28 May 2001

PHYSICS LETTERS A

ELSEVIER

Physics Letters A 284 (2001) 1–5

www.elsevier.nl/locate/pla

The mean king's problem: prime degrees of freedom

Berthold-Georg Englert [a,b,*], Yakir Aharonov [c,d]

[a] *Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Wien, Austria*
[b] *Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, 85748 Garching, Germany*
[c] *School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 69978, Israel*
[d] *Physics Department, University of South Carolina, Columbia, SC 29208, USA*

Received 27 March 2001; accepted 17 April 2001
Communicated by P.R. Holland

Abstract

We show how one can ascertain the values of a complete set of mutually complementary observables of a prime degree of freedom. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Quantum kinematics; Complementary observables; Complete sets of observables; Entanglement

1. Introduction

In 1987, one of us (Y.A.) co-authored a paper [1] with the somewhat provocative title "How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle". It reports the solution of what later became known as *The King's Problem*: A mean king challenges a physicist, who got stranded on the remote island ruled by the king, to prepare a spin-1/2 atom in any state of her choosing and to perform a control measurement of her liking. Between her preparation and her measurement, the king's men determine the value of either σ_x, or σ_y, or σ_z. Only after she completed her control measurement, the physicist is told which spin component has been measured, and she must then state the result of that intermediate measurement correctly. How does she do it?

This thought experiment has not been realized as yet. But recently an optical analog has been formulated [2], and experimental data should be at hand shortly. Somewhat unexpectedly, and rather rewardingly, the photon version of the king's problem suggested a new scheme for quantum cryptography [3].

Also very recently, we reported a generalization of the king's problem [4] where, instead of the traditional spin-1/2 atom, a spin-1 atom is used. This generalization required answers to two questions: What are the appropriate spin-1 analogs of the spin-1/2 observables $\sigma_x, \sigma_y, \sigma_z$? And, how does the physicist rise to the challenge now?

In the present Letter we deal with the further generalization to arbitrary prime degrees of freedom, where measurements can have at most p different outcomes, p being any prime number. Of course, the situations of Refs. [1] and [4], spin-1/2 ($p = 2$) and spin-1 ($p = 3$), respectively, are particular realizations of the prime case. We believe that this extension of the idea of Ref. [1] teaches us a potentially important lesson about the mathematical structure of quantum kinematics.

* Corresponding author.
E-mail address: bge@mpq.mpg.de (B.-G. Englert).

PII: S0375-9601(01)00271-7

In Section 2 we answer the general-prime version of the first question asked above. The analogs of the three spin-1/2 observables are identified as complete sets of mutually complementary observables. Then the answer to the second question is given in Section 3; it employs essentially the same strategy that works in the cases of spin-1/2 and spin-1, so that we have a genuine generalization indeed. We leave it as a moot point whether generalizations to non-prime degrees of freedom are possible, or if there are analogs of the variants of the spin-1/2 problem that were found by Ben-Menahem [5] and Mermin [6]. Also, we do not address the intriguing question of whether the geometrical reasoning that works so well in the spin-1/2 case [7] lends itself to generalizations for spin-1 or richer degrees of freedom.

2. Pairwise complementary observables

The three spin-1/2 observables $\sigma_x, \sigma_y, \sigma_z$ are *complete* in the sense that the probabilities for finding their eigenvalues as the results of measurements specify uniquely the statistical operator that characterizes the spin-1/2 degree of freedom of the ensemble under consideration. They are not overcomplete because this unique specification is not ensured if one of the spin components is left out.

In addition to being complete, the observables $\sigma_x, \sigma_y, \sigma_z$ are also pairwise *complementary*, which is to say that in a state where one of them has a definite value, all measurement results for the other ones are equally probable. For example, if $\sigma_x = 1$ specifies the ensemble, say, then the results of σ_y measurements are utterly unpredictable: $+1$ and -1 are found with equal frequency; and the same is true for σ_z measurements.

What is essential here are not the eigenvalues of $\sigma_x, \sigma_y, \sigma_z$, but their sets of eigenstates. In technical terms, the fact that the transition probabilities

$$\begin{aligned}
&\bigl|\langle\sigma_x = \pm 1|\sigma_y = \pm 1\rangle\bigr|^2 = \frac{1}{2},\\
&\bigl|\langle\sigma_y = \pm 1|\sigma_z = \pm 1\rangle\bigr|^2 = \frac{1}{2},\\
&\bigl|\langle\sigma_z = \pm 1|\sigma_x = \pm 1\rangle\bigr|^2 = \frac{1}{2}
\end{aligned} \tag{1}$$

do not depend on the quantum numbers ± 1, is the statement of the pairwise complementary nature of σ_x, σ_y, and σ_z. Their algebraic completeness is then an immediate consequence of the insight that a spin-1/2 degree of freedom can have at most three mutually complementary observables.

