Meaner king uses biased bases

Michael Reimpell and Reinhard F. Werner
Institut für Mathematische Physik, Technische Universität Braunschweig, Mendelssohnstraße 3, D-38106 Braunschweig, Germany

(Received 14 December 2006; revised manuscript received 22 May 2007; published 28 June 2007)

The mean king problem is a quantum mechanical retrodiction problem, in which Alice has to name the outcome of an ideal measurement made in one of several different orthonormal bases. Alice is allowed to prepare the state of the system and to do a final measurement, possibly including an entangled copy. However, Alice gains knowledge about which basis was measured only after she no longer has access to the quantum system or its copy. We give a necessary and sufficient condition on the bases, for Alice to have a strategy to solve this problem, without assuming that the bases are mutually unbiased. The condition requires the existence of an overall joint probability distribution for random variables, whose marginal pair distributions are fixed as the transition probability matrices of the given bases. In particular, in the qubit case the problem is decided by Bell's original three variable inequality. In the standard setting of mutually unbiased bases, when they do exist, Alice can always succeed. However, for randomly chosen bases her success probability rapidly goes to zero with increasing dimension.

DOI: 10.1103/PhysRevA.75.062334 PACS number(s): 03.67.−a, 02.50.Cw, 03.65.Ta

I. INTRODUCTION

The mean king problem was first introduced by Vaidman *et al.* [1], and has since received a lot of attention as a basic quantum mechanical retrodiction problem: In the story, physicist Alice faces the mean king, who asks her to prepare a quantum system, on which his men will perform a von Neumann measurement in one of a specified set of orthonormal bases. Alice is not present during this measurement, and knows neither the basis chosen nor the result obtained. She is then allowed a final check on the system (typically including entangled records of the initial preparation), leaving her with some classical measurement values only. She is then told which basis was used and is asked to correctly name the values found by the king's men. In this article we establish a simple necessary and sufficient condition on the king's bases to decide whether Alice can solve this problem with certainty.

The solution to the mean king problem appears to be paradox: For the given state, the measurement results of the three incompatible spin components can be reconstructed from the results of a single measurement on the system and an entangled copy.

Apart from its foundational interest, in a cryptographic setting the scheme allows to get a raw key bit from every quantum particle exchanged, without having to discard some particles because of mismatched bases.

Most works on this subject assume that the king uses mutually unbiased bases (MUB), which means that after preparing a basis state of any of these bases, the probability distributions in all other bases will be uniform. It was shown that a maximal set of $(d+1)$ mutually unbiased bases exist for a d-dimensional Hilbert space, whenever d is a power of a prime [2,3], and that Alice can always retrodict the outcome in this case [4]. But to decide the existence of such a set for other dimensions (e.g., $d=6$) has proved to be very hard [5].

However, the basic statement of the problem makes no reference to the MUB property of the king's bases. It might seem as the hardest case for Alice, because if the game were to be played many times, Alice could improve her guesses using the correlations between bases. This gain is nullified in the MUB case. But the problem is not set like that: We demand of a solution that Alice is right *in every single run*, and this is not made easier in the least by the existence of some statistical correlations between the bases. In other words, the intuition that unbiased bases are an especially mean choice by the king is fallacious.

We therefore drop the assumption of unbiasedness and ask, for *any* choice of finitely many bases by the king: Can Alice find a strategy, consisting of an initial entangled preparation and a suitable measurement on the joint system after the king's men are through with their part, such that she gets the right value with probability one?

Not very much has been done about the retrodiction problem without assuming mutual unbiasedness. Some special cases have been discussed in [4,6–9]. However, the available studies apparently remain incomplete even in the qubit case.

