

Constructive quantum Shannon decomposition from Cartan involutions

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2008 J. Phys. A: Math. Theor. 41 395305

(<http://iopscience.iop.org/1751-8121/41/39/395305>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 171.66.16.150

The article was downloaded on 03/06/2010 at 07:13

Please note that [terms and conditions apply](#).

Constructive quantum Shannon decomposition from Cartan involutions

Byron Drury and Peter Love

Department of Physics, 370 Lancaster Ave., Haverford College, Haverford, PA 19041, USA

E-mail: plove@haverford.edu

Received 21 June 2008, in final form 31 July 2008

Published 4 September 2008

Online at stacks.iop.org/JPhysA/41/395305

Abstract

The work presented here extends upon the best known universal quantum circuit, the quantum Shannon decomposition proposed by Shende *et al* (2006 *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **25** 1000). We obtain the basis of the circuit's design in a pair of Cartan decompositions. This insight gives a simple constructive factoring algorithm in terms of the Cartan involutions corresponding to these decompositions.

PACS numbers: 03.67.Lx, 03.67.—a, 03.67.Mn

1. Introduction

Quantum computation has attracted interest in recent years because it appears to violate the strong form of the Church–Turing thesis; quantum computers seem to be fundamentally more powerful than any possible classical computer [1]. In 1994 Peter Shor published efficient quantum algorithms for the prime factorization of integers and the calculation of discrete logarithms modulo arbitrary primes [2]. Lov Grover's 1995 introduction of the quantum search algorithm provided a polynomial speedup for unstructured searches [3]. As early as 1982 Richard Feynman pointed out the inherent difficulties in simulating quantum systems with classical processors and suggested the possibility that the use of quantum information processing could produce exponential speedups in such simulations [4]. Subsequently efficient quantum algorithms for performing simulations of physical systems were developed [5–11], vindicating Feynman's prediction and further motivating theoretical and experimental work towards realizing quantum computation.

In this paper we focus on the quantum circuit model of quantum computation [12]. In this setting a quantum computation is a unitary transformation applied to n ideal qubits (we ignore decoherence throughout). Given the irrelevance of global phases the set of all such transformations is the special unitary group $SU(2^n)$. To represent an element of $SU(2^n)$ by a circuit we must specify a fixed set of elementary gates which act on a fixed number of qubits. A typical choice is the controlled-NOT (CNOT) and arbitrary one-qubit gates. The length of a circuit is the number of elementary gates which it contains, however, because of

the relative difficulty of multi-qubit operations we shall only consider the number of CNOT gates in a circuit. There are several means of physically implementing a quantum computation [13–18]. One qubit local operations and a few two qubit operations, such as the controlled-NOT (CNOT) gate have been experimentally implemented [19–24].

The set of all allowed transformations for a quantum computer form the group $SU(2^n)$ and a generic element of $SU(2^n)$ requires a circuit of length $\Omega(4^n)$ gates. Specific transformations corresponding to efficient quantum algorithms are of particular interest. A quantum algorithm specifies a circuit family, with a circuit defined for each value of n . For a quantum algorithm to be efficient each of these circuits must be composed of a number of operations bounded above by a polynomial in n . Each of these operations must involve a subset of the n qubits with size bounded above by a polynomial in the logarithm of n . Some algorithms, for example the quantum Fourier transform, naturally decompose into elementary gates acting on qubits [25]. In other cases, for example generic quantum Fourier transforms of functions on groups other than $Z/(2^n Z)$ [26, 27], and in application of phase estimation to problems of quantum simulation [8, 10], bounded size operations arise which do not naturally factor into elementary gates. Before such quantum algorithms may be implemented experimentally one is therefore faced with a problem of quantum compilation—given a set of unitary operators of fixed size and an elementary gate set, constructively produce the quantum circuit realizing the operators.

It was shown by construction in 1995 that the set of one qubit operations and the CNOT are universal: any unitary operation on any number of qubits can be realized as a circuit over these gates. However, the number of CNOT gates required for n qubits was of order $n^3 4^n$ [28]. Since 1995 a number of advances have been made towards the CNOT optimization of universal quantum circuits. We divide these into three categories: circuit optimization, Lie algebra decompositions, and explicit algorithms.

Knill proved that the asymptotic CNOT cost of universal quantum circuits could be reduced by a factor of n^2 to $\Omega(n 4^n)$ [29]. In 2004 Shende, Markov and Bullock proved the highest known lower bound on asymptotic CNOT cost, $\lceil \frac{1}{4}(4^n - 3n - 1) \rceil$ [30], and Vartiainen *et al* simplified the best existing circuit using Gray codes to achieve for the first time a leading order CNOT cost of $\Omega(4^n)$ (in fact, for large n , the cost was approximately 8.7×4^n), a multiplicative factor away from the highest known lower bound [31]. Later that year, the same authors, along with Bergholm, presented a decomposition based on the cosine-sine matrix decomposition (CSD) which produced asymptotic behavior scaling as $4^n - 2^{n+1}$ [32]. For more details on the CSD see [33, 34]. Vatan and Williams published a three CNOT universal two qubit gate along with a proof that fewer CNOTs could never achieve universality [35], and proposed a 40 CNOT universal three qubit gate which was, at the time, the best known [36]. The current best known circuit decomposition applicable to systems of more than two qubits was introduced by Shende, Bullock and Markov. Using intuition drawn from the Shannon decomposition of classical logic circuit design, along with the application of some circuit identities, Shende, Bullock and Markov have designed a universal circuit requiring 20 CNOTs in the three qubit case and $\frac{23}{48} 4^n - \frac{3}{2} 2^n + \frac{4}{3}$ CNOTs asymptotically [37]. This decomposition is known as the quantum Shannon decomposition (QSD), by analogy with the Shannon decomposition of classical circuit design, and brings the upper bound on asymptotic CNOT cost to within a factor of 2 of the highest known lower bound while halving the cost of implementing a general three qubit gate to 20 CNOTs.

The second area of research is the exploration of the various ways of decomposing the Lie algebra of the special unitary group. Essentially all of the work in this area has made use of the Cartan decomposition. In the first part of the 20th century Cartan proved that (up to conjugacy) there exist only three types of Cartan decomposition of the unitary lie algebra, **AI-III** [38, 39]. The CNOT optimal two qubit circuit of Vatan and Williams

[35] is, as described in detail below, based on a type **AI** Cartan decomposition. Khaneja and Glaser proposed a scheme based on a Cartan decomposition of $\mathfrak{su}(2^n)$ (now known as the Khaneja Glaser decomposition, or KGD) which lends itself to efficient recursive circuit decompositions [40], and, working with Brockett, they showed that this scheme was time optimal for NMR-based implementations of quantum computation [41]. Bullock identified the Khaneja Glaser decomposition, as well as the CSD, as type **AIII** Cartan decompositions and thereby established an equivalence between the two [42]. The KGD was used by Vatan and Williams to produce their efficient two and three qubit circuits [36, 35]. Bullock and Brennen and more recently Dagli, D’Alessandro and Smith have used type **AI** and **AII** decompositions, including the concurrence canonical decomposition (CCD) and the odd-even decomposition (OED), to study entanglement dynamics in quantum circuits [43, 44].

