

Construction of mutually unbiased bases with cyclic symmetry for qubit systems

Ulrich Seyfarth¹ and Kedar S. Ranade²¹*Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a, D-64289 Darmstadt, Germany*²*Institut für Quantenphysik, Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany*

(Received 17 June 2011; published 17 October 2011)

For the complete estimation of arbitrary unknown quantum states by measurements, the use of mutually unbiased bases has been well established in theory and experiment for the past 20 years. However, most constructions of these bases make heavy use of abstract algebra and the mathematical theory of finite rings and fields, and no simple and generally accessible construction is available. This is particularly true in the case of a system composed of several qubits, which is arguably the most important case in quantum information science and quantum computation. In this paper, we close this gap by providing a simple and straightforward method for the construction of mutually unbiased bases in the case of a qubit register. We show that our construction is also accessible to experiments, since only Hadamard and controlled-phase gates are needed, which are available in most practical realizations of a quantum computer. Moreover, our scheme possesses the optimal scaling possible, i.e., the number of gates scales only linearly in the number of qubits.

DOI: [10.1103/PhysRevA.84.042327](https://doi.org/10.1103/PhysRevA.84.042327)

PACS number(s): 03.67.Lx, 03.65.Aa, 03.67.Ac, 03.65.Ta

I. INTRODUCTION

In quantum physics, the estimation of the state of a system is of high practical value [1]. It is well known that for the complete estimation of a state, known as state tomography, a single measurement is not sufficient, even if performed many times to get the statistics of such measurement. It is necessary to measure a state in various different bases. The best choice of such bases for an arbitrary system is so-called mutually unbiased bases (MUBs), which offer the highest information outcome, as already stated by Wootters and Fields [2]: mutually unbiased bases provide an optimal means of determining an ensemble's state. Experimental results demonstrate the practicability of those schemes [3–5]. Different construction methods for MUBs are known [2,6–10]. For a d -level system, i.e., a system described by a $d \times d$ density matrix, one would need $d + 1$ mutually unbiased bases, since any measurement statistically reveals $d - 1$ parameters. Unfortunately, it is not even known whether $d + 1$ such bases exist in every d -level system. Mutually unbiased bases are related to different topics in mathematics and physics, e.g., quantum cryptography, foundations of physics [11], orthogonal Latin squares or hidden-variable models [12,13], and even Feynman's path integral [14].

In this paper, we want to focus on a system which is of particular interest in quantum information processing, namely, a quantum register built of qubits. We propose a complete set of mutually unbiased bases for quantum registers of size 1,2,4,8,...,256. In general, the construction of MUBs is quite involved and uses methods from abstract algebra and the mathematical theory of finite fields and rings [10], which are far apart from most methods that are commonly used in physics. We overcome this problem in such a way, that our construction (although not its proof) is very easy to follow and to apply by anyone with just basic knowledge of linear algebra. Moreover, our construction is applicable to experiments with only limited effort. In particular, the experimentator must only be able to perform, on a system of m qubits, a single unitary operation U_m , by which all the $d + 1$ MUBs are generated. (Obviously, he must be

able to perform measurements in at least one basis, say, the standard basis.) This single unitary operator is of the particular form $U_m = e^{i\psi_m} 2^{-m/2} H^{\otimes m} P_m$, where $2^{-m/2} H^{\otimes m}$ denotes the m -fold tensor product of Hadamard matrices, P_m is a diagonal phase matrix, and $e^{i\psi}$ is a global phase. The columns of $U, U^2, U^3, \dots, U^{2^m+1} = \mathbb{1}_{2^m}$ then define mutually unbiased bases. Any phase matrix P_m can be decomposed into CPHASE gates and together with the one-qubit Hadamard gate, belongs to the building blocks of one of the several universal sets of gates for a quantum computer. As any reasonable quantum computer will be able to perform such operations [15], no extra effort is needed to implement our measurement; an example circuit is given in Fig. 1.

