Multiphoton Tomography with Linear Optics and Photon Counting

Leonardo Banchi, W. Steven Kolthammer, and M. S. Kim
QOLS, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom

(Received 3 July 2018; published 18 December 2018; corrected 8 March 2019)

Determining an unknown quantum state from an ensemble of identical systems is a fundamental, yet experimentally demanding, task in quantum science. Here we study the number of measurement bases needed to fully characterize an arbitrary multimode state containing a definite number of photons, or an arbitrary mixture of such states. We show this task can be achieved using only linear optics and photon counting, which yield a practical though nonuniversal set of projective measurements. We derive the minimum number of measurement settings required and numerically show that this lower bound is saturated with random linear optics configurations, such as when the corresponding unitary transformation is Haar random. Furthermore, we show that for N photons, any unitary $2N$ design can be used to derive an analytical, though nonoptimal, state reconstruction protocol.

DOI: 10.1103/PhysRevLett.121.250402

Introduction.—An unknown quantum state can be determined by making a set of suitable measurements on identically prepared copies [1–5]. This procedure, known as quantum state tomography, is a fundamental concept in quantum science with wide ranging applications. For example, tomography allows one to assess quantum systems for use in quantum information processing by quantifying resources such as entanglement [6], quantum correlations [7], and coherence [8]. Indeed, since most measures of these resources require complete knowledge of the density matrix describing a system, full quantum tomography is often necessary. Similarly, tomography can be applied to quantum sensing [9,10] to evaluate the capacity of a quantum probe state to yield enhanced measurement precision [11,12].

A well-established framework for photonic quantum information uses a single photon and multiple modes to encode discrete-variable quantum states. A qubit may be encoded using a single-photon, two-mode state [13], and a qudit may be encoded by incorporating additional modes [14]. Multiqubit states of this form have been employed widely, including entanglement-based quantum-key distribution [15], quantum simulation [16], tests of quantum nonlocality [17], entanglement generation [18], and linear optical quantum computing [19]. For these states, optical tomography can be readily achieved using combinations of single-qudit measurements [2,20], which require only linear optics and single-photon detection. Exact reconstruction of N qubits can thus be achieved using $2^N + 1$ measurement bases. Using this method, full tomography of up to six single-photon qubits has been demonstrated [21].

However, this approach to optical tomography does not apply to more general states of multiple modes containing a definite total number of photons. In this case, a mode may contain multiple photons, which enables new applications including approaches to quantum sampling [22], imaging [23], and error correction [24,25]. An alternate approach to state tomography for such states is to use balanced homodyne detection and well-developed continuous-variable algorithms to reconstruct the phase-space Wigner function [26–28]. In the general continuous variable setting, however, only partial reconstruction is possible with a finite number of measurement settings. Furthermore, this detection scheme adds substantial experimental requirements, including access to a mode-matched, multimode phase-stable local oscillator. In contrast, since the state has a definite photon number, tomographically complete measurements can theoretically be formulated using a finite number of measurement bases. Whether or not these measurement bases can be achieved using photon counting, though, has not been previously known.

Here we prove that an arbitrary state of N indistinguishable photons in M modes can be reconstructed using a finite number of measurement bases that correspond to different configurations of an M-mode linear-optical interferometer followed by photon counting. Notably, this result is not limited to states that can be created from Fock states using linear optics. Furthermore, we derive a minimal number of interferometer configurations required for a given N and M.

Our results extend to arbitrary mixtures of states with fixed, but possibly different, number of photons and to measurement strategies that incorporate additional modes through the use of ancillary vacuum states. As the number of measured modes increases, the required number of interferometer configurations decreases, eventually reaching one. In this limit, our work relates to previous studies of tomography using a single measurement basis in an extended Hilbert space [29,30], a concept first applied experimentally to nuclear spins [31] and then to single-photon qubits measured using a multimode quantum walk

[32,33]. The latter approach was recently extended to two-photon, two-mode states using a six-mode interferometer and it was conjectured this method would work for larger systems [34,35]. Related work has investigated how the number of additional modes required for high-fidelity state estimation depends on the purity of the input state [36]. Our results generalize these photonic studies that use a single measurement configuration by proving tomographic feasibility, deriving a bound on the minimum number of measurement modes, and providing an explicit reconstruction protocol.

We numerically show that use of random interferometer configurations, in particular those corresponding to Haar-random transformations, enable tomography using the minimum number of configurations. Additionally, we derive an analytical algorithm for state tomography that employs any unitary $2N$-design [37], thus generalizing a known result for qudit systems [38] to the multiphoton case. While unitary designs are not optimal for our task, an advantage is they have been extensively studied in the past for their relevance in many quantum information theory protocols [39] and quantum metrology [40]. Indeed, unitary designs can be obtained either with random circuits [41–44], random basis switching [45] or, more physically, by applying random pulses to a controllable system [46].