In order to make practical use of a CNOT-optimized quantum circuit or a novel Lie algebra decomposition it is necessary to have an algorithm which can extract the parameters which appear in the decomposition from an arbitrary unitary operation. Sousa and Ramos provided an algorithm based on the generalized singular value decomposition for computing the parameters in a CNOT-optimized two qubit circuit (the parameters for Vatan and Williams circuit can be extracted from their algorithm with a little algebra, and other equivalent circuits can be computed with a similar amount of effort) [45]. Just as Vatan and Williams’ work on small numbers of qubits does not generalize to larger operators, however, Sousa and Ramos’ algorithm does not generalize beyond two qubits. Earp and Pachos provided a constructive algorithm to perform a type **AIII** Cartan decomposition of an arbitrary n qubit operator (they use the Khaneja Glaser decomposition specifically, but their algorithm can be modified to implement other forms of the **AIII** decomposition) [46]. Earp and Pachos’ algorithm relies on numerical optimization and a truncation of the Baker–Campbell–Hausdorff formula. Nakajima *et al* published the first algorithm to compute Cartan decompositions of the unitary group making explicit use of Cartan involutions [47]; their algorithm computes parameters for circuits composed of uniformly controlled operations, similar to the circuits produced by CSD based schemes. Their algorithm requires $4^n - 2^{n-1}$ CNOT gates asymptotically. In the three-qubit case this number can be reduced by taking advantage of the known CNOT-optimized two qubit circuit developed by Vatan and Williams to produce a 44 CNOT universal three qubit circuit (see figure 2). Since a lower bound of $\frac{1}{4}(4^n - 3n - 1)$ has been proven on the asymptotic CNOT cost of arbitrary n -qubit operations with a lower bound of 14 CNOTs in the three qubit case [30], this efficiency cannot be improved by more than a factor of 4. Circuits produced by Nakajima *et al*’s algorithm are a factor of 2 longer than circuits obtained from the quantum Shannon decomposition (QSD). However, the QSD lacks a constructive Lie algebra based factoring algorithm in the published literature so far. It is to this issue we turn in the remainder of the paper.

We first give some mathematical background introducing important definitions and theorems which will be used later in the work. We then discuss the important special cases of one and two qubit operations, and provide Cartan involution based algorithms for extracting parameters for CNOT optimal quantum circuits from arbitrary one and two qubit unitary operations. We then place the QSD, the best known circuit decomposition in terms of CNOT cost, into a Lie algebraic context by showing it to be an alternating series of Cartan decompositions. We define the Cartan involutions which correspond to these decompositions, and we show that these involutions can be used recursively to obtain the QSD for unitary operators on any number of qubits.

2. Mathematical background

In the interest of making our presentation more self-contained, we briefly review some basic definitions which will be important throughout this work. For a fuller presentation we refer the reader to [48, 49]. Throughout, we use $[ab]$ to denote the Lie bracket in general, and the notation $[a, b]$ to denote the Lie bracket for matrix algebras where it is the commutator $[a, b] = ab - ba$.

Definition 1. *If a subalgebra I of a Lie algebra \mathfrak{g} satisfies the condition that $[xy] \in I$ for all $x \in \mathfrak{g}, y \in I$ then I is called an ideal in \mathfrak{g} .*

Example 1. Clearly 0 and \mathfrak{g} are trivial ideals of \mathfrak{g} . An important example of an ideal is the *derived algebra* of \mathfrak{g} , denoted $[\mathfrak{g}\mathfrak{g}]$, which consists of all linear combinations of brackets $[xy]$, with $x, y \in \mathfrak{g}$.

Definition 2. *A non-abelian Lie algebra \mathfrak{L} (i.e. $[\mathfrak{L}\mathfrak{L}] \neq 0$) in which the only ideals are 0 and all of \mathfrak{L} is called simple. Observe that since the derived algebra is an ideal, for any simple Lie algebra S the derived algebra is equal to the entire algebra: $[SS] = S$.*

We may define a sequence of ideals, the *derived series* of an algebra A , as follows:

$$A^{(0)} = A, \quad A^{(1)} = [AA], \quad A^{(2)} = [A^{(1)}A^{(1)}], \dots, A^{(i)} = [A^{(i-1)}A^{(i-1)}], \dots$$

If $A^{(n)} = 0$ for some n we call A *solvable*. Observe that all abelian Lie algebras are solvable, while all simple Lie algebras are nonsolvable. We shall simply state the fact that every Lie algebra contains a unique maximal solvable ideal (maximal in the sense that it is contained in no larger solvable ideal), which is referred to as the *radical* of the algebra. If L is a non-zero Lie algebra and $\text{Rad } L = 0$, we call L *semi-simple*. This condition for the semi-simplicity of a Lie algebra is equivalent to the condition that the algebra is the direct sum of simple Lie algebras. Most of the Lie algebras which occur in physics are semi-simple, and there exists a very rich and well-developed structure theory of semi-simple Lie algebras which we shall exploit throughout the remainder of this work. The essential structure theorem which lies behind both the CSD, the KGD, and as we shall show later the QSD, is the Cartan decomposition.

Definition 3. *A Cartan decomposition of a real semi-simple Lie algebra \mathfrak{g} is a decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ where $\mathfrak{m} = \mathfrak{k}^\perp$, for which \mathfrak{k} and \mathfrak{m} satisfy the commutation relations:*

$$[\mathfrak{k}, \mathfrak{k}] \subset \mathfrak{k} \tag{1}$$

$$[\mathfrak{m}, \mathfrak{k}] = \mathfrak{m} \tag{2}$$

$$[\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{k}. \tag{3}$$

A few further features of the Cartan decomposition are essential.