More generally, there can be no more than $p+1$ such observables for a degree of freedom with a p-dimensional space of state vectors [8]. Following Weyl [9,10] and Schwinger [11–13], we shall find it convenient to deal with unitary operators, rather than the Hermitian operators to which they would be closely related. Thus the $p+1$ observables $U_0, U_1, \ldots, U_p$ are unitary and of period p,

$$\begin{aligned}
&U_m^p = 1,\\
&U_m^r \neq 1 \quad \text{if } r = 1, 2, \ldots, p-1,
\end{aligned} \tag{2}$$

for $m = 0, 1, \ldots, p$. The eigenvalues of each U_m are powers of

$$q \equiv e^{2\pi i/p}, \tag{3}$$

the basic pth root of unity, and we denote by $|m_k\rangle$ the kth eigenstate of U_m, so that

$$U_m|m_k\rangle = |m_k\rangle q^k \tag{4}$$

for $m = 0, 1, \ldots, p$ and $k = 1, 2, \ldots, p$.

Both the orthonormality of the $|m_k\rangle$'s for each m and the mutual complementarity for different m's are summarized in

$$\begin{aligned}
\bigl|\langle m_k|m'_{k'}\rangle\bigr|^2 &= \delta_{mm'}\delta_{kk'} + \frac{1}{p}(1-\delta_{mm'})\\
&= \begin{cases} \delta_{kk'} & \text{if } m = m',\\ p^{-1} & \text{if } m \neq m', \end{cases}
\end{aligned} \tag{5}$$

for $m, m' = 0, 1, \ldots, p$ and $k, k' = 1, 2, \ldots, p$. With

$$U_m = \sum_{k=1}^{p} |m_k\rangle q^k \langle m_k| \tag{6}$$

this implies

$$p^{-1}\,\mathrm{tr}\bigl\{U_m^r U_{m'}^s\bigr\} = \delta_{mm'}\delta^{(p)}_{r,-s} + (1-\delta_{mm'})\delta^{(p)}_{r,0}\delta^{(p)}_{s,0}, \tag{7}$$

where $m, m' = 0, 1, \ldots, p$ and $r, s = 0, \pm 1, \pm 2, \ldots$, and

$$\delta^{(p)}_{rs} \equiv \left\{ \begin{array}{ll} 1 & \text{if } q^r = q^s \\ 0 & \text{otherwise} \end{array} \right\} = \frac{1}{p}\sum_{k=1}^{p} q^{(r-s)k} \tag{8}$$

is the appropriate p-periodic version of Kronecker's delta symbol. The reverse is also true: (7) implies (5), as can be shown with the aid of

$$|m_k\rangle\langle m_k| = \frac{1}{p}\sum_{r=1}^{p}\bigl(q^{-k}U_m\bigr)^r. \tag{9}$$

Thus, given a set of $p+1$ unitary operators of period p, we can verify the defining property (5) of their pairwise complementarity by demonstrating that (7) holds.

Repeated measurements of the observables U_m (on identically prepared systems) eventually determine the probabilities $w_k^{(m)}$ for finding their eigenstates $|m_k\rangle$. As a consequence of their mutual complementarity, knowledge of the probabilities for one U_m contains no information whatsoever about the probabilities for any other one. These $(p+1)\times p$ probabilities represent p^2-1 parameters in total, since

$$\sum_{k=1}^{p} w_k^{(m)} = 1 \tag{10}$$

for each of the $p+1$ measurements. The statistical operator that characterizes the ensemble of identically prepared systems,

$$\rho = \sum_{m=0}^{p}\sum_{k=1}^{p}|m_k\rangle\left(w_k^{(m)} - \frac{1}{p+1}\right)\langle m_k|, \tag{11}$$

is therefore uniquely determined by the probabilities $w_k^{(m)} = \langle m_k|\rho|m_k\rangle$. Indeed, the U_m's constitute a complete set of pairwise complementary observables for the prime degree of freedom under consideration.