Feasibility of tomography.—Consider a generic quantum state of N indistinguishable photons in M modes. Our goal is to completely characterize the state by measuring multiple copies of it using linear optics and photon counting, as illustrated in Fig. 1. In this approach, a measurement basis corresponds to a particular configuration of linear optics. We also allow for measurements over $M' \geq M$ modes, achieved by appending $M' - M$ vacuum modes to the state of interest. Our first main result is that full tomography can always be achieved using a finite number of measurement configurations:

Theorem 1: An N-photon, M-mode state can be reconstructed using photon counting and an M-mode linear optical interferometer with a finite number R of configurations, where

$$R < \binom{N + M^2 - 1}{N}^2. \tag{1}$$

The theorem is proved by building an explicit reconstruction algorithm. Let $|\nu\rangle$ be the multimode Fock basis $|\nu\rangle \equiv |k_1, \ldots, k_M\rangle$, where k_j is the number of particles in mode j and $\sum_j k_j = N$, while we use a prime to denote a Fock basis $|\nu'\rangle \equiv |k_1, \ldots, k_{M'}\rangle$, where the number of output modes M' may be higher than the number of inputs M. Moreover, let $U(g)$ be a set of available unitary operations that can be made in the system. In linear optics the most general SU(M') transformation can be obtained with a collection of beam splitters and phase shifters [47], as shown in Fig. 1. Such transformation can be expressed

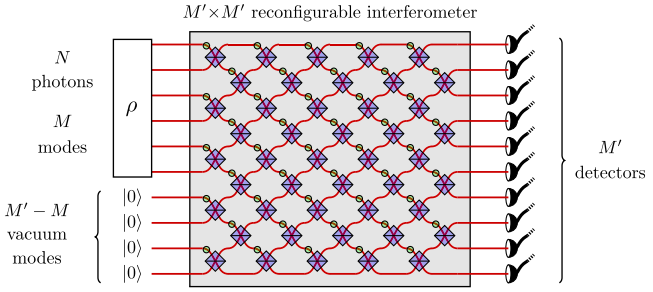

FIG. 1. Tomography of a generic unknown state ρ of N photons in M modes. Our protocol uses configurations of an M'-mode linear optical interferometer followed by photon counting. When $M' > M$, vacuum modes are appended to the state ρ.

in the second quantized notation as $U(g) = e^{i\sum_{kl} H_{kl} a_k^\dagger a_l}$, where $g = e^{iH}$ is a $M' \times M'$ unitary matrix.

State tomography requires reconstruction of the state ρ from measurement outcomes, each specified by a series of photon counts ν'. These outcome probabilities are readily calculated as $p_{\nu',g} = \langle \nu' | U(g)^\dagger \rho U(g) | \nu' \rangle$ for a specified interferometer configuration g. Expanding the above equation gives

$$p_{\nu',g} = \sum_{\alpha,\beta} \langle \nu' | U(g)^\dagger | \alpha \rangle \langle \alpha | \rho | \beta \rangle \langle \beta | U(g) | \nu' \rangle \equiv [\mathcal{L}(\rho)]_{\nu',g}, \tag{2}$$

with the superoperator $\mathcal{L}_{\nu' g,\alpha\beta} = \langle \nu' | U(g)^\dagger | \alpha \rangle \langle \beta | U(g) | \nu' \rangle$. The superoperator $\mathcal{L}$ is constructed using different configurations g_j, with $j = 1, \ldots, R$. The numbers α and β index the elements of the Fock space, whose dimension is $D_{N,M} = \binom{N+M-1}{N}$, while $\nu' = 1, \ldots, D_{N,M'}$. As such, $\mathcal{L}$ is normally a rectangular operator. Tomography is possible if there is a large enough R such that the linear system [Eq. (2)] admits a unique solution for any p. A unique solution is obtained [48] when the Gramian matrix $\mathcal{L}^\dagger \mathcal{L}$ has full rank. In this case, the best reconstruction algorithm [48] is given by the pseudo-inverse $\rho_{\text{best}} \coloneqq (\mathcal{L}^\dagger \mathcal{L})^{-1} \mathcal{L}^\dagger [p]$, which is always the best fit solution that minimizes the least-square error.

