Consistent assignment of quantum probabilities

Manas K Patra\textsuperscript{1,2} and Ron van der Meyden\textsuperscript{3}

\textsuperscript{1} Department of Computer Science, University of York, York YO10 5GH, UK
\textsuperscript{2} Laboratoire d’Information Quantique, Université Libre de Bruxelles, Campus Plaine, Bruxelles 1050, Belgium
\textsuperscript{3} School of Computer Science and Engineering, University of New South Wales, Sydney 2052, Australia

E-mail: manas@cs.york.ac.uk and meyden@cse.unsw.edu.au

Received 8 September 2011, in final form 26 December 2011
Published 30 January 2012
Online at stacks.iop.org/JPhysA/45/075304

Abstract

We pose and solve a problem concerning consistent assignment of quantum probabilities to a set of bases associated with maximal projective measurements. We show that our solution is optimal. We also consider some consequences of the main theorem in this paper in conjunction with Gleason’s theorem. Some potential applications to state tomography and probabilistic quantum secret-sharing scheme are discussed.

PACS numbers: 03.65.Wj, 03.67.Ac, 02.10.Ud

1. Assignment of quantum probabilities

Consider a finite quantum system $\mathcal{S}$ of dimension $n$. Define a quantum probability assignment (QPA) for $\mathcal{S}$ to be a set $\mathcal{F} = \{ (B_1, S_1), \ldots, (B_m, S_m) \}$ consisting of $m$ pairs $(B_k, S_k)$, where

(1) each $B_k = \{ P^k_1, \ldots, P^k_n \}$ is a sequence of $n$ one-dimensional projection operators $P^k_i = |\alpha^{k}_i\rangle \langle \alpha^{k}_i|$ corresponding to an orthonormal basis $|\alpha^{k}_1\rangle, \ldots, |\alpha^{k}_n\rangle$ and

(2) each $S_k = \{ p^k_1, p^k_2, \ldots, p^k_n \}$ is a sequence of $n$ real numbers such that $p^k_i \geq 0$ and $\sum_i p^k_i = 1$.

Clearly, the sequences $S_k$ can be considered as distributions on a probability space with $n$ elements (atomic events).

Suppose now it is claimed that these probabilities correspond to projective measurements in these $m$ bases. Thus, the claim is that there is a (mixed) quantum state $\rho$ (a positive semidefinite matrix with trace 1) such that

$$\text{Tr} (\rho P^k_i) = p^k_i \quad \text{for all } 1 \leq k \leq m, \quad 1 \leq i \leq n. \quad (1)$$

If such a state exists, we say that the collection $\mathcal{F}$ is a consistent QPA. How do we verify this claim? Potentially $m$ could be infinite. A related question is the following.
Problem. What is the smallest number $r$ such that if all the probability assignments $\mathcal{G} \subseteq \mathcal{F}$ with $|\mathcal{G}| \leq r$ ($|\mathcal{G}|$ denotes cardinality of $\mathcal{G}$) are consistent, then the whole collection $\mathcal{F}$ is consistent?

The number depends on the assignment $\mathcal{F}$. So we ask what is the largest value of $r(\mathcal{F})$ as we vary $\mathcal{F}$? This value depends only on the dimension $n$. Call it the consistency number $r_n$. Equivalently, $r_n$ is the smallest number such that for every collection of QPAs $\mathcal{F}$, if every subset of $\mathcal{F}$ of size $r_n$ is consistent, then $\mathcal{F}$ is consistent. This problem first came up in our attempt at formal axiomatization of a logic of finite-dimensional quantum systems [1]. The problem we address in this paper is the calculation of the consistency number.

We mention that a related problem was posed by Bell, and Kochen and Specker [2, 3] in their analysis of non-contextual hidden-variable theories. Projection operators of rank 1 are attempts at formal axiomatization of a logic of finite-dimensional quantum systems [1].

This paper is structured as follows. In sections 2 and 3, we prove that $r_n = n^2 - n + 1$ for $n \geq 3$. We first prove a weaker result that if every subset consisting of $r_n + 1 = n^2 - n + 2$ probability assignments is consistent, then so is the whole set $\mathcal{F}$. The proof in the case of $r_n$ is surprisingly much harder. There is one exceptional case where one has to investigate in detail the structure of the bases themselves (unlike the case for $r_n + 1$). But we get extra dividends in gaining information about the measurement bases. In fact, there is essentially one case where we need the maximal value $n^2 - n + 1$. We use this in section 3 to construct examples to demonstrate that the number $r_n$ is indeed optimal. More precisely, if $r' < r_n$, there exist QPAs $\mathcal{F}$ such that all subcollections of $\mathcal{F}$ of size $r'$ are consistent but $\mathcal{F}$ itself is not consistent. The tricky part in the construction of these examples is that we have to ensure that positive-definite matrices with trace 1 (states) exist which satisfy the assignments corresponding to every subcollection of size $r'$. We conclude the section with a simple application of the main result in conjunction with Gleason’s famous theorem [6].

In section 4, we outline some applications of our constructions to (probabilistic) secret sharing and state tomography. Section 5 makes some concluding remarks.

2. Solution to the problem

This section is devoted to establishing upper bounds for the consistency number. We assume first that the number of assignments $m$ is finite, but we will show later that this assumption can be dropped. More precisely, we prove the following.

Theorem 1. Let $H$ be the Hilbert space of an $n$-dimensional quantum system. Define a QPA $\mathcal{F} = \{(B_1, S_1), \ldots, (B_m, S_m)\}$ consisting of $m$ pairs $(B_k, S_k)$, where

(i) $B_k = \{P_1^k, \ldots, P_n^k\}$ is a sequence of $n$ projection operators $P_i^k = |\alpha_i^k\rangle \langle \alpha_i^k|$ corresponding to an orthonormal basis $|\alpha_1^k\rangle, \ldots, |\alpha_n^k\rangle$ and

(ii) $S_k = (p_1^k, p_2^k, \ldots, p_n^k)$ is a sequence of $n$ real numbers such that $p_i^k \geq 0$ and $\sum_i p_i^k = 1$.

Then, $\mathcal{F}$ is a consistent QPA to an $n$-dimensional quantum system if and only if every subset $\mathcal{G} \subseteq \mathcal{F}$ of size at most

$$R_n = \begin{cases} 4, & \text{if } n = 2, \\ n^2 - n + 1, & \text{if } n > 2, \end{cases}$$  \hspace{1cm} (2)

is consistent. That is, $r_n \leq R_n$. 

