J. Opt. B: Quantum Semiclass. Opt. **6** (2004) L19–L20 PII: S1464-4266(04)82660-0

## LETTER TO THE EDITOR

# Mutually unbiased bases and finite projective planes

**Metod Saniga[1,4], Michel Planat[2] and Haret Rosu[3]**

[1] Astronomical Institute, Slovak Academy of Sciences, 05960 Tatranská Lomnica, Slovak Republic
[2] Institut FEMTO-ST, Département LPMO, CNRS, 32 Avenue de l'Observatoire, 25044 Besançon, France
[3] Department of Applied Mathematics, IPICyT, Apartado Postal 3-74 Tangamanga, San Luis Potosí, Mexico

E-mail: msaniga@astro.sk

Received 30 June 2004, accepted for publication 19 July 2004
Published 23 July 2004
Online at stacks.iop.org/JOptB/6/L19
doi:10.1088/1464-4266/6/9/L01

**Abstract**
It is conjectured that the question of the existence of a set of $d + 1$ mutually unbiased bases in a $d$-dimensional Hilbert space if $d$ differs from a power of a prime number is intimately linked with the problem of whether there exist projective planes whose order $d$ is not a power of a prime number.

**Keywords:** mutually unbiased bases, MUBs, finite projective planes, Hopf fibrations

Recently, there has been a considerable resurgence of interest in the concept of the so-called mutually unbiased bases (see, e.g., [1–7]), especially in the context of quantum state determination, cryptography, quantum information theory and the King problem. We recall that two different orthonormal bases $A$ and $B$ of a $d$-dimensional Hilbert space $\mathcal{H}^d$ are called *mutually unbiased* if and only if $|\langle a|b\rangle| = 1/\sqrt{d}$ for all $a \in A$ and all $b \in B$. An aggregate of mutually unbiased bases is a set of orthonormal bases which are pairwise mutually unbiased. It has been found that the maximum number of such bases cannot be greater than $d + 1$ [8, 9]. It is also known that this limit is reached if $d$ is a power of a prime number. Yet, a still unanswered question is whether there are non-prime-power values of $d$ for which this bound is attained. The purpose of this letter is to draw the reader's attention to the fact that the answer to this question may well be related to the (non-)existence of finite projective planes of certain orders.

A finite *projective* plane is an incidence structure consisting of points and lines such that any two points lie on just one line, any two lines pass through just one point, and there exist four points, no three of them on a line [10]. From these properties it readily follows that for any finite projective plane there exists an integer $d$ with the properties that any line contains exactly $d + 1$ points, any point is the meet of exactly $d+1$ lines, and the number of points is the same as the number of lines, namely $d^2+d+1$. This integer $d$ is called the *order* of the projective plane. The most striking issue here is that the order of known finite projective planes is a power of a prime number [10]. The question of which other integers occur as orders of finite projective planes remains one of the most challenging problems of contemporary mathematics. The only 'no-go' theorem known so far in this respect is the Bruck–Ryser theorem [11] saying that there is no projective plane of order $d$ if $d-1$ or $d-2$ is divisible by four and $d$ is not the sum of two squares. Out of the first few non-prime-power numbers, this theorem rules out finite projective planes of orders 6, 14, 21, 22, 30 and 33. Moreover, using massive computer calculations, it was proved by Lam [12] that there is no projective plane of order ten. It is surmised that the order of *any* projective plane is a power of a prime.

From what has already been said it is quite tempting to hypothesize that the above described two problems are nothing but different aspects of one and the same problem. That is, we conjecture that *non-existence of a projective plane of the given order d implies that there are less than d+1 mutually unbiased bases (MUBs) in the corresponding* $\mathcal{H}^d$, and vice versa. Or,

[4] Author to whom any correspondence should be addressed.

slightly rephrased, we say that if the dimension $d$ of Hilbert space is such that the maximum of MUBs is less than $d + 1$, then there does not exist any projective plane of this particular order $d$.

An important observation speaking in favour of our claim is the following one. Let us find the minimum number of different measurements we need to determine uniquely the state of an ensemble of identical $d$-state systems. The density matrix of such an ensemble, being Hermitian and of unit trace, is specified by $(2d^2/2) - 1 = d^2 - 1$ real parameters. As a given non-degenerate measurement applied to a sub-ensemble gives $d - 1$ real numbers (the probabilities of all but one of the $d$ possible outcomes), the minimum number of different measurements needed to determine the state uniquely is $(d^2 - 1)/(d - 1) = d + 1$ [8]. On the other hand, it is a well known fact (see, e.g., [13]) that the number of $k$-dimensional linear subspaces of the $n$-dimensional projective space over Galois fields of order $d$ is given by

$$\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_d \equiv \frac{(d^{n+1}-1)(d^{n+1}-d)\cdots(d^{n+1}-d^k)}{(d^{k+1}-1)(d^{k+1}-d)\cdots(d^{k+1}-d^k)},$$

which for the number of *points* ($k = 0$) of a projective *line* ($n = 1$) yields

