

# Linear optics toolbox for integrated optics

K. Kieling<sup>1</sup>, J.L. O'Brien<sup>2</sup>, and J. Eisert<sup>1,3</sup>

1: Institute for Physics und Astronomy, University of Potsdam, 14476 Potsdam-Golm, Germany

2: Centre for Quantum Photonics, H.H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB

3: Institute for Advanced Study, 14193 Berlin, Germany

Considering optical modes and restricting the allowed operations to be energy conserving, one ends up in the framework of linear optics. By further fixing an encoding of a computational Hilbert space into the modes' Fock space, these devices can be employed for quantum information processing. For a given task a variety of figures of merit – such as the probability of success or the number of auxiliary photons – can be studied. We introduce methods to assess those quantities in the single-photon (discrete variables) regime and give construction prescriptions for integrated optics networks implementing controlled phase-gates, state transformations and measurements in an optimal fashion.

## Network construction

### Post-selected gate without additional photons

- Fix encoding  $|i\rangle_{\text{logical}} \mapsto |c_i\rangle_{\text{physical}}$  using  $c \in \mathbb{N}^{d \times n}$ ,  $\sum_i c_{j,i} = k$ .

Example: dual-rail qubits such as polarisation- or path-encoded ( $d = 2$  and  $c_0 = (1, 0)$ ,  $c_1 = (0, 1)$ ).

- Given the unitary  $\mathcal{U}$ , the defining equations [1, 2] for the network are

$$\text{per} A[c_{i_1} \oplus \dots \oplus c_{i_n} | c_{j_1} \oplus \dots \oplus c_{j_n}] = \langle i_1, \dots, i_n | \mathcal{U} | j_1, \dots, j_n \rangle \quad (1)$$

$\forall i, j \in [0, d-1]^n$ . These are polynomial equations of degree  $kn$  in  $(dn)^2$  complex variables.

- Not easy to impose unitarity-constraints, solutions will be non-unitary in general.

### Unitary extension

Let  $\sigma_1 \geq \dots \geq \sigma_n \geq 0$  denote the singular values of  $A$  and  $\nu$  the multiplicity of the largest one (w.l.o.g.  $\sigma_1 = 1$ ).

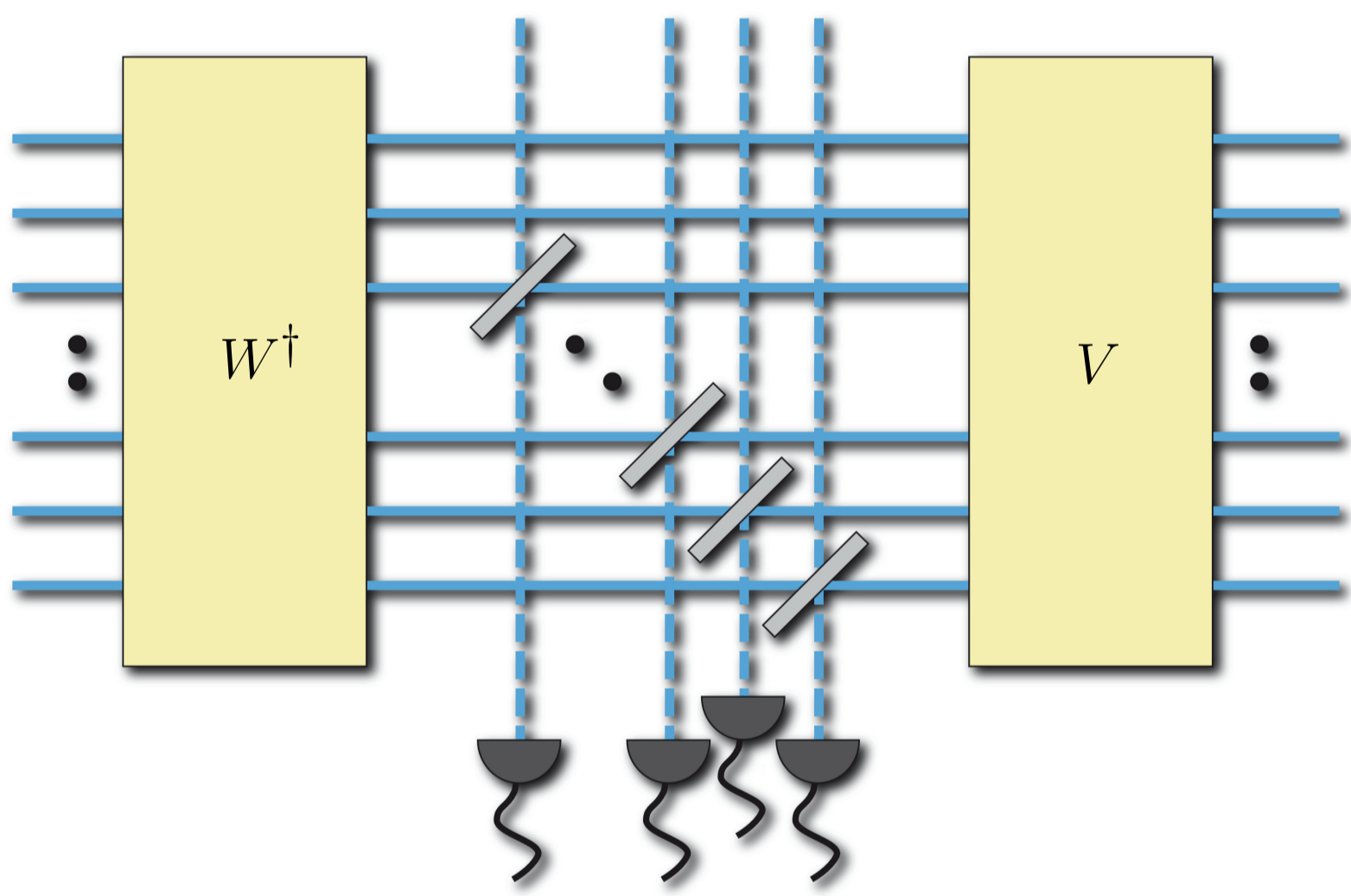
For any matrix  $A \in \mathbb{C}^{n \times n}$ , with the largest singular value  $\sigma_1 \leq 1$ , there exists an extension [3]

