Unknown quantum state discrimination and its physical realization

by
Bing He

A dissertation submitted to the Graduate Faculty in Physics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2008

This manuscript has been read and accepted for the Graduate Faculty in Physics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Date	Professor Janos A. Bergou Chair of Examining Committee
Date	Professor Steve Greenbaum Executive Officer
Professor Ying–Chin Chen	
Professor Christoph Gerry	
Professor Mark Hillery	
	Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Unknown quantum state discrimination and its physical realization

by

Bing He

Adviser: Professor János A. Bergou

The discrimination of completely unknown quantum states is a difficult problem in quantum state discrimination. We study the general case of unknown qubit discrimination, where the input states are constructed with arbitrary number of the unknown qubits as the reference. The optimal measurements for the unknown qubit discrimination are derived in two different approaches. Implementation of unknown state discrimination is realized by unitary transformation in the extended space of inputs. To study the discrimination of unknown single photon states and unknown coherent states, we present the methods for linear optical realization of the general transformations on single photon states and coherent state products. Finally, we describe two physical systems for unknown optical qubit discrimination and unknown coherent state discrimination. One application of unknown coherent state discrimination is efficient and non-destructive quantum database searching.

Dedication

To my family: my parents, sister, and my wife

Acknowledgments

I wish to express the deepest gratitude to my advisor, Prof. János A. Bergou, for guiding me to the research in quantum state discrimination. His profound knowledge in this field and offering ample freedom in choosing problems facilitated my exploration into many interesting topics.

I especially thank Prof. Mark Hillery for the valuable help at the beginning stage of my research.

I also thank the people who shared views with me or helped me in one or more research projects. Among them are Yonatan Abranyos, Yuhang Ren, Yuqing Sun.

Table of contents

List of Tables

List of Figures

Chapter I

1 Introduction

1.1 Discrimination of unknown quantum states

The discrimination of quantum states is a nontrivial problem since a quantum state cannot be cloned perfectly if it is unknown to us [1]. There are strategies of achieving the optimal results in the discrimination of a set of quantum states $\{|\rho_i\rangle\}$, where $i = 1, \cdots, N$. The strategy discovered first is minimum error discrimination [2, 3], where each measurement outcome select one of the possible states and the error probability is minimized. The other strategy, which has wide applications in quantum information processing, is optimal unambiguous states discrimination (USD) for the linearly independent states [4, 5, 6, 7, 8], where unambiguity is paid by the possibility of getting inconclusive results from the measurement. For the linearly dependent state sets, there is an analogue of optimal USD—maximum confidence measurement [9]. In all these approaches, the input states to be discriminated could occur or be prepared with some *a prior* probabilities η_i.

When we discriminate a pair of completely unknown quantum states $|\psi_i\rangle$, for $i = 1, 2$, the only possible way is to have copies of these unknown states as the reference. Then we can design the proper measurement that is capable of distinguishing

the inputs in the form of, for example, $|\psi_1\rangle|\psi_2\rangle|\psi_i\rangle$. In these inputs the data states $|\psi_i\rangle$ are appended to the reference copies to form the states with the permutation symmetry. If we require that the incoming unknown data states should be unambiguously discriminated, our device will output three possible results: 1 corresponding to the input being $|\psi_1\rangle$, 2 to that being $|\psi_2\rangle$, and 0 for inconclusiveness. The optimal unambiguous measurement of these symmetric input states has been studied in both the Bayesian [10] and the minimax approaches [11]. Another feature we need to have for such a device is the universality: it will perform optimally for any pair of unknown states. Since the input states are unknown, the quantity we use to indicate how well the device works is the average success probability over the Hilbert spaces of all randomly distributed $|\psi_1\rangle$ and $|\psi_2\rangle$.

In the original work of two completely unknown states discrimination without ambiguity [10], the authors used a sort of programmable quantum devices, which have been studied both theoretically and experimentally in the recent years [12, 13, 14, 15, 16, 17, 43], to relate the program part of the inputs in a simple way to the unknown states $|\psi_1\rangle$ and $|\psi_2\rangle$ one is trying to identify. The total input states measured by the device are prepared with the extra copy of the unknown states as $|\psi_1\rangle_A|\psi_1\rangle_B|\psi_2\rangle_C$ and $|\psi_1\rangle_A|\psi_2\rangle_B|\psi_2\rangle_C$, and the optimal measurement for the USD of the inputs is designed with the permutation symmetry of the program registers A, C and the data register B. If the *a priori* probabilities of the inputs are equal, the

maximum average success probability of discriminating a pair of unknown qubits can be as large as 1/6.

1.2 Quantum measurements

In this section, we briefly review the basic measurements in quantum state discrimination. The standard measurement in quantum mechanics is the projection valued measurement (PVM) or the von Neumann meaurement. In an N-dimensional space $\mathcal{H}$ such a measurement is given as a set of projective operators:

$$P_i = |v_i\rangle\langle v_i|, \tag{1.2.1}$$

where $|v_i\rangle$, for $i = 1, \cdots, N$, form an orthogonal basis for the space $\mathcal{H}$. These operators satisfy the relations

$$\begin{aligned} P_i^2 &= P_i; \\ \sum_{i=1}^{N} P_i &= I. \end{aligned} \tag{1.2.2}$$

If the system is in the state $|\psi\rangle$, the probability of obtaining the result P_i is $p_i = \langle\psi|P_i|\psi\rangle$. There are only two possible eigenvalues 0 and 1 for each operator P_i in the case of a PVM.

The PVM can be generalized with P_i replaced by contractions Π_i ($||\Pi_i|| \leq 1$). In this generalized measurement, the probability of obtaining Π_i is $p_i = \langle\psi|\Pi_i|\psi\rangle$. These

contractions satisfy

$$\sum_{i=1}^{N} \Pi_i = I. \tag{1.2.3}$$

Because Π_i take the positive eigenvalue between 0 and 1, the generalized measurement is termed the positive operator valued measurement (POVM).

If the states we want to discriminate are known, we can use the given information to find the optimal measurements, which can be either PVM or POVM, to discriminate the elements in the set of states. If we know nothing about these states, however, the only information available will be the permutation symmetry with respect to a given number of the unknown state copies provided to us.

1.3 Outline of dissertation

This dissertation covers the discrimination of unknown states in two different approaches and its physical realization for unknown optical qubits and unknown coherent states.

In chapter II, we study the discrimination of two unknown qubits with multiple copies of them as the reference. Moreover, we will provide a method to realize the optimal USD of unknown quantum states. The related publications to chapter II are as follows:

- A generalized programmable unambiguous state discriminator for unknown qubit

systems. Bing He and Janos A. Bergou, Physics Letters A, Volume 359, 103 (2006).

• A general approach to physical realization of unambiguous quantum-state discrimination. Bing He and Janos A. Bergou, Physics Letters A, Volume 356, 306 (2006).

In chapter III, we reformulate the general problem of unknown qubit discrimination as that of distinguishing between two known mixed states, which are obtained through averaging over the Bloch sphere of the unknown qubits. We discuss the optimal USD and the minimum-error discrimination of the averaged or dephased inputs constructed with the unknown qubits. The material in this chapter is from the following paper:

• Programmable unknown quantum-state discriminators with multiple copies of program and data: A Jordan basis approach. Bing He and Janos A. Bergou, Physical Review A, Volume 75, 032316 (2007).

Unknown state discrimination can be of potential value in quantum information processing, so it is interesting to study its feasible implementations. In this dissertation we study the implementation of discriminating two types of unknown photonic states—discrete optical qubits and coherent states. In chapter IV we provide the general tools for processing these two types of signals. All possible transformations on discrete single photon states and coherent state products are discussed in this chapter. We will follow the developments in the following papers:

• Implementation of quantum operations on single photon *qudits*. Bing He, Janos A. Bergou and Zhiyong Wang, Physical Review A, Volume 76, 042326 (2007).

• Coherent states engineering with linear optics: possible and impossible tasks. Bing He and Janos A. Bergou, Physical Review A, Volume 77, 053818 (2008).

The practical unknown state discrimination systems are discussed in chapter V. A universal unknown optical discriminator and a quantum database searching device to identify an unknown coherent state are described in detail. The related publications are the following:

• Universal discriminator for completely unknown optical qubits. Bing He, Janos A. Bergou and Yuhang Ren, Physical Review A, Volume 76, 032301 (2007).

• Coherent states engineering with linear optics: possible and impossible tasks. Bing He and Janos A. Bergou, Physical Review A, Volume 77, 053818 (2008).

Finally, we conclude by summarizing the main results in the last chapter.

Chapter II

2 Unknown state discrimination—approach without dephasing

2.1 Discrimination with multiple reference copies

In this section, we first follow the approach in [10] to study the discrimination of two unknown qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ with multiple copies of such states as the reference. The results about the optimal discrimination with the general situation of n copies of reference and their dependence on the input copy number and the *a prior* probabilities of the input states are originally presented in [19].

As the general inputs, we place n copies of reference qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ in the program sector of the quantum registers as follows:

$$\begin{aligned} |\Psi_1^{in}\rangle &= |\psi_1\rangle_1|\psi_2\rangle_2\cdots|\psi_1\rangle_{2n-1}|\psi_2\rangle_{2n}|\psi_1\rangle_{2n+1} \\ |\Psi_2^{in}\rangle &= |\psi_1\rangle_1|\psi_2\rangle_2\cdots|\psi_1\rangle_{2n-1}|\psi_2\rangle_{2n}|\psi_2\rangle_{2n+1}, \end{aligned} \tag{2.1.1}$$

where the data, either $|\psi_1\rangle$ or $|\psi_2\rangle$, at the tail is appended to the program. Without loss of generality in the preparation of the program parts, we place $|\psi_1\rangle$ in the odd positions and $|\psi_2\rangle$ in the even positions of the inputs. We need to find an optimal measurement to unambiguously distinguish between these inputs, bearing in mind

the data qubits,

$$|\psi_i\rangle = \cos(\theta_i/2)|0\rangle + \sin(\theta_i/2)e^{i\phi_i}|1\rangle \ , \tag{2.1.2}$$

where $i = 1, 2$, are randomly distributed on Bloch sphere with no available information about θ_i's and ϕ_i's. Generally these quantum registers are assumed to be prepared with *a prior* probabilities η_1 and η_2, respectively.

The optimal measurement performed by our device is generally achieved by a positive operator value measure (POVM), and we denote its element of unambiguously detecting $|\Psi_1^{in}\rangle$ as Π_1, that of unambiguously detecting $|\Psi_2^{in}\rangle$ as Π_2, and that corresponding to failure as Π_0. They satisfy unit decomposition:

$$I = \Pi_1 + \Pi_2 + \Pi_0 \ . \tag{2.1.3}$$

The probabilities of successfully identifying these two possible input states are given by

$$\langle\Psi_1^{in}|\Pi_1|\Psi_1^{in}\rangle = p_1 \qquad \langle\Psi_2^{in}|\Pi_2|\Psi_2^{in}\rangle = p_2 \ , \tag{2.1.4}$$

and the condition of no error implies that

$$\Pi_2|\Psi_1^{in}\rangle = 0 \qquad \Pi_1|\Psi_2^{in}\rangle = 0 \ . \tag{2.1.5}$$

Without any knowledge about $|\psi_1\rangle$ and $|\psi_2\rangle$, what we can make use of in determining the inputs is their symmetry, i.e. $|\Psi_1^{in}\rangle$ is invariant under the action of symmetric group on the odd positions and the tail position, while $|\Psi_2^{in}\rangle$ invariant under the corresponding action on the even positions and the tail. To construct Π_1 and Π_2 that

perform the UD of the inputs, we define the following orthornormal basis:

$$
\begin{aligned}
|e_0\rangle &= \frac{1}{\sqrt{C_n^0}}|0,0,\ldots,0\rangle \\
|e_1\rangle &= \frac{1}{\sqrt{C_n^1}}(|1,0,\ldots,0\rangle + |0,1,\ldots,0\rangle + \cdots + |0,0,\ldots,1\rangle) \\
&\ldots \\
|e_k\rangle &= \frac{1}{\sqrt{C_n^k}}(\underbrace{|1,1,\ldots,0,0\rangle}_{k's\ 1\ in\ n\ digits} + |0,1,1,\ldots,,0\rangle + \cdots + |0,0,\ldots,1,1\rangle) \\
&\qquad\qquad \underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{summation\ of\ C_n^k\ terms} \\
&\ldots \\
|e_n\rangle &= \frac{1}{\sqrt{C_n^n}}|1,1,\ldots,1\rangle\ , \qquad (2.1.6)
\end{aligned}
$$

where C_n^k is the number of ways to choose k objects from a group of n objects without regard to order. In terms of this basis, the tensor product of n copies of a qubit is expanded as follows:

$$(\cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle)^{\otimes n} = \sum_{k=0}^{n} \cos^{n-k}(\theta/2)\sin^k(\theta/2)e^{ik\phi}\sqrt{C_n^k}|e_k\rangle\ . \quad (2.1.7)$$

Thus we construct the POVM elements satisfying the unambiguity (no error) in measurement:

$$
\begin{aligned}
\Pi_1 &= c_1(I_{E,T} - P_{E,T}) \otimes I_O \\
\Pi_2 &= c_2(I_{O,T} - P_{O,T}) \otimes I_E, \qquad (2.1.8)
\end{aligned}
$$

where $P_{E,T} = \sum_{k=0}^{n+1} |e_k\rangle_{E,T\ \ E,T}\langle e_k|$ (resp. $P_{O,T} = \sum_{k=0}^{n+1} |e_k\rangle_{O,T\ \ O,T}\langle e_k|$) is the projection operator onto the totally symmetric subspace with respect to the n even (resp. odd) positions and the tail position, $I_{E,T}$ (resp. $I_{O,T}$) the direct product of unit matrices

in these positions, and c_1, c_2 the non-negative parameters arising from the unequal *a priori* probabilities of $|\Psi_1^{in}\rangle$ and $|\Psi_2^{in}\rangle$. I_O and I_E are the direct products of the unit matrices in the odd and the even positions of the input states, respectively.

Using these Π_i, where $i = 1, 2$, we find their detecting probabilities

$$p_i = \langle\Psi_i^{in}|\Pi_i|\Psi_i^{in}\rangle = c_i - c_i\langle\Psi_i^{in}|P_{R,T} \otimes I_S|\Psi_i^{in}\rangle \ , \tag{2.1.9}$$

where $R = E, O$ but $S = O, E$. We use two tricks to calculate the average of the projection operators more conveniently. First, by the expansion

$$|e_k\rangle_{R,T} \ = \ \sqrt{\frac{C_n^k}{C_{n+1}^k}}|e_k\rangle_R|0\rangle_T + \sqrt{\frac{C_n^{k-1}}{C_{n+1}^k}}|e_{k-1}\rangle_R|1\rangle_T, \tag{2.1.10}$$

for $k = 1, 2, \cdots, n$, we rewrite the projection operators as

$$\begin{aligned} P_{R,T} \otimes I_S \ = \ & \{|e_0\rangle_R|0\rangle_T \ {}_R\langle e_0| \ {}_T\langle 0| \\ & + \sum_{l=1}^{n}(\sqrt{\frac{C_n^l}{C_{n+1}^l}}|e_l\rangle_R|0\rangle_T + \sqrt{\frac{C_n^{l-1}}{C_{n+1}^l}}|e_{l-1}\rangle_R|1\rangle_T) \\ & \times (\sqrt{\frac{C_n^l}{C_{n+1}^l}} \ {}_R\langle e_l| \ {}_T\langle 0| + \sqrt{\frac{C_n^{l-1}}{C_{n+1}^l}} \ {}_R\langle e_{l-1}| \ {}_T\langle 1|) \\ & + |e_n\rangle_R|1\rangle_T \ {}_R\langle e_n| \ {}_T\langle 1|\} \otimes I_S. \end{aligned} \tag{2.1.11}$$

Second, we apply Eq. (2.1.7) to expand the input states by two parts:

$$|\Psi_i^{in}\rangle = \underbrace{\sum_{l=0}^{n} \cos^{n-l}(\theta_j/2)\sin^l(\theta_j/2)e^{il\phi_j}\sqrt{C_n^l}|e_l\rangle_R\left(\cos(\theta_i/2)|0\rangle_T + \sin(\theta_i/2)e^{i\phi_i}|1\rangle_T\right)}_{|\Psi_i'\rangle}$$
$$\times \underbrace{\sum_{k=0}^{n} \cos^{n-k}(\theta_i/2)\sin^k(\theta_i/2)e^{ik\phi_i}\sqrt{C_n^k}|e_k\rangle_S}_{|\Psi_i''\rangle} , \quad (2.1.12)$$

where $i = 1, 2$ but $j = 2, 1$. Putting the expectation values from these parts together, we obtain

$$\begin{aligned}
&\langle\Psi_i^{in}|P_{R,T}\otimes I_S|\Psi_i^{in}\rangle \\
&= \sum_{k=0}^{n}\left(\frac{n-k+1}{n+1}\ cos^2(\theta_i/2) + \frac{k+1}{n+1}\ sin^2(\theta_i/2)\right) C_n^k\ cos^{2(n-k)}(\theta_j/2)\ sin^{2k}(\theta_j/2) \\
&+ \sum_{k=1}^{n}\ \frac{2k}{n+1}\ C_n^k\ cos^{2(n-k)}(\theta_j/2) sin^{2k}(\theta_j/2)\ cot(\theta_j/2)\ cos(\theta_i/2)\ sin(\theta_i/2) \\
&\times cos(\phi_i - \phi_j)\ . \quad (2.1.13)
\end{aligned}$$

The total success probability P to discriminate between the two unknown states, assuming $|\Psi_1^{in}\rangle$ is produced with *a priori* probability η_1 and $|\Psi_2^{in}\rangle$ with η_2, is given by

$$P = \eta_1 p_1 + \eta_2 p_2\ . \quad (2.1.14)$$

Since we have no knowledge about the data states, what we use to indicate how well the device performs is the average of this success probability:

$$\begin{aligned}
\overline{P} &= \frac{1}{(4\pi)^2}\prod_{j=1}^{2}\int_0^{2\pi} d\phi_j \int_0^{\pi} d\theta_j \sin\theta_j(\eta_1\langle\Psi_1^{in}|\Pi_1|\Psi_1^{in}\rangle + \eta_2\langle\Psi_2^{in}|\Pi_2|\Psi_2^{in}\rangle) \\
&= (\eta_1 c_1 + \eta_2 c_2)\frac{n}{2(n+1)}. \quad (2.1.15)
\end{aligned}$$

We want to maximize this expression subject to the constraint that Π_0 is a positive operator.

Let H be the Hilbert space of the input states given in Eq. (2.2.2), which, as it is seen from Eq. (2.1.10), is spanned by the orthonormal basis $\{|e_l\rangle_O|e_m\rangle_E|0\rangle_T, |e_l\rangle_O|e_m\rangle_E|1\rangle_T\}$, where $l, m = 0, 1, \cdots, n$. To have a nice matrix representation of the inconclusive operator,

$$\Pi_0 = I - \Pi_1 - \Pi_2 = (1 - c_1 - c_2)I + c_1 P_{E,T} \otimes I_O + c_2 P_{O,T} \otimes I_E \ , \qquad (2.1.16)$$

we apply the following orthogonal transformations:

$$\begin{aligned} |\eta_{lm}\rangle &= \sqrt{\frac{C_n^m}{C_{n+1}^m}}|e_l\rangle_O|e_m\rangle_E|0\rangle_T + \sqrt{\frac{C_n^{m-1}}{C_{n+1}^m}}|e_l\rangle_O|e_{m-1}\rangle_E|1\rangle_T \\ |\chi_{lm}\rangle &= \sqrt{\frac{C_n^{m-1}}{C_{n+1}^m}}|e_l\rangle_O|e_m\rangle_E|0\rangle_T - \sqrt{\frac{C_n^m}{C_{n+1}^m}}|e_l\rangle_O|e_{m-1}\rangle_E|1\rangle_T, \end{aligned} \qquad (2.1.17)$$

where $l = 0, 1, \cdots, n$, and $m = 1, 2, \cdots, n$. The transformed vectors $|\eta_{lm}\rangle$ and $|\chi_{lm}\rangle$ satisfy $\langle\eta_{lm}|\chi_{l'm'}\rangle = 0$, $\langle\eta_{lm}|\eta_{l'm'}\rangle = \delta_{l,l'}\delta_{m,m'}$, and $\langle\chi_{lm}|\chi_{l'm'}\rangle = \delta_{l,l'}\delta_{m,m'}$. If we put them together with the untransformed $|e_l\rangle_O|e_0\rangle_E|0\rangle_T$ and $|e_l\rangle_O|e_n\rangle_E|1\rangle_T$, for $l = 0, 1, \cdots, n$, all these unit vectors form an orthornormal basis,

$$\{|v\rangle_k\} = \{|\eta_{lm}\rangle, |\chi_{lm}\rangle, |e_l\rangle_O|e_0\rangle_E|0\rangle_T, |e_l\rangle_O|e_n\rangle_E|1\rangle_T\}, \qquad (2.1.18)$$

of H.