Actually, the prime nature of p has not been significant so far, but it is for the explicit construction of the set $U_0, U_1, \ldots, U_p$ that we turn to now. We pick an arbitrary period-p unitary operator for U_0. The unitary operator that permutes the eigenvectors of U_0 cyclically is used for U_p. Its eigenvectors in turn are cyclically permuted by U_0, so that U_0 and U_p are jointly characterized by

$$\langle 0_k|U_p = \langle 0_{k+1}|, \qquad U_0|p_k\rangle = |p_{k+1}\rangle \tag{12}$$

for $k = 1, 2, \ldots, p-1$ and, to complete the cycle,

$$\langle 0_p|U_p = \langle 0_1|, \qquad U_0|p_p\rangle = |p_1\rangle. \tag{13}$$

The fundamental Weyl commutation relation

$$U_0U_p = q^{-1}U_pU_0 \tag{14}$$

is an immediate consequence of this reciprocal definition of U_0 and U_p. The other U_m's are chosen as

$$U_m = U_0^m U_p. \tag{15}$$

Since p is a prime — what follows is not true for composite numbers; try $p=6$, for instance, to see what goes wrong — the powers of the U_m's that appear in (9) comprise all products of powers of U_0 and U_p, and since the unitary operators

$$U_0^r U_p^s \quad \text{with } r, s = 1, 2, \ldots, p, \tag{16}$$

which are p^2 in number, are a basis in the p^2-dimensional operator algebra [9–13], the p^2-1 unitary operators

$$U_m^r \quad \text{with } r = 1, 2, \ldots, p-1, \tag{17}$$

supplemented by $1 = U_0^p = U_1^p = \cdots = U_p^p$ are also such an operator basis. As it should be, these bases are complete, but not overcomplete; none of the basis operators is superfluous.

As a consequence of (12) and (13), all operators in (16) are traceless with the sole exception of the identity operator that obtains for $r = s = p$. It is then a matter of inspection to verify that the U_m's thus constructed obey (7) and are, therefore, a set of pairwise complementary observables, indeed. From the point of view of the information-theoretical approach to quantum mechanics that is being developed by Brukner and Zeilinger [14], the U_m's form a complete set of mutually complementary propositions.

3. The mean king's problem generalized

In the generalized version of the king's problem then, either one of the observables $U_0, U_1, \ldots, U_p$ is measured by the mean king's men, on a p-system suitably prepared by the physicist. Without knowing which measurement was done actually, the physicist performs a subsequent measurement of her own, and — after then being told which U_m was measured by the king's men — she has to state correctly what they found: $|m_1\rangle$, or $|m_2\rangle$, …, or $|m_p\rangle$.

The physicist solves the problem by first preparing a state $|\Psi_0\rangle$ in which the given p-system, the *object*, is entangled with an auxiliary p-system, the *ancilla*, whose operators and states are barred for distinction.

For the ancilla, there are analogs $\overline{U}_0$ and $\overline{U}_p$ of the fundamental Weyl operators U_0 and U_p that we have for the object. It is advantageous, however, to interchange the roles of $\overline{U}_0$ and $\overline{U}_p$ in their reciprocal definition. So, rather than just copying the object relations (12) and (13), we write for the ancilla

$$\overline{U}_p\big|\bar{0}_k\big\rangle = \big|\bar{0}_{k+1}\big\rangle, \qquad \langle\bar{p}_k|\overline{U}_0 = \langle\bar{p}_{k+1}| \tag{18}$$

for $k = 1, 2, \ldots, p-1$ and

$$\overline{U}_p\big|\bar{0}_p\big\rangle = \big|\bar{0}_1\big\rangle, \qquad \langle\bar{p}_p|\overline{U}_0 = \langle\bar{p}_1|, \tag{19}$$

and the corresponding analog of (15) is

$$\overline{U}_m = \overline{U}_p\overline{U}_0^m \tag{20}$$

for $m = 1, \ldots, p-1$. Then the transition amplitudes $\langle 0_j|m_k\rangle$ and $\langle\bar{0}_j|\bar{m}_k\rangle$ between the eigenstates of U_0 and U_m and between those of $\overline{U}_0$ and $\overline{U}_m$, respectively, obey recurrence relations

$$\frac{\langle 0_{j+1}|m_k\rangle}{\langle 0_j|m_k\rangle} = q^{-jm+k}, \qquad \frac{\langle\bar{0}_{j+1}|\bar{m}_k\rangle}{\langle\bar{0}_j|\bar{m}_k\rangle} = q^{jm-k} \tag{21}$$