For any linear optics configuration g, the matrix elements $\langle \beta | U(g) | \nu' \rangle$ can be calculated exactly, either using combinatorial expressions or matrix permanents [22,49,50]: for $|\alpha\rangle = |a_1, a_2, \ldots\rangle$ and $|\beta\rangle = |b_1, b_2, \ldots\rangle$, one finds $\langle \alpha | U(g) | \beta \rangle = \text{per}(g_{\{\alpha,\beta\}}) / \sqrt{\alpha! \beta!}$ where $\alpha! = a_1! a_2! \ldots$, and similarly for $\beta!$, while $g_{\{\alpha,\beta\}}$ is the $N \times N$ matrix obtained by copying a_i times the ith columns of g, and b_j times the jth row of g. Although the computation of the matrix permanent is #P-hard, it is still possible for the values of N and M available in near-term devices [51]. Moreover, there are cases for which specific values of the permanent can be computed analytically [52–54]. In the worst case, without making any simplifications about

the permanents, in the Supplemental Material [55] we show that the number of operations to reconstruct the state from Eq. (2) is $\mathcal{O}(\mathrm{poly}(D_{N,M}, 2^N))$. Therefore, as in qubit systems, the difficulty is mostly due to exponentially growing Hilbert space, rather than to the complexity of the permanent.

Given the above framework, we now sketch our proof of Theorem 1, which is elaborated in the Supplemental Material [55]. In particular, we show that with interferometer configurations $\{g_j\}_{j=1,\ldots,R}$ corresponding to a unitary $2N$-design, exact reconstruction is possible from experimental measurements of p_{ν',g_j} for all $j = 1, \ldots, R$. Our theorem then follows from known properties of unitary designs [37]: they exist for all N and M, and their size is bounded by $R < D^2_{N,M^2}$.

To connect our tomographic task to unitary designs, we first note that the matrix $\mathcal{L}$ is composed by $U(g) \otimes U(g)^*$ matrices. Although $U(g)$ is an irreducible representation of g, $U(g) \otimes U(g)^*$ is not, and indeed it can be written as a direct sum of Wigner-D matrices $\mathcal{D}^{\lambda_r}_{m,m'}$ where λ_r refer to different irreducible representations and m, m' are Gelfand-Tsetlin patterns that index the different states (see Supplemental Material [55]). Since the matrices $\mathcal{D}^{\lambda_r}_{m,m'}(g)$ are orthogonal over g and $\mathcal{L} \propto \mathcal{D}(g)$, one can use the matrix $\mathcal{D}(g)^*$ to construct an operator $X^{\nu'}_{\alpha\beta}(g)$ such that $\langle\alpha|\rho|\beta\rangle = \sum_{\nu'} \int dg X^{\nu'}_{\alpha\beta}(g) p_{\nu',g}$, where $p_{\nu',g}$ are the outcome probabilities in Eq. (2).

Tomography is therefore achieved via a formal average over the continuous group. However, this is not practical as it would require an infinite number of measurement configurations. Instead we use the theory of weighted unitary designs [37], to replace the continuous average with a discrete average over a discrete set of unitaries g_j. A q-design is a discrete set of unitaries such that the weighted average of group functions $f(g)$ over those unitaries is equal to the average over the continuous group $\int dg f(g)$, provided that $f(g)$ is a polynomial of at most degree q in g and g^*. Since the matrices $\mathcal{D}(g)$ are a polynomial of at most degree N in g and g^*, one can choose any weighted $2N$-design protocol to analytically perform full-state tomography, as shown in the Supplemental Material [55]. Calling g_j those unitaries, $\langle\alpha|\rho|\beta\rangle = \sum_{\nu',j} X^{\nu'}_{\alpha\beta}(g_j) p_{\nu',g_j}$. This concludes the proof of Theorem 1. We note, however, that unitary $2N$-designs satisfy a more stringent requirement than the simpler inversion of Eq. (2), and consequently, this approach is generally not optimal in terms of the number of measurement configurations used. Theorem 1 can be trivially extended to mixtures $\rho = \sum_{N=1}^{N_{\max}} \pi_N \rho_N$ where ρ_N is an M-mode N-photon state, as each N-photon state can be reconstructed independently via postselection (see Supplemental Material [55]).

Minimum measurement configurations.—We now consider the minimum number of linear optics configurations R required to achieve tomography. Our second main result gives a lower bound on the number of configurations required:

Theorem 2: An N-photon, M-mode state can be reconstructed with photon counting and an M-mode linear optical interferometer using at least

$$R_{N,M} = \binom{N+M}{N} - \binom{N+M-2}{M} \tag{3}$$

configurations. More generally, for an interferometer with $M' > M$ modes and ancillary vacuum states, the minimal number of reconfigurations is

$$R_{N,M,M'} = \left[\frac{(N+M-2)!(M'-2)!}{(N+M'-2)!(M-2)!} R_{N,M}\right], \tag{4}$$

where $[x]$ is the smallest integer greater than or equal to x.

