INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 435–440 doi:10.1088/0305-4470/39/2/013

Hjelmslev geometry of mutually unbiased bases

Metod Saniga[1] **and Michel Planat**[2]

[1] Astronomical Institute, Slovak Academy of Sciences, 05960 Tatranská Lomnica, Slovak Republic
[2] Institut FEMTO-ST, CNRS, Laboratoire de Physique et Métrologie des Oscillateurs, 32 Avenue de l'Observatoire, F-25044 Besançon, France

E-mail: msaniga@astro.sk and planat@lpmo.edu

Received 24 June 2005, in final form 9 November 2005
Published 14 December 2005
Online at stacks.iop.org/JPhysA/39/435

Abstract
The basic combinatorial properties of a complete set of mutually unbiased bases (MUBs) of a q-dimensional Hilbert space $\mathcal{H}_q$, $q = p^r$ with p being a prime and r a positive integer, are shown to be 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.

PACS numbers: 02.10.Hh, 02.40.Dr, 03.65.Ca
Mathematics Subject Classification: 51C05, 81R99, 81Q99

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., [1–9] 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 a projective plane of order q. In this paper, we extend and qualitatively finalize this picture by showing that individual vectors of all such bases can also 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].

To this end, we shall first introduce the basics of the Galois ring theory (see, e.g., [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 $\mathrm{GR}(p^2, r) \equiv \mathcal{Z}_{p^2}[x]/(f)$ is a ring, called a *Galois ring*, of characteristic p^2 and rank r, whose maximal ideal is $p\mathrm{GR}(p^2, r)$. 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 $\mathrm{GR}(p^2, r)$ can uniquely be written in the form

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

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

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

having

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

elements. From equation (1) it is obvious that g is a unit (i.e., an invertible element) of $\mathrm{GR}(p^2, r)$ iff $a \neq 0$ and a zero divisor iff $a = 0$. It then follows that $\mathrm{GR}(p^2, r)$ has $\#_{\mathrm{t}} = q^2$ elements in total, out of which there are $\#_{\mathrm{z}} = q$ zero divisors and $\#_{\mathrm{u}} = q^2 - q = q(q-1)$ units. Next, let '$\overline{\ }$' denote reduction modulo p; then obviously $\overline{\mathcal{T}}_r = \mathrm{GF}(q)$, the Galois *field* of order q, and $\overline{\zeta}$ is a primitive element of $\mathrm{GF}(q)$. 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 $\mathrm{GR}(p^2, r)$, henceforth referred to as $\mathrm{PH}(2, q)$.[3] $\mathrm{PH}(2, q)$ is an incidence structure whose points are classes of ordered triples $(\varrho\check{x}_1, \varrho\check{x}_2, \varrho\check{x}_3)$, where both ϱ and at least one $\check{x}_i$ $(i = 1, 2, 3)$ are units, whose lines are classes of ordered triples $(\sigma\check{l}_1, \sigma\check{l}_2, \sigma\check{l}_3)$, where both σ and at least one $\check{l}_i$ $(i = 1, 2, 3)$ are units, and the incidence relation is given by

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

From this definition it follows that in $\mathrm{PH}(2, q)$—as in any *ordinary* projective plane—there is a perfect duality between points and lines; that is, instead of 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

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

points/lines and that the number of points/lines incident with a given line/point is, in light of equation (4), equal to the number of non-equivalent couples $(\varrho\check{x}_1, \varrho\check{x}_2)/(\sigma\check{l}_1, \sigma\check{l}_2)$, 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 $\overline{\#}_{\mathrm{coup}} = q + 1$ (e.g., [16]).