With this basis, the operator Π_0 is represented by the direct sum of two series of

block diagonal matrices:

$$\Pi_0 = \Pi_0^{(1)} \oplus \Pi_0^{(2)}, \tag{2.1.19}$$

where

$$\Pi_0^{(1)} = \begin{pmatrix} J_0 & & & & \\ & J_1 & & & \\ & & J_2 & & \\ & & & \ddots & \\ & & & & J_n \end{pmatrix}, \quad \Pi_0^{(2)} = \begin{pmatrix} K_0 & & & & \\ & K_1 & & & \\ & & K_2 & & \\ & & & \ddots & \\ & & & & K_n \end{pmatrix}. \tag{2.1.20}$$

These block diagonal matrices are generated regularly; J_0 and K_0 are 1×1 matrix 1, and J_1 is a 3×3 matrix:

$$J_1 = \begin{pmatrix} 1 - \frac{1}{n+1}c_2 & \frac{\sqrt{n}}{(n+1)^{3/2}}c_2 & -\frac{n}{(n+1)^{3/2}}c_2 \\ \frac{\sqrt{n}}{(n+1)^{3/2}}c_2 & 1 - \frac{n}{(n+1)^2}c_2 & \frac{n^{3/2}}{(n+1)^2}c_2 \\ -\frac{n}{(n+1)^{3/2}}c_2 & \frac{n^{3/2}}{(n+1)^2}c_2 & 1 - c_1 - \frac{n^2}{(1+n)^2}c_2 \end{pmatrix}, \tag{2.1.21}$$

and then the size of them grows up with the general J_l given as a $(2l+1) \times (2l+1)$

matrix:

$$J_l = \begin{pmatrix} 1-\frac{l}{n+1}c_2 & \frac{\sqrt{l(n+1-l)}}{(n+1)^{3/2}}c_2 & -\frac{\sqrt{ln(n+1-l)}}{(n+1)^{3/2}}c_2 & \cdots & 0 \\ \frac{\sqrt{l(n+1-l)}}{(n+1)^{3/2}}c_2 & 1+\frac{l-nl-1}{(n+1)^2}c_2 & \frac{(n+2-2l)\sqrt{n}}{(n+1)^2}c_2 & \cdots & 0 \\ -\frac{\sqrt{ln(n+1-l)}}{(n+1)^{3/2}}c_2 & \frac{(n+2-2l)\sqrt{n}}{(n+1)^2}c_2 & 1-c_1+\frac{(l-1)n+1-l-n^2}{(n+1)^2}c_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1-c_1+\frac{ln-n-n^2}{(n+1)^2}c_2 \end{pmatrix}. \tag{2.1.22}$$

The matrices K_l, for $l = 1, 2, \cdots, n$, differ from the corresponding J_l only with the signs of some off-diagonal elements:

$$K_l = \begin{pmatrix} 1-\frac{l}{n+1}c_2 & \frac{\sqrt{l(n+1-l)}}{(n+1)^{3/2}}c_2 & \frac{\sqrt{ln(n+1-l)}}{(n+1)^{3/2}}c_2 & \cdots & 0 \\ \frac{\sqrt{l(n+1-l)}}{(n+1)^{3/2}}c_2 & 1+\frac{l-nl-1}{(n+1)^2}c_2 & -\frac{(n+2-2l)\sqrt{n}}{(n+1)^2}c_2 & \cdots & 0 \\ \frac{\sqrt{ln(n+1-l)}}{(n+1)^{3/2}}c_2 & -\frac{(n+2-2l)\sqrt{n}}{(n+1)^2}c_2 & 1-c_1+\frac{(l-1)n+1-l-n^2}{(n+1)^2}c_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1-c_1+\frac{ln-n-n^2}{(n+1)^2}c_2 \end{pmatrix}. \tag{2.1.23}$$

All these real symmetric matrices can be diagonalized by finding their eigenvalues. To guarantee the positivity of Π_0, we just need to let all its eigenvalues, which are real due to the symmetry in the above matrices, be non-negative. For any fixed n, we can analytically solve the eigenvalue problem of every J_l or K_l with Mathematica or Mathelab. Through the induction on n, we obtained the eigenvalues of J_l or K_l in

the diagonal of the following diagonalized matrices:

$$J_l' = \begin{pmatrix} \frac{2-c_1-c_2}{2} - \sqrt{\frac{c_1^2+c_2^2}{4} + \frac{(n^2-2n-1)c_1c_2}{2(n+1)^2}} & 0 & \cdots & 0 \\ 0 & \frac{2-c_1-c_2}{2} + \sqrt{\frac{c_1^2+c_2^2}{4} + \frac{(n^2-2n-1)c_1c_2}{2(n+1)^2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} .$$

$$= K_l' \qquad (2.1.24)$$

The constant eigenvalue 1 exists for all J_l's and K_l's, where $l = 0, 1, \cdots, n$. All the rest eigenvalues exist in couples, and the sum of each is $2 - c_1 - c_2$. After arranging the obtained couples in all J_l''s and K_l''s by the members with the minus sign before the square root in an ascending order, we see that the least couple, $1 - \frac{1}{2}c_1 - \frac{1}{2}c_2 \pm \sqrt{\frac{1}{4}c_1^2 + \frac{1}{4}c_2^2 + \frac{n^2-2n-1}{2(n+1)^2}c_1c_2}$, are the common eigenvalues of J_l and K_l for $l = 1, 2, \cdots, n$, and the second least, $1 - \frac{1}{2}c_1 - \frac{1}{2}c_2 \pm \sqrt{\frac{1}{4}c_1^2 + \frac{1}{4}c_2^2 + \frac{n^2-6n+1}{2(n+1)^2}c_1c_2}$, the common eigenvalues of J_l and K_l for $l = 2, 3, \cdots .n$, and so on. Therefore, if we require that the least common eigenvalue of all matrices except for J_0 and K_0, the eigenvalue of which is the constant 1, be non-negative, i.e.

$$1 - \frac{1}{2}c_1 - \frac{1}{2}c_2 - \sqrt{\frac{1}{4}c_1^2 + \frac{1}{4}c_2^2 + \frac{n^2-2n-1}{2(n+1)^2}c_1c_2} \geq 0 \ , \qquad (2.1.25)$$

the inconclusive operator Π_0 will be guaranteed to be positive.

Since $\langle\phi|\Pi_i|\phi\rangle \leq 1$ for $\forall|\phi\rangle \in H$ and all n, we have $c_i \leq 1$ for $i = 1, 2$ and a non-negative number $1 - \frac{1}{2}c_1 - \frac{1}{2}c_2$. Then, from the above inequality, we express c_2

in terms of c_1:

$$c_2 \leq \frac{1-c_1}{1-\frac{2n+1}{(n+1)^2}c_1} \ . \tag{2.1.26}$$

To achieve the maximum success probability, we choose the equal sign, i.e. let the least eigenvalue of Π_0 be 0. Inserting the resulting expression into Eq. (2.1.15) gives

$$\overline{P} = (\eta_1 c_1 + \eta_2 \frac{1-c_1}{1-\frac{2n+1}{(n+1)^2}c_1}) \frac{n}{2(n+1)}. \tag{2.1.27}$$

We can easily find $c_{1,opt}$ where the right-hand side of this expression is maximized and the corresponding $c_{2,opt}$:

$$\begin{aligned} c_{1,opt} &= \frac{(n+1)^2}{2n+1}(1-\frac{n}{n+1}\sqrt{\frac{1-\eta_1}{\eta_1}}), \\ c_{2,opt} &= \frac{(n+1)^2}{2n+1}(1-\frac{n}{n+1}\sqrt{\frac{\eta_1}{1-\eta_1}}). \end{aligned} \tag{2.1.28}$$

Substituting these optimum values into (2.1.27) gives the optimum result for POVM:

$$\overline{P}_{POVM}(n,\eta_1) = \frac{n}{4n+2}\left(n+1-2n\sqrt{\eta_1(1-\eta_1)}\right). \tag{2.1.29}$$

Then we have the following optimum POVM elements:

$$\begin{aligned} \Pi_{1,opt}(n,\eta_1) &= \frac{(n+1)^2}{2n+1}(1-\frac{n}{n+1}\sqrt{\frac{1-\eta_1}{\eta_1}})(I_{E,T}-P_{E,T})\otimes I_O \\ \Pi_{2,opt}(n,\eta_1) &= \frac{(n+1)^2}{2n+1}(1-\frac{n}{n+1}\sqrt{\frac{\eta_1}{1-\eta_1}})(I_{O,T}-P_{O,T})\otimes I_E \ . \end{aligned} \tag{2.1.30}$$

Here we have assumed that *a prior* probabilities of the inputs satisfy $\eta_1+\eta_2=1$, i.e. no failure in the preparation period.

2.2 Optimal measurement in different *a prior* probability ranges

This optimal POVM, however, holds valid only within the range of η_1 or η_2 where both $0 \leq c_{1,opt} \leq 1$ and $0 \leq c_{2,opt} \leq 1$ are satisfied simultaneously. From Eq. (2.1.26) we can find the range:

$$\frac{n^2}{n^2+(n+1)^2} \leq \eta_1, \eta_2 \leq \frac{(n+1)^2}{n^2+(n+1)^2} \ . \tag{2.2.1}$$

If $\eta_1 = \frac{(n+1)^2}{n^2+(n+1)^2}$ ($\eta_2 = \frac{n^2}{n^2+(n+1)^2}$), $\Pi_{1,opt} = (I_{E,T} - P_{E,T}) \otimes I_O$ and $\Pi_{2,opt} = 0$. The continuity to the outside of the POVM's validity domain requires this structure remain for $1 \geq \eta_1 \geq \frac{(n+1)^2}{n^2+(n+1)^2}$. In other words, when the preparation is dominated by the first input, the optimal measurement is realized by standard von Neumann measurement, which projects the input onto the compliment of the totally symmetric subspace with respect to all the even digits in the program and the data digit. Then, we get the success probability for each operator: $p_{1,opt} = \langle \Psi_1^{in} | (I_{E,T} - P_{E,T}) \otimes I_O | \Psi_1^{in} \rangle$ and $p_{2,opt} = 0$, indicating the second input is sacrificed completely. These results yield the average success probability,

$$\overline{P}_1(n, \eta_1) = \eta_1 \frac{n}{2(n+1)}, \tag{2.2.2}$$

for $\eta_1 \geq \frac{(n+1)^2}{n^2+(n+1)^2}$. Conversely, for $\eta_1 = \frac{n^2}{n^2+(n+1)^2}$ ($\eta_2 = \frac{(n+1)^2}{n^2+(n+1)^2}$), $\Pi_{2,opt} = (I_{O,T} - P_{O,T}) \otimes I_E$ and $\Pi_{1,opt} = 0$. Also from the continuity, we require this structure remain for $0 \leq \eta_1 \leq \frac{n^2}{n^2+(n+1)^2}$. This is a standard von Neumann measurement projecting the input onto the compliment of the totally symmetric subspace with respect to all

the odd digits in the program and the data digit. Since the first input is sacrificed completely in this case, we have

$$\overline{P}_2(n,\eta_1) = \eta_2 \frac{n}{2(n+1)} = (1-\eta_1)\frac{n}{2(n+1)}, \tag{2.2.3}$$

for $0 \leq \eta_1 \leq \frac{n^2}{n^2+(n+1)^2}$. The situation is fully symmetric in the *a priori* probabilities of inputs. In the intermediate range, where neither of the input states dominates, the POVM does the job of discrimination between them better than von Neumann measurement, while outside the range two full projectors do the work of identifying them at best. The optimal average success probability of the device working in the whole range of *a priori* probability, as the generalization of the result in [10], is summarized as follows:

$$\overline{P}^{opt}(n,\eta_1) = \begin{cases} \overline{P}_2(n,\eta_1) & 0 \leq \eta_1 < \frac{n^2}{n^2+(n+1)^2}, \\ \overline{P}_{POVM}(n,\eta_1) & \frac{n^2}{n^2+(n+1)^2} \leq \eta_1 \leq \frac{(n+1)^2}{n^2+(n+1)^2}, \\ \overline{P}_1(n,\eta_1) & \frac{(n+1)^2}{n^2+(n+1)^2} < \eta_1 \leq 1. \end{cases} \tag{2.2.4}$$

It is seen from the above results that the optimal success probability changes continuously at the boundaries of the respective regions of validity for the three measurements.

Some features should be noticed for this device: First, from Eq. (2.2.4), the validity range of the POVM measurement will become narrower and narrower with the increase of n, the number of copies used in the program. As n tends to infinity, this range will shrink to a point at $\eta_1 = \eta_2 = 0.5$. It means that the optimum measure-

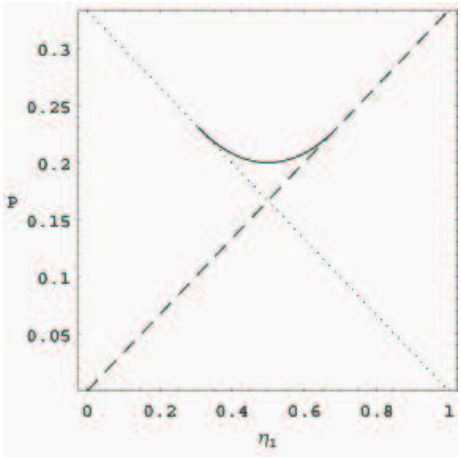

Figure 1: Optimal average success probability, P, vs. the *a priori* probability, η_1, for $n = 2$. Dashed line: P_1 from Eq. (2.2.2), dotted line: P_2 from Eq. (2.2.3), and solid curve: P_{POVM} from Eq. (2.1.29). The optimal P is given by P_2 for $\eta_1 < 4/13$, by P_{POVM} for $4/13 \leq \eta_1 \leq 9/13$ and by P_1 for $9/13 < \eta_1$. The lower bound if the optimal average success probability reaches 0.2.

ment will reduce to only von Neumann in this extreme. Second, if the preparation probability is fixed, the success probability of the device will increase with the number of copies of the states stored in the program. The larger size of the program yields more information about the unknown states. For example, at $\eta_1 = \eta_2 = 0.5$, where the identification of the input state is the hardest and the difference between the POVM and two full projectors is the largest, the average success probability, $\overline{P}_{POVM}(n) = n/(4n + 2)$, increases from 1/6 to 1/4 by 50% as n goes from 1 to

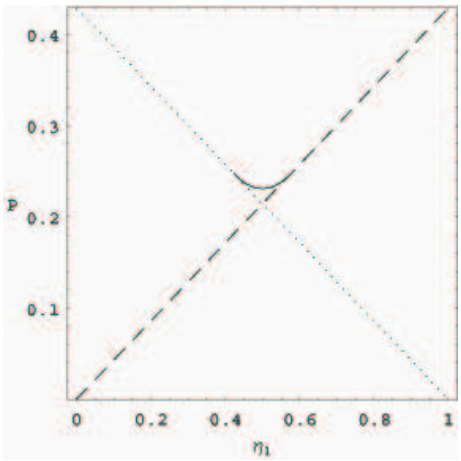

Figure 2: Optimal average success probability, P, vs. the *a priori* probability, η_1, for $n = 6$. The optimal P is given by P_2 (dotted line) for $\eta_1 < 36/85$, by P_{POVM} (solid curve) for $36/85 \leq \eta_1 \leq 49/85$ and by P_1 (dashed line) for $49/85 < \eta_1$. The lower bound if the optimal average success probability reaches 0.23.

infinity. We depict these features with Fig. 1-3 for three different n ($n = 2, 6$, and ∞).

Another interesting feature is that the optimal measurement operators and the validity domain depend only on the number of the states we put into the program and their preparation probabilities. Since they are independent of the information encoded in a specific pair of unknown qubits $|\psi_1\rangle$ and $|\psi_2\rangle$, the device performs universally. It can be programed with whatever couple of unknown qubits we want

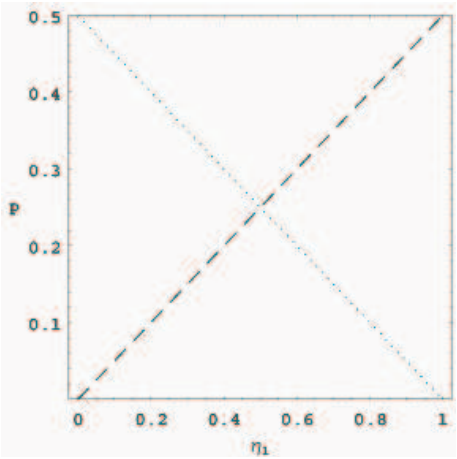

Figure 3: Optimal average success probability, P, vs. the *a priori* probability, η_1, for $n = \infty$. In this upper bound limit, the optimal scheme reduces to two full projector probabilities P_1 (dashed line) and P_2 (dotted line). The minimum value can reach 0.25.

to identify and discriminates between the produced registers with the best chance of success and no error.

So far we have worked out a scheme for a device that unambiguously discriminate between pairs of quantum registers produced with more than one copy of unknown qubits used in the program or reference digits. Its maximum average success probability increases with the number of the copies we store in the program, and also depends on the *a prior* probability of the states to be distinguished between. Given such an ideal device, we can tune its parameters, c_1 and c_2, according to the copy number n

and the *a prior* probability η_1 or η_2, so that it reaches the optimal performance for the required measurement.

2.3 Implementation of unknown state discrimination

In the optimal USD of nonorthogonal states, we need to use general positive operator-valued measures (POVMs) instead of orthogonal projectors, and their realization in the original signal Hilbert space of the measured system is usually impossible. Through Neumark's theorem [20], however, a POVM can be realized in the extended Hilbert spaces by performing unitary transformations and von Neumann projections together. The necessary unitary operators in the extended space can be constructed with the success probabilities, $p_i = Tr(\rho_i \Pi_k)\delta_{i,k}$, of the POVM elements Π_k and the corresponding inconclusive probabilities, $q_i = 1 - p_i$ [21]. However, for the USD of a set of unknown states, we don't have the information available to obtain these probabilities and, therefore, are unable to find such unitary transformations in this way.

Here we present a general method [22] to realize *any* POVM for USD only with its elements Π_k we have set up to unambiguously measure a particular set of pure or mixed inputs. The required unitary (orthogonal) transformations are found in an extended $2N$ dimensional Hilbert space if the dimension of the original signal Hilbert space is N.

We start the direct sum realization of USD with the observation that the inconclusive operator Π_0 is positive and Hermitian in any of an orthonormal basis $\{|e_i\rangle\}$, where $i = 1, 2, \cdots, N$, in our N dimensional Hilbert space H. Then we will find a unitary transformation U that transforms the general orthonormal basis $\{|e_i\rangle\}$ to a unique orthonormal basis $\{|\alpha_i\rangle\}$ (up to some permutation), where Π_0 is diagonalized:

$$U\Pi_0 U^\dagger = \sum_{i=1}^{N} c_i |\alpha_i\rangle\langle\alpha_i|. \tag{2.3.1}$$

Because Π_0 is a positive operator and $\langle\phi|\Pi_0|\phi\rangle \leq 1$ for any $|\phi\rangle$ in H, all its eigenvalues satisfy $0 \leq c_i \leq 1$. From this fact we obtain the following well-defined operators:

$$A_0 = A_0^\dagger = U^\dagger \left(\sum_{i=1}^{N} \sqrt{c_i} |\alpha_i\rangle\langle\alpha_i| \right) U, \tag{2.3.2}$$

and

$$(I - A_0^\dagger A_0)^{\frac{1}{2}} = U^\dagger \left(\sum_{i=1}^{N} \sqrt{1 - c_i} |\alpha_i\rangle\langle\alpha_i| \right) U, \tag{2.3.3}$$

if we represent them with the general orthonormal basis $\{|e_i\rangle\}$. With these operators we construct Σ and other three unitary, or more exactly orthogonal transformation, operators in the extended $2N$ dimensional space as follows:

$$\Sigma = \begin{pmatrix} (I - A_0^\dagger A_0)^{\frac{1}{2}} & -A_0 \\ A_0 & (I - A_0^\dagger A_0)^{\frac{1}{2}} \end{pmatrix}. \tag{2.3.4}$$

The other three such operators are obtained by putting the minus sign in the upper right sub-matrix of Σ to the other three sub-matrix blocks, respectively. It is straightforward to prove $\Sigma^\dagger\Sigma = \Sigma\Sigma^\dagger = I$ with the operators defined in Eq. (2.3.2) and Eq.

(2.3.3). In the most general situation when we have n inputs to be unambiguously discriminated among themselves, $I - A_0^\dagger A_0$ in the square root equals $\Sigma_{i\in I}\Pi_i$, where $I = \{1, 2, \cdots, n\}$.

We take Σ to act on a set of states $\{\rho_i\}$ $(i = 1, 2, \cdots, n)$, which are to be distinguished between each other in a USD process, in the extended $2N$ dimensional Hilbert space:

$$\Sigma \begin{pmatrix} \rho_i & \\ & o \end{pmatrix} \Sigma^\dagger = \begin{pmatrix} (I - A_0^\dagger A_0)^{\frac{1}{2}} \rho_i (I - A_0^\dagger A_0)^{\frac{1}{2}} & (I - A_0^\dagger A_0)^{\frac{1}{2}} \rho_i A_0^\dagger \\ A_0 \rho_i (I - A_0^\dagger A_0)^{\frac{1}{2}} & A_0 \rho_i A_0^\dagger \end{pmatrix}, \quad (2.3.5)$$

where the blank blocks and the o sub-matrix represent the parts with all the entries 0. The trace of the upper left diagonal block gives the success probability p_i of unambiguously determining ρ_i because $Tr(\rho_i \Pi_j) = p_i \delta_{i,j}$ for the Π_i's, and the trace of the lower right diagonal block gives the failure probability q_i in the ancilla space A, and in the whole extended space $K = H \oplus A$ we have $p_i + q_i = Tr\rho_i = 1$.

