Clifford algebras and universal sets of quantum gates

Alexander Yu. Vlasov*
Federal Radiological Center (IRH), 197101, Mira Street 8, St. Petersburg, Russia
(Received 20 October 2000; published 17 April 2001)

In this paper is shown an application of Clifford algebras to the construction of computationally universal sets of quantum gates for n-qubit systems. It is based on the well-known application of Lie algebras together with the especially simple commutation law for Clifford algebras, which states that all basic elements either commute or anticommute.

DOI: 10.1103/PhysRevA.63.054302 PACS number(s): 03.67.Lx, 03.65.Fd, 02.20.Sv

I. INTRODUCTION

In this paper is discussed an algebraic approach to the construction of computationally universal sets of quantum gates. A quantum gate U for a system of n qubits is a unitary $2^n \times 2^n$ matrix. It is possible to write $U = e^{iH}$, where H is the Hermitian $2^n \times 2^n$ matrix.

A set of quantum gates U_k is *(computationally) universal* if any unitary matrix can be obtained with given precision as a product of matrices U_k. Algebraic conditions of universality can be described using the Lie algebra $\mathfrak{u}$ of the Lie group of unitary matrices [1,2]: if there is a set of Hermitian matrices H_k and if it is possible to generate a basis of space of all Hermitian $2^n \times 2^n$ matrices using only the commutators $i[H,G] \equiv i(HG - GH)$, then $U_k = \exp(i\tau H_k)$ are a universal set of quantum gates if τ is small enough.

In this paper is presented an alternative approach to the construction of a universal set of gates using both Lie and Clifford algebras. It is possible because the algebra $\mathbb{C}(2^n \times 2^n)$ of all $2^n \times 2^n$ complex matrices is the complex Clifford algebra with $2n$ generators, i.e., there are $2n$ matrices Γ_k with the property $\{\Gamma_k, \Gamma_l\} \equiv \Gamma_k \Gamma_l + \Gamma_l \Gamma_k = 2\delta_{kl}\mathbb{1}$ (where $\mathbb{1}$ is unit matrix) and 2^{2n} different *products* of Γ_k generate a basis of $\mathbb{C}(2^n \times 2^n)$ [3,4].

The $2n$ matrices Γ_k are not enough for proof of universality, because we may not use arbitrary *products* of Γ_k, but only *commutators*. In this paper it is shown that by using commutators of Γ_k, it is possible to generate only the $(2n^2 + n)$-dimensional subspace, but it is enough to add only one element Γ_u and the new set is universal, i.e., it generates a full 4^n-dimensional space $\mathfrak{u}(2^n)$.

All $2n$ matrices Γ_k may be chosen to be Hermitian and the full complex algebra was used for simplification. The extra Hermitian matrix is $\Gamma_u = i\Gamma_{123} \equiv i\Gamma_1\Gamma_2\Gamma_3$ or Γ_{1234}, or any such product of three or four different Γ_k.

A constructive proof of universality using the language of the Clifford algebras is based on a simple commutation law of 4^n basic elements: they either commute or anticommute, because any such element is a product of up to $2n$ Γ_k. Direct construction of any $2^n \times 2^n$ matrix $\Gamma_I \equiv \Pi_{k \in I}\Gamma_k$ of the Clifford basis by commutators of $2n+1$ initial elements is shown below in Sec. II D, theorem 1.

The question about universality is widely investigated [1,2,5–9], but the method discussed in the present work has some special properties. Construction of a universal set of gates uses *only* infinitesimal and continuous symmetries of group $\mathrm{U}(2^n)$ and does not require such discrete operations as permutations of qubits or basic vectors related to the "classical limit of quantum circuits." The properties of discrete, binary transformations of qubits simply emerge here from the structure of infinitesimal transformations of Hilbert space, i.e., directly from Hamiltonians, cf. [1,9].

