Quantum-state preparation with universal gate decompositions

Martin Plesch[1,2,3] and Časlav Brukner[1,4]
[1]*Faculty of Physics, University of Vienna, Vienna, Austria*
[2]*Faculty of Informatics, Masaryk University, Brno, Czech Republic*
[3]*Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia*
[4]*Institute of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Vienna, Austria*
(Received 30 March 2010; published 3 March 2011)

In quantum computation every unitary operation can be decomposed into quantum circuits—a series of single-qubit rotations and a single type entangling two-qubit gates, such as controlled-NOT (CNOT) gates. Two measures are important when judging the complexity of the circuit: the total number of CNOT gates needed to implement it and the depth of the circuit, measured by the minimal number of computation steps needed to perform it. Here we give an explicit and simple quantum circuit scheme for preparation of arbitrary quantum states, which can directly utilize any decomposition scheme for arbitrary full quantum gates, thus connecting the two problems. Our circuit reduces the depth of the best currently known circuit by a factor of 2. It also reduces the total number of CNOT gates from 2^n to $\frac{23}{24}2^n$ in the leading order for even number of qubits. Specifically, the scheme allows us to decrease the upper bound from 11 CNOT gates to 9 and the depth from 11 to 5 steps for four qubits. Our results are expected to help in designing and building small-scale quantum circuits using present technologies.

DOI: 10.1103/PhysRevA.83.032302 PACS number(s): 03.67.Ac, 03.67.Lx, 42.50.Dv

I. INTRODUCTION

Quantum information and computation theory ([1] and references therein) is receiving increased attention in the past few decades due to its possibility of outperforming information processing based on classical physics in the areas of secure communication [2] or efficient implementation of certain computation tasks, e.g., prime number factorization [3].

Similarly to classical computation, every quantum computation, represented as a unitary operation performed on a desired state of qubits, can be decomposed into small operation blocks, where only a subset of qubits is changed nontrivially. Whereas one-qubit operations cannot be composed to a general unitary operation, as they never change the degree of entanglement within the state, a single type of two-qubit operation (for example, a controlled-NOT, or CNOT [4]) in combination with arbitrary one-qubit rotations suffices [5].

The complexity of quantum circuits is usually measured by the number of CNOT gates needed to perform the desired unitary operation. The reason for counting the number of two-qubit gates is mainly experimental since their realization is much more demanding and introduces more imperfections than the realization of one-qubit gates. Adding every new CNOT gate to the circuit increases its overall imperfection. This constitutes the main obstacle preventing realization of quantum computation within sufficient precision. It is therefore crucial to design circuits with the least possible number of entangling gates.

In general, an exponential number of CNOT gates with respect to the number of qubits involved is needed to implement a general unitary operation. This can be seen by simple counting of parameters of an n-qubit unitary operation. Several attempts have been made to optimize the number of gates needed for general operations [6–15].

In situations where the input for a quantum computer or a quantum communication protocol is a known quantum state, we are not interested in performing a completely defined unitary transformation. Instead, we aim only to prepare a given state $|\phi\rangle$, i.e., to perform a transformation from an initial state $|\psi\rangle$ to a different target state, $|\psi\rangle \rightarrow |\phi\rangle$, where a whole class of unitaries U fulfills the condition $U|\psi\rangle = |\phi\rangle$.

It is known that one needs an exponential number of CNOT gates to prepare a generic quantum state; i.e., in the leading order this number is $N_{\text{CNOT}} = c \cdot 2^n$, where c is a prefactor and n is the number of qubits. Any optimization can only decrease the prefactor but cannot beat the exponential dependence. The best known result so far is $c = 1$ [9]. Here we give an explicit quantum circuit reducing the prefactor to $c = \frac{23}{24}$ for n even. Specifically, using our scheme we decrease the known upper bound from 11 CNOT gates to 9 for four qubits and from 57 CNOT gates down to 46 for six qubits, keeping the existing bound of 26 CNOT gates for five qubits. The lower bounds are 6, 13, and 29 CNOT gates, respectively (see below).

