Improved heralded schemes to generate entangled states from single photons

F. V. Gubarev,[1,2,*] I. V. Dyakonov ,[2] M. Yu. Saygin,[2] G. I. Struchalin ,[2] S. S. Straupe ,[2] and S. P. Kulik[2]

[1]*DATADVANCE LLC, Nauchny proezd 17, 15 Floor, Moscow 117246, Russian Federation*
[2]*Quantum Technology Centre, Faculty of Physics, Lomonosov Moscow State University, Moscow 119991, Russian Federation*

We present a semianalytical methodology to construct optimal linear-optical circuits for the heralded production of three-photon Greenberger-Horne-Zeilinger (3-GHZ) and two-photon Bell states. We provide a detailed description and analysis of the resulting optical schemes, which deliver success probabilities of 1/54 and 2/27 for dual-rail encoded 3-GHZ and Bell-state generation, respectively. Our results improve the known constructive bounds on the success probabilities for 3-GHZ states and are of particular importance for a ballistic quantum computing model [M. Gimeno-Segovia *et al.*, Phys. Rev. Lett. **115**, 020502 (2015)], for which these states provide an essential resource.

I. INTRODUCTION

Contemporary quantum computing technology is capable of engineering quantum devices operating with tens of qubits. Various physical platforms are competing in a race to implement quantum algorithms in practice. The linear-optical platform is attractive in many ways but suffers from a major hindrance—a probabilistic nature of multi-qubit gates [1]. Even though current theoretical proposals explore ways to seamlessly incorporate nondeterministic entangling gates [2], the currently known linear-optical quantum computer (LOQC) architectures still have to consume small entangled states as a resource for successful operation. A current state-of-the-art model for linear-optical quantum computing requires a deterministic source of entangled three-photon states of the Greenberger-Horne-Zeilinger (GHZ) type (3-GHZ) [3]. There are approaches to deterministic generation of such states [4], however, high-quality deterministic preparation is still out of reach for the current technology. Alternatively, active multiplexing and heralded entangled state generation circuits provide a solution to the problem at the cost of additional resources. A cornerstone of this approach is the success probability of the entangling gate used, which determines the required volume of supplementary resources.

Probabilistic entangling gates may be divided in two classes—postselected and heralded ones. The successful operation of a postselected gate is identified postfactum at the latest stage of an experiment and requires detection of all photons in the circuit. Such gates cannot be concatenated since the input of each gate has to be encoded exclusively in the logical basis—a requirement which is impossible to fulfill due to the unitary behavior of the circuit [5]. In other words, the output of any postselected gate with nonunity success probability will contain unwanted states (often outside the logical basis), which will ruin the operation of the consequent gates. Furthermore, recent work [6] provides evidence that

postselected entangling gates cannot span the full space of multiphoton entangled states. Last, but not least, the post-selected setting demands the photons to pass through the whole circuit which poses extremely stringent requirements on loss in the optical circuit. For the reasons above the use of postselected gates for scalable quantum computing appears to be infeasible. However, we must note that in specific small-scale cases the interconnection between different degrees of freedom of a single photon can help to overcome the issue [7].

In turn, the heralded gates use some of the input photons to trigger the successful operation event without detecting and thus destroying the photons carrying the logical information. The heralding principle enables a completely different strategy for a linear-optical quantum computer architecture: Since the successful trigger event exists, the photons carrying the logical information can be measured during the circuit operation and not at the very end of it. The consequence is a drastic increase of the tolerable loss in the optical circuit. It has been shown that a specific large-scale cluster state generation procedure tolerates a few percent of photon loss [3,8]. Throughout the rest of the paper we will discuss only the problem of designing heralded entangling gates.

Let us briefly review the existing results on the optical circuit for heralded entangled state generation. We will focus on the circuits using nonentangled ancillary photons and dual-rail encoded logical qubits. The first example of the heralded controlled-Z (CZ) gate was reported in the seminal work by Knill *et al.* [9] and had a success probability of 1/16. Later on Knill devised a CZ gate circuit with two ancillary single photons [10] succeeding with probability 2/27 and a loose upper bound for any linear-optical CZ gate of 3/4 [5]. The best result for Bell-state generation is due to Zhang *et al.* [11] who experimentally demonstrated a circuit with a success probability of 3/16. The GHZ states [12] are substantially harder to generate and few results are known for the general case [13,14]. To our knowledge, the best result for heralded 3-GHZ generation is reported in Ref. [15] and guarantees a success probability of 1/256 without feedforward and 1/32 if feedforward is allowed.

*gubarev@datadvance.net

The step-by-step recipe for designing a circuit implementing a particular multiqubit linear-optical gate does not exist. A few examples of insights on linear-optical gate construction may be found in the literature [9–11]. However, for a general problem of finding an optical circuit guaranteeing maximal gate success probability, a more generic approach should be considered. For instance, the linear-optical transformation of the input Fock state may be described in terms of a system of polynomial equations [16], which has a well-known numerical solution—the Buchberger algorithm—unfortunately, with an EXPSPACE complexity.

Better performance may be achieved by formulating the circuit design task as an optimization problem, which fits the unitary transformation of the circuit to a desired quantum gate and minimizes some figure of merit, for example, fidelity of the desired gate and the current gate computed during the procedure [17]. This methodology of the quantum gate design is highly sensitive to the details of the numerical optimization problem setup and thus requires accurate formulation.

Here, we report a detailed analysis of the numerical optimization procedure of finding linear-optical circuits for the heralded generation of a 3-GHZ state. As a result, we present a circuit for dual-rail encoded 3-qubit GHZ state generation with a probability of 1/54 representing a nearly fivefold improvement over the best known result [15]. A part of this circuit may be used to generate two-qubit Bell states with a probability of 2/27. Both circuits do not require any feedforward.