II. SUMMARY OF RESULTS

To state our main results, let us fix some notation for the rest of the paper. The system Hilbert space on which the king's men make their measurement will be denoted by $\mathcal{H}$, and has dimension d. The number of bases chosen will be k, and the bases themselves will be denoted by $\Phi_b(i)$, for $b=1,\ldots,k$ and $i=1,\ldots,d$. An important property of a choice of bases is the space $\mathcal{R}$ of Hermitian operators spanned by all the $|\Phi_b(i)\rangle\langle\Phi_b(i)|$. This space describes how many density operators we can distinguish with measurements in the given bases. Since $\Sigma_i|\Phi_b(i)\rangle\langle\Phi_b(i)|=\mathbb{1}$ for any basis, we expect only $(d-1)$ dimensions giving new information for each basis, so together with the identity we expect $\mathcal{R}$ to be $[k(d-1)+1]$-dimensional. If this number is achieved, we will call the chosen basis set *nondegenerate*. Of course, dim $\mathcal{R}$ cannot exceed the dimension d^2 of the space of all Hermitian operators on $\mathcal{H}$, so for $k>(d+1)$ every choice of bases is degenerate in this sense. The interesting property in this case is that dim $\mathcal{R}=d^2$, i.e., that the set of bases is *tomographically complete*. Of course, for $k=(d+1)$, which is the standard case, nondegeneracy and tomographic completeness are the same property.

For any pair of bases, the values

$$p_{bc}(i,j) = \frac{1}{d}|\langle\Phi_b(i)|\Phi_c(j)\rangle|^2 \tag{1}$$

are the joint probabilities of a pair of d-valued random variables, each of which is uniformly distributed. We say that a collection of k bases *admits a classical model*, if these probabilities are marginals of some joint distribution of all k variables (each taking d values). Since this property only involves the absolute values of scalar products, not their phases, and therefore captures only a small part of the information about the relative position of the bases, it is perhaps rather unexpected that the existence of a classical model is very closely linked to the existence of Alice's strategy. This is described in the following theorem, our main result.

Theorem. Let $\{\Phi_b(i)\}$ *be a collection of* k *orthonormal bases in a* d *dimensional Hilbert space. Then* (1) *if the bases are nondegenerate* [*in particular*, $k\leq(d+1)$] *and the bases admit a classical model*, *then Alice can find a safe strategy in the mean king's problem with these bases*. (2) *Conversely*, *if the set of bases is tomographically complete* [*in particular*, $k\geq(d+1)$], *and if Alice has a strategy*, *then the bases allow a classical model*. (3) *In the case* (1), *Alice's strategy may begin with a maximally entangled state*, *and in the case (2) a pure initial state is necessarily maximally entangled.*

Before going into the proof, let us see what this theorem says about some basic examples.

A. Mutually unbiased bases

By definition a set of k bases in d dimensions is mutually unbiased if, with the notation from Eq. (1), we have

$$p_{bc}(i,j) = \delta_{bc}\delta_{ij}\frac{1}{d} + (1-\delta_{bc})\frac{1}{d^2}. \tag{2}$$

From this a classical model is obvious, namely k *statistically independent* uniformly distributed random variables. In order to compute the dimension of the span of the $|\Phi_b(i)\rangle\langle\Phi_b(i)|$, let us take the $(kd)\times(kd)$ matrix of Hilbert Schmidt scalar products [defined for operators A,B by $\langle A|B\rangle_{\text{HS}}:=\text{tr}(A^*B)$] of these vectors, which is just the expression (2), interpreted as a matrix $M_{bi,cj}$. Its rank is the dimension we are looking for, and easily computed as $k(d-1)+1$, by determining all eigenvalues of M. Hence MUBs are nondegenerate for all $k\leq(d+1)$, and for any number of MUBs the mean king can come up with, Alice has a strategy. This result was previously obtained by another method in [4].

B. Qubits

Another interesting special case, discussed in [6], is $d=2$, $k=3$. Choosing a basis in $d=2$ is the same as choosing a pair of antipodal points on the Bloch sphere. Three bases are tomographically complete iff these points do not lie in a plane. The existence of a classical model in this case is one of the ancestral problems of quantum information theory, namely precisely the existence of such models for three dichotomic variables characterized by Bell's original three-variable inequality [10]. The joint distribution (1) belonging to two bases b, c is characterized (for $d=2$) by the single number $p_{bc}(1,1)$. Figure 1 shows the possible range of triples $[p_{ab}(1,1),p_{bc}(1,1),p_{ca}(1,1)]$. The range of triples admitting a classical model, and hence a safe strategy for Alice, is described by Bell's inequalities as the tetrahedron inside this body. If the bases are chosen independently and with unitarily invariant distribution (Haar measure), the probability for this subset is exactly 1/3. This can be computed analytically by reducing it to a problem of three independent uniformly distributed vectors on the Bloch sphere.