2
Note that arbitrary $k$-subsets $\mathcal{F}$ may be separately consistent. However, the proof below will produce a state in which the whole of $\mathcal{F}$ is a consistent assignment provided the conditions of the theorem are satisfied. Observe also that the problem of assignment arises because of the unitary transformation connecting two bases. We will later see that these bounds are optimal in the sense that for a positive integer $r' < R_n$, there are bases and corresponding probability assignments such that every subset of size $r'$ is consistent but the whole set is inconsistent.

We will start with a relatively simpler result.

**Lemma 1.** With the notation as above, $\mathcal{F} = \{(B_1, S_1), \ldots, (B_m, S_m)\}$ is a consistent probability assignment to an $n$-dimensional quantum system if and only if every subset $\mathcal{G} \subseteq \mathcal{F}$ of size at most $n^2 - n + 2$ is consistent.

**Proof.** Let $\mathcal{F} = \{(B_1, S_1), \ldots, (B_m, S_m)\}$, where $B_i$ are bases and $S_i$ are the corresponding probability assignments. We may assume that $m > n^2 - n + 2$. Let $I$ denote the unit matrix of order $n$. Now, for each $1 \leq k \leq m$, we have a set of consistency equations

\[
\begin{align*}
\text{Tr}(\rho I) &= \text{Tr}(\rho) = 1, \\
\text{Tr}(\rho P_{ki}) &= p_{ki} \quad \text{for} \quad 1 \leq i \leq n - 1,
\end{align*}
\]

in the real variables $x_{jk}$ and $y_{jk}$, where $\rho_{jk} = x_{jk} + iy_{jk}$, the $(jk)$th entry of the quantum state $\rho$. Note that we omit the equation $\text{Tr}(\rho P_{ni}) = p_{ni}$ for the case $i = n$ since this follows from others using the facts that $\sum_j p_{ij} = 1$ and $\sum_i p_{ij} = 1$. The Hermiticity of $\rho$ implies that there are $n^2$ independent parameters. Any one set of equations corresponding to a single-basis assignment fixes the trace condition. We call the set of equations corresponding to the assignment to the $k$th basis the $k$th block, $B_k$. So we have $n^2$ independent real variables and any block, say the first, has $n$ independent equations. That is, the rank of the coefficient matrix of the first block is $n$. But after the normalization ($\text{Tr}(\rho) = 1$) is fixed, each block from the second block onward can contribute at most $n - 1$ to the overall rank. Given an arbitrary set $\mathcal{A}$ of assignments, let $\text{rank}(\mathcal{A})$ denote the rank of the coefficient matrix of the corresponding set of linear equations (3). However, $\rho$ has $n^2$ real variables $\text{rank}(\mathcal{A}) \leq n^2$. Now consider a subset $\mathcal{G} \subseteq \mathcal{F}$ of cardinality $l \geq n^2 - n + 2$. Call such subsets the $l$-subsets of $\mathcal{F}$. We will show that if every $l$-subset is consistent, then any $(l + 1)$-subset is consistent. Then, induction will complete the proof. Hence, we have to show that given any $(l + 1)$-subset $\mathcal{K} = \{(B_i, S_i) : 1 \leq i \leq l + 1\}$, it is consistent if every $l$-subset of $\mathcal{K}$ is consistent.

By assumption, $\mathcal{G}_i = \mathcal{K} - \{(B_i, S_i)\}$ is consistent for all $1 \leq i \leq l + 1$. Now consider the sets $\mathcal{G}_i = \mathcal{G}_i - \{(B_i, S_i)\}$. Suppose $\text{rank}(\mathcal{G}_i) < n^2$. Since $|\mathcal{G}_i| \geq n^2 - n + 1$, this implies that at least one of the blocks say $B_k$ in $\mathcal{G}_i$ is dependent on the rest in the sense that $\text{rank}(\mathcal{G}_i - \{(B_k, S_k)\}) = \text{rank}(\mathcal{G}_i)$. Suppose this is not the case. Then, we must have

\[n = \text{rank}(\{(B_1, S_1)\}) < \text{rank}(\{(B_1, S_1), (B_2, S_2)\}) < \cdots < \text{rank}(\mathcal{G}_i) < n^2.\]

But this is impossible since $|\mathcal{G}_i| \geq n^2 - n + 1$. We have shown that there is some $k$ such that $\langle B_k, S_k \rangle \in \mathcal{G}_i$ and $\text{rank}(\mathcal{G}_i - \{(B_k, S_k)\}) = \text{rank}(\mathcal{G}_i)$. Let $\mathcal{G}_i' = \mathcal{G}_i - \{(B_k, S_k)\}$. Then, every equation in the block $B_k$ can be written as a linear combination of equations of $\mathcal{G}_i'$. Hence, consistency of $\mathcal{G}_i'$ implies that any solution to $\mathcal{G}_i'$ is a solution for $\mathcal{G}_i$. The cardinality of $\mathcal{G}_i' \cup \{\{(B_1, S_1), (B_2, S_2)\}\}$ is $l$, and by hypothesis, it is consistent. But from what we have shown above, a solution $\rho$ to this system is also a solution to $\mathcal{G}_i' \cup \{\{(B_1, S_1), (B_2, S_2), (B_k, S_k)\}\} = \mathcal{K}$. The proof is complete in this case.

Next consider the second alternative, $\text{rank}(\mathcal{G}_i) = n^2$. This is the maximal rank since there are $n^2$ variables. Hence, any solution to the system $\mathcal{G}_i$ is unique. This implies that $\mathcal{G}_i$ and $\mathcal{G}_i'$ have the same unique solution. But then so does $\mathcal{K}$ and the proof is complete. $\square$
The following lemma provides one of the key elements in improving the bound so as to obtain our main result.

**Lemma 2.** Let $B = \{\epsilon_1, \ldots, \epsilon_n\}$ and $B' = \{\beta_1, \ldots, \beta_n\}$ be two bases in an $n$-dimensional Hilbert space. Let $B$ and $B'$ be, respectively, the associated matrices of coefficients for the systems of real equations

$$\text{Tr}(\langle \epsilon_i \rangle \langle \epsilon_i | \rho \rangle) = p_i, \quad \text{and} \quad \text{Tr}(\langle \beta_i | \beta_i \rangle) = q_i, \quad (\text{both for } i = 1, \ldots, n). \quad (4)$$

Here, $\sum p_i = \sum q_i = 1$, where $\rho$ is positive-semidefinite matrix and the entries of $\rho$ are treated as unknown variables. Suppose that the rank of the combined system $B$ and $B'$ is $n + 1$, exactly 1 higher than the rank of $B$ (or $B'$). Then, two of the vectors from $B'$, say, $\beta_1$ and $\beta_2$, lie in the plane determined by two vectors from $B$. Assuming (without loss of generality) that the latter is spanned by $\epsilon_1$ and $\epsilon_2$, we also have $\langle \epsilon_i | \beta_j \rangle \neq 0$ for $i, j \in \{1, 2\}$. Furthermore, the set $\{\beta_j : 3 \leq j \leq n\}$ is a permutation of $\{\epsilon_j : 3 \leq j \leq n\}$.