Definition 4. *Consider a semi-simple Lie algebra with Cartan decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ and a subalgebra \mathfrak{h} of \mathfrak{g} contained in \mathfrak{m} . Because $[\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{k}$, \mathfrak{h} must be Abelian. We refer to a maximal Abelian subalgebra contained in \mathfrak{m} as a Cartan subalgebra of \mathfrak{g} and \mathfrak{k} .*

Definition 5. *The Lie group G acts on its Lie algebra \mathfrak{g} through a conjugation, known as the adjoint action, $Ad_G : \mathfrak{g} \rightarrow \mathfrak{g}$ defined by*

$$Ad_U X = U^\dagger X U \tag{4}$$

for $U \in G$ and $X \in \mathfrak{g}$, and for $K = \exp(\mathfrak{k})$ we define the Adjoint orbit of X to be

$$Ad_K X = \bigcup_{k \in K} Ad_k X. \tag{5}$$

Any two Cartan subalgebras \mathfrak{h} and \mathfrak{h}' are related to one another through the adjoint action of the group G on its Lie algebra \mathfrak{g} . With these definitions, we now state

Theorem 1. For any two maximal Abelian subalgebras \mathfrak{h} and \mathfrak{h}' in \mathfrak{m} there is an element $k \in K$ such that $Ad_k(\mathfrak{h}) = \mathfrak{h}'$. Furthermore, the adjoint orbit of \mathfrak{h} is equal to \mathfrak{m} , i.e.

$$\mathfrak{m} = \bigcup_{k \in K} Ad_k \mathfrak{h}. \tag{6}$$

Finally, we come to the key definition in this paper:

Definition 6. Given a semisimple Lie algebra \mathfrak{g} with Cartan decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ and a Cartan subalgebra \mathfrak{h} , let $A = \exp(\mathfrak{h})$ and $K = \exp(\mathfrak{k})$, then $G = KAK$ is called a (global) Cartan decomposition of the semi-simple Lie group G .

The theorem which establishes the existence of such a decomposition for any semi-simple Lie group is proved in [48–50]. The $G = KAK$ structure has been used widely in work on quantum circuit decompositions in the past, most notably in Khaneja and Glaser’s work, as well as in CSD based circuit designs (as explained by Bullock [42]) and in subsequent work based on these decompositions (cf e.g. [32, 36, 40, 44]). The task of computing the Cartan factors for a specific unitary matrix is greatly facilitated by the existence of Cartan involutions.

Definition 7. A Cartan involution, denoted θ , is a non-identity automorphism on a Lie algebra \mathfrak{u} such that θ^2 is the identity, and the global Cartan involution has the equivalent action on $U = \exp(\mathfrak{u})$ with the property that

$$\theta(g) = \begin{cases} g & g \in \mathfrak{k} \\ -g & g \in \mathfrak{m}, \end{cases} \quad \Theta(G) = \begin{cases} G & G \in \exp(\mathfrak{k}) \\ G^\dagger & G \in \exp(\mathfrak{m}). \end{cases} \tag{7}$$

In the case of $\mathfrak{su}(n)$ there are only three classes of Cartan decomposition, denoted **AI**, **AII** and **AIII**. The \mathfrak{k} subalgebras of $\mathfrak{su}(n)$ are isomorphic to $\mathfrak{so}(n)$, $\mathfrak{sp}(\frac{n}{2})$ and $\mathfrak{s}[\mathfrak{u}(p) \oplus \mathfrak{u}(q)]$ for any $p + q = n$ for **AI**, **AII** and **AIII** decompositions, respectively (**AII** only exists for unitary groups acting on an even number of dimensions, a common situation in quantum information where the state-spaces of n -qubit registers have dimension 2^n) [44]. In this work we are particularly concerned with decompositions of type **AI** and **AIII** because in certain important cases there are straightforward and efficient means of physically implementing real orthogonal or direct sum unitary operators. Since we are concerned in this work only with the unitary group, whose elements satisfy the condition $U^{-1} = U^\dagger$, we may exploit the Cartan involution to factor matrices.

Theorem 2. For any $G \in SU(2^n)$ with Cartan decomposition $G = KM$, $K \in \exp(\mathfrak{k})$, $M \in \exp(\mathfrak{m})$, M^2 is uniquely determined by $M^2 = \Theta(G^\dagger)G$.

Proof. $\Theta(G^\dagger)G = \Theta(M^\dagger K^\dagger)KM = \Theta(M^\dagger)\Theta(K^\dagger)KM = MK^\dagger KM = M^2$. □

A KAK type decomposition of the special unitary group is desirable because there is a considerable amount of freedom in selecting the \mathfrak{k} subalgebra and a Cartan subalgebra \mathfrak{h} , and with appropriate selection of \mathfrak{k} and \mathfrak{h} the factors returned for an arbitrary unitary operator are

of a form which may readily be translated into physically realizable quantum gate sequences. Indeed, the Khaneja–Glaser decomposition has been shown to be time optimal for NMR quantum computing, as compared to other published decompositions [41]. The existence of this decomposition is of no practical use, however, without an algorithm for explicitly calculating the factors K_1 , K_2 and A for a given specific unitary matrix.

Notation. When discussing the generators of the Lie algebras of multi-qubit operator groups we will use a streamlined notation. We define $ZI = \sigma_z \otimes \mathbf{1}$, $IX = \mathbf{1} \otimes \sigma_x$, $ZY = \sigma_z \otimes \sigma_y$ and so on, where σ_x , σ_y and σ_z are the familiar Pauli spin matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Additionally, we define $X^{(n)}$ to be a Pauli- x (likewise y and z) acting on the n th qubit, i.e. $Z^{(3)} = ZII$.

3. Special cases: one and two qubits

3.1. One qubit factoring: Euler angle decomposition of $SU(2)$ as a Cartan decomposition

We now provide a simple, illustrative example of a Cartan decomposition and an involution based algorithm for converting an arbitrary one qubit unitary operator into a Cartan inspired circuit. This is the simplest possible case of a Cartan decomposition of a unitary group, however, the factoring of multi-qubit gates inevitably reduces in the end to a series of one-qubit gates which must themselves be decomposed. The structure of the algorithm for this simple example is identical to the more involved cases to follow.

Definition. The Lie algebra $\mathfrak{su}(2)$ is generated by the Pauli spin matrices. The decomposition $\mathfrak{su}(2) = \mathfrak{k} \oplus \mathfrak{m}$ where $\mathfrak{k} = \text{span}_{\mathbb{R}}\{Y\}$ and $\mathfrak{m} = \text{span}_{\mathbb{R}}\{X, Z\}$ satisfies the criteria to be a Cartan decomposition. Furthermore, either $\text{span}_{\mathbb{R}}\{X\}$ or $\text{span}_{\mathbb{R}}\{Z\}$ is a maximally abelian subalgebra of $\mathfrak{su}(2)$ contained in \mathfrak{m} . Thus the decomposition of $SU(2)$ given by $U = e^{iAY} e^{iBZ} e^{iCY}$ is a Cartan decomposition. Using the fact that $SU(2)$ is the double cover of $SO(3)$, we recognize this Cartan decomposition as the Euler angle decomposition of three-dimensional rotations. We now explicitly calculate the Euler angle decomposition of an arbitrary single qubit unitary using a Cartan involution.

