Generation of multidimensional Bell states in photonics

Quandela Internship Report

September 2023 - February 2024

Student:

Paul Bagourd

Swiss Federal Institute of Technology

Under the guidance of :

Dr Boris Bourdoncle, Quantum Scientist at Quandela

Quandela

Contents

1 Presentation **2**

2 The setting **3**
2.1 Notations . . . 3
2.2 The optical network . . . 3
2.3 Fock space . . . 3
2.4 The linear transformation . . . 3
2.5 Amplitudes of probability . . . 4
2.6 Choosing an encoding . . . 4
2.7 Logical quantum states . . . 5
2.8 Auxiliary photons . . . 5
2.9 d-rail encoding . . . 5
2.10 Post-selection and heralding . . . 6
2.11 A proof of impossibility . . . 7

3 A first proof of the feasibility therem **9**
3.1 The feasibility theorem . . . 9
3.2 Towards a more general theorem . . . 12
3.3 Example with post-selected Bell state with $a = 0$ . . . 12

4 A second proof of the feasibility theorem **14**

5 Discussion **17**
5.1 Comparing the first and second method . . . 17
5.2 Improving success probability . . . 17
5.2.1 optimising on the free parameters . . . 17
5.2.2 Multiple heralding signals . . . 18
5.3 Generalisation to more qudits . . . 18

6 Implementations for standard Bell states **19**
6.1 Using first method . . . 19
6.2 Using second method . . . 19

7 Conclusions **21**

1 Presentation

This paper is the report of my internship at Quandela from September to February 2024 as part of the Quandela theory team. It is the result of a nice collaboration with Grégoire de Gliniasty and Sébastien Draux, under the supervision of Boris Bourdoncle. I thank them very much for their time and for sharing their knowledge. I am also thankful to Hugo Thomas who greatly helped with Julia programming language. Finally, I thank the whole Quandela team for their enthusiasm and welcome.
The goal of my internship was to generate generalised multi-dimensional Bell states in post-selection and heralding using SPS (single photon sources) and PNRD (photon number resolving detector). The development of a general mathematical framework appeared to be relevant, this paper presents the results we established. More precisely, it presents two approaches for generating logical qudit states in post-selection and heralding using SPS and PNRD.

2 The setting

2.1 Notations

- We will sometimes use the notation $[n) = \{0, \ldots, n-1\}, n \in \mathbb{N}$.
- If l_i denote the rows of a matrix for $i = 1, \ldots, n$, we will use the shortcut $(l_1, \ldots, l_n)$ for the matrix $(l_1^T, \ldots, l_n^T)^T$.

2.2 The optical network

Let us briefly summarize the functioning of Ascella, the single-photon-based quantum computing platform of Quandela detailed in [8]. Photons generated via quantum dots (Single Photon Sources) enter the optical network $\mathcal{A}$ constituted of parametrized beam splitters and phase shifters. Once the quantum operations (superpositions and entanglements) are performed, photons are detected by SPD (Single Photon Detectors). Depending on a suitable ordering and parameterization of the beamsplitters and phase shifters, establishing the statistics of the detected photons conditionally on the input photons can constitute a logical computation. Hence, we investigate for such suitable orderings and parametrisations.

2.3 Fock space

Photons as quantum particles are described by creation operators. Therefore, as explained in [7], Fock states in the Hilbert space of N photons on m modes (here optical fibers) are described by

$$|n_1 \ldots n_N\rangle_{\mathcal{F}} = \prod_{i=1}^{m} \frac{\left(a_i^\dagger\right)^{n_i}}{\sqrt{n_i!}} |vac\rangle$$

2.4 The linear transformation

In linear optics, systems described by Hamiltonians preserve the overall photon number. Hence, an optical network $\mathcal{A}$ acting on m modes and involving c input photons is described by a linear transformation written as a complex matrix

$$A = \begin{bmatrix} a_{0,0} & \ldots & a_{0,c-1} \\ \vdots & & \vdots \\ a_{m-1,0} & \ldots & a_{m-1,c-1} \end{bmatrix}$$

A acts on the modes with creation operators as described by the formula explained in [7]

$$\mathcal{A} : |\psi_{in}\rangle = |n_1 \dots n_N\rangle_{\mathcal{F}} = \prod_{i=1}^{m} \frac{\left(a_i^\dagger\right)^{n_i}}{\sqrt{n_i!}} |vac\rangle$$

$$\longmapsto |\psi_{out}\rangle = \mathcal{A} |n_1 \dots n_N\rangle_{\mathcal{F}} \coloneqq \prod_{i=1}^{m} \frac{1}{\sqrt{n_i!}} \left(\sum_{j=1}^{n} U_{i,j} a_i^\dagger \right)^{n_i} |vac\rangle$$

inducing the amplitudes of probability given in the formula below 2.1.

Remark 2.1. *We don't require the matrix to be unitary here. A can be unitarised afterward, decreasing the success probability.*

2.5 Amplitudes of probability

Let $ones(n) = (1, \dots, 1)$ be the tuple of ones of size n and let us define the following maps:

$$conc : tuple_1, \dots, tuple_n \longrightarrow (tuple_1, \dots, tuple_n)$$

and

$$\mathcal{N} : (n_0, ..., n_{m-1}) \longrightarrow conc(ones(n_0), \dots, ones(n_{m-1}))$$

Moreover let $w! = \prod_i w_i!$ for any tuple w.
For a given input of photons $\mathbf{In} = (n_0, ..., n_{c-1}) \in \Omega$ at the optical network and a given output pattern to be detected $\mathbf{Out} = (m_0, ..., m_{m-1}) \in \Omega$, let $\tilde{A}$ be the matrix where we duplicated the $i-th$ line of A $m_i - 1$ times and columns $n_j - 1$ of A times. The probability of detecting the output pattern **Out** given the input **In** is given by

$$\langle \mathbf{Out}| A |\mathbf{In}\rangle = \frac{\mathsf{Per}\left(\tilde{A}[\mathcal{N}(m_0, ..., m_{m-1})][\mathcal{N}(n_0, ..., n_{c-1})]\right)}{\sqrt{(m_0, ..., m_{m-1})!}\sqrt{(n_0, ..., n_{c-1})!}} \tag{2.1}$$

This formula is the generalisation of the classical case described in [1] as follows: suppose there are n balls and n final locations, and ball i has probability a_{ij} of landing at location j. Then the probability of obtaining one ball in each of the n locations is $\mathsf{Per}\,(A)$.