**Proof.** Writing the matrix elements of $\rho$ in the $B$ basis, we observe that the equations corresponding to $B$ determine the diagonal elements $\rho_{ii}$ along with the constraint $\sum_i \rho_{ii} = 1$. Now, let $\beta_j = \sum_i c_{ji} \epsilon_i$. Then, the equations in $B'$ are equivalent to the following:

$$\sum_j |c_{jl}|^2 x_{jj} + \sum_{j \neq k} (\overline{c}_{jl} c_{kl} + c_{jl} \overline{c}_{kl}) x_{jk} + i(\overline{c}_{jl} c_{kl} - c_{jl} \overline{c}_{kl}) y_{jk} = q_l, \quad \text{where}$$

$$\rho_{jk} = \langle \epsilon_j | \rho | \epsilon_k \rangle = x_{jk} + iy_{jk}.$$

Using $B$ we can eliminate the diagonal terms from these equations (corresponding to $j = k$). Then, the hypothesis that the rank of the combined system $B$ and $B'$ is exactly 1 more than that of $B$ alone implies that

$$\overline{c}_{jl} c_{kl} = \alpha_{lm} \overline{c}_{jm} c_{km} \quad \forall j \neq k. \quad (5)$$

Here, $\alpha_{lm}$ are the real constants depending on the basis vectors $\beta_l$ and $\beta_m$ or equivalently the $l$th and $m$th row vectors of $B'$. Now, among $\beta_l$'s there must be at least two vectors which have at least two nonzero coefficients when expressed in the vectors of $B$. Otherwise, $B$ and $B'$ are the same basis apart from permutation. We may take these two vectors to be $\beta_1$ and $\beta_2$. We may also assume without loss of generality that $c_{11}$ and $c_{21}$ are both nonzero. Suppose for $\beta_3$ the coefficients $c_{32}$ and $c_{22}$ are nonzero. Then, addition of either of the equations corresponding to $\beta_1$ or $\beta_2$ to the system corresponding to $B$ increases rank by 1. Equation (5) then shows that $\alpha_{12}$ and $\alpha_{21} (= \alpha_{12}^*)$ are both nonzero. Hence, $c_{21}$ and $c_{22}$ must be nonzero. Then, equation (5) implies that $c_{12}$ and $c_{22}$ are both nonzero. Using equation (5) again, we infer that there is a nonzero constant $\gamma$ such that $c_{j2} = \gamma c_{j1}$ for $j = 3, \ldots, n$. If a third basis vector, say $\beta_3$, had two nonzero coefficients, a similar type of argument would show the existence of a nonzero constant $\gamma'$ such that $c_{3j} = \gamma' c_{j1}, \quad j = 2, 3, \ldots, n$. But then $\beta_1$, $\beta_2$ and $\beta_3$ will not be linearly independent. Hence, all $\beta_i, \quad i = 3, \ldots, n$, must have exactly one nonzero coefficient $c_{il}$. Since they are unit vectors, this must be 1 (apart from an inconsequential factor of modulus 1). That is, $\beta_i = \epsilon_i$. Since $\beta_i$'s constitute an orthogonal basis $\epsilon_i$ cannot be any of $\epsilon_k$ whose coefficients $c_{k1}$ (and $c_{k2}$) are nonzero. In particular, $j_i \neq 1$ or 2. But there are $n - 2$ such $\beta_i$'s. Hence, the set $\{\beta_3, \beta_4, \ldots, \beta_n\}$ must be a permutation of $\{\epsilon_3, \epsilon_4, \ldots, \epsilon_n\}$ and $\{\beta_1, \beta_2\}$ forms an orthonormal basis in the two-dimensional space spanned by $\epsilon_1$ and $\epsilon_2$. Moreover, from the fact that $c_{11}, c_{21}, c_{12}$ and $c_{22}$ are all nonzero, we conclude that $\langle \epsilon_i | \beta_j \rangle \neq 0$ for $i, j \in \{1, 2\}$.

The proof of the lemma is complete. □

We now improve lemma 1 so as to yield a proof of theorem 1, by considering several special cases.
Proof (Theorem 1). The implication from left to right is trivial—any subset of a consistent set is consistent. To prove the converse, we may assume \( m > R_n \).

The case \( n = 2 \) is covered by lemma 1. So we assume that \( n \geq 3 \) and that any \( R_n \)-subset of \( \mathcal{F} \) is consistent. The problem can be restated as follows. Find a positive-semidefinite matrix \( \rho \) satisfying the set of linear equations (3). There are \( n^2 \) independent real variables corresponding to the real and imaginary parts of entries of \( \rho \), and hence, the real rank of system is \( \leq n^2 \). Any one of the blocks corresponding to one basis assignment has a rank \( n \). For each of the rest of blocks of equations corresponding to the pair \( \langle B_i, S_i \rangle \), we need to verify \( n - 1 \) equations in each block since the last one is guaranteed by the condition \( \sum_j p_{ij} = 1 \). Again using lemma 1, it suffices to show that every \( (R_n + 1) \)-subset of \( \mathcal{F} \) is consistent. Assume otherwise that there is a set \( \mathcal{F} = \{ \{ B_1, S_1 \}, \ldots, \{ B_{R_n + 1}, S_{R_n + 1} \} \} \) such that \( \mathcal{F} \) is inconsistent, while every proper subset of \( \mathcal{F} \) is consistent.

Recall that the rank of a QPA is defined to be the rank of the coefficient matrix of the consistency equations (3) corresponding to \( \mathcal{F} \). The set \( \mathcal{F}' = \{ \{ B_1, S_1 \}, \ldots, \{ B_{R_n}, S_{R_n} \} \} \) is consistent by hypothesis. Suppose that for some pair \( \langle B_i, S_i \rangle, \langle B_j, S_j \rangle \in \mathcal{F}' \), the rank of the combined system satisfies

\[
\text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle) \geq n + 2.
\]