II. CONSTRUCTION OF MUBS

We shall now present our construction in detail. For a single qubit we have the Hadamard transformation $2^{-1/2} H$ with $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, which switches between the mutually unbiased z and the x bases. (It is convenient to choose the matrix H to be non-normalized, so that it and its tensor products contain only ± 1 .) Multiplying this by a phase $P_1 = \text{diag}(1, -i)$, we find that $T := 2^{-1/2} H P_1$ cyclically switches between the mutually unbiased z, x , and y bases (up to a global phase). This matrix is well known, e.g., in quantum key distribution where it is used in the six-state protocol (cf., e.g., [16,17]). We want to generalize this construction to higher numbers of qubits. If we take a number m of qubits, it is obvious that the m -fold tensor product $H^{\otimes m}$ switches between two mutually unbiased bases, composed of local z and x bases. We can switch between $2^m + 1$ mutually unbiased bases, if we apply a diagonal phase gate (such as P_1 above). Determining these local phases, which turn out to be either ± 1 or $\pm i$, is nontrivial, not even numerically, but can be achieved by our method. Given the unitary T as above, we can construct a two-qubit phase matrix by reading it out row-wise, i.e., $P_2 = \text{diag}(1, -i, 1, i)$. It turns out that $U_2 = i 2^{-1} H^{\otimes 2} P_2$ produces a cycle of five MUBs. We can iterate this procedure to get MUBs for 4, 8, etc.. qubits. Although these choices of P_4, P_8 , etc., appear to be accidental for now, this

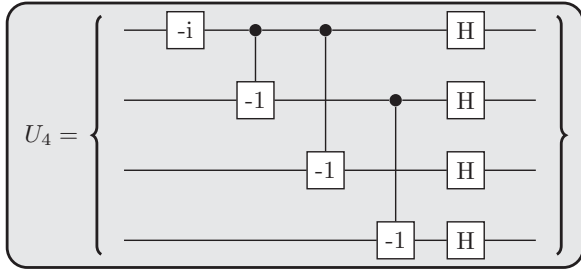


FIG. 1. Quantum circuit for the generator U_4 for a four-qubit register.

structure has deep mathematical roots, which we will elaborate on later in this paper. In particular, this construction is related to Wiedemann's conjecture [18] from finite-field theory, and is, as such, only valid for up to 256 qubits. However, it may hold for even higher numbers such as 512, 1024, etc. If this is true for all powers of 2, this would prove Wiedemann's conjecture.

A. Circuit implementation

To implement these unitaries in experiments we will now give decomposition of the phase system P_m into elementary gates. To do so, we will have to touch the mathematical roots of this matrix structure. But let us start with two elementary gates, the one-qubit PHASE gate and the two-qubit controlled-PHASE (CPHASE) gate:

$$\text{PHASE}_q(e^{i\varphi}) = |0\rangle_q \langle 0| + e^{i\varphi} |1\rangle_q \langle 1|, \quad (1)$$

$$\begin{aligned} \text{CPHASE}_{s \rightarrow t}(e^{i\varphi}) &= |0\rangle_s \langle 0| \otimes |0\rangle_t \langle 0| + |0\rangle_s \langle 0| \otimes |1\rangle_t \langle 1| \\ &+ |1\rangle_s \langle 1| \otimes |0\rangle_t \langle 0| + e^{i\varphi} |1\rangle_s \langle 1| \otimes |1\rangle_t \langle 1|. \end{aligned} \quad (2)$$

The prototype of a phase gate is Pauli's σ_z with $e^{i\varphi} = -1$, but in our case we usually have $e^{i\varphi} = \pm i$. Note that in the case of a CPHASE gate, source and target qubits are interchangeable, and moreover, all these gates commute since they are diagonal.

The recursive procedure we use to construct P_{2m} from P_m results from a similar procedure for an $m \times m$ matrix $B_m = (b_{kl})_{k,l=1}^m$ with entries 0 and 1 and arithmetics modulo 2 (more formally, over the finite field \mathbb{F}_2), which describes the phase system. This matrix has to fulfill several properties [19,20] related to a stabilizer structure (that is why we call it the reduced stabilizer matrix), e.g., it must be symmetric. However, in our case it is more advisable to view it as the adjacency matrix of an undirected graph with m qubits (as vertices) and edges between qubits i and j , if $b_{ij} = 1$. We allow loops, i.e., $b_{ii} = 1$ is possible, but they need to be treated separately.

