We present a novel semi-analytical methodology to construct optimal linear optical circuits for heralded production of 3-photon GHZ and 2-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 states 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 [1], 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 multiqubit gates [2]. Even though current theoretical proposals explore ways to seamlessly incorporate non-deterministic entangling gates [3], the currently known linear optical quantum computer (LOQC) architectures still have to consume small entangled states as a resource for successful operation. Current state-of-the-art model for linear-optical quantum computing requires a deterministic source of entangled 3-photon states of the Greenberger-Horne-Zeilinger (GHZ) type [1]. 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. Successful operation of a postselected gate is identified post-factum 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 behaviour of the circuit [5]. In other words, the output of any postselected gate with non-unity 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 multi-photon entangled states. Last, but not least, the postselected 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.

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 new 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 percents of photon loss [1, 7]. 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 non-entangled ancillary photons and dual-rail encoded logical qubits. The first example of the heralded CZ gate was reported in the seminal work by Knill et al. [8] and had success probability of 1/16. Later on Knill devised a CZ gate circuit with 2 ancillary single photons [9] 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. [10] who experimentally demonstrated a circuit with success probability of 3/16. The GHZ states [11] are substantially harder to generate and few results are known for the general case [12, 13]. To our knowledge, the best result for heralded 3-GHZ generation is reported in [14] and guarantees the success probability of 1/256 without feedforward and 1/32 if feedforward is allowed.

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 [8–10]. However, for a general problem of finding an optical circuit guaranteeing maximal gate success probabil-
ity, 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 [15], 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 [16]. This methodology of the quantum gate design is highly sensitive to the details of 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 heralded generation of a 3-GHZ state. As a result we present a circuit for dual-rail encoded 3-qubit GHZ state generation with probability of 1/54 representing a nearly five-fold improvement over the best known result [14]. A part of this circuit may be used to generate two-qubit Bell states with probability of 2/27. Both circuits do not require any feedforward.

II. PROBLEM SETUP

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

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

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 2- and 3-photon target states (Bell-like and GHZ families), assuming the detectors are capable to distinguish zero, one, and more than one photons, and focus on single-photon ancillary states. The transformation $U$ 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 $U$ are related to permanents of the matrix $U$ [17].

Quantitatively, there are two objects to consider: probability $P_a = \sum_m |\langle m,a|U|\psi_{in}\rangle|^2$ of ancillary state $|a\rangle$ detection and corresponding overlaps $M_{t,a} = P_a^{-1} |\langle t,a|U|\psi_{in}\rangle|^2$ of the heralded wave function with target vectors, where $|m,a\rangle$ denotes a normalized Fock-space state $|m_1, m_2, a_1, \ldots, a_M\rangle$ with $M_{ph} = \sum a_i$ being the number of ancillary photons. Post-selection (probability $P_a$) of a particular target state means that the $a$-th column of the $M$ matrix has a single unit element (remaining entries are zero), for multiple targets overall success probability is a sum of all appropriate $P_a$.

![FIG. 1. Generic problem setup illustrated for the case $N = N_{ph} = 6$, $M = 4$.](image-url)

Therefore, the goal is to find both the optimal set $A(U)$ of admissible ancillary states and the corresponding unitary transformation $U$ of optical modes

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

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

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 non-trivial $U(2)$ factors (optical elements) required to realize a given unitary transformation. There are various ways to factorize unitary matrices [18–25], here we stick exclusively with the approach of Ref. [23]

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

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”):

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

$$\theta \in [0,\pi/2], \varphi \in [-\pi,\pi]$$

embedded in $(m,n)$ 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

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

$$+ \delta \sum_i |D_i - 1|^2,$$

where $\varepsilon$ and $\delta$ 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 analytic post-processing 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 $A$ are established, we numerically solve (5) supplemented with appropriately lower-bounded ancilla probabilities $P_a$, $a \in A$ and corresponding requirements on the overlap matrix elements.

