Quantum Information and Computation, Vol. 6, No. 1 (2005) 058–066
© Rinton Press

A DISCRETE LOCAL INVARIANT FOR QUANTUM GATES

LAURA KOPONEN[a], VILLE BERGHOLM, MARTTI M. SALOMAA
Laboratory of Physics, TKK, P.O. Box 4100
02015 TKK, Finland

Received May 22, 2005
Revised September 21, 2005

In this paper we study the properties of two-qubit gates. We review the most common parameterizations for the local equivalence classes of two-qubit gates and the connections between them. We then introduce a new discrete local invariant, namely the number of local degrees of freedom that a gate can bind. The value of this invariant is calculated analytically for all the local equivalence classes of two-qubit gates. We find that almost all two-qubit gates can bind the full six local degrees of freedom and are in this sense more effective than the controlled-NOT gate which only can bind four local degrees of freedom.

Keywords: quantum computation, local gate invariants
Communicated by: I Cirac & B Terhal

1 Introduction

Quantum computation is a novel information processing method in which classical information is encoded into a quantum-mechanical system [1], called the quantum register. In most quantum computers the quantum register is a collection of two-level systems, termed qubits. The computation is performed by the unitary temporal evolution of the register, followed by a measurement. In order to execute a quantum algorithm, one has to be able to generate the required unitary propagators that are usually referred to as quantum gates.

It has been shown that almost any fixed two-qubit gate together with arbitrary single-qubit gates is universal [2, 3], i.e., any n-qubit gate may be constructed using only a finite number of these gates. Conventionally, the elementary gate library is chosen to consist of the single-qubit rotations R_x, R_y, R_z and the controlled-NOT gate (CNOT). However, in many realizations, the CNOT is not the natural choice for the entangling two-qubit gate. Recently, an optimal construction of an arbitrary two-qubit gate using three CNOTs and 15 single-qubit rotations has been introduced [4]. In addition, constructions for the double-CNOT (DCNOT) [5], the controlled-unitary gates [5] and the so-called super controlled gates [6] have been published. A construction using only two applications of the B gate has been introduced in Ref. [7], and in Ref. [8] it is shown that no other construction using only two applications of a fixed two-qubit gate exists. Extensions to the n-qubit case are mainly uninvestigated. However, several CNOT-based constructions with $O(4^n)$ asymptotic behaviour exist, the best of which [9, 10] have CNOT counts of twice the highest known lower bound [4].

[a]Present address: VTT Information Technology, Microsensing, P.O. Box 1207, 02044 VTT, Finland

In many of the proposed realizations for quantum computers the individual qubits are fully controllable, whereas the interqubit interactions are often fixed. In addition, single-qubit operations tend to be considerably faster to implement than multiqubit operations. This is why it often makes sense to study the *local equivalence classes* of multiqubit gates instead of the gates themselves. Two gates are considered equivalent if they can be converted to each other using only local operations, i.e., tensor products of single-qubit gates. The equivalence classes are characterized by local invariants, which are quantities that are not affected by local operations.

In this paper we briefly review the currently used parameterizations for the local equivalence classes of two-qubit gates and point out their equivalence. We then introduce a new discrete local invariant which describes the number of local degrees of freedom a gate can *bind*. Finally, we calculate the value of this invariant for all the local equivalence classes of two-qubit gates.

2 Local equivalence classes of two-qubit gates

An n-qubit quantum gate k is said to be *local* iff it consists solely of single-qubit rotations: $k \in SU(2)^{\otimes n} =: \mathbb{L}_n$. Two n-qubit gates $U_1, U_2 \in SU(2^n)$ are said to be locally equivalent iff $U_2 = k_1 U_1 k_2$, where $k_1, k_2 \in \mathbb{L}_n$. This constitutes an equivalence relation, which we denote by $U_1 \sim U_2$.