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_d = (d^2 - 1)/(d - 1) = d + 1.$$

Another piece of support for our conjecture comes from the ever increasing use of geometry in describing simple quantum mechanical systems. Here we would like to point out the crucial role the so-called Hopf fibrations play in modelling one-qubit, two-qubit and three-qubit states. Namely, the $s$-qubit states, $s = 1, 2, 3$, are intimately connected with the Hopf fibration of type $S^{2^{(s+1)}-1} \xrightarrow{S^{2^s-1}} S^{2^s}$ [14–16], and there exists an isomorphism between the sphere $S^{2^s}$, $s = 1, 2, 3$, and the *projective line* over the algebra of complex numbers, quaternions and octonions, respectively [17].

Perhaps the most serious backing of our surmise is found in a recent paper by Wootters [18]. Associating a line in a finite geometry with a pure state in the quantum problem, the author shows that a complete set of MUBs is, in some respects, analogous to a finite *affine* plane, and another kind of quantum measurement, the so-called symmetric informationally complete positive-operator-valued measure (SIC POVM), is also analogous to the same configuration, but with the swapped roles of points and lines. It represents no difficulty to show that this 'dual' view of quantum measurement is deeply rooted in our conjecture. To this end, it suffices to recall two facts [10]. First, any affine plane is a particular subplane (subgeometry) of a projective plane, namely a plane which arises from the latter if one *line*, the so-called 'line at infinity', is deleted. Second, in a projective plane, there is a perfect *duality* between points and lines; that means, to every projective plane, $S_2$, there exists a dual projective plane, $\Sigma_2$, whose points are the lines of $S_2$ and whose lines are the points of $S_2$ [19]. So, *affinizing* $S_2$ means deleting a *point* of $\Sigma_2$ and thus, in light of our conjecture, qualitatively recovering the results of Wootters, also shedding important light on some others of the most recent findings [20, 21]. The latter reference, in fact, gives several strong arguments that there are no more than three MUBs in dimension six, the smallest non-prime-power dimension.

Finally, at the level of applications, finite projective spaces have already found their proper place in classical enciphering [10]. By identifying the points of a (finite) projective space with the eigenvectors of the MUBs endowed with a Singer cycle structure one should, in principle, be able to engineer quantum enciphering procedures. These should play a role in the emerging quantum technologies of quantum cryptography and quantum computing [22].

## References

[1] Chaturvedi S 2002 *Phys. Rev.* A **65** 044301 (*Preprint* quant-ph/0109003)
[2] Bandyopadhay S, Boykin O P, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512–28 (*Preprint* quant-ph/0103162)
[3] Klappenecker A and Rötteler M 2003 Constructions of mutually unbiased bases *Preprint* quant-ph/0309120
[4] Archer C 2003 There is no generalization of known formulas for mutually unbiased bases *Preprint* quant-ph/0312204
[5] Gibbons K S, Hoffman M J and Wootters W K 2004 Discrete phase space based on finite fields *Preprint* quant-ph/0401155
[6] Aravind P K 2002 Solution to the King's problem in prime power dimensions *Preprint* quant-ph/0210007
[7] Lawrence J, Brukner Č and Zeilinger A 2002 *Phys. Rev.* A **65** 032320 (*Preprint* quant-ph/0104012)
[8] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363–81
[9] Calderbank A R, Cameron P J, Kantor W M and Seidel J J 1997 *Proc. Lond. Math. Soc.* **75** 436–80
[10] Beutelspacher A and Rosenbaum U 1998 *Projective Geometry: From Foundations to Applications* (Cambridge: Cambridge University Press)
[11] Bruck R H and Ryser H J 1949 *Can. J. Math.* **1** 88–93
[12] Lam C W H 1991 *Am. Math. Month.* **98** 305–18
[13] Hirschfeld J W P 1998 *Projective Geometries Over Finite Fields* (Oxford: Oxford University Press) p 87
[14] Mosseri R and Dandoloff R 2001 *J. Phys. A: Math. Gen.* **34** 10243–52
[15] Bernevig B A and Chen H-D 2003 *J. Phys. A: Math. Gen.* **36** 8325–39 (*Preprint* quant-ph/030208)
[16] Mosseri R 2003 Two and three qubit geometry and Hopf fibrations *Preprint* quant-ph/0310053
[17] Baez J C 2002 *Bull. Am. Math. Soc.* **39** 145–205
[18] Wootters W K 2004 Quantum measurements and finite geometry *Preprint* quant-ph/0406032
[19] Levy H 1964 *Projective and Related Geometries* (New York: Macmillan) p 108
[20] Bengtsson I 2004 MUBs, polytopes, and finite geometries *Preprint* quant-ph/0406174
[21] Grassl M 2004 On SIC-POVMs and MUBs in dimension six *Preprint* quant-ph/0406175
[22] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902 (*Preprint* quant-ph/0107130)