These steps are repeated multiple times to assure a global search of an optimal solution, 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 non-linear 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. [26],

$$U = \arg \max_{U} \sum_{t,a} P_a M^a_{t,a},$$

where the summation is done over all targets and ancillas and $p$ is some positive power, which ensures sufficient suppression of small matrix elements $M_{t,a}$ (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.

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

$$U = U_0 \cdot \frac{i - H}{i + H},$$

where $H$ is an $(N + M) \times (N + M)$ Hermitian matrix with $(N + M)^2$ unconstrained real parameters.

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

$$P_a \geq P_a^*, \quad M^a_{t,a} = 1, \quad a \in A,$$

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 non-trivial optical elements within the decomposition (3). 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 STATES GENERATION

In this Section we consider the problem of optimal three particle GHZ-states generation using six unentangled photons and four ancillary modes, which corresponds to $N = N_{ph} = 6, M = 4$ in the setup in Fig. 1. Without loss of generality the input state is taken to be $|\psi_{in}\rangle = |1\rangle^{\otimes 6} |0\rangle^{\otimes 4}$. The target vectors are $\pm$ superpositions of states with 3 photons in 6 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 3 photons in 4 ancillary modes, where each mode contains zero or one photon (thus, there are only four
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. 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. Extension or reduction of the number of target GHZ states does not change this property, the corresponding success probabilities remain \( P_a = 0.00925926(1) \approx 1/108 \) per each successful measurement.

Candidates tuning via (5), (8) indicated that the transformation complexity varies greatly, the required minimal number of two-mode elements might be as large as \( \sim 30 \). However, we attribute this to inherent multimodality of the considered formulation, because of which only locally optimal designs are often identified. Globalization is achieved as usual via 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, at least we never encountered a better solution.

Finally, we collected a few dozens of 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 \( \varphi = 0 \), 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 post-processing (phase shifters reduction and removal of unnecessary optical path crossings) and guessing of 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 ports 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. Till 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:

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

where only non-zero matrix elements are shown. In accordance with Fig. 3, the total transformation matrix is obtained from the block diagonal \( [U_T, U_B] \) matrix via a permutation of rows (output ports), left application of two 45° splitters (rows mixing) and relabeling of modes to arrive to 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 equals to \( P_{\text{success}} = 1/54 \).

To justify the above assertion let us note that the transformed state is determined by the polynomial (27·
Therefore, the relevant terms in the transformed state correspond to the products 
\[ a_i^\dagger a_i^\dagger (a_k^\dagger + a_k^\dagger) \] 
and 
\[ a_i^\dagger a_i^\dagger (a_k^\dagger - a_k^\dagger) \]
which are entirely contained in the terms proportional to 
\[ (A_{6,7}^\dagger)^2 A_{8,9}^\dagger \] (all sign combinations). The structure of the above expression reveals that the monomials 
\[ (A_{6,7}^\dagger)^2 A_{8,9}^\dagger \] enter with zero coefficients. The coefficients of the remaining same-sign monomials are given by:

\[
2 \sqrt{3} \left( C^{(4)} - C^{(3)} \right) \left( a_1^\dagger \left[ C^{(1)} + C^{(2)} \right] - 2 a_0 a_1^\dagger \right) = - \frac{1}{\sqrt{2}} (2\sqrt{3})^3 a_1^\dagger a_3^\dagger a_5^\dagger,
\]

\[
2 \sqrt{3} \left( C^{(2)} - C^{(1)} \right) \left( a_0^\dagger \left[ C^{(3)} + C^{(4)} \right] + 2 a_0 a_4^\dagger \right) = \frac{1}{\sqrt{2}} (2\sqrt{3})^3 a_0^\dagger a_2^\dagger a_4^\dagger.
\]

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

\[
a_{00}^\dagger a_{00}^\dagger a_{00}^\dagger : -\frac{1}{6\sqrt{3}} \cdot \frac{a_{00}^\dagger a_{00}^\dagger a_{00}^\dagger + a_{00}^\dagger a_{00}^\dagger a_{00}^\dagger}{\sqrt{2}},
\]

\[
a_{01}^\dagger a_{01}^\dagger a_{01}^\dagger : \frac{1}{6\sqrt{3}} \cdot \frac{a_{01}^\dagger a_{01}^\dagger a_{01}^\dagger - a_{01}^\dagger a_{01}^\dagger a_{01}^\dagger}{\sqrt{2}},
\]
confirming our assertion.