Using the theory of Lie groups [11] it can be shown [12, 13] that any two-qubit gate $U \in SU(4)$ can be decomposed using the Cartan decomposition as

$$U = k_1 A k_2 = k_1 \exp\left(\frac{i}{2}(c_1\sigma_x \otimes \sigma_x + c_2\sigma_y \otimes \sigma_y + c_3\sigma_z \otimes \sigma_z)\right) k_2, \tag{1}$$

where σ_i denote the Pauli matrices, $k_1, k_2 \in \mathbb{L}_2$ and $c_1, c_2, c_3 \in \mathbb{R}$. The matrix A is a member of the Cartan subgroup of the decomposition and carries all the nonlocal properties of the gate U. Hence the local equivalence classes of two-qubit gates can be parameterized by the three scalars $[c_1, c_2, c_3]$, known as canonical parameters. This is a minimal set of parameters since the group $SU(4)$ is 15-dimensional and the local rotations eliminate $2 \times \dim(SU(2)^{\otimes 2}) = 12$ degrees of freedom thereof. The canonical parameterization is visualized in Fig. 1. The tetrahedron $OA_1A_2A_3$ in the figure is called a Weyl chamber. It is defined by the inequalities $\pi \geq c_1 \geq c_2 \geq c_3 \geq 0, \pi - c_1 \geq c_2$. The Weyl chamber contains all the local equivalence classes of two-qubit gates exactly once, excepting the fact that the triangles LA_1A_2 and LOA_2 are equivalent.

The matrix

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -i & -i & 0 \\ 0 & 1 & -1 & 0 \\ -i & 0 & 0 & i \end{pmatrix} \tag{2}$$

is the transformation from the standard basis of states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ into the Bell basis, also known as the magic basis [14]. We use the lower index B to denote the change of basis: $U_B := QUQ^\dagger$. The magic basis has the special property that local gates expressed in it are orthogonal. In other words, conjugation by Q is a group isomorphism between

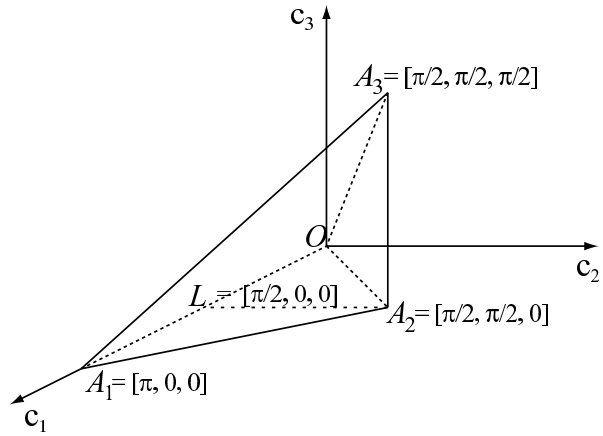

Fig. 1. Weyl chamber. Points O and A_1 correspond to the identity gate I, A_3 to the SWAP gate, L to the controlled-NOT gate (CNOT) and A_2 to the double controlled-NOT gate (DCNOT) [13].

$SU(2) \otimes SU(2)$ and $SO(4)$. Furthermore, it renders our chosen Cartan subgroup (generated by $\frac{i}{2}(\sigma_x \otimes \sigma_x)$, $\frac{i}{2}(\sigma_y \otimes \sigma_y)$ and $\frac{i}{2}(\sigma_z \otimes \sigma_z)$) diagonal. These two properties enable us to calculate the canonical parameters of any given $SU(4)$ gate $U = k_1 A k_2$. The parameters are obtained from the spectrum of the matrix $M(U) := U_B^T U_B$ which is given by

$$\lambda\left(M(U)\right) = \left\{e^{i(c_1+c_2-c_3)}, e^{i(c_1-c_2+c_3)}, e^{i(-c_1+c_2+c_3)}, e^{-i(c_1+c_2+c_3)}\right\}. \tag{3}$$

Ref. [15] presents an algorithm for extracting the canonical parameters c_i from this spectrum in a convenient way although it uses a slightly different notation. The equivalence of the methods becomes apparent using the equality $Q^T Q = -\sigma_y \otimes \sigma_y$, since

$$\begin{aligned}\lambda\left(M(U)\right) &= \lambda\left((QUQ^\dagger)^T QUQ^\dagger\right) = \lambda\left((\sigma_y \otimes \sigma_y)^\dagger U^T (\sigma_y \otimes \sigma_y) U\right) \\ &= \lambda\left(U(\sigma_y \otimes \sigma_y) U^T (\sigma_y \otimes \sigma_y)\right) = \lambda(U\tilde{U}).\end{aligned} \tag{4}$$

Ref. [4] presents another system of invariants, namely the characteristic polynomials $\chi[\gamma_2(U)]$, where $\gamma_2(U) = U(\sigma_y \otimes \sigma_y)U^T(\sigma_y \otimes \sigma_y)$. They are completely equivalent to the canonical parameters since the characteristic polynomial $\chi[\gamma_2(U)]$ carries exactly the same information as $\lambda\left(M(U)\right) = \lambda(\gamma_2(U))$.