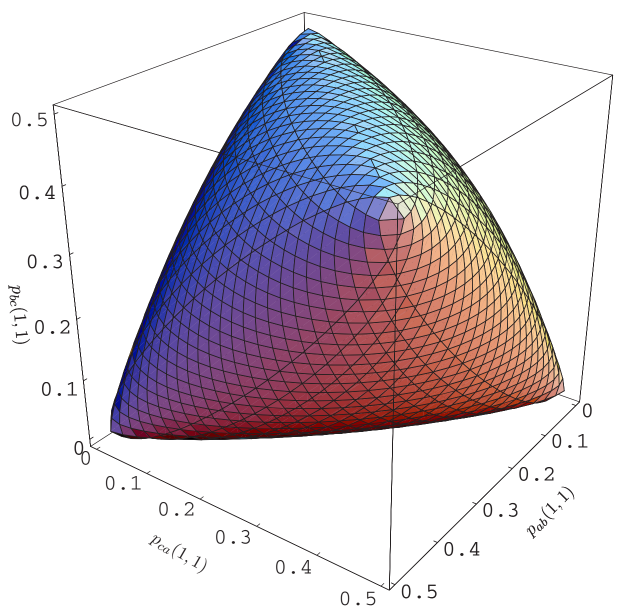

FIG. 1. (Color online) Possible range of triples $[p_{ab}(1,1),p_{bc}(1,1),p_{ca}(1,1)]$. The range of triples admitting a classical model is described as tetrahedron inside this body, with the same corners.

III. PROOF OF MAIN RESULT

In the first round, Alice chooses a Hilbert space $\mathcal{K}$ and prepares a density operator ρ on $\mathcal{H}\otimes\mathcal{K}$. The first system is left to the king's men, who perform their von Neumann measurement in one of the bases Φ_b, leaving a state $[|\Phi_b(i)\rangle\langle\Phi_b(i)|\otimes\mathbb{1}]\rho[|\Phi_b(i)\rangle\langle\Phi_b(i)|\otimes\mathbb{1}]$, conditional on their measured result being i. Finally, Alice will make a measurement on $\mathcal{H}\otimes\mathcal{K}$, with some outcomes $x\in X$. This is described by positive operators F_x on $\mathcal{H}\otimes\mathcal{K}$, with $\Sigma_x F_x=\mathbb{1}$. The precise nature of the outcomes is irrelevant. All that counts is that the value x provides Alice with a rule what to answer, if the king discloses that basis b was used by his men. We can express this by introducing a "guessing function," but we might just as well take the rule itself as the outcome (possibly grouping together some outcomes leading to the same guesses). Hence we choose the outcome set

$$X = \{1, \ldots, d\}^k = \{x:\{1, \ldots, k\} \to \{1, \ldots, d\}\}$$

with the interpretation that $x(b)$ is the answer Alice will give, if her measurement gave the value "x," and the King discloses b. The requirement that she is right every time is the basic equation for ρ and F_x we have to solve

$$\begin{aligned}&\mathrm{tr}(\rho[|\Phi_b(i)\rangle\langle\Phi_b(i)| \otimes \mathbb{1}]F_x[|\Phi_b(i)\rangle\langle\Phi_b(i)| \otimes \mathbb{1}])\\ &\quad = \lambda_{i,x}\delta_{i,x(b)}, \quad \lambda_{i,x} \geq 0, \quad \sum_{i,x} \lambda_{i,x} = 1.\end{aligned} \tag{3}$$