II. PROBLEM SETUP

We consider a problem of finding a unitary transformation $\mathcal{U}$ of an initial separable state of N_{ph} photons in $N + M$ modes,

$$|\psi_{\mathrm{in}}\rangle = \prod_{k=1}^{N_{\mathrm{ph}}} a_{i_k}^{\dagger} |0\rangle^{\otimes[N+M]}, \qquad (1)$$

such that particular measurement patterns in M ancillary modes herald the desired N-mode target states with maximal success probability (see Fig. 1). In particular, we will be most interested in maximally entangled two- and three-photon target states (Bell-like and GHZ families), assuming
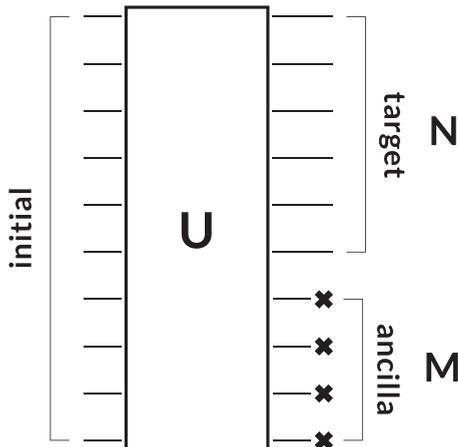

FIG. 1. Generic problem setup illustrated for the case $N = N_{\mathrm{ph}} = 6$, $M = 4$.

the detectors are capable of distinguishing zero, one, and more than one photons, and focus on single-photon ancillary states. The transformation $\mathcal{U}$ of the photonic state in the Fock space corresponds to a unitary transformation U of the annihilation operators, describing an underlying $N + M$ mode interferometer. Matrix elements of $\mathcal{U}$ are related to permanents of the matrix U [18].

Quantitatively, there are two objects to consider: Probability $P_a = \sum_m |\langle m, a|\mathcal{U}|\psi_{\mathrm{in}}\rangle|^2$ of ancillary state $|a\rangle$ detection and corresponding overlaps $\mathcal{M}_{t,a} = P_a^{-1}|\langle t, a|\mathcal{U}|\psi_{\mathrm{in}}\rangle|^2$ of the heralded wave function with target vectors, where $|m, a\rangle$ denotes a normalized Fock-space state $|m_1, \ldots, m_N, a_1, \ldots, a_M\rangle$ with $M_{\mathrm{ph}} = \sum_i a_i$ being the number of ancillary photons. Postselection (probability P_a) of a particular target state means that the ath column of the $\mathcal{M}$ matrix has a single unit element (remaining entries are zero), and for multiple targets the overall success probability is a sum of all appropriate P_a. Therefore, the goal is to find both the optimal set $\mathcal{A}(U)$ of admissible ancillary states and the corresponding unitary transformation U of optical modes,

$$\mathcal{A}(U) = \{a | \exists t^* : \mathcal{M}_{t^*,a}(U) = 1\},$$

$$U = \arg\max_V \sum_{a \in \mathcal{A}(V)} P_a(V). \qquad (2)$$

Note that the solution is not expected to be unique, therefore, it makes sense to augment the problem with additional performance measure(s). A natural choice comes from practical considerations: Among various equivalent solutions the "simplest" one is preferable, where "simplicity" is defined as the minimal number of nontrivial $U(2)$ factors (optical elements) required to realize a given unitary transformation. There are various ways to factorize unitary matrices [19–26], and here we stick exclusively with the approach of Ref. [24],

$$U(N) \ni U = D \cdot T_1^{(n_1, m_1)} \cdots T_Q^{(n_Q, m_Q)}, \qquad (3)$$

where $Q = N(N - 1)/2$, D is a diagonal matrix of pure phases, and $T^{(n,m)}$ are $U(2)$ rotations (two-mode "splitters"),

$$T = \begin{bmatrix} e^{i\varphi}\cos\theta & -\sin\theta \\ e^{i\varphi}\sin\theta & \cos\theta \end{bmatrix},$$

$$\theta \in [0, \pi/2], \quad \varphi \in [-\pi, \pi], \qquad (4)$$

embedded in (n, m) rows/columns. The transformation T becomes trivial at $\theta = \{0, \pi/2\}$—up to a global phase it reduces either to an identity or a permutation matrix. Therefore, an additional performance measure to be minimized is

$$S(U) = \sum_i \{(1 - \cos[4\theta_i]) + \varepsilon(1 - \cos[2\varphi_i])\}$$

$$+ \delta \sum_i |D_i - 1|^2, \qquad (5)$$

where ε and δ are small parameters, which gently push the respective phases towards "trivial" values (e.g., $\varphi_i = 0, \pm\pi$).

III. SOLUTION METHODOLOGY

We solve the above described problem using numerical optimization methods, supplemented with an analytic

postprocessing of the results. Our methodology consists of two main stages:

(1) A particular approximate solution of (2) is obtained using numerical methods (see below for details).

(2) Once the candidate ancillary indices $\mathcal{A}$ are established, we numerically solve (5) supplemented with appropriately lower-bounded ancilla probabilities P_a, $a \in \mathcal{A}$, and corresponding requirements on the overlap matrix elements.

These steps are repeated multiple times to assure a global search of an optimal solution, and the best results obtained are collected for further processing.

A silent feature of (2) is that it does not admit a direct formulation as a constrained optimization problem because neither the relevant set of ancillary indices A nor the target states with unit overlaps are known *a priori*. Theoretically, one could try to introduce additional discrete variables, however, available methods to solve the resulting nonlinear constrained mixed-integer task are rather inefficient and are likely to reduce to exhaustive enumeration. Experience revealed that the most efficient approach is to consider, following Ref. [27],

$$U = \arg\max_U \sum_{t,a} P_a \mathcal{M}_{t,a}^p, \qquad (6)$$

where the summation is done over all targets and ancillas and p is some positive power, which ensures sufficient suppression of small matrix elements $\mathcal{M}_{t,a}$ (in practice, we used $p = 3, 4, 5$). The resulting formulation has no explicit constraints and can be solved efficiently. However, optimal solutions of the original problem (2) generically become only local optima of (6), therefore, all extremal points of the latter are to be considered. Fortunately, this limitation is not very relevant in practice, since the most powerful gradient-based local optimization methods, which we use, find only local optima anyway. In more detail, the considered objective function is smoothly differentiable almost everywhere and its derivatives are known analytically. It follows then that (locally) optimal points are to be found most efficiently with second-order gradient-based algorithms of the (quasi-)Newton family. Specifically, we utilized a particular modern numerical realization of the dumped Broyden-Fletcher-Goldfarb-Shanno (BFGS) method stabilized with Wolf-like line search rules, which constitutes an inherent part of the *pSeven Core* algorithmic package (see Ref. [28] for more details). Although other suitable optimization techniques are applicable as well, their performance in the present context is expected to be much worse.

