Solution to the mean king's problem with mutually unbiased bases for arbitrary levels

doi: 10.1103/PhysRevA.73.050301

PHYSICAL REVIEW A **73**, 050301(R) (2006)

Solution to the mean king's problem with mutually unbiased bases for arbitrary levels

Gen Kimura,* Hajime Tanaka,† and Masanao Ozawa‡

Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai 980-8579, Japan

(Received 24 January 2006; revised manuscript received 12 April 2006; published 5 May 2006)

The mean king's problem with mutually unbiased bases is reconsidered for arbitrary d-level systems. Hayashi *et al.* [Phys. Rev. A **71**, 052331 (2005)] related the problem to the existence of a maximal set of $d-1$ mutually orthogonal Latin squares, in their restricted setting that allows only measurements of projection-valued measures. However, we then cannot find a solution to the problem when, e.g., $d=6$ or $d=10$. In contrast to their result, we show that the king's problem always has a solution for arbitrary levels if we also allow positive operator-valued measures. In constructing the solution, we use orthogonal arrays in combinatorial design theory.

DOI: 10.1103/PhysRevA.73.050301 PACS number(s): 03.67.Hk

I. INTRODUCTION

The *mean king's problem* is a problem to retrodict the outcome of a measurement of a basis randomly chosen from a maximal set of *mutually unbiased bases* (MUBs) [1–3]. It was first introduced in [4] for spin-$\frac{1}{2}$ systems, and later considered for systems with prime number levels [5] and prime power levels [6–8]. The problem is often stated as a tale [5,8]:

"Once upon a time, there lived a mean King who loved cats. The King hated physicists since the day when he first heard what had happened to Schrödinger's cat. One day, a terrible storm came on, and Alice, a physicist, got stranded on the island that was ruled by the King. The King called Alice to the royal laboratory and gave her a challenge: First, Alice can prepare a d-level quantum system (a d-level atom) in any state of her own liking and hand it over to the King. The King will then secretly measure the atom with respect to one of $d+1$ mutually unbiased bases and return it to Alice. Alice is then allowed to perform one more measurement on the atom. Afterwards, the King reveals his measurement basis and then Alice must immediately guess the correct output of the King's measurement, or she will die a cruel death."

Here, the king's measurement is assumed to be a standard projective measurement of a basis $\{|\varphi_m\rangle\}_{m=0}^{d-1}$ of the atom system, so that the measurement in the state $|\psi\rangle$ leads to the output (index) m with probability $|\langle\varphi_m|\psi\rangle|^2$ and leaves the system in the state $|\varphi_m\rangle$. On the other hand, Alice is assumed to be allowed any measurement not restricted to that of a basis of the atom system.

The standard approach to the king's problem is to make use of entanglement [4–8]. Alice prepares two d-level quantum systems $\mathbb{C}^d\otimes\mathbb{C}^d$, one to be handed over to the king and the other to be kept by Alice in secret, in a maximally entangled state. After the king's measurement of one of $d+1$ MUBs, Alice is then supposed in the literature to carry out a measurement of projection-valued measure (PVM) on the space $\mathbb{C}^d\otimes\mathbb{C}^d$.

Under the above assumptions, Hayashi *et al.* [7] showed the equivalence of the existence of a solution to the king's problem and that of a maximal set of $d-1$ mutually orthogonal Latin squares, or equivalently, $d+1$ mutually unbiased striations [9]. Then, it turns out that we cannot find a solution when, e.g., $d=6$ or $d=10$, in which cases $d-1$ mutually orthogonal Latin squares do not exist, even if there might be a maximal set of $d+1$ MUBs; the existence of the latter is still an open problem except for prime power levels. The purpose of the present paper is to show that the king's problem always has a solution for arbitrary levels if we relax the above assumption to allow Alice to carry out any measurement of a positive operator-valued measures (POVM) on the same space $\mathbb{C}^d\otimes\mathbb{C}^d$.