Another useful parameterization for the two-qubit local equivalence classes is provided by the Makhlin invariants G_1 and G_2 [14]. For a gate $U \in U(4)$, they are defined as

$$G_1 = \frac{\mathrm{Tr}^2\, M(U)}{16 \det U}, \qquad G_2 = \frac{\mathrm{Tr}^2\, M(U) - \mathrm{Tr}\, M(U)^2}{4 \det U}. \tag{5}$$

The Makhlin invariants are by far the easiest ones to calculate. They, too, provide the same information as the previous invariants since $\lambda\left(M(U)\right)$ is fully determined by them. G_1 may be complex but G_2 is always a real number, which leads to three real-valued invariants. If U

Table 1. Values of the canonical and Makhlin invariants for some common two-qubit gates. $\bigwedge_1(U)$ denotes a controlled-unitary gate and SPE a special perfect entangler [16, 6].

Gate	c_1	c_2	c_3	g_1	g_2	g_3
I	0	0	0	1	0	3
SWAP	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	-1	0	-3
CNOT	$\frac{\pi}{2}$	0	0	0	0	1
DCNOT	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0	0	-1
$\sqrt{\text{SWAP}}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	0	$\frac{1}{4}$	0
$\sqrt{\text{SWAP}}^{-1}$	$\frac{3\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	0	-$\frac{1}{4}$	0
B	$\frac{\pi}{2}$	$\frac{\pi}{4}$	0	0	0	0
$\bigwedge_1(U)$	α	0	0	$\cos^2(\alpha)$	0	$2\cos^2(\alpha)+1$
SPE	$\frac{\pi}{2}$	α	0	0	0	$\cos(2\alpha)$

is represented as in Eq. (1), the Makhlin invariants reduce to [13]

$$\begin{aligned} g_1 &:= \operatorname{Re} G_1 = \cos^2 c_1 \cos^2 c_2 \cos^2 c_3 - \sin^2 c_1 \sin^2 c_2 \sin^2 c_3, \\ g_2 &:= \operatorname{Im} G_1 = \frac{1}{4} \sin 2c_1 \sin 2c_2 \sin 2c_3, \\ g_3 &:= G_2 = 4\cos^2 c_1 \cos^2 c_2 \cos^2 c_3 - 4\sin^2 c_1 \sin^2 c_2 \sin^2 c_3 - \cos 2c_1 \cos 2c_2 \cos 2c_3. \end{aligned} \tag{6}$$

Example values of the invariants of different gates are given in Table 1. The set of all the two-qubit gate equivalence classes in the Makhlin parameter space is presented in Fig. 2. The surface and the inside of the object correspond to the surface and the inside of the Weyl chamber, respectively. On the surface of the set the canonical parameters have the form $[s,t,t]$, where $s \in [0,\pi]$, $t \in [0,\pi/2]$. The surface is thus given by the equations

$$\begin{aligned} g_1 &= \cos^2 s \cos^4 t - \sin^2 s \sin^4 t \\ g_2 &= \frac{1}{4} \sin(2s) \sin^2(2t) \\ g_3 &= 4g_1 - \cos(2s)\cos^2(2t). \end{aligned} \tag{7}$$

3 The local invariant η

Let us use

$$L_n^k(\mathbf{a},\vec{\theta}) := \exp\left(\sum_{j=1}^{3n} a_j(\vec{\theta}) X_j\right), \qquad L_n^k(\mathbf{a},\vec{\theta}) \in \mathbb{L}_n \quad \forall \vec{\theta} \in \mathbb{R}^k, \tag{8}$$

where j runs over the $3n$ local generators of $SU(2^n)$, to denote a k-parameter family of n-qubit local gates. It is defined by the continuous function $\mathbf{a} : \mathbb{R}^k \to \mathbb{R}^{3n}$. The generators $X_j \in \mathfrak{su}(2^n)$ are normalized such that they are orthonormal with respect to the inner product $\langle X, Y\rangle := \operatorname{Tr}\left(X^\dagger Y\right)$. We also arrange our basis $\mathcal{B}$ of $\mathfrak{su}(2^n)$ such that the local generators precede the nonlocal ones.