The reduction of the overall number of CNOT gates might be, however, not the only aim of the optimization procedure. In searching for efficient algorithms, the depth of the quantum circuit, i.e., the minimal number of computation steps required for accomplishing the computation, is crucial [16]. In a general case, the depth might be as high as the overall number of CNOT gates, not allowing us to perform more than one gate in parallel as is the case in Ref. [9]. In our scheme the depth is at most half the number of CNOT gates; i.e., at least two gates can be implemented in parallel in every step.

II. LOWER BOUNDS

A general n-qubit pure state is fully described by $2^{n+1} - 2$ real parameters. During the preparation process, these parameters are introduced sequentially by performing single-qubit rotations (in which each rotation introduces three Euler angles) along with CNOT gates. CNOT gates as such do not introduce any parameters, but they are a kind of barriers that separate one-qubit rotations such that they cannot merge into a resulting single rotation for each qubit. Naively, one could expect that every CNOT gate can be accompanied by two one-qubit operations—one for the control and one for the target qubit—applied after every CNOT gate. Due to existing identities [6], however, only four real parameters can be introduced with one CNOT gate. This can be understood as follows: Rotation about the z axis applied on the control qubit commutes with the CNOT gate. Similarly, rotation about the x axis applied on the target qubit commutes with the CNOT gate. In this way, the two types of rotations can be commuted backward through the CNOT gate and combined with the rotations applied after the previous CNOT gates acting on the respective qubits. Thus for every CNOT we can implement four real parameters of the desired state.

Further parameters can be added by local unitary transformations on qubits in the beginning of the process. Trivially, one would expect to introduce three real parameters per qubit, corresponding to the three Euler angles. However, this is not the case. By starting in a specific product state (e.g., $|0\rangle^{\otimes N}$), we may only rotate every single qubit into a given direction, which gives us two parameters per qubit. The third (missing) parameter is just a phase on every qubit, which sums up through all qubits and influences only the global phase. Therefore on n qubits, with k CNOT gates, we may introduce altogether up to $4k + 2n$ real parameters. This gives a lower bound on the number of CNOT gates needed to prepare a state: 6 for four qubits, 13 for five qubits and 29 for six qubits. For large numbers of n we get a lower bound on the number of CNOT gates of $k = \frac{1}{2}2^n$ in the leading order.

The lower limit for the depth of the circuit also grows exponentially with the number of qubits, with a linear correction. This can be seen from the fact that in one computation step no more than $\frac{n}{2}$ CNOT gates can be performed. The only possible optimization for the depth is also the reduction of the prefactor with up to a linear correction, with the lower bound $\frac{2^n}{n}$.

III. FOUR QUBITS

The Hilbert space of four qubits can be factorized into two parts, where each part is associated with two qubits. An arbitrary pure state $|\Psi\rangle$ of four qubits can then be expressed using the (standard) Schmidt decomposition as

$$|\Psi\rangle = \sum_{i=1}^{4} \alpha_i |\psi\rangle_i |\phi\rangle_i. \qquad (1)$$

Here $|\psi\rangle_i, i = 1, \ldots, 4$, are four normalized orthogonal states of the first two qubits and similarly $|\phi\rangle_i$ are four normalized orthogonal states of the second two qubits. The states are given with a nontrivial global phase. The coefficients α_i are real and positive and they obey $\sum_{i=1}^{4} \alpha_i^2 = 1$. Without loss of generality we can rewrite the decomposition (1) in such a way that $|\psi\rangle_i$ and $|\phi\rangle_i$ will be defined only up to a global phase. Their relative phases (with respect to different i's) will then be included in the generalized coefficients α_i, which become complex. As we are interested in $|\Psi\rangle$ up to its global phase, we can make the choice of having α_1 real and positive.

The pure state $|\Psi\rangle$ is specified by $2^5 - 2 = 30$ real parameters. The four states $|\psi\rangle_i$ are specified by 6, 4, 2, and 0 parameters (due to the orthogonality condition), and so are the four states $|\phi\rangle_i$. The four coefficients α_i require six independent real parameters to be determined due to the normalization condition and the choice of the global phase. This gives altogether 30 parameters, as expected.