The notion of POVM measurement was introduced by Helstrom [10] to generalize conventional PVM measurements and to show that there is a class of optimization problems to which the optimum is achieved by a POVM measurement but not by any PVM measurements. Nowadays, POVM measurement is considered the most general description of measurement concerning the single measurement statistics, apart from the notion of instrument introduced by Davies and Lewis [11] that describes also the state change that determines the repeated or successive measurement statistics. By virtue of the Naimark theorem, every POVM measurement can be realized by a PVM measurement of an extended system with the so-called ancilla; see Holevo [12] for mathematical foundations of POVM measurements. This is considered a static realization with a nonlocal measurement. A dynamical realization with a local measurement is obtained by the general realization theorem of completely positive instruments [13], so that any measurements can be realized as the unitary evolution of the composite system of the measured system and the probe followed by a subsequent PVM measurement of the probe. Then, the difference between POVM and PVM measurements arises only from the difference of the interaction or the probe preparation, and in some cases, a POVM measurement is more feasible than the corresponding PVM measurement, in particular, for measuring a continuous observable [13] or for the measurement under conservation laws [14].

As above, it is natural to assume that Alice can carry out, in principle, any POVM measurements on the same space $\mathbb{C}^d\otimes\mathbb{C}^d$ without considerable change of the resource allowed

*Electronic address: gen@ims.is.tohoku.ac.jp

†Electronic address: htanaka@ims.is.tohoku.ac.jp

‡Electronic address: ozawa@math.is.tohoku.ac.jp

for her. In this formulation, we first derive a simple criterion for the existence of a solution to the king's problem in Sec. II. Then in Sec. III, we give a construction of a solution based on *orthogonal arrays* in combinatorial design theory [15], instead of mutually orthogonal Latin squares.

We note, however, that our result gives no information on the existence of MUBs. It is well known that there can never be more than $d+1$ MUBs (cf. [3]). There always exists a maximal set of $d+1$ MUBs when d is a prime power [2,3], but a construction (or even the existence) of $d+1$ MUBs for other values of d is a long-standing problem, even for the smallest case $d=6$. For the rest of this paper, we just assume that we have a set of k MUBs $\{|A,a\rangle_K\}_{a=0}^{d-1}$, $A\in\{0,1,\ldots,k-1\}$, for the king's Hilbert space $\mathbb{C}^d$ (where $2\le k\le d+1$),

$$\left|\langle A,a|A',a'\rangle_K\right|^2 = \delta_{A,A'}\delta_{a,a'} + (1-\delta_{A,A'})\frac{1}{d}. \tag{1}$$

Of course, what we have in mind is the case $k=d+1$, but the problem itself makes sense even for smaller k [16].

II. CRITERION FOR THE SOLUTION

We shall construct Alice's POVM on $\mathbb{C}^d\otimes\mathbb{C}^d$ from a suitable orthonormal basis $\{|I\rangle\}_{I=0}^{dd'-1}$ on a larger Hilbert space $\mathbb{C}^{d'}\otimes\mathbb{C}^d$ $(d'\ge d)$. Let $V:\mathbb{C}^d\to\mathbb{C}^{d'}$ be the natural isometric embedding of the space $\mathbb{C}^d$ into the extended space $\mathbb{C}^{d'}$. Then,

$$M_I \equiv (V\otimes\mathbb{I})^\dagger|I\rangle\langle I|(V\otimes\mathbb{I}),$$

where $I\in\{0,1,\ldots,dd'-1\}$, defines a POVM on $\mathbb{C}^d\otimes\mathbb{C}^d$. (The exact value for $d'\in\mathbb{N}$ will be specified later.)

Following [4–8], let Alice prepare the initial state in a maximally entangled state,

$$|\Phi\rangle \equiv \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle_A\otimes|i\rangle_K \in \mathbb{C}^{d'}\otimes\mathbb{C}^d, \tag{2}$$

with reference orthonormal bases $\{|i\rangle_A\}_{i=0}^{d'-1}$ and $\{|i\rangle_K\}_{i=0}^{d-1}$ for $\mathbb{C}^{d'}$ and $\mathbb{C}^d$, respectively. Using any member $\{|A,a\rangle_K\}_{a=0}^{d-1}$ of the MUBs, (2) can be rewritten as

$$|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}\overline{|A,a\rangle}_A\otimes|A,a\rangle_K,$$

where $\overline{|A,a\rangle}_A\equiv\sum_{i=0}^{d-1}\langle i|A,a\rangle_K^*|i\rangle_A$. If the king measured the basis $\{|A,a\rangle_K\}_{a=0}^{d-1}$ and obtained the output a, then the post-measurement state will be

$$|\Phi_{A,a}\rangle \equiv \overline{|A,a\rangle}_A\otimes|A,a\rangle_K.$$

We observe $\langle\Phi_{A,a}|\Phi_{A',a'}\rangle=\delta_{A,A'}\delta_{a,a'}+(1-\delta_{A,A'})/d$.