(for $m \neq 0$, of course), which allow and invite to choose the phase conventions such that

$$\langle 0_j|m_k\rangle = \big\langle\bar{m}_k\big|\bar{0}_j\big\rangle. \tag{22}$$

We note in passing that the $|m_k\rangle$'s, or the $|\bar{m}_k\rangle$'s, are essentially identical with the states found by Wootters and Fields [8] if one opts for the solutions

$$\langle 0_j|m_k\rangle = p^{-1/2}q^{jk-j(j-1)m/2} = \big\langle\bar{0}_j\big|\bar{m}_k\big\rangle^* \tag{23}$$

of recursions (21).

Joint states in which the object is in $|m'_{k'}\rangle$ and the ancilla in $|\bar{m}_k\rangle$ are denoted by $|m'_{k'}\bar{m}_k\rangle$. Then

$$|\Psi_0\rangle = p^{-1/2}\sum_{k=1}^{p}|m_k\bar{m}_k\rangle \tag{24}$$

is the entangled object-ancilla state that the physicist prepares. Thanks to the phase conventions (22), the m dependence is only apparent. For either value of $m = 0, 1, \ldots, p$ we get the same $|\Psi_0\rangle$.

If the king's men then measure the object observable U_m and find the eigenvalue q^k, the resulting object-ancilla state is $|m_k\bar{m}_k\rangle$. After their measurement, there are thus all together $p+1$ sets (labeled by m) of p possible object-ancilla states each. These $(p+1)\times p$ states cannot be linearly independent because the state space is only p^2-dimensional. Indeed, each of the p-dimensional subspaces spanned by the $p+1$ sets contains $|\Psi_0\rangle$ by construction. In addition, there are $(p+1)\times(p-1) = p^2-1$ other states, and we now proceed to show that they *are* linearly independent.

Consider $m \neq m'$ and any pair of values for k and k'. Then

$$\big\langle m_k\bar{m}_k\big|m'_{k'}\bar{m}'_{k'}\big\rangle = p^{-1} \tag{25}$$

as a consequence of (5) and (22), and definition (24) of $|\Psi_0\rangle$ implies

$$\langle\Psi_0|m_k\bar{m}_k\rangle = p^{-1/2} = \big\langle\Psi_0\big|m'_{k'}\bar{m}'_{k'}\big\rangle. \tag{26}$$

The two vectors

$$|m_k\bar{m}_k\rangle - p^{-1/2}|\Psi_0\rangle,$$
$$\big|m'_{k'}\bar{m}'_{k'}\big\rangle - p^{-1/2}|\Psi_0\rangle \tag{27}$$

are therefore orthogonal to $|\Psi_0\rangle$ and orthogonal to each other. Accordingly, $|\Psi_0\rangle$ together with the p^2-1 vectors $|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_{p^2-1}\rangle$ that are defined by

$$|\Psi_{(p-1)m+j}\rangle = p^{-1/2}\sum_{k=1}^{p}|m_k\bar{m}_k\rangle q^{-jk} \tag{28}$$

for $m = 0, 1, 2, \ldots, p$ and $j = 1, 2, \ldots, p-1$ constitute an orthonormal basis,

$$\langle\Psi_n|\Psi_{n'}\rangle = \delta_{nn'} \quad \text{for } n, n' = 0, 1, \ldots, p^2-1, \tag{29}$$

in the p^2-dimensional object-ancilla state space.

Two $|\Psi_n\rangle$'s that have the same m value in (28) are orthogonal by construction. And if $|\Psi_n\rangle$ and $|\Psi_{n'}\rangle$ belong to different m values, their orthogonality follows immediately as soon as one replaces $|m_k\bar{m}_k\rangle$ in (28) by the difference of (27), which does not alter the value of the sum.

Let us now see how all of this helps the physicist to meet the mean king's challenge. She will be able to state correctly the measurement result found by the king's men if she can find an object-ancilla observable P with eigenstates $|P_1\rangle, \ldots, |P_{p^2}\rangle$ such that each $|P_n\rangle$ is orthogonal to $p-1$ members each of the $p+1$ sets of states that are potentially the case after the measurement by the king's men. We characterize the looked-for eigenstates of P by an ordered set of numbers $k_0, k_1, \ldots, k_p$ that indicate which members

they are *not* orthogonal to, so that

$$\big|[k_0k_1\ldots k_p]\big\rangle \tag{30}$$

has the defining property of being orthogonal to the object-ancilla states that result when measurements of U_m do *not* give the eigenvalue q^{k_m}.