2.6 Choosing an encoding

The encoding links the abstract logical space and the physics of the photons. Logically speaking, a quantum state is described by logical qudits, an abstract vector lying in a Hilbert space. Moreover, a logical quantum gate is a logical operation applied on multiple logical qudits. We say that a physical quantum state encodes a logical qudit when its physical description matches the definition of a given encoding. There is a lot of more or less general possible encoding such as photon number encoding or dual-rail encoding, all with advantages and drawbacks.

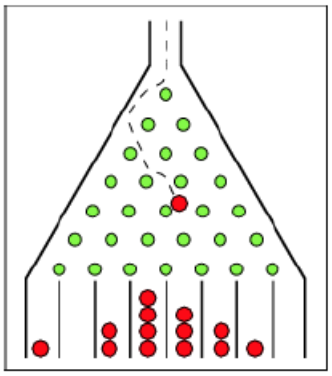


Figure 1: Galton's board, a simple "computer" to output samples from the binomial distribution. From MathWorld.

2.7 Logical quantum states

From the encoding, we can define the abstract logical quantum state

$$\sum_{k_1 \dots k_q = 0}^{d-1} c_{k_1 \dots k_q} \left| k_1 \dots k_q \right\rangle_{\mathcal{L}}$$

where

- d is the dimension of the logical qudit
- q is the number of logical qudits

2.8 Auxiliary photons

To generate such logical quantum states, we might need additional photons at the input. Hence we will denote by a the number of auxiliary photons. This implies that the number of input photons in the optical network is $q + a$.

2.9 d-rail encoding

Here we present the d-rail encoding which seems well adapted to the current photonic technology using single-photon resolving detectors. The d-rail encoding on the modes proceeds as follows:

$$\left| k_1 \dots k_q \right\rangle_{\mathcal{L}} = \prod_{i=1}^{q} a^{\dagger}_{k_i + (i-1)\cdot d} \left| vac \right\rangle_{\mathcal{F}}$$

In this encoding, the transformation can be read as

$$A = \begin{bmatrix} a_{0,0} & \cdots & a_{0,qd-1} & a_{0,qd} & \cdots & a_{0,qd+a-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{qd-1,0} & \cdots & a_{qd-1,qd-1} & a_{qd-1,qd} & \cdots & a_{qd-1,qd+a-1} \\ a_{qd,0} & \cdots & a_{qd,qd-1} & a_{qd,qd} & \cdots & a_{qd,qd+a-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{qd+a-1,0} & \cdots & a_{qd+a-1,qd-1} & a_{qd+a-1,qd} & \cdots & a_{qd+a-1,qd+a-1} \end{bmatrix}$$

where we made the separation between the modes of the computational space and the auxiliary space apparent.

2.10 Post-selection and heralding

The generalised d-dimensional Bell state is defined as follows

$$B_d = \sum_{k=0}^{d-1} c_k \left|kk\right\rangle$$

We call it generalised because the coefficients corresponding to each ket can take any complex value up to normalisation, contrary to "standard" d-dimensional Bell state where the coefficient's values are $\frac{1}{\sqrt{d}}$.

Let us take for instance the standard Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. In $2-$rail encoding, this state can be described on 4 modes with 4 single-photon detectors, via Fock space notation. Indeed, given an interferometer on 4 modes with 4 single-photon detectors at the end of each modes, we say that the interferometer generates the Bell state in post-selection if whenever the output pattern (using Fock space notation) detected lies in the encoding space (hence called a valid pattern, here $\left|1010\right\rangle_{\mathcal{F}}, \left|0110\right\rangle_{\mathcal{F}}, \left|0101\right\rangle_{\mathcal{F}}, \left|1001\right\rangle_{\mathcal{F}}$), the relative probability of such a pattern among the probability of all valid patterns corresponds to the modulus of the coefficient associated to the encoding described by the state.

Post-selecting a state is useful for establishing for instance quantum statistics, to describe the entanglement of a photonic system using self-testing protocols. However, since the state is generated only up to its detection, it is automatically destroyed and we cannot use it for further computations. Hence, to generate a state without destroying it one should herald it via some photon signals occurring on additional modes. For instance, would it be possible to generate an entangled 4 photons state on an interferometer with $4+2=6$ modes such that the statistics on the modes 0 to 3 conditionally on the detection of 2 photons on modes 4 and 5 actually corresponds to the statistics of the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ in post-selection ? That is, can we herald a "simulation" of the Bell state via additional modes? The answer is affirmative, but we should be careful about the number of auxiliary photons involved and about the probability of success of such a generation.

2.11 A proof of impossibility

We now present a smooth proof of the impossibility to post-select the generalised d-dimensional Bell state

$$B_d = \sum_{k=0}^{d-1} c_k \, |kk\rangle$$

in d-rail encoding with no auxiliary photons and $d \geq 3$. The idea of this proof due to Grégoire de Gliniasty allows us to prove the generalised theorem 3.1 that will be presented in the next section.