Consider the chain of inequalities

\[
\begin{align*}
\text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle) &= n < n + 2 \leq \text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle) \\
\text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle, \langle B_1, S_1 \rangle) &\leq \cdots \leq \text{rank}(\mathcal{F}') \leq n^2,
\end{align*}
\]

where in each term we add exactly one new basis assignment to the previous set. Since there are \( R_n = n^2 - n + 1 \) terms at least one of the relations \( \leq \) must be an equality. Hence, the equations corresponding to at least one of the assignments, say, \( \langle B_k, S_k \rangle \), must be dependent on the rest. Thus, every solution of \( \mathcal{F}' - \{ \{ B_i, S_i \} \} \) must be a solution of \( \mathcal{F}' \). Now, \( \mathcal{F}_k = \mathcal{F}' - \{ \{ B_k, S_k \} \} \) is consistent being a set of cardinality \( R_n \). From what we have just seen, any solution to \( \mathcal{F}_k \) is also a solution for \( \langle B_k, S_k \rangle \). Hence, \( \mathcal{F} \) is consistent, i.e. a contradiction. We observe that in general we arrive at the same conclusion if any of the relations in the chain

\[
\text{rank}(\langle B_i, S_i \rangle) \leq \text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle) \leq \cdots \leq \text{rank}(\mathcal{F}')
\]

where \( (i, i_2, \ldots, i_{R_n}) \) is a permutation of \( (1, 2, \ldots, R_n) \), is an equality. Note also that if \( \text{rank}(\mathcal{F}') < n^2 \), then an argument similar to the above would show that some assignment \( \{ B_k, S_k \} \) must be dependent on the rest without requiring the condition in (6). We can then show that \( \mathcal{F} \) is consistent. Hence, to complete the proof, we have to consider only the following case.

**Condition 1.** For every distinct pair \( (i, j) \) in \( 1 \ldots R_n + 1 \),

\[
\text{rank}(\langle B_i, S_i \rangle, \langle B_j, S_j \rangle) = \text{rank}(\langle B_i, S_i \rangle) + 1 = n + 1,
\]

and for every \( R_{n'} \)-subset \( \mathcal{F}' = \{ \{ B_{i_1}, S_{i_1} \}, \{ B_{i_2}, S_{i_2} \}, \ldots, \{ B_{i_{R_n}}, S_{i_{R_n}} \} \} \) of \( \mathcal{F} \), in the chain

\[
\text{rank}(\langle B_{i_1}, S_{i_1} \rangle) < \text{rank}(\langle B_{i_1}, S_{i_1}, B_{i_2}, S_{i_2} \rangle) < \cdots < \text{rank}(\mathcal{F}')
\]

the rank increases exactly by 1 at each step. \( \square \)

This condition implies that the set of consistency equations corresponding to every \( R_{n'} \)-subset \( \mathcal{F}' \) of \( \mathcal{F} \) have the rank \( n^2 \). Let us write the basis vectors of the basis \( B_k \) as

\[ B_k = \{ \beta_{k1}, \beta_{k2}, \ldots, \beta_{kn^2} \}. \]
Without loss of generality, we may take the basis $B_1$ to be any fixed basis, say, the ‘computational’ basis $\{\epsilon_1, \ldots, \epsilon_n\}$. Then, relation (8) and lemma 2 imply that for the pair of distinct indices $(1, j)$ from 1 to $R_n + 1$, there exist pairs of distinct indices $(r, s)$ and $(j, j_j)$ from 1 to $n$ such that

$$\beta^r_j = a_i^j \epsilon_j + a_{s}^j \epsilon_j,$$

and

$$\beta^r_s = a_i^j \epsilon_j + a_{s}^j \epsilon_j,$$

(10)

where $a_i^j, a_{s}^j, \ldots$ are the nonzero complex numbers. Moreover, the set $B_1 - \{\epsilon_1, \epsilon_n\}$ is a permutation of $B_1 - \{\epsilon_1, \epsilon_n\}$. Before we write $\rho_{ij} = \langle \epsilon_i | \rho | \epsilon_j \rangle = x_{ij} + iy_{ij}$ in the computational basis $B_1$. Then, the assignment $(B_1, S_1)$ fixes the diagonal entries $\rho_i$ and the addition of equations corresponding to $(B_j, S_j)$ to those of $(B_1, S_1)$ yields exactly two relations

$$\Re(\overline{a}_j^1 | \rho_j, \delta_j) = p_j^i$$

and

$$\Re(\overline{a}_j^1 | \rho_j, \delta_j) = p_j^i.$$ 

Observe that $\langle \beta_j | \beta_j \rangle = 0$ implies that $a_i^j a_{s}^j = -a_i^s a_{s}^j$. From this, it follows that the left-hand sides of the two equations are dependent. Since they are consistent, the right-hand sides have similar dependence. That is, the addition of an arbitrary assignment $(B_j, S_j) \in \mathcal{G}$ to $(B_1, S_1)$ yields exactly one additional equation involving $x_{j,j}$ and $y_{j,j}$. Call it the $j$-incremental equation $E_j$.

It follows that the equations for $\mathcal{G}$ are equivalent to the set of equations for $(B_1, S_1)$, which fix the diagonal, together with the equations $E_2, \ldots, E_{R_n+1}$, each of which gives exactly one equation on the real and complex parts of some off-diagonal entry. (To obtain this from the above, note that the equations for $\{(B_1, S_1) \cup X \cup \{(B_j, S_j)\}$ are equivalent to those for $\{(B_1, S_1) \cup X \cup \{(B_1, S_1), (B_1, S_1)\}$, which are equivalent to $\{(B_1, S_1) \cup X \cup \{(B_1, S_1), E_j \}$, i.e., $\{(B_1, S_1) \cup X \cup \{E_j \}$, and apply induction.) Moreover, since rank$(\mathcal{G}) = n^2$, for each off-diagonal entry, there are exactly two indices $j, k$ in $2 \ldots R_n$ such that $E_j$ and $E_k$ concern that entry. Taking the entry to be that which is constrained by $E_{R_n+1}$, we find that $E_j$ and $E_k$ and $E_{R_n+1}$ concern the same entry. But $\mathcal{G}$ is equivalent to $(B_1, S_1)$ with $E_2, \ldots, E_{R_n}$, which is consistent, and $\mathcal{G}$ is equivalent to adding to this $E_{R_n+1}$, producing an inconsistency. The only way this is possible is if $E_j$, $E_k$ and $E_{R_n+1}$ are inconsistent. Since $R_n > 4$ for $n > 3$, we may find a $R_n$-subset $\mathcal{G}'$ of $\mathcal{G}$ that contains $(B_1, S_1), (B_1, S_1), (B_1, S_1)$ and $(B_{R_n+1}, S_{R_n+1})$. But the equations for this set then imply the inconsistent set $\{E_j, E_k, E_{R_n+1}\}$, and so $\mathcal{G}'$ is inconsistent. This contradicts the assumption that every $R_n$-subset of $\mathcal{G}$ is consistent.