A gate $U \in SU(2^n)$ is said to *leak* k local degrees of freedom iff there exist injections $\mathbf{a}$ and $\mathbf{b}$ such that

$$U L_n^k(\mathbf{a},\vec{\theta}) = L_n^k(\mathbf{b},\vec{\theta}) U \quad \forall \vec{\theta} \in \mathbb{R}^k. \tag{9}$$

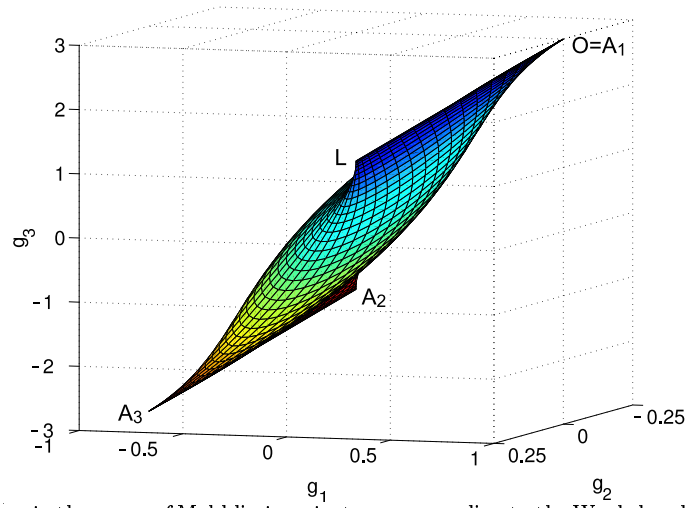

Fig. 2. Volume in the space of Makhlin invariants corresponding to the Weyl chamber. The surface of the set is given by Eq. (7).

A gate binds the local degrees of freedom that it does not leak. We define a function $\eta : SU(2^n) \to \mathbb{N}$ to indicate the number of local degrees of freedom that an n-qubit gate U binds. We always have $\max \eta \leq 3n$, i.e., at most three degrees of freedom for each qubit.

We now introduce a matrix representation for the adjoint representation of U in the basis $\mathcal{B}$:

$$W_{ij} := \langle X_i, \mathrm{Ad}(U) X_j \rangle = \left\langle X_i, U X_j U^\dagger \right\rangle = \mathrm{Tr}\left(X_i^\dagger U X_j U^\dagger \right), \quad \mathrm{Ad}(U) X_j = \sum_i X_i W_{ij}. \tag{10}$$

Equation (9) is seen to be equivalent to

$$U \exp\left(\sum_{j=1}^{3n} a_j(\vec{\theta}) X_j \right) U^\dagger = \exp\left(\sum_{j=1}^{3n} a_j(\vec{\theta}) \,\mathrm{Ad}(U) X_j \right) = \exp\left(\sum_{k=1}^{3n} b_k(\vec{\theta}) X_k \right) \quad \forall \vec{\theta} \in \mathbb{R}^k. \tag{11}$$

This is fulfilled if

$$\sum_{j=1}^{3n} a_j(\vec{\theta}) \,\mathrm{Ad}(U) X_j = \sum_{j=1}^{3n} \sum_i X_i W_{ij} a_j(\vec{\theta}) = \sum_{k=1}^{3n} b_k(\vec{\theta}) X_k. \tag{12}$$

Taking sidewise inner products with X_l, we obtain in matrix form

$$W \mathbf{a}(\vec{\theta}) = \begin{pmatrix} W_{LL} \\ W_{NL} \end{pmatrix} \mathbf{a}(\vec{\theta}) = \begin{pmatrix} \mathbf{b}(\vec{\theta}) \\ \vec{0} \end{pmatrix} \quad \forall \vec{\theta} \in \mathbb{R}^k, \tag{13}$$

where $W_{LL} \in \mathbb{R}^{3n \times 3n}$, $W_{NL} \in \mathbb{R}^{(4^n - 1 - 3n) \times 3n}$, and the indices L and N stand for local and nonlocal, respectively. From Eq. (13) we must have $\mathbf{a}(\vec{\theta}) \in \ker W_{NL}$ for all values of $\vec{\theta}$. Using the rank-nullity theorem we finally obtain