Another cornerstone of the proposed methodology is a proper parametrization of the unitary group. In this study an open neighborhood of an arbitrary $U_0 \in U(N + M)$ is parametrized via the Cayley transform

$$U = U_0 \frac{i - H}{i + H}, \qquad (7)$$

where H is an $(N + M) \times (N + M)$ Hermitian matrix with $(N + M)^2$ unconstrained real parameters. Representation (7) is well known in matrix analysis [29] and was proven to be efficient in various applications (see, e.g., Refs. [30,31]). In our case, for an arbitrary constant unitary U_0, the real parameters of H define the design space for the problem (6), the exploration of which is to be started at $H = 0$ with

local optimization methods. To ensure a globalized search we considered tens of thousands of Haar-random initial U_0, each of which were then locally optimized using the parametrization (7). Note that an appropriate solution to (6) is not always established—there is a large number of improper stationary points, $\mathcal{M}_{t,a} \neq 0, 1$, which do not admit identification of an optimal set $\mathcal{A}(U)$ and thus are to be rejected.

A suitable solution of (6) establishes both the subset of ancillary indices $\mathcal{A}$ and the set of overlaps $\mathcal{M}_{t,a}$ to be kept at unit value during the second stage. Therefore, next we consider the problem (5) supplemented with additional constraints

$$P_a \geqslant P_a^*, \quad \mathcal{M}_{t^*,a} = 1, \quad a \in \mathcal{A}, \qquad (8)$$

where P_a^* denotes the ancilla probabilities obtained at the first stage. In turn, the quality of the second stage solution is given by the minimal number of nontrivial optical elements within the decomposition (3). Therefore, at the second stage one has to solve a constrained single-objective optimization task (5) and (8), the solution of which was obtained with a sequential quadratically constrained quadratic programming (SQCQP) algorithm provided by *pSeven Core* [28]. The above two-step procedure is repeated several thousand times with different random starting points U_0 and different powers p. The selected set of best U's is left for further analytic treatment, to which we turn next.

IV. 3-GHZ STATE GENERATION

In this section we consider the problem of optimal three-particle GHZ state generation using six unentangled photons and four ancillary modes, which corresponds to $N = N_{\mathrm{ph}} = 6$, $M = 4$ in the setup in Fig. 1. Without loss of generality the input state is taken to be $|\psi_{\mathrm{in}}\rangle = |1\rangle^{\otimes 6}|0\rangle^{\otimes 4}$. The target vectors are $\pm$ superpositions of states with three photons in six modes and all mode occupation numbers being zero or one, e.g., $|t_k\rangle \propto |100110\rangle \pm |011001\rangle$ and all unique particle number permutations thereof (the second component is a binary complement of the first). Such states correspond to 3-qubit GHZ states in appropriately chosen dual-rail encodings. Admissible measurement patterns include states with three photons in four ancillary modes, where each mode contains zero or one photon (thus, there are only four legitimate heralding patterns).

Extensive numerical experiments revealed that solutions of (6) with the same quality appear quite often, e.g., a Haar-uniform distribution of initial points U_0 results in the same quality transformations in $\sim 20\%$ of cases. Meanwhile, the typical distance $\rho(U^*, U_0) = 1 - \mathrm{Tr}[U^* U_0^\dagger]/(N + M)$ between U_0 and the reached optimal element U^* is of the order $1/2$ [more precisely, it is $\langle \rho \rangle = 0.45(15)$ under a Gaussian approximation to the attained statistics]. A distinguishing feature of all numerically identified unitary matrices is that two and only two ancillary states have appropriate overlaps with the selected targets. Specific ancilla indices as well as heralded states might change, however, they always come in pairs. The extension or reduction of the number of target GHZ states does not change this property—the corresponding success probabilities remain $P_a = 0.009\,259\,26(1) \approx 1/108$ per each successful measurement.
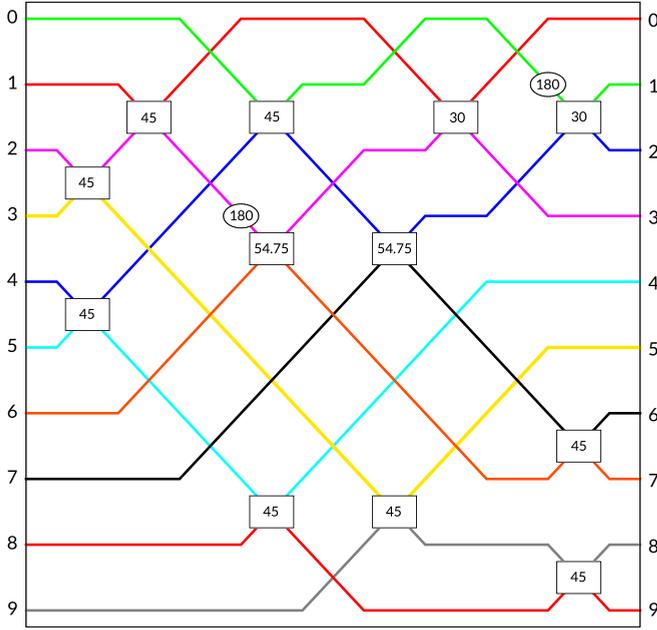
FIG. 2. The simplest scheme identified (12 two-mode elements). The port assignment agrees with Fig. 1 (the input state $|1\rangle^{\otimes 6}|0\rangle^{\otimes 4}$ is on the left). Ellipses represent single-mode phase shifters, and boxes stand for splitters (4) with $\varphi = 0$. All angles are in degrees rounded to the second digit when appropriate, in particular, $54.75° = \arccos\frac{1}{\sqrt{3}}$.
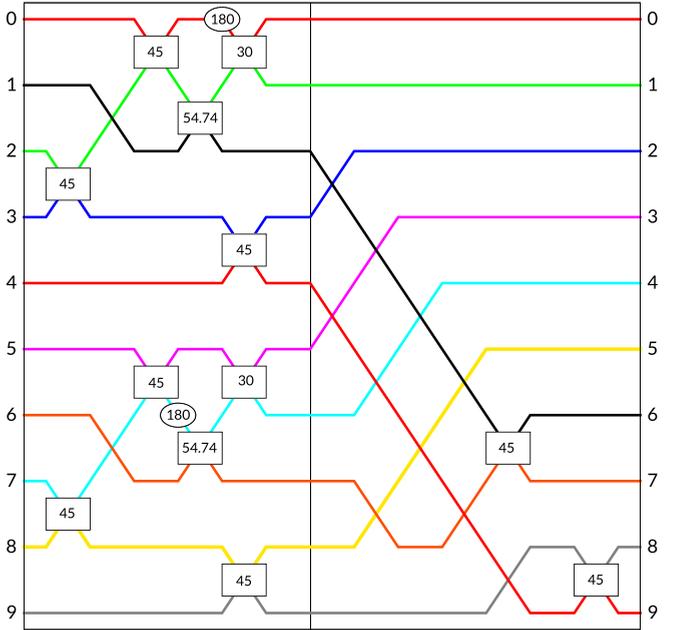