Proof. Let Enc be the set of tuples that lie in the logical dual-rail encoding space. Following the rules of the previous paragraph 2.5, A should satisfy a system of $|Enc| = d^2$ non-linear equations with $2 \cdot (2d) = 4d$ free complex variables :

$$\begin{aligned} \forall (k,l) \in Enc : \alpha_{k,l} =& c_k \delta_{k,l-d} \\ =& Per(\tilde{A}[k,l][0,d]) \end{aligned}$$

Let $E = (\mathbb{C}^2, <\cdot,\cdot>)$ be a Hilbert space with the usual scalar product and let us define $e_i \coloneqq (a_{i,0}, a_{i,d}) \in E, i \in \{0, \dots, 2d-1\}$. Moreover, let us define :

$$\begin{aligned} f :& E \times E \to \mathbb{C} \\ & (x,y) \mapsto x_1 y_2 + x_2 y_1 \end{aligned}$$

and for all $k = 0, \dots, d-1$:

$$\begin{aligned} f_k :& E \to \mathbb{C} \\ & y \mapsto f(e_k, y) = a_{k,0} y_2 + a_{kd} y_1 \end{aligned}$$

E is a $\mathbb{C}$-vector space of dimension 2 and we can check that f_k is a linear map on E. Hence by the rank theorem, we have :

$$2 = dim(E) = dim(ker(f_k)) + rk(f_k)$$

Moreover, since A_G creates B_d by post-selection, the permanent specifications from 2 imposes that for all $k = 0, \dots, d-1$ and for all $l = d, ..., 2d-1$

$$f_k(e_l) = c_k \delta_{k,l-d} \tag{2.2}$$

Let us use the notation $E_k \coloneqq ker(f_k)$ for $k = 0, \dots, d-1$. Expression 2.2 shows that A_G should satisfy $rank(f_k) \geq 1$ and $1 \leq dim(E_k) \leq dim(E) - 1 = q + a - 1$, with $rank(f_k) > 1$ only if $a > 0$.
From the symmetry of B_d follows d equalities :

$$\begin{aligned} f_0(e_{1+d}) = ... = f_0(e_{d-1+d}) = 0 \\ f_1(e_{0+d}) = ... = f_1(e_{d-1+d}) = 0 \\ \dots \\ f_{d-1}(e_{0+d}) = ... = f_{d-1}(e_{d-2+d}) = 0 \end{aligned}$$

Hence, $e_{i+d} \in E_k, i \in \{0, \ldots, d-1\} \setminus \{k\}$. Let us look at the first equality, that is $k = 0$ (any one would do for symmetry reasons). The set $\{e_{i+d}, i = 1, \ldots, d-1\} \subseteq E_0$ contains $d-1$ elements since

$$i \neq j \implies e_{i+d} \neq e_{j+d}$$

Let us recall that $dim(E_0) \leq dim(E) - 1 = 2 - 1 = 1$ and

$$2 < d$$

by the theorem hypothesis. Hence

$$d - 1 - dim(E_0) \geq 1$$

so we must have at least one vector from $\{e_{i+d}, i = 1, \ldots, d-1\}$ that is linearly dependent with the others, that is

$$\exists k \in \{1, \ldots, d-1\} : e_{k+d} = \sum_{l=1, l \neq k}^{d-1} \gamma_{k,l} e_{l+d}$$

but by linearity of f_k

$$1 = f_k(e_{k+d}) = \sum_{l=1, l \neq k}^{d-1} \gamma_{k,l} f_k(e_{l+d}) = 0$$

which is a contradiction. □

3 A first proof of the feasibility therem

Generalizing the idea of constructing linear functions out of permanents appeared to be fruitful, especially if those linear functions are gathered into a matrix to be equated to some matrix G imposed by the constraints of the problem. From this setup followed the possibility to prove the following theorem that sets theoretical boundaries on what is possible to do or not using SPS and photon detectors, which we call the feasibility theorem. More interestingly is the constructive proof that allows us to understand the generation of states and gates completely and so to optimise the corresponding success probability afterwards.

3.1 The feasibility theorem

The theorem is stated as follows:

Theorem 3.1. *For $q = 2$ and $d \geq 1$, a logical transformation*

$$\mathcal{C} : |00\rangle_{\mathcal{L}} \longmapsto \sum_{k,l=0}^{d-1} c_{k,l} \, |kl\rangle_{\mathcal{L}} =: S_C$$

on the Hilbert space $\mathcal{H}_{d^q}$ of logical qudits described by a matrix $C = \{c_{k,l}\}_{k,l<d}$ can be heralded by some passive optical network $\mathcal{A}$ in dual-rail encoding using only SPS and SPD if and only if $a \geq q \cdot (rank(C) - 1)$.

Remark 3.2. *The proof also works for any more sophisticated and multiple heralding signals $\{\mathcal{S}_k, k > 0\}$: the use of PNRD does not affect the feasibility.*

Proof. Let A be a matrix describing an optical network $\mathcal{A}$ and C be a matrix describing a logical state. Moreover, let $\mathcal{S}$ be a heralding signal on a photons, described as a dictionary $\mathcal{S} = \{m : s_m \geq 0, m = qd, \ldots, qd + a - 1\}$ such that $\sum_m s_m = a$ auxiliary photons, that is, heralding if and only if we detect exactly s_m photons on the mode m for $m = qd, \ldots, qd+a-1$. We can say the following:

By definition, A heralds $S_C = \sum_{kl} c_{k,l}^{i,j} \, |kl\rangle_{\mathcal{L}}$ in dual rail encoding with heralding signal $\mathcal{S} = \{m : s_m \geq 0, m = qd, \ldots, qd + a - 1\}$ such that $\sum_m s_m = a$ auxiliary photons **if and only if** there exists a Hilbert space

$$E = (\mathbb{C}^{a+q}, < \cdot, \cdot >)$$

containing each row $e_k, k = 0, \ldots, dq + a - 1$ of A that satisfies :

$$\mathcal{G}(e_0, \ldots, e_{2d-1}, S(e_{2d}, \ldots, e_{2d+a-1})) = \begin{bmatrix} \mathbf{0} & \mathbf{C} \\ \mathbf{C} & \mathbf{0} \end{bmatrix} =: G_C$$

where:

$$\begin{aligned} \mathcal{G} : & E^{2d+a} \longrightarrow \mathcal{M}_{2d}(\mathbb{C}) \\ & y_0, \ldots, y_{2d+a-1} \longmapsto \{f_k(y_l)\}_{k,l}, k, l = 0, \ldots, 2d-1 \end{aligned}$$

with

$$f_k(y) \coloneqq \mathsf{Per}\,(y, y_k, S(y_{2d}, \ldots, y_{2d+a-1})) \in \mathcal{L}_{\mathbb{C}}(E)$$

and S the function such that

$$S(y_{2d}, \ldots, y_{2d+a-1}) \coloneqq conc_{m=2d}^{2d+a-1}\left((y_m, \ldots, y_m)_{\mathcal{S}(m)}\right)$$

with replicating y_m exactly $\mathcal{S}(m)$ times.
By linearity, this whole set of conditions are satisfied **if and only if**:

$$\tilde{\mathcal{G}}(\tilde{e}_0, \ldots, \tilde{e}_{2d-1}, S(e_{2d}, \ldots, e_{2d+a-1})) = \begin{bmatrix} \mathbf{0} & \tilde{\mathbf{I}}_\mathbf{b} \\ \tilde{\mathbf{I}}_\mathbf{b} & \mathbf{0} \end{bmatrix} =: G_C \tag{3.1}$$

where:

$$\tilde{\mathbf{I}}_\mathbf{b} = \begin{bmatrix} \mathbf{I}_\mathbf{b} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$$

and

$$\begin{aligned} \tilde{\mathcal{G}} :& E^{2d+a} \longrightarrow \mathcal{M}_{2d}(\mathbb{C}) \\ & y_0, \ldots, y_{2d+a-1} \longmapsto \{\tilde{f}_k(y_l)\}_{k,l}, k, l = 0, \ldots, 2d-1 \end{aligned}$$

with

$$\tilde{e}_0, \ldots, \tilde{e}_{2d-1} = Row_C(e_0, \ldots, e_{2d-1})$$

and

$$\tilde{f}_k(y) = Col_C(f_0, \ldots, f_{2d-1})$$

where $Row/Col_C(y_0, \ldots, y_{2d-1})$ are the Gaussian elimination operations of C applied on a set of $2d$ vectors $y_0, \ldots, y_{2d-1}$.

Now we have to split the proof into two parts, one for the sufficient and one for the necessary condition.
For the necessary condition, let us remind that each $\tilde{f}_k$ are linear map on E which is of dimension $a+2$. Hence the kernel should be of dimension $a+1$. However, we also see from equality 3.1 and the shape of G_C that the kernel of each $\tilde{f}_k, k < rank(C)$ must be of dimension at least $2 \cdot (rank(C) - 1)$. Hence this implies

$$a \geq 2 \cdot (rank(C) - 1)$$

For the sufficient condition, let $b \coloneqq rank(C)$. if $a \geq 2 \cdot (b-1)$, any basis of $E = (\mathbb{C}^{2b}, < \cdot, \cdot >)$ would be fine for the first $2b$ rows. Then we should apply $Col/Row_C(y_0, \ldots, y_{2d-1})$ in the inverse order on this basis, completing by $2 \cdot (d-b)$ rows and finally determining the last a rows of A given the constraints we imposed, that is, solving a system of $\frac{(2d)^2-2d}{2}$ polynomial equations.
However, we don't know if this system always has a solution. To overcome this issue, we can say the following : we know that the optical network heralding the b-dimensional Bell state with signal $\mathcal{S} = \{m : s_m = 1, m = 2b, \ldots, 2b+a-1\}$ given by Timothée Goubault 3.1 uses a tight amount of $a = 2 \cdot (b-1)$ auxiliary

photons. Hence, the unitary matrix $U = matrix(u_0, \ldots, u_{2b+a-1})$ describing the optical network solves the former system of equations and satisfies

$$\mathcal{G}(u_0, \ldots, u_{2b-1}) = \begin{bmatrix} \mathbf{0} & \mathbf{I_b} \\ \mathbf{I_b} & \mathbf{0} \end{bmatrix}$$

Hence, it suffices to apply $Col/Row_C(y_0, \ldots, y_{2d-1})$ in the inverse order on the basis $(u_0, \ldots, u_{2b-1})$ of the Hilbert space $E = (\mathbb{C}^{2b}, < \cdot, \cdot >)$ and on the basis of its dual E^* to retrieve the matrix A heralding the state S_C:

$$A = matrix(Col/Row_C(u_0, \ldots, S(u_{2b-1}, u_{2b}, \ldots, u_{2b+a-1})))$$

□

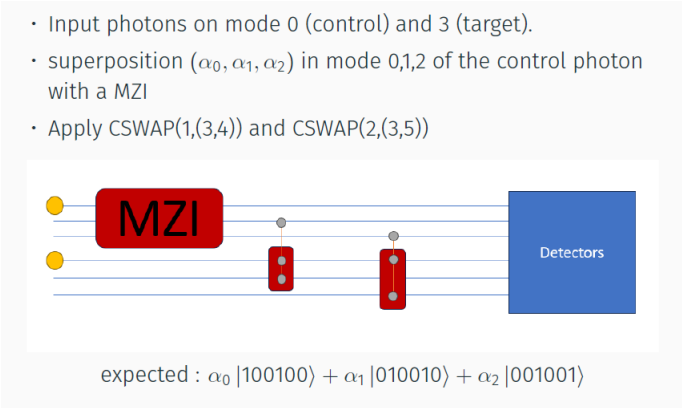


Figure 2: Optical network given by Timothée Goubault to generate a generalised 3-dimensional Bell state out of two heralded CZ gates using 4 auxiliary photons.