If $\{\rho_i\}$ is a set of linearly independent pure states $\{|\psi_i\rangle\}$, we will prove that the parts of their outputs after the action of Σ are mutually orthogonal in the original signal Hilbert space H. Before the transformation, they are extended to the inputs $|\psi_i^{in}\rangle = (|\psi_i\rangle, \mathbf{0})^T$, where $(\mathbf{0})$ represents a N-tuple of zero's, $(0, 0, \cdots, 0)$, in A. The

output states are obtained as follows:

$$
\begin{aligned}
|\psi_i^{out}\rangle &= \begin{pmatrix} (I - A_0^\dagger A_0)^{\frac{1}{2}} & -A_0 \\ A_0 & (I - A_0^\dagger A_0)^{\frac{1}{2}} \end{pmatrix} \begin{pmatrix} |\psi_i\rangle \\ \mathbf{0} \end{pmatrix} \\
&= \begin{pmatrix} (I - A_0^\dagger A_0)^{\frac{1}{2}} |\psi_i\rangle \\ A_0 |\psi_i\rangle \end{pmatrix}. \qquad (2.3.6)
\end{aligned}
$$

Then the inner product of the outputs for any pair of different $|\psi_i\rangle$ and $|\psi_j\rangle$ in H is

$$
\langle\psi_j|(I - A_0^\dagger A_0)^{\frac{1}{2}}(I - A_0^\dagger A_0)^{\frac{1}{2}}|\psi_i\rangle = \langle\psi_j| \sum_{k=1}^{n} A_k^\dagger A_k |\psi_i\rangle = 0, \qquad (2.3.7)
$$

and in A is

$$
\langle\psi_j|A_0^\dagger A_0|\psi_i\rangle = \langle\psi_j|\psi_i\rangle. \qquad (2.3.8)
$$

For the mixed states we act Σ on the products $\rho_i\rho_j$ $(i \neq j)$ in the same way as in Eq. (2.3.5), and find that the trace of the outputs in H vanishes while in A is the same as those of the inputs $\rho_i\rho_j$. Therefore, the unitary (orthogonal) transformation Σ in the extended $2N$ dimensional Hilbert space realizes a scheme to unambiguously discriminate any set of quantum states $\{\rho_i\}$.

Chapter III

3 Unknown state discrimination—approach with dephasing

3.1 Introduction

The most general problem of discriminating a pair of unknown states $|\psi_1\rangle$ and $|\psi_2\rangle$ is formulated as discriminating the inputs prepared with n_A copies of the state of the program system A, n_C copies of the state of the program system C, and n_B copies of the state of the data system B:

$$\begin{aligned} |\Psi_1^{in}\rangle &= |\psi_1\rangle_A^{\otimes n_A}|\psi_1\rangle_B^{\otimes n_B}|\psi_2\rangle_C^{\otimes n_C} \ , \\ |\Psi_2^{in}\rangle &= |\psi_1\rangle_A^{\otimes n_A}|\psi_2\rangle_B^{\otimes n_B}|\psi_2\rangle_C^{\otimes n_C} \ . \end{aligned} \tag{3.1.1}$$

We should optimally distinguish between these inputs, keeping in mind that one has no knowledge of $|\psi_1\rangle$ and $|\psi_2\rangle$ beyond their *a priori* probabilities. In this chapter we will apply a dephasing approach to study the efficiency of discriminating the inputs prepared with $n_A = n_C = n$ and $n_B = m$. As in the related works [23, 24, 25], we assume that the unknown qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ uniformly and independently distribute over the Bloch spheres, so it is convenient to obtain the averaged or dephased inputs in Eq. (3.1.1). The efficiency in the discrimination of these averaged or dephased inputs indicates how well two unknown states can be discriminated.

Here we demonstrate that the discrimination of the average or dephased inputs in Eq. (3.1.1) is equivalent to that of two uniformly distributed mixed states. For the uniformly distributed unknown qubits $|\psi_1\rangle$, $|\psi_2\rangle$, the averages of the inputs for $n_A = n_C = n$ and $n_B = m$ are given in terms of the basis in Eq. (2.1.6) as follows:

$$\begin{aligned}
\rho_1 &= \frac{1}{(4\pi)^2}\int d\psi_1 \int d\psi_2 |\Psi_1^{in}\rangle\langle\Psi_1^{in}| \\
&= \left(\frac{1}{n+m+1}\sum_{i=0}^{n+m} |e_i\rangle_{A,B\ A,B}\langle e_i|\right) \otimes \left(\frac{1}{n+1}\sum_{j=0}^{n} |e_j\rangle_{C\ C}\langle e_j|\right), \\
&= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} |v_i\rangle\langle v_i| \\
\rho_2 &= \frac{1}{(4\pi)^2}\int d\psi_1 \int d\psi_2 |\Psi_2^{in}\rangle\langle\Psi_2^{in}| \\
&= \left(\frac{1}{n+1}\sum_{i=0}^{n} |e_i\rangle_{A\ A}\langle e_i|\right) \otimes \left(\frac{1}{n+m+1}\sum_{j=0}^{n+m} |e_j\rangle_{B,C\ B,C}\langle e_j|\right) \\
&= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} |v_i'\rangle\langle v_i'|, \qquad (3.1.2)
\end{aligned}$$

where $|v_i\rangle \equiv |e_j\rangle_{A,B} \otimes |e_k\rangle_C$ and $|v_i'\rangle \equiv |e_j\rangle_A \otimes |e_k\rangle_{B,C}$, and we have also used the integral:

$$2\int_0^{\frac{\pi}{2}} sin^{2m-1}x\ cos^{2n-1}x\ dx = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}. \qquad (3.1.3)$$

In taking this average, we actually realize the one-to-one maps from the *unknown* qubit ensembles $\{|\psi_1\rangle\}$, $\{|\psi_2\rangle\}$ (the wave barckets means a set) to two *known* mixed states:

$$\begin{aligned}
\{|\psi_1\rangle\} &\longmapsto \rho_1 \\
\{|\psi_2\rangle\} &\longmapsto \rho_2, \qquad (3.1.4)
\end{aligned}$$

for our identification procedure. Generally these mixed states are produced from the unknown qubit ensembles with some different *a prior* probabilities η and $1-\eta$, respectively, if we suppose there is no failure in the preparation period.

Two uniformly distributed mixed states can be discriminated as two sub-spaces by Jordan basis method [27] and, in our problem, all the inner products of the Jordan basis vectors in the supports of these mixed states are derived by finding an inherent symmetry which exists only under the condition $n_A = n_C$. In the limit of very large numbers of both the program and the data copies, we show that discrimination the unknown states can be certainly realized for all *a priori* probabilities. The original results of the study are given in [26].

3.2 Structure of average inputs

The problem to distinguish between two unknown states is transformed to that of discriminating the mixed states ρ_1 and ρ_2 prepared with the probabilities η and $1-\eta$, respectively. Then we can apply the Jordan basis method [27] to derive the optimal schemes for it.

Let H_1 be the Hilbert space generated by the support of ρ_1 and H_2 the Hilbert space generated by the support of ρ_2, respectively. We here study the structure of these spaces. We use the symbol (n, m, n) to represent how many copies of program digits and how many data digits used in $|\Psi_1^{in}\rangle$ and $|\Psi_2^{in}\rangle$, e.g. (1,1,1) means 1 copy of

program and 1 copy of data, and (n,1,n) n copies program and 1 copy data. Counting the number of the basis $|e_i\rangle$ in the respective parts, we get $dimH_i = (n+m+1)(n+1)$ $(i = 1, 2)$ in the general (n, m, n) case. Moreover, we have $dimH_1 \cap H_2 = 2n + m + 1$, and the dimension of the total Hilbert space H is therefore

$$dimH = dimH_1 \cup H_2 = dimH_1 + dimH_2 - dimH_1 \cap H_2 = 2n^2 + 2nm + 2n + m + 1.$$

For a particular $|v_i\rangle$ in H_1, we need to find out with which members of $\{|v'_j\rangle\}$ spanning H_2 it has non-zero overlaps , i.e. to find out all $|v'_j\rangle$'s such that $\langle v_i|v'_j\rangle \neq 0$. To do it, we first split $|e_j\rangle_{A,B}$ in $|v_i\rangle$ and $|e_k\rangle_{B,C}$ in $|v'_i\rangle$ into the summation of a series tensor-products by parts as follows:

$$\begin{aligned} |e_k\rangle_{A,B} &= \sqrt{\frac{C_n^i C_m^j}{C_{n+m}^k}}|e_i\rangle_A|e_j\rangle_B + \sqrt{\frac{C_n^{i+1} C_m^{j-1}}{C_{n+m}^k}}|e_{i+1}\rangle_A|e_{j-1}\rangle_B + \cdots \\ &+ \sqrt{\frac{C_n^{i+l} C_m^{j-l}}{C_{n+m}^k}}|e_{i+l}\rangle_A|e_{j-l}\rangle_B, \end{aligned} \tag{3.2.1}$$

where $i + j = k$, and l is determined by how many combinations of two non-negative integers summed up to be k. The derivation of this formula and its usage are given in the appendix A.

Next, we use $[n_1, n_2, n_3]$ symbol defined as follows to classify the mutually overlapped subspaces of H_1 and H_2. With the help of the above formula, we find that any basis vector $|v_p\rangle$ in H_1 or $|v'_p\rangle$ in H_2 has a unique representation in terms of this

symbol:

$$
\begin{aligned}
|v_p\rangle &= \sqrt{\frac{C_n^i C_m^j}{C_{n+m}^{i+j}}}|e_i\rangle_A|e_j\rangle_B|e_k\rangle_C + \sqrt{\frac{C_n^{i+1}C_m^{j-1}}{C_{n+m}^{i+j}}}|e_{i+1}\rangle_A|e_{j-1}\rangle_B|e_k\rangle_C \\
&\quad + \cdots + \sqrt{\frac{C_n^{i+l}C_m^{j-l}}{C_{n+m}^{i+j}}}|e_{i+l}\rangle_A|e_{j-l}\rangle_B|e_k\rangle_C \\
&\equiv [i,j,k] + [i+1,j-1,k] + \cdots + [i+l,j-l,k], \qquad (3.2.2)
\end{aligned}
$$

$$
\begin{aligned}
|v'_p\rangle &= \sqrt{\frac{C_n^i C_m^j}{C_{n+m}^{i+j}}}|e_k\rangle_A|e_i\rangle_B|e_j\rangle_C + \sqrt{\frac{C_n^{i+1}C_m^{j-1}}{C_{n+m}^{i+j}}}|e_k\rangle_A|e_{i+1}\rangle_B|e_{j-1}\rangle_C \\
&\quad + \cdots + \sqrt{\frac{C_n^{i+l}C_m^{j-l}}{C_{n+m}^{i+j}}}|e_k\rangle_A|e_{i+l}\rangle_B|e_{j-l}\rangle_C \\
&\equiv [k,i,j] + [k,i+1,j-1] + \cdots + [k,i+l,j-l], \qquad (3.2.3)
\end{aligned}
$$

where the combinatorics number coefficients before the vectors have been absorbed into the square brackets. Obviously, we see from this expression that any couple of $|v_p\rangle$ and $|v'_p\rangle$ satisfy $\langle v'_p|v_p\rangle \neq 0$ only if they have a common $[n_1, n_2, n_3]$ term.

In the above $[n_1, n_2, n_3]$ representation of $|v_p\rangle$ or $|v'_p\rangle$, each term has the same total number, $N \equiv n_1 + n_2 + n_3$, in the square brackets, which goes from 0 to $2n + m$. We'll show that each distinct N corresponds to two closed chains of basis vectors in H_1 and H_2, the elements of which may have non-zero mutual overlaps.

Let's first look at $N = 0$ and $N = 2n + m$, the two simplest cases. $[0, 0, 0] = |0, 0, \cdots, 0\rangle$ and $[n, m, n] = |1, 1, \cdots, 1\rangle$ are shared by H_1 and H_2, and their overlaps are just $\langle v'|v\rangle = 1$. They are two initial closed chains of basis with only one element.

When $N = 1$, let's pick out one basis, $[0, 1, 0] + [1, 0, 0]$, in H_1 (in $[n_1, n_2, n_3]$

representation all the terms of a basis in H_1 have the same last digit n_3), and then one of the basis in H_2, which is overlapped with it, is $[0,1,0]+[0,0,1]$ (the first digit n_1 are the same in $[n_1,n_2,n_3]$ representation). The only other basis vector in H_1, with which $[0,1,0]+[0,0,1]$ of H_2 also has overlap, is $[0,0,1]$, while $[0,1,0]+[1,0,0]$ in H_1 is also overlapped with $[1,0,0]$ in H_2. Thus we exhausted all basis in H_1 and H_2 with $N=1$ and obtain such two closed chains of basis in these two spaces:

$$\begin{aligned} |v_1\rangle &= [0,1,0]+[1,0,0], \\ |v_2\rangle &= [0,0,1]; \end{aligned} \tag{3.2.4}$$

$$\begin{aligned} |v_1'\rangle &= [0,1,0]+[0,0,1], \\ |v_2'\rangle &= [1,0,0]. \end{aligned} \tag{3.2.5}$$

These two closed chains have 2 elements and, by retriving the coefficients absorbed in the square brackets, we can easily find their overlaps:

$$\begin{aligned} \langle v_1'|v_1\rangle &= \frac{C_m^1}{C_{n+m}^1}, \\ \langle v_1'|v_2\rangle &= \langle v_1|v_2'\rangle = \sqrt{\frac{C_n^1}{C_{n+m}^1}}. \end{aligned} \tag{3.2.6}$$

For $N=2n+m-1$, we find in the same way the following two closed chains:

$$\begin{aligned} |v_1\rangle &= [n,m-1,n]+[n-1,m,n], \\ |v_2\rangle &= [n,m,n-1]; \end{aligned} \tag{3.2.7}$$

$$
\begin{aligned}
|v_1'\rangle &= [n, m-1, n] + [n, m, n-1], \\
|v_2'\rangle &= [n-1, m, n]; \qquad (3.2.8)
\end{aligned}
$$

and, with the combinatorics identities, we find that they have the same overlaps as in $N = 1$ case, so we call them the conjugate chains of $N = 1$.

As N increases to any $i \leq n$, the closed chains of basis vectors can be found inductively in the above way:

$$
\begin{aligned}
|v_1\rangle &= [0, i, 0] + [1, i-1, 0] + [2, i-2, 0] + \cdots + [i, 0, 0], \\
|v_2\rangle &= [0, i-1, 1] + [1, i-2, 1] + \cdots + [i-1, 0, 1], \\
|v_3\rangle &= [0, i-2, 2] + \cdots + [i-2, 0, 2] \\
&\cdots \\
|v_{i+1}\rangle &= [0, 0, i]; \qquad (3.2.9)
\end{aligned}
$$

$$
\begin{aligned}
|v_1'\rangle &= [0, i, 0] + [0, i-1, 1] + [0, i-2, 2] + \cdots + [0, 0, i], \\
|v_2'\rangle &= [1, i-1, 0] + [1, i-2, 1] + \cdots + [1, 0, 1-1], \\
|v_3'\rangle &= [2, i-2, 0] + \cdots + [2, 0, i-2] \\
&\cdots \\
|v_{i+1}'\rangle &= [i, 0, 0]. \qquad (3.2.10)
\end{aligned}
$$

For every $|v_j\rangle$ $(j \leq i+1)$ in a chain of H_1, the last index $n_3 = j-1$ increases as j from 0 to i, while for every $|v_j'\rangle$ a $(j \leq i+1)$ in a chain of H_2, the first index $n_1 = j-1$

increases as j from 0 to i. The number of different terms in a $|v_j\rangle$ (resp. $|v'_j\rangle$) is how many ways the non-negative integers n_1 and n_2 (resp. n_2 and n_3) can be added up to $i-j+1$, so it goes down from $i+1$ to 1 as j increases.

The $N = 2n+m-i$ case just has two chains conjugate to those of $N = i$: the last index n_3 of $|v_j\rangle$ decreases from n to $n-i$ as j goes up, while the first index n_1 of $|v'_j\rangle$ also decreases from n to $n-i$ as j goes up. The number of different terms in a $|v_j\rangle$ (resp. $|v'_j\rangle$) is how many ways the non-negative integers n_1 and n_2 (resp. n_2 and n_3) can be added up to $n+m-i+j-1$.

As we see from the closed chains with mutual overlaps, whenever N increases its values by 1, the number of the elements in closed chains will increase by 1, if $0 \leq N \leq n-1$. On the other hand, the number of the elements in closed chains increases by 1 as N decreases by 1, if $n+m+1 \leq N \leq 2n+m$. However, the last index n_3 of the $|v_i\rangle$ in H_1 (and the first index n_1 of the $|v'_i\rangle$ in H_2) cannot increase beyond n or decrease beyond 0 and, therefore, in a closed chain the number of its elements cannot be larger than $n+1$.

Thus the number of elments in a closed chain increases in two directions from $N = 0$ and $N = 2n+m$ and, as N increases to the medium values $n-1$ or decreases to the medium value $n+m+1$, the size of a closed chain will be fixed with $n+1$ elements. The number of these chains with $n+1$ elements in H_1 and H_2 is $m+1$.

Therefore, the total number of the elements in closed chains in H_1 or H_2 equals

$$2 \times \frac{n(n+1)}{2} + (m+1)(n+1) = (n+m+1)(n+1),$$

the dimension of the Hilbert space H_1 or H_2.

After we obtain all closed chains with mutual overlaps this way, we check by induction that the $\{|v_i\rangle\}$ in H_1 and $\{|v_i'\rangle\}$ in H_2 can be permutated such that they have symmetric overlaps: $\langle v_i'|v_j\rangle = \langle v_i|v_j'\rangle$, for each couple of $i \neq j$ (see Appendix B). We here call it a *mirror symmetry* (the prime sign over the shoulders of v's is reflected by the perpendicular bar at the center of the inner product like a mirror), and it is very useful in finding the Jordan basis products in each closed chain.

3.3 Jordan basis for average input state spaces

As it has been proved for any couple of sub-spaces [27], we can find the Jordan basis $\{|\phi_i\rangle\}$ in H_1 and $\{|\phi_i'\rangle\}$ in H_2 such that

$$\begin{aligned} \rho_1 &= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} |\phi_i\rangle\langle\phi_i| \\ \rho_2 &= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} |\phi_i'\rangle\langle\phi_i'|, \end{aligned} \tag{3.3.1}$$

with $\langle\phi_i|\phi'_j\rangle = 0$ for each couple of $i \neq j$. It is to determine the orthogonal transformations:

$$\begin{aligned}
|\phi_1\rangle &= a_{11}|v_1\rangle + a_{12}|v_2\rangle + a_{13}|v_3\rangle + \cdots + a_{1n}|v_n\rangle \\
|\phi_2\rangle &= a_{21}|v_1\rangle + a_{22}|v_2\rangle + a_{23}|v_3\rangle + \cdots + a_{2n}|v_n\rangle \\
|\phi_3\rangle &= a_{31}|v_1\rangle + a_{32}|v_2\rangle + a_{33}|v_3\rangle + \cdots + a_{3n}|v_n\rangle \\
&\cdots \\
|\phi_n\rangle &= a_{n1}|v_1\rangle + a_{n2}|v_2\rangle + a_{n3}|v_3\rangle + \cdots + a_{nn}|v_n\rangle
\end{aligned} \tag{3.3.2}$$

for all closed basis chains in H_1 and the corresponding orthogonal transforms

$$\begin{aligned}
|\phi'_1\rangle &= a'_{11}|v'_1\rangle + a'_{12}|v'_2\rangle + a'_{13}|v'_3\rangle + \cdots + a'_{1n}|v'_n\rangle \\
|\phi'_2\rangle &= a'_{21}|v'_1\rangle + a'_{22}|v'_2\rangle + a'_{23}|v'_3\rangle + \cdots + a'_{2n}|v'_n\rangle \\
|\phi'_3\rangle &= a'_{31}|v'_1\rangle + a'_{32}|v'_2\rangle + a'_{33}|v'_3\rangle + \cdots + a'_{3n}|v'_n\rangle \\
&\cdots \\
|\phi'_n\rangle &= a'_{n1}|v'_1\rangle + a'_{n2}|v'_2\rangle + a'_{n3}|v'_3\rangle + \cdots + a'_{nn}|v'_n\rangle
\end{aligned} \tag{3.3.3}$$

for all chains in H_2.

Let's first look at the original basis of these two Hilbert spaces. If we permuatate the basis vectors properly, we will obatin the ordered vectors with the *mirror symmetry* $\langle v_i|v'_j\rangle = \langle v'_i|v_j\rangle$ for any couple of i, j ($i = j$ or $i \neq j$) in a closed chain (more explanation is given in appendix B).

By the inverse orthogonal transformations, we can write $|v_i\rangle = \sum_k a_{ki}|\phi_k\rangle$, etc, and the *mirror symmetry* implies

$$\sum_k a_{ki}a'_{kj}\langle\phi_k|\phi'_k\rangle = \sum_k a'_{ki}a_{kj}\langle\phi'_k|\phi_k\rangle, \tag{3.3.4}$$

so we can choose $a_{ij} = a'_{ij}$ for all i and j, i.e. the orthogonal transformations from the original to Jordan basis in two Hilbert spaces will be the same.