Here we remark the following. Let $\omega\equiv\exp(2\pi i/d)$, and for $A\in\{0,1,\ldots,k-1\}$ and $j\in\{0,1,\ldots,d-1\}$ let

$$|\widehat{\Phi}_{A,j}\rangle \equiv \frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}\omega^{aj}|\Phi_{A,a}\rangle.$$

Then $|\widehat{\Phi}_{A,0}\rangle=|\Phi\rangle$ and it is easy to see that

$$\langle\widehat{\Phi}_{A,j}|\widehat{\Phi}_{A',j'}\rangle = \delta_{A,A'}\delta_{j,j'} + (1-\delta_{A,A'})\delta_{j,0}\delta_{j',0}. \tag{3}$$

Let $\mathcal{A}$ be the one-dimensional subspace spanned by $|\Phi\rangle$, and for each $A\in\{0,1,\ldots,k-1\}$ let $\mathcal{A}_A$ be the orthogonal complement of $\mathcal{A}$ in the linear span of $|\Phi_{A,0}\rangle$, $|\Phi_{A,1}\rangle,\ldots,|\Phi_{A,d-1}\rangle$, i.e., $\mathrm{span}\{|\Phi_{A,a}\rangle\}_{a=0}^{d-1}=\mathcal{A}\oplus\mathcal{A}_A$. Then, it follows from (3) that $\mathcal{A}_A$ is spanned by $|\widehat{\Phi}_{A,1}\rangle$, $|\widehat{\Phi}_{A,2}\rangle,\ldots,|\widehat{\Phi}_{A,d-1}\rangle$,and Alice's space $\mathbb{C}^{d'}\otimes\mathbb{C}^d$ is decomposed into the orthogonal direct sum

$$\mathbb{C}^{d'}\otimes\mathbb{C}^d = \mathcal{A}\oplus\mathcal{A}_0\oplus\ \ldots\ \oplus\mathcal{A}_{k-1}\oplus\mathcal{B}, \tag{4}$$

where

$$\mathcal{B}\equiv(\mathrm{span}\{|\Phi_{A,a}\rangle\}_{A=0,a=0}^{k-1,d-1})^\perp. \tag{5}$$

It seems that this structure is fundamental in the discussion of MUBs (cf. [3]).

With the above setting, now Alice has to find the basis $\{|I\rangle\}_{I=0}^{dd'-1}$ on $\mathbb{C}^{d'}\otimes\mathbb{C}^d$ and an *estimation function* $s(I,A)\in\{0,1,\ldots,d-1\}$, namely her guess for the king's output a based on her output I and the king's choice A. For fixed A and a, Alice's (conditional) success probability is then given by $\sum_{I=0}^{dd'-1}\delta_{a,s(I,A)}|\langle I|\Phi_{A,a}\rangle|^2$. Thus, in order to save her life with certainty we must have [7]

$$\langle I|\Phi_{A,a}\rangle = 0 \quad \text{whenever} \quad s(I,A)\neq a. \tag{6}$$

Now, we associate the basis $\{|I\rangle\}_{I=0}^{dd'-1}$ with a $dd'\times kd$ matrix H defined by

$$H(I;A,a)\equiv\langle I|\Phi_{A,a}\rangle.$$

Then, obviously

$$H(I;A,a)=0 \quad \text{whenever} \quad s(I,A)\neq a, \tag{7}$$

and moreover it follows that

$$(H^\dagger H)(A,a;A',a') = \delta_{A,A'}\delta_{a,a'} + (1-\delta_{A,A'})\frac{1}{d}. \tag{8}$$

Thus, we have shown that if we have an estimation function $s(I,A)$ and an orthonormal basis $\{|I\rangle\}_{I=0}^{dd'-1}$ for $\mathbb{C}^{d'}\otimes\mathbb{C}^d$ satisfying the survival condition (6), then there is a matrix H such that (7) and (8) hold. Now, we shall show the converse statement that given an estimation function $s(I,A)$ and a matrix H satisfying (7) and (8), we can find an orthonormal basis $\{|I\rangle\}_{I=0}^{dd'-1}$ for $\mathbb{C}^{d'}\otimes\mathbb{C}^d$ satisfying (6). To show this, suppose that a function $s(I,A)\in\{0,1,\ldots,d-1\}$ and a $dd'\times kd$ matrix H satisfy (7) and (8). Let $|\Psi_{A,a}\rangle\rangle$ denote the (A,a)-th column vector of H. Then, since $\langle\langle\Psi_{A,a}|\Psi_{A',a'}\rangle\rangle=\langle\Phi_{A,a}|\Phi_{A',a'}\rangle$, there is a unique unitary operator