3.2 Towards a more general theorem

In fact, the proof we established above seems to be related to a theorem that we have not proved yet but which seems to rely on a suitable rewriting of Lemma 5.8. from paper [3]. We further denote by l_k the $k-th$ row of $A \in \mathcal{M}_{(qd+a)\times(a+q)}(\mathbb{C})$. Let us denote by $(y, l_{k_1}, \ldots, l_{k_{a+q-1}})$ the matrix obtained by concatenating the rows $y, l_{k_1}, \ldots, l_{k_{a+q-1}}$.
Given a heralding signal $\mathcal{S}$, let us define for $k_i \in [dq)$ the linear functions

$$f_{k_1,\ldots,k_{q-1}}(y) = \mathsf{Per}\left((y, l_{k_1}, \ldots, l_{k_{q-1}}, S(l_{qd}, \ldots, l_{qd+a-1}))\right) \tag{3.2}$$

we can define the following map

$$\begin{aligned}\mathcal{G}_{\mathcal{S}} :&\mathcal{M}_{(qd+a)\times(a+q)}(\mathbb{C}) \longrightarrow \mathcal{T}_{qd}(\mathbb{C}) \\ &A \longmapsto \{f_{k_1,\ldots,k_{q-1}}(l_{k_0}, S(l_{qd}, \ldots, l_{qd+a-1})\}_{k_i\in[dq),i=0,\ldots,q-}\end{aligned}$$

where S is the function associated to $\mathcal{S}$ described in 3.1.

Theorem 3.3 (Surjectivity of $\mathcal{G}_{\mathcal{S}}$)**.** *Given a tensor $G \in \mathcal{T}_{dq}(\mathbb{C})$, there exists a matrix $A_G \in \mathcal{M}_{(qd+a)\times(a+q)}(\mathbb{C})$ such that $\mathcal{G}_{\mathcal{S}}(A_G) = G$ if and only if $rankG \leq a+q$, where rank is the rank defined in [3].*

Proof. The necessary condition is straightforward since

$$rankG > a+q \implies ker\tilde{f} > c-1$$

for some linear form $\tilde{f}$ on $E = (\mathbb{C}^{a+q}, <\cdot,\cdot>)$, which is a contradiction. However, the sufficient condition remains to be proven but seems to rely on a suitable rewriting of Lemma 5.8. from paper [3]. □

3.3 Example with post-selected Bell state with $a = 0$

To post-select a 2-dimensional Bell state in dual-rail encoding, the induced matrix of constraints that should be specified is

$$G = \begin{bmatrix} b_0 & c_0 & 1 & 0 \\ c_0 & b_1 & 0 & 1 \\ 1 & 0 & b_2 & c_2 \\ 0 & 1 & c_2 & b_3 \end{bmatrix}$$

where the success probability is directly given by

$$p_s = \frac{4}{4 + \sum_{i=0}^{3} |b_i|^2 + |c_0|^2 + |c_2|^2}$$

Applying the method in the proof of 3.1 or directly applying the last theorem, we deduce that the associated optical transformation A_G exists if and only if

$rank(G) - 1 \leq dim(E) - 1 = 1$. Hence, A_G exists if and only if $rank(G) \leq 2$. Since G can be reduced as

$$G = \begin{bmatrix} 0 & 0 & 1 - b_0 b_2 - c_0 c_2 & -b_0 c_2 - c_0 b_3 \\ 0 & 0 & -c_0 b_2 - b_1 c_2 & 1 - c_0 c_2 - b_1 b_3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

we deduce that G should satisfy

$$\begin{aligned} 1 - b_0 b_2 - c_0 c_2 &= 0 \\ b_0 c_2 + c_0 b_3 &= 0 \\ c_0 b_2 + b_1 c_2 &= 0 \\ 1 - c_0 c_2 - b_1 b_3 &= 0 \end{aligned}$$

onto which we can optimise the success probability, reaching a maximum of $1/2$.

In fact, in the case of two input photons, we can state a general formula found by Konrad Kieling in [7]:

Theorem 3.4. *Let $S(1)$ and $S(2)$ be two bi-photon states on n modes. Then, $S(1)$ can be transformed into $S(2)$ with linear optics, vacuum detectors, and empty ancilla modes if and only if $rank(S_1) \geq rank(S_2)$. The optimal success probability of such a transformation is given by*

$$p_s S(2)|S(1) = \mu^2$$

where

$$\mu = \max_{\pi \in Sym(n)} \min \left\{ 1, \sigma^{(1)}_{\pi(1)} / \sigma^{(2)}_1, \ldots, \sigma^{(1)}_{\pi(v(1))} / \sigma^{(2)}_{v(1)} \right\}$$

Remark 3.5. *In some sense, this theorem goes further than the feasibility theorem since it gives the success probability. However, it only applies to bi-photon states and does not indicate the number of auxiliary photons required.*