The Cartan involution corresponding to our chosen Cartan decomposition ($\mathfrak{k} = \text{span}_{\mathbb{R}}\{Y\}$, $\mathfrak{m} = \text{span}_{\mathbb{R}}\{X, Z\}$ and $\mathfrak{h} = \text{span}_{\mathbb{R}}\{Z\}$) is $\theta(u) = YuY$, $\Theta(U) = YUY$. We compute the Cartan KAK decomposition of an arbitrary $G \in SU(2)$ as follows:

- (1) We exploit theorem 2 to calculate $M^2 = YG^\dagger YG$.
- (2) Diagonalize $M^2 = PDP^\dagger$. Note that as a diagonal element of $SU(2)$, D must be of the form $e^{i\alpha Z}$, i.e. $D \in \exp(\mathfrak{h})$, and, furthermore, theorem 1 implies that $P \in \exp(\mathfrak{k})$.
- (3) We now have $M = PD^{1/2}P^\dagger$ and we may find $K = GM^\dagger$.
- (4) This constitutes a complete decomposition of G into the form $e^{iAY} e^{iBZ} e^{iCY}$: $G = KPD^{1/2}P^\dagger$, and it is trivial to extract the angles A , B and C from the matrix forms of these operators.

3.2. Two qubit factoring from a Cartan decomposition

The task of factoring two qubit operators is facilitated by several unique properties of $SU(4)$. Firstly, $SO(4)$ is the Lie group corresponding to the \mathfrak{k} subalgebra of $\mathfrak{su}(4)$ under a type

AI involution. $SO(4)$ and the group of local operations acting on two qubits separately, $SU(2) \otimes SU(2)$, share a simply connected covering group, $Spin(4)$. In fact, elements of $SO(4)$ are mapped uniquely onto elements of $SU(2) \otimes SU(2)$ by changing to the ‘magic basis’ of Bell states through conjugation by the matrix [35]:

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & i & -1 \\ 1 & -i & 0 & 0 \end{pmatrix}. \quad (8)$$

There is no equivalent connection between $SO(2^n)$ and $SU(2^{n-1}) \otimes SU(2^{n-1})$ for $n > 2$. As a result of this close connection between the type **AI** Cartan decomposition of $SU(4)$ and the group of local operations (which may be implemented without the use of CNOT gates) it is possible to construct a universal two qubit circuit requiring only three CNOT gates in the worst case (see figure 1) [35, 45, 51, 52].

Definition. The involution for type **AI** Cartan decompositions of $\mathfrak{su}(N)$ is given by

$$\theta(u) = -u^T \quad \text{for } u \in \mathfrak{su}(N), \quad \Theta(U) = (U^{-1})^T = U^* \quad \text{for } U \in SU(N). \quad (9)$$

The involution given by (9) fixes a \mathfrak{k} -subalgebra corresponding to $\mathfrak{so}(4)$, $\mathfrak{k} = \text{span}_{\mathbb{R}}\{IY, XY, ZY, YI, YX, YX\}$, and the diagonal elements of \mathfrak{m} , i.e. $\mathfrak{h} = \text{span}_{\mathbb{R}}\{IZ, ZI, ZZ\}$ constitute a Cartan subalgebra. Furthermore, as discussed in the introduction, a transformation to the basis of Bell states (the ‘magic basis’) maps this \mathfrak{k} subalgebra onto $\mathfrak{su}(2) \oplus \mathfrak{su}(2)$ and also maps the maximal abelian subalgebra of diagonal matrices onto the subalgebra chosen by both Khaneja and Glaser and Vatan and Williams, $\mathfrak{h}' = \text{span}_{\mathbb{R}}\{XX, YY, ZZ\}$. As a result, we may use the Cartan involution of equation (9) and matrix diagonalization to compute the parameters necessary for Vatan and Williams two-qubit CNOT optimal circuit.

The parameters for an arbitrary two qubit unitary U may be calculated as follows:

- (1) We define a new operator $U' = B^\dagger U B$ where B is defined in equation (8).
- (2) Compute $M^2 = \Theta(U')U' = (U'^\dagger)^*U' = U'TU'$, which is in the exponentiation of \mathfrak{m} .
- (3) Diagonalize: $M^2 = PDP^\dagger$ where $D \in \exp(\mathfrak{h})$ and $P \in SO(4)$.
- (4) Find $D^{\frac{1}{2}}$ and hence $K' = U'PD^{-\frac{1}{2}}P^\dagger$.
- (5) $K'P$ and P^\dagger are both elements of $SO(4)$, so $K_1 = BK'PB^\dagger$ and $K_2 = BP^\dagger B^\dagger \in SU(2) \otimes SU(2)$ and $A = BD^{\frac{1}{2}}B^\dagger \in \exp(\mathfrak{h}')$. Hence

$$K_1AK_2 = BK'PB^\dagger BD^{\frac{1}{2}}B^\dagger BP^\dagger B^\dagger = BK'PD^{\frac{1}{2}}P^\dagger B^\dagger = BU'B^\dagger = U \quad (10)$$

is a Cartan decomposition of U of the type used by Vatan and Williams.

- (6) Simple algebraic manipulations of $D^{\frac{1}{2}}$ yield the parameters α , β and γ which appear in the center portion of the circuit in figure 6 of [35] and the partial trace may be used to separate K_1 and K_2 into the local operations of which they are composed, which may then be decomposed as described in the previous section.

4. The QSD from Cartan involutions

In this section we give a Cartan decomposition and constructive algorithm for obtaining the QSD (recall that it is not possible to exceed the QSD’s efficiency by even a factor of 2 for any number of qubits). This algorithm is constructive and produces circuits which are less than half as long as the constructive algorithms of Nakajima *et al* [46, 47]. The

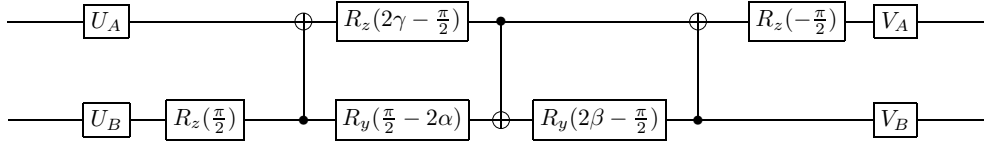


Figure 1. The CNOT optimized universal two qubit circuit; U_A, U_B, V_A and V_B may be decomposed into three single qubit rotations each by the Euler angle decomposition given above, and V_A and U_B may absorb the z -rotations preceding and following them respectively yielding a circuit consisting of three CNOT gates and 15 single qubit rotations.

principle difference between those algorithms and the QSD is that they proceed by reducing an n -qubit circuit to a circuit involving uniformly controlled $n - 1$ qubit gates. These uniformly controlled gates are then reduced to controlled and uncontrolled $n - 1$ qubit gates. The uncontrolled $n - 1$ qubit gates, and the controlled $n - 1$ qubit gates are then factored again using the Cartan decomposition. However, all gates obtained by this decomposition must be controlled, leading to a doubling of the number of CNOTs over the best known decompositions. This problem arises because only part of the decomposition is handled at the Lie algebra level—after the first decomposition circuit identities are introduced before the Cartan decomposition is applied again. In what follows we take the Lie algebraic point of view throughout: the uniformly controlled operations are treated as a Lie-subgroup, and a Cartan decomposition of the corresponding Lie-subalgebra is obtained. This Cartan decomposition results in uncontrolled $n - 1$ qubit operations which remain to be factored, and so the first part of the algorithm of Nakajima *et al* can be applied again. The resulting algorithm is an alternating pair of Cartan decompositions, each of which has a simple Cartan involution which enables the factors to be obtained explicitly. Inspection of the resulting procedure reveals precisely the QSD of [37] and so this algorithm gives a Cartan decomposition based derivation of the QSD and a Cartan involution based explicit algorithm for obtaining the QSD.