II. CLIFFORD ALGEBRAS

A. General definitions

For n-dimensional vector space with a quadratic form (metric) $g(\vec{x})$, the Clifford algebra $\mathfrak{A}$ is a formal way to represent a square root of $-g(\vec{x})$ [3,4] or, more formally, $-g(\vec{x})\mathbb{1}$, where $\mathbb{1}$ is the unit of algebra $\mathfrak{A}$. The vector space corresponds to the n-dimensional subspace $\mathcal{V}$ of $\mathfrak{A}$: $\vec{x} \mapsto \mathbf{x} \equiv \sum_{l=0}^{n-1} x_l \mathfrak{e}_l$, where $\mathbf{x}$, $\mathfrak{e}_l \in \mathcal{V} \subset \mathfrak{A}$. From $\mathbf{x}^2 = -g(\vec{x})$, i.e., $(\sum_{l=0}^{n-1} x_l \mathfrak{e}_l)^2 = \sum_{i,j=0}^{n-1} g_{ij} x_i x_j$, follow the main properties of the generators $\mathfrak{e}_l$ of the Clifford algebra:

$$\{\mathfrak{e}_i, \mathfrak{e}_j\} \equiv \mathfrak{e}_i \mathfrak{e}_j + \mathfrak{e}_j \mathfrak{e}_i = -2g_{ij}. \tag{2.1}$$

Let g_{ij} be diagonal and $g_{ii} = \pm 1$ (the case $g_{ii} = 0$ is not considered here, but see [3]). Then,

$$\mathfrak{e}_i \mathfrak{e}_j = -\mathfrak{e}_j \mathfrak{e}_i \quad (i \neq j), \tag{2.2a}$$

$$\mathfrak{e}_i^2 = \pm 1. \tag{2.2b}$$

It is clearer from Eq. (2.2) that it is possible to generate no more than 2^n different products of up to n $\mathfrak{e}_i$. A linear span of all the products is a full algebra $\mathfrak{A}$ [4]. Let us use the notations $\mathfrak{e}_I = \mathfrak{e}_{i_1 i_2 \cdots i_k} \equiv \mathfrak{e}_{i_1}\mathfrak{e}_{i_2} \cdots \mathfrak{e}_{i_k}$, where k is the number of multipliers or *the order* of $\mathfrak{e}_I$, $k = \mathcal{N}(I)$.

If there are no algebraic relations other than Eq. (2.2), then the algebra has a maximal dimension 2^n and is called the *universal* Clifford algebra, $\mathfrak{Cl}(g)$, because for any other Clifford algebra $\mathfrak{A}$ with the same metric $g(\vec{x})$ there is a homomorphism $\mathfrak{Cl}(g) \to \mathfrak{A}$ (see Ref. [4]).

Let us use the notation $\mathfrak{Cl}(l,m)$ for the diagonal metric Eq. (2.2) with l pluses and m minuses in Eq. (2.2b), i.e., for

*Email address: qubeat@mail.ru, alex@protection.spb.su

pseudo-Euclidean (Minkowski) space $\mathbb{R}^{l,m}$. There is a special notation for Euclidean space: $\mathfrak{Cl}(n) \equiv \mathfrak{Cl}(n,0)$ and $\mathfrak{Cl}_+(n) \equiv \mathfrak{Cl}(0,n)$.

Complexification of any Clifford algebra $\mathfrak{Cl}(l,m)$ with $l+m=n$ is the same complex algebra $\mathfrak{Cl}(n,\mathbb{C})$, because all signs in Eq. (2.2b) may be ''adjusted'' by the substitution $\mathfrak{e}_k \to i\mathfrak{e}_k$.

Let us denote $\mathfrak{e}_I^\sigma \equiv \sqrt{\mathfrak{e}_I^2}\mathfrak{e}_I$, i.e., if $\mathfrak{e}_I^2=1$, then $\mathfrak{e}_I^\sigma=\mathfrak{e}_I$, but if $\mathfrak{e}_I^2=-1$, then $\mathfrak{e}_I^\sigma=i\mathfrak{e}_I$ and so always $(\mathfrak{e}_I^\sigma)^2=1$.

B. Matrix representations

All complex Clifford algebras in even dimension $\mathfrak{Cl}(2n,\mathbb{C})$ are isomorphic with a full algebra of $2^n \times 2^n$ complex matrices [3,4]. The simplest case $\mathfrak{Cl}(2,\mathbb{C})$ is the Pauli algebra. Matrices σ_x and σ_y can be chosen as generators $\mathfrak{e}_0$, $\mathfrak{e}_1$ and σ_z is $i\mathfrak{e}_0\mathfrak{e}_1=\mathfrak{e}_{01}^\sigma$.