Equation (3) shows that the number of measurement configurations is larger than estimated from a simple counting argument. In particular, the number of M-mode Fock states with N total photons, $D_{N,M} = \binom{N+M-1}{N}$, gives the dimension of the symmetric Hilbert space. A generic state is thus specified by $D^2_{N,M} - 1$ independent elements.

A single measurement configuration involves $D_{N,M}$ different outcomes, which provide $D_{N,M} - 1$ independent parameters. Therefore, one may expect that $D_{N,M} + 1$ configuration may be sufficient for full state reconstruction. Instead, our theorem shows a larger number is required, $R_{N,M} > D_{N,M} + 1$. This increased requirement is due to linear optics providing only a subset of the possible unitary operations on the multiparticle state. Nonetheless, complete tomography with a smaller set of configurations is possible with ancillary output modes, as $R_{N,M,M'} < D_{N,M} + 1 < R_{N,M}$ for any $M' > M$.

For the two-mode case, $M = 2$, an explicit measurement protocol which saturates our bound $R_{N,2} = 2N + 1$ is known [61]. This protocol exploits the Schwinger boson formalism that maps our problem onto the tomography of a spin $S = N/2$, allowing the use of known algorithms for large spin systems [48,62,63]. However, this approach exploits properties of SU(2) representations that cannot be easily adapted to larger M [64,65]. Our theorem generalizes the above construction to the general multimode case.

Two proofs of Theorem 2 are presented in the Supplemental Material [55], one based on representation theory and one based on irreducible tensors. Here we briefly describe the main steps of the second proof. Measuring diagonal elements in the Fock basis is equivalent to the measurement of all the expectation values of polynomials of number operators $T^k_k = a^\dagger_k a_k$. According to Wick's theorem, all independent polynomials in the number operators can be written via the rank r tensors

$T^{k_1,\ldots,k_r}_{k_1,\ldots,k_r} = a^\dagger_{k_1}\cdots a^\dagger_{k_r} a_{k_1}\cdots a_{k_r}$. However, not all $\langle T^{k_1,\ldots,k_r}_{k_1,\ldots,k_r}\rangle$ are independent. For instance, if one measures $\langle T^k_k\rangle$ for $k = 1,\ldots,M-1$, then one gets $\langle T^M_M\rangle = N - \sum_{k=1}^{M-1}\langle T^k_k\rangle$ without further measurements. In the Supplemental Material [55] we show that the number of independent rank-r tensors is $D_{r,M-1}$. Their expectation values for $r = 1,\ldots,N$ completely and uniquely specify photodetection measurements. Similarly, the full state is completely and uniquely specified by the expectation value of the tensors $T^{k_1,\ldots,k_r}_{\ell_1,\ldots,\ell_r} = a^\dagger_{k_1}\cdots a^\dagger_{k_r} a_{\ell_1}\cdots a_{\ell_r}$. The number of such independent rank-r tensors is $D^2_{r,M} - D^2_{r-1,M}$.

Tomography then consists in reconstructing the expectation value of off-diagonal tensors from the measurement of $\langle T^{k_1,\ldots,k_r}_{k_1,\ldots,k_r}\rangle$ after different configurations $U(g)$. Since the latter corresponds to $\langle U(g)^\dagger T^{k_1,\ldots,k_r}_{k_1,\ldots,k_r} U(g)\rangle = [g^{\dagger\otimes r}\langle T\rangle g^{\otimes r}]^{k_1,\ldots,k_r}_{k_1,\ldots,k_r}$, all off-diagonal tensors with different rank r can be reconstructed independently for $r = 1,\ldots,N$. The most difficult tensor to reconstruct is then that with $r = N$. Via dimensional counting, this reconstruction requires $[D^2_{N,M} - D^2_{N-1,M}]/D_{N,M-1} \equiv R_{N,M}$ transformations. Equation (3) follows by assuming that the same configurations are sufficient for reconstructing an even lower rank tensor. This latter assumption is the reason why Eq. (3) is a lower bound. Similarly, Eq. (4) appears for a different number of modes as $R_{N,M,M'} = [(D^2_{N,M} - D^2_{N-1,M})/D_{N,M'-1}] \equiv [R_{N,M}D_{N,M-1}/D_{N,M'-1}]$.