Observe that the proof of theorem 1 actually provides an algorithm for verifying consistency of a given set $\mathcal{F}$ of assignments. Thus, we start with an arbitrary $\mathcal{G} \subset \mathcal{F}$ of cardinality $R_n$. If it is inconsistent, stop and declare that $\mathcal{F}$ is inconsistent. Otherwise, find rank$(\mathcal{G}) = k$, say. If $k = n^2$, then we have the Hermitian matrix $\rho$ which satisfies the assignments in $\mathcal{G}$. The problem then is to check whether the solution is positive definite. This can be done by using the algorithm for the Cholesky decomposition [4]. If the algorithm succeeds, then, of course, $\rho$ is positive (semi)definite. If it fails, then we stop, declaring the system inconsistent. Next, suppose $k < n^2$. Choose a subset of $\mathcal{G}'$ of $\mathcal{G}$ that has a maximal rank and let $|\mathcal{G}'| = s$. Add $R_n - s$ new assignments and continue the process. If we exhaust $\mathcal{F}$ before attaining full rank, then we have a system of equations with rank $r < n^2$. Then, the Hermitian matrix $\rho$ is determined with $n^2 - r$ free parameters. To determine whether there is a positive-definite solution in the corresponding parameter space, we may again follow a Cholesky decomposition type of algorithm but now symbolic. In the next section, we present bases in two and three dimensions, inspired by the proof of the theorem, to demonstrate that $R_n$ is optimal for the dimension $n$. That is, we have determined the consistency number.

---

4 Here, the computational basis denotes the standard basis in $\mathbb{C}^n$, where $\epsilon_i$ is the vector with 0’s everywhere except the $i$th entry which is 1.
We conclude this section with an application of Tukey’s lemma (equivalent to the axiom of choice) [5] that yields the following corollary. We use the notations explained before.

**Corollary 1.** Let $\mathcal{F} = \{(B_j, S_j) | j \in J\}$ be a collection of QPAs to bases $B_j$ in an $n$-dimensional space, indexed by a set $I$ of arbitrary cardinality. Then, $\mathcal{F}$ is consistent if and only if every finite subset of cardinality $n^2 - n + 1$ is consistent.

### 3. Optimality

In this section, we complete the proof that the consistency number $R_n$ given in theorem 1 is optimal. We show that there exist QPAs $\mathcal{F} = \{(B_k, S_k) | k = 1, 2, \ldots, m \geq R_n\}$ such that every $(R_n - 1)$-subset of $\mathcal{F}$ is consistent (hence also every $r$-subset of $\mathcal{F}$ for $r < R_n$ is consistent) but $\mathcal{F}$ is not. For example, in two dimensions, the bound is 4. So we have to show that there exist inconsistent probability assignments to four bases such that any three of them is consistent. For three dimensions, the bound is 7. We obviously expect the construction of bases and corresponding probability assignments to be much harder in three and higher dimensions. We construct these examples in this section.

#### 3.1. Dimension 2

Let the dimension $n = 2$ and define one-dimensional projections

\[
P_1^1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_1^2 = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad P_1^3 = \frac{1}{2} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}
\]

and $P_1^4 = \frac{1}{5} \begin{pmatrix} 4 & (6 + 8i)/5 \\ (6 - 8i)/5 & 1 \end{pmatrix}$.

Let the four bases (rather the projections corresponding to the basis vectors) be given by

\[B_j = \{P_1^j, I - P_1^j\}, \quad j = 1, \ldots, 4,\]

where $I$ is the two-dimensional unit matrix. Then, the following simultaneous probability assignment is unsatisfiable although any three of them is satisfiable:

\[p(P_1^1) = \frac{1}{2}, \quad p(P_1^2) = \frac{5}{12}, \quad p(P_1^3) = \frac{3}{8} \quad \text{and} \quad p(P_1^4) = \frac{5}{16}.\]

In two dimensions, we need to specify the probability corresponding to only one of the outcomes in a projective measurement. It is routine to verify that this assignment is satisfiable for any three bases but not for all four. The two-dimensional case is exceptional as evidenced by the failure of theorems of Kochen, and Specker and Gleason [6].

#### 3.2. Dimension 3 and higher

In three dimensions, the consistency number according to theorem 1 is $r_3 \leq 7$. We will construct a projective measurement system consisting of seven bases and corresponding probability assignments such that any subset with six bases is consistent but the whole set is not satisfiable showing that the consistency number is indeed 7. The bases will be specified by the corresponding projectors and since each basis is a complete set (the projectors add to $I$, the identity matrix in three dimensions) we need to specify only two of them. Let

\[B_i = \{P_i^1, P_i^2, P_i^3\}, \quad i = 1, \ldots, 7,\]
with a more complicated structure:

\[
\begin{align*}
\text{Tr} & \quad \rho = \frac{1}{2} \left( \begin{array}{ccc}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{array} \right), \\
\text{Tr} & \quad \rho_1 = \frac{1}{2} \left( \begin{array}{ccc}
1 & 1 & 0 \\
1 & 0 & 1 \\
0 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_2 = \frac{1}{2} \left( \begin{array}{ccc}
1 & 1 & 0 \\
1 & 1 & 0 \\
0 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_3 = \frac{1}{2} \left( \begin{array}{ccc}
0 & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_4 = \frac{1}{2} \left( \begin{array}{ccc}
0 & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_5 = \frac{1}{2} \left( \begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_6 = \frac{1}{2} \left( \begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{array} \right), \\
\text{Tr} & \quad \rho_7 = \frac{1}{2} \left( \begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{array} \right).
\end{align*}
\]

The seven bases given above are particularly simple. We now add another base \( B' = \{Q_1, Q_2\} \) with a more complicated structure:

\[
Q_1 = \frac{1}{3} \begin{pmatrix} e^{\pi i/12} & e^{\pi i/3} \\ e^{-\pi i/12} & e^{-\pi i/4} \\ e^{-\pi i/3} & e^{\pi i/4} \end{pmatrix} \quad \text{and} \quad Q_2 = \frac{1}{6} \begin{pmatrix} e^{-3\pi i/4} & e^{-\pi i/3} \\ e^{3\pi i/4} & e^{\pi i/4} \\ e^{3\pi i/4} & e^{\pi i/12} \end{pmatrix}.
\]

Now suppose we have the probability assignments

\[
v(P_j) = p_j \quad \text{and} \quad v(Q_j) = q_j, \quad i = 1, \ldots, 7 \quad \text{and} \quad j = 1, 2.
\]