4 A second proof of the feasibility theorem

Separately, Grégoire De Glistiany and Sébastien Draux found another smooth proof of the feasibility theorem 3.1 which reveals another convenient way to generate any states with a high probability of success. Here is the detailed proof:

Proof. Let $A \in \mathcal{M}_{(dq+a)\times(q+a)}(\mathbb{C})$ and let us denote l_i the i-th row of A, index going from 1 to $dq+a$ for convenience. Let us fix the values of the rows $l_{dq+1}\ldots,l_{dq+a}$ and let us define the bi-linear form $\mathcal{F}_{\mathcal{S}}$ associated to the permanents $\mathsf{Per}\,(\cdot,\cdot,S(l_{dq+1}\ldots,l_{dq+a}))$ depending on the last a parameterised rows and on the heralding signal $\mathcal{S}$. Using the canonical basis $\{b_i=(\delta_{i,1},\ldots,\delta_{i,q+a}), i=1,\ldots,q+a\}$ of the Hilbert space $\mathcal{H}=(\mathbb{C}^{q+a},<.,.>)$, we have that $\mathcal{F}_{\mathcal{S}}$ can be represented by a matrix

$$F_{\mathcal{S}}=\{F_{\mathcal{S}}(l_{dq},\ldots,l_{dq+a})\}_{i,j}=\{\mathsf{Per}\,(b_i,b_j,S(l_{dq+1}\ldots,l_{dq+a}))\}_{i,j}\in\mathcal{M}_{(q+a)\times(q+a)}(\mathbb{C})$$

We further omit the subscript $\mathcal{S}$ in $F_{\mathcal{S}}$. If we let $E=(l_1,\ldots,l_{dq})\in\mathcal{M}_{(dq)\times(q+a)}(\mathbb{C})$ be the matrix of the dq first rows of A, then the amplitudes of probability can be written as

$$\{\mathsf{Per}\,(l_i,l_j,l_{dq+1}\ldots,l_{dq+a}))_{i,j}\}=\{E^TFE\}_{i,j}$$

Hence, the matrix A describes an optical network heralding the logical transformation $\mathcal{C}$ with the heralding signals $\{\mathcal{S}_k,k>0\}$ if and only if

$$E^TFE=\begin{bmatrix}\mathbf{0} & \mathbf{C}\\ \mathbf{C} & \mathbf{0}\end{bmatrix}=:G_C \tag{4.1}$$

By inherent construction, F and G are complex symmetric. Hence from Takagi factorisation (a detailed explanation of existence and unicity up to an equivalence class is provided in[5]), there exists $Q\in\mathcal{O}_{dq}((C))$ and $D_G\in diag_{dq}(\mathbb{C})$ such that

$$G=QD_GQ^T$$

There also exists $P\in\mathcal{O}_{a+q}((C))$ and $D_F\in diag_{a+q}(\mathbb{C})$ such that

$$F=PD_FP^T$$

Hence we can rewrite equation 4.1 as

$$E^TPD_FP^TE=QD_GQ^T$$

if and only if

$$(Q^TE^TP)D_F(Q^TE^TP)^T=D_G \tag{4.2}$$

Let us define $r_f\coloneqq rank(F)$, $r_g\coloneqq rank(G)=q\cdot rank(C)$. Moreover, let us define $H\coloneqq Q^TE^TP\in\mathcal{M}_{(dq)\times(a+q)}(\mathbb{C})$. Then one has $E=QHP^T$ with

$$HD_FH^T=D_G$$

Determining H from the last equality would lead to E. However, H is not fixed and can take several values that we don't know, up to the last equality. Hence, the next step is to understand to what extent H can vary without influencing E. To this end, let

$$H = U\Lambda V^T$$

be an SVD of H where Λ is unique up to the choice of H and an arbitrary ordering on the singular values. Hence

$$\Lambda = (QU)^T E^T (PV)$$

We show that up to the choice of U and V, H can be assumed to be a diagonal matrix that is uniquely determined, again only up to some sign choices. Let $D_F^{(V)}$ and $D_G^{(U)}$ be the unique diagonal matrices such that

$$VD_F^{(V)}V^T = D_F; UD_G^{(U)}U^T = D_G$$

Then we can write

$$\begin{aligned} E^T F E = G &\iff (Q^T E^T P) D_F (Q^T E^T P)^T = D_G \\ &\iff ((QU)^T E^T PV) D_F^{(V)} ((QU)^T E^T PV)^T = D_G^{(U)} \\ &\iff \Lambda D_F^{(V)} \Lambda^T = D_G^{(U)} \end{aligned}$$

Hence, up to $\pm$ signs resulting from square modulus, Λ is uniquely determined by the choice of the orthonormal basis U and V from the SVD of H. Hence,

$$E = (QU)\Lambda_{(U,V,\pm)}(PV)^T$$

More precisely, let us assume for simplicity that F, G, H contains distinct singular values. Then writing $U(\theta) = matrix(u_1 e^{i\theta_1}, \ldots, u_n e^{i\theta_n})$ for some unitary matrix $U = matrix(u_1, \ldots, u_n)$, Takagi factorisation and SVD tells that there are unique vectors of angles $\theta_G, \theta_H, \theta_F$ such that

$$E = (Q(\theta_{\mathbf{G}})U(\theta_{\mathbf{H}}))\Lambda_{(U(\theta_{\mathbf{H}})V(\theta_{\mathbf{H}}),\pm)}(P(\theta_{\mathbf{F}})V(\theta_{\mathbf{H}})^T$$