FIG. 3. Optical scheme decomposition, obtained via relabeling of the input (left-hand side) ports so that the appropriate initial state is $|1011010110\rangle$. Output ports are ordered in accordance with the $10 = 6 + 4$ convention, and the heralded state is in the first six modes. The vertical line separates the disjoint structure from the two-mode mixing elements and the output port permutations.

Candidate tuning via (5) and (8) indicated that the transformation complexity varies greatly, and the required minimal number of two-mode elements might be as large as ~ 30. However, we attribute this to the inherent multimodality of the considered formulation, because of which only locally optimal designs are often identified. Globalization is achieved as usual via the selection of the simplest unitaries demonstrating the same performance from those collected in all conducted runs. It turns out that the minimal attainable number of elementary splitters is 12, and at least we never encountered a better solution.

Finally, we collected a few dozen of the best optical transformations with the number of splitters equal to 12 and 13 [which is to be compared with the generic case of $10(10 - 1)/2 = 45$ elements]. It turned out that all of them are just the repetitions (up to permutations of ports and rearrangement of phase shifters) of the same scheme, presented in Fig. 2. Note that each box in the figure represents a two-mode transformation (4) taken at $\varphi = 0$, where ellipses denote single-mode phase shifts (actually, sign flips). The scheme of Fig. 2 is not a direct result of a numerical experiment—it was obtained with extensive analytic postprocessing (the reduction of phase shifters and the removal of unnecessary optical path crossings) and guessing of the involved algebraic numbers. Nevertheless, the numeric treatment was invaluable in its determination.

In fact, the established optical scheme is almost disjoint and consists of two nearly symmetric arms interconnected via a couple of 45° splitters at the output. The corresponding decomposition, equivalent to Fig. 2 up to the input port permutation, is shown in Fig. 3, where we kept a conventional $6 + 4$ ordering of the output ports at the expense of a perhaps redundant number of optical path crossings. Until the end of

the current section we will concentrate on this representation, although it seems not to be the most illuminating: We argue below that further scheme surgery delivers more comprehensive insights and reveals its connections with some known protocols.

An analytic form of the established transformation is easy to derive. The unitaries, corresponding to the top U_T and bottom U_B disjoint parts (to the right of the vertical line in Fig. 3), are almost the same,

$$
U_{T,B} = \begin{bmatrix}
\mp\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} & \frac{\pm 1}{2\sqrt{3}} & \frac{\mp 1}{2\sqrt{3}} \\
 & \frac{-1}{\sqrt{2}} & \frac{\pm 1}{2} & \frac{\mp 1}{2} \\
\frac{\pm 1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{\pm 1}{\sqrt{6}} & \frac{\mp 1}{\sqrt{6}} \\
 & & \frac{1}{2} & \frac{1}{2} & \frac{-1}{\sqrt{2}} \\
 & & \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{2}}
\end{bmatrix}, \quad (9)
$$

where only nonzero matrix elements are shown. In accordance with Fig. 3, the total transformation matrix is obtained from the block-diagonal $\mathrm{diag}[U_T, U_B]$ matrix via a permutation of rows (output ports), the left application of two 45° splitters (rows mixing), and relabeling of modes to arrive at the $10 = 6 + 4$ convention. The GHZ state is heralded in modes (0–5) if and only if single photons are detected in both (6,7) and in either one of (8,9) ports (the remaining one is to be found in a vacuum state). Each event happens with probability $P_a = 1/108$, so that the overall success rate is equal to $P_{\mathrm{success}} = 1/54$.