A. Phase 1

To prepare the state $|\Psi\rangle$ starting from the initial state $|0000\rangle$, we first generate the state with the generalized (complex) Schmidt coefficients on the first two qubits:

$$|0000\rangle \rightarrow (\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle)|00\rangle. \qquad (2)$$

This operation does not define a unitary operation completely, but it is a state-preparation operation on two qubits (in which starting from a known state $|00\rangle$ we end in a state specified by the generalized Schmidt decomposition coefficients). Therefore, as shown in Ref. [11], it can be realized by one CNOT operation in combination with suitable one-qubit rotations.

B. Phase 2

We perform two CNOT operations, one with the control on the first qubit and the target on the third qubit and the other one with the control on the second qubit and the target on the fourth qubit. In such a way we can "copy" the basis states of the first two qubits onto the respective states of the second two qubits. In this way we obtain a state of four qubits, which has the same Schmidt decomposition coefficients as the target state (1):

$$\begin{aligned} &(\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle)|00\rangle \\ &\rightarrow (\alpha_1|00\rangle|00\rangle + \alpha_2|01\rangle|01\rangle + \alpha_3|10\rangle|10\rangle + \alpha_4|11\rangle|11\rangle). \end{aligned} \qquad (3)$$

For this phase we obviously only need two CNOT operations; one-qubit rotations are not necessary.

C. Phase 3

Keeping the Schmidt decomposition form we apply the unitary operation that transforms the basis states of the first two qubits into the four states $|\psi\rangle_i$. We obtain

$$\begin{aligned} &|00\rangle \rightarrow |\psi\rangle_1, \quad |01\rangle \rightarrow |\psi\rangle_2, \\ &|10\rangle \rightarrow |\psi\rangle_3, \quad |11\rangle \rightarrow |\psi\rangle_4. \end{aligned} \qquad (4)$$

As for any two-qubit unitary operation we do not need more than three CNOT gates [11].

D. Phase 4

In the final phase of the circuit we perform a unitary operation on the third and fourth qubits in order to transform their computational basis states into the Schmidt basis states of Eq. (1):

$$\begin{aligned} &|00\rangle \rightarrow |\phi\rangle_1, \quad |01\rangle \rightarrow |\phi\rangle_2, \\ &|10\rangle \rightarrow |\phi\rangle_3, \quad |11\rangle \rightarrow |\phi\rangle_4. \end{aligned} \qquad (5)$$

Similarly to the previous phase, we again use three CNOT operations. We conclude that altogether we have used $1 + 2 + 3 + 3 = 9$ CNOT gates for the entire quantum state preparation circuit (see Fig. 1), which is less than the best result of 11 CNOT

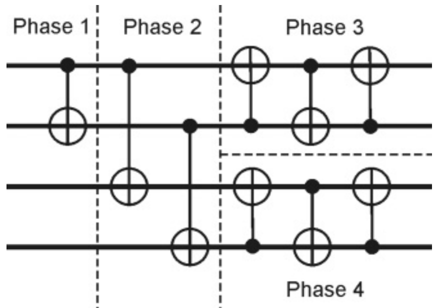

FIG. 1. Gate sequence for preparation of an arbitrary four-qubit state. Individual one-qubit rotations (not depicted) need to be applied between CNOT gates. The four individual phases are described in the text. The two CNOT gates in phase 2, as well as in phases 3 and 4, can be performed in parallel, as they address different qubits. Altogether one needs 9 CNOT gates, 4 pairs of which can be performed in parallel.

gates, which can be deduced from [9]. However, it stays above the minimum of 6 gates obtained from parameter counting.

The depth of the circuit is 5, where the second phase can be done in one computation step and the third and fourth phases can be done in parallel in three computation steps. This is less than half of the result of Ref. [9] and is optimal for 9 CNOT gates. The theoretical minimal depth is 3, deduced from the fact that at least 6 CNOT gates are needed and no more than two can be performed in one step.