Suppose the physicist finds the state $|[325\ldots7]\rangle$. She then knows that if the king's men had measured U_0, U_1, U_2, or U_p, the respective results must have been q^3, q^2, q^5, and q^7, because she would never find $|[325\ldots7]\rangle$ for other measurement results.

Accordingly, all that is needed to complete the solution of the generalized mean king's problem is the demonstration that we can have a complete orthonormal set of object-ancilla states of the kind (30). First note that the expansion of $|[k_0k_1\ldots k_p]\rangle$ in the $|\Psi_n\rangle$ basis is given by

$$\big|[k_0k_1\ldots k_p]\big\rangle = \frac{1}{p}\left(|\Psi_0\rangle + \sum_{m=0}^{p}\sum_{j=1}^{p-1} q^{jk_m}|\Psi_{(p-1)m+j}\rangle\right). \tag{31}$$

Then observe that

$$\big\langle[k_0k_1\ldots k_p]\big|\big[k'_0k'_1\ldots k'_p\big]\big\rangle = \frac{1}{p}\sum_{m=0}^{p}\delta_{k_m,k'_m} - \frac{1}{p}, \tag{32}$$

so that two such states are orthogonal if $k_m = k'_m$ for one and only one m value. Therefore, a possible choice of basis states for the physicist's final measurement is given by those p^2 states for which $k_0, k_1 = 1, 2, \ldots, p$ and

$$k_m = (m-1)k_0 + k_1 \ (\mathrm{mod}\ p) \tag{33}$$

for $m = 2, 3, \ldots, p$. The prime nature of p is crucial for the otherwise straightforward demonstration of the orthogonality of two such states that differ in their values of k_0, or k_1, or both.

So, the physicist just has to choose her object-ancilla observable P such that it distinguishes the states specified in (33). After being told which measurement the king's men performed on the object, she can then infer their measurement result correctly, and with certainty, in the manner described above for $|[325\ldots7]\rangle$.

Acknowledgements

Y.A. gratefully acknowledges the kind hospitality extended to him by Herbert Walther during a visit at the MPI für Quantenoptik in Garching. B.G.E. would like to thank Wolfgang Schleich and the University of Ulm for financial support while part of this work was done, and he expresses his sincere gratitude for the hospitable environment provided by Gerald Badurek and Helmut Rauch at the Atominstitut and for the financial support by the Technical University of Vienna. Y.A.'s research is supported in part by Grant No. 471/98 of the Basic Research Foundation (administered by the Israel Academy of Sciences and Humanities), by NSF Grant No. PHY-9971005, and by ONR Grant No. N00014-00-1-0383.

References

[1] L. Vaidman, Y. Aharonov, D.Z. Albert, Phys. Rev. Lett. 58 (1987) 1385.
[2] B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, Phys. Rev. A 63 (2001) 032303.
[3] A. Beige, B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, quant-ph/0101066, Phys. Rev. Lett., submitted.
[4] Y. Aharonov, B.-G. Englert, Z. Naturforsch. 56a (2001) 16.
[5] S. Ben-Menahem, Phys. Rev. A 39 (1989) 1621.
[6] N.D. Mermin, Phys. Rev. Lett. 74 (1995) 831.
[7] Y. Aharonov, L. Vaidman, J. Phys. A: Math. Gen. 24 (1991) 2315.
[8] W.K. Wootters, B.D. Fields, Ann. Phys. (NY) 191 (1989) 363.
[9] H. Weyl, Z. Phys. 46 (1927) 1.
[10] H. Weyl, Gruppentheorie und Quantenmechanik, Hirzel, Leipzig, 1928;
English translation by H.P. Robertson, Theory of Groups and Quantum Mechanics, E.P. Dutton, New York, 1932.
[11] J. Schwinger, Proc. Natl. Acad. Sci. USA 46 (1960) 570.
[12] J. Schwinger, in: W. Deppert, K. Hübner, A. Oberschelp, V. Weidemann (Eds.), Exact Sciences and Their Philosophical Foundations, Verlag Peter Lang, Frankfurt am Main, 1985.
[13] J. Schwinger, Quantum Mechanics. Symbolism of Atomic Measurements, Springer, Berlin, 2001.
[14] Č. Brukner, A. Zeilinger, Phys. Rev. Lett. 83 (1999) 3354.