To justify the above assertion let us note that the transformed state is determined by the polynomial $(27 \cdot 2^5)^{-1} Q(a_0^\dagger \cdots a_9^\dagger)$ in creation operators,

$$Q = [A_{6,7}^+ - 2a_0^\dagger][A_{6,7}^- + 2a_3^\dagger]\left[A_{6,7}^+ - \sqrt{\frac{3}{2}}A_{8,9}^- + C^{(1)}\right]\left[A_{6,7}^- + \sqrt{\frac{3}{2}}A_{8,9}^+ + C^{(3)}\right]$$

$$\times \left[A_{6,7}^+ + \sqrt{\frac{3}{2}}A_{8,9}^- + C^{(2)}\right]\left[A_{6,7}^- - \sqrt{\frac{3}{2}}A_{8,9}^+ + C^{(4)}\right],$$

$$C^{(1,2)} = a_0^\dagger + \sqrt{3}(a_1^\dagger \pm a_2^\dagger),$$

$$C^{(3,4)} = -a_3^\dagger - \sqrt{3}(a_4^\dagger \mp a_5^\dagger),$$

(10)

where $A_{i,j}^\pm = a_i^\dagger \pm a_j^\dagger$. The required measurement patterns correspond to the products $a_6^\dagger a_7^\dagger a_8^\dagger$ and $a_6^\dagger a_7^\dagger a_9^\dagger$, which are entirely contained in the terms proportional to $(A_{6,7}^\pm)^2 A_{8,9}^\pm$ (all sign combinations). The structure of the above expression reveals that the monomials $(A_{6,7}^+)^2 A_{8,9}^-$ and $(A_{6,7}^-)^2 A_{8,9}^+$ enter with zero coefficients. The coefficients of the remaining same-sign monomials are given by

$$(A_{6,7}^+)^2 A_{8,9}^+ = 2a_6^\dagger a_7^\dagger(a_8^\dagger + a_9^\dagger) : 2\sqrt{\frac{3}{2}}(C^{(4)} - C^{(3)})(a_3^\dagger[C^{(1)} + C^{(2)}] - 2a_0^\dagger a_1^\dagger) = \frac{-1}{\sqrt{2}}(2\sqrt{3})^3 a_1^\dagger a_3^\dagger a_5^\dagger,$$

(11)

$$(A_{6,7}^-)^2 A_{8,9}^- = 2a_6^\dagger a_7^\dagger(a_9^\dagger - a_8^\dagger) : 2\sqrt{\frac{3}{2}}(C^{(2)} - C^{(1)})(a_0^\dagger[C^{(3)} + C^{(4)}] + 2a_0^\dagger a_3^\dagger) = \frac{1}{\sqrt{2}}(2\sqrt{3})^3 a_0^\dagger a_2^\dagger a_4^\dagger.$$

(12)

Therefore, the relevant terms in the transformed state are readily obtained,

$$a_6^\dagger a_7^\dagger a_8^\dagger : \frac{-1}{6\sqrt{3}}\frac{(a_0^\dagger a_2^\dagger a_4^\dagger + a_1^\dagger a_3^\dagger a_5^\dagger)}{\sqrt{2}},$$

(13)

$$a_6^\dagger a_7^\dagger a_9^\dagger : \frac{1}{6\sqrt{3}}\frac{(a_0^\dagger a_2^\dagger a_4^\dagger - a_1^\dagger a_3^\dagger a_5^\dagger)}{\sqrt{2}},$$

(14)

confirming our assertion.

V. SCHEME ANALYSIS AND BELL-STATE GENERATION

The above considerations were somewhat formal and only show that the established scheme operates properly, producing 3-GHZ states with a success probability of 1/54. In this section we perform a more detailed analysis and generalize the scheme to the case of maximally entangled two-photon Bell-state generation. It turns out that the resulting transformation shares some similarities with known protocols. Specifically, we will demonstrate how a well-known result of 2/27 probability for Bell-state generation [32] is reproduced using the building blocks identified in the 3-GHZ generation circuit.

Figure 4 represents a useful dissection of the optical scheme described above. Note that the heralded state (3-GHZ in this case) is to be found in the target ports $t_0 \cdots t_5$, the remaining ancillary modes are marked with the appropriate measured photon numbers, and the input occupation numbers are indicated explicitly (all other conventions are the same as before). Ω blocks to be discussed shortly are defined in Fig. 5, from which it follows that the scheme of Fig. 4 is identical to what we considered previously.

Despite its rather complex look, Fig. 4 admits a straightforward interpretation. Indeed, the four leftmost 45° splitters are designated to prepare an appropriate input state to be further processed in the Ω blocks, while the two analogous rightmost devices are dedicated to heralding measurements.

One can observe that the input ports $\Omega.1$ can receive zero or two photons only due to the Hong-Ou-Mandel interference at the preceding beam splitters [33]. For the same reasons and because of the indicated heralding measurements only the coherent superpositions of zero and two photons at the output ports $\Omega.2$ are relevant. Therefore, the scheme functions via a coordinated operation of two Ω blocks, while the complicated
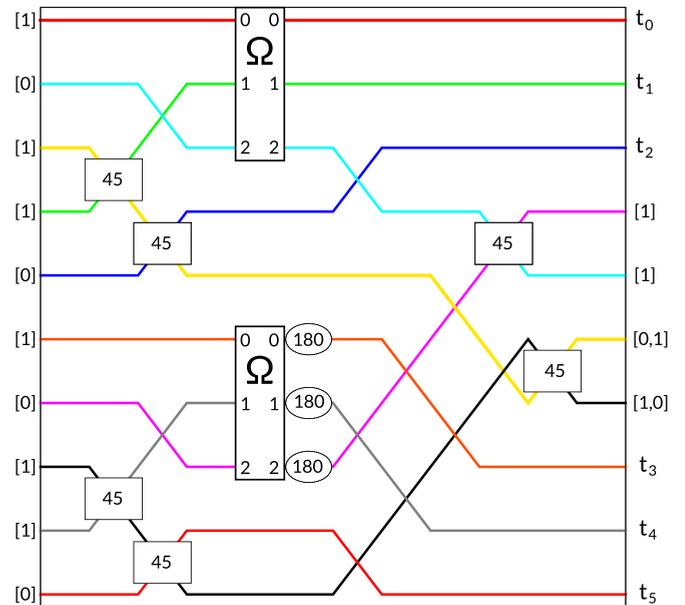