Theorem 2 can be extended to mixtures $\rho = \sum_{N=1}^{N_{\max}} \pi_N \rho_N$ where ρ_N is a M-mode N-photon state. In this case, the minimal number of settings is $\max_{N\le N_{\max}} R_{N,M,M'}$ (see Supplemental Material [55]). Theorem 2 also determines the number of ancillary modes needed to achieve tomography with a single measurement configuration:

Corollary: An N-photon, M-mode state can be reconstructed with a single configuration of an M'-mode linear optical interferometer if

$$D_{N,M'-1} \ge D^2_{N,M} - D^2_{N-1,M} = R_{N,M}D_{N,M-1}. \tag{5}$$

The scaling of Eq. (5) can be investigated for large N and M using the entropic expansion $\binom{n}{k} \approx 2^{nH_2(k/n)}$, where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. If additionally $N \gg M$, we find that $R_{N,M}D_{N,M-1} \approx N^{2M-3}$, and $D_{N,M'-1} \approx N^{M'-2}$. Therefore the minimum number of measurement modes required is given by

$$M' \overset{N\gg M}{\gtrsim} 2M - 1. \tag{6}$$

In this limit, tomography can be achieved using a single measurement configuration with photon counting over twice as many modes as the input state, and this result is independent of N.

In the opposite limit $N \ll M$, we approximate $\binom{N+M}{M} \approx M^N/N!$ to find

$$M' \overset{N\ll M}{\gtrsim} \frac{M^2}{\sqrt[N]{N!}}. \tag{7}$$

This seemingly counterintuitive result shows that the required number of measured modes decreases as the number of photons increases. This is due to the large increase in the number of measurement outcomes that results from an increase in the number of photons.

Practical implementation.—We have done extensive numerical experiments showing that the bound Eq. (3) is achieved by Haar-random configurations $\{g_\alpha\}_{\alpha=1,\ldots,R}$, which can be implemented using programmable interferometers [66,67]. In particular, we find that $\mathcal{L}$ has full-rank $D^2_{N,M}$ only when $R_{N,M}$, or more, configurations are used. For $M' > M$, we find that the lower bound Eq. (4) is achievable with $R_{N,M,M'}$, or slightly more, configurations. The slightly larger number of configurations or modes required for full tomography when $M' \ne M$ may be due to the simple reconstruction algorithm, which does not explicitly take into account independent components and normalization.

The minimum number of measurement modes M' required for a single interferometer is shown in Fig. 2, which shows agreement of numerical results calculated using a single sample from the Haar distribution and the minimal number that satisfies Eq. (6). As predicted by Eq. (7), M' initially decreases as a function of N and then becomes constant for $N \approx M$. When $N \approx M$, we find $H_2 \approx 1$ and hence $M' \gtrsim \alpha M$, thus confirming the scaling

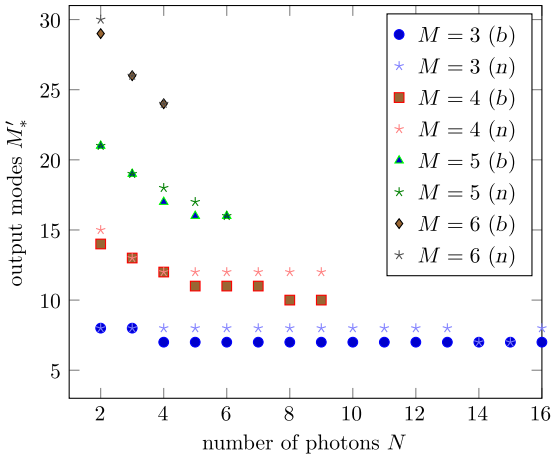

FIG. 2. Number of measurement output modes required for full tomography with a single experimental setup. The lower bound (b) is estimated from the minimal M' that satisfies Eq. (5). The observed numerical value (n) is obtained from the minimal M' such that Eq. (2) is invertible. For $M = 2$ we always observe $M' = 4$, consistently with Eq. (5).

relation Eq. (6), and its independence on N, although with a larger $\alpha > 2$. Based on these numerical experiments, we conjecture that with a single Haar-random configuration one can perform full reconstruction with a number of measurement modes that increases linearly with M.

In a realistic experiment, the number of detected photons will sometimes fluctuate, either because of imperfect photon sources (where N-photon states ρ_N are generated with probability π_N), photon losses [68], or imperfect detector efficiency [69,70]. When there are either imperfect sources or losses, the subset of detection events containing exactly the right number of photons is sufficient to reconstruct the state, provided these events occur at an acceptable rate. On the other hand, if losses are low and well characterized, one can use all the measured data to reconstruct the entire state $\rho = \sum_{N=1}^{N_{\max}} \pi_N \rho_N$ as we show in the Supplemental Material [55].

