



Problem 13

## Mutually unbiased bases

contact:	B.-G. Englert	solved by:	—
date:	31 Jan 2003	last progress:	07 Jan 2004

Version of 11 Apr 2005

For information about the QI open problems project at IMaPh refer to the web-pages <http://www.imaph.tu-bs.de/qi/problems/>. Please support us by suggesting further interesting problems!

For questions, partial results or solutions concerning this problem please contact B.-G. Englert at <http://www.imaph.tu-bs.de/qi/links.html>.

## Problem

Determine the maximal number  $K$  of orthonormal bases in a  $D$ -dimensional Hilbert space, which are mutually unbiased in the following sense: If  $e_i^k$  denotes the  $i$ th vector of the  $k$ th basis, all scalar products  $\langle e_i^k, e_j^n \rangle$  with  $k \neq n$  have the same absolute value (namely  $D^{-1/2}$ ).

It is known that if  $D$  is the power of a prime,  $K = D + 1$  can be reached, but this is not known for any other composite number. So the problem is already to decide whether there exist  $K = 7$  mutually unbiased bases in  $D = 6$  dimensions.

## Background

The problem comes up in at least three (related) contexts:

(1) **State determination** [Iv], [WF]

Suppose we want to determine the density operator of a source by measuring  $K$  observables (with  $D$  one-dimensional projections each). Each such measurement allows us to determine  $D-1$  independent parameters, so we can determine  $K(D-1)$  out of  $D^2 - 1$  parameters in the density operator. Hence  $K = D + 1$  should suffice. In order to achieve best estimation results, the measurements should duplicate no information already contained in other measurements, i. e., the observables should be pairwise complementary, or the bases mutually unbiased in the above sense.

(2) **Cryptography**

Suppose Alice sends  $D$ -level systems prepared in one of the  $D$  pure states  $e_i^k$  belonging to a set of  $K$  orthonormal bases agreed between Alice and Bob. If Bob measures in the same basis, he can decode the value  $i$  perfectly. In cryptography one also wants that if an eavesdropper measures the system in any one of the other bases, she can extract no information whatsoever about  $i$ . This requires the bases to be mutually unbiased.

It is known that a higher error level can be tolerated in the channel for protocols using maximal families of mutually unbiased bases (e. g., the “six state protocol”,  $D = 2$ ,  $K = 3$ ) rather than non-maximal ones (e. g., BB84, using  $D = 2$ ,  $K = 2$ ).

(3) **The Mean King** [AE]

A ship-wrecked physicist gets stranded on a far-away island that is ruled by a mean king who loves cats and hates physicists since the day when he first heard what happened to Schrödinger’s cat. A similar fate is awaiting the stranded physicist. Yet, mean as he is, the king enjoys defeating physicists on their own turf, and therefore he maliciously offers an apparently virtual chance of rescue.

He takes the physicist to the royal laboratory, a splendid place where experiments of any kind can be performed perfectly. There the king invites the physicist to prepare a certain silver atom in any state she likes. The king's men will then measure one of the three cartesian spin components of this atom – they'll either measure  $\sigma_x$ ,  $\sigma_y$ , or  $\sigma_z$  without, however, telling the physicist which one of the measurements is actually done. Then it is again the physicist's turn, and she can perform any experiment of her choosing. Only after she's finished with it, the king will tell her which spin component had been measured by his men. To save her neck, the physicist must then state correctly the measurement result that the king's men had obtained.

Much to the king's frustration, the physicist rises to the challenge – and not just by sheer luck: She gets the right answer any time the whole procedure is repeated. How does she do it?

More generally, the king's men might be allowed to perform one out of  $K$  complete von Neumann measurements on a  $D$ -dimensional system. The problem first came up in [VA+], together with a solution for  $D = 2$ . Solutions involving mutually unbiased bases are presented in [AE], [Ara], [Arb], [EA]. Confer also the experimental realization in [SS+].

## Partial Results

H. Barnum [Ba] points out a close connection of this problem with “spherical 2-designs”, which are collections of pure states such that the average of a polynomial of degree 2 on these states equals the integral of the polynomial over all pure states.

For the case  $D = 6$  there are a number of different but equivalent formulations of this problem.

A. Pittenger and M. Rubin [PR] give a constructive proof for the case of prime power dimension [WF]. They also address the question of separability and provide an appendix on the necessary parts of algebraic field extensions. Another proof can be found in [KR].

C. Archer [Arc] shows that even generalizations of these constructions do not extend the results beyond prime power dimension.

## References

- [AE] Y. Aharonov, B.-G. Englert, *The mean king's problem: Spin 1*, Z. Naturforsch. **56a**, 16 (2001) and quant-ph/0101065 (2001).
- [Ara] P.K. Aravind, *Solution to the King's Problem in prime power dimensions*, Z. Naturforsch. **58a**, 2212 (2003) and quant-ph/0210007 (2002).

- [Arb] P.K. Aravind, *Best conventional solutions to the King's Problem*, quant-ph/0306119 (2003).
- [Arc] C. Archer, *There is no generalization of known formulas for mutually unbiased bases*, quant-ph/0312204 (2003).
- [Ba] H. Barnum, *Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases*, quant-ph/0205155 (2002).
- [EA] B.-G. Englert, Y. Aharonov, *The mean king's problem: Prime degrees of freedom*, Phys. Lett. A **284**, 1 (2001) and quant-ph/0101134 (2001).
- [Iv] I. D. Ivanovic, *Geometrical description of quantal state determination*, J. Phys. A **14**, 3241 (1981).
- [KR] A. Klappenecker, M. Roetteler, *Constructions of Mutually Unbiased Bases*, quant-ph/0309120 (2003).
- [PR] A. O. Pittenger and M. H. Rubin, *Mutually Unbiased Bases, Generalized Spin Matrices and Separability*, quant-ph/0308142 (2003).
- [SS+] O. Schulz, R. Steinhübl, M. Weber, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, *Ascertaining the Values of  $\sigma_x$ ,  $\sigma_y$ , and  $\sigma_z$  of a Polarization Qubit*, quant-ph/0209127 (2002).
- [VA+] L. Vaidman, Y. Aharonov, and D. Z. Albert, *How to ascertain the values of  $\sigma_x$ ,  $\sigma_y$ , and  $\sigma_z$  of a spin-1/2 particle*, Phys. Rev. Lett. **58**, 1385 (1987).
- [WF] W.K. Wootters, B.D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Phys. **191**, 363 (1989).