IV. FIVE QUBITS

To illustrate our state preparation procedure for the case of odd number of qubits—where the entire Hilbert space cannot be factorized into Hilbert spaces of equal dimensions—we give an example for five qubits. We first factorize the Hilbert space into two parts, with one part associated with two qubits and the other one with three qubits. The Schmidt decomposition of an arbitrary five-qubit state with respect to such Hilbert space factorization has almost the same structure as in the case of four qubits in Eq. (1). One has

$$|\Psi\rangle = \sum_{i=1}^{4} \alpha_i |\psi\rangle_i |\phi\rangle_i. \tag{6}$$

Again, the summation goes at most over four terms and the only difference is that states $|\phi\rangle_i$, $i = 1, \ldots, 4$, are now three-qubit states. We again choose to include the relative phase of the states into the coefficients α_i and proceed with phases 1–3 in the same way as for four qubits. The only difference is in the fourth phase, where we perform a three-qubit unitary operation:

$$\begin{aligned} |00\rangle|0\rangle &\to |\phi\rangle_1, \quad |01\rangle|0\rangle \to |\phi\rangle_2, \\ |10\rangle|0\rangle &\to |\phi\rangle_3, \quad |11\rangle|0\rangle \to |\phi\rangle_4. \end{aligned} \tag{7}$$

Such unitary can be implemented by no more than 20 CNOT gates [11]. Moreover, this unitary is not completely defined (since the third qubit is initially exclusively in the state $|0\rangle$) and thus further reduction of the number of CNOT gates might be possible. Even without such optimizations, our state preparation procedure for five qubits requires $1 + 2 + 3 + 20 = 26$ CNOT gates, which achieves the result of Ref. [9]. The lover limit of 13 CNOT gates suggests that further optimization is possible.

The depth of the procedure is 22 computation steps, with 1 step for phase 1, 1 step for phase 2, and 20 steps for performing phases 3 and 4 in parallel. This is less than the lowest known depth of 26 of Ref. [9], but more than the theoretical lower bound of 7.

V. GENERAL CASE

We will now apply the main idea presented for four and five qubits to the general case of n qubits. We begin with factorization of the Hilbert space of n qubits into two parts of equal dimension for n even, so that each part is associated with $\frac{n}{2}$ qubits. For an odd number of qubits we factorize the Hilbert space into $\frac{n-1}{2}$ and $\frac{n+1}{2}$ qubits. On the first part of the qubits we will prepare a state whose amplitudes in the computational basis will be defined by the generalized Schmidt coefficients. Then we will apply a set of CNOT gates between the qubits in the first and second parts. In the end we will perform two unitary operations, one on the first part and one on the second part of the qubits. We will separately treat the case of even and odd numbers of qubits.

A. Even number of qubits

We write the number of qubits as $n = 2k$. The qubits are divided into two parts, each containing k qubits. With respect to this division the Schmidt decomposition of an arbitrary state of n qubits has the following form:

$$|\Psi\rangle = \sum_{i=1}^{2^k} \alpha_i |\psi\rangle_i |\phi\rangle_i, \tag{8}$$

where both $|\psi\rangle_i$ and $|\phi\rangle_i$ are normalized states of k qubits and α_i are complex coefficients.

The initial state of qubits is assumed to be the product state $|0\rangle^{\otimes 2k}$ in which each qubit is in state $|0\rangle$. On the first k qubits we prepare a superposition state whose amplitudes are the Schmidt coefficients in the computational basis:

$$|0\rangle^{\otimes 2k} \to \left(\sum_{i=1}^{2^k} \alpha_i |i\rangle \right) |0\rangle^{\otimes k}. \tag{9}$$

The sequence of 0's and 1's in the computational basis states $\{|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle\}$ represents the binary encoding of the index i in the states $|i\rangle$: Qubits in state $|1\rangle$ stand exactly on those positions where there is a 1 in the binary notation of i. All other qubits are in the state $|0\rangle$. To prepare a state on k qubits as required in Eq. (9), we can utilize the existing bound from Ref. [9], which allows us to prepare it with the help of $2^k - k - 1$ CNOT gates. We will later return to a discussion about further optimization possibilities of this particular phase.