FIG. 4. Representation of the 3-GHZ state generation scheme equivalent to Fig. 3. The output ports are $t_0 \cdots t_5$, and the inputs are marked with appropriate photon numbers. The ancillary mode measurement patterns (on the left) are labeled with heralding photon counts. The 45° elements are the matrices (4) taken at $\varphi = 0$, ellipses represent π-phase shifts, and Ω blocks are detailed in Fig. 5.
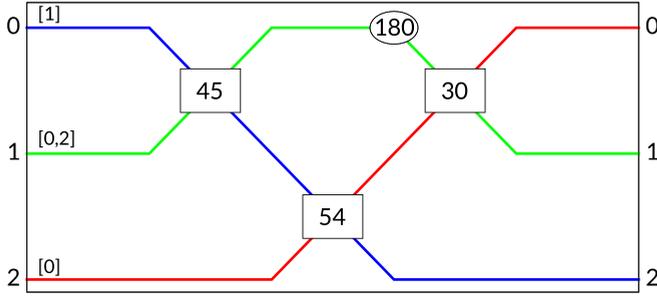
FIG. 5. Ω block of the considered optical circuit, and the appropriate number of photons is indicated in square brackets for each input port.

combination of 45° splitters is somewhat auxiliary and, in fact, is well known. It was proposed in Ref. [34] for multiphoton GHZ state production and provides a success probability of 1/64 in the three-photon case.

Therefore, it makes sense to consider a simplified version of the scheme (Fig. 6), which is aimed to produce Bell states. The only different element is an optional $\pi/2$-phase shift, marked as an s circle ($s = \pm 1$ or simply $s = \pm$), which implements a sign flip of a two-photon component amplitude, $|2\rangle \to s|2\rangle$. Qualitatively, the circuit operates in the same way as before, however, its quantitative characteristics deserve a separate discussion. Qubits a and b are identified with the output mode pairs (a_0, a_1), (b_0, b_1) and we use a set of Bell states associated with this dual-rail encoding: $|\phi^\pm\rangle \propto (a_0^\dagger b_0^\dagger \pm a_1^\dagger b_1^\dagger)|0\rangle$, $|\psi^\pm\rangle \propto (a_0^\dagger b_1^\dagger \pm a_1^\dagger b_0^\dagger)|0\rangle$. Below, we will need to analyze a few different Ω-like blocks, therefore, in accordance with expected input states and heralding measurements, it is worth considering a generic transformation of $\omega_0^\dagger$, $(\omega_1^\dagger)^2$,

$$\omega_0^\dagger \to \alpha \omega_2^\dagger + \beta_\omega,$$
$$\tfrac{1}{2}(\omega_1^\dagger)^2 \to A(\omega_2^\dagger)^2 + 2B_\omega \omega_2^\dagger + C_\omega, \quad (15)$$
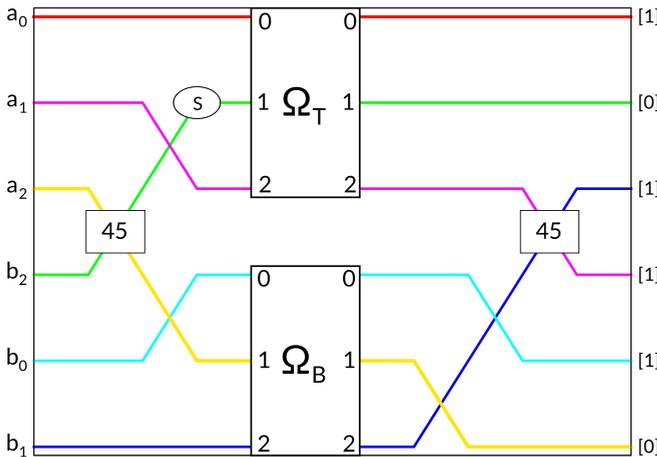

FIG. 6. Scheme to generate maximally entangled Bell states of two photons [ports (a_0, a_1) and (b_0, b_1)] using Ω blocks from Fig. 5. The ancillary modes are a_2, b_2, and input photon numbers are indicated in square brackets.

where α, A are block-specific numbers and B_ω, β_ω (C_ω) are linear (quadratic) in $\omega_{0,1}^\dagger$ creation operators, naturally assigned to respective modes. The transformation rule for $\omega_0^\dagger (\omega_1^\dagger)^2/2$ reads

$$\tfrac{1}{2}\omega_0^\dagger (\omega_1^\dagger)^2 \to (\omega_2^\dagger)^0(\cdots) + (\omega_2^\dagger)^1(D_\omega)$$
$$+ (\omega_2^\dagger)^2(A\beta_\omega + 2B_\omega\alpha) + (\omega_2^\dagger)^3(\cdots), \quad (16)$$

where $D_\omega = \alpha C_\omega + 2B_\omega\beta_\omega$ and dots denote unimportant terms. Indeed, in the proposed scheme of Fig. 6, heralding measurements require two photons in modes a_2, b_2 and select only the terms quadratic in $\omega_{T,2}^\dagger, \omega_{B,2}^\dagger$ operators. After the action of the very first 45° splitter the state is proportional to $\omega_{T,0}^\dagger \omega_{B,0}^\dagger[(\omega_{T,1}^\dagger)^2 - s(\omega_{B,1}^\dagger)^2]$, from which it follows that quadratic in $\omega_{T,2}^\dagger, \omega_{B,2}^\dagger$ expressions cannot arise from $\sim(\omega_2^\dagger)^0$, $\sim(\omega_2^\dagger)^3$ terms in Eq. (16). Finally, accounting for the leftmost 45° splitter and naturally identifying $\omega_{T,k}^\dagger = a_k^\dagger$, $\omega_{B,k}^\dagger = b_k^\dagger$, $k = \{0, 1\}$, one obtains the following expressions in front of the relevant operators,

$$a_2^\dagger b_2^\dagger : -[(1+s)A\beta_a\beta_b + 2\alpha(B_b\beta_a + sB_a\beta_b)], \quad (17)$$

$$\frac{(a_2^\dagger)^2}{\sqrt{2}}, \frac{(b_2^\dagger)^2}{\sqrt{2}} : \frac{1}{\sqrt{2}}[(1-s)A\beta_a\beta_b$$
$$+ 2\alpha(B_b\beta_a - sB_a\beta_b) \mp \alpha(D_b - sD_a)]. \quad (18)$$