The Pauli algebra is four-dimensional complex algebra and can also be considered as eight-dimensional real algebra, $\mathfrak{Cl}_+(3)$. Prevalent applications of Clifford algebras in the theory of NMR quantum computation [10,11] are based on a real representation $\mathfrak{Cl}_+(3)$ rather than on a complex one $\mathfrak{Cl}(2,\mathbb{C})$, discussed in the present work. These two approaches are very close, but may be different in some of the details.

There is simple recursive construction of the complex Clifford algebra with an even number of generators $\mathfrak{Cl}(2n,\mathbb{C})$ with $\mathfrak{Cl}(2,\mathbb{C})$. For $n=1$, it is the Pauli algebra, and if there is some algebra $\mathfrak{Cl}(2n,\mathbb{C})$ for $n \geqslant 1$, then

$$\mathfrak{Cl}(2n+2,\mathbb{C}) \cong \mathfrak{Cl}(2n,\mathbb{C}) \otimes \mathfrak{Cl}(2,\mathbb{C}). \tag{2.3}$$

The proof of Eq. (2.3) is as follows: if $\mathfrak{e}_0,\dots,\mathfrak{e}_{2n-1}$ are $2n$ generators of $\mathfrak{Cl}(2n,\mathbb{C})$, then $\mathbb{1}_{2n}\otimes\mathfrak{e}_0$ and $\mathbb{1}_{2n}\otimes\mathfrak{e}_1$ together with $2n$ elements $\mathfrak{e}_k\otimes\mathfrak{e}_{01}^\sigma$ are $2n+2$ generators of $\mathfrak{Cl}(2n+2,\mathbb{C})$.

Direct construction of $\mathfrak{Cl}(2n,\mathbb{C})$ is [3,4]

$$\Gamma_{2k} = \underbrace{\mathbb{1}\otimes\cdots\otimes\mathbb{1}}_{n-k-1}\otimes\sigma_x\otimes\underbrace{\sigma_z\otimes\cdots\otimes\sigma_z}_{k} \tag{2.4a}$$

$$\Gamma_{2k+1} = \underbrace{\mathbb{1}\otimes\cdots\otimes\mathbb{1}}_{n-k-1}\otimes\sigma_y\otimes\underbrace{\sigma_z\otimes\cdots\otimes\sigma_z}_{k} \tag{2.4b}$$

with $\mathfrak{e}_l \triangleq \Gamma_l$, $\mathfrak{e}_l^2=\mathbb{1}$, $\forall\, l\in 0,\dots,2n-1$. More generally, algebraic properties of elements $\mathfrak{e}_l$ used in the paper are the same for different matrix representations $\mathfrak{e}_l \triangleq M\Gamma_l M^{-1}$, where $M \in \mathrm{SU}(2^n)$.

C. Spin groups

Most known physical applications of Clifford algebras are due to *spin groups*. The group has 2:1 homorphism with an orthogonal (or pseudo-orthogonal) group and is related to the Dirac equation [4] and the transformation properties of wave functions in quantum mechanics.

Each element $\mathbf{x}\in\mathcal{V}$ (see the definition of $\mathcal{V}$ above in Sec. II A) has an inverse $\mathbf{x}^{-1}=-\mathbf{x}/g(\vec{x})$ if $g(\vec{x})\neq 0$. All possible products of an *even* number of such elements with $|g|=1$ is the *spin group*. It is $\mathrm{Spin}(n)$ for $\mathfrak{Cl}(n)$ and for $\mathfrak{Cl}_+(n)$. The group has 2:1 homorphism with $\mathrm{SO}(n)$. For $s\in\mathrm{Spin}(n)$, an element of $\mathrm{SO}(n)$ is represented as $r_s:\mathbf{x}\mapsto s\mathbf{x}s^{-1}$ [4].