Any projective Hjelmslev plane, $\mathrm{PH}(2, q)$ 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., [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;

[3] 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 [12–14].

otherwise, they are called non-neighbour or remote. The same symbol and the dual definition are 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 $\varrho\check{x}_i$, $i = 1, 2, 3$, the points that are its neighbours must be of the form $\varrho(\check{x}_i + p\check{y}_i)$, with $\check{y}_i \in \mathcal{T}_r$; for two points are neighbour iff their corresponding coordinates differ by a zero divisor [12–14]. Although there are q^3 different choices for the triple $(\check{y}_1, \check{y}_2, \check{y}_3)$, only $q^3/q = q^2$ of the classes $\varrho(\check{x}_i + p\check{y}_i)$ represent distinct points because $\varrho(\check{x}_i + p\check{y}_i)$ and $\varrho(\check{x}_i + p(\check{y}_i + \kappa\check{x}_i))$ 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 $(q^2/q =)\, q$ 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), $A \odot B$ imply $B \odot A$ (symmetry) and $A \odot B$ and $B \odot C$ imply $A \odot C$ (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 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 figure 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*, which is a curve $\mathcal{Q}$ of PH(2, q) whose points obey the equation

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

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., [17]) that the equation of a proper conic of PH(2, q) can always be brought into a 'canonical' form

$$\mathcal{Q}^\star : \check{x}_1\check{x}_3 - \check{x}_2^2 = 0 \tag{8}$$

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

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

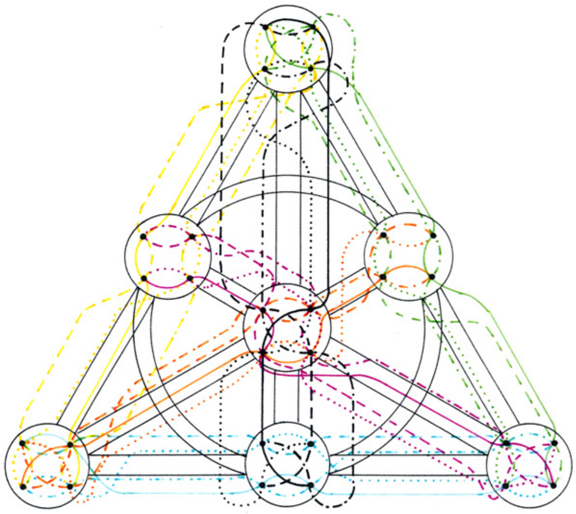

Figure 1. A schematic sketch of the structure of the simplest projective Hjelmslev plane, PH(2, 2). Shown are all the 28 of its points (represented by small filled circles), grouped into seven pairwise disjoint sets (neighbour classes), each of cardinality 4, as well as 24 of its lines (drawn as solid, 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 colours. 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. Note 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.

(This figure is in colour only in the electronic version)

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

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

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

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

and there are obviously 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). To illustrate the case, several proper conics in PH(2, 2) are shown in figure 2.

At this point our algebraic geometrical machinery is elaborate enough to generalize and qualitatively complete the geometrical picture of MUBs proposed in [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 in the manner of 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

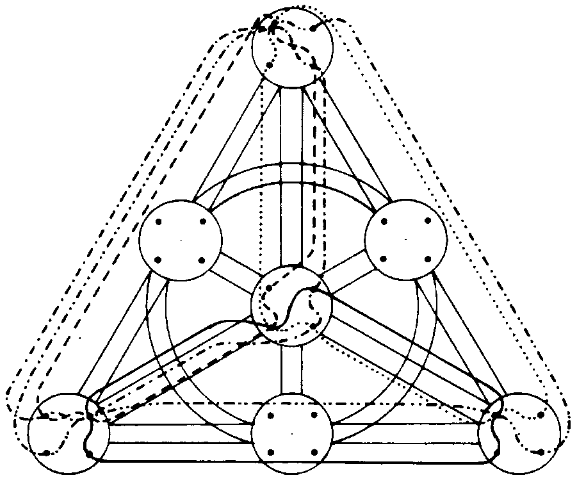

Figure 2. The forms of five different proper conics located in PH(2, 2): $\breve{x}_1\breve{x}_3 - \breve{x}_2^2 = 0$ (solid curve), $\breve{x}_1\breve{x}_2 - \breve{x}_3^2 = 0$ (dashed), $\breve{x}_2\breve{x}_3 - \breve{x}_1^2 = 0$ (dotted), $\breve{x}_1\breve{x}_2 + \breve{x}_3^2 = 0$ (dot-dashed) and $\breve{x}_1\breve{x}_2 + \breve{x}_1\breve{x}_3 + \breve{x}_2\breve{x}_3 = 0$ (dash-doubledotted). Note the intricacies of pairwise intersections between the conics.