$$\eta(U) = 3n - \dim(\ker W_{NL}). \tag{14}$$

It still remains to be shown that η is a local invariant. Assume that the functions $\mathbf{a}$ and $\mathbf{b}$ satisfy Eq. (9) for the gate U. For a gate $V = k_1 U k_2$, where $k_1, k_2 \in \mathbb{L}_n$, we obtain

$$V \left[k_2^\dagger L_n^k(\mathbf{a}, \vec{\theta}) k_2\right] = k_1 U k_2 \, k_2^\dagger L_n^k(\mathbf{a}, \vec{\theta}) k_2 = k_1 L_n^k(\mathbf{b}, \vec{\theta}) \, U k_2 = \left[k_1 L_n^k(\mathbf{b}, \vec{\theta}) k_1^\dagger\right] V. \tag{15}$$

We also have

$$k_1 L_n^k(\mathbf{b}, \vec{\theta}) k_1^\dagger = \exp\left(\sum_{j=1}^{3n} b_j(\vec{\theta}) \operatorname{Ad}(k_1) X_j\right) = \exp\left(\sum_{j=1}^{3n} \tilde{b}_j(\vec{\theta}) X_j\right) = L_n^k(\tilde{\mathbf{b}}, \vec{\theta}), \tag{16}$$

since $\operatorname{Ad}(g)$ is a linear bijection and k_1 is a local gate [13]. If $\mathbf{b}$ is an injection then so is $\tilde{\mathbf{b}}$. A similar argument holds for $k_2^\dagger L_n^k(\mathbf{a}, \vec{\theta}) k_2$, which yields $V L_n^k(\tilde{\mathbf{a}}, \vec{\theta}) = L_n^k(\tilde{\mathbf{b}}, \vec{\theta}) V$ and completes our proof.

4 η for two-qubit gates

For the set of two-qubit gates $U \in SU(4)$, $\max \eta \leq 6$. It is obvious that $\eta(\mathrm{I}) = 0$ and $\eta(\mathrm{SWAP}) = 0$ since all local gates and hence all local degrees of freedom may be commuted through these gates. It is also known that $\eta(\mathrm{CNOT}) = 4$ and $\eta(\mathrm{DCNOT}) = 4$. The result for CNOT is obtained by combining the commutation properties of CNOT with the Euler rotations R_z and R_x and the fact that an arbitrary two-qubit gate may be implemented using at most three CNOTs [4, 17, 18, 19]. Similar arguments for the DCNOT are presented in Ref. [5], including the explicit implementation of an arbitrary two-qubit gate using three DCNOTs. Also, from the construction of Ref. [7], it is clear that $\eta(B) \geq 5$. Apart from such observations, no explicit calculations for η have been presented in the literature so far.

We will now proceed to derive an analytical expression for η for an arbitrary two-qubit gate. Because η is a local invariant, it is enough to consider gates of the type

$$\begin{aligned} A &= \exp\left(\frac{i}{2}(c_1 \sigma_x \otimes \sigma_x + c_2 \sigma_y \otimes \sigma_y + c_3 \sigma_z \otimes \sigma_z)\right) \\ &= \exp\left(\frac{i}{2}\begin{pmatrix} c_3 & 0 & 0 & c_1 - c_2 \\ 0 & -c_3 & c_1 + c_2 & 0 \\ 0 & c_1 + c_2 & -c_3 & 0 \\ c_1 - c_2 & 0 & 0 & c_3 \end{pmatrix}\right) \end{aligned} \tag{17}$$

which represent all the nonlocal equivalence classes. The calculation of the elements of W_{LL} and W_{NL} is straightforward. Calculating the matrix exponential and simplifying the expression using elementary trigonometric identities results in

$$W_{NL} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & n_{1,1}^3 & 0 & 0 & n_{1,2}^3 \\ 0 & n_{1,1}^2 & 0 & 0 & n_{1,2}^2 & 0 \\ 0 & 0 & n_{2,1}^3 & 0 & 0 & n_{2,2}^3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ n_{1,1}^1 & 0 & 0 & n_{1,2}^1 & 0 & 0 \\ 0 & n_{2,1}^2 & 0 & 0 & n_{2,2}^2 & 0 \\ n_{2,1}^1 & 0 & 0 & n_{2,2}^1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{18}$$

Table 2. η, or the number of local degrees of freedom bound, for the local equivalence classes of two-qubit gates.