We shall label the basis vectors of an m -qubit system by bit strings of length m , namely, by $\vec{j} = (j_1, \dots, j_m)^T$, where $j_i \in \{0, 1\}$ for all $i \in \{1, \dots, m\}$. The relation between B_m and the phase system $P_m = \text{diag}[(p_{\vec{j}})_{\vec{j} \in \mathbb{F}_2^m}]$ was derived before [19,20] and can be written as

$$p_{\vec{j}} = i^{\sum_{k,l=1}^m b_{kl} j_k j_l} (-1)^{\sum_{k=1}^m b_{kk} j_k}. \quad (3)$$

Note that the sums are *not* performed modulo 2. We may rewrite the first factor as $\prod_{k,l=1}^m (i^{j_k j_l})^{b_{kl}}$ or

$\prod_{k < l} [(-1)^{j_k j_l}]^{b_{kl}} \prod_k (i^{j_k})^{b_{kk}}$, as B_m is symmetric. The second factor of this expression may be joined with the second factor of $p_{\vec{j}}$ to find

$$p_{\vec{j}} = \prod_{k,l=1, k < l}^m [(-1)^{j_k j_l}]^{b_{kl}} \prod_{k=1}^m [(-i)^{j_k}]^{b_{kk}}. \quad (4)$$

This can be interpreted as follows:

- (a) If $b_{kk} = 1$, perform PHASE $_k(-i)$.
- (b) If $b_{kl} = 1$ for $k < l$, perform CPHASE $_{k \rightarrow l}(-1)$.

The experimental resources (together with the Hadamard gate) are therefore precisely the same as for the preparation of graph states. More precisely, the number of gates is directly related to the number of nonzero entries in B .

We go on to discuss the doubling scheme from m to $2m$ qubits explicitly. We start with a single qubit and $B_1 = (1)$. To go from m qubits to $2m$ qubits, we use the block-matrix mapping

$$B_m \mapsto B_{2m} = \begin{pmatrix} B_m & \mathbb{1}_m \\ \mathbb{1}_m & 0_m \end{pmatrix}. \quad (5)$$

For example, for one to four qubits, the mapping reads

$$(1) \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \text{ etc.} \quad (6)$$

To check that these matrices B_m fulfill the criteria for generating mutually unbiased bases [19] is, in general, nontrivial, but is in our case for $m \in \{1, 2, 4, 8, \dots, 256\}$ guaranteed by previous results [20] in connection with the work of Wiedemann [18].

Note that the number of nonzero entries scales linearly in m . The only diagonal nonzero element is b_{11} for any number m , so there is just a single PHASE gate, and Eq. (4) implies that the value of $p_{\vec{j}}$ with $\vec{j} = (j_1, \dots, j_m)^T$ is real if $j_1 = 0$, and purely imaginary otherwise. The number of CPHASE gates, which is the number of upper diagonal elements, increases by m , if we go from m to $2m$ qubits. Altogether we have a single PHASE gate and $m - 1$ CPHASE gates for a system composed of m qubits, i.e., linear scaling with the number of qubits.

B. Unitary construction

By now, we have constructed a matrix which cyclically switches between $2^m + 1$ mutually unbiased bases in two ways: first, by using the explicit doubling scheme for a unitary phase matrix P_m , and second, by invoking a matrix B_m for a decomposition into elementary gates. Although not directly relevant to experiments, the matrix $V_m = H^{\otimes m} P_m$ still lacks normalization and a global phase $e^{i\psi_m}$ to give the generating matrix U_m , such that $U_m^{2^m+1} = \mathbb{1}$. It is necessary that the 2^m eigenvalues of U_m are $(2^m + 1)$ th roots of unity. Using a conjecture, which was numerically checked, that U_m and therefore V_m are nondegenerate [19], we may choose $\lambda = 1$ not to be an eigenvalue of U_m . As the characteristic polynomial of U_m is then given by $\chi(\lambda) = \det(\lambda \mathbb{1}_{2^m} - U_m) = (\lambda^{2^m+1} - 1)/(\lambda - 1) = \sum_{k=0}^{2^m} \lambda^k$, we see that we have to divide our matrix V_m by $-\text{tr } V_m$ to get U_m . This trace is given by $1 + i$

for $m = 1$ and $i2^{m/2}$ for $m \in \{2, 4, 8, \dots, 256\}$, which we derive later in this paper.