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 [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.

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 is to construct an explicit mapping by associating a MUB with each neighbour class of the points of the conic and a state vector of this MUB with 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, namely, the plane defined over the Galois ring GR(p^2, r) and the one defined over the ring of 'dual' numbers, $\mathrm{GF}(q)[x]/(x^2) \cong \mathrm{GF}(q) + eGF(q)$, where $e^2 = 0$. 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 does not (see, e.g., [18]). 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, is therefore a principal theoretical task for making further progress in this direction.

Acknowledgments

The first author is grateful to Professor Olav Arnfinn Laudal for a number of enlightening comments concerning the structure of projective geometries over (Galois) rings and to Professor Mark Stuckey for being a great help to him in obtaining a copy of [13]. We also thank two of the referees for their constructive comments and Mr Pavol Bendík for careful drawing of the figures.

References

[1] Planat M and Rosu H 2005 Mutually unbiased phase states, phase uncertainties, and Gauss sums *Eur. Phys. J.* D **36** 133 (*Preprint* quant-ph/0506128)

[2] Oscar Boykin P, Sitharam M, Tiep P H and Wocjan P 2005 Mutually unbiased bases and orthogonal decompositions of Lie algebras *Preprint* quant-ph/0506089

[3] Klappenecker A and Roetteler M 2005 Mutually unbiased bases are complex projective 2-designs *Preprint* quant-ph/0502031

[4] Aschbacher M, Childs A M and Wocjan P 2004 The limitations of nice mutually unbiased bases *Preprint* quant-ph/0412066

[5] Bengtsson I and Ericsson A 2005 Mutually unbiased bases and the complementarity polytope *Open Syst. Inf. Dyn.* **12** 107 (*Preprint* quant-ph/0410120)

[6] Durt T 2005 About mutually unbiased bases in even and odd prime power dimensions *J. Phys. A: Math. Gen.* **38** 5267 (*Preprint* quant-ph/0409090)

[7] Klappenecker A and Roetteler M 2004 Constructions of mutually unbiased bases *Lect. Notes Comput. Sci.* **2948** 137 (*Preprint* quant-ph/0309120)

[8] Wootters W K 2004 Quantum measurements and finite geometry *Preprint* quant-ph/0406032 (*Found. Phys.* to appear)

[9] Saniga M, Planat M and Rosu H 2004 Mutually unbiased bases and finite projective planes *J. Opt. B: Quantum Semiclass. Opt.* **6** L19 (*Preprint* math-ph/0403057)

[10] Saniga M and Planat M 2005 Viewing sets of mutually unbiased bases as arcs in finite projective planes *Chaos Solitons Fractals* **26** 1267 (*Preprint* quant-ph/0409184)

[11] Hjelmslev J 1923 Die natürliche geometrie *Abh. Math. Sem. Univ. Hamburg* **2** 1

[12] Klingenberg W 1954 Projektive und affine Ebenen mit Nachbarelementen *Math. Z.* **60** 384

[13] Kleinfeld E 1959 Finite Hjelmslev planes *Illinois J. Math.* **3** 403

[14] Dembowski P 1968 *Finite Geometries* (Berlin–New York: Springer) pp 291–300

[15] Wan Z-X 2003 *Lectures on Finite Fields and Galois Rings* (NJ–London–Singapore–Hong Kong: World Scientific) pp 309–33

[16] Hirschfeld J W P 1998 *Projective Geometries Over Finite Fields* (Oxford: Oxford University Press)

[17] Chvál V and Jurga R 1998 Tangents of conics in Hjelmslev planes over a local ring of even characteristic *Math. Slovaca* **48** 69

[18] Honold T and Landjev I 2001 On arcs in projective Hjelmslev planes *Discrete Math.* **231** 265