$[c_1, c_2, c_3]$	Set in the Weyl chamber	η
$[0,0,0] \hat{=} [\pi,0,0]$	O, A_1	0
$[\pi/2, \pi/2, \pi/2]$	A_3	0
$[x,x,x], x \neq 0, x \neq \pi/2$	$OA_3 \setminus \{O, A_3\}$	3
$[\pi - x, x, x], x \neq 0, x \neq \pi/2$	$A_1A_3 \setminus \{A_1, A_3\}$	3
$[x,0,0] \hat{=} [\pi - x, 0, 0], x \neq 0$	$OA_1 \setminus \{O, A_1\}$	4
$[\pi/2, \pi/2, x], x \neq \pi/2$	$A_2A_3 \setminus \{A_3\}$	4
$[x,x,y], x \neq y, x \neq \pi/2$	$OA_1A_3 \setminus \{OA_3, A_1A_3\}$	5
$[x,y,y], x \neq y, x + y \neq \pi, y \neq 0$	$OA_2A_3 \setminus \{OA_3, A_2A_3\}$	5
$[\pi - x, x, y], x \neq y, x \neq \pi/2$	$A_1A_2A_3 \setminus \{A_1A_3, A_2A_3\}$	5
{All other points}	{All other points}	6

where the non-zero elements are

$$N^1 := \begin{pmatrix} n^1_{1,1} & n^1_{1,2} \\ n^1_{2,1} & n^1_{2,2} \end{pmatrix} = \begin{pmatrix} \sin c_2 \cos c_3 & -\cos c_2 \sin c_3 \\ -\cos c_2 \sin c_3 & \sin c_2 \cos c_3 \end{pmatrix},$$
$$N^2 := \begin{pmatrix} n^2_{1,1} & n^2_{1,2} \\ n^2_{2,1} & n^2_{2,2} \end{pmatrix} = \begin{pmatrix} -\sin c_1 \cos c_3 & \cos c_1 \sin c_3 \\ \cos c_1 \sin c_3 & -\sin c_1 \cos c_3 \end{pmatrix},$$
$$N^3 := \begin{pmatrix} n^3_{1,1} & n^3_{1,2} \\ n^3_{2,1} & n^3_{2,2} \end{pmatrix} = \begin{pmatrix} \sin c_1 \cos c_2 & -\cos c_1 \sin c_2 \\ -\cos c_1 \sin c_2 & \sin c_1 \cos c_2 \end{pmatrix}. \tag{19}$$

From Eqs. (18)–(19) it is seen that Eq. (13) decomposes into six separate equations:

$$N^i \begin{pmatrix} a_i \\ a_{i+3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad i = 1, 2, 3. \tag{20}$$

Each block N^i produces a two-dimensional null space iff all the elements of N^i equal zero, and a one-dimensional null space iff $\det N^i = (-1)^{i+1} \sin(c_j + c_k) \sin(c_j - c_k) = 0$, where $\epsilon_{ijk} = 1$, but $N^i \neq 0$.

In the two-qubit case we have $\eta = 6 - \dim(\ker W_{NL})$. The results for all the possible values of $[c_1, c_2, c_3]$ are collected in Table 2. One notices that everywhere inside the Weyl chamber η reaches its maximum value of 6. At the vertices $O = A_1$ and A_3 $\eta = 0$, on the edges between them $\eta = 3$, on the edges OA_1, A_2A_3 $\eta = 4$ and on the faces $OA_1A_3, OA_2A_3, A_1A_2A_3$ $\eta = 5$.

The number of local degrees of freedom that the gate U leaks is obtained as the number of pairs of equal eigenvalues λ_i in the spectrum of the matrix $M(U)$, presented in Eq. (3). In other words, any n-fold eigenvalue of $M(U)$ indicates $n(n-1)/2$ local degrees of freedom that pass through the gate U. Translated to the language of the Weyl chamber, each Weyl symmetry plane the point $[c_1, c_2, c_3]$ touches causes the gate to leak one local degree of freedom.

5 Conclusion

In this paper we have introduced a local invariant η for quantum gates, indicating the number of local degrees of freedom a gate can bind. Furthermore, we have analytically calculated the

value of this invariant for all two-qubit gates. We have found that almost all two-qubit gates can bind the full six local degrees of freedom. However, most of the commonly occurring gates such as CNOT or $\sqrt{\text{SWAP}}$ are exceptions to the rule, performing worse in this sense.