Single-photon detectors (SPDs) that merely distinguish between vacuum and nonvacuum states are often employed in realistic experiments, instead of true photon-counting detectors. To achieve sensitivity to the photon number, a nondeterministic number resolving detector (NRD) can be built by multiplexing SPDs using linear optics and ancillary vacuum states [71–73]. We note that this concept is consistent with the scheme shown in Fig. 1, and therefore for sufficiently large M', complete state reconstruction can be achieved with SPDs. Since a NRD sensitive to N photons requires N SPDs, Eq. (6) implies that $\mathcal{O}(NM)$ SPDs are required. For $N \ll M$ fewer SPDs are required, due to the vanishing probability that multiple photons emerge in the same mode of a random interferometer with $M > \mathcal{O}(N^2)$ [22]. More precisely, from Eq. (7) we get $M' > \mathcal{O}(M^2 N/\sqrt[N]{N!}) \approx \mathcal{O}(M^2)$.

Conclusion.—We have studied the feasibility and number of measurement configurations required to perform quantum tomography of a multimode multiphoton Fock state using linear optics and photon counting. We have shown that any such state can be tomographically reconstructed with a finite number of linear optics configurations (Theorem 1). To do so, we show that configurations corresponding to any unitary $2N$-design [37] define an analytical, thought nonoptimal, reconstruction protocol. Moreover, Theorem 2 quantifies the minimal number of configurations, even when the number of detectors M' is larger than M. For sufficiently many detectors, as specified by Eq. (5), this leads to tomography with a single measurement configuration. Our results can be used to test the optimality of tomography protocols with a finite number of particles. For instance, the two-photon protocol presented in Ref. [61] saturates our bound, and is therefore optimal. Finally, we presented a simple reconstruction algorithm based on Haar sampled unitary configurations, and we have observed that it is optimal for $M' = M$ and nearly optimal for $M' > M$.

The authors thank S. Filippov, S. Paesani, R. Santagati, N. Spagnolo, and B. Yadin, for discussions. This work is supported by the UK EPSRC Grant No. EP/K034480/1. M. S. K. thanks the Royal Society, the KIST Institutional Program (2E26680-18-P025), and the Samsung GRO grant for their financial support.

[1] G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, Quantum tomography, Adv. Imaging Electron Phys. **128**, 206 (2003).
[2] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Measurement of qubits, Phys. Rev. A **64**, 052312 (2001).
[3] K. Banaszek, G. M. Dariano, M. G. A. Paris, and M. F. Sacchi, Maximum-likelihood estimation of the density matrix, Phys. Rev. A **61**, 010304 (1999).
[4] M. Christandl and R. Renner, Reliable Quantum State Tomography, Phys. Rev. Lett. **109**, 120403 (2012); arXiv:1108.5329.
[5] H. Paul, P. Törmä, T. Kiss, and I. Jex, Photon Chopping: New Way to Measure the Quantum State of Light, Phys. Rev. Lett. **76**, 2464 (1996).
[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[7] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson, Unified View of Quantum and Classical Correlations, Phys. Rev. Lett. **104**, 080501 (2010).
[8] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. **89**, 041003 (2017).
[9] C. L. Degen, F. Reinhard, and P. Cappellaro, Quantum sensing, Rev. Mod. Phys. **89**, 035002 (2017).
[10] D. Braun, G. Adesso, F. Benatti, R. Floreanini, U. Marzolino, M. W Mitchell, and S. Pirandola, Quantum enhanced measurements without entanglement, Rev. Mod. Phys. **90**, 035006 (2018).
[11] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5**, 222 (2011).
[12] M. D. Vidrighin, G. Donati, M. G. Genoni, X.-M. Jin, W. S. Kolthammer, M. S. Kim, A. Datta, M. Barbieri, and I. A. Walmsley, Joint estimation of phase and phase diffusion for quantum metrology, Nat. Commun. **5**, 3532 (2014).
[13] I. L. Chuang and Y. Yamamoto, Simple quantum computer, Phys. Rev. A **52**, 3489 (1995).
[14] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment, Phys. Rev. Lett. **93**, 053601 (2004).
[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[16] I. Pitsios, L. Banchi, A. S Rab, M. Bentivegna, D. Caprara, A. Crespi, N. Spagnolo, S. Bose, P. Mataloni, R. Osellame *et al.*, Photonic simulation of entanglement growth and engineering after a spin chain quench, Nat. Commun. **8**, 1569 (2017).
[17] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[18] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska,