If there exists a density matrix

\[
\rho = \left( \begin{array}{ccc}
a_1 & z_3 & \bar{z}_2 \\
z_3 & a_2 & \bar{z}_1 \\
\bar{z}_2 & \bar{z}_1 & a_3
\end{array} \right), \quad a_i \geq 0 \quad \text{and} \quad a_1 + a_2 + a_3 = 1,
\]

with the measurement probabilities \( \text{Tr}(\rho P_j) = p_j \), then the following sets of equations determine the real parts of \( z_i \):

\[
a_1 = p_1^1 \quad \text{and} \quad a_2 = p_2^1, \quad (13a)
\]

\[
\text{Re}(z_3) = p_1^2 - (a_1 + a_2)/2 = (a_1 + a_2)/2 - p_2^2, \quad (13b)
\]

\[
\text{Re}(z_2) = p_1^3 - (a_1 + a_3)/2 = (a_1 + a_3)/2 - p_2^3, \quad (13c)
\]

\[
\text{Re}(z_1) = p_1^4 - (a_2 + a_3)/2 = (a_2 + a_3)/2 - p_2^4. \quad (13d)
\]

Similarly, we have the imaginary parts determined by the bases \( B_5, B_6 \) and \( B_7 \):

\[
\text{Im}(z_3) = (a_1 + a_2)/2 - p_1^2 = p_2^2 - (a_1 + a_2)/2, \quad (14a)
\]

\[
\text{Im}(z_2) = (a_1 + a_3)/2 - p_1^3 = p_2^3 - (a_1 + a_2)/2, \quad (14b)
\]

\[
\text{Im}(z_1) = (a_2 + a_3)/2 - p_1^4 = p_2^4 - (a_1 + a_2)/2. \quad (14c)
\]
Note that the addition of each of the blocks for the bases $B_3, \ldots, B_7$ to the block for basis $B_1$ increases the rank by exactly 1. Finally, for the base $B' = \{Q_1, Q_2\}$, we have

$$q_1 = \frac{a_1}{3} + \frac{a_2}{2} + \frac{a_3}{6} + \frac{2 \text{Re}(z_3 e^{i\pi/6})}{\sqrt{6}} + \frac{2 \text{Re}(\bar{z}_3 e^{i\pi/6})}{\sqrt{6}} + \frac{\text{Re}(z_1 e^{i\pi/3})}{\sqrt{3}},$$

$$q_2 = \frac{6}{11} \left(\frac{a_1}{2} + \frac{a_2}{3} + a_3 + \frac{2 \text{Re}(z_3 e^{i\pi/6})}{\sqrt{6}} + \frac{2 \text{Re}(\bar{z}_3 e^{i\pi/6})}{\sqrt{6}} + \frac{2 \text{Re}(z_1 e^{i\pi/3})}{\sqrt{3}}\right).$$

The choice of bases yielding these equations follows a pattern. Each block for the basis $B_i$, $i > 1$, determines exactly one unknown. For example, $B_3$ fixes $\text{Re}(z_3)$ (see (13b)). Moreover, it is clear that the blocks (13a)–(13d) and (14a)–(14c) are independent. So, if two distinct subsets consisting of six equations each are satisfied by some density matrix, then we have already found a unique solution. We infer that this set of seven bases cannot be used to show that $r_3 = 7$. Hence, we have an additional base $B'$. Let us then drop one of the bases, say $B_7$, and replace it with $B'$. Let $O = \{B_1, \ldots, B_6, B'\}$. The last basis $B'$ has the property that if we omit any other basis say $B_i$ from $O$, then the remaining system of equations has the maximal rank. That is, the resulting system of equations (13a)–(13d), (14a)–(14b) (omitting (14c)) and (15) is overdetermined. We describe below a ‘procedure’ for finding probability assignments to the bases in $O$ such that any six of them are consistent but the whole set is not.

First, a necessary and sufficient condition for $\rho$ given in (12) to be the density matrix is that the following relations are satisfied:

$$\det(\rho) = a_1 a_2 a_3 - \sum_{i=1}^{3} a_i |z_i|^2 + 2 \text{Re}(z_1 z_3) \geq 0,$$

$$a_1 a_2 - |z_1|^2 \geq 0, \quad a_3 a_1 - |z_3|^2 \geq 0, \quad a_1 a_2 - |z_1|^2 \geq 0 \quad \text{and} \quad a_1, a_2 \geq 0. \quad (16)$$

These conditions reflect the fact that for a Hermitian matrix to be positive definite, it is necessary and sufficient that all the principal minors have a non-negative determinant. Now choose a density matrix $\rho$ such that the inequalities in (16) are strict. We also choose $a_1, a_2 > 0$ such that $a_1 + a_2 < 1$ and substitute $a_3 = 1 - a_1 - a_2$. Now treat $a_0, \text{Re}(z_1)$ and $\text{Im}(z_3)$ as (real) variables. Then, the left-hand sides of all the inequalities above are the continuous functions of these variables. Here, we consider $\rho$, parametrized by $\{a_1, a_2, \text{Re}(z_1), \text{Im}(z_3) : i = 1, 2, 3\}$, as a member of $\mathbb{R}^3$. Hence, there is an open neighborhood $N_1$ of $\rho$ such that these inequalities hold everywhere in $N_1$. Compute $\text{Tr}(\rho P_i) = p_i', i = 1, \ldots, 6$, $\text{Tr}(\rho Q_1) = q_1'$ and $\text{Tr}(\rho Q_2) = q_2'$ (note the ‘prime’). From the set of bases $O$ if we drop any base from the set $\{B_1, \ldots, B_6\}$, then the remaining set of equations have the maximal (real) rank 8. Let $A_i$ denote the invertible matrix of maximal rank consisting of coefficients of a set of independent equations corresponding to the omission of $B_i, i = 2, \ldots, 6$.

The invertibility of the matrices $A_i, i = 1, \ldots, 6$, implies that the images $A_i(N_1)$ are the open sets, and hence, $\bigcap_i A_i(N_1) \equiv G$ is open. The point $\alpha' = (p_1', p_2', \ldots, p_6', p_7', q_1', q_2')$ is in $G$ as it is the image of $\rho$. We choose a point $q_2 \neq q_2'$ such that if the last ‘coordinate’ $q_2$ in $\alpha'$ is replaced by $q_2$, then the resulting vector $\alpha \in G$. Since $G$ is open, such a choice is always possible. This choice of $q_2$ makes the new assignments for $O$ inconsistent. But restricting this assignment to any six bases is still consistent. First, if we omit $B'$, then clearly the assignment in rest of the bases is satisfiable by $\rho$ itself. If we omit any other base say $B_6$, then a desired density matrix, say, $\gamma$ is given by $A_6^{-1}(\alpha)$. We thus conclude that