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SU(N).$$

It is given by

$$U = (V \oplus \mathbb{1}_{n-\nu}) \left( \mathbb{1}_\nu \oplus \bigoplus_{i=\nu+1}^n U^{(i)} \right) (W^\dagger \oplus \mathbb{1}_{n-\nu}) \quad (2)$$

which has a straight-forward linear optics interpretation:



### Polynomial factorisation

Write any pure state  $|\psi\rangle$  of  $k$  photons in  $n$  modes with  $P \in \mathbb{C}[a_1^\dagger, \dots, a_n^\dagger] =: \mathbb{P}$  homogeneous and of degree  $k$  as

$$|\psi\rangle = P(\mathbf{a}^\dagger) |\text{vac}\rangle$$

$|\psi\rangle$  can be generated by linear optics without additional photons from "smaller states" iff  $\exists g, h \in \mathbb{P}$  such that  $P(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})$ .

This condition can be reduced to checking matrix ranks by using results on polynomial factorisation [4].

### References

- [1] Scheel, arXiv:quant-ph/0406127.
- [2] Kieling, PhD thesis, Imperial College London (2008).
- [3] VanMeter *et al*, *Phys. Rev. A* **76** 063808 (2007).
- [4] Ruppert, *J. Number Theory* **77** 62 (1999); Kaltöfen, *J. Computer and System Sciences* **50** 274 (1995).
- [5] Hofmann and Takeuchi, *Phys. Rev. A* **66** 024308 (2002); Ralph *et al*, *Phys. Rev. A* **65** 062324 (2002).
- [6] Kieling, O'Brien, and Eisert, *New J. Phys.* **12** 013003 (2009).
- [7] Lanyon *et al*, *Phys. Rev. Lett.* **100** 060504 (2008).

## Controlled phase-gates

### Variable controlled phase-gates

Generalise the post-selected linear optical controlled-Z gate [5] in dual-rail encoding to arbitrary phases  $\varphi$ :

$$|ij\rangle \mapsto |ij\rangle e^{i\varphi i \cdot j}$$

Identify the optimal probability of success  $p_s$  and construct a network achieving this optimum.