In the second phase, we perform k CNOT gates with qubits j as the control and qubits $j + k$ as the target for j running from 1 to k. This will bring us to the desired Schmidt form of our state,

$$\left(\sum_{i=1}^{2^k}\alpha_i|i\rangle\right)|0\rangle^{\otimes k} \rightarrow \sum_{i=1}^{2^k}\alpha_i|i\rangle|i\rangle. \tag{10}$$

Phases 3 and 4 are k-qubit unitary operations performed on the first and second halves of the qubits, respectively. We obtain

$$\sum_{i=1}^{2^k}\alpha_i|i\rangle|i\rangle \rightarrow \sum_{i=1}^{2^k}\alpha_i|\psi\rangle_i|i\rangle \tag{11}$$

$$\rightarrow \sum_{i=1}^{2^k}\alpha_i|\psi\rangle_i|\phi\rangle_i, \tag{12}$$

which is the aimed target state (8). Every unitary operation acting on k qubits can be performed by $\frac{23}{48}2^{2k} - \frac{3}{2}2^k + \frac{4}{3}$ CNOT gates [11]. We thus need altogether $2^k - k - 1 + k + \frac{23}{24}2^{2k} - \frac{3}{2}2^{k+1} + \frac{8}{3}$ CNOT gates. This number is bounded from above by its leading term in k. Taking $n = 2k$ we obtain

$$N_{\text{CNOT}}^{\text{even}} < \frac{23}{24}2^n. \tag{13}$$

This is the new lowest number of CNOT gates needed for construction of a universal circuit for preparation of an arbitrary state.

In the first phase (9) of the procedure given above we used a method for state preparation, which requires more entangling gates than our method. Naturally, we can use our result recursively to obtain a slightly lower number of CNOT operations needed to prepare the state of the first k qubits. However, this part of the process does not contribute to the leading order of the number of CNOT gates needed for preparation as calculated in Eq. (13). The first phase contributes only with the order of $2^{\frac{n}{2}}$, whereas the phases 3 and 4 contribute with the order of 2^n.

The depth of the circuit is, in the leading order, given by the depth of phases 3 and 4, which is $\frac{23}{48}2^n$, less than the best previous result of 2^n, but weaker than the theoretical limit of $\frac{2^n}{n}$.

B. Odd number of qubits

We express the number of qubits as $n = 2k + 1$. The first three phases, as described by Eqs. (9)–(11) of the procedure, remain exactly the same as for the case of even number of qubits. In the fourth phase (12) we perform a unitary operation on $k + 1$ instead of k qubits. Summing up contributions from all four phases we obtain the overall number of CNOT gates required: $2^k - k - 1 + k + \frac{23}{48}2^{2k} - \frac{3}{2}2^k + \frac{4}{3} + \frac{23}{48}2^{2k+2} - \frac{3}{2}2^{k+1} + \frac{4}{3}$. Similarly to the previous case the leading order of this sum bounds the number of the CNOT gates from above. It can be simplified to $N_{\text{CNOT}}^{\text{odd}} < \frac{115}{96}2^n$. This result is weaker then the bound (13) for an even number of qubits. However, further optimizations are possible since in phase 4 the operation required is not a completely defined unitary and one does not necessarily need the whole number of CNOT gates as required for a general unitary rotation on $k + 1$ qubits. Moreover, even in this case the depth of the circuit bounded by $\frac{115}{192}2^n$ is smaller than the best known result.

VI. CONCLUSIONS

We give an explicit and efficient circuit for preparation of arbitrary states of n qubits using a gate library consisting of a single two-qubit gate (CNOT) and one-qubit rotations. For an even number of qubits we have slightly reduced the previously known upper bound on the number of CNOT gates needed. For the special case of four qubits our scheme requires only 9 CNOT gates (compared to 11 previously known), which should be within the scope of near-future quantum technology.