The probability assignments to the seven bases $O$ given above are such that any six of them is consistent with a quantum state (density matrix) but the whole set is not.
Next, it is clear that we can mimic the construction of the bases given above for three dimensions in any dimension \( n > 3 \). Thus, define the bases \( B_0 \) and \( B_{ij} \), \( i > j \), as follows. Let \( e_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T \) (ith coordinate = 1) be the standard basis (the computational basis). Then, \( B_0 = \{ P_0^i = e_i e_i^T : i = 1, \ldots, n-1 \} \) is the basis consisting of projectors on the standard basis. They determine the diagonal elements of the state \( \rho \). Next, let

\[
B_{ij} = \{ P_{ij}^k : 1 \leq i < j \leq n \text{ and } 1 \leq k \leq n-1 \}, \quad P_{ij}^k = \frac{1}{2}(e_i - e_j)(e_j - e_i)^T,
\]

\[
P_{ij}^k = \frac{1}{2}(e_i - e_j)(e_j - e_i)^T \text{ and } P_{ij}^k = e_i e_i^T \quad k \neq i, j.
\]

These \( n(n-1)/2 \) bases determine the real parts of the off-diagonal elements of \( \rho \). These correspond to \( B_2, B_3 \) and \( B_4 \) in the three-dimensional case above. We similarly define the \( n(n-1)/2 \) bases for the imaginary parts of off-diagonal elements of \( \rho \):

\[
B'_{ik} = \{ P_{ik}^{jk} : 1 \leq i < k \leq n \text{ and } 1 \leq k \leq n-1 \}, \quad P_{ik}^{jk} = \frac{1}{2}(e_j + i e_k)(e_j + i e_k)^T,
\]

\[
P_{ik}^{jk} = \frac{1}{2}(e_j - i e_k)(e_j - i e_k)^T \text{ and } P_{ij}^k = e_i e_i^T \quad l \neq j, k.
\]

As in the three-dimensional case, we replace one of the bases, say \( B_{ij} \), by a basis \( Q \). Call the new system of bases \( Z \). The basis \( Q \) is chosen so that the probability assignments to all the bases in \( Z \) yield an over-determined system of equations. This can be achieved by ensuring that the rank of the system corresponding to \( \mathcal{G} = B_{ij} \) and \( Z = B_{ij} \), \( \forall 1 \leq i < j \leq n \), is maximal (\( = n^2 \)). We can then use topological arguments similar to the three-dimensional case to show that every subsystem of \( Z \) has a consistent solution but the full system \( Z \) consisting of \( R_n = n^2 - n + 1 \) bases does not. Thus, the number \( R_n \) in theorem 1 is the best possible. We can now state the following.

**Theorem 2.** The consistency number of an \( n \)-dimensional quantum system is \( r_n = R_n \).

Combining this theorem with Gleason’s theorem [6], we obtain the following theorem. First, recall some definitions needed to state Gleason’s famous result. Let \( v \) be a function on the set \( \mathcal{P}(H) \) of projections on a finite-dimensional Hilbert space \( H \) such that

\[
0 \leq v(E) \leq 1, \quad v(I) = 1, \quad \text{(19a)}
\]

\[
v(E + F) = v(E) + v(F) \quad \text{if } EF = 0(\text{orthogonal projections}). \quad \text{(19b)}
\]

Such a function is called a frame function.

**Theorem 3.** Let \( \mathcal{Z} = \{ \mathcal{U}_i \mid i \in I \} \), where \( I \) is an indexing set and \( \mathcal{U}_i = \{ E_i^1, \ldots, E_i^k \} \) consists of orthogonal projections: \( E_i^l E_i^j = \delta_{ij} \) on a Hilbert space of dimension \( n \geq 3 \). Suppose a real-valued function \( f \) on \( \mathcal{Z} \) satisfies (19a). Furthermore, assume that for every set \( S \subset \mathcal{Z} \) of cardinality \( n^2 - n + 1 \), there exists a frame function \( v_\mathcal{S} \) such that \( f(E) = v_\mathcal{S}(E) \) for all \( e \in \cup \mathcal{S} \). Then, there exists a frame function \( v \) such that \( f = v \) on \( \cup \mathcal{Z} \).

**Proof.** Gleason’s theorem states that any frame function \( w \) on a Hilbert space of dimension at least 3 is induced by some density operator \( \rho \): \( w(E) = \text{Tr}(\rho E) \). This implies that for every subset \( S \) of \( \mathcal{Z} \) of cardinality \( n^2 - n + 1 \), the function \( f \) defines a consistent QPA in the sense explained in section 1. However, as the projections \( E_i^l \) may not be one-dimensional, we cannot apply theorem 1 directly. In this case, we adopt the following procedure. Let \( E \) be a projection operator of rank \( k > 1 \). We decompose \( E = E_1 + \cdots + E_k \), where \( E_i \) are one-dimensional projection operators with \( E_i E_j = \delta_{ij} \). We replace each member of \( \mathcal{U}_i \) by the projectors in its one-dimensional decomposition. Let the resulting set of orthonormal projectors be \( \mathcal{U}'_i \). It is easy to see that any \( S \subset \mathcal{Z}' \) has consistent probability assignment induced by the original assignment on \( S \subset \mathcal{Z} \). Therefore, from theorem 1, there is a frame function \( v \) (given by a density matrix) which yields the same probabilities. The additivity of the frame functions now implies that \( f = v \) on \( \cup \mathcal{Z} \). \( \square \)
4. Applications

In this section, we consider some applications of the constructions in the previous section. First, we sketch a secret sharing scheme involving copies of entangled qubits. A version of the secret sharing problem [7] is as follows. A group of \(k\) players is to share a secret (represented by a number). If any subset of at least \(r\) players pool their resources (their shares) the secret is revealed, otherwise it is not. This is called a \((k, r)\) (threshold) secret sharing scheme. Our scheme is probabilistic and we only require that any set of \(r\) players can discover the secret with a high probability, whereas for less than \(r\) players, the probability is low. We sketch a scheme using entangled qubits.

Suppose we prepare multiple copies of a composite quantum system of dimension \(N\). To each of the \(k\) players, we send a number of copies of the system (or some part thereof) along with instructions for specific measurements. If we arrange it so that the probability of reconstructing the set from any \(r \leq k\) expectation values is high, but negligible for any subset of cardinality \(r' < r\) measurements, then we have a \((k, r)\) secret sharing scheme. We outline below such a scheme for a system of \(n\) qubits. Let \(N = 2^n\), the dimension of the system. For simplicity, we will only consider a \((k, k)\) secret sharing scheme.