Because every other step in our recursive procedure is identical to the first step of Nakajima *et al*'s algorithm, we first define the corresponding components \mathfrak{k} and \mathfrak{m} of the Cartan decomposition of $SU(2^n)$, and the Cartan subalgebra \mathfrak{h} . The \mathfrak{k} -subalgebra is of type **AIII**: the direct sum of two lower dimensional unitary Lie algebras $\mathfrak{k} = \mathfrak{su}(p) \oplus \mathfrak{u}(q)$ where $p + q = 2^n$.

Definition. For the n -qubit case the decomposition is defined by

$$\mathfrak{k} = \text{span}_{\mathbb{R}}\{A \otimes Z, B \otimes \mathbf{1}, iZ^{(n)} | A, B \in \mathfrak{su}(2^{n-1})\} \tag{11}$$

$$\mathfrak{m} = \text{span}_{\mathbb{R}}\{A \otimes X, B \otimes Y, iX^{(n)}, iY^{(n)} | A, B \in \mathfrak{su}(2^{n-1})\}. \tag{12}$$

Definition. The Cartan involution is

$$\theta(u) = Z^{(n)} u Z^{(n)}, \quad \Theta(U) = Z^{(n)} U Z^{(n)}. \tag{13}$$

Hence we may compute the global Cartan decomposition $G = KM$ of $SU(2^n)$ as in theorem 2.

We must now define a Cartan subalgebra \mathfrak{h} contained in \mathfrak{m} . Here Nakajima *et al* make a different choice of \mathfrak{h} to that used by Khaneja and Glaser in [40, 41]. Recall that all maximal Abelian subalgebras share an adjoint orbit, namely \mathfrak{m} itself, and that one may, as a result, switch between them with relative ease.

Definition. Nakajima *et al* choose to define

$$\mathfrak{h} = \text{span}_{\mathbb{R}}\{|j\rangle\langle j| \otimes i\sigma_x | j = 0, \dots, 2^{n-1} - 1\}. \tag{14}$$

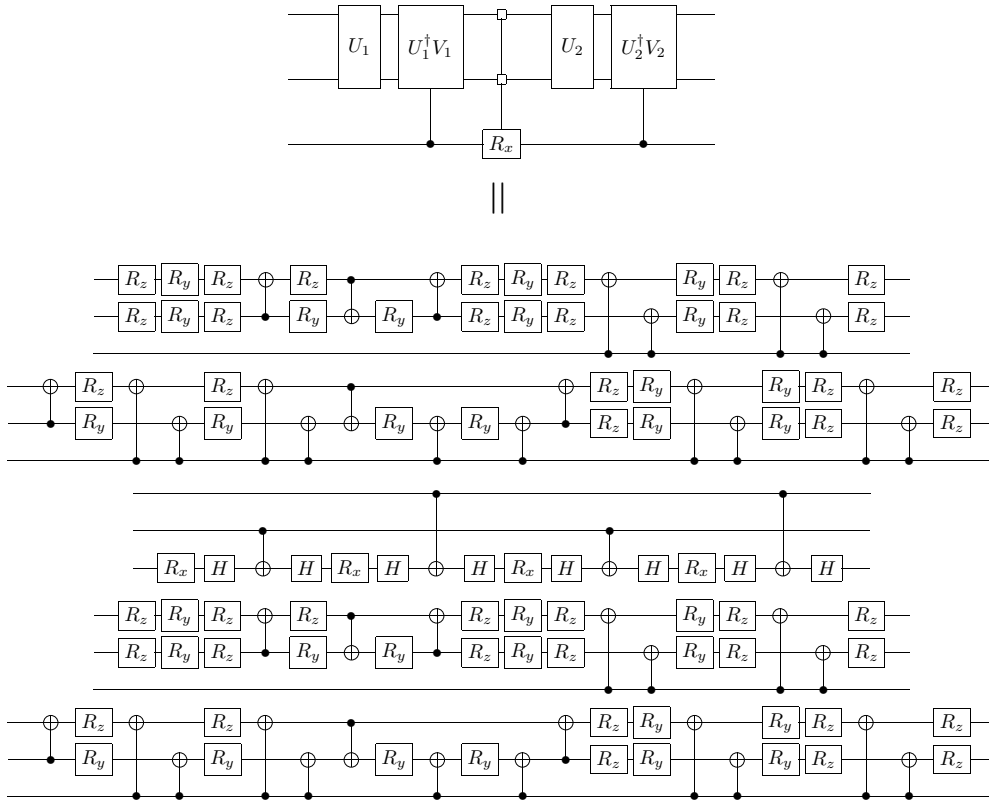


Figure 2. A simplified three qubit circuit based on Nakajima *et al*'s algorithm: uniformly controlled two qubit operations are built using Vatan and Williams' optimal two qubit circuit to produce a universal 44 CNOT three qubit circuit with a constructive algorithm. The operator represented here is $(U_1 \otimes |0\rangle\langle 0| + V_1 \otimes |1\rangle\langle 1|)(R_{x1} \oplus R_{x2} \oplus R_{x3} \oplus R_{x4})(U_2 \otimes |0\rangle\langle 0| + V_2 \otimes |1\rangle\langle 1|)$, in accordance with the NKS algorithm.

The algorithm of [47] based upon this choice of \mathfrak{h} corresponds to a decomposition of an n -qubit quantum logic circuit into $2^{n-1} - 1$ uniformly controlled one qubit elementary rotations, requiring $4^n - 2^{n-1}$ CNOT gates.

Note that Nakajima *et al* Cartan decompose $SU(2^n)$ yielding two elements of $SU(2^{n-1}) \oplus SU(2^{n-1})$. These are then treated as if they were four elements of $SU(2^{n-1})$ with no further special structure, and precisely the same Cartan decomposition is applied to each of these smaller unitary operators. This approach is implicitly based on the assumption that the tensor sum of Cartan decompositions is the Cartan decomposition of tensor sums. This assumption, however, can easily be proven to be false. Thus, we now set out to find a Cartan decomposition of the Lie algebra $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})$.