Then we go further to find the transformations toward Jordan basis for all closed chains of the original basis. Since what are useful to the discrimination of the mixed states are *only* the inner products, $\langle\phi_k|\phi'_k\rangle$, of these Jordan basis, we will just derive these inner products instead of the exact forms of Jordan basis.

For $N = 1$ and $N = 2n + m$ the Jordan basis are just the original ones, and the inner product is obviously $\langle\phi_1|\phi'_1\rangle = 1$ (they belong to the intersection of two spaces).

In $N = 1$ (similarly in $N = 2n+m-1$) case, we first list the original basis arranged in the order of mirror symmetry:

$$\begin{aligned} |v_1\rangle &= [0,1,0] + [1,0,0], \\ |v_2\rangle &= [0,0,1]; \end{aligned} \tag{3.3.5}$$

$$\begin{aligned} |v'_1\rangle &= [0,1,0] + [0,0,1], \\ |v'_2\rangle &= [1,0,0]. \end{aligned} \tag{3.3.6}$$

For simplicity we use the notations $s \equiv \sin\theta$, $c \equiv \cos\theta$ and $t \equiv \tan\theta$. An orthogonal

transformation $T_{1,2}$,

$$\begin{pmatrix} |\phi_1\rangle \\ |\phi_2\rangle \end{pmatrix} = T_{1,2} \begin{pmatrix} |v_1\rangle \\ |v_2\rangle \end{pmatrix} = \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \begin{pmatrix} |v_1\rangle \\ |v_2\rangle \end{pmatrix},$$
$$\begin{pmatrix} |\phi_1'\rangle \\ |\phi_2'\rangle \end{pmatrix} = T_{1,2} \begin{pmatrix} |v_1'\rangle \\ |v_2'\rangle \end{pmatrix} = \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \begin{pmatrix} |v_1'\rangle \\ |v_2'\rangle \end{pmatrix}, \tag{3.3.7}$$

suffices to obtain $\{|\phi_1\rangle, |\phi_2\rangle\}$ and $\{|\phi_1'\rangle, |\phi_2'\rangle\}$ such that

$$\langle\phi_1|\phi_2'\rangle = \langle\phi_1'|\phi_2\rangle = -\langle v_1|v_1'\rangle sc + \langle v_1|v_2'\rangle c^2 - \langle v_1|v_2'\rangle s^2 = 0 \tag{3.3.8}$$

Using the trigonometry identities:

$$\sin 2\theta = \frac{2\tan\theta}{1+\tan^2\theta},$$
$$\cos 2\theta = \frac{1-\tan^2\theta}{1+\tan^2\theta},$$

we reduce the last equation to

$$-\langle v_1|v_1'\rangle t + \langle v_1|v_2'\rangle(1-t^2) = 0, \tag{3.3.9}$$

a quadratic equation that can be solved easily. Substituting t and $\langle v_1|v_1'\rangle$, $\langle v_1|v_2'\rangle$ into the following inner products of Jordan basis, we obtain

$$\begin{aligned} \langle\phi_1|\phi_1'\rangle &= \langle v_1|v_1'\rangle\frac{1}{1+t^2} + \langle v_1|v_2'\rangle\frac{2t}{1+t^2} = 1, \\ \langle\phi_2|\phi_2'\rangle &= \langle v_1|v_1'\rangle\frac{t^2}{1+t^2} - \langle v_1|v_2'\rangle\frac{2t}{1+t^2} = -\frac{n}{n+m}. \end{aligned} \tag{3.3.10}$$

Here we select out one of the solutions with $|\langle\phi_i|\phi_i'\rangle|$ in a descending order (the other solution is just the permutation of the above results).

The $N = 2$ Jordan basis inner products are obtained by first applying $T = T_{1,3}T_{2,3}$ (a 3×3 matrix) to seperate one couple of basis in the chains from others, and then using $T_{1,2}$ to seperate the remaining couples. The rotation $T_{i,j}$ in the space of a chain is defined as an $n \times n$ (n is the number of chain elements) identity matrix with the elements in the positions $\{i,i\}$, $\{i,j\}$, $\{j,i\}$ and $\{j,j\}$ replaced by the corresponding elements of an $O(2)$ matrix. Following the procedure we obtain the solution with $|\langle\phi_i|\phi'_i\rangle|$ in a descending order as follows:

$$\begin{aligned} \langle\phi_1|\phi'_1\rangle &= 1, \\ \langle\phi_2|\phi'_2\rangle &= -\frac{n}{n+m}, \\ \langle\phi_3|\phi'_3\rangle &= \frac{n(n-1)}{(n+m)(n+m-1)}. \end{aligned} \tag{3.3.11}$$

The first two values also exist in $N = 1$ case, so the recurrence of these inner product values leads to the multiplicities of them in the whole Hilbert space.

In the cases of still larger N we apply successive orthogonal transformations, $T_1 = T_{1,N}T_{2,N}\cdots T_{N-2,N}T_{N-1,N}$, $T_2 = T_{1,N-1}T_{2,N-1}\cdots T_{N-2,N-1}$, $\cdots$, to seperate the basis and then obtain all Jordan basis inner products. By induction on N, we find that, as N grows, some inner product values repeat from chain to chain in the same way as N goes from 1 to 2.

For each closed chain of the original basis, which has been arranged by permutation such that they satisfy the *mirror symmetry* $\langle v_i|v'_j\rangle = \langle v'_i|v_j\rangle$, we can prove the

existence following invariant (see appendix B):

$$\sum_i \langle v_i | v_i' \rangle = \sum_i \langle \phi_i | \phi_i' \rangle. \tag{3.3.12}$$

Moreover, we also show that this invariant sum is *only* determined by how many elements in a closed chain. With the recurrence of the Jordan basis inner products, this invariant allows us to easily obtain their values for all N.

Finally, we list all inner products of Jordan basis and their multiplicities in the following table.

inner product	multiplicity
1	2n+m+1
$-\frac{n}{n+m}$	$2n+m-1$
$\frac{n(n-1)}{(n+m)(n+m-1)}$	$2n+m-3$
$-\frac{n(n-1)(n-2)}{(n+m)(n+m-1)(n+m-2)}$	$2n+m-5$
$\vdots$	$\vdots$
$\pm\frac{n(n-1)\cdots 1}{(n+m)(n+m-1)\cdots(m+1)}$	$m+1$

The last inner product's sign is determined by whether n is even or odd integer. The inner products $\langle \phi | \phi' \rangle = 1$ correspond to the intersection subspace of H_1 and H_2, and we also see that each closed chain in H_1 has a one-dimensional joint space with the corresponding chain in H_2.

3.4 Unambiguous discrimination of average inputs of unknown qubits

For two uniformly distributed mixed states represented by the Jordan basis,

$$\begin{aligned} \rho_1 &= \sum_i \alpha_i |\phi_i\rangle\langle\phi_i| \\ \rho_2 &= \sum_i \beta_i |\phi_i'\rangle\langle\phi_i'|, \end{aligned} \tag{3.4.1}$$

the optimum POVM to unambiguously discriminate them can achieve the success probability of

$$P(\eta) = 1 - 2\sqrt{\eta(1-\eta)} \sum_i \sqrt{\alpha_i \beta_i} |\langle\phi_i|\phi_i'\rangle|, \tag{3.4.2}$$

if the Hilbert spaces generated by their supports only join at the origin. In our problem, however, there is a non-trivial intersection space of the Hilbert spaces H_1 and H_2, so this intersection contribute to failure and the summation of the absolute of Jordan basis inner products only includes those satisfying $0 < \langle\phi_i'|\phi_i\rangle < 1$.

In the general (n, m, n) case, the success probabilities is therefore given by

$$\begin{aligned} P(\eta) &= 1 - \frac{2n+m+1}{(n+m+1)(n+1)} - 2\sqrt{\eta(1-\eta)} \frac{1}{(n+m+1)(n+1)} \\ &\quad \times \{ \frac{n(2n+m-1)}{n+m} + \frac{n(n-1)(2n+m-3)}{(n+m)(n+m-1)} + \frac{n(n-1)(n-2)(2n+m-5)}{(n+m)(n+m-1)(n+m-2)} \\ &\quad + \cdots + \frac{n(n-1)\cdots 1}{(n+m)(n+m-1)\cdots(m+2)} \}. \end{aligned} \tag{3.4.3}$$

We have

$$\begin{aligned} P(\eta) &< 1-\frac{2n+m+1}{(n+m+1)(n+1)}-2\sqrt{\eta(1-\eta)}\frac{m+1}{(n+m+1)(n+1)} \\ &\times\{\frac{n}{n+m}+\frac{n(n-1)}{(n+m)(n+m-1)}+\frac{n(n-1)(n-2)}{(n+m)(n+m-1)(n+m-2)} \\ &+\cdots+\frac{n(n-1)\cdots 1}{(n+m)(n+m-1)\cdots(m+1)}\}, \end{aligned} \tag{3.4.4}$$

and

$$\begin{aligned} P(\eta) &> 1-\frac{2n+m+1}{(n+m+1)(n+1)}-2\sqrt{\eta(1-\eta)}\frac{2n+m-1}{(n+m+1)(n+1)} \\ &\times\{\frac{n}{n+m}+\frac{n(n-1)}{(n+m)(n+m-1)}+\frac{n(n-1)(n-2)}{(n+m)(n+m-1)(n+m-2)} \\ &+\cdots+\frac{n(n-1)\cdots 1}{(n+m)(n+m-1)\cdots(m+1)}\}, \end{aligned} \tag{3.4.5}$$

Therefore, within the validity range of the optimal POVM, $\frac{n^2}{(n+m)^2+n^2} \leq \eta \leq \frac{(n+m)^2}{(n+m)^2+n^2}$, $P(\eta)$ will tend to a certain 1 as both n and m tend to infinity, since the summation inside the wave bracket in these inequalities is a typical convergent series.

We here give some examples when $P(\eta)$ can be reduced to closed forms:

If $(n,m,n)=(1,n,1)$, one copy program and n copies data,

$$P(\eta)=1-\frac{n+3}{2(n+2)}-\frac{1}{n+2}\sqrt{\eta(1-\eta)}; \tag{3.4.6}$$

If $(n,m,n)=(2,n,2)$,

$$P(\eta)=1-\frac{n+5}{3(n+3)}-(\frac{2}{3}\times\frac{1}{(n+2)}+\frac{2}{3}\times\frac{1}{(n+2)(n+3)})\times 2\sqrt{\eta(1-\eta)}; \tag{3.4.7}$$

If $(n, m, n) = (n, 1, n)$, n copies program and 1 copy data,

$$\begin{aligned} P(\eta) &= 1 - \frac{2}{n+2} - \frac{2}{(n+1)(n+2)} \times 2\sqrt{\eta(1-\eta)} \\ &\quad \times \frac{1}{n+1}(n^2 + (n-1)^2 + \cdots + 2^2 + 1^2) \\ &= 1 - \frac{2}{n+2} - \frac{1}{3} \times \frac{n(2n+1)}{(n+1)(n+2)} \times 2\sqrt{\eta(1-\eta)}. \end{aligned} \tag{3.4.8}$$

When $\eta = 0.5$ and n goes to infinity, it will tend to $1/3$. This result is equal to the optimum IDP average in discriminating $|\psi_1\rangle$ and $|\psi_2\rangle$ if they are known to us, but the difference here is that η indicates how probable one of the uniformly distributed mixed states can be produced from the unknown qubit ensembles $\{|\psi_1\rangle\}$ and $\{|\psi_2\rangle\}$.

3.5 Minimum-error discrimination of average inputs of unknown qubits

To find the measurement operators Π_1 and Π_2 ($\Pi_1 + \Pi_2 = I$) performing with the minimum error probability,

$$P_E = \eta_1 Tr(\rho_1 \Pi_2) + \eta_2 Tr(\rho_2 \Pi_1), \tag{3.5.1}$$

in discriminating two mixed states ρ_1 and ρ_2, Helstrom gave a method by classifying the eigenvalues of the operator [2],

$$\Lambda = \eta_2 \rho_2 - \eta_1 \rho_1 = \sum_{k=1}^{dimH} \lambda_k |\omega_k\rangle\langle\omega_k|, \tag{3.5.2}$$

which has been decomposed into its eigenvalue spectrum λ_k's here. The optimum measurements are given by two projectors:

$$\begin{aligned} \Pi_1 &= \sum_{k=1}^{k_0-1} |\omega_k\rangle\langle\omega_k| \\ \Pi_2 &= \sum_{k=k_0}^{dim H} |\omega_k\rangle\langle\omega_k|, \end{aligned} \tag{3.5.3}$$

where Π_1 corresponds to the negative spectrum and Π_2 to the non-negative spectrum. The minimum error probability is therefore achieved to be

$$P_E = \frac{1}{2}(1 - Tr|\Lambda|) = \frac{1}{2}(1 - Tr|\eta_2\rho_2 - \eta_1\rho_1|), \tag{3.5.4}$$

with $|\Lambda| = \sqrt{\Lambda^\dagger\Lambda}$. With the above expression the operator Λ is given as

$$\begin{aligned} \Lambda &= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} \Lambda_i \\ &= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{(n+1)(n+m+1)} (\eta_2|\phi_i'\rangle\langle\phi_i'| - \eta_1|\phi_i\rangle\langle\phi_i|)\,. \end{aligned} \tag{3.5.5}$$

The sub-space spanned by each couple of $\{|\phi_i\rangle, |\phi_i'\rangle\}$, where $1 \le i \le (n+1)(n+m+1)$, is orthogonal to the rest part of Hilbert space H. In it we introduce in the following new bases:

$$|\omega_i\rangle = |\phi_i\rangle = |\phi_i'\rangle, \tag{3.5.6}$$

if $\langle\phi_i|\phi_i'\rangle = 1$; and

$$\begin{aligned} |\omega_i\rangle &= \frac{1}{\sqrt{2(1+\langle\phi_i|\phi_i'\rangle)}}(|\phi_i\rangle + |\phi_i'\rangle), \\ |\omega_i'\rangle &= \frac{1}{\sqrt{2(1-\langle\phi_i|\phi_i'\rangle)}}(|\phi_i\rangle - |\phi_i'\rangle), \end{aligned} \tag{3.5.7}$$

if $\langle\phi_i|\phi_i'\rangle \neq 1$. All these new bases are orthonormal ($\langle\omega_i|\omega_j\rangle = \delta_{i,j}$, $\langle\omega_i'|\omega_j'\rangle = \delta_{i,j}$ and $\langle\omega_i|\omega_j'\rangle = 0$).

With this new basis, the Λ_i in the second case is given as

$$\begin{aligned}\Lambda_i &= \begin{pmatrix} \langle\omega_i|\Lambda_i|\omega_i\rangle & \langle\omega_i|\Lambda_i|\omega_i'\rangle \\ \langle\omega_i'|\Lambda_i|\omega_i\rangle & \langle\omega_i'|\Lambda_i|\omega_i'\rangle \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2}(\eta_2-\eta_1)(1+\kappa_i) & -\frac{1}{2}\sqrt{1-\kappa_i^2} \\ -\frac{1}{2}\sqrt{1-\kappa_i^2} & \frac{1}{2}(\eta_2-\eta_1)(1-\kappa_i) \end{pmatrix}, \end{aligned} \tag{3.5.8}$$

where $\kappa_i \equiv \langle\phi_i|\phi_i'\rangle$. We thus obtain the following eigenvalues of the Λ_i:

$$\begin{aligned}\lambda_1^{(i)} &= \frac{1}{2}(c + \sqrt{1-(1-c^2)\kappa_i^2}) \\ \lambda_2^{(i)} &= \frac{1}{2}(c - \sqrt{1-(1-c^2)\kappa_i^2}), \end{aligned} \tag{3.5.9}$$

where $c \equiv \eta_2 - \eta_1$. The eigenvalue spectrum of Λ is therefore obtained as follows:

$$\begin{aligned}\Lambda &= \frac{1}{(n+1)(n+m+1)} \sum_{i=1}^{2n+m+1} c|\omega_i\rangle\langle\omega_i| \\ &+ \frac{1}{2(n+1)(n+m+1)} \sum_{i=2n+m+2}^{(n+m+1)(n+1)} \left(c + \sqrt{1-(1-c^2)\kappa_i^2}\right)|\lambda_i\rangle\langle\lambda_i| \\ &+ \frac{1}{2(n+1)(n+m+1)} \sum_{i=2n+m+2}^{(n+m+1)(n+1)} \left(c - \sqrt{1-(1-c^2)\kappa_i^2}\right)|\lambda_i'\rangle\langle\lambda_i'|, \end{aligned} \tag{3.5.10}$$

where $|\lambda_i\rangle$ and $|\lambda_i'\rangle$ are the eigen-vectors corresponding to the eigenvalues $\lambda^{(i)}$ and $\lambda_2^{(i)}$, respectively.

Together with the table of Jordan basis inner products $\langle\phi_i|\phi_i'\rangle$ in Section 3.3, this eigenvalue spectrum of Λ allows us to obtain the minimum error probability

for arbitrary n and m in the input states. Here we give two examples when $c = 0$ (equal preparation probabilities $\eta_1 = \eta_2$) and compare their results with those of unambiguous discrimination we obtained previously.

First, we take 1 copy of program and n copies of data ($n = 1$, $m = n$). Let's look at the limit of the minimum error probability when n tends to infinity. In this case there is a multiplicity of $n+1$ for $\langle \phi_i | \phi_i' \rangle = -1/(n+1)$ and none of other Jordan bases inner product that is not equal to 1. Plugging these results into Helstrom formula [2], we obtain

$$P_E = \frac{1}{2}\left(1 - \frac{1}{2}\sqrt{\frac{n}{n+2}}\right). \tag{3.5.11}$$

As n goes to infinity, P_E tends to $1/4$. In the unambiguous discrimination for this case, the least failure probability Q_L has the limit of $1/2$ as n tends to infinity. So we have the limit relation $P_E = 0.5Q_L$ if we have the minimum error discrimination and the optimum unambiguos discrimination for $n = 1$ and $m = n$.

The other example is to have n copies of program and 1 copy data. After substituting the Jordan basis inner products into the Helstrom formula [2], we obtain the minimum error probability as follows:

$$P_E = \frac{1}{2}\left(1 - \frac{2}{n+2}\sum_{i=1}^{n}\sqrt{1 - (\frac{i}{n+1})^2}\ \frac{i}{n+1}\right). \tag{3.5.12}$$

If $n \to \infty$, the limit of the above formula is

$$P_E = \frac{1}{2}\left(1 - 2\int_0^1 \sqrt{1-x^2}\ x\ dx\right) = \frac{1}{6}. \tag{3.5.13}$$

So we have 5/6 as the upper bound of the success probability in the minimum error discrimination measurements for this case and it is consistent with the result obtained by other method in [24]. Compared with the corresponding least failure probability $Q_L = 2/3$ in the unambiguous discrimination, we have the limit relation $P_E = \frac{1}{4}Q_L$ if we are dealing with the inputs carrying n copies program and 1 copy data.

In these extreme situations of the above two examples the error probability and the failure probability of the unambiguous state discrimination satisfy the general relation $1 - 2P_E \geq 1 - Q_L$ [21]. Moreover, we see from them a prominent difference of the minimum-error discrimination from the unambiguous discrimination, which is that more copies of program copies will give higher success probability while in the unambiguous discrimination more data copies gives higher success probability.

Chapter IV

4 Tools for physical realization of quantum state discrimination

4.1 Introduction

Linear optics is considered as one of the promising candidates for quantum computing (for a recent overview see, e.g., [28]) and can be also applied to many other areas such as quantum cryptography (for a review see. e.g., [29]). In these applications an essential technique is the implementation of all possible operations, including generalized quantum measurements in the form of Positive Operator Value Measures (POVMs), on the signals encoded as photon states by practical linear optics circuits.

A typical and important case of the signal states is single photon *qudits*, i. e., the linear combinations of the modes $a_k^\dagger|0\rangle$, $k = 1, \cdots, N$ (multiple-rail encoding). It was proposed by Reck *et al.* [30] that any unitary operator $\mathcal{U} \in U(N)$ on the N-dimensional *qudits*, $\sum_{i=1}^{N} c_i a_i^\dagger|0\rangle$, can be realized by an N-port interferometer, which is an array of beam splitters and phase shifters performing $SU(2)$ elements, because this unitary operator can be decomposed into the product of these $SU(2)$ elements (see Fig. 4). This scheme was further studied in [31, 32, 33] and has been applied to

a variety of research fields in quantum information theory and experiment.

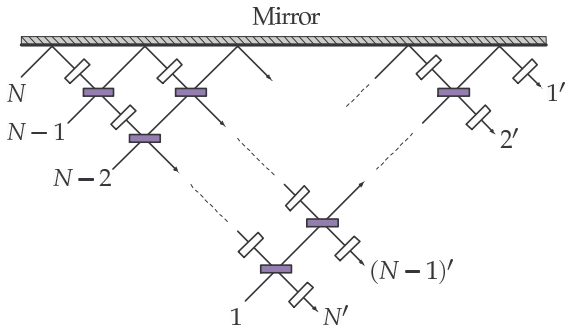

Figure 4: Linear optical module to implement unitary transformations on single photon states. The unitary transformation module constructed with beam splitters (dark square) and phase shifters (white square). Any unitary operator U can be decomposed into the product of $SU(2)$ elements implemented by the beam splitters and the phase shifters, and the maximum number of beam splitters needed is $N(N-1)/2$. The input ports are with unprimed numbers and output ports with primed numbers.