The meaning of η is illustrated by considering the lower bounds on gate counts for a generic n-qubit circuit. Let the gate library consist of all one-qubit gates and a fixed two-qubit gate U. Then almost all n-qubit gates cannot be accurately simulated with a circuit consisting of fewer than

$$N_U = \left\lceil \frac{4^n - 3n - 1}{\eta(U)} \right\rceil \tag{21}$$

applications of the two-qubit gate. This result is a straightforward generalization of Proposition III.1 in Ref. [4]. The most efficient building blocks for multiqubit gates are thus expected to belong to the set of gates binding the full six degrees of freedom. Hence, using CNOT as the entangling two-qubit gate in generic n-qubit circuit decompositions is probably not the optimal choice. For example, the B gate, lying at the point of high symmetry in the Weyl chamber, seems a good candidate instead.

Acknowledgements

This research is supported by the Academy of Finland (project No. 206457). VB thanks the Finnish Cultural Foundation for financial support.

In memoriam Prof. Martti M. Salomaa (1949-2004).

References

1. M.A. Nielsen and I.L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press (Cambridge).
2. D. Deutsch, A. Barenco and A. Ekert (1995), *Universality in Quantum Computation*, Proc. R. Soc. London A, 449, pp. 669-677, quant-ph/9505018.
3. S. Lloyd (1995), *Almost Any Quantum Logic Gate Is Universal*, Phys. Rev. Lett., 75, pp. 346-349.
4. V.V. Shende, I.L. Markov and S.S. Bullock (2004), *Minimal Universal Two-qubit Quantum Circuits*, Phys. Rev. A, 69, 062321, quant-ph/0308033.
5. J. Zhang, J. Vala, S. Sastry and K.B. Whaley (2004), *Optimal quantum circuit synthesis from controlled-U gates*, Phys. Rev. A, 69, 042309, quant-ph/0308167.
6. M.-Y. Ye, G.-C. Guo and Y.-S. Zhang (2004), *Super controlled gates and controlled gates in two-qubit gate simulations*, quant-ph/0407108.
7. J. Zhang, J. Vala, S. Sastry and K.B. Whaley (2004), *Minimum construction of two-qubit quantum operations*, Phys. Rev. Lett., 93, 020502, quant-ph/0312193.
8. Y.-S. Zhang, M.-Y. Ye and G.-C. Guo (2004), *Conditions for optimal construction of two-qubit non-local gates*, quant-ph/0411058.
9. V.V. Shende, S.S. Bullock and I.L. Markov (2004), *Practical Top-down Approach to Quantum Circuit Synthesis*, quant-ph/0406176.
10. V. Bergholm, J.J. Vartiainen, M. Möttönen and M.M. Salomaa (2004), *Quantum circuits with uniformly controlled one-qubit gates*, quant-ph/0410066.
11. S. Helgason (1978), *Differential geometry, Lie groups, and symmetric spaces*, Academic Press (New York).
12. N. Khaneja, R. Brockett and S.J. Glaser (2001), *Time Optimal Control in Spin Systems*, Phys. Rev. A, 63, 032308, quant-ph/0006114.

13. J. Zhang, J. Vala, S. Sastry and K.B. Whaley (2003), *Geometric theory of nonlocal two-qubit operations*, Phys. Rev. A, 67, 042313.
14. Yu. Makhlin (2002), *Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations*, Quantum Inf. Process., 1, pp. 243-252, quant-ph/0002045.
15. A.M. Childs, H.L. Haselgrove and M.A. Nielsen (2003), *Lower bounds on the complexity of simulating quantum gates*, Phys. Rev. A, 68, 052311, quant-ph/0307190.
16. A.T. Rezakhani (2004), *Characterization of two-qubit perfect entanglers*, Phys. Rev. A, 70, 052313, quant-ph/0405046.
17. S.S. Bullock and I.L. Markov (2003), *Arbitrary two-qubit computation in 23 elementary gates* Phys. Rev. A, 68, 0123318.
18. G. Vidal and C.M. Dawson (2004), *Universal quantum circuit for two-qubit transformations with three controlled-NOT gates*, Phys. Rev. A, 69, 010301.
19. F. Vatan and C.P. Williams (2004), *Optimal quantum circuits for general two-qubit gates*, Phys. Rev. A, 69, 032315, quant-ph/0308006.