V. SCHEME ANALYSIS AND BELL STATES GENERATION

The above considerations were somewhat formal and only show that the established scheme operates properly, producing 3-GHZ states with 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 states generation. It turns out that the resulting transformation shares some similarities with known protocols. Specifically, we will demonstrate how a

![FIG. 4. Representation of the 3-GHZ states generation scheme equivalent to Fig. 3. The output ports are t0 ... t5, the inputs are marked with appropriate photon numbers. The ancillary modes measurement patterns (on the left) are labelled with heralding photon counts. 45° elements are the matrices (4) taken at ϕ = 0, ellipses represent π-phase shifts, Ω blocks are detailed in Fig. 5.](image-url)
and, in fact, is well known. It was proposed in Ref. [29] for multi-photon GHZ states production and provides the 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 new element is an optional 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, $|2\rangle \rightarrow s|2\rangle$. 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: $|\psi^\pm\rangle \propto (a_0 b_0^\dagger \pm a_1 b_1^\dagger)|0\rangle$, $|\psi^\mp\rangle \propto (a_0 b_0^\dagger \pm a_1 b_1^\dagger)|1\rangle$. Below we will need to analyze a few different $\Omega$-like blocks, therefore, in accordance with expected input states and heralding measurements, it is worth to consider a generic transformation of $\omega_0^\dagger$, $\omega_1^\dagger$: $\omega_0^\dagger \rightarrow \alpha \omega_0^\dagger + \beta_\omega$ \hspace{1cm} (15)

where $\alpha$, $A$ are block-specific numbers and $B_\omega$, $\beta_\omega$, $[C_\omega]$ are linear [quadratic] in $\omega_{0,1}^\dagger$ creation operators, naturally assigned to respective modes. The transformation rule for $\omega_1^\dagger(\omega_1^\dagger)^2/2$ reads:

$$\frac{1}{2}(\omega_1^\dagger)^2 \rightarrow A(\omega_2^\dagger)^2 + 2B_\omega \omega_3^\dagger + C_\omega,$$

where $A$, $B_\omega$, $\beta_\omega$, $C_\omega$, $[C_\omega]$ are linear [quadratic] in $\omega_{0,1}^\dagger$ creation operators, naturally assigned to respective modes. The transformation rule for $\omega_1^\dagger(\omega_1^\dagger)^2/2$ reads:

$$\frac{1}{2} \omega_1^\dagger(\omega_1^\dagger)^2 \rightarrow (\omega_2^\dagger)^0 \cdot (\ldots) + (\omega_2^\dagger)^1 \cdot (D_\omega) + \cdot (\omega_3^\dagger)^2 \cdot (A_\beta_\omega + 2B_\omega \alpha) + (\omega_3^\dagger)^3 \cdot (\ldots),$$

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 $\omega_{1,2}^\dagger$, $\omega_{1,2}^\dagger$ operators. After the action of the very first $45^\circ$ splitter the state is proportional to $\omega_{1,2}^\dagger(\omega_{1,2}^\dagger)^2 - s(\omega_{1,2}^\dagger)^2$, from which it follows that quadratic in $\omega_{1,2}^\dagger$, $\omega_{1,2}^\dagger$ expressions cannot arise from $\sim (\omega_2^\dagger)^0$, $\sim (\omega_3^\dagger)^3$ terms in Eq. (16). Finally,

accounting for the left-most $45^\circ$ splitter and naturally identifying $\omega_{1,2}^\dagger = a_k^\dagger$, $\omega_{1,2}^\dagger = b_k^\dagger$, $k = \{0, 1\}$ one obtains the following expressions in front of the relevant operators:

$$a_k^\dagger b_k^\dagger : -[(1 + s)A_\beta_\omega 2 + 2\alpha(B_\omega \beta_\omega + sB_\omega \beta_\omega)],$$

$$\frac{(a_2^\dagger)^2}{\sqrt{2}}, \frac{(b_2^\dagger)^2}{\sqrt{2}} : \frac{1}{\sqrt{2}}[(1 - s)A_\beta_\omega + \alpha(D_\omega - sD_\omega)]$$