D. Bacco *et al.*, Multidimensional quantum entanglement with large-scale integrated optics, Science **360**, eaar7053 (2018).
[19] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, Rev. Mod. Phys. **79**, 135 (2007).
[20] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, Qudit quantum-state tomography, Phys. Rev. A **66**, 012303 (2002).
[21] C. Schwemmer, G. Tóth, A. Niggebaum, T. Moroder, D. Gross, O. Gühne, and H. Weinfurter, Experimental Comparison of Efficient Tomography Schemes for a Six-Qubit State, Phys. Rev. Lett. **113**, 040503 (2014).
[22] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (ACM, San Jose, CA, 2011), pp. 333–342.
[23] P. C. Humphreys, M. Barbieri, A. Datta, and I. A. Walmsley, Quantum Enhanced Multiple Phase Estimation, Phys. Rev. Lett. **111**, 070403 (2013).
[24] I. L. Chuang, D. W. Leung, and Y. Yamamoto, Bosonic quantum codes for amplitude damping, Phys. Rev. A **56**, 1114 (1997).
[25] W. Wasilewski and K. Banaszek, Protecting an optical qubit against photon loss, Phys. Rev. A **75**, 042316 (2007).
[26] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Measurement of the Wigner Distribution and the Density Matrix of a Light Mode using Optical Homodyne Tomography: Application to Squeezed States and the Vacuum, Phys. Rev. Lett. **70**, 1244 (1993).
[27] G. M. Dariano, M. F. Sacchi, and P. Kumar, Universal homodyne tomography with a single local oscillator, Phys. Rev. A **61**, 013806 (1999).
[28] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, Rev. Mod. Phys. **81**, 299 (2009).
[29] G. M. D'Ariano, Universal quantum observables, Phys. Lett. A **300**, 1 (2002).
[30] A. E. Allahverdyan, R. Balian, and Th. M. Nieuwenhuizen, Determining a Quantum State by Means of a Single Apparatus, Phys. Rev. Lett. **92**, 120402 (2004).
[31] J. Du, M. Sun, X. Peng, and T. Durt, Realization of entanglement-assisted qubit-covariant symmetric-informationally-complete positive-operator-valued measurements, Phys. Rev. A **74**, 042341 (2006).
[32] Y.-y. Zhao, N.-k. Yu, P. Kurzyński, G.-y. Xiang, C.-F. Li, and G.-C. Guo, Experimental realization of generalized qubit measurements based on quantum walks, Phys. Rev. A **91**, 042101 (2015).
[33] Z. Bian, J. Li, H. Qin, X. Zhan, R. Zhang, B. C. Sanders, and P. Xue, Realization of Single-Qubit Positive-Operator-Valued Measurement Via a One-Dimensional Photonic Quantum Walk, Phys. Rev. Lett. **114**, 203602 (2015).
[34] J. G. Titchener, A. S. Solntsev, and A. A. Sukhorukov, Two-photon tomography using on-chip quantum walks, Opt. Lett. **41**, 4079 (2016).
[35] J. Titchener, M. Gräfe, R. Heilmann, A. Solntsev, A. Szameit, and A. Sukhorukov, Scalable on-chip quantum state tomography, npj Quantum Inf. **4**, 19 (2018).
[36] D. Oren, M. Mutzafi, Y. C. Eldar, and M. Segev, Quantum state tomography with a single measurement setup, Optica **4**, 993 (2017).
[37] A. Roy and A. J. Scott, Unitary designs and codes, Des. Codes Cryptogr. **53**, 13 (2009).
[38] A. Roy and A. J. Scott, Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements, J. Math. Phys. (N.Y.) **48**, 072110 (2007).
[39] A. Ambainis and J. Emerson, Quantum t-designs: *t*-wise independence in the quantum world, in *Computational Complexity, 2007, CCC'07, Twenty-Second Annual IEEE Conference on* (IEEE, 2007), pp. 129–140.
[40] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acin, and M. Lewenstein, Random Bosonic States for Robust Quantum Metrology, Phys. Rev. X **6**, 041044 (2016).
[41] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, Commun. Math. Phys. **250**, 371 (2004).
[42] F. G. S. L. Brandao, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, Commun. Math. Phys. **346**, 397 (2016).
[43] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, Phys. Rev. A **80**, 012304 (2009).
[44] W. G. Brown and L. Viola, Convergence Rates for Arbitrary Statistical Moments of Random Quantum Circuits, Phys. Rev. Lett. **104**, 250501 (2010).
[45] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics, Phys. Rev. X **7**, 021006 (2017).
[46] L. Banchi, D. Burgarth, and M. J. Kastoryano, Driven Quantum Dynamics: Will It Blend?, Phys. Rev. X **7**, 041015 (2017).
[47] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, Optimal design for universal multiport interferometers, Optica **3**, 1460 (2016).
[48] G. Klose, G. Smith, and P. S. Jessen, Measuring the Quantum State of a Large Angular Momentum, Phys. Rev. Lett. **86**, 4721 (2001).
[49] S. Scheel, Permanents in linear optical networks, arXiv:quant-ph/0406127.
[50] L. C. Biedenharn, R. A. Gustafson, and S. C. Milne, $U(n)$ Wigner coefficients, the path sum formula, and invariant g-functions, Adv. Appl. Math. **6**, 291 (1985).
[51] A. Neville, C. Sparrow, R. Clifford, E. Johnston, P. M. Birchall, A. Montanaro, and A. Laing, Classical boson sampling algorithms with superior performance to near-term experiments, Nat. Phys. **13**, 1153 (2017).
[52] M. C. Tichy, K. Mayer, A. Buchleitner, and K. Mølmer, Stringent and Efficient Assessment of Boson-Sampling Devices, Phys. Rev. Lett. **113**, 020502 (2014).
[53] C. Dittel, R. Keil, and G. Weihs, Many-body quantum interference on hypercubes, Quantum Sci. Technol. **2**, 015003 (2017).
[54] N. Viggianiello, F. Flamini, L. Innocenti, D. Cozzolino, M. Bentivegna, N. Spagnolo, A. Crespi, D. J. Brod, E. F.