1. A large number of copies of a state randomly chosen from an initial set \(S\) of \(K_0\) states is prepared by the dealer.
2. The dealer provides the players with \(m\) copies each from the original ensemble called their shares.
3. The players are also given instructions about their respective bases in which projective measurements are to be performed: the bases are from \(B_{ij}\) or \(B'_{ij}\) given in (17) and (18), respectively. There are \(N^2 - N\) such bases. Thus, each player is actually measuring the real or the imaginary part of an off-diagonal element of the density matrix.
4. We assume that the diagonal elements are conveyed to each player along with the measurement instruction. These may be used as group ‘password’ and/or as a check for interference.
5. We assume that the set \(S\) of states are so chosen that when all but one of the (real) parameters characterizing the off-diagonal elements of \(\rho\) are fixed, there still a large number \(\geq K_1\) of possible states with different values of the remaining parameter. We omit the details of how this is done in this sketch. It implies that \(K_0 = O(K_1 n^2)\). The values of each parameter are separated by a distance \(> \lambda\).
6. Suppose \(\alpha\) is one of the parameters. We see from equations like (17) and (18) that the expectation values yield the probabilities and, hence, the value of \(\alpha\). Using the Chernoff bound (classical) it is seen that if \(\alpha_0\) is the correct value of \(\alpha\) and \(\tilde{\alpha}\) is the calculated value, then
   \[
   \text{probability}(|\alpha - \tilde{\alpha}| > \lambda) < O(e^{-\lambda^2/m}).
   \]
   Therefore, if we are aware of the states in \(S\), then with a high probability we can determine the parameter \(\alpha\).
7. If all the \(N^2 - N\) players combine their measurement results, then (along with the information about diagonal elements) the particular state \(\rho\) is determined with a high probability. However, with just one player missing, the probability drops to \(< 1/K_1\).

In this probabilistic protocol, we assume that we have secure quantum channels with negligible errors. It is possible to devise a more elaborate scheme to accommodate insecure channels. Similarly, we can devise a general \((k, r)\) secret sharing scheme combining the quantum scheme with a classical one involving polynomial evaluation.
The selection of the set $S$ is a bit more challenging. However, there are several possible approaches. One is to start with a positive-definite matrix and then keeping all the values of the parameter vary one of the parameters characterizing the off-diagonal elements. For example, let $\alpha_{ij} = \text{Re}(\rho_{ij})$ and $\beta_{ij} = \text{Im}(\rho_{ij}), \ i < j$, and suppose we want to vary $\beta_{12}$. Using topological arguments as before we know that there is some neighborhood of $\beta_{12}$ such that for all values of the latter in that neighborhood we obtain a positive-definite matrix (fixing the normalization is trivial). We divide the neighborhood into segments of appropriate size (fixing $\lambda$) and pick our values for $\beta_{12}$. Alternatively, we could use the fact that for any Hermitian matrix $A$, $A^2$ is positive definite. We vary the parameters of $A$ to achieve our goal. We will not go into a detailed analysis here as our primary goal was to demonstrate potential applications of the constructions of preceding sections.

Our protocol has some similarity to the one given in [8]. The difference is ours is probabilistic. However, our protocol accommodates a larger number of players at the expense of requiring multiple copies of states. Thus, using four qubits ($N = 16$), we can accommodate $N^2 - N = 240$ players.

The state $\rho$ may also be prepared by a purification process [9]. Thus, given a density matrix $\rho$ in an $N$-dimensional Hilbert space $H_N$, we can find a pure state $|\Psi\rangle$ in $H_M \otimes H_N$, where $H_M$ is an $M$-dimensional space, such that

$$
\rho = \text{Tr}_{H_M} (|\Psi\rangle \langle \Psi|).
$$

The operation $\text{Tr}_{H_M}$ is the partial trace with respect to $H_M$. This method eliminates the need for creating a mixed state by random selection. The dealer prepares the state $|\Psi\rangle$ and the players get only the components (qubits) in $H_N$. An added advantage of this procedure is that the dealer can use the fact that $|\Psi\rangle$ is entangled with states in $H_M$ to ensure that the players are using their assigned measurements.

The bases given in equations (17) and (18) could be used for quantum state tomography. In this case, we do not require maximal outcomes in all the bases. Thus, assuming that the diagonal elements of the density matrix have been estimated, we need only measurements with three alternatives. For example, if we want to estimate $\text{Re}(\rho_{12})$, then using the notation in (17) the orthogonal projections $P_{12}^1, P_{12}^2$ and $M_{12} = \sum_{k \neq 1,2} P_{12}^k$ form a complete set and provide the three outcomes. Note also that projections $P_{ij}^1$ and $P_{ij}^2$ can be obtained by repeated applications of Hadamard and control gates.

5. Discussion

In this work, we stated and solved a problem of consistent probability assignments for maximal projective measurements, i.e. the number of projection operators in each measurement equals the dimension. This can be relaxed. For example, in the measurement bases in section 3.2, it is immaterial for the basis $B_i, \ i > 0$, whether we take the complete basis or three projectors—two orthogonal projectors on a ‘plane’ spanned by two vectors from $B_0$ and one projector orthogonal to the plane. The problem of consistency number $r_n$ arises in the first place because we have no a priori knowledge about the independence of the projection operators corresponding to the bases. We can visualize such a situation when different observers have no initial communication and can perform only local measurements. Furthermore, it is not easy to define general procedures for constructing such independent bases. One notable exception is the explicit recipe for mutually unbiased bases (MUB). MUBs were first introduced by Schwinger [10] in low dimension and later extended to prime and prime-power dimensions by Ivanovic [11] and Wootters and Fields [12], respectively. The problem is this recipe does not work when the dimension has two distinct prime factors.
The next logical question would be to consider the problem of consistent probability assignment for more general measurement schemes, in particular, for local measurements of entangled states. The most general problem regarding consistency number would be the following. What is the consistency number of a collection of measurements (positive operator valued in general) given some prior information about the state? In this format we have to satisfy some extra constraints. For example, we may have information that the unknown state is pure. The constraints would be nonlinear in general. More interesting protocols would result from these investigations. We hope to investigate these questions in future.

References

[1] van der Meyden R and Patra M 2003 Proc. Computer Science Logic and 8th Kurt Gödel Colloquium (Vienna: Springer)
[2] Bell J S 1966 Rev. Mod. Phys. 38 447
[3] Kochen S and Specker E P 1967 J. Math. Mech. 17 59
[4] Stewart G W 1998 Matrix Algorithms vol 1 (Philadelphia, PA: SIAM) p 188
[5] Kelley J L 1975 General Topology (Berlin: Springer) p 33
[6] Gleason A M 1957 J. Math. Mech. 6 885
[7] Shamir A 1979 Comm. ACM 22 612
[8] Hillery M, Buzek V and Berthiaume A 1999 Phys. Rev. A 59 1829
[9] Nielsen M A and Chuang I L 2000 Quantum Computation and Information (Cambridge: Cambridge University Press)
[10] Schwinger J 1960 Proc. Natl Acad. Sci. 46 570
[11] Ivanovic I D 1981 J. Phys. A: Math. Gen. 14 3241
[12] Wootters W K and Fields B D 1989 Ann. Phys. 191 363