Consider the basis of $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})$: $\text{span}_{\mathbb{R}}\{A \otimes Z, B \otimes \mathbf{1}, iZ^{(n)} | A, B \in \mathfrak{su}(2^{n-1})\}$.

Definition. It is straightforward to confirm that the decomposition

$$\mathfrak{k}' = \text{span}_{\mathbb{R}}\{A \otimes \mathbf{1}, iZ^{(n)} | A \in \mathfrak{su}(2^{n-1})\}$$

$$\mathfrak{m}' = \text{span}_{\mathbb{R}}\{A \otimes Z | A \in \mathfrak{su}(2^{n-1})\}$$

satisfies the definition of a Cartan decomposition for $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})$. Note that $Z^{(n)}$ represents a phase and commutes with every element of \mathfrak{k}' , indeed it commutes with

every element of $\mathfrak{s}[\mathfrak{u}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})]$. We may factor out the $Z^{(n)}$ component from $\mathfrak{s}[\mathfrak{u}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})]$ to get $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{su}(2^{n-1})$. If we define $\tilde{\mathfrak{k}}' = \mathfrak{k}' \setminus \text{span}_{\mathbb{R}} Z^{(n)}$, then $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{su}(2^{n-1}) = \tilde{\mathfrak{k}}' \oplus \mathfrak{m}'$ is a Cartan decomposition.

Definition. A Cartan involution to separate these subsets is $\theta(m) = X^{(n)}mX^{(n)}$. Furthermore we find that if we apply this involution to an element of $\mathfrak{s}[\mathfrak{u}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})]$ which has not had its $Z^{(n)}$ phase factored out, the phase lands in the -1 eigenspace. We must also choose a Cartan subalgebra in \mathfrak{m}' ; for simplicity, we choose the set of diagonal elements of \mathfrak{m}' : $\mathfrak{h}' = \text{span}_{\mathbb{R}}\{IZZ, ZIZ, ZZZ\}$ in the three qubit case.

We now compute the Cartan KAK factors of an arbitrary element (G) of $S[U(2^{n-1}) \oplus U(2^{n-1})]$. First we use the method of theorem 2 to compute the component of G not in $\exp(\tilde{\mathfrak{k}}')$, i.e. we compute $\tilde{M}^2 = M^2P^2$ where M is from $G = KM$ and P is the $Z^{(n)}$ factor. Next we diagonalize \tilde{M}^2 —this diagonal matrix is A^2P^2 , where $M = LAL^\dagger$ for $A \in \exp(\mathfrak{h}')$, $L \in \exp(\tilde{\mathfrak{k}}')$. Finally we take the square root of this diagonal matrix and compute K . To be completely explicit, we present here the algorithm.

- (1) Compute $\tilde{M}^2 = M^2P^2 = \Theta(G^\dagger)G$ where $\Theta(U) = X^{(n)}UX^{(n)}$ (see theorem 2).
- (2) Compute the eigenvalue decomposition of \tilde{M}^2 : let $\tilde{M}^2 = LD^2L^\dagger$ be the eigenvalue decomposition. Since D^2 is diagonal and unitary it must be an element of the exponentiation of $\mathfrak{h}' \cup \text{span}_{\mathbb{R}} Z^{(n)}$ and L must be an element of $\exp(\tilde{\mathfrak{k}}')$.
- (3) Compute $\tilde{A} = D^{1/2} = AP$ where $A \in \exp(\mathfrak{h}')$ and P is the phase term. Each entry in the diagonal unitary D is of the form $e^{i\theta}$, so we may simply replace each of these entries with $e^{\frac{i\theta}{2}}$ and we have \tilde{A} . Now $\tilde{M} = L\tilde{A}L^\dagger$.
- (4) Compute $K = G\tilde{M}^\dagger$. We have $G = P(KLAL^\dagger)$ where P commutes with all of the other factors and therefore may be placed according to convenience, $K, L \in \exp(\tilde{\mathfrak{k}}')$ and $A \in \exp(\mathfrak{h}')$, that is K and L are general $(n-1)$ qubit operations which leave the low qubit fixed and A is a uniformly controlled z -rotation on the low qubit.

The operations in $\exp(\tilde{\mathfrak{k}}')$ do nothing to the n th qubit and can perform any unitary operation on the remaining $n-1$ qubits, i.e. we can treat them precisely as we would any element of $SU(2^{n-1})$, and we may absorb the diagonal P into A and implement $\tilde{A} = AP$ according to the decomposition offered in [37], which leaves us with a uniformly controlled z -rotation on the low qubit and a diagonal operator acting on the remaining qubits which may simply be absorb into a neighboring $n-1$ qubit operation.

Given an operation on any number of qubits n , we apply Nakajima *et al*'s algorithm to produce two elements of $S[U(2^{n-1}) \oplus U(2^{n-1})]$, then we apply the algorithm we have just described to these uniformly controlled operations to yield four elements of $SU(2^{n-1})$ to which we apply the NKS algorithm, and so on, until we are left with 4^{n-2} two qubit operations, to which we apply the **AI** algorithm described earlier. This recursive decomposition scheme generates a complete constructive factorization (see figure 3 for the three qubit case and figure 4 for an illustration of the recursion applied to four qubits). Using no further refinements, this algorithm yields a 24 CNOT three qubit gate and has an asymptotic CNOT cost of $\frac{9}{16}4^n - \frac{3}{2}2^n$, an improvement of nearly a factor of 2 over the standard NKS circuit.

5. Conclusions and future work

This scheme of alternating Cartan decompositions of $\mathfrak{su}(2^n)$ with Cartan decompositions of $\mathfrak{s}[\mathfrak{u}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})]$ is the best known circuit decomposition paradigm. This chain of decompositions yields precisely the QSD circuit structure that Shende, Bullock and Markov derived by analogy from the classical Shannon decomposition in [37]. Further