For the Ω block illustrated in Fig. 5, the respective unitary transformation matrix is

$$U_\Omega = \begin{bmatrix} -\sqrt{2/3} & 1/\sqrt{6} & 1/\sqrt{6} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{bmatrix}, \quad (19)$$

from which it follows that

$$\alpha = 1/\sqrt{3}, \quad A = 1/6, \quad \beta_a = -\sqrt{2/3}a_0^\dagger,$$
$$B_a = \tilde{a}_0^\dagger/3\sqrt{2}, \quad C_a = (\tilde{a}_1^\dagger)^2/3, \quad D_a = \tilde{a}_0^\dagger \tilde{a}_1^\dagger/3, \quad (20)$$

where operators $\tilde{a}_{0,1}^\dagger$ are related to $a_{0,1}^\dagger$ via a 60° rotation, $\tilde{a}_{0,1}^\dagger = a_{0,1}^\dagger/2 \pm a_{1,0}^\dagger \sqrt{3}/2$. Using (17), one derives

$$a_2^\dagger b_2^\dagger : \frac{\sqrt{2}}{3\sqrt{3}} \frac{a_0^\dagger b_1^\dagger + s a_1^\dagger b_0^\dagger}{\sqrt{2}} = \frac{\sqrt{2}}{3\sqrt{3}}|\psi^s\rangle, \quad (21)$$

which implies that the measurement of the $|1_{a_2} 1_{b_2}\rangle$ ancillary state heralds the maximally entangled state of a and b qubits for either choice of sign s with a success probability of 2/27.

Finally, let us consider the significance of the rightmost 30° splitter in the Ω block discussed above. Upon removal of this optical element the scheme in Fig. 6 becomes similar to the one presented in Ref. [32], which, as claimed, operates with a 2/27 success rate [35]. Note, however, that this similarity is somewhat formal: In the scheme of Ref. [32], the coherent superposition of $|02\rangle$ and $|20\rangle$ states is fed to the 54° splitters (the input modes of $\Omega.2$ in Figs. 5 and 6), while our scheme requires it to be in $\Omega.1$. In either case, the modified Ω' block of Fig. 7 corresponds to

$$U_{\Omega'} = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 1/\sqrt{6} & 1/\sqrt{6} & -\sqrt{2/3} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{bmatrix}, \quad (22)$$
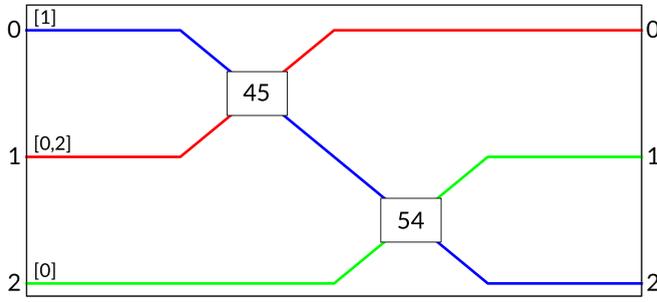
FIG. 7. Modified block Ω', which corresponds to (22). It leads to (23), when used within the circuit of Fig. 6.

from which one obtains the coefficients in the transformed wave function relevant for heralding measurements,

$$
\begin{aligned}
a_2^\dagger b_2^\dagger &: \frac{-\sqrt{2}}{3\sqrt{3}} \begin{cases} \frac{1}{2}|\psi^+\rangle - \frac{\sqrt{3}}{2}|\phi^-\rangle, & s = +, \\ |\psi^-\rangle, & s = -, \end{cases} \\[2ex]
\frac{(a_2^\dagger)^2}{\sqrt{2}} &: \frac{\sqrt{2}}{3\sqrt{3}} \begin{cases} (|\tilde{\psi}^-\rangle + |\tilde{\chi}^-\rangle)/\sqrt{2}, & s = +, \\ \frac{\frac{\sqrt{3}}{2}|\tilde{\phi}^-\rangle + \frac{1}{2}|\tilde{\psi}^+\rangle - |\tilde{\chi}^+\rangle}{\sqrt{2}}, & s = -, \end{cases} \quad (23) \\[2ex]
\frac{(b_2^\dagger)^2}{\sqrt{2}} &: \frac{\sqrt{2}}{3\sqrt{3}} \begin{cases} (|\tilde{\psi}^-\rangle - |\tilde{\chi}^-\rangle)/\sqrt{2}, & s = +, \\ \frac{\frac{\sqrt{3}}{2}|\tilde{\phi}^-\rangle + \frac{1}{2}|\tilde{\psi}^+\rangle + |\tilde{\chi}^+\rangle}{\sqrt{2}}, & s = -, \end{cases}
\end{aligned}
$$

where $|\chi^\pm\rangle \propto (a_0^\dagger a_1^\dagger \pm b_0^\dagger b_1^\dagger)|0\rangle$. One can see that a particular choice of sign s allows one to herald the states which are the closest to a conventional Bell basis. In particular, for $s = +1$ the modified scheme operates similarly, and the deleted $30°$ element effectively rotates $\frac{1}{2}|\psi^+\rangle - \frac{\sqrt{3}}{2}|\phi^-\rangle$ to $|\psi^+\rangle$.

VI. DISCUSSION

We have presented a general methodology for the numerical search of optimal linear-optical circuits for heralded entanglement generation. We discussed its application to design the circuit for a 3-GHZ state of dual-rail encoded photonic qubits. The obtained circuit has a success probability of $1/54$. Importantly, the proposed circuit does not require any feedforward and may be used with detectors resolving up to two photons.

It is important to note that although our heralding scheme (as well as most of the others) requires a minimal photon number resolution to detect the required ancillary Fock state correctly, recent progress in photon-number-resolving superconducting nanowire single-photon detectors (SNSPDs) [36,37] indicates that this technology is now available. Although the ancillary states heralding successful outcomes in our schemes contain only single-photon or vacuum states in each ancillary mode, the photon number resolution is required to dismiss the terms with higher occupation numbers leading to incorrect results. At the same time, since the gate scheme is designed in such a way that the number of ancillary photons heralding a successful result is always three and they are distributed in three distinct modes (two in two modes for Bell states), experimentally challenging heralding on vacuum is not required.