Our quantum state preparation scheme provides also a lower computational depth than the previously known results. It can be divided into four phases, where the last two can be performed in parallel, which leads to roughly half the computational steps compared to the previous results. This opens up further optimization possibilities for experimental implementation of the state preparation. Our results can help in designing and building small-scale quantum circuits using present technologies (see, e.g., Refs. [17,18]).

Our procedure introduces a conceptually simple utilization of efficient decomposition of arbitrary quantum gates for the problem of state preparation. In fact, the efficiency of our procedure is based on the best results for gate decompositions. If better results can be obtained in the future, they will directly lead to lowering of our bounds. Moreover, this utilization itself is very efficient: A circuit for gate decomposition reaching the lower bound of $4^{(n-2)}$ [6] CNOT gates in leading order would lead to state preparation with $2^{(n-1)}$ CNOT gates, reaching the lower bound in the leading order as well.

Using our scheme one can also efficiently apply operations that transform any given state $|\psi\rangle$ of n qubits to any other given state $|\phi\rangle$. We first run the preparation procedure for $|\psi\rangle$ in the reversed order, which results in the state $|0\rangle^{\otimes n}$. Then, we continue with preparing the aimed state $|\phi\rangle$. The number of CNOT gates needed to perform this composite transformation is just double the number needed to prepare an arbitrary state from $|0\rangle^{\otimes n}$. However, the reduction in the depth of the complete circuit is even greater than a factor of 2, as the last phase of the reversed process and the first phase of the preparation process can run on distinct qubits and therefore be performed in parallel.

ACKNOWLEDGMENTS

This work was supported by the Action Austria—Slovakia, SoMoPro project SIGA 862, the Austrian Science Foundation FWF within Project No. P19570-N16, SFB and CoQuS No. W1210-N16, and the European Commission Project QESSENCE. The collaboration is a part of the ÖAD/APVV SK-AT-0015-10 project.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[2] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984*, pp. 175–179.

[3] P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[4] CNOT, or controlled-NOT operation reverts the state of the target qubit if and only if the control qubit is in the state $|1\rangle$. It can be described in the computation basis as $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$, and $|11\rangle \rightarrow |10\rangle$, where, e.g., $|00\rangle$ denotes a product state in which both qubits are in the $|0\rangle$ state.

[5] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[6] V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).

[7] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004).

[8] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Phys. Rev. Lett. **93**, 130502 (2004).

[9] M. Möttönen, J. J. Vartiainen, V. Bergholm *et al.*, Quantum Inf. Comput. **5**, 467 (2005); V. Bergholm, J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. A **71**, 052330 (2005).

[10] V. V. Shende and I. L. Markov, Quantum Inf. Comput. **5**, 49 (2005); M.-Y. Ye, D. Sun, Y.-S. Zhang, and G.-C. Guo, Phys. Rev. A **70**, 022326 (2004).

[11] M. Möttönen and J. J. Vartiainen, *Trends in Quantum Computing Research* (Nova Science, Hauppauge, NY, 2006); V. Shende, S. Bullock, and I. Markov, IEEE Trans. Computer-Aided Design **25**, 1000 (2006).

[12] Y. Nakajima, Y. Kawano, and H. Sekigawa, Quantum Inf. Comput. **6**, 67 (2006).

[13] B. Drury and P. Love, J. Phys. A Math. Theor. **41**, 395305 (2008).

[14] M. Sedlak and M. Plesch, Cent. Euro. J. Phys. **6**, 128 (2008).

[15] M. Saeedi, M. Arabzadeh, M. S. Zamani, and M. Sedighi, e-print arXiv:1011.2159 [quant-ph].

[16] As a “computation step” only the performance of CNOT gates is considered. Several CNOT gates performed in parallel are considered as one step.

[17] M. Riebe, K. Kim, P. Schindler, T. Monz, P. O. Schmidt, T. K. Korber, W. Hansel, H. Haffner, C. F. Roos, and R. Blatt, Phys. Rev. Lett. **97**, 220407 (2006).

[18] R. Prevedel, G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, Phys. Rev. Lett. **103**, 020503 (2009).