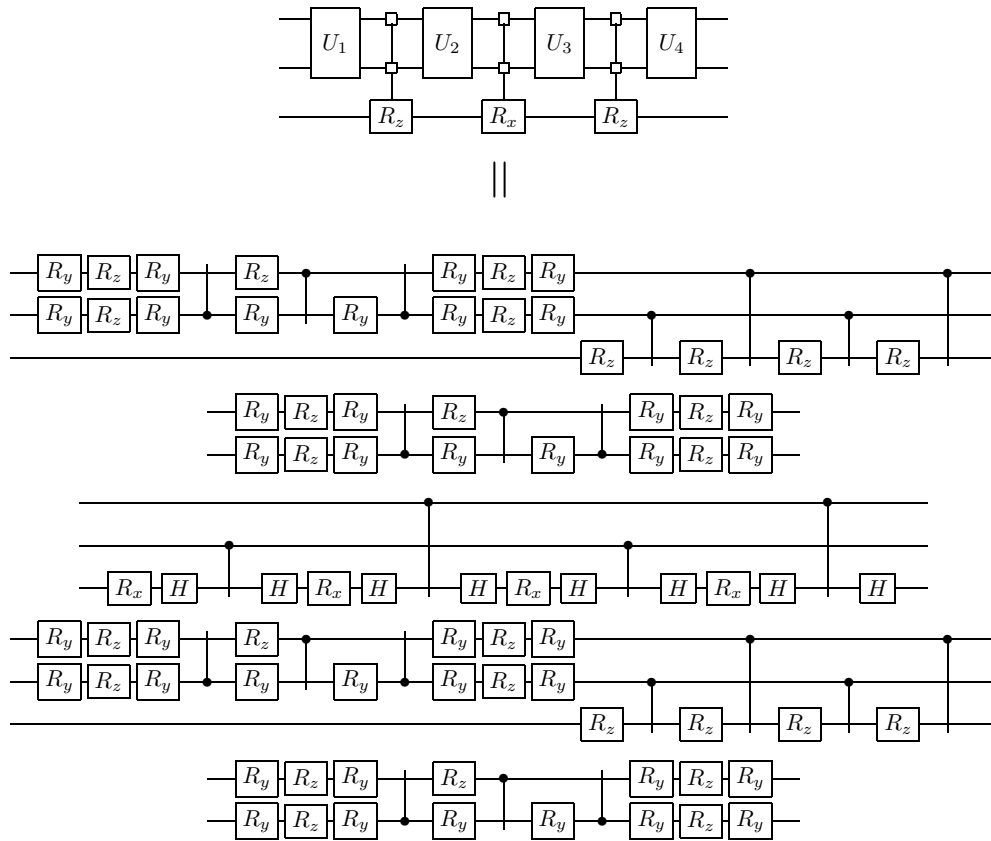


Figure 3. The 24 CNOT universal three qubit quantum circuit derived without further simplification from the Cartan decomposition of $\mathfrak{su}(2^{n-1}) \oplus \mathfrak{u}(2^{n-1})$.

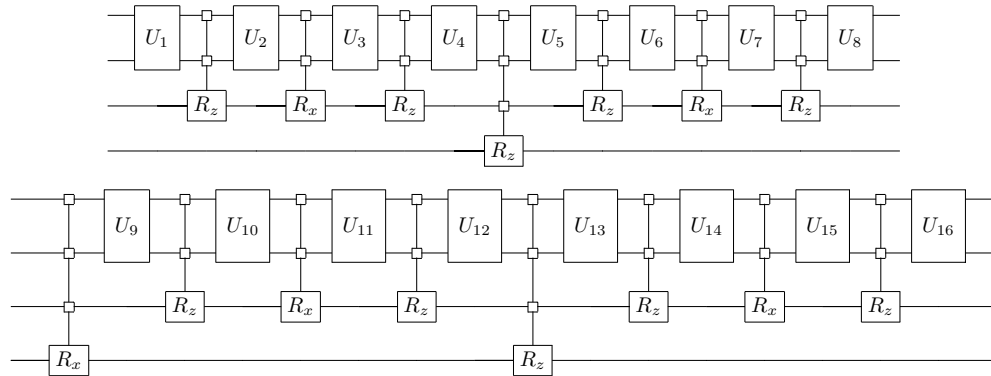


Figure 4. A block diagram of the QSD applied to a four qubit operation; note that it consists of only three thrice controlled rotations on the low qubit and four general three qubit QSD circuits on the higher qubits.

slight improvements can be made to the CNOT cost of the tensor sum Cartan circuit by the application of the identities given in appendix A and theorem (14) of [37], reducing the overall

cost of a three qubit gate to 20 CNOTs, and the asymptotic cost to $\frac{23}{48}4^n - \frac{3}{2}2^n + \frac{4}{3}$, but the decomposition is still fundamentally the same, and these simplifications can be incorporated into the constructive algorithm presented here with very little effort. By constructing the QSD from its Lie algebraic roots this work puts the QSD—the best known generic quantum circuit decomposition, less than a factor of two from the highest lower bound—into its proper Lie algebraic context as a series of Cartan decompositions, and provides a new Cartan involution based algorithm to implement the QSD explicitly.

Another significant advantage of this sort of decomposition, especially in light of the fact that historically few-qubit circuit optimization has at times advanced ahead of asymptotic circuit optimization (cf [36]), is that any future improvements to few-qubit efficiency can simply be plugged into this algorithm at its lowest level of recursion (where we turn to Vatan and Williams' circuit in this case) and translated instantly into improved asymptotic gate counts. For example, one could use existing methods (e.g. [53, 54]) to test whether a particular two-qubit gate has non-generic structure which means that it requires one or two CNOT gates rather than three. Substantially shorter circuits could be obtained by the application of such methods, and by their extension to three qubit circuits.

References

- [1] Deutsch D 1985 Quantum theory, the church-turing principle and the universal quantum computer *Proc. R. Soc. Lond. A* **400**
- [2] Shor P W 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Sci. Stat. Comput.* **26** 1484
- [3] Grover L K 1997 Quantum mechanics helps in searching for a needle in a haystack *Phys. Rev. Lett.* **79** 325–8
- [4] Feynman R P 1982 Simulating physics with computers *Int. J. Theor. Phys.* **21** 467–88
- [5] Wiesner S 1996 Simulations of many-body quantum systems by a quantum computer <http://www.arxiv.org/abs/quant-ph/9603028>
- [6] Zalka C 1998 Simulating quantum systems on a quantum computer *Proc.: Math. Phys. Eng. Sci.* **454** 313–22
- [7] Lloyd S 1996 Universal quantum simulators *Science* **273** 1073–8
- [8] Abrams D S and Lloyd S 1997 Simulation of many-body fermi systems on a universal quantum computer *Phys. Rev. Lett.* **79** 2586–9
- [9] Boghosian B M and IV Taylor W 1998 Simulating quantum mechanics on a quantum computer *Physica D* **120** 30–42
- [10] Aspuru-Guzik A, Dutoi A D, Love P J and Head-Gordon M 2005 Simulated quantum computation of molecular energies *Science* **309** 1704–7
- [11] Kassal I, Jordan S P, Love P J, Mohseni M and Aspuru-Guzik A 2008 Quantum algorithms for the simulation of chemical dynamics arXiv:0801.2986
- [12] Yao A C-C 1993 *Quantum circuit complexity 34th Annual Symposium on Foundations of Computer Science* pp 352–61
- [13] Gershenfeld N A and Chuang I L 1997 Bulk spin-resonance quantum computation *Science* **275** 350–6
- [14] Gulde S, Riebe M, Lancaster G P T, Becher C, Eschner J, Häffner H, Schmidt-Kaler F, Chuang I L and Blatt R 2003 Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer *Nature* **421** 48–50
- [15] Kim M D and Hong J 2004 Coupling of Josephson current qubits using a connecting loop *Phys. Rev. B* **70** 184525
- [16] Vandersypen L M K, Steffen M, Breyta G, Yannoni C S, Sherwood M H and Chuang I L 2001 Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance *Nature* **414** 883–7
- [17] Wrachtrup J, Kilin S Y and Nizovtsev A P 2001 Quantum computation using the ^{13}C nuclear spins near the single NV defect center in diamond *Opt. Spectrosc.* **91** 429–37
- [18] Jones J A and Mosca M 1998 Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer *J. Chem. Phys.* **109** 1648–53
- [19] Chuang I L and Nielsen M A 2000 *Quantum Computation and Quantum Information* (New York: Cambridge University Press)
- [20] Leibfried D *et al* 2003 Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate *Nature* **422** 412–5
- [21] Monroe C, Meekhof D M, King B E, Itano W M and Wineland D J 1995 Demonstration of a fundamental quantum logic gate *Phys. Rev. Lett.* **75** 4714–7