We also identify an elementary subcircuit which enables the dual-rail encoded Bell-state generation with probability $2/27$ and has the potential to be applied to other entanglement generation problems in linear-optical systems.

An important issue in real-world implementations of linear-optical circuits is the effect of loss. If the photon loss probability is uniform for all channels of the circuit, the overall effect will be just in reduction of the success probability. If, however, different channels experience different loss, the fidelity of the heralded state may be compromised [26,38,39]. If the proposed scheme is to be realized as an integrated optical circuit, it is therefore important to design the circuit topology in such a way that all the relevant paths are of equal length, such that the optical loss is distributed uniformly. This is, however, a general requirement for any implementation of an optical mode transforming unitary [24].

The main advantage of our numerical method, as shown by these two examples, is the possibility to find simple decompositions for the required unitaries by an optimization procedure, which may be used to bring insight to linear-optical entangling gate design.

[1] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[2] K. Kieling, T. Rudolph, and J. Eisert, Phys. Rev. Lett. **99**, 130501 (2007).

[3] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **115**, 020502 (2015).

[4] I. Schwartz, D. Cogan, E. R. Schmidgall, Y. Don, L. Gantz, O. Kenneth, N. H. Lindner, and D. Gershoni, Science **354**, 434 (2016).

[5] E. Knill, Phys. Rev. A **68**, 064303 (2003).

[6] J. C. Adcock, S. Morley-Short, J. W. Silverstone, and M. G. Thompson, Quantum Sci. Technol. **4**, 015010 (2019).

[7] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, Nat. Phys. **5**, 134 (2008).

[8] M. Pant, D. Towsley, D. Englund, and S. Guha, Nat. Commun. **10**, 1070 (2019).

[9] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[10] E. Knill, Phys. Rev. A **66**, 052306 (2002).

[11] Q. Zhang, X.-H. Bao, C.-Y. Lu, X.-Q. Zhou, T. Yang, T. Rudolph, and J.-W. Pan, Phys. Rev. A **77**, 062316 (2008).

[12] D. M. Greenberger, M. A. Horne, and A. Zeilinger, arXiv:0712.0921.

[13] D. B. Uskov, P. M. Alsing, M. L. Fanto, L. Kaplan, R. Kim, A. Szep, and A. M. Smith, J. Phys. B: At., Mol. Opt. Phys. **48**, 045502 (2015).

[14] V. Caprara Vivoli, J. Ribeiro, and S. Wehner, Phys. Rev. A **100**, 032310 (2019).

[15] M. Varnava, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **100**, 060502 (2008).

[16] N. M. VanMeter, P. Lougovski, D. B. Uskov, K. Kieling, J. Eisert, and J. P. Dowling, Phys. Rev. A **76**, 063808 (2007).

[17] D. B. Uskov, L. Kaplan, A. M. Smith, S. D. Huver, and J. P. Dowling, Phys. Rev. A **79**, 042326 (2009).

[18] S. Scheel, arXiv:quant-ph/0406127.

[19] A. Hurwitz, Nachr. Ges. Wiss. Goettingen, Math.-Phys. Kl. **1897**, 71 (1897).

[20] C. Jarlskog, J. Math. Phys. **46**, 103508 (2005).

[21] P. Dita, J. Phys. A: Math. Gen. **15**, 3465 (1982).

[22] P. A. Ivanov and N. V. Vitanov, Phys. Rev. A **77**, 012335 (2008).

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

[24] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, Optica **3**, 1460 (2016).

[25] M. Y. Saygin, I. V. Kondratyev, I. V. Dyakonov, S. A. Mironov, S. S. Straupe, and S. P. Kulik, Phys. Rev. Lett. **124**, 010501 (2020).

[26] S. A. Fldzhyan, M. Y. Saygin, and S. P. Kulik, Opt. Lett. **45**, 2632 (2020).

[27] S. Stanisic, N. Linden, A. Montanaro, and P. S. Turner, Phys. Rev. A **96**, 043861 (2017).

[28] DATADVANCE LLC, *pSeven Core Documentation*, https://www.datadvance.net/product/pseven-core.

[29] G. Golub and C. Van Loan, *Matrix Computations*, Johns Hopkins Studies in the Mathematical Sciences (Johns Hopkins University Press, Baltimore, 2013).

[30] F. Diele, L. Lopez, and R. Peluso, Adv. Comput. Math. **8**, 317 (1998).

[31] G. Hori, in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (IEEE, Piscataway, NJ, 2011), pp. 2116–2119.

[32] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, Science **349**, 711 (2015).

[33] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

[34] X. B. Zou, K. Pahlke, and W. Mathis, J. Opt. B: Quantum Semiclass. Opt. **7**, 119 (2005).

[35] Unfortunately, it appears impossible to reproduce the details of the cited circuit: The paper itself provides insufficient details, while the unitary matrix given in the Supplemental Material is misprinted and does not correspond to the required transformation.

[36] E. Schmidt, E. Reutter, M. Schwartz, H. Vural, K. Ilin, M. Jetter, P. Michler, and M. Siegel, IEEE Trans. Appl. Supercond. **29**, 2905566 (2019).

[37] D. Zhu, M. Colangelo, C. Chen, B. A. Korzh, F. N. C. Wong, M. D. Shaw, and K. K. Berggren, Nano Lett. **20**, 3858 (2020).

[38] N. J. Russell, L. Chakhmakhchyan, J. L. O'Brien, and A. Laing, New J. Phys. **19**, 033007 (2017).

[39] R. Burgwal, W. R. Clements, D. H. Smith, J. C. Gates, W. S. Kolthammer, J. J. Renema, and I. A. Walmsley, Opt. Express **25**, 28236 (2017).