For the $\Omega$ block illustrated in Fig. 5 the respective unitary transformation matrix is

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

from which it follows that

$$\alpha = 1/\sqrt{3}, \quad A = 1/6, \quad \beta_\omega = -\sqrt{2/3}a_0^\dagger,$$

$$B_\omega = a_0^\dagger/3\sqrt{2}, \quad C_\omega = (a_1^\dagger)^2/3, \quad D_\omega = a_0^\dagger a_1^\dagger/3,$$

where operators $a_0^\dagger$ are related to $a_0^\dagger$ via a $60^\circ$ rotation, $a_0^\dagger = a_{0,1}^\dagger - a_{0,1}^\dagger 1/3$. Using (17) one derives

$$a_{2,3}^\dagger b_{2,3}^\dagger : \frac{\sqrt{2}}{3\sqrt{3}} a_{2,3}^\dagger b_{2,3}^\dagger + sa_{2,3}^\dagger b_{2,3}^\dagger = \frac{\sqrt{2}}{3\sqrt{3}} |\psi^\gamma\rangle,$$

which implies that the measurement of the $|1_{a_21_{b_2}\rangle}$ ancillary state heralds the maximally entangled state of $a$ and $b$ qubits for either choice of sign $s$ with success probability of $2/27$. 

FIG. 5. $\Omega$ block of considered optical circuit, the appropriate number of photons is indicated in square brackets for each input port.

FIG. 6. Scheme to generate maximally entangled Bell states of two photons (ports $(a_0,a_1)$ and $(b_0,b_1)$) using $\Omega$ blocks from Fig. 5. The ancillary modes are $a_2$, $b_2$, input photon numbers are indicated in square brackets.
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. [27], which, as claimed, operates with a 2/27 success rate [30]. Note however that this similarity is somewhat formal: in the scheme of Ref. [27] the coherent superposition of |0⟩ and |2⟩ states is fed to the 54° splitters (the input modes of Ω 2 in Fig. 5 and 6), while our scheme requires it to be in Ω 1. In either case, the modified Ω′ block of Fig. 7 corresponds to

$$U_{Ω'} = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 1/\sqrt{6} & 1/\sqrt{6} & -\sqrt{2}/3 \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{bmatrix}, \quad (22)$$

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

$$a_{2}^\dagger b_{0}^\dagger : \frac{-\sqrt{2}}{3\sqrt{3}} \begin{cases} \frac{1}{\sqrt{2}}|ψ^+⟩ - \frac{\sqrt{3}}{2}|ϕ^−⟩, & s = +1 \\ |ϕ^−⟩, & s = −1 \end{cases} \quad (23)$$

$$a_{0}^\dagger a_{1}^\dagger : \frac{\sqrt{2}}{3\sqrt{3}} \begin{cases} (|ψ^+⟩ + |ϕ^−⟩)/\sqrt{2}, & s = +1 \\ 2\sqrt{2}|ϕ^−⟩ + |ϕ^+⟩ = |χ^−⟩, & s = −1 \end{cases}$$

$$b_{0}^\dagger : \frac{\sqrt{2}}{3\sqrt{3}} \begin{cases} (|ψ^−⟩ + |ϕ^−⟩)/\sqrt{2}, & s = +1 \\ 2\sqrt{2}|ϕ^−⟩ + |ϕ^+⟩ = |χ^−⟩, & s = −1 \end{cases}$$

where |χ^±⟩ ∝ (a_{0}^\dagger a_{1}^\dagger ± b_{0}^\dagger b_{1}^\dagger)|0⟩. 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 $\frac{1}{2}|ψ^+⟩ - \frac{\sqrt{3}}{2}|ϕ^−⟩$ to $|ψ^+⟩$.