- [22] Pittman T B, Fitch M J, Jacobs B C and Franson J D 2003 Experimental controlled-not logic gate for single photons in the coincidence basis *Phys. Rev. A* **68** 032316
- [23] Zhao Z, Zhang A-N, Chen Y-A, Zhang H, Jiang-Feng D, Yang T and Pan J-W 2005 Experimental demonstration of a nondestructive controlled-not quantum gate for two independent photon qubits *Phys. Rev. Lett.* **94** 030501
- [24] Rauschenbeutel A, Nogues G, Osnaghi S, Bertet P, Brune M, Raimond J M and Haroche S 1999 Coherent operation of a tunable quantum phase gate in cavity QED *Phys. Rev. Lett.* **83** 5166–9
- [25] Jozsa R 1998 Quantum algorithms and the Fourier transform *Proc.: Math. Phys. Eng. Sci.* **454** 323–37
- [26] Beals R 1997 Quantum computation of Fourier transforms over symmetric groups *STOC '97: Proc. Twenty-Ninth Annual ACM Symposium on Theory of Computing* (New York: ACM) pp 48–53
- [27] Moore C, Rockmore D and Russell A 2006 Generic quantum Fourier transforms *ACM Trans. Algorithms* **2** 707–23
- [28] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev. A* **52** 3457–67
- [29] Knill E 1995 Approximation by quantum circuits <http://arxiv.org/abs/quant-ph/9508006>
- [30] Shende V V, Markov I L and Bullock S S 2004 Minimal universal two-qubit controlled-not-based circuits *Phys. Rev. A* **69** 062321
- [31] Vartiainen J J, Möttönen M and Salomaa M M 2004 Efficient decomposition of quantum gates *Phys. Rev. Lett.* **92** 177902
- [32] Möttönen M, Vartiainen J J, Bergholm V and Salomaa M M 2004 Quantum circuits for general multiqubit gates *Phys. Rev. Lett.* **93** 130502
- [33] Paige C C and Wei M 1994 History and generality of the CS decomposition *Linear Alg. App.* **208** 303
- [34] Sutton B D 2008 Computing the complete CS decomposition *Numer. Algorithms* **48** 97–117
- [35] Vatan F and Williams C 2004 Optimal quantum circuits for general two-qubit gates *Phys. Rev. A* **69** 032315
- [36] Vatan F and Williams C P 2004 Realization of a general three-qubit quantum gate <http://www.arxiv.org/abs/quant-ph/0401178>
- [37] Shende V V, Bullock S S and Markov I L 2006 Synthesis of quantum-logic circuits *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **25** 1000–10
- [38] Cartan E 1926 Sur une classe remarquable d'espaces de Riemann *Bull. Soc. Math. France* **54** 214–64
- [39] Cartan E 1927 Sur une classe remarquable d'espaces de Riemann: II. *Bull. Soc. Math. France* **55** 114–34
- [40] Khaneja N and Glaser S J 2001 Cartan decomposition of $su(2^n)$ and control of spin systems *Chem. Phys.* **267** 11–23
- [41] Khaneja N, Brockett R and Glaser S J 2001 Time optimal control in spin systems *Phys. Rev. A* **63** 032308
- [42] Bullock S S 2004 Note on the khaneja glaser decomposition *Quantum Inf. Comput.* **4** 396
- [43] Bullock S S and Brennen G K 2004 Canonical decompositions of n -qubit quantum computations and concurrence *J. Math. Phys.* **45** 2447–67
- [44] Dagli Mehmet, D'Alessandro Domenico and Smith J D H 2008 A general framework for recursive decompositions of unitary quantum evolutions *J. Phys. A: Math. Theor.* **41** 155302
- [45] Sousa P B M and Ramos R V 2006 Universal quantum circuit for n -qubit quantum gate: a programmable quantum gate <http://www.arxiv.org/abs/quant-ph/0602174>
- [46] Sá Earp Henrique N and Pachos Jiannis K 2005 A constructive algorithm for the cartan decomposition of $su(2^n)$ *J. Math. Phys.* **46** 082108
- [47] Nakajima Yumi, Kawano Yasuhito and Sekigawa Hiroshi 2005 A new algorithm for producing quantum circuits using kak decompositions <http://www.arxiv.org/abs/quant-ph/0509196>
- [48] Segal G, Carter R and MacDonald I 1995 *Lectures on Lie Groups and Lie Algebras* (Cambridge: Cambridge University Press)
- [49] Helgason Sigurdur 1978 *Differential Geometry, Lie Groups, and Symmetric Spaces* (New York: Academic)
- [50] Gilmore R 1974 *Lie Groups, Lie Algebras, and Some of Their Applications* (Mineola, NY: Dover)
- [51] Zhang J, Vala J, Sastry S and Whaley K B 2003 Exact two-qubit universal quantum circuit *Phys. Rev. Lett.* **91** 027903
- [52] Shende V V, Bullock S S and Markov I L 2004 Recognizing small-circuit structure in two-qubit operators *Phys. Rev. A* **70** 012310
- [53] Makhlin Y 2003 Nonlocal properties of two qubit gates and mixed states, and the optimization of quantum computations *Quantum Inf. Proc.* **1** 243–52 <http://arxiv.org/abs/quant-ph/0002045>
- [54] Shende V V, Bullock S S and Markov I L 2004 Recognizing small-circuit structure in two qubit operators *Phys. Rev. A* **70** 012310