$$U:\mathrm{span}\{|\Phi_{A,a}\rangle\}_{A=0,a=0}^{k-1,d-1}\to\mathrm{span}\{|\Psi_{A,a}\rangle\rangle\}_{A=0,a=0}^{k-1,d-1},$$

such that

$$U|\Phi_{A,a}\rangle = |\Psi_{A,a}\rangle\rangle. \tag{9}$$

Specifically, U is determined by $U|\widehat{\Phi}_{A,j}\rangle\equiv|\widehat{\Psi}_{A,j}\rangle\rangle$, where

$$|\widehat{\Psi}_{A,j}\rangle\rangle \equiv \frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}\omega^{aj}|\Psi_{A,a}\rangle\rangle.$$

Now, arbitrarily extend U to a unitary operator

$$\widetilde{U}:\mathbb{C}^{d'}\otimes\mathbb{C}^{d}\to\mathbb{C}^{dd'}, \tag{10}$$

and let

$$|I\rangle \equiv \widetilde{U}^{\dagger}|I\rangle\rangle,$$

where $\{|I\rangle\rangle\}_{I=0}^{dd'-1}$ denotes the standard basis for the column space $\mathbb{C}^{dd'}$. Then $\{|I\rangle\}_{I=0}^{dd'-1}$ is an orthonormal basis for $\mathbb{C}^{d'}\otimes\mathbb{C}^{d}$ and by (9) we have $\langle I|\Phi_{A,a}\rangle=\langle\langle I|\Psi_{A,a}\rangle\rangle=H(I;A,a)$ and thus (6) holds.

To summarize, we have the following:

Theorem 1. Given an estimation function $s(I,A)\in\{0,1,\ldots,d-1\}$, there exists an orthonormal basis $\{|I\rangle\}_{I=0}^{dd'-1}$ for $\mathbb{C}^{d'}\otimes\mathbb{C}^{d}$ satisfying (6) if and only if there is a $dd'\times kd$ matrix H such that (7) and (8) hold.

III. ORTHOGONAL ARRAYS AND THE EXISTENCE OF A SOLUTION

An *orthogonal array* of *degree k*, *order d*, and *index n*, denoted $\mathrm{OA}_n(k,d)$, is an $nd^2\times k$ array with entries from $\{0,1,\ldots,d-1\}$ such that every pair of symbols from $\{0,1,\ldots,d-1\}$ occurs exactly n times as a 1×2 submatrix in the $nd^2\times 2$ matrix consisting of any pair of two distinct columns chosen from the array (cf. [15]). It follows immediately from the definition that every symbol occurs exactly nd times in each column of an $\mathrm{OA}_n(k,d)$. Thus, in other words, an $nd^2\times k$ array T with entries from $\{0,1,\ldots,d-1\}$ is an $\mathrm{OA}_n(k,d)$ if and only if

$$\frac{1}{nd}\sum_{I=0}^{nd^2-1}\delta_{a,T(I,A)}\delta_{a',T(I,A')}=\delta_{A,A'}\delta_{a,a'}+(1-\delta_{A,A'})\frac{1}{d}. \tag{11}$$

[Compare this equation with (1).] We note that an $\mathrm{OA}_1(k,d)$ is equivalent to a set of $k-2$ mutually orthogonal Latin squares of side d. An $\mathrm{OA}_1(4,3)$ is given in Table I. Hayashi *et al.* [7] constructed an estimation function using a maximal set of $d-1$ mutually orthogonal Latin squares. There always exist $d-1$ mutually orthogonal Latin squares if d is a power of a prime, but as mentioned in the Introduction, it is known that this is not the case for some other values of d, such as $d=6$ and $d=10$. On the other hand, we can always find an orthogonal array for each k and d. In fact, the array obtained by arranging all the k-tuples (in, e.g., the lexicographic order) obviously defines an $\mathrm{OA}_{d^{k-2}}(k,d)$. In particular, it is known [17] that there exists an $\mathrm{OA}_n(7,6)$ for all $n\geq 2$[18].