Unfortunately, we haven't found evidence that the term $U(\theta_{\mathbf{H}}))\Lambda_{(U(\theta_{\mathbf{H}})V(\theta_{\mathbf{H}}),\pm)}V(\theta_{\mathbf{H}})^T$ can be cast into a known and easy computable diagonal matrix up to some suitable choice of angles θ_G, θ_F. Hence, to compute every possible matrix E from H, we have to solve equality 4.2 which can be written as

$$\forall i, j = 1, \ldots, d \cdot q : \sum_{k=1}^{r_f} v_{ik} v_{jk} d_{f_k} = d_{g_i} \cdot \delta_{i,j}$$

which is a system of $(d \cdot q)^2$ homogeneous polynomial equations of $a + q$ terms of degree 2 with a total of $(dq) \times (a + q)$ variables.
While this system adds quite a lot of degree of freedom, it is always true that one such Λ exists if and only if

$$r_f \geq r_g$$

Indeed, if $VD_FV^T = D_G$, then

$$r_f = rank(F) \geq rank(VD_FV^T) = rank(D_G) = r_g$$

and if $r_f \geq r_g$, then for instance

$$H = \begin{bmatrix} \frac{d_{g_1}}{d_{f_1}} & \dots & 0 & 0 & \dots & 0 \\ 0 & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & \frac{d_{g_{r_g}}}{d_{f_{r_g}}} & 0 & \dots & 0 \end{bmatrix} \tag{4.3}$$

satisfies $VD_FV^T = D_G$.
Since $\mathcal{F}$ is a bi-linear form on $\mathcal{H}$, we have that $rank(F) \leq a+q$, but this bound can be reached by taking $l_i = (1, \dots, 1)$ since in this case $F = J_{a+q} - I_{a+q}$, which is full rank. Noticing that $r_g = q \cdot rank(C)$, we obtain that the state can be heralded if and only if

$$a + q = r_f \geq r_g = q \cdot rank(C)$$

Moreover, A is directly given in the proof by the block matrix

$$A = \begin{bmatrix} PHQ^T \\ L \end{bmatrix} \tag{4.4}$$

□

5 Discussion

We observe that the two proofs are connected vessels and constitute two approaches to solve the same problem: fixing first the first dq rows or the last a rows of A and then determining the remaining rows in each case.

5.1 Comparing the first and second method

The first proof gives a way to construct any logical two qudits states starting from any basis of $E = (\mathbb{C}^{a+q}, <\cdot,\cdot>)$. Then we have to find the last a rows of A by solving a system of

- $\frac{(2d)^2-2d}{2}$ polynomial equations
- homogenized to degree $a+1$
- with $(a+q)!$ or $(a+q)!+1$ terms
- with a total of $a \cdot (a+q)$ variables

The second proof gives a way to construct any logical two-qudits state starting from any (suitable) vectors dedicated to the last a rows of A. Then the first dq rows are determined by finding the matrix H by solving a system of

- $(2d)^2$ polynomial equations
- homogenized to degree $2+1=3$
- with $a+q+1$ terms
- and a total of $a \cdot (a+q)$ variables

A priori, the first system seems to be easier to solve, at least when $a < dq$ since there are fewer polynomials and fewer variables. However, the second proof seems to give more insights into the success probability. For instance, it seems that we can retrieve the max min formula in Kieling's theorem 3.4 recalling that for any permutation π of the columns of D_G, a matrix H_π can be found if the hypothesis are satisfied. Moreover, some investigations could show that without decreasing the success probability, H can be assumed to be diagonal on its first $2d$ columns, decreasing drastically the size of the system to solve.

5.2 Improving success probability

5.2.1 optimising on the free parameters

For the first method, the free parameters are the free variables of the system to be solved after choosing a basis of E. For the second method, the free parameters are the free variables and the three real vectors $\theta_{\mathbf{F}}, \theta_{\mathbf{G}}, \theta_{\mathbf{H}}$ of $a+2$,$2d$ and $2d$ angles respectively, although it might not influence the success probability.

5.2.2 Multiple heralding signals

Given multiple heralding signals $\{\mathcal{S}_s, s = 1, \ldots, k\}$ to herald a state S_C, we propose the following framework:
Let $\gamma_{ij}^{(s)} \in \mathbb{C}$ and $C_s = \{\gamma_{ij}^{(s)}\}$ such that

$$\forall i, j < d : \sum_{s=1}^{k} |\gamma_{ij}^{(s)}|^2 = |c_{ij}|^2$$

and let

$$G_s \coloneqq \begin{bmatrix} \mathbf{0} & \mathbf{C_s} \\ \mathbf{C_s} & \mathbf{0} \end{bmatrix}$$

Then A heralds S_C if and only if

$$E^T F_{\mathcal{S}_s} E = G_s, \forall s \leq k \tag{5.1}$$

if and only if

$$E = P_s H_s Q_s^T, \forall s \leq k$$

with H_s such that

$$H_s D_{F_s} H_s^T = D_{G_s}$$

Of course, we have to be careful that E stays independent of s $\forall s \leq k$ in equality 5.1 and so we conjecture that we can choose the parameters $\gamma_{ij}^{(s)}$ such this can be achievable.

Remark 5.1. *The feasibility theorem remains true whether we use single or multiple heralding signals. This can be seen for example with the first proof: multiple heralding signals generate linear functions* $f_k^s(y) \coloneqq \mathsf{Per}\left(y, y_k, S_s(y_{2d}, \ldots, y_{2d+a-1})\right)$ *for all* $s \leq k$ *and we can prove that they can be suitably rearranged and summed into one linear function of maximal dimension kernel exactly* $2 \cdot (rank(C) - 1)$.

5.3 Generalisation to more qudits

As explained in 3.2, the generalisation to more logical qudits state seems to be possible via theorem 3.2 or via a generalisation of the first and second proof of this paper. We conjecture the following generalisation.