### The optimal solution

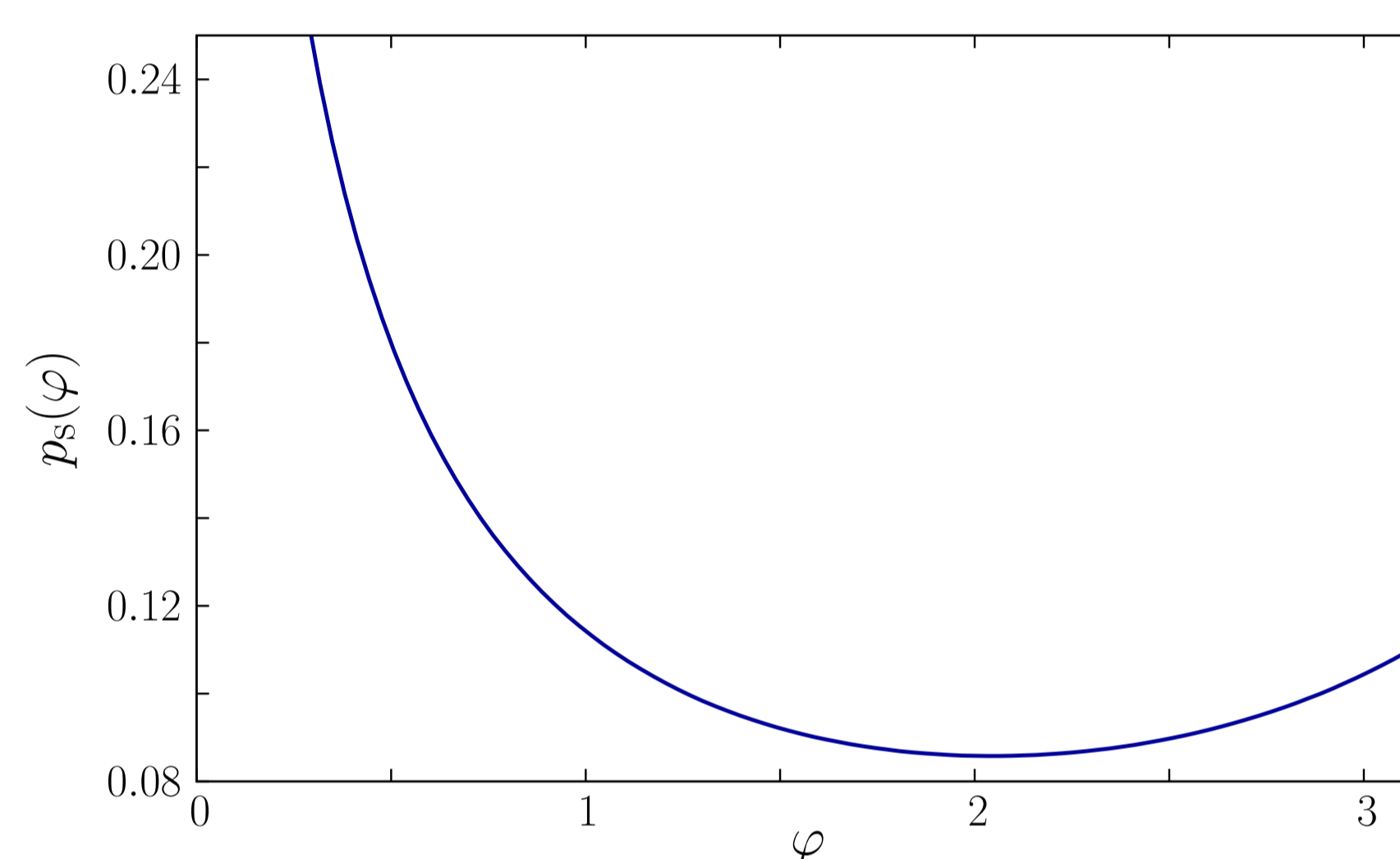
- Solutions to Eqn.(1) are all of the form  $A = \mathbb{1}_2 \oplus B$  with

$$B = p_s^{1/4} \begin{bmatrix} x & (e^{i\varphi} - 1)x/y \\ y/x & 1/x \end{bmatrix},$$

so effectively a single-rail core.