Galvao, and R. Osellame *et al.*, Experimental generalized quantum suppression law in sylvester interferometers, New J. Phys. **20**, 033017 (2018).

[55] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.121.250402 for the proofs of the main theorems, the study of imperfect photon sources and detectors, and other detailed analyses. Supplemental Material contains extra Refs. [56–60].

[56] A. Alex, M. Kalus, A. Huckleberry, and J. von Delft, A numerical algorithm for the explicit calculation of su(n) and sl(n, c) clebsch–gordan coefficients, J. Math. Phys. (N.Y.) **52**, 023507 (2011).

[57] M. Moshinsky, Gelfand states and the irreducible representations of the symmetric group, J. Math. Phys. (N.Y.) **7**, 691 (1966).

[58] N. J. Vilenkin and A. U. Klimyk, *Representation of Lie Groups and Special Functions: Recent Advances* (Springer Science & Business Media, Dordrecht, 2013), Vol. 316.

[59] N. J. Vilenkin and A. U. Klimyk, *Representation of Lie groups and special functions: Volume 3: Classical and quantum groups and special functions*, Vol. 75 (Springer Science & Business Media, 2013).

[60] H. J. Ryser, *Combinatorial Mathematics* (Mathematical Association of America; distributed by Wiley, New York, 1963), Vol. 14.

[61] R. Walser, Measuring the State of a Bosonic Two-Mode Quantum Field, Phys. Rev. Lett. **79**, 4724 (1997).

[62] R. G. Newton and B.-l. Young, Measurability of the spin density matrix, Ann. Phys. (N.Y.) **49**, 393 (1968).

[63] H. F. Hofmann and S. Takeuchi, Quantum-state tomography for spin-l systems, Phys. Rev. A **69**, 042108 (2004).

[64] S. N. Filippov and V. I. Manko, Spin tomography and star-product kernel for qubits and qutrits, J. Russ. Laser Res. **30**, 129 (2009).

[65] S.-H. Tan, Y. Y. Gao, H. de Guise, and B. C. Sanders, Su(3) Quantum Interferometry with Single-Photon Input Pulses, Phys. Rev. Lett. **110**, 113603 (2013).

[66] N. J. Russell, L. Chakhmakhchyan, J. L. OBrien, and A. Laing, Direct dialling of haar random unitary matrices, New J. Phys. **19**, 033007 (2017).

[67] R. Burgwal, W. R. Clements, D. H. Smith, J. C. Gates, W. S. Kolthammer, J. J. Renema, and I. A. Walmsley, Using an imperfect photonic network to implement random unitaries, Opt. Express **25**, 28236 (2017).

[68] R. García-Patrón, J. J. Renema, and V. Shchesnovich, Simulating boson sampling in lossy architectures, arXiv:1712.10037.

[69] H. Lee, U. Yurtsever, P. Kok, G. M. Hockney, C. Adami, S. L. Braunstein, and J. P. Dowling, Towards photostatistics from photon-number discriminating detectors, J. Mod. Opt. **51**, 1517 (2004).

[70] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Photon-number-resolving detection using time-multiplexing, J. Mod. Opt. **51**, 1499 (2004).

[71] D. Achilles, C. Silberhorn, C. Śliwa, K. Banaszek, and I. A. Walmsley, Fiber-assisted detection with photon number resolution, Opt. Lett. **28**, 2387 (2003).

[72] J. Řeháček, Z. Hradil, O. Haderka, J. Peřina, Jr., and M. Hamar, Multiple-photon resolving fiber-loop detector, Phys. Rev. A **67**, 061801 (2003).

[73] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Photon-number resolution using time-multiplexed single-photon detectors, Phys. Rev. A **68**, 043814 (2003).

Correction: Equation (4) contained minor typographical errors and has been fixed.