Theorem 5.2. *For* $q \geq 2$*, a logical transformation*

$$\mathcal{C} : |0\rangle_{\mathcal{L}}^{\otimes q} \longrightarrow \sum_{\mathbf{k}} t_{\mathbf{k}} |\mathbf{k}\rangle_{\mathcal{L}}$$

on the Hilbert space $\mathcal{H}_{d^q}$ *of logical qudits described by a tensor* $\mathcal{T} = \{t_{\mathbf{k}}\}$ *can be heralded by some passive optical network* $\mathcal{A}$ *in dual-rail encoding using only SPS and SPD if and only if* $a \geq q \cdot (rank(\mathcal{T}) - 1)$.

6 Implementations for standard Bell states

6.1 Using first method

We implemented the first method by choosing the canonical basis for the first dq rows of E and then found the remaining rows by solving the polynomial system using the compiled Julia programming language [2] to speed up the running time and using the Groebner.jl package [4] to solve via Groebner basis. The way we proceed is as follows:

1. we create the system to be solved on Python using symbolic variables from Sympy. The system depends on the dimension d and on the basis (the canonical basis per default)
2. we find a Groebner basis of the system on Julia
3. we solve the Groebner basis on Python using the solve method from Sympy
4. we construct the matrix A from the solutions, taking arbitrary values for the remaining free variables if any
5. we unitarise A (via Gram-Schmidt orthogonalisation, Naimark's dilation or Keiling optimised procedure)
6. we compute the success probability on Perceval
7. we optimize the success probability on the free variables by repeating steps 4 to 7 into an objective function f that we optimise with Scipy.optimize method on the complex domains by separating real and imaginary parts.

Solving the system on the real domain leads to a probability of success of 0.018 for $d = 2$ and $6{\cdot}10^{-4}$ for $d = 3$. Of course, it remains to be tested on various basis and not only the canonical one, which should improve consequently the probability of success. Solving the system on the complex domain by separating real and imaginary parts doubles the number of variables and equations. For $d = 2$ the Groebner basis can be reasonably reduced by doing some guesses, however, the final state we obtain is not exactly the Bell state so there must be an error somewhere in the code.

6.2 Using second method

Implementing the second method with the simplified assumption that H is diagonal leads to encouraging results. The way we proceed is as follows:

1. we choose arbitrary values ($\frac{1}{\sqrt{2}}$ per default) for the last rows of A (free variable)
2. from there we determine the matrix E via Takagi factorisations and the assumption that H is diagonal (this assumption avoids having a polynomial system to solve by setting some off-diagonal variables of H to zero)

3. we build the matrix A from E and the last chosen rows.

4. we unitarise A and then check success probability

5. we optimise the success probability on the free variables from the beginning using Scipy.optimise and separating real and imaginary parts.

We tested it both on the bunched and "spread" signals, on the same starting vector of entry value $\frac{1}{\sqrt{2}}$. From what we have observed, the bunched signal performed better. Results for the bunched signal are summarised in the following table:

a/d	2	3	4
2	0.110		
3	0.096		
4	0.037	0.023	
5			
6			runtime error (before opt: 8.45e-08)

Table 1: Summary of the results of the second method

In the case $d = 2$, we retrieve the best-known success probability $1/9$ found in [6]. In the case $d = 3$, the probability of success of 0.023 outperforms the best-known result presented in [9] (approximately 0.0214) as far as we know. Investigations on the same method with a more complex matrix H could be interesting, for example, choosing H to be tridiagonal should generate polynomial systems of reasonable size. The fact that success probability decreases when adding auxiliary photons can also be understood when considering the simplified H in 4.3 and the fact that when $a > 2 \cdot (d-1)$, H is not square anymore and has extra columns, adding more parameters onto which we didn't optimise since we set them to 0.

7 Conclusions

The investigations we conducted exhibit two methods to generate any logical qudit states. Moreover, we now better understand the aspects to focus on for improving the efficiency of such state preparations. Nonetheless, a lot of work remains to complete concerning what can or cannot influence the success probability and how to implement suitably such methods.

References

[1] Scott Aaronson and Alex Arkhipov. "The computational complexity of linear optics". In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. 2011, pp. 333–342.

[2] Jeff Bezanson et al. "Julia: A fresh approach to numerical computing". In: *SIAM review* 59.1 (2017), pp. 65–98.

[3] Wojciech Bruzda, Shmuel Friedland, and Karol Życzkowski. "Rank of a tensor and quantum entanglement". In: *Linear and Multilinear Algebra* (2023), pp. 1–64.

[4] Alexander Demin and Shashi Gowda. *Groebner.jl: A package for Gröbner bases computations in Julia*. 2024. arXiv: `2304.06935 [cs.MS]`.

[5] Luca Dieci, Alessandra Papini, and Alessandro Pugliese. "Takagi factorization of matrices depending on parameters and locating degeneracies of singular values". In: *SIAM Journal on Matrix Analysis and Applications* 43.3 (2022), pp. 1148–1161.

[6] Suren A Fldzhyan, Mikhail Yu Saygin, and Sergei P Kulik. "Compact linear optical scheme for Bell state generation". In: *Physical Review Research* 3.4 (2021), p. 043031.

[7] Konrad Kieling. "Linear optics quantum computing-construction of small networks and asymptotic scaling". PhD thesis. Citeseer, 2008.

[8] Nicolas Maring et al. "A general-purpose single-photon-based quantum computing platform". In: *arXiv preprint arXiv:2306.00874* (2023).

[9] Stefano Paesani et al. "Scheme for universal high-dimensional quantum computation with linear optics". In: *Physical Review Letters* 126.23 (2021), p. 230504.