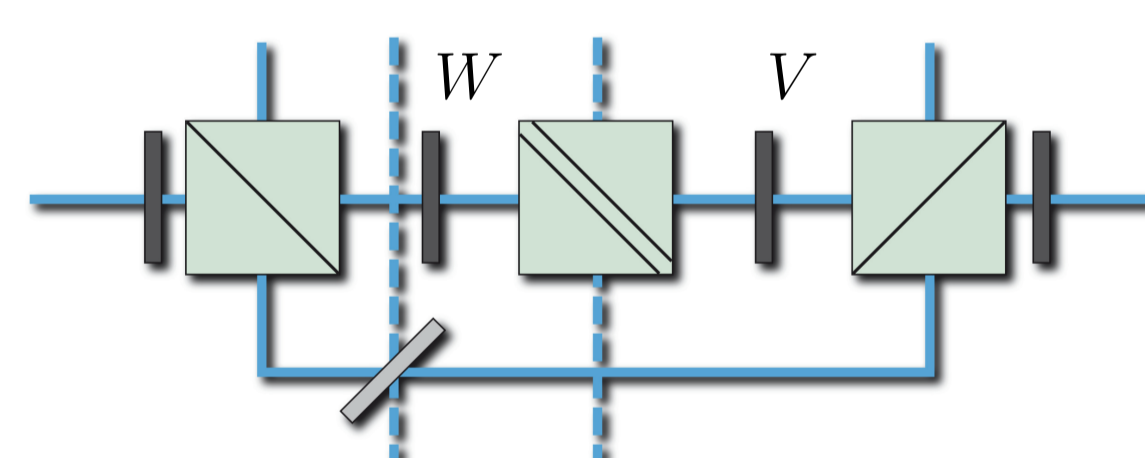
- Maximising  $p_s$  subject to  $\sigma_1(B) \leq 1$  yields:

$$p_s(\varphi) = \left( 1 + 2 \left| \sin \frac{\varphi}{2} \right| + 2 \sin \frac{\pi - \varphi}{4} \sqrt{\left| \sin \frac{\varphi}{2} \right|} \right)^{-2}$$



### The corresponding network

- SVD  $B = V \cdot \Sigma \cdot W$  with  $\Sigma := \text{diag}\{\sigma_+, \sigma_-\}$
- Global rescaling by  $\sigma_+^{-1}$ .
- A physical interpretation ( $SU(2)$ ) of  $V$  and  $W$  can be found by shifting their phases  $\phi_\pm$  to  $\Sigma$ .



$$V = W e^{i\phi_+ \sigma_z}$$

$$W = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}$$

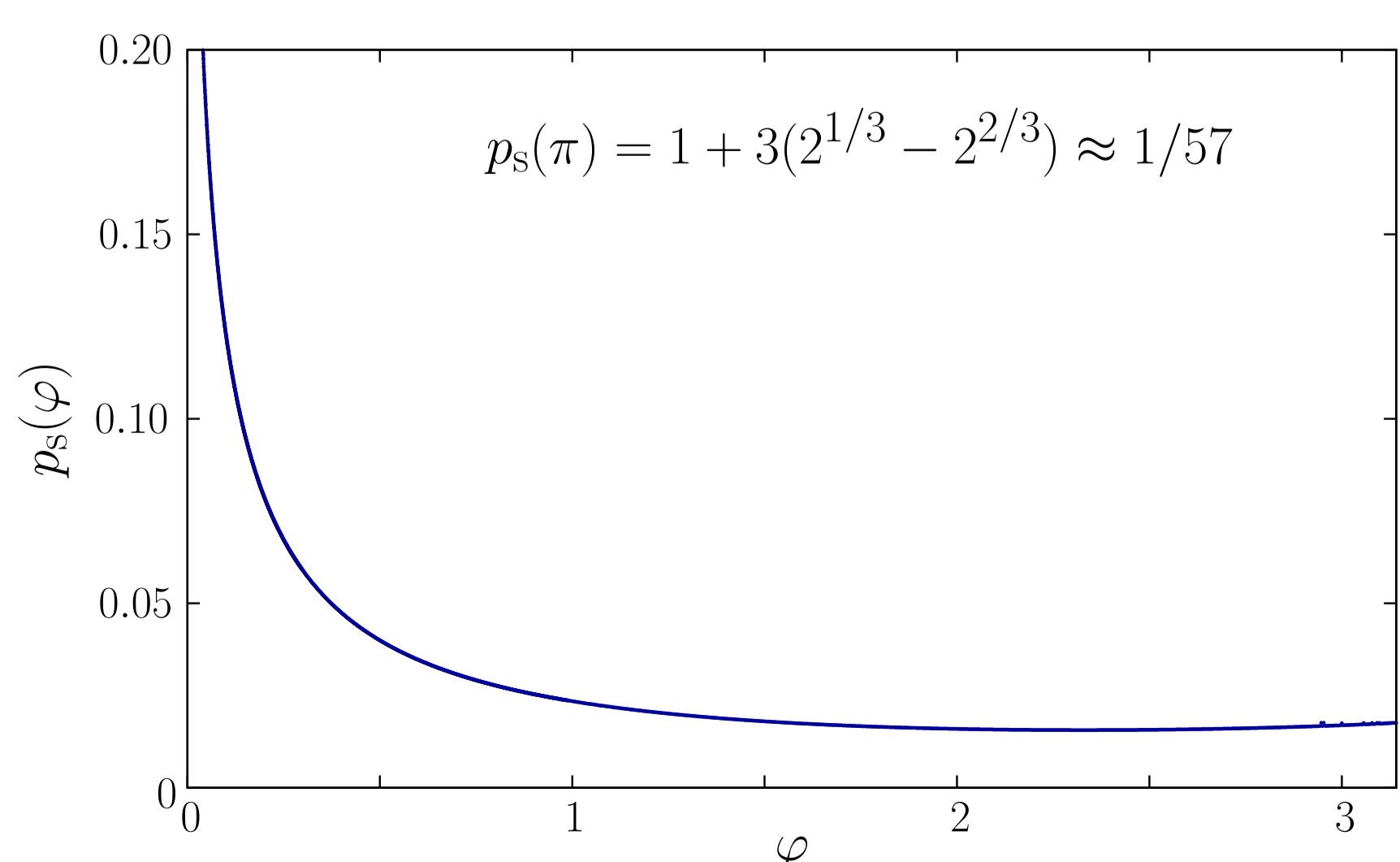
$$\phi_\pm = \arccot \left[ \cot \frac{\varphi + \pi}{4} \pm \left( (2 - 2\cos \varphi)^{1/4} \sin \frac{\varphi + \pi}{4} \right)^{-1} \right]$$