Now, we construct a solution to the king's problem based on orthogonal arrays. Set $d'=nd$ and let $[s(I,A)]_{I=0,A=0}^{nd^2-1,k-1}$ form an $\mathrm{OA}_n(k,d)$. We define an $nd^2\times kd$ matrix H by

TABLE I. An $\mathrm{OA}_1(4,3)$. We may think of the first two columns as representing the row and column indices of 3×3 matrices, respectively. Then the third and fourth columns correspond to two mutually orthogonal Latin squares of side 3.

0	0	0	0
0	1	1	1
0	2	2	2
1	0	1	2
1	1	2	0
1	2	0	1
2	0	2	1
2	1	0	2
2	2	1	0

$$H(I;A,a)\equiv\frac{1}{\sqrt{nd}}\delta_{a,s(I,A)}.$$

Then by (11) H satisfies (7) and (8), and Theorem 1 shows that there is a solution to the problem. In fact, the proof of Theorem 1 yields a somewhat explicit formula for the corresponding basis $\{|I\rangle\}_{I=0}^{nd^2-1}$ in this case. Let $\{|\Xi_b\rangle\}_{b=0}^{e-1}$ be an orthonormal basis for $\mathcal{B}$, where $e\equiv\dim\mathcal{B}=nd^2-k(d-1)-1$. Then by (4) we have

$$|I\rangle=\langle\Phi|I\rangle|\Phi\rangle+\sum_{A=0}^{k-1}\sum_{j=1}^{d-1}\langle\widehat{\Phi}_{A,j}|I\rangle|\widehat{\Phi}_{A,j}\rangle+\sum_{b=0}^{e-1}\langle\Xi_b|I\rangle|\Xi_b\rangle.$$

Since $|\widehat{\Phi}_{A,0}\rangle=|\Phi\rangle$, $\langle\Phi|I\rangle=1/(d\sqrt{n})$ and

$$\sum_{j=0}^{d-1}\langle\widehat{\Phi}_{A,j}|I\rangle|\widehat{\Phi}_{A,j}\rangle=\frac{1}{d\sqrt{nd}}\sum_{j=0}^{d-1}\sum_{a=0}^{d-1}\omega^{(a-s(I,A))j}|\Phi_{A,a}\rangle$$
$$=\frac{1}{\sqrt{nd}}|\Phi_{A,s(I,A)}\rangle,$$

we find

$$|I\rangle=\frac{1}{\sqrt{n}}|I'\rangle+\sum_{b=0}^{e-1}\langle\Xi_b|I\rangle|\Xi_b\rangle, \tag{12}$$

where

$$|I'\rangle\equiv\frac{1}{\sqrt{d}}\sum_{A=0}^{k-1}|\Phi_{A,s(I,A)}\rangle-\frac{k-1}{d}|\Phi\rangle.$$

[Compare this expression with Eq. (10) in [7].]

IV. EXAMPLE

We illustrate the above construction of a solution to the problem in the case of the (trivial) $\mathrm{OA}_{d^{k-2}}(k,d)$. Each $I\in\{0,1,\ldots,d^k-1\}$ has a unique d-adic expansion,

$$I=\sum_{A=0}^{k-1}I_Ad^A,\quad \text{where } I_A\in\{0,1,\ldots,d-1\}.$$

We

define the array $[s(I,A)]_{I=0,A=0}^{d^k-1,k-1}$ by $s(I,A) \equiv I_A$.

In order to carry out the construction (12) of the basis $\{|I\rangle\}_{I=0}^{d^k-1}$ explicitly, we must specify $\widetilde{U}|\Xi_b\rangle$ for an orthonormal basis $\{|\Xi_b\rangle\}_{b=0}^{e-1}$ for $\mathcal{B}$ in (5) (where $e=d^k-k(d-1)-1$). The space $\mathcal{B}$ depends on the particular set of MUBs. When $k=d+1$ for instance, $\mathcal{B}$ is spanned by $\{|i\rangle_A \otimes |j\rangle_K\}_{i=d,j=0}^{d^d-1,d-1}$.