For a single-qubit register we take the solution that we find with the help of matrix $B_1 = (1)$, i.e., $V_1 = H \text{diag}(1, -i)$, where $\text{diag}(\cdot)$ maps values from a d -dimensional row vector to the diagonal of a $d \times d$ matrix. By dividing V_1 by $-\text{tr } V_1 = -(1 + i)$, we receive the matrix U_1 that switches between three mutually unbiased bases of a single qubit. To get an operator that switches between five mutually unbiased bases for a two-qubit register, we introduce a *chop map* \mathcal{M} that behaves in the following way: For V being an arbitrary $d \times d$ matrix, $v = \mathcal{M}(V)$ is a d^2 -dimensional row vector, where the first row of V is mapped to v_1, \dots, v_d , the second row of V is mapped to v_{d+1}, \dots, v_{2d} , etc. If we use this vector as a phase vector such as $V_2 = H^{\otimes 2} \text{diag}[\mathcal{M}(V_1)]$ and apply normalization and the associated global phase, i.e., $U_2 = V_2 / (-\text{tr } V_2)$, we obtain the desired operator for a two-qubit register. As stated before, this construction works until a register length of 256, and it holds for an arbitrary number of register length doublings, if and only if Wiedemann's conjecture is correct.

In the following we will show how to transfer the doubling scheme of B_m as in Eq. (5) to the doubling scheme of V_m and U_m . We need a particular ordering of the entries of the basis vectors in U_m . We label each vector with an m -bit string $\vec{j} = (j_1, \dots, j_m)^T$ of zeros and ones and sort them in binary increasing order. For the non-normalized Hadamard matrix this results in Sylvester's construction $H_m \in M_{2^m}(\mathbb{C})$ for $m \in \mathbb{N}_0$. For $m = 0$, we have $H_0 := (1)$ and recursively define

$$H_{m+1} := \begin{pmatrix} H_m & H_m \\ H_m & -H_m \end{pmatrix} \in M_{2^{m+1}}(\mathbb{C}); \quad (7)$$

we see that $H = H_1$ is the well-known regular Hadamard matrix in the qubit case. It is obvious that the entries in every H_m are either $+1$ or -1 and further, H_m can be seen as the explicit construction of the m -fold tensor product $H^{\otimes m}$.

We can now relate the chop-map doubling scheme for P_m to the doubling scheme for B_m of Eq. (5). We want to construct the explicit phases p'_j of P_{2m} to the phases p_j of P_m . As the length of \vec{j}' is twice the length of \vec{j} , we may write $\vec{j}' = (\vec{j}_1, \vec{j}_2)^T$. In our case of B_m , the exponent of the second factor of p_j as in Eq. (3) depends only on b_{11} and remains unchanged by the doubling. The exponent of the first factor can be separated into two parts, one arising from the old B_m and another arising from the doubling. By invoking Eq. (3), this directly results in the exponent being $\vec{j}_1 \cdot B_m \vec{j}_1 + 2\vec{j}_1 \cdot \vec{j}_2$. The first part is exactly the phase system of the old matrix P_m , while working out the second part results in a factor $(-1)^{\vec{j}_1 \cdot \vec{j}_2}$, which represents the old non-normalized Hadamard matrix, where \vec{j}_1 and \vec{j}_2 indicate rows and columns, respectively. We conclude that the calculation of the phases of V_{2m} can be done by applying the local phases of V_m to a Hadamard matrix of the right size and then concatenating the resulting rows one after the other.

