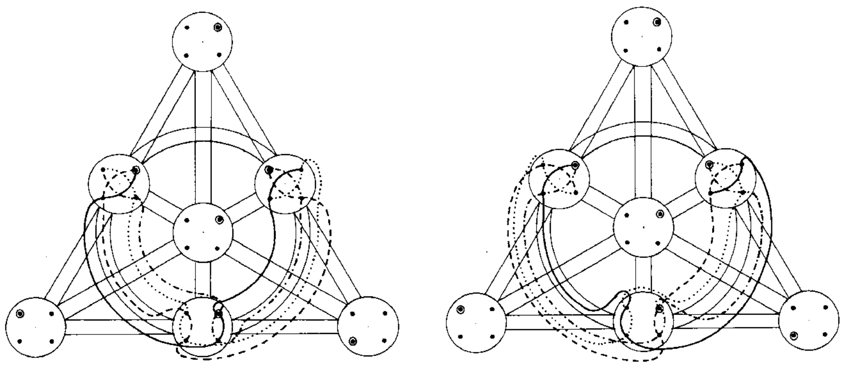

Fig. 2. A sketchy illustration of the difference between the structures of the projective Hjelmslev plane defined over the Galois ring $GR(4,1)$ (i.e., $PH(2,2)$) and that defined over the ring of dual numbers $GF(2)[x]/(x^2)$. Both the planes can be represented in such a way that they are made identical in their point sets as well as in six neighbour classes of lines (Fig. 1), differing only in the structure of the remaining neighbour class of lines. Selecting properly seven points (bold circles) of a different neighbour class each, with the help of Fig. 1 it can easily be checked that no three of them are collinear in the former case (*left*) while this property fails in the latter case (*right*) as there exists a triple lying on the same line (namely that represented by a dot-dashed curve).

4. Conclusion

To conclude, it must be stressed that this remarkable analogy between complete sets of MUBs and ovals/conics is worked out at the level of cardinalities only and thus still remains a conjecture. Hence, the next crucial step to be done is to construct an expliciting mapping by associating a MUB to each neighbour class of the points of the conic and a state vector of this MUB to a particular point of the class. This is a much more delicate issue, as there are (at least) two non-isomorphic kinds of projective Hjelmslev planes of order $q = p^r$ that have exactly the same "cardinality" properties, viz. the plane defined over the Galois ring $GR(p^2, r)$ and the one defined over the ring of "dual" numbers, $GF(q)[x]/(x^2) \cong GF(q)+e\,GF(q)$, where $e^2 = 0, e \neq 0$. Even for the simplest case ($p = 2$ and $r = 1$) there is an intricate difference in geometry between the two planes, as the former contains ($q^2 + q + 1 =$)7-arcs, while the latter not (see, e.g., Ref. 18 and Fig. 2); it is also worth noticing that while in the former plane the quadratic forms $\mathcal{Q}^{(+)}$ and $\mathcal{Q}^{(-)}$ define, as we have seen, *two distinct* proper conics, in the latter one these forms represent *one and the same* conic because the ring $GF(2)[x]/(x^2)$ is of characteristic *two* (and, so, enjoying the property $+1 = -1$). A thorough exploration of the fine structure of these two Hjelmslev geometries, as well as of a number of other finite Hjelmslev and related ring planes[19,20] and geometries,[21] is therefore a principal theoretical task for making further progress in this direction. To furnish this task, we have already made an important step by addressing the structure of a projective plane over the ring of double numbers over Galois fields.[22]

Acknowledgments

The first author is grateful to Prof. Olav Arnfinn Laudal for a number of enlightening comments concerning the structure of projective geometries over (Galois) rings and to Prof. Mark Stuckey for being a great help to him in obtaining a copy of Ref. 13. We also thank Mr. Pavol Bendík for careful drawing of the figures and Dr. Richard Komžík for computer-related assistance. This work was supported in part by the Science and Technology Assistance Agency (Slovak Republic) under the contract No. APVT–51–012704 and by the VEGA project # 2/6070/26 (Slovak Republic).

References

1. M. Saniga, M. Planat and H. Rosu, *J. Opt. B: Quantum Semiclass. Opt.* **6**, L19 (2004).
2. M. Planat and H. Rosu, *Europ. Phys. J.* **D36**, 133 (2005).
3. P. Oscar Boykin, M. Sitharam, P. H. Tiep and P. Wocjan, "Mutually unbiased bases and orthogonal decompositions of Lie algebras", quant-ph/0506089.
4. A. Klappenecker and M. Roetteler, "Mutually unbiased bases are complex projective 2-designs", quant-ph/0502031.
5. M. Aschbacher, A. M. Childs and P. Wocjan, "The limitations of nice mutually unbiased bases", quant-ph/0412066.
6. I. Bengtsson and A. Ericsson, *Open Systems and Information Dynamics* **12**, 107 (2005).
7. T. Durt, *J. Phys. A: Math. Gen.* **38**, 5267 (2005).
8. A. Klappenecker and M. Roetteler, *Lecture Notes in Computer Science* **2948**, 137 (2004).
9. W. K. Wootters, *Foundations of Physics* (2004), to appear.
10. M. Saniga and M. Planat, *Chaos, Solitons and Fractals* **26**, 1267 (2005).
11. J. Hjelmslev, *Abh. Math. Sem. Univ. Hamburg* **2**, 1 (1923).
12. W. Klingenberg, *Math. Z.* **60**, 384 (1954).
13. E. Kleinfeld, *Illinois J. Math.* **3**, 403 (1959).
14. P. Dembowski, *Finite Geometries* (Springer, Berlin — New York, 1968), pp. 291–300.
15. Z. X. Wan, *Lectures on Finite Fields and Galois Rings* (World Scientific, New Jersey — London — Singapore — Hong Kong, 2003), pp. 309–333.
16. J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields* (Oxford University Press, Oxford, 1998).
17. V. Chvál and R. Jurga, *Math. Slovaca* **48**, 69 (1998).
18. T. Honold and I. Landjev, *Discrete Math.* **231**, 265 (2001).
19. F. D. Veldkamp, *Geom. Dedicata* **11**, 285 (1981).
20. F. D. Veldkamp, in *Handbook of Incidence Geometry*, ed F. Buekenhout (Elsevier Science, Amsterdam, 1995), pp. 1033–1084.
21. A. Herzer, in *Handbook of Incidence Geometry*, ed F. Buekenhout (Elsevier Science, Amsterdam, 1995), pp. 781–842.
22. M. Saniga and M. Planat, "Projective planes over "Galois" double numbers and a geometrical principle of complementarity", math.NT/0601261.