At this point we can make the first simplifications. Suppose, for example, that Alice has found a solution using a mixed state ρ, and that Ψ is some unit vector in the support of ρ, so that $|\Psi\rangle\langle\Psi| \leq \lambda\rho$ for some positive λ. Then after replacing ρ by $|\Psi\rangle\langle\Psi|$, the zeros in Eq. (3) will still all be in the right places, and since we chose Ψ as a unit vector, we have found a solution with a pure initial state $\rho=|\Psi\rangle\langle\Psi|$. Next, we write Ψ as

$$\Psi = (\mathbb{1} \otimes S)\Omega \quad \text{with } \Omega = \sum_{\alpha=1}^{d} |\alpha\alpha\rangle \in \mathcal{H} \otimes \mathcal{H}. \tag{4}$$

Ω is the maximally entangled vector, and S is an operator, whose matrix elements in a suitable basis of $\mathcal{K}$ are the vector components of Ψ, normalized so that $\mathrm{tr}(S^*S)=1$. Then in Eq. (3) we can commute S past the projections acting only on the first factor, and simplify the expression by introducing the vectors

$$\hat{\Phi}(i) = [|\Phi_b(i)\rangle\langle\Phi_b(i)| \otimes \mathbb{1}]\Omega = \Phi_b(i) \otimes \overline{\Phi_b(i)} \quad \in \mathcal{H} \otimes \mathcal{H}, \tag{5}$$

where the bar indicates componentwise complex conjugation in the basis $|\alpha\rangle$, in which Ω takes the form (4). Then the basic equation (3) becomes

$$\langle\hat{\Phi}_b(i)|(\mathbb{1} \otimes S)^* F_x(\mathbb{1} \otimes S)|\hat{\Phi}_b(i)\rangle = \lambda_{i,x}\delta_{i,x(b)}. \tag{6}$$

Now suppose η is a vector in the support of the operator in this bracket. Then substituting $|\eta\rangle\langle\eta|$ for the operator will still give zero, whenever $i \neq x(b)$, and hence

$$\langle\hat{\Phi}_b(i)|\eta\rangle = 0 \quad \text{if } i \neq x(b). \tag{7}$$

But also the scalar products for $i=x(b)$ are essentially fixed: We have $\Sigma_i|\Phi_b(i)\rangle\langle\Phi_b(i)|=\mathbb{1}$ for any basis b, which translates to $\Sigma_i\hat{\Phi}_b(i)=\Omega$ via Eq. (5). Therefore, we can sum Eq. (7) over i, obtaining

$$\langle\hat{\Phi}_b(i)|\eta\rangle = \langle\Omega|\eta\rangle\delta_{i,x(b)}. \tag{8}$$

We will call such vectors *safe vectors* for Alice (and the particular outcome x).

A. Structure of safe vectors

How many safe vectors can Alice find? A key role for answering this question is played by the space $\mathcal{R}$ introduced in Sec. II, or, equivalently by its image $\hat{\mathcal{R}} \subset \mathcal{H} \otimes \mathcal{H}$ under the identification of operators on $\mathcal{H}$ and elements of $\mathcal{H} \otimes \mathcal{H}$:

$$\hat{\mathcal{R}} = \mathrm{lin}_{\mathbb{R}}\{\Phi_b(i)\}, \tag{9}$$

its complex linear span $\hat{\mathcal{R}}_{\mathbb{C}}$, and its orthogonal complement $\hat{\mathcal{R}}^{\perp}$. For every $x \in X$ we arrive at the following alternative: It may happen that there is no vector η satisfying Eq. (8) with $\langle\Omega|\eta\rangle \neq 0$. Then all solutions of that equation are in $\hat{\mathcal{R}}^{\perp}$, which also means that such values x can never occur as a result of Alice's measurement. Alice's strategy will have to rely on the other cases, i.e., the subset of those $x \in X$, for which a nontrivial solution η of Eq. (8) exists. To get a standard solution, we multiply η with a scalar so that $\langle\Omega|\eta\rangle=1$. Moreover, we can apply to η the orthogonal projection to $\hat{\mathcal{R}}_{\mathbb{C}}$, thus obtaining a solution which is *uniquely* determined, since all scalar products with vectors from this space are fixed. We note that since all its scalar products with the $\hat{\Phi}_b(i)$ are real, we can even conclude that $\eta_x \in \hat{\mathcal{R}}$. Hence whenever a nonzero solution exists for some $x \in X$, we can pick a unique solution η_x, determined by the conditions

$$\langle\hat{\Phi}_b(i)|\eta_x\rangle = \delta_{i,x(b)} \quad \text{with } \eta_x \in \hat{\mathcal{R}}. \tag{10}$$