The generalization of the scheme is the implementation of all possible linear maps on single photon *qudits*, which is a fundamental task in processing quantum information. It is intimately related to the realization of POVMs that are at the heart of many quantum information processing protocols. In this chapter, we present the linear optics schemes (including the photon detection) to realize all possible POVMs on a single photon *qudit* [38]. The circuits to perform all the relevant tasks are only the combinations of some scalable unitary operator modules which have been widely

applied in quantum information processing. Given current technologies, our schemes can realize all linear transformations and POVMs on single photon signals in a deterministic way.

Another type of photonic states we use to encode information are coherent states, a typical example of continuous variable (CV) states. In addition to the theoretical research to apply them as the qubits in computation, coherent states are proposed to perform other quantum information processing tasks, e.g., quantum cryptography protocols [34, 35] and quantum database searching [36]. These non-computation quantum information schemes are much more feasible to realize, since they apply linear optics only. Recently, the simplest version of unambiguous identification of coherent states, which is possible to be developed to quantum database searching, has been experimentally realized with fiber optics [37].

We will also provide a general structure for the transformations of coherent state products that are realizable with linear optical circuits [39]. Coherent states are regarded as the antithesis of single photon states. However, as far as the signal processing with linear optics concerned, it can be shown that there is a correspondence between the transformations of these two different types of photonic states. If we process the signals of $|\psi_{in}\rangle = \prod_{i=1}^{N} |\alpha_i\rangle$, the tensor product of coherent states $|\alpha_i\rangle$, with the same setup, the vector $(\alpha_1^*, \cdots, \alpha_N^*)$ (the star stands for the complex conjugate) will transform in the same way as $(c_1, \cdots, c_N)$, the coefficient vector of single photon

states. This correspondence between the linear transformations of two types of vectors shows that the different tasks respectively working with coherent states and single photon states can be performed by the same setup.

4.2 Implementation of non-unitary transformation and general POVM on single photon states

A finite-element POVM is a set of non-negative operators $\{\Pi_i\}$, where Π_i are its elements, satisfying

$$\sum_{i=1}^{n} \Pi_i = I, \tag{4.2.1}$$

with I being the identity operator. It has been proved that any rank-one POVM in the form of $\Pi_i = k_i^2 |\phi_i\rangle\langle\phi_i|$, where $\langle\phi_i|\phi_j\rangle \neq \delta_{ij}$ and $|k_i| \leq 1$, can be realized by the Neumark extension [20], which extends the POVM elements to the orthogonal projectors in a larger space. For the input signals prepared with single photons, such a POVM can be implemented with linear optics circuits, performing unitary transformations, and photon detectors only [40]. The realization of POVMs with arbitrary rank is, however, much more difficult. Since $\Pi_i \geq 0$, it can be decomposed into $\Pi_i = A_i^\dagger A_i$ [41]. The general POVM will be implemented if we simultaneously realize the maps,

$$\rho_{in} \rightarrow \rho_{out,i} = \frac{A_i \rho_{in} A_i^\dagger}{Tr(A_i \rho_{in} A_i^\dagger)}, \tag{4.2.2}$$

and successfully detect these outputs. The detection operators A_i (and their transforms by an arbitrary unitary operator $A'_i = U_i A_i$) can be any allowed linear map in quantum mechanics with equal dimensional input and output signal space, i.e., an $N \times N$ square matrix.

The detection operators of a POVM are, however, only a special case of more general maps called quantum operations (QOs). A QO connects pair of input and output states via the map,

$$\rho_{in} \rightarrow \rho_{out} = \frac{\mathcal{E}(\rho_{in})}{\mathrm{Tr}\big(\mathcal{E}(\rho_{in})\big)}. \tag{4.2.3}$$

$\mathcal{E}$ is a linear, trace-decreasing map that preserves the complete positivity (CP), and generally occurs with non-unit probability $\mathrm{Tr}\big(\mathcal{E}(\rho_{in})\big) \leq 1$. The general form of $\mathcal{E}$ is given as [42]

$$\mathcal{E}(\rho_{in}) = \sum_i K_i \rho_{in} K_i^\dagger \ , \tag{4.2.4}$$

with the independent Kraus operators K_i satisfying the bound $\sum_i K_i^\dagger K_i \leq I$. If a QO transforms pure states to pure it is called a pure map. In this case there is only one term $K\rho_{in}K^\dagger$ in the above equation with K being a *contraction*, i.e., $||K|| \leq 1$. For an isolated pure state input $\rho_{in} = |\psi_{in}\rangle\langle\psi_{in}|$ which does not couple to the environment ρ_E or any other system to evolve as the tensor product $\rho_{in} \otimes \rho_E$, the QOs in Eq. (3) can be therefore written in the form [43],

$$|\psi_{in}\rangle \rightarrow |\psi_{out}\rangle = \frac{K|\psi_{in}\rangle}{||K|\psi_{in}\rangle||} \ . \tag{4.2.5}$$

The output signal of such a linear map, with K as contraction, is detected with a probability $\langle\psi_{in}|K^\dagger K|\psi_{in}\rangle \leq 1$. These contractions can be more general than the detection operators of a POVM because the input space dimension N_1 and the output space dimension N_2 of K can be different, so K is an $N_2 \times N_1$ matrix whose entries are complex numbers. The detection operators A_i of a POVM correspond to a special case of contractions when $N_1 = N_2 \equiv N$.

We now address the problem of how to realize any possible linear map K on single photon *qudits* with *only* three unitary operator modules of the kind shown in Fig. 4. We realize K by its unitary dilation, $\mathcal{U}$, the unitary operator constructed from K in a larger space, which we obtain by using the direct sum extension of the system with an ancilla, $\mathcal{H}_S \oplus \mathcal{H}_A$. In terms of Hilbert space dimensionality, this scheme minimizes the physical resources needed to realize a QO [44]. We embed the state vector $(c_1, c_2, \cdots, c_{N_1})^T$ (T stands for transpose) of the input signal, $|\psi_{in}\rangle = \sum_{i=1}^{N_1} c_i a_i^\dagger|0\rangle$, into a larger space and map it by $\mathcal{U}$ to a vector containing the state vector of the output, $|\psi_{out}\rangle = \sum_{i=1}^{N_2} c_i' a_i'^\dagger|0\rangle$ (unnormalized), of K:

$$\begin{pmatrix} c_1' \\ \vdots \\ c_{N_2}' \\ \vdots \end{pmatrix} = \begin{pmatrix} \mathcal{U}_{1,1} & \mathcal{U}_{1,2} & \mathcal{U}_{1,3} & \cdots \\ \mathcal{U}_{2,1} & \mathcal{U}_{2,2} & \mathcal{U}_{2,3} & \cdots \\ \mathcal{U}_{3,1} & \mathcal{U}_{3,2} & \mathcal{U}_{3,3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_{N_1} \\ \vdots \\ 0 \end{pmatrix}. \tag{4.2.6}$$

It should be noted that we realize this unitary dilation always with a vacum state

ancilla $(0, 0, \cdots, 0)^T$ added to the input state vector as a direct sum. Next, we will derive the algorithm to generate the unitary dilation $\mathcal{U}$ of linear map K.

$K^\dagger K$ and $KK^\dagger$ are positive matrices of $N_1 \times N_1$ and $N_2 \times N_2$, respectively. Suppose $N_1 \geq N_2$, we choose to diagonalize $KK^\dagger$ by a unitary operator U. We can also construct an $N_1 \times N_1$ unitary matrix V to obtain the Singular Value Decomposition (SVD), $K = U\Sigma V^\dagger$, with the uniquely determined *singular values* on the diagonal of the $N_2 \times N_1$ matrix Σ. If $N_1 < N_2$, on the other hand, we will choose to diagonalize $K^\dagger K$ to get a similar result.

Then we extend the rectangular matrix Σ to the following $max(N_1, N_2) \times max(N_1, N_2)$ square matrix

$$\Sigma' = \begin{pmatrix} |\sigma_1| & & & & & \\ & \ddots & & & & \\ & & |\sigma_{N_2}| & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}, \tag{4.2.7}$$

where the singular values σ_i satisfy $|\sigma_i| \leq 1$ since K is a contraction. The extension of Σ in the case of $N_1 < N_2$ also takes the above form except that $|\sigma_{N_2}|$ is replaced by $|\sigma_{N_1}|$. Using the fact that Σ' is still a contraction, we can obtain a $max(2N_1, 2N_2) \times$

$max(2N_1, 2N_2)$ unitary dilation

$$G = \begin{pmatrix} \Sigma' & (I - \Sigma'^2)^{1/2} \\ (I - \Sigma'^2)^{1/2} & -\Sigma' \end{pmatrix} \tag{4.2.8}$$

of it (see, e.g., Ex. I.3.6 in [41]), which acts on a space $\mathcal{H} \oplus \mathcal{H}$ with $\mathcal{H}$ being $max(N_1, N_2)$ dimensional. We also extend U and V to $max(2N_1, 2N_2)$ by $max(2N_1, 2N_2)$ matrices by adding the identity matrix I in the diagonal and zero matrices off the diagonal. A general linear map K is therefore realized by the following unitary dilation:

$$\mathcal{U} = UGV^\dagger. \tag{4.2.9}$$

In our setup, we perform its equivalence by acting $\mathcal{U}^\dagger$ on the spatial mode vector $(a_1^\dagger, \cdots, a_{N_1}^\dagger)$. The circuits to implement V and $U^\dagger$ are the corresponding N_1-port and N_2-port modules. After the input spatial mode vector is processed by V, we redirect the output to a $max(2N_1, 2N_2)$-port module of G with the input ports numbered from $N_1 + 1$ to $max(2N_1, 2N_2)$ in Fig. 1 black or a vacuum state. Here is some detail about the step to implement Σ through its unitary dilation G. Picking out the entries containing only one of the singular values σ_i from the matrix of G, we form a 2×2

sub-matrix, which can be transformed by a rotation $T_{i,i+max(N_1,N_2)}$ to a diagonal one:

$$\begin{pmatrix} |\sigma_i| & (1-\sigma_i^2)^{1/2} \\ (1-\sigma_i^2)^{1/2} & -|\sigma_i| \end{pmatrix} \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.2.10}$$

With a series of rotations in the form of $T_{i,i+max(N_1,N_2)} \otimes I_{\text{rest}}$, for $i = 1, \cdots, min(N_1, N_2)$, G can be realized by $min(N_1, N_2)$ beam splitters with the reflection coefficients $R = 1 - \sigma_i^2$ and phase shifters giving rise to $e^{i\pi}$. Therefore, the upper bound of the total number of the beam splitters required in the scheme is

$$N_{max} = \frac{N_1^2}{2} + \frac{N_2^2}{2} - |\frac{N_1}{2} - \frac{N_2}{2}|, \tag{4.2.11}$$

which is determined by the dimensions of the input and output Hilbert spaces. In the whole extended space, we will obtain two outputs after the action of the three unitary operator modules: one is the exact output $(a_1'^{\dagger}, \cdots, a_{N_2}'^{\dagger})$ of the linear map K from the output ports of $U^{\dagger}$, and the other is an extra output $(a_{N_2+1}'^{\dagger}, \cdots, a_{max(2N_1,2N_2)}'^{\dagger})$ from the output ports of G numbered from $(N_2+1)'$ to $(max(2N_1, 2N_2))'$. Fig. 5 displays the scheme that realizes the effect of K on the input state ρ_{in}.

This linear optics scheme can be directly applied to where we need non-unitary transformation on photon states, e.g., in the production of single photon *qudits* in any form of $\sum_i c_i a_i^{\dagger}|0\rangle$, where $\sum_i |c_i|^2 \leq 1$ (possibly unnormalized), by multiple-rail encoding, and in the enhancement of the entanglement of a pair of partially entangled

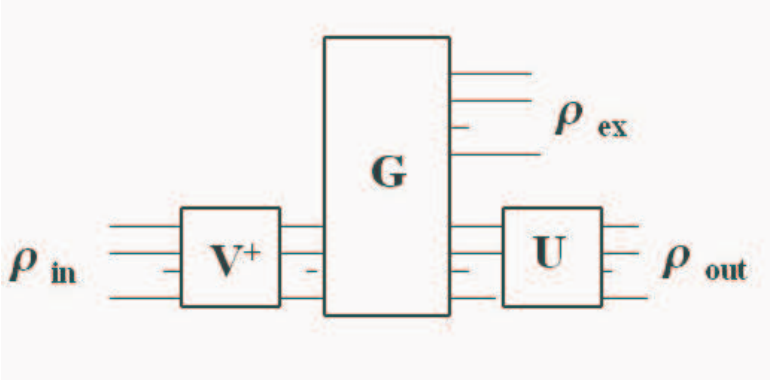

Figure 5: The circuit to perform the unitary dilation $\mathcal{U}$ of contraction K, the general linear transformation on a pure state input. We will obtain two outputs, $\rho_{out} = |\psi_{out}\rangle\langle\psi_{out}|$ of K and an extra $\rho_{ex} = |\psi_{ex}\rangle\langle\psi_{ex}|$, from the corresponding terminals. Because the linear map K is not generally inversable, we need to add an ancilla $|\psi_{ex}\rangle$ to $|\psi_{out}\rangle$, i.e., $|\psi'_{in}\rangle = |\psi_{out}\rangle \oplus |\psi_{ex}\rangle$, if we are to convert it back to the original $|\psi_{in}\rangle$ by using the same circuit from the inverse direction.

photons like $\sum_i c_i a_i^\dagger|0\rangle_1 a_i^\dagger|0\rangle_2$, with different $|c_i|$ unequal, by one party operation.

Now we look in some detail at the realization of POVMs as one important application of our scheme. We start with the simplest situation of $n = 2$, where the two POVM elements are always commutative, $[\Pi_1, \Pi_2] = 0$. Suppose that the dimension of the signal space is N, and the $N \times N$ detection operators A_i of the POVM can be factorized by SVD as $A_i = V_i \Sigma_i U_i$ with U_i, V_i unitary and Σ_i diagonal. We first set up a N-port module for U_1 and, after the signal leaving U_1 module, we process

it with a $2N$-port module to implement the unitary dilation of Σ_1. From its output ports numbered from $1'$ to N' we get an output $|\psi^1_{mid}\rangle \sim \Sigma_1 U_1|\psi_{in}\rangle$, while from the ports numbered from $(N+1)'$ to $2N'$ another output $|\psi^2_{mid}\rangle \sim \Sigma_{1C} U_1|\psi_{in}\rangle$, with $\Sigma^2_{1C} = I - \Sigma^2_1$. Then we will just redirect them to modules of V_1 and V_2 and finally obtain the outputs $A_1|\psi_{in}\rangle/||A_1|\psi_{in}\rangle||$ or $A_2|\psi_{in}\rangle/||A_2|\psi_{in}\rangle||$ from the corresponding terminals.

For a POVM with the number of elements $n \geq 3$, the situation is much trickier. Instead of Π_2, what we realize from the corresponding output ports of $|\psi^2_{mid}\rangle$ is the operator $I - \Pi_1$. By the diagonalization, all elements of a general POVM can be factorized into $\Pi_i = U_i^\dagger \Sigma_i^2 U_i$, where the different U_i do not generally commute, i.e., $[U_i, U_j] \neq 0$ for $i \neq j$.

In the realization of Π_2, therefore, we need to consider two different situations:

(1) If $||\Pi_1|| < 1$, because $I - \Pi_1 > \Pi_2$ when $n \geq 3$, we can find a diagonal matrix Σ_2^* with $||\Sigma_2^*|| \leq 1$ and a unitary operator U_{2L} such that

$$\Pi_2 \;=\; U_1^\dagger \Sigma_{1C} U_{2L}^\dagger \Sigma_2^{*2} U_{2L} \Sigma_{1C} U_1 = U_2^\dagger \Sigma_2^2 U_2. \tag{4.2.12}$$

Since $||UAV|| = ||A||$ for an arbitary linear operator A and all unitary matrices U and V, we obtain the following from Eq. (4.2.2):

$$||\Sigma_2^*|| = ||\Sigma_2^* U_{2L} U_1|| = ||\Pi_2^{1/2}(I - \Pi_1)^{-1/2}|| \leq 1, \tag{4.2.13}$$

where we have used Lemma V.1.7 in [41] with the existence of $(I - \Pi_1)^{-1}$ due to

the fact that $||\Pi_1|| < 1$. These two matrices Σ_2^* and U_{2L} are obtained by a standard digonalization procedure following the above equation. Then, after performing U_{2L} with a N-port module, Σ_2^* as a contraction map can be implemented by a $2N$-port linear optics module with at most N beam splitters. To realize A_2 completely, we add one more module of a proper V_2.

(2) If $||\Pi_1|| = 1$, after the signal goes through the part of circuit implementing $I - \Pi_1$, some of the output ports will be black because the corresponding components have been projected out by Π_1. In this case the diagonalized form of a POVM element with the unit norm, e.g., Σ_j^2, has some entries 1. From Eq. (4.2.1), on the other hand, we have

$$\Sigma_j^2 + \sum_{i \neq j} U_j U_i^\dagger \Sigma_i^2 U_i U_j^\dagger = I,$$

and then we find that the corresponding entries of Σ_i^2, for all $i \neq j$, are 0. Then we will just inverse the remaining $(N-D) \times (N-D)$ non-zero part of Σ_{1C} matrix, where D is the multiplicity of the unit eigenvalue of Π_1, in finding U_{2L} and Σ_2^* of this size in Eq. (4.2.12).

Repeating the above procedure from the output ports where the operator $I - \Pi_1 - \Pi_2$ is realized, we add all the corresponding modules performing U_{nL}, Σ_n^*, etc., for $n \geq 3$, to implement the remaining A_3, A_4, $\cdots$, A_n, respectively. The total number of modules of Fig. 4 needed in our scheme to realize a general POVM with n elements is $3n-2$. As an illustration of this general scheme, Fig. 6 shows the setup to perform

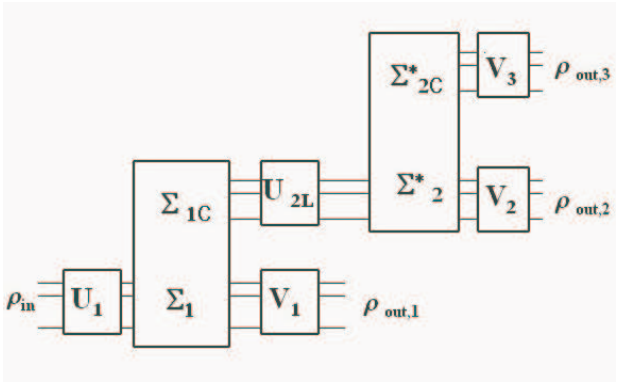

Figure 6: The setup to perform any three-element POVM on single photon states. The seven unitary operator modules, two of which perform the pairs of operators Σ_1 and $\Sigma_{1C} = (I - \Sigma_1^2)^{1/2}$, Σ_2^* and $\Sigma_{2C}^* = (I - \Sigma_2^{*2})^{1/2}$, respectively, are designed with the POVM elements. The detectors at the terminals effect a dephasing to eliminate the interference between $A_i|\psi_{in}\rangle$ [46], and capture the outputs $\rho_{out,i} = A_i\rho_{in}A_i^\dagger/Tr(A_i\rho_{in}A_i^\dagger)$, for $i = 1, 2, 3$, with the probabilities $p_i = Tr(A_i\rho_{in}A_i^\dagger)$. The outputs redirected to only one set of detectors form a probability distribution as the mixture [47], $\sum_i p_i\rho_{out,i} = \sum_i A_i\rho_{in}A_i^\dagger$, there.

any POVM with three elements.

We have reduced the problem of realizing a POVM to that of finding a sequence of unitary operators with the POVM elements and realizing them with the ancilla states of vacuum and then detecting the outputs with the standard projective measurements on the extended space. The algorithm to obtain these unitary operators is given, and

the implementation of any POVM, with elements of arbitrary rank, can be therefore realized for single photon input signals. Using this method, we will directly obtain the output states of a POVM, which can be tailored by choosing the appropriate V_i modules, from the corresponding terminals where the signal detectors are placed. If our signals are just single photon polarization qubits, $|\psi_{in}\rangle = c_1|H\rangle + c_2|V\rangle$ (polarization modes H and V), we can use much simpler circuit to implement any POVM on them as in [45], where a POVM is realized as the decomposition of an identity operator but the necessary algorithm to obtain, e.g., Σ_n^*, U_{nL} for the implementation of all specified Π_i is not given. Given the beyond-linear-optics methods to implement unitary operations on more complicated quantum systems than single photon states, this scheme can be applied to more general situations of photonic states as well as the signals of any other type of radiation.