VI. DISCUSSION

We have presented a general methodology for numerical search of optimal linear optical circuits for heralded entanglement generation. We discussed its application to design the circuit for 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 feed-forward and may be used with detectors resolving up to two photons, and, to the best of our knowledge, its success probability surpasses all known results for such type of linear optical entangling gates. It is important to note that although our heralding scheme (as well as most of the others) requires minimal photon number resolution to detect the required ancillary Fock state correctly, recent progress in photon-number-resolving SNSPDs [31, 32] indicates that this technology is now available.

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, fidelity of the heralded state may be compromised [25, 33, 34]. 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 [23].

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 new insight to the linear optical entangling gate design.

VII. ACKNOWLEDGEMENTS

The authors acknowledge financial support under the Russian National Technological Initiative via MSU Quantum Technology Centre and RFBR grant 19-52-80034. I.V. Dyakonov acknowledges support from RFBR grant 19-32-80020.

[1] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, From three-photon greenberger-horne-zeilinger states to ballistic universal quantum computa-
A. Hurwitz, *Ber die Erzeugung der Invarianten durch*

C. Jarlskog, *A Recursive Parametrization of Unitary Matrices*

N. M. VanMeter, P. Lougovski, D. B. Uskov, K. Kieling, D. B. Uskov, L. Kaplan, A. M. Smith, S. D. Huver, and M. Varnava, *D. E. Browne, and T. Rudolph, How Good*

J. C. Adcock, S. Morley-Short, J. W. Silverstone, and M. G. Thompson, *Hard Limits on the Postselectability of Optical Graph States*

I. Schwartz, D. Cogan, E. R. Schmidgall, Y. Don, L. Gantz, O. Kenneth, N. H. Lindner, and D. Gershoni, *Deterministic Generation of a Cluster State of Entangled Photons*

J. C. F. Matthews, T. Hashimoto, J. L. O’Brien, and A. Laing, *Universal Linear Optics*

D. Zhu, M. Colangelo, C. Chen, B. A. Korzh, F. N. C. Wong, M. D. Shaw, and K. K. Berggren, *Resolving Photon-Number Resolving SNSPD Using Poissonian and Sub-Poissonian Light*

M. Zhu, M. Colangelo, C. Chen, B. A. Korzh, F. N. C. Wong, M. D. Shaw, and K. K. Berggren, *Resolving Photon-Number Resolving SNSPD Using Poissonian and Sub-Poissonian Light*

M. Varnava, D. E. Browne, and T. Rudolph, *How Good*

D. B. Uskov, P. M. Alsing, M. L. Fanto, L. Kaplan, R. Kim, A. Szep, and A. M. Smith, *Resource-Efficient Generation of Linear Cluster States by Linear Optics with Postselection*

E. Knill, Quantum gates using linear optics and postselection, *Phys. Rev. A 66, 052306 (2002)*

Q. Zhang, X.-H. Boo, C.-Y. Lu, X.-Q. Zhou, T. Yang, T. Rudolph, and J.-W. Pan, *Demonstration of a Scheme for the Generation of “Event-Ready” Entangled Photon Pairs from a Single-Photon Source*

D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going Beyond Bell’s Theorem*, arXiv e-prints, arXiv:0712.0921 (2007), arXiv:0712.0921 [quant-ph]

D. B. Uskov, P. M. Alsing, M. L. Fanto, L. Kaplan, R. Kim, A. Szep, and A. M. Smith, *Resource-Efficient Generation of Linear Cluster States by Linear Optics with Postselection*, *Journal of Physics B: Atomic, Molecular and Optical Physics 48, 045502 (2015)*

V. Caprara Vivoli, J. Ribeiro, and S. Wehner, *High-Fidelity Greenberger-Horne-Zeilinger State Generation within Nearby Nodes*, *Phys. Rev. A 100, 032310 (2019)*

M. Varnava, D. E. Browne, and T. Rudolph, *How Good Must Single Photon Sources and Detectors Be for Efficient Linear Optical Quantum Computation?*, *Phys. Rev. Lett. 100, 060502 (2008)*