The fact that η_x lies in this real-linear subspace means that the corresponding operator on $\mathcal{H}$ is Hermitian, or, expressed in the standard basis that

$$\langle\alpha\beta|\eta_x\rangle = \overline{\langle\beta\alpha|\eta_x\rangle}. \tag{11}$$

It is clear that if Alice can find any safe vectors at all, she has some success at a *unambiguous retrodiction* game, in which she is allowed to pass, but has to be absolutely sure of her guess otherwise. As in the problem of "unambiguous discrimination" [11] her aim would be to minimize the probability for pass moves. In the mean king problem, however, her success probability is required to be unity, which is the same as saying that $\Sigma_x F_x=\mathbb{1}$, and a guess $x \in X$ is produced in every run.

B. Necessary conditions

The theorem states necessary conditions for the existence of a strategy only in the tomographically complete case. Then $\hat{\mathcal{R}}^{\perp}=\{0\}$, and the only choice Alice has is to pick safe vectors, which are multiples of the η_x as in Eq. (10). This fixes the operators in Eq. (6) to be

$$(\mathbb{1} \otimes S)^* F_x(\mathbb{1} \otimes S) = p(x)|\eta_x\rangle\langle\eta_x|, \tag{12}$$

with $p(x) \geq 0$. The values for x not allowing a nonzero safe vector can be subsumed by setting $p(x)=0$. The overall normalization condition $\Sigma_x F_x=\mathbb{1}$ then reads

$$N = \sum_x p(x)|\eta_x\rangle\langle\eta_x| = (\mathbb{1} \otimes S^*S). \tag{13}$$

Taking matrix elements of this equation in the standard basis and using the Hermiticity (11), we find

$$\langle\alpha\beta|N|\alpha'\beta'\rangle = \overline{\langle\beta\alpha|N|\beta'\alpha'\rangle}. \tag{14}$$

By Eq. (13) this amounts to $\delta_{\alpha\alpha'}n_{\beta\beta'} = \delta_{\beta\beta'}\overline{n_{\alpha\alpha'}}$, where n is the matrix of S^*S. With $\alpha=\alpha'=1$ we find that S^*S is also a multiple of the identity matrix. From the normalization condition tr $S^*S=1$ this multiple must be $1/d$. Since S^*S is just the reduced density operator of the restricted state, we have thus shown item (3) of the theorem: In the tomographically complete case, the initial state of Alice must be maximally entangled.

The connection with classical models is seen by taking the matrix elements of Eq. (13) with other vectors. To begin with, let us consider the matrix element with Ω. Then, since $N=(1/d)\mathbb{1}$, and $\langle\eta_x|\Omega\rangle=1$ whenever $p(x)\neq 0$, we get $\langle\Omega|N|\Omega\rangle=(1/d)\langle\Omega|\Omega\rangle=1=\Sigma_x p(x)$. Hence the $p(x)$ must indeed be a probability distribution on X, which is the same as the collection of all measurement outcomes. Furthermore, for any bases b,c, and associated outcomes i,j,

$$\langle\hat{\Phi}_b(i)|N|\hat{\Phi}_c(j)\rangle = \sum_x p(x)\,\delta_{i,x(b)}\delta_{j,x(c)}. \tag{15}$$

Clearly, the right-hand side is exactly the marginal $p_{bc}(i,j)$ of the probability distribution p with respect to the d-valued variables b and c. On the other hand, since $N=(1/d)\mathbb{1}$, the left-hand side evaluates to $(1/d)\langle\hat{\Phi}_b(i)|\hat{\Phi}_c(j)\rangle=(1/d)|\langle\Phi_b(i)|\Phi_c(j)\rangle|^2$, so p is exactly a classical model in the sense described in Sec. II.