4.3 General transformation of coherent state products with linear optics

We start with the simple situations of the input

$$|\psi_{in}\rangle = |\alpha_1\rangle|\alpha_2\rangle = D(\alpha_1)D(\alpha_2)|0\rangle \tag{4.3.1}$$

being sent to a beamsplitter and a phase shifter. $D(\alpha)$ here represents the displacement operator $e^{\alpha a^\dagger - \alpha^* a}$. With the interaction Hamiltonian

$$H_{BS} = \theta e^{i\varphi} a_1^\dagger a_2 + \theta e^{-i\varphi} a_1 a_2^\dagger, \tag{4.3.2}$$

of the beamsplitter, the creation operators of the input modes are transformed to those of the output modes $b_1^\dagger$ and $b_2^\dagger$ as a $SU(2)$ map,

$$\begin{aligned}\begin{pmatrix} b_1^\dagger \\ b_2^\dagger \end{pmatrix} &= \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} a_1^\dagger \\ a_2^\dagger \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta & ie^{-i\varphi}\sin\theta \\ ie^{i\varphi}\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a_1^\dagger \\ a_2^\dagger \end{pmatrix}, \end{aligned} \tag{4.3.3}$$

which defines the unitary operation U_{BS} of a beamsplitter [28]. The reflection and transmission coefficients R and T of the beamsplitter are given in terms of the parameters as $R = \sin^2\theta$ and $T = 1 - R = \cos^2\theta$, and the relative phase φ ensures that the transformation is unitary. The input state of the product of two coherent states is therefore transformed as follows:

$$\begin{aligned}|\psi_{out}\rangle &= U_{BS}|\psi_{in}\rangle = U_{BS}D(\alpha_1)D(\alpha_2)U_{BS}^\dagger U_{BS}|0\rangle \\ &= e^{\alpha_1(U_{11}^* b_1^\dagger + U_{21}^* b_2^\dagger) - \alpha_1^*(U_{11}b_1 + U_{21}b_2)} e^{\alpha_2(U_{12}^* b_1^\dagger + U_{22}^* b_2^\dagger) - \alpha_2^*(U_{12}b_1 + U_{22}b_2)}|0\rangle \\ &= e^{(U_{11}^*\alpha_1 + U_{12}^*\alpha_2)b_1^\dagger - (U_{11}\alpha_1^* + U_{12}\alpha_2^*)b_1} e^{(U_{21}^*\alpha_1 + U_{22}^*\alpha_2)b_2^\dagger - (U_{21}\alpha_1^* + U_{22}\alpha_2^*)b_2}|0\rangle, \end{aligned} \tag{4.3.4}$$

where we apply Campbell-Baker-Hausdorff formula $e^A e^B = e^{A+B}e^{\frac{1}{2}[A,B]}$ from the second line, as well as the unitary transformation in Eq. (4.3.3). If we define

$$\begin{pmatrix} \beta_1^* \\ \beta_2^* \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} \alpha_1^* \\ \alpha_2^* \end{pmatrix}, \tag{4.3.5}$$

the output state will be given as

$$|\psi_{out}\rangle = D(\beta_1)D(\beta_2)|0\rangle = |\beta_1\rangle|\beta_2\rangle. \tag{4.3.6}$$

Eq. (4.3.5) characterizes the transformation of the product of two coherent states under the action of Eq. (4.3.3).

Another basic ingredient in a linear optical circuit is a phase shifter with the interaction Hamiltonian $H = \phi a^\dagger a$. The creation operator $a^\dagger$ of an input mode is mapped to $b^\dagger = e^{i\phi} a^\dagger$ by the phase shifter, and one input coherent state is thus transformed to $|\beta\rangle = |e^{i\phi}\alpha\rangle$. Analogous to Eq. (4.3.5), this relation is also given as

$$\beta^* = e^{-i\phi}\alpha^*. \tag{4.3.7}$$

The unit module of any linear optical circuit is an array of beamsplitters and phase shifters shown in Fig. 4. Sending a single photon state $\sum_{i=1}^{N} c_i a_i^\dagger$ to this array with the different modes $a_i^\dagger$ entering the different input ports from $i = 1$ to N, we will have the following unitary transformation $\mathcal{U}(N)$ of the mode vector,

$$\begin{pmatrix} b_1^\dagger \\ b_2^\dagger \\ \vdots \\ b_N^\dagger \end{pmatrix} = \begin{pmatrix} \mathcal{U}_{1,1} & \mathcal{U}_{1,2} & \cdots & \mathcal{U}_{1,N} \\ \mathcal{U}_{2,1} & \mathcal{U}_{2,2} & \cdots & \mathcal{U}_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{U}_{N,1} & \mathcal{U}_{N,2} & \cdots & \mathcal{U}_{N,N} \end{pmatrix} \begin{pmatrix} a_1^\dagger \\ a_2^\dagger \\ \vdots \\ a_N^\dagger \end{pmatrix}, \tag{4.3.8}$$

since it is the product of $SU(2)$ maps $T_{i,j} = T_{i,j} \otimes I_{rest}$ and $U(1)$ maps $e^{i\phi_{i,j}}$ respectively performed by the single beamsplitters and the single phase shifters, which is obtained through the iterative decomposition [30]

$$\mathcal{U}(N) T_{N,N-1} \cdots T_{N,1} = \mathcal{U}(N-1) \oplus e^{i\phi}. \tag{4.3.9}$$

The coefficient vector $\vec{c} = (c_1, \cdots, c_n)$ is correspondingly transformed as $\vec{c'} = \vec{c}\,\mathcal{U}^\dagger$.

Replacing the input with a product of coherent states $|\psi_{in}\rangle = \prod_{i=1}^{N} |\alpha_i\rangle$, with $|\alpha_1\rangle$ entering the port 1, $|\alpha_2\rangle$ entering port 2, and so on, we will obtain the following transformation

$$\begin{pmatrix} \beta_1^* \\ \beta_2^* \\ \vdots \\ \beta_N^* \end{pmatrix} = \begin{pmatrix} \mathcal{U}_{1,1} & \mathcal{U}_{1,2} & \cdots & \mathcal{U}_{1,N} \\ \mathcal{U}_{2,1} & \mathcal{U}_{2,2} & \cdots & \mathcal{U}_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{U}_{N,1} & \mathcal{U}_{N,2} & \cdots & \mathcal{U}_{N,N} \end{pmatrix} \begin{pmatrix} \alpha_1^* \\ \alpha_2^* \\ \vdots \\ \alpha_N^* \end{pmatrix} \tag{4.3.10}$$

under the action of the map of the creation operators in Eq. (4.3.8), which is generalized from that of Eq. (4.3.5) under the action in Eq. (4.3.3). If we decompose the above unitary transformation into the product of $SU(2)$ and $U(1)$ maps to make the different components of α_i^* transform as in Eqs. (4.3.5) and (4.3.7), combining all these separate maps will give the above transformation of $(\alpha_1^*, \cdots, \alpha_N^*)^T$ (T stands for transpose) exactly.

From this unitary transformation, we also obtain an invariant

$$\sum_{i=1}^{N} |\alpha_i|^2 = \sum_{i=1}^{N} |\beta_i|^2. \tag{4.3.11}$$

It is the conservation of the average total photon number $\langle\psi_{in}| \sum_i \hat{n}_i |\psi_{in}\rangle$ under the unitary transformation induced by linear optical circuit. On the other hand, for two sets of coherent states $\{|\alpha_1\rangle, \cdots, |\alpha_N\rangle\}$ and $\{|\beta_1\rangle, \cdots, |\beta_N\rangle\}$ satisfying this relation, we can always find a unitary map $\mathcal{U}$ realizing the transformations between their

products.

Next, we generalize this type of unitary transformations to the non-unitary ones. In [38] we present a method of combining three linear optical modules in Fig. 4 to realize any non-unitary map $\mathcal{K}$ of contraction ($||\mathcal{K}|| \leq 1$) on the coefficient vector $(c_1, \cdots, c_N)$ of a single photon state. It is effectively performed by the unitary transformation

$$\mathcal{U} = \begin{pmatrix} \mathcal{K} & -(I - \mathcal{K}\mathcal{K}^\dagger)^{1/2} \\ (I - \mathcal{K}^\dagger\mathcal{K})^{1/2} & \mathcal{K}^\dagger \end{pmatrix} \tag{4.3.12}$$

in the extended Hilbert space. $\mathcal{K}$ here can be any $M \times N$ matrix with the non-zero eigenvalues of $\mathcal{K}\mathcal{K}^\dagger$ or $\mathcal{K}^\dagger\mathcal{K}$ being less than or equal to 1. If $M \neq N$, it can be enlarged by the direction sum with a unit matrix to a square matrix. Following Eq. (4.3.10), we can implement this extended unitary map on an input of coherent states by sending $|\psi_{in}\rangle = \prod_{i=1}^{N} |\alpha_i\rangle$ to the input ports of the module, with $|\alpha_i\rangle$ entering the port numbered from $i = 1$ to N, respectively, and the rest $2 \times max(M, N) - N$ ports being dark. A linear optical circuit modules implementing the unitary transformation $\mathcal{U}\,(2 \times max(M, N))$ thus realizes the following non-unitary map

$$\begin{pmatrix} \beta_1^* \\ \beta_2^* \\ \vdots \\ \beta_M^* \end{pmatrix} = \begin{pmatrix} \mathcal{K}_{1,1} & \mathcal{K}_{1,2} & \cdots & \mathcal{K}_{1,N} \\ \mathcal{K}_{2,1} & \mathcal{K}_{2,2} & \cdots & \mathcal{K}_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{K}_{M,1} & \mathcal{K}_{M,2} & \cdots & \mathcal{K}_{M,N} \end{pmatrix} \begin{pmatrix} \alpha_1^* \\ \alpha_2^* \\ \vdots \\ \alpha_N^* \end{pmatrix} \tag{4.3.13}$$

in a subspace. The output $\prod_{i=1}^{M} |\beta_i\rangle$ is obtained from the output ports numbered from $1'$ to M' in Fig. 4, and some other coherent states also output from the remaining

ports. A contraction map on a product of coherent states can be, therefore, realized with the same linear optical circuit to implement this contraction map on a single photon state. It is the primary result of this section and, in the next chapter, we will apply some special forms of Eqs. (4.3.10) and (4.3.13) in designing the circuit to discriminate unknown coherent states.

Chapter V

5 Unknown state discrimination systems

5.1 Introduction

The unknown state discriminators can be of potential value in quantum communication and quantum computing, so it is interesting to study their feasible physical implementations. In [22] we propose a pure optical way based on interferometry [30] to deterministically realize the optimal measurements in [10] under the assumption that all the symmetric input states can be prepared as single photon states in multi-rail representation. The quantum circuit to realize the unknown qubits discrimination without achieving the optimal measurement and the possible implementation of its ingredient logic gates in ion traps are studied in [48]. The design of the unitary operators to implement the discrimination of a pair of unknown qubits is also discussed in [49].

In this chapter, we design an experimental setup to unambiguously and optimally discriminate the symmetric input states $|\psi_1\rangle|\psi_2\rangle|\psi_i\rangle$ $(i = 1, 2)$ prepared with *any* pair of linearly independent unknown single photon polarization qubits [50]. This is a device to process the unknown triple photon input signals, and all the technologies involved have been experimentally realized thus far. Furthermore, we will apply the

correspondence between the transformations of the single photon and coherent states to design a linear optical system to discriminate unknown coherent states. This system can be a prototypical quantum database searching device.

5.2 Physical basis for unknown optical qubit discrimination

We first give a brief review of the optimal measurements for discriminating any pair of unknown states we aim to realize for single photon polarization qubits. The input signals processed by our device are given as follows:

$$\begin{aligned} |\Psi_{1,in}\rangle &= |\psi_1\rangle_1|\psi_2\rangle_2|\psi_1\rangle_3 \\ |\Psi_{2,in}\rangle &= |\psi_1\rangle_1|\psi_2\rangle_2|\psi_2\rangle_3, \end{aligned} \tag{5.2.1}$$

where $|\psi_i\rangle = \alpha_i|H\rangle + \beta_i|V\rangle$, for $i = 1, 2$, and H, V are their horizontal and perpendicular polarization modes. Since $|\psi_1\rangle$ and $|\psi_2\rangle$ are linearly independent, there exist different permutation symmetries in these two inputs, and we can therefore design the POVMs, with the elements Π_1 and Π_2 satisfying $\Pi_1|\Psi_2^{in}\rangle = \Pi_2|\Psi_1^{in}\rangle = 0$, to unambiguously discriminate them. In the Bayesian approach [10], the optimal POVM elements for the unambiguous discrimination of the above inputs are

$$\begin{aligned} \Pi_1 &= \frac{2}{3}\left(2 - \sqrt{\frac{\eta_2}{\eta_1}}\right) I_1 \otimes |\Psi_{23}^{as}\rangle\langle\Psi_{23}^{as}|, \\ \Pi_2 &= \frac{2}{3}\left(2 - \sqrt{\frac{\eta_1}{\eta_2}}\right) I_2 \otimes |\Psi_{13}^{as}\rangle\langle\Psi_{13}^{as}|, \end{aligned} \tag{5.2.2}$$

where $|\Psi_{ij}^{as}\rangle = 1/\sqrt{2}\,(|H\rangle_i|V\rangle_j - |V\rangle_i|H\rangle_j)$ and I_i the identity operators, if the *a priori* probability η_1 of the data $|\psi_1\rangle$ is in the range of $1/5 \leq \eta_1 \leq 4/5$. For $4/5 \leq \eta_1 \leq 1$, the optimal measurement reduces to the projection valued measurement (PVM) as

$$\begin{aligned} \Pi_1 &= I_1 \otimes |\Psi_{23}^{as}\rangle\langle\Psi_{23}^{as}| \\ \Pi_2 &= 0; \end{aligned} \tag{5.2.3}$$

and for $0 \leq \eta_1 \leq 4/5$, the index 1 and 2 of the above PVM operators should be interchanged to get the optimal measurement. In the minimax approach without the available *a priori* information of the input data [11], on the other hand, the optimal POVM for discriminating the inputs in Eq. (5.2.1) is given as

$$\begin{aligned} \Pi_1 &= \frac{2}{3}\, I_1 \otimes |\Psi_{23}^{as}\rangle\langle\Psi_{23}^{as}|, \\ \Pi_2 &= \frac{2}{3}\, I_2 \otimes |\Psi_{13}^{as}\rangle\langle\Psi_{13}^{as}|. \end{aligned} \tag{5.2.4}$$

In both approaches, there is inconclusive measurement result corresponding to the operator $\Pi_0 = I - \Pi_1 - \Pi_2$.

The physical fundamentals to realize the optimal measurements on the unknown input signals are the teleportation of unknown quantum states [51] and the deterministic implementation of a POVM on single photon signals [38]. A teleportation protocol is applied to transform the triple photon input signals in Eq. (5.2.1) to the

corresponding single photon signals running on different tracks:

$$\begin{aligned}
|\Psi_{1,in}\rangle &= |\psi_1\rangle_1|\psi_2\rangle_2|\psi_1\rangle_3 \\
&= c_1|HHH\rangle + c_2|VHH\rangle + c_3|HHV\rangle + \cdots + c_8|VVV\rangle \\
&\rightarrow c_1|0_A, 0_B, H\rangle + c_2|1_A, 0_B, H\rangle + c_3|0_A, 0_B, V\rangle + \cdots + c_8|1_A, 1_B, V\rangle, \quad (5.2.5)
\end{aligned}$$

where c_i are unknown coefficients, and 0_A, 1_A, 0_B and 1_B the symbols related to the which-path degree of freedom of the photon. After some of the input signal's polarization degree of freedom is mapped this way to the which-path degree of freedom, we will obtain a single polarization photon running on 4 different tracks (the total dimensionality of the quantum system is 8) so that any POVM performed on it can be deterministically implemented by linear optics.

To teleport three input qubits in a combined way, we need to have three entangled pairs, e.g.,

$$\begin{aligned}
|\Phi_1^+\rangle &= \frac{1}{\sqrt{2}}\left(|H\rangle|H\rangle + |V\rangle|V\rangle\right), \\
|\Phi_2^+\rangle &= \frac{1}{\sqrt{2}}\left(|H\rangle|0_A\rangle + |V\rangle|1_A\rangle\right), \\
|\Phi_3^+\rangle &= \frac{1}{\sqrt{2}}\left(|H\rangle|0_B\rangle + |V\rangle|1_B\rangle\right). \quad (5.2.6)
\end{aligned}$$

We here define the four Bell states as follows:

$$\begin{aligned}
|\Phi^\pm\rangle &\equiv \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right), \\
|\Psi^\pm\rangle &\equiv \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right), \quad (5.2.7)
\end{aligned}$$

where 0 can be H, 0_A, 0_B, etc, and 1 can be V, 1_A, 1_B, etc. Two of the states in Eq. (5.2.6) involve both polarization and which-path degrees of freedom. How to effectively produce them is what we will discuss in the next section.

5.3 Conversion to single photon signal

In this section, we give a rather detailed description of a circuit to map the triple photon input signals to the corresponding single photon signals as in Eq. (5.2.5). To begin with, we look at the transformation of a double photon polarization state $|\Psi_{in}\rangle = |\psi_1\rangle_1|\psi_2\rangle_2$, where $|\psi_i\rangle = \alpha_i|H\rangle + \beta_i|V\rangle$, to the corresponding single photon state by a combined teleportation procedure. We use two extra photon sources $1/\sqrt{2}(|H\rangle_A + |V\rangle_A)$ and $1/\sqrt{2}(|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C)$, and let the first photon on track A control the part B of the second entangled photon pair through a CNOT gate taking the following action:

$$U_{CNOT} = (|H\rangle_A\langle H| \otimes I_B + |V\rangle_A\langle V| \otimes \sigma_{x,B}) \otimes I_C. \tag{5.3.1}$$

The above equation means that there will be no action on track B if the photon component on track A is in the state of $|H\rangle$ and there will be a bit flip $\sigma_{x,B}$ of $\{H, V\}$ on track B if that photon component is in $|V\rangle$. After the joint unitary map U_{CNOT}, the total state on the track A, B and C will be as follows (here we neglect the common

factors for brevity):

$$\begin{aligned} & U_{CNOT}\big(|H\rangle_A + |V\rangle_A\big)\big(|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C\big) \\ = \;& |H\rangle_A|H\rangle_B|H\rangle_C + |H\rangle_A|V\rangle_B|V\rangle_C + |V\rangle_A|V\rangle_B|H\rangle_C + |V\rangle_A|H\rangle_B|V\rangle_C. \quad (5.3.2) \end{aligned}$$

This type of non-destructive optical CNOT gate has been experimentally demonstrated [52] and, theoretically, a CNOT gate for two independent single photon polarization qubits can be realized near deterministically [53].

The output state of the CNOT gate in Eq. (5.3.2) is divided into two sets for part B and C: the even parity $\{|H\rangle_B|H\rangle_C, |V\rangle_B|V\rangle_C\}$ and the odd parity $\{|H\rangle_B|V\rangle_C, |V\rangle_B|H\rangle_C\}$, and they can be discriminated near deterministically by a polarization parity quantum non-demolition detection (QND) [53]. The setup to realize this QND includes a laser probe initially in a coherent state $|\alpha\rangle_p$ and the cross-Kerr nonlinearities, which have a Hamiltonian $H = \hbar\chi a_s^\dagger a_s a_p^\dagger a_p$, where the signal (probe) mode has the creation and destruction operators given by $a_s^\dagger, a_s (a_p^\dagger, a_p)$ and χ the strength of nonlinearity which can be weak. Through the interaction in the weak nonlinear cross-Kerr, the photon states on track B, C and the probe evolve together to $|\psi_T\rangle \sim (|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C)|\alpha\rangle_p + |H\rangle_B|V\rangle_C|\alpha e^{i\theta}\rangle_p + |V\rangle_B|H\rangle_C|\alpha e^{-i\theta}\rangle_p$, where $\theta = \chi t$ with t being the interaction time. $|\alpha\rangle$ and $|\alpha e^{\pm i\theta}\rangle$ can be distinguished between each other by a homodyne-heterodyne measurement on the probe.