- The singular values are 1 (do nothing) and  $\frac{\sigma_-}{\sigma_+} e^{i(\phi_+ + \phi_-)}$  (BS with this reflectivity and phase upon reflection).

### Toffoli-like gates

The same route can be used to investigate single-rail gates of the form

$$|ijk\rangle \mapsto |ijk\rangle e^{i\varphi i \cdot j \cdot k}$$



## State transformations

### State tensors

Write homogeneous polynomials as

$$|\psi\rangle = P_\psi(\mathbf{a}^\dagger) |\text{vac}\rangle = S^{i_1, \dots, i_k} a_{i_1}^\dagger \dots a_{i_k}^\dagger$$

with  $S$  being a symmetric ( $S_{i_1, \dots, i_k} = S_{\pi(i_1), \dots, \pi(i_k)} \forall \pi \in [1, n]^k$ ,  $\pi \in \text{Sym}(k)$ ) tensor of order  $k$ . Linear optical networks ( $\mathbf{a}^\dagger \mapsto U \mathbf{a}^\dagger$ ) act as

$$|\psi\rangle \mapsto U |\psi\rangle = S^{j_1, \dots, j_k} U_{j_1}^{i_1} \dots U_{j_k}^{i_k} a_{i_1}^\dagger \dots a_{i_k}^\dagger$$

### 2 Photons

For  $k = 2$ ,  $S$  is a matrix, diagonalisable using linear optics ( $S \mapsto U^T S U$ ) via the Takagi-factorisation.

State transformations not increasing the rank amount to  $U \in \mathbb{C}^{n \times n}$  instead of  $SU(n)$  and can be realised by the decomposition given in Eqn. (2).

A bi-photon state  $S^{(1)}$  on  $n$  modes can be transformed into  $S^{(2)}$  using linear optics, vacuum detectors and vacuum ancilla modes iff

$$\nu^{(1)} := \text{rank}(S^{(1)}) \geq \text{rank}(S^{(2)}) =: \nu^{(2)}.$$

The optimal success probability is given by

$$p_s(S^{(2)} | S^{(1)}) = \max_{\pi \in \text{Sym}(n)} \min \left\{ 1, \frac{\sigma_{\pi(1)}^{(1)}}{\sigma_1^{(1)}}, \dots, \frac{\sigma_{\pi(\nu^{(1)})}^{(1)}}{\sigma_{\nu^{(1)}}^{(1)}} \right\}^2$$

The rank  $\nu$  of a state can be increased by 1 by using the NLS gate. Conjecture: A total of  $\Delta \nu = \nu^{(2)} - \nu^{(1)}$  additional photons is required.