Before concluding this paper, we shall provide the reader with an explicit form of the matrix U_m , which generates the complete set of mutually unbiased bases; to this end, we derive the form of V_m and then calculate its trace, so that $U_m = -V_m / \text{tr } V_m$. As seen above, we may write the matrices V_m recursively as $V_{2m} = H^{\otimes 2m} \text{diag}[\mathcal{M}(V_m)]$ with $V_1 = \begin{pmatrix} 1 & -i \\ 0 & -i \end{pmatrix} =$

$H \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$. Since the entries of H are given by $(-1)^{\vec{i} \cdot \vec{j}}$, we can write V_1 as

$$(V_1)_{i,j} = \begin{cases} 1 \times (-1)^{\vec{i} \cdot \vec{j}}, & \text{if } j \equiv 0 \pmod{2}, \\ -i \times (-1)^{\vec{i} \cdot \vec{j}}, & \text{if } j \equiv 1 \pmod{2}, \end{cases} \quad (8)$$

with \vec{i} representing the rows and \vec{j} the columns of V_1 and the indices starting with zero. In the V_1 case, \vec{i} and \vec{j} are one bit long, respectively. In the V_2 case they are two bits long, for the V_4 case four bits, and so forth, so we write the vector as a bit string with the lowest bit on the left like $\vec{i} = (i_1, \dots, i_m)^T$. To calculate V_2 , we have to chop map V_1 to a diagonal matrix and multiply this to $H^{\otimes 2}$. By iteration, this results in the expression

$$(V_m)_{i,j} = \begin{cases} 1 \times (-1)^x, & \text{if } j \equiv 0 \pmod{2}, \\ -i \times (-1)^x, & \text{if } j \equiv 1 \pmod{2}, \end{cases} \quad (9)$$

with $x = (i_1, \dots, i_m) \cdot (j_1, \dots, j_m)^T + (j_1, \dots, j_{m/2}) \cdot (j_{m/2+1}, \dots, j_m)^T + \dots + (j_1) \cdot (j_2)$. We shall now derive the trace of V_m . To simplify matters we consider the real and imaginary part of V_m separately. Since the trace is the sum over the diagonal entries, we set $\vec{i} = \vec{j}$ in Eq. (9).

For the real part, $j_1 = 0$ holds due to Eq. (9). To calculate the sum of the real part, we add the terms \vec{j} for which $j_{(m/2)+1} = 0$ pairwise to those terms \vec{j}' , where $j'_{(m/2)+1} = 1$. The Hamming weight of \vec{j} and \vec{j}' differs by one, so $(-1)^{\vec{j} \cdot \vec{j}} + (-1)^{\vec{j}' \cdot \vec{j}'} = 0$. All subsequent terms of \vec{j} and \vec{j}' are equal, since \vec{j} and \vec{j}' differ only in the right half of their bits. The first terms are equal due to the fact that the lowest bits of \vec{j} and \vec{j}' are zero. Thus the real part of $\text{tr } V_m$ vanishes. For $m = 1$ the real part equals 1, since there is only a single term with $j_1 = 0$.

The imaginary part of $\text{tr } V_m$ is given by the sum over every second element of the diagonal, i.e., $j_1 = 1$. We will split this calculation into two steps. In the first step, we take those terms where the left half of \vec{j} is filled by 1's. One of those terms is given by

$$-(-1)^{\vec{j} \cdot \vec{j} + (1, \dots, 1) \cdot (j_{(m/2)+1}, \dots, j_m)^T + (1, \dots, 1) \cdot (1, \dots, 1)^T + \dots + (1) \cdot (1)}. \quad (10)$$

The first summand in the exponent calculates the Hamming weight of \vec{j} , whereas the second summand calculates the Hamming weight of the right half of \vec{j} . Since m is a power of 2, for those cases with $m > 1$, the first two summands give the same result modulo 2. All subsequent summands without the last one result in powers of 2, the last term, $(1) \cdot (1)$, gives one. For $m = 1$ we have only this last summand, so in all cases of m the summands add up to an odd integer, thus these terms give one. There are $2^{m/2}$ ways for \vec{j} to have only 1's in the left half, so they contribute with $2^{m/2}$ to the imaginary part of the trace.

There remain those elements of \vec{j} for which the left half has at least one zero bit, but the lowest bit has to be one for the imaginary elements. We can pair them like in the real part, and the same argument brings their sum to zero. Thus the trace of V_m is given by $i2^{m/2}$, and we find

$$U_m = i2^{-m/2} H^{\otimes m} \text{diag}\{\mathcal{M}[H^{\otimes m/2} \dots H \text{diag}(1, -i)]\}$$

for $m \in \{2, 4, 8, \dots, 256\}$; in the case $m = 1$ we have $U_1 = -H \text{diag}(1, -i) / (1 + i)$.