Then we classically feedforward two actions to the output on track B: if the the detection result is $|\alpha e^{\pm i\theta}\rangle$, we let the photon component on track B go to path B_1 and

denote the action 0_A (the index A means the control from track A photon component); and if the result is $|\alpha\rangle$, the photon component on track B is redirected to track B_2 with an action named 1_A. A bit flip (plus the phase shift redressing due to the QND) on B_1 track is performed to restore the odd parity of the photon components on track B and C to the even parity, i.e., $|HV\rangle, |VH\rangle \rightarrow |HH\rangle, |VV\rangle$. As the result, we obtain a state,

$$\begin{aligned} |\psi^{ent}\rangle &\sim |H\rangle_A|H\rangle_{B_1,0_A}|H\rangle_C + |H\rangle_A|V\rangle_{B_1,0_A}|V\rangle_C + |V\rangle_A|H\rangle_{B_2,1_A}|H\rangle_C + |V\rangle_A|V\rangle_{B_2,1_A}|V\rangle_C \\ &= (|H\rangle_A|0_A\rangle + |V\rangle_A|1_A\rangle)(|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C), \end{aligned} \tag{5.3.3}$$

which can be factorized into the product of two entangled states. $|0_A\rangle$ and $|1_A\rangle$ are defined as two *controlling switch actions* on the track B photon component from the photon component on track A. These two fictitious quantum states describe the effective action of track B photon component to go to different paths B_1 and B_2 under the control:

$$\begin{aligned} &|0_A\rangle|H\rangle_B \equiv |H\rangle_{B_1,0_A}, \quad |1_A\rangle|H\rangle_B \equiv |H\rangle_{B_2,1_A}, \\ &|0_A\rangle|V\rangle_B \equiv |V\rangle_{B_1,0_A}, \quad |1_A\rangle|V\rangle_B \equiv |V\rangle_{B_2,1_A}. \end{aligned} \tag{5.3.4}$$

It is feasible, therefore, to use these two entangle states to teleport $|\Psi_{in}\rangle =$

$|\psi_1\rangle_1|\psi_2\rangle_2$ to a single photon polarization state:

$$
\begin{aligned}
&|\psi_1\rangle_1\big(|H\rangle_A|0_A\rangle + |V\rangle_A|1_A\rangle\big)|\psi_2\rangle_2\big(|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C\big) \\
&\sim \big(|\Phi^+\rangle_{1,A}|\psi_1\rangle_{A_{Ct}} + |\Psi^+\rangle_{1,A}(\sigma_{x,A_{Ct}}|\psi_1\rangle_{A_{Ct}}) + |\Psi^-\rangle_{1,A}(-i\sigma_{y,A_{Ct}}|\psi_1\rangle_{A_{Ct}}) \\
&+|\Phi^-\rangle_{1,A}(\sigma_{z,A_{Ct}}|\psi_1\rangle_{A_{Ct}})\big)\big(|\Phi^+\rangle_{2,C}|\psi_2\rangle_B + |\Psi^+\rangle_{2,C}(\sigma_{x,B}|\psi_2\rangle_B) + |\Psi^-\rangle_{2,C}(-i\sigma_{y,B}|\psi_2\rangle_B) \\
&+|\Phi^-\rangle_{2,C}(\sigma_{z,B}|\psi_2\rangle_B)\big), \qquad (5.3.5)
\end{aligned}
$$

where the *controlling action qubit* is defined as $|\psi_1\rangle_{A_{Ct}} = \alpha_1|0_A\rangle + \beta_1|1_A\rangle$, and σ_x, σ_y and σ_z the Pauli matrices. With a final restoring unitary transformation U_{rest} on both the tracks B_1, B_2 and the polarization modes H, V according to the information fed forwarded after the Bell state analysis on track 1, A and 2, C, respectively, we will obtain a single photon polarization state running on track B_1 and B_2 (the total dimensionality of the outputs is 4 as the inputs):

$$
\begin{aligned}
|\Psi_{out}\rangle &= |\psi_1\rangle_{A_{Ct}}|\psi_2\rangle = \big(\alpha_1|0_A\rangle + \beta_1|1_A\rangle\big)\big(\alpha_2|H\rangle_B + \beta_2|V\rangle_B\big) \\
&= \alpha_1\alpha_2|H\rangle_{B_1,0_A} + \alpha_1\beta_2|V\rangle_{B_1,0_A} + \beta_1\alpha_2|H\rangle_{B_2,1_A} + \beta_1\beta_2|V\rangle_{B_2,1_A}. \qquad (5.3.6)
\end{aligned}
$$

The complete (and close to deterministic) Bell state analysis setups can be found in [54, 55, 56], and also in [57] a practical method for teleporting optical qubits is given. These experimental schemes can be modified to realize the operations in our setup. The whole scheme to realize the transformation from double to single photon states is given in Fig. 8.

So far we have put together all necessary ingredients of a circuit to transform

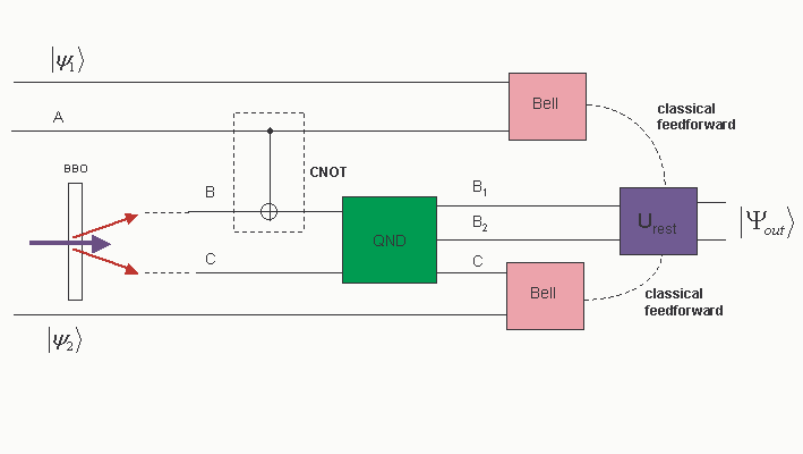

Figure 7: The setup to transform a two-photon state, $|\Psi_{in}\rangle = |\psi_1\rangle|\psi_2\rangle$, to a single photon polarization state running on two different tracks, $|\Psi_{out}\rangle$. We use a BBO to generate an entangled pair $1/\sqrt{2}(|H\rangle_B|H\rangle_C + |V\rangle_B|V\rangle_C)$ on track B and C, and put a single photon $1/\sqrt{2}(|H\rangle_A + |V\rangle_A)$ on track A. The CNOT gate can be a modified version of the cited, and the QND unit is in [53]. The results of two Bell state analysis are sent through the classical channels to where the restoration unitary map U_{rest} is performed. U_{rest} is chosen from a finite set of operations.

the triple photon inputs in Eq. (5.2.1) to the corresponding single photon states. To teleport the triple photon inputs to the corresponding single photon states, we just need to continue the above procedure before the Bell state analysis by adding one more single photon source, $1/\sqrt{2}(|H\rangle_D + |V\rangle_D)$, and two more CNOT gates and parity QNDs. We use a 50-50 beam splitter to split the second single photon into two

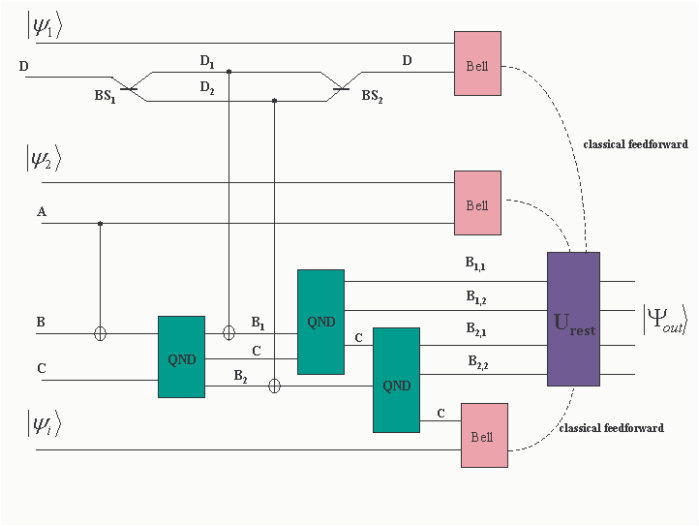

Figure 8: The setup to teleport any symmetric unknown three-photon input state $|\psi_1\rangle|\psi_2\rangle|\psi_i\rangle$, for $i = 1, 2$, to the corresponding single photon state. One more single photon source is used on track D, and it is split by a 50-50 beam splitter BS_1 (and the necessary phase shifters) into two paths to control the respective photon components. Another identical beam splitter BS_2 merges the photon components on track D_1 and D_2 to a single path again.

different paths:

$$|H\rangle_D + |V\rangle_D \rightarrow |H\rangle_{D_1} + |V\rangle_{D_1} + |H\rangle_{D_2} + |V\rangle_{D_2}, \tag{5.3.7}$$

and the photon components running on D_1 (D_2) track controls the photon component on B_1 (B_2) track through an optical CNOT gate. Then, performing the polarization parity QNDs on track B_1, C and B_2, C, respectively, and the necessary bit flips

and phase redressing, we will seperate the photon components on B_1 and B_2 to those on 4 tracks $B_{1,1}$, $B_{1,2}$, $B_{2,1}$ and $B_{2,2}$, and thus obtain the output state which can be factorized into the product of three entangled states (similar to the state in Eq. (5.3.3)). We are now able to teleport 3 unknown qubits together to a single photon polarization state running on 4 different tracks. The complete scheme of the teleportation of the triple-qubit to a single photon state is shown in Fig. 8.

5.4 Optimal POVM implementation circuit

The circuit in Fig. 8 generates the following single photon states as the inputs of the POVM modules to discriminate the data $|\psi_1\rangle$ and $|\psi_2\rangle$:

$$\begin{aligned}
|\Psi'_{i,in}\rangle &= |\Psi_{i,out}\rangle = |\psi_1\rangle_{D_{Ct}}|\psi_2\rangle_{A_{Ct}}|\psi_i\rangle_B \\
&= \big(\alpha_1|0_D\rangle + \beta_1|1_D\rangle\big)\big(\alpha_2|0_A\rangle + \beta_2|1_A\rangle\big)\big(\alpha_i|H\rangle_B + \beta_i|V\rangle_B\big) \\
&= \alpha_1\alpha_2\alpha_i|0_D, 0_A, H_B\rangle + \alpha_1\alpha_2\beta_i|0_D, 0_A, V_B\rangle + \alpha_1\beta_2\alpha_i|0_D, 1_A, H_B\rangle \\
&+ \alpha_1\beta_2\beta_i|0_D, 1_A, V_B\rangle + \beta_1\alpha_2\alpha_i|1_D, 0_A, H_B\rangle + \beta_1\alpha_2\beta_i|1_D, 0_A, V_B\rangle \\
&+ \beta_1\beta_2\alpha_i|1_D, 1_A, H_B\rangle + \beta_1\beta_2\beta_i|1_D, 1_A, V_B\rangle \\
&= \alpha_1\alpha_2\alpha_i|H\rangle_{B_{1,1}} + \alpha_1\alpha_2\beta_i|V\rangle_{B_{1,1}} + \alpha_1\beta_2\alpha_i|H\rangle_{B_{2,1}} \\
&+ \alpha_1\beta_2\beta_i|V\rangle_{B_{2,1}} + \beta_1\alpha_2\alpha_i|H\rangle_{B_{1,2}} + \beta_1\alpha_2\beta_i|V\rangle_{B_{1,2}} \\
&+ \beta_1\beta_2\alpha_i|H\rangle_{B_{2,2}} + \beta_1\beta_2\beta_i|V\rangle_{B_{2,2}}. \qquad (5.4.1)
\end{aligned}$$

With 4 polarization beam splitters (PBS) we can thus obtain the multi-rail single photon signal states running on 8 tracks. Any POVM with n elements Π_i, for $i = 1, \cdots, n$, on such single photon states can be deterministically implemented with at most $3n - 2$ linear optics modules shown in Fig. 4 [38].

The POVM for unambiguously discriminating these states satisfies more condition, $\Pi_1|\Psi'_{2,in}\rangle = \Pi_2|\Psi'_{1,in}\rangle = 0$, so we can use a linear optics scheme, which requires fewer and much simpler modules, to realize the unambiguous discrimination of $|\Psi'_{1,in}\rangle$ and $|\Psi'_{2,in}\rangle$. Such a scheme works with the following unitary map [22],

$$U_{module} = \begin{pmatrix} (I-\Pi_0)^{\frac{1}{2}} & -\Pi_0^{\frac{1}{2}} \\ \Pi_0^{\frac{1}{2}} & (I-\Pi_0)^{\frac{1}{2}} \end{pmatrix}, \tag{5.4.2}$$

which is realizable by one 16×16-port module shown in Fig. 10. This module transforms the signals embeded in a larger space of the double of the signal space dimension, $(|\Psi'_{i,in}\rangle, \mathbf{0})^T$, to the components in two orthogonal output subspaces:

$$U_{module} \begin{pmatrix} |\Psi'_{i,in}\rangle \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} (I-\Pi_0)^{\frac{1}{2}}|\Psi'_{i,in}\rangle \\ \Pi_0^{\frac{1}{2}}|\Psi'_{i,in}\rangle \end{pmatrix}. \tag{5.4.3}$$

The component $(I-\Pi_0)^{\frac{1}{2}}|\Psi'_{i,in}\rangle$ corresponds to the success of the measurement with a probability $P = \langle\Psi'_{i,in}|I-\Pi_0|\Psi'_{i,in}\rangle = \langle\Psi'_{i,in}|\Pi_i|\Psi'_{i,in}\rangle$, and the component $\Pi_0^{\frac{1}{2}}|\Psi'_{i,in}\rangle$ to the inconclusive result, which occurs with a probability $Q = \langle\Psi'_{i,in}|\Pi_0|\Psi'_{i,in}\rangle$. It is easy to verify that $|\Psi'_{1,in}\rangle$ and $|\Psi'_{2,in}\rangle$ are mapped to distingushable orthogonal states in the first subspace, since $\langle\Psi'_{1,in}|I-\Pi_0|\Psi'_{2,in}\rangle = 0$.

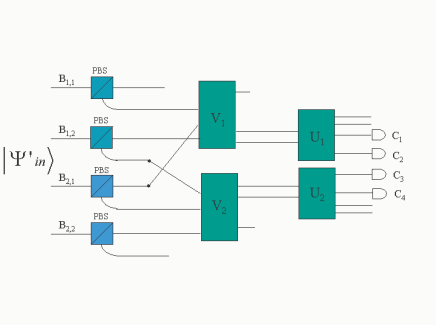

Figure 9: The layout of the optimal POVM for the discrimination of unknown optical qubits. The input $|\Psi'_{in}\rangle$ is the output $|\Psi_{out}\rangle$ in Fig. 8. The polarization beam splitters (PBS) separate the input into the 8 dimensional single photon state in multi-rail representation. The V_i are 3×3-port modules, and U_i 4×4-port modules with two input ports black. Only 4 photon detectors are required to place on the terminals where the useful information is output. At all other terminals (2 of the PBS, 2 of V_i modules and 4 of U_i modules), there are only useless signals contributing to the inconclusiveness. We can set the output in such a pattern: if the detector C_1 or C_3 clicks, we conclude that the unknown input is $|\psi_1\rangle$; and if C_2 or C_4 clicks, the input date must be $|\psi_2\rangle$. From each counter, we detect the photon with a probability 1/12, if the data $|\psi_1\rangle$ and $|\psi_2\rangle$ occur with the same *a priori* probability.

The linear optics circuit to perform U_{module} can be simplified further. We first decompose the inputs in Eq. (5.4.1) into the components in the orthogonal subspaces $\mathcal{H}_1 = \{|0_D, 0_A, V_B\rangle, |0_D, 1_A, H_B\rangle, |1_D, 0_A, H_B\rangle\}$, $\mathcal{H}_2 = \{|1_D, 0_A, V_B\rangle, |0_D, 1_A, V_B\rangle, |1_D, 1_A, H_B\rangle\}$ $\mathcal{H}_3 = \{|0_D, 0_A, H_B\rangle\}$ and $\mathcal{H}_4 = \{|1_D, 1_A, V_B\rangle\}$, respectively. We introduce a unitary

map V_1,

$$\begin{aligned} |\Phi_1\rangle &= \sqrt{\frac{1}{2}}\big(|0_D, 0_A, V_B\rangle - |0_D, 1_A, H_B\rangle\big) \\ |\Phi_2\rangle &= \sqrt{\frac{1}{6}}\big(|0_D, 0_A, V_B\rangle + |0_D, 1_A, H_B\rangle\big) - \sqrt{\frac{2}{3}}|1_D, 0_A, H_B\rangle \end{aligned}$$

$$|\Phi_3\rangle = \sqrt{\frac{1}{3}}\big(|0_D, 0_A, V_B\rangle + |0_D, 1_A, H_B\rangle + |1_D, 0_A, H_B\rangle\big), \tag{5.4.4}$$

in $\mathcal{H}_1$, and another unitary map V_2,

$$\begin{aligned} |\Phi_1'\rangle &= \sqrt{\frac{1}{2}}\big(|1_D, 0_A, V_B\rangle - |1_D, 1_A, H_B\rangle\big) \\ |\Phi_2'\rangle &= \sqrt{\frac{1}{6}}\big(|1_D, 0_A, V_B\rangle + |1_D, 1_A, H_B\rangle\big) - \sqrt{\frac{2}{3}}|1_D, 0_A, V_B\rangle \end{aligned}$$

$$|\Phi_3'\rangle = \sqrt{\frac{1}{3}}\big(|1_D, 0_A, V_B\rangle + |1_D, 1_A, H_B\rangle + |0_D, 1_A, V_B\rangle\big) \tag{5.4.5}$$

in $\mathcal{H}_2$, respectively. These two unitary maps on the modes of the relevant tracks correspond to two simple and identical 3×3-port modules processing the relevant components of the input signals. In the subspaces $\mathcal{H}_1' = \{|\Phi_1\rangle, |\Phi_2\rangle\}$ and $\mathcal{H}_2' = \{|\Phi_1'\rangle, |\Phi_2'\rangle\}$, Π_0 of the optimal POVM is given as a 2×2 matrix [10]:

$$\Pi_0^{(i)} = \begin{pmatrix} -\frac{2}{3}(1 - \sqrt{\frac{\eta_1}{\eta_2}} - \sqrt{\frac{\eta_2}{\eta_1}}) & -\frac{\sqrt{3}}{6}(2 - \sqrt{\frac{\eta_1}{\eta_2}}) \\ -\frac{\sqrt{3}}{6}(2 - \sqrt{\frac{\eta_1}{\eta_2}}) & \frac{2}{3}\sqrt{\frac{\eta_1}{\eta_2}} \end{pmatrix}, \tag{5.4.6}$$

for $i = 1, 2$, and the total Π_0 is the direct sum,

$$\Pi_0 = \Pi_0^{(1)} \oplus \Pi_0^{(2)} \oplus I. \tag{5.4.7}$$

Therefore, the signal components outside $\mathcal{H}_1'$ and $\mathcal{H}_2'$ only contribute to the inconclusive results, and we only need to process the signal components in these two subspaces.

For the *a priori* probabilities $\eta_1 = \eta_2 = 1/2$, i.e., the most difficult situation to discriminate the input data, as well as the optimal POVM obtained in the minimax approach [11], the operator $\Pi_0^{(1)}$ and $\Pi_0^{(2)}$ are therefore reduced to

$$\Pi_0^{(1)} = \Pi_0^{(2)} = \begin{pmatrix} \frac{2}{3} & -\frac{\sqrt{3}}{6} \\ -\frac{\sqrt{3}}{6} & \frac{2}{3} \end{pmatrix}. \tag{5.4.8}$$

The unitary transformations in Eq. (5.4.2) constructed by these two non-unitary operators are, respectively, implemented by two identical circuits consisting of only 3 beam splitters, one of which performs the unitary map,

$$U_{i,1} = \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \tag{5.4.9}$$

which diagonalizes $\Pi_0^{(1)}$ and $\Pi_0^{(2)}$, and the other two of which perform the unitary map in the extended space,

$$U_{i,2} = \begin{pmatrix} \sqrt{\frac{1}{3} - \frac{\sqrt{3}}{6}} & & -\sqrt{\frac{2}{3} + \frac{\sqrt{3}}{6}} & \\ & \sqrt{\frac{1}{3} + \frac{\sqrt{3}}{6}} & & -\sqrt{\frac{2}{3} - \frac{\sqrt{3}}{6}} \\ \sqrt{\frac{2}{3} + \frac{\sqrt{3}}{6}} & & \sqrt{\frac{1}{3} - \frac{\sqrt{3}}{6}} & \\ & \sqrt{\frac{2}{3} - \frac{\sqrt{3}}{6}} & & \sqrt{\frac{1}{3} + \frac{\sqrt{3}}{6}} \end{pmatrix}. \tag{5.4.10}$$

Through all these unitary transformations the different input signal components from $|\Psi_{1,in}'\rangle$ and $|\Psi_{2,in}'\rangle$, respectively, have been mapped to the orthogonal states. Adding

one more 50-50 beam splitter to separate the signals from the different inputs, we realize the target to discriminate the data input: the input data is determined to be $|\psi_1\rangle$ if the output photon is recorded by one single photon detector and $|\psi_2\rangle$ if the output photonis recorded by the other. In Fig. 9 we use U_i to represent a whole package of these unitary maps including $U_{i,1}$ and $U_{i,2}$.

By a straightforward calculation considering Eq. (5.4.2) and (5.4.3), we see that in one of the photon detectors in Fig. 9 there is an average probability of 1/12 to detect the photon. With the detection of the photon, we can draw the conclusion about which the input data is. Adding together the contribution of another photon detector placed at one terminal of the other U_i module, we obtain the optimal average success probability 1/6 in the discrimination of a pair of unknown qubits [10]. The layout of the optimal POVM implementation is given in Fig. 9.