This completes the proof of the theorem, part (2), and the corresponding statement in part (3).

C. Sufficient conditions

Let us now suppose, as in part (1) of the theorem, that we are given $k\leq(d+1)$ bases. Then, for each x, Eq. (10)) is an inhomogeneous linear system of equations for the vector η_x. Taking only the first $d-1$ equations for each basis, plus one normalization equation $\langle\Omega|\eta_x\rangle=1$ eliminates the trivial dependencies between these equations, so we have $k(d-1)+1$ equations for a vector in $\hat{\mathcal{R}}$. The condition of nondegeneracy described in Sec. II is equivalent to saying that all these equations are nonsingular, hence under the hypothesis of part (1) of the theorem, η_x exists for all x.

Now suppose that a classical model exists in the form of a set of $p(x)\geq 0$ such that the marginals (15) are consistent with $N=(1/d)\mathbb{1}$. Note, however, that $\hat{\mathcal{R}}$ may now be a proper subspace, and the matrix elements with all $\hat{\Phi}_b(i)$ do not determine the operator N completely. Nevertheless, we can set

$$F_x = dp(x)|\eta_x\rangle\langle\eta_x| + \widetilde{F}_x \tag{16}$$

with $\widetilde{F}_x\geq 0$ summing to the projection onto $\hat{\mathcal{R}}^\perp$. Then it is immediate that with a maximally entangled initial state, i.e., with the choice $S=(1/\sqrt{d})\mathbb{1}$, the basic equation (6) is satisfied. This completes the proof of part (1) of the theorem.

IV. FINDING A STRATEGY NUMERICALLY

Given the marginals of Eq. (1), the existence of a classical model is a linear feasibility program in the $p(x)$. It can also be cast as a semidefinite program, namely to maximize $\Sigma_x p(x)$ subject to the constraints $p(x)\geq 0$ and $\Sigma_x p(x)|\eta_x\rangle\langle\eta_x|\leq\mathbb{1}/d$. If the maximum turns out to be $\Sigma_x p(x)=1$, we have found the desired joint distribution. Otherwise, this is the probability for Alice to find an answer in the unambiguous retrodiction game described at the end of Sec. III A. The following table lists the numerical results for low dimensions with independent Haar distributed bases, where p_S is the probability that a safe strategy exists, E_S is the expected overall success probability for unambiguous retrodiction, and N is the sample size we used

d	p_S	E_S	$\log_{10} N$
2	0.3334	0.6666	7
3	0.0013	0.398	6
4	0	0.34	3

Higher dimensions, with d^{d+1} variables and constraints, are a serious challenge for PC based computation. For $d=6$, a strategy rarely exists, but one can first "debias" the bases with a gradient search minimizing $\Sigma_{i,j,a,b}p_{ab}(i,j)^2$. Instead of a semidefinite program one can then use the so-called EM algorithm [12,13] to find a joint distribution, and this is typically successful for the debiased case, although convergence is rather slow.

ACKNOWLEDGMENTS

We thank Richard Gill for valuable discussions. This work has been supported by the DFG and JOMC, Braunschweig.

[1] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).
[2] B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 15 (2001).
[3] P. K. Aravind, Z. Naturforsch., A: Phys. Sci. **58a**, 2212 (2003).
[4] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A **73**, 050301(R) (2006).
[5] *Mutually unbiased bases*, Problem 13, Open Problems Website, http://www.imaph.tu-bs.de/qi/problems
[6] M. Horibe, A. Hayashi, and T. Hashimoto, Phys. Rev. A **71**, 032337 (2005).
[7] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A **71**, 052331 (2005).
[8] S. Ben-Menahem, Phys. Rev. A **39**, 1621 (1989).
[9] Y. Aharonov and L. Vaidman, J. Phys. A **24**, 2315 (1991).
[10] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[11] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[12] A. P. Dempster, N. M. Laird, and D. B. Rubin, J. R. Stat. Soc. Ser. B (Methodol.) **39**, 1 (1977).
[13] R. Gill (private communication).