III. CONCLUSIONS

To summarize, we have shown in this paper how to construct a maximal set of mutually unbiased bases for a quantum system composed of qubits by a single unitary generator, and we have shown how this operation can be decomposed into Hadamard, phase, and controlled-phase gates. The necessary resources to implement our scheme may be compared to those for preparing graph states, and the number of gates scales only linearly in the number of qubits. This scaling is optimal, since the graph must be connected. We believe that our approach may be of interest in the one-way quantum computer by Raussendorf and Briegel [21–24], where one uses a nearest-neighbor Ising-type interaction to generate a cluster state and one-qubit measurements. In our case, we only need measurements in the standard bases, but due to our construction, we may need CPHASE gates with possibly long distances between source and target qubits. It would be useful to overcome this limitation by a new construction which uses band matrices of limited size, or to use qubit implementations which make such long-distance CPHASE gates possible in an experiment.

A slight disadvantage of our system is that we restrict ourselves to numbers of qubits which are powers of 2. Further work may continue in finding generators of mutually unbiased bases for qubit registers of different length. For example, if $m = 3$, we can choose any of the matrices B_m with $m = 2^k$. A doubling scheme similar to Eq. (5), more precisely,

$$B_m \mapsto B_{3m} = \begin{pmatrix} B_m & B_m & B_m \\ B_m & B_m & 0_m \\ B_m & 0_m & 0_m \end{pmatrix}, \quad (11)$$

produces mutually unbiased bases, at least for $m \in \{6, 12, 24\}$. But investigations to be performed in more detail require a more thorough understanding of the mathematical principles underlying this construction, but this is beyond the scope of this paper.

ACKNOWLEDGMENTS

The authors acknowledge financial support by CASED and BMBF/QuOREP.

-
- [1] *Quantum State Estimation*, edited by M. Paris and J. Řeháček (Springer-Verlag, Berlin, 2004).
- [2] W. K. Wootters and B. D. Fields, *Ann. Phys.* **191**, 363 (1989).
- [3] R. B. A. Adamson and A. M. Steinberg, *Phys. Rev. Lett.* **105**, 030406 (2010).
- [4] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino, *Phys. Rev. A* **81**, 052317 (2010).
- [5] G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra, *Opt. Express* **19**, 3542 (2011).
- [6] J. Schwinger, *Proc. Natl. Acad. Sci. USA.* **46**, 570 (1960).
- [7] W. O. Alltop, *IEEE Trans. Inf. Theory* **26**, 350 (1980).
- [8] I. D. Ivanović, *J. Phys. A* **14**, 3241 (1981).
- [9] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, *Algorithmica* **34**, 512 (2002).
- [10] A. Klappenecker and M. Rötteler, *Lect. Notes Comput. Sci.* **2948**, 137 (2004).
- [11] H. Maassen and J. B. M. Uffink, *Phys. Rev. Lett.* **60**, 1103 (1988).
- [12] T. Paterek, M. Pawłowski, M. Grassl, and Č. Brukner, *Phys. Scr., T* **140**, 014031 (2010).
- [13] T. Paterek, B. Dakić, and Č. Brukner, *Phys. Rev. A* **79**, 012109 (2009).
- [14] J. Tolar and G. Chadzitaskos, *J. Phys. A* **42**, 245306 (2009).
- [15] D. P. DiVincenzo, *Fortschritte der Physik* **48**, 771 (2000).
- [16] D. Gottesman, *Phys. Rev. A* **57**, 127 (1998).
- [17] D. Gottesman and H.-K. Lo, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
- [18] D. Wiedemann, *Fib. Quart.* **26**, 290 (1988).
- [19] O. Kern, K. S. Ranade, and U. Seyfarth, *J. Phys. A* **43**, 275305 (2010).
- [20] U. Seyfarth and K. S. Ranade, e-print arXiv:1104.0202v1.
- [21] H. J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86**, 910 (2001).
- [22] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [23] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [24] P. Walther *et al.*, *Nature (London)* **434**, 169 (2005).