For each $J \in \{0,1,\ldots,d^k-1\}$ let

$$|\widehat{\Psi}_J\rangle\rangle \equiv \frac{1}{\sqrt{d^k}} \sum_{I=0}^{d^k-1} \omega^{\Sigma_{A=0}^{k-1} I_A J_A} |I\rangle\rangle.$$

Then $\{|\widehat{\Psi}_J\rangle\rangle\}_{J=0}^{d^k-1}$ forms an orthonormal basis for the column space $\mathbb{C}^{d^k}$. Note that $|\widehat{\Psi}_{jd^A}\rangle\rangle = |\widehat{\Psi}_{A,j}\rangle\rangle$ for $j \in \{0,1,\ldots,d-1\}$. Let $\Theta:\{0,1,\ldots,e-1\} \to \{J:|\{A:J_A \neq 0\}| \geq 2\}$ be any bijection and define the extension $\widetilde{U}:\mathbb{C}^{d^{k-1}} \otimes \mathbb{C}^d \to \mathbb{C}^{d^k}$ of U in (10) by setting $\widetilde{U}|\Xi_b\rangle \equiv |\widehat{\Psi}_{\Theta(b)}\rangle\rangle$ for $b \in \{0,1,\ldots,e-1\}$. Then we find

$$|I\rangle = \frac{1}{\sqrt{d^{k-2}}}|I'\rangle + \frac{1}{\sqrt{d^k}} \sum_{b=0}^{e-1} \omega^{-\Sigma_{A=0}^{k-1} I_A \Theta(b)_A} |\Xi_b\rangle.$$

V. CONCLUDING REMARKS

In contrast to the results in [7], we showed that for any d we can always find a solution to the king's problem by performing a suitable POVM measurement, instead of a PVM measurement. We note that our method in this paper also indicates how Alice constructs that POVM: She just prepares a $d'(=nd)$ level ancilla to maximally entangle the d-level atom, and carries out the PVM measurement with respect to $\{|I\rangle\}_{I=0}^{dd'-1}$ constructed in the previous sections based on orthogonal arrays.

The authors are grateful to Akihiro Munemasa and Masahiro Hotta for fruitful discussions and comments on the mean king's problem and the structure of MUBs. G.K. would like to thank Andrzej Kossakowski for introducing the notion of MUBs to him. G.K. and H.T. are supported by grants from the Japan Society for the Promotion of Science. M.O. is supported in part by the SCOPE Project of MPHPT of Japan.

[1] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[2] I. D. Ivanović, J. Phys. A **14**, 3241 (1981).

[3] W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).

[4] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[5] Y. Aharonov and B.-G. Englert, Z. Naturforsch., A: Phys. Sci. **56a**, 16 (2001); B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001).

[6] P. K. Aravind, Z. Naturforsch., A: Phys. Sci. **58a**, 2212 (2003); T. Durt, e-print quant-ph/0401037.

[7] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A **71**, 052331 (2005).

[8] A. Klappenecker and M. Rötteler, e-print quant-ph/0502138.

[9] W. K. Wootters, e-print quant-ph/0406032.

[10] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[11] E. B. Davies and J. T. Lewis, Commun. Math. Phys. **17**, 239 (1970); E. B. Davies, *Quantum Theory of Open Systems* (Academic, London, 1976).

[12] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).

[13] M. Ozawa, J. Math. Phys. **25**, 79 (1984); M. Ozawa, in *Squeezed and Nonclassical Light*, edited by P. Tombesi and E. R. Pike (Plenum, New York, 1989), p. 263.

[14] M. Ozawa, Phys. Rev. Lett. **88**, 050402 (2002).

[15] C. J. Colbourn, in *The CRC Handbook of Combinatorial Designs*, edited by C. J. Colbourn and J. H. Dinitz (CRC, Boca Raton, FL, 1996), Part II, Chap. 4.

[16] We remark that, in the case $k=2$, Alice can in fact survive with probability 1 without any ancilla at the stage of state preparation. For instance, take any one of the pure states in $\{|0,a\rangle_K\}_{a=0}^{d-1}$ as the initial state and perform the PVM with respect to $\{|1,a\rangle_K\}_{a=0}^{d-1}$.

[17] H. Hanani, in *Combinatorics, Part 1: Theory of Designs, Finite Geometry and Coding Theory*, edited by M. Hall, Jr. and J. H. van Lint (Mathematical Centre Tracts, No. 55., Mathematisch Centrum, Amsterdam, 1974), p. 42.

[18] More generally, Ray-Chaudhuri and Singhi proved that for fixed positive integers k and d, there exists an integer n_0 such that an $\mathrm{OA}_n(k,d)$ exists for all $n \geq n_0$. D. K. Ray-Chaudhuri and N. M. Singhi, J. Comb. Theory, Ser. A **47**, 28 (1988); **66**, 327 (E) (1994); see, also, S. J. Rosenberg, Discrete Math. **137**, 315 (1995).