### Dual-rail states (2 photons in 4 modes)

For non-increasing rank the optimal state transformation probabilities are

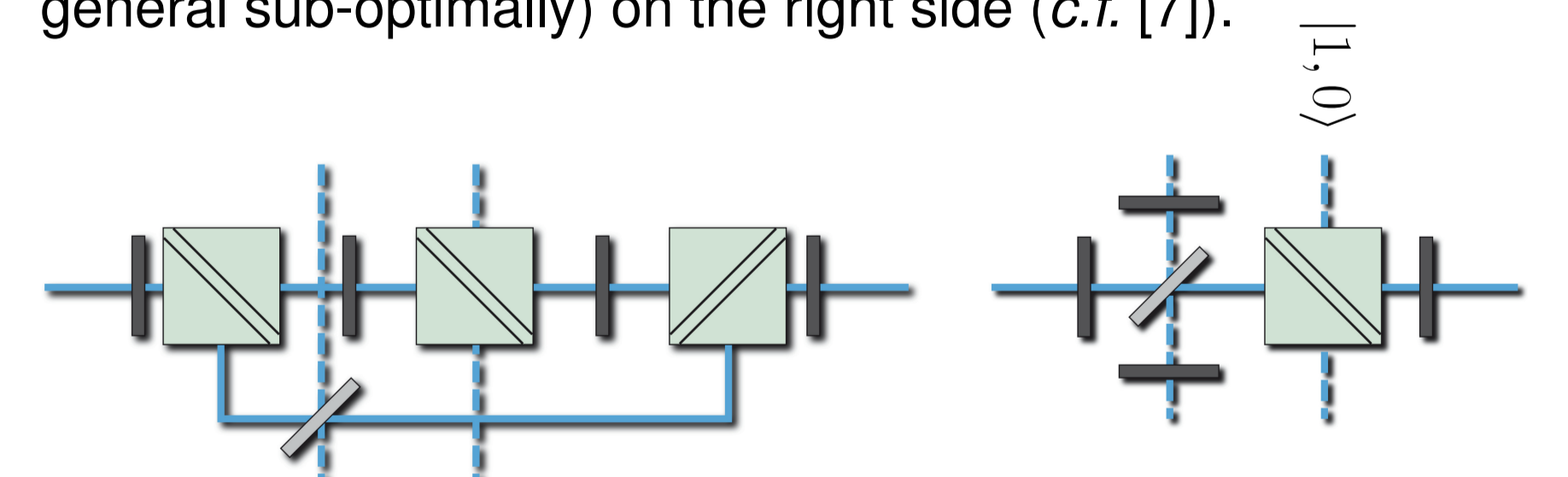
$$p_s \left( S_{\text{dr}}^{(2)} | S_{\text{dr}}^{(1)} \right) = \begin{cases} \left( 2\sigma_+^{(1)} \right)^2 & \det S_{\text{dr}}^{(2)} = 0 \quad (\nu^{(2)} = 2) \\ \left( \sigma_+^{(1)} / \sigma_+^{(2)} \right)^2 & 0 < \left| \det S_{\text{dr}}^{(2)} \right| < \left| \det S_{\text{dr}}^{(1)} \right| \\ \left( \sigma_-^{(1)} / \sigma_-^{(2)} \right)^2 & \text{else.} \end{cases}$$

with singular values

$$\sigma_\pm := \frac{1}{\sqrt{8}} \sqrt{1 \pm \sqrt{1 - 64 \left| \det S_{\text{dr}}^{(2)} \right|^2}}$$

### Qutrits (2 photons in 2 modes)

Qutrits are the special case where  $n = k = 2$ . The most general set of transformations of polarisation qutrits – including the optimal one – is shown on the left side, a simplified network achieving all transformations (though in general sub-optimally) on the right side (c.f. [7]).



### More photons

In order to include more photons, the problem of tensor diagonalisation arises (similar to generalised Schmidt decomposition). Tools to assess this task are polynomial normal forms and symmetric tensor decompositions.

We can give some solution for the ququad case ( $n = 2$ ,  $k = 3$ ).