5.5 Unknown coherent state discriminator—quantum database searching

We demonstrate the principle of quantum database searching with the simplest case of identifying only two states $|\alpha_1\rangle$ and $|\alpha_2\rangle$. The comparison of states can be realized by a map

$$\mathcal{K} = c \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}, \tag{5.5.1}$$

which acts on the input $(\alpha_0^*, \alpha_1^*, \alpha_2^*)^T$. The largest parameter, $c_{max} = \frac{1}{\sqrt{3}}$, is determined by making the eigenvalues of $\mathcal{K}\mathcal{K}^\dagger$ or $\mathcal{K}^\dagger\mathcal{K}$ less than or equal to 1. We then apply the following unitary map for the identification of $|\alpha_0\rangle$:

$$\vec{\beta}^* = \mathcal{U}\vec{\alpha}^* = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ \sqrt{\frac{1}{3}} & -\sqrt{\frac{1}{3}} & 0 & 0 & \sqrt{\frac{1}{6}} & -\sqrt{\frac{1}{6}} \\ \sqrt{\frac{1}{3}} & 0 & -\sqrt{\frac{1}{3}} & 0 & -\sqrt{\frac{1}{6}} & \sqrt{\frac{1}{6}} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & \sqrt{\frac{1}{3}} & \sqrt{\frac{1}{3}} \\ \frac{1}{3} & \frac{2+\sqrt{6}}{6} & \frac{2-\sqrt{6}}{6} & 0 & -\sqrt{\frac{1}{3}} & 0 \\ \frac{1}{3} & \frac{2-\sqrt{6}}{6} & \frac{2+\sqrt{6}}{6} & 0 & 0 & -\sqrt{\frac{1}{3}} \end{pmatrix} \begin{pmatrix} \alpha_0^* \\ \alpha_1^* \\ \alpha_2^* \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{(\alpha_0^* - \alpha_1^*)}{\sqrt{3}} \\ \frac{(\alpha_0^* - \alpha_2^*)}{\sqrt{3}} \\ \beta_4^* \\ \beta_5^* \\ \beta_6^* \end{pmatrix}. \quad (5.5.2)$$

If there is at least one photon detected form the third output port of the circuit corresponding to this map, the input $|\alpha_0\rangle$ will be identified to be $|\alpha_1\rangle$; similarly, it will be $|\alpha_2\rangle$ if at least one photon is detected from the second output port. Except for the output $|\gamma\rangle = |\frac{\alpha_1 - \alpha_2}{\sqrt{3}}\rangle$ or $|\frac{\alpha_2 - \alpha_1}{\sqrt{3}}\rangle$ consumed in the detection to identify the unknown data, the remaining output states $|\beta_4\rangle$, $|\beta_5\rangle$ and $|\beta_6\rangle$, which are generated through a non-unitary map

$$\begin{pmatrix} \beta_4^* \\ \beta_5^* \\ \beta_6^* \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2+\sqrt{6}}{6} & \frac{2-\sqrt{6}}{6} \\ \frac{1}{3} & \frac{2-\sqrt{6}}{6} & \frac{2+\sqrt{6}}{6} \end{pmatrix} \begin{pmatrix} \alpha_0^* \\ \alpha_1^* \\ \alpha_2^* \end{pmatrix}, \quad (5.5.3)$$

can be well preserved in delay lines. If we input them, together with another prepared $|\gamma\rangle$, to the same circuit but from the inverse direction, the identified data $|\alpha_0\rangle$, as well as the reference states $|\alpha_1\rangle$, $|\alpha_2\rangle$, will be restored from the initial input ports as

the result of the $\mathcal{U}^{\dagger}$ operation. In the case that $|\alpha_0\rangle$ is input with the equal *a prior* probabilities as $|\alpha_1\rangle$ and $|\alpha_2\rangle$, the success probability of this identification process is

$$P_{succ} = 1 - e^{-\frac{|\alpha_1 - \alpha_2|^2}{3}}, \tag{5.5.4}$$

which is as large as the best probability of identifying $|\alpha_1\rangle$ and $|\alpha_2\rangle$ in [36]. Provided that the distance, $|\alpha_1 - \alpha_2|$, between two states is large enough, a setup like this will realize a near deterministic identification, in which the identified input data and the reference states in the database can be also restored for the further processing and the second round searching.

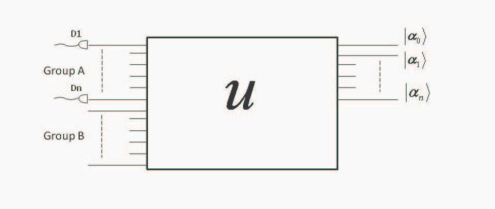

Figure 10: Non-destructive quantum database searching setup. The unidentified data $|\alpha_0\rangle$ is sent together with the reference states to the circuit, which implemenets the unitary operation $\mathcal{U}$. Half of the outputs in group A are measured to determine their identities, and the other half in group B are kept in delay lines. After the measurement results are compared, another set of the determined states are input to the ports of group A, while the outputs of group B are sent back to the circuit. The identified data $|\alpha_0\rangle$ and the reference states are thus retrieved from the initial input ports. Only photodiodes that are unable to resolve photon numbers are required in the detection.

For the general situation of arbitrary number of states, the similar contraction map can be given as

$$\mathcal{K} = \frac{1}{\sqrt{N+1}} \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{pmatrix} \tag{5.5.5}$$

The corresponding setup performs the database searching among the set $\{|\alpha_1\rangle, |\alpha_2\rangle, \cdots, |\alpha_N\rangle\}$. Two group of outputs are illustrated in Fig.10: the coherent states in group A will be consumed in the detection for identifying the input data, while those in group B are untouched. The consumed coherent states in group A can be replenished from the extra copies of $|\alpha_i\rangle$ $(i = 1, \cdots, N)$ processed by the same circuit ahead of the searching. The maximum number of the required linear optical elements for the circuit grows quadratically with the volume of the database N as $(N+1)(2N+1)$.

Chapter VI

6 Conclusions

Unknown state discrimination and its physical realization are challenging problems in quantum information processing. Because the only information available in discriminating a pair of unknown states is the permutation symmetry from using the reference copies of the states, the space structure of the inputs can be very complicated, and the realization of such operations in physical systems also involves sophisticated techniques. If the inputs constructed with the unknown states are prepared with some different *a prior* probabilities, the problem of optimally discriminating unknown states will be even harder.

We adopt two approaches to study the theoretical problem of unknown qubit discrimination. First, we design a universal programmable discriminator that directly processes the inputs prepared with multiple copies of the reference states as the program part of the setup. The data (unknown qubits) are discriminated with the permutation symmetry of the program and data parts. We find the optimal measurement for the USD of the general inputs, which are prepared with the different *a prior* probabilities. In the different ranges of *a prior* probability, the optimal measurement takes the form of PVM and POVM, respectively. In the limit of infinity copies of ref-

erence states, the optimal measurement is reduced to a pure PVM or von Neumann measurement.

The second approach to discriminating unknown states is dephasing the unknown symmetric inputs constructed with the references and the data to the known mixed states. The dephased or averaged input states inherit the permutation symmetry from the original ones, and we can find an invariant of the sum of inner products of the basis vectors if the program parts have the same number of copies. With the invariant it is straightforward to find the Jordan basis inner products of the input state space. Then the optimal unambiguous and the minimum-error discrimination strategies of the dephased inputs can be found for the general case of n copies of reference and m copies of data.

We also discuss how to implement the USD of unknown states by presenting a method to realize the necessary POVMs. This method applies to USD of quantum states in the general situation.

The second half of the dissertation concerns the physical realization of unknown quantum state discrimination. To study the discrimination of unknown optical qubits and unknown coherent states, we develop the general methods to process these two types of photonic states. The general linear transformation and general POVM on single photon states are realized with linear optics (together with photon detection in implementing POVMs). We demonstrate a correspondence between the transforma-

tion of single photon states and those of coherent state products, and show that the same linear optical setup can be used to perform the different tasks involving these two different types of states. These methods are also applicable to other quantum information processing tasks.

Finally we describe two setups to realize the discrimination of unknown optical qubits and unknown coherent sates, respectively. In the implementation of unknown optical qubit discrimination, we teleport the input of three photon states to a single photon state in which-path space, and then use a linear optical circuit to perform the optimal POVM to identify the unknown data. The unknown coherent state discrimination is much more efficient if their difference is large enough. The setup of unknown coherent state discrimination can be developed to a non-destructive quantum database searching system.

There are still many interesting further studies of unknown state discrimination, such as the discrimination of the unknown signals encoded in other states than single photon and coherent states. Unknown quantum state discrimination could be also applied in many other areas of quantum information processing. These problems would be explored in the future works.

Appendix

A Appendix A: Procedure to Obtain Symmetric Closed Basis Vector Chains

In this appendix we give a procedure of obtaining the closed basis vector chains discussed in chapter II. The *mirror symmetry*, $\langle v_i|v'_j\rangle = \langle v'_i|v_j\rangle$, for any couple of indices i and j, exists for the input with $n_1 = n_3$.

Step 1: Generating the closed basis vector chains of any fixed $N \equiv n_1 + n_2 + n_3$.

In H_1, since each term of a basis vector in this representation has the same digit n_3, we start from $n_3 = 0$ and obtain the corresponding basis vector (that is to find out all the combinations of non-zero intergers that added up to be N). Then we increase n_3 by 1 each time till $n_3 = n$ and obtain in this way all basis vectors in this closed chain. Similarly we obtain the corresponding chain in H_2, each element of which has the same first digit n_1 for all terms.

Step 2: Permutation of the basis vectors, which is given by $[n_1, n_2, n_3]$ representation, in the obtained closed basis chains.

Remember that $[i, j, k] \equiv \sqrt{\frac{C_n^i C_m^j}{C_{n+m}^{i+j}}}|e_i\rangle_A|e_j\rangle_B|e_k\rangle_C$ in H_1 and $[k, j, i] \equiv \sqrt{\frac{C_n^i C_m^j}{C_{n+m}^{i+j}}}|e_k\rangle_A|e_j\rangle_B|e_i\rangle_C$ in H_2. Pick out in a closed chain all couples of basis vectors carrying $[l_1, l_2, l_3]$ and

$[l_3, l_2, l_1]$ terms (the terms with n_1 and n_3 interchanged), which are guranteed to exist by the fact that N is constant for any of a closed chain, and let the basis vector with $[l_1, l_2, l_3]$ be $|v_i\rangle$, and that with $[l_3, l_2, l_1]$ be $|v_{i+k}\rangle$, where i, k are the integers within the range of the size for a closed chain, in H_1. Correspondingly in H_2, we set the basis vector carrying $[l_3, l_2, l_1]$ to be $|v'_i\rangle$ instead and that carrying $[l_1, l_2, l_3]$ $|v'_{i+k}\rangle$.

Then we proceed from other terms in the basis vectors to obtain two whole chains with the *mirror symmetry*. If the number of program copies n_A and n_C are unequal, we cannot guarantee the existence of the couples in the form $\{[l_1, l_2, l_3], [l_3, l_2, l_1]\}$, and the *mirror symmetry* of the basis vectors doesn't exist.

With a not so large N, we here give an example of how to perform the procedure. For the case of 4 copies of program and 1 copy of data in the input states, suppose that we need to obtain the chains of $N = 4$ with the *mirror symmetry*.

There are 5 elements in the chains as we studied previously. Starting from $n_3 = 0$ and $n_1 = 0$, we see that the couple $\{[l_1, l_2, l_3], [l_3, l_2, l_1]\}$ in the basis vectors is $\{[4, 0, 0], [0, 0, 4]\}$. Adding the rest terms in these basis vectors, we set $|v_1\rangle = [4, 0, 0] + [3, 1, 0]$, $|v_2\rangle = [0, 0, 4]$ in H_1, and $|v'_1\rangle = [0, 0, 4] + [0, 1, 3]$, $|v'_2\rangle = [4, 0, 0]$ in H_2. These two couples of basis satisfy $\langle v_1|v'_2\rangle = \langle v'_2|v_1\rangle = \sqrt{\frac{C_4^4 C_1^0}{C_5^4}}\sqrt{\frac{C_4^0 C_1^0}{C_5^0}}$.

The basis in H_2 carrying $[3, 1, 0]$ is $[3, 0, 1] + [3, 1, 0]$, and we set it as $|v'_3\rangle$. In H_1 the basis carrying $[0, 1, 3]$ is $[1, 0, 3] + [0, 1, 3]$, which is set as $|v_3\rangle$. We have

$\langle v_1|v_3'\rangle = \langle v_1'|v_3\rangle = \sqrt{\frac{C_4^3 C_1^1}{C_5^4}}\sqrt{\frac{C_4^0 C_1^1}{C_5^1}}$. Then we set $|v_4\rangle = [3,0,1] + [2,1,1]$ and $|v_4'\rangle = [1,0,3] + [1,1,2]$, and there is $\langle v_3|v_4'\rangle = \langle v_3'|v_4\rangle = \sqrt{\frac{C_4^1 C_1^0}{C_5^1}}\sqrt{\frac{C_4^3 C_1^0}{C_5^3}}$.

Finally we consider the terms with $[2,1,1]$ and $[1,1,2]$; in H_1 we set $|v_5\rangle = [2,0,2] + [1,1,2]$ and in H_2 we set $|v_5'\rangle = [2,0,2] + [2,1,1]$, and $\langle v_4|v_5'\rangle = \langle v_4'|v_5\rangle = \sqrt{\frac{C_4^2 C_1^1}{C_5^3}}\sqrt{\frac{C_4^1 C_1^1}{C_5^2}}$.

Thus we obtain the following two closed chains having the *mirror symmetry*.

$$\begin{aligned}
|v_1\rangle &= [4,0,0] + [3,1,0], \\
|v_2\rangle &= [0,0,4], \\
|v_3\rangle &= [1,0,3] + [0,1,3], \\
|v_4\rangle &= [3,0,1] + [2,1,1], \\
|v_5\rangle &= [2,0,2] + [1,1,2]; \qquad \text{(A.0.1)}
\end{aligned}$$

$$\begin{aligned}
|v_1'\rangle &= [0,0,4] + [0,1,3], \\
|v_2'\rangle &= [4,0,0], \\
|v_3'\rangle &= [3,0,1] + [3,1,0], \\
|v_4'\rangle &= [1,0,3] + [1,1,2], \\
|v_5'\rangle &= [2,0,2] + [2,1,1]. \qquad \text{(A.0.2)}
\end{aligned}$$

Even if N is very large, we can search out all these couples with symmetric inner product and perform the above procedure by a computer program.

B Appendix B: Calculation of Invariant Sum of Basis Vector Inner Products

With the $[n_1, n_2, n_3]$ symbol defined in section 3.2, it is very easy to calculate the invariants, $S_N = \sum_i \langle v_i|v_i'\rangle = \sum_i \langle \phi_i|\phi_i'\rangle$, for the pairs of closed basis vector chains, given arbitrary n program and m data copies in the input states. In a pair of closed chains with the *mirror symmetry*, only the terms in the form of $[i, j, i]$ ($n_1 = n_3$) contribute to this invariant sum, because $|v_i\rangle$'s and $|v_i'\rangle$'s carrying the terms in all other forms are orthogonal, so it is obtained by picking out the terms of $[i, j, i]$ satisfying $i \leq n$, $j \leq m$ and summing up the square of the coefficients absorbed in these square brackets. It can be done easily by a computer program for any pair of closed chains.

Here we use the situation of 4 copies of program and 3 copies of data in the input states for an example. We calculate the invariant sums for $N = 4, 5, 6, 7$ chains with 5 elements together as shown previously.

For $N = 4$ the contribution to the sum come from the terms $[2, 0, 2]$ and $[1, 2, 1]$, so the invariant sum is

$$\sum_i \langle \phi_i|\phi_i'\rangle = \sum_i \langle v_i|v_i'\rangle = \frac{C_4^2 C_3^0}{C_7^2} + \frac{C_4^1 C_3^2}{C_7^3} = \frac{22}{35}. \tag{B.0.1}$$

For $N = 5$ the contribution to the sum come from the terms $[2, 1, 2]$ and $[1, 3, 1]$,

so the invariant sum is

$$\sum_i \langle \phi_i | \phi_i' \rangle = \sum_i \langle v_i | v_i' \rangle = \frac{C_4^2 C_3^1}{C_7^3} + \frac{C_4^1 C_3^3}{C_7^4} = \frac{22}{35}. \tag{B.0.2}$$

For $N = 6$ the contribution to the sum come from the terms $[2, 2, 2]$ and $[3, 0, 3]$, so the invariant sum is

$$\sum_i \langle \phi_i | \phi_i' \rangle = \sum_i \langle v_i | v_i' \rangle = \frac{C_4^2 C_3^2}{C_7^4} + \frac{C_4^3 C_3^0}{C_7^3} = \frac{22}{35}. \tag{B.0.3}$$

For $N = 7$ the contribution to the sum come from the terms $[3, 1, 3]$ and $[2, 3, 2]$, so the invariant sum is

$$\sum_i \langle \phi_i | \phi_i' \rangle = \sum_i \langle v_i | v_i' \rangle = \frac{C_4^3 C_3^1}{C_7^4} + \frac{C_4^2 C_3^3}{C_7^5} = \frac{22}{35}. \tag{B.0.4}$$

All these pairs of chains with 5 elements have the same invariant sum. By induction on n and m, we see that this invariant sum is determined by the size of the closed basis vector chains.

References

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

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

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

[4] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[5] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[6] A. Peres, Phys. Lett. A **128**, 19 (1988).

[7] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).

[8] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[9] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson and J. Jeffers, Phys. Rev. Lett. **96**, 070401 (2006).

[10] J. Bergou and M. Hillery, Phys. Rev. Lett. **94**, 160501 (2005).

[11] C. Zhang, M. Ying and B. Qiao, Phys. Rev. A **74**, 042308 (2006).

[12] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[13] M. Hillery, V. Buzek and M. Ziman, Phys. Rev. A **65**, 022301 (2002).

[14] M. Dusek and V. Buzek, Phys. Rev. A **66**, 022112 (2002).

[15] J. Fiurasek, M. Dusek and R. Filip, Phys. Rev. Lett. **89**, 190401 (2002).

[16] J. Fiurasek and M. Dusek, Phys. Rev. A **69**, 032302 (2004).

[17] J. Soubusta, A. Cernoch, J. Fiurasek and M. Dusek, Phys. Rev. A **69**, 052321 (2004).

[18] G. M. D'Ariano and P. Perinotti, Phys. Rev. Lett. **94**, 090401 (2005).

[19] B. He and J. Bergou, Phys. Lett. A **359**, 103 (2006).

[20] M. A. Neumark, Izv. Akad. Nauk. SSSR, Ser. Mat. **4**, 277 (1940).

[21] J. Bergou, U. Herzog and M. Hillery, *Discrimination of quantum states*, Lecture Notes in Physics, **649** (Springer, Berlin, 2004), p. 417.

[22] B. He and J. Bergou, Phys. Lett. A **356**, 306 (2006).

[23] A. Hayashi, M. Horibe and T. Hashimoto, Phys. Rev. A **73**, 012328 (2006).

[24] A. Hayashi, T. Hashimoto and M. Horibe, Phys. Rev. A **72**, 032325 (2005).

[25] J. Bergou, V. Buzek, E. Feldman, U. Herzog and M. Hillery, Phys. Rev. A **73**, 062334 (2006).

[26] B. He and J. Bergou, Phys. Rev. A **75**, 032316 (2007).

[27] P. X. Gallagher and R. J. Proulx, in *Contributions to Algebra*, Bass, Cassidy, and Kovacic eds. (Academic Press, New York, 1977).

[28] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).

[29] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[30] M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[31] P. Törmä and S. Stenholm, Phys. Rev. A **54**, 4701 (1996).

[32] P. Törmä, S. Stenholm and I. Jex, Phys. Rev. A **52**, 4853 (1995).

[33] I. Jex, S. Stenholm and A. Zeilinger, Opt. Commun. **117**, 95 (1995).

[34] S. J. van Enk, Phys. Rev. A **66**, 042313 (2002).

[35] E. Anderson, M. Curty and I. Jex, Phys. Rev. A **74**, 022304 (2006).

[36] M. Sedlak, M. Ziman, O. Pribyla, V. Buzek, and M. Hillery, Phys. Rev. A **76**, 022326 (2007).

[37] L. Bartuskova, A. Cernoch, J. Soubusta and M. Dusek, Phys. Rev. A **77**, 034306 (2008).

[38] B. He, J. Bergou and Z.-Y. Wang, Phys. Rev. A **76**, 042326 (2007).

[39] B. He and J. Bergou, Phys. Rev. A **77**, 053818 (2008).

[40] J. Calsamiglia, Phys. Rev. A **65**, 030301(R) (2002).

[41] R. Bhatia, *Matrix Analysis*, (Springer, New York, 1997).

[42] K. Kraus, *Lecture Notes: States, Effects and Operations*, (Springer, New York, 1983).

[43] G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **86**, 4195 (2001).

[44] F. Buscemi, G. M. D'Ariano and M. F. Sacchi, Phys. Rev. A **68**, 042113 (2003).

[45] S. E. Ahnert and M. C. Payne, Phys. Rev. A **71**, 012330 (2005).

[46] P. van Loock and N. Lütkenhaus, Phys. Rev. A **69**, 012302 (2004).

[47] J. Watrous, CPSC 701 Lecture Notes: *Theory of Quantum Information*, University of Waterloo.

[48] J. Bergou and M. Orszag, J. Opt. B **24**, 384 (2007).

[49] T. Probst-Schendzielorz, A. Wolf, M. Freyberger, I. Jex, B. He and J. Bergou, Phys. Rev. A **75**, 052116 (2007).

[50] B. He, J. Bergou and Y. Ren, Phys. Rev. A **76**, 032301 (2007).

[51] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[52] Z.-Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J. Du, T. Yang and J.-W. Pan, Phys. Rev. Lett. **94**, 030501 (2005).

[53] K. Nemoto and W. J. Munro, Phys. Rev. Lett **93**, 250502 (2004).

[54] P. Walther and A. Zeilinger, Phys. Rev. A **72** 010302 (R) (2005).

[55] N. K. Langford, T. J. Weinhold, R. Prevedel, A. Gilchrist, J. L. O'Brien, G. J. Pryde and A. G. White, Phys. Rev. Lett. **95**, 210504 (2005).

[56] C. Schuck, G. Huber, C. Kurtsiefer and H. Weinfurter, Phys. Rev. Lett. **96**, 190501 (2006).

[57] Y.-H. Kim, S. P. Kulik and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).