N. M. VanMeter, P. Lougovski, D. B. Uskov, K. Kieling, J. Eisert, and J. P. Dowling, *General Linear-Optical Quantum State Generation Scheme: Applications to Maximally Path-Entangled States*, *Phys. Rev. A 76, 063808 (2007)*

D. B. Uskov, L. Kaplan, A. M. Smith, S. D. Huver, and J. P. Dowling, *Maximal Success Probabilities of Linear-Optical Quantum Gates*, *Phys. Rev. A 79, 042326 (2009)*

S. Scheel, *Permanents in Linear Optical Networks*, arXiv:quant-ph/0406127 (2004)

A. Hurwitz, *Ber die Erzeugung der Invarianten durch Integration*, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse 1897, 71 (1897)*

C. Jarlskog, *A Recursive Parametrization of Unitary Matrices*, *Journal of Mathematical Physics 46, 103508 (2005)*

P. Dita, *Parametrisation of Unitary Matrices*, *Journal of Physics A: Mathematical and General 15, 3465 (1982)*

P. A. Ivanov and N. V. Vitanov, *Synthesis of Arbitrary Unitary Transformations of Collective States of Trapped Ions by Quantum Householder Reflections*, *Phys. Rev. A 77, 012335 (2008)*

M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Experimental Realization of Any Discrete Unitary Operator*, *Physical Review Letters 73, 58 (1994)*

W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Koltzhammer, and I. A. Walmsley, *Optimal Design for Universal Multiport Interferometers*, *Optica 3, 1460 (2016)*

M. Y. Saygin, I. V. Kondratyev, I. V. Dyakonov, S. A. Mironov, S. S. Straupe, and S. P. Kulik, *Robust Architecture for Programmable Universal Unitaries*, *Phys. Rev. Lett. 124, 010501 (2020)*

S. A. Fldzhyan, M. Y. Saygin, and S. Kulik, *Optimal Design of Error-Tolerant Universal Multiport Interferometers*, *Opt. Lett. 45, 1 (2020)*

S. Stanisic, N. Linden, A. Montanaro, and P. S. Turner, *Generating Entanglement with Linear Optics*, *Phys. Rev. A 96, 043861 (2017)*

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, *Universal Linear Optics*, *Science 349, 711 (2015)*

C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of Subpicosecond Time Intervals between Two Photons by Interference*, *Phys. Rev. Lett. 59, 2044 (1987)*

X. B. Zou, K. Pahlke, and W. Mathis, *Generation of a Multi-Photon Greenberger–Horne–Zeilinger State with Linear Optical Elements and Photon Detectors*, *Journal of Optics B: Quantum and Semiclassical Optics 7, 10.1088/1464-4266/7/7/m01 (2005)*

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 supplementary materials is misprinted and does not correspond to the required transformation.

E. Schmidt, E. Reutter, M. Schwartz, H. Vural, K. Ilin, M. Jetter, P. Michler, and M. Siegel, *Characterization of a Photon-Number Resolving SNSPD Using Poissonian and Sub-Poissonian Light*, *IEEE Transactions on Applied Superconductivity 29, 2905566 (2019), arXiv:1810.11256 [physics.ins-det]*

D. Zhu, M. Colangelo, C. Chen, B. A. Korzh, F. N. C. Wong, M. D. Shaw, and K. K. Berggren, *Resolving Photon Numbers Using a Superconducting Tapered Nanowire Detector*, arXiv e-prints, arXiv:1911.09485 (2019), arXiv:1911.09485 [physics.ins-det]

N. J. Russell, L. Chakhmakhchyan, J. L. O’Brien, and A. Laing, *Direct Dialling of Haar Random Unitary Matrices*, *New Journal of Physics 19, 033007 (2017)*

R. Burgwal, W. R. Clements, D. H. Smith, J. C. Gates, W. S. Koltzhammer, J. J. Renema, and I. A. Walmsley, *Using an Imperfect Photonic Network to Implement Random Unitaries*, *Optics Express 25, 28236 (2017)*