Because only products of an even number of elements of $\mathfrak{Cl}(n)$ are used in the definition of $\mathrm{Spin}(n)$, the group is a subset of even subalgebra $\mathfrak{Cl}^e(n)\subset\mathfrak{Cl}(n)$. In the Euclidean case, $\mathfrak{Cl}^e(n)$ is isomorphic with $\mathfrak{Cl}(n-1)$ and the property $\mathrm{Spin}(n+1)$ is defined as a subset of $\mathfrak{Cl}(n)$.

Construction of the $\mathrm{Spin}(n+1)$ group from $\mathfrak{Cl}(n)$ is sometimes called the *Spoin group* [4], $\mathrm{Spoin}(n)\cong\mathrm{Spin}(n+1)$.

Let us consider $(n+1)$-dimensional space $\lambda\mathbb{1}\oplus\mathcal{V}$, i.e., combinations $\mathbf{y}=\lambda+\mathbf{x}$, $\mathbf{x}\in\mathcal{V}$. Let $\Delta(\mathbf{y})\equiv\lambda^2+g(\vec{x})$. The elements have an inverse $(\lambda+\mathbf{x})^{-1}=(\lambda-\mathbf{x})/\Delta(\mathbf{y})$ if $\Delta(\mathbf{y})\neq 0$. Products of *any* number of such elements with $|\Delta|=1$ is the $\mathrm{Spoin}(n)$ group [4].

The group $\mathrm{Spoin}(n)$ is 2:1 homorphic with $\mathrm{SO}(n+1)$. For $s\in\mathrm{Spoin}(n)$, an element of $\mathrm{SO}(n+1)$ is represented as $r_s:\mathbf{y}\mapsto s\mathbf{y}(s')^{-1}$, where $\mathbf{y}=y_n+\Sigma_{l=0}^{n-1}y_l\mathfrak{e}_l$ and $(')$ is the algebra automorphism defined with basis elements as $\mathfrak{e}_I'=(-1)^{\mathcal{N}(I)}\mathfrak{e}_I$ [4].

D. Lie algebras and Clifford algebras

Clifford algebra is Lie algebra with respect to a bracket operation $[a,b]\equiv ab-ba$ [4]. Here we prove a result that is necessary for the construction of a universal set of gates.

Theorem 1. Let $\mathfrak{Cl}(n,\mathbb{C})$ be the Clifford algebra and n be even. There are enough n generators $\mathfrak{e}_k$, $k=0,\dots,n-1$ and any element $\mathfrak{e}_I$ with $\mathcal{N}(I)=3$ or $\mathcal{N}(I)=4$ to generate elements of any order only using commutators of these $n+1$ elements.

A proof of this result has several steps.

(i) If there are n elements $\mathfrak{e}_0,\dots,\mathfrak{e}_{n-1}$, it is possible by using commutators to generate also all elements of second order, i.e., $[\mathfrak{e}_i,\mathfrak{e}_j]=2\mathfrak{e}_i\mathfrak{e}_j\equiv 2\mathfrak{e}_{ij}$.

(ii) If there are all elements of second order and an element of third order, for example $\mathfrak{e}_{012}$, it is possible to generate any element of third order, i.e., $2\mathfrak{e}_{01m}=[\mathfrak{e}_{012},\mathfrak{e}_{2m}]$, $2\mathfrak{e}_{0nm}=[\mathfrak{e}_{01m},\mathfrak{e}_{1n}]$, $2\mathfrak{e}_{pnm}=[\mathfrak{e}_{0nm},\mathfrak{e}_{0p}]$.

(iii) Analogously, if there is any element of order $2k+1$, it is possible to generate any element of the same order using no more than $2k+1$ commutators with elements $\mathfrak{e}_{ij}$.

(iv) If we have all elements of third order, it is possible to generate any element of fourth order, $2\mathfrak{e}_{ijkl}=[\mathfrak{e}_{ijk},\mathfrak{e}_l]$.

(v) Analogously, if we have all elements with the order $\mathcal{N}(I)=2k+1$, it is possible to generate any element of order $2k+2$, $2\mathfrak{e}_{I\cup l}=[\mathfrak{e}_I,\mathfrak{e}_l]$, where $l\notin I$.

(vi) If we have an element of fourth order, it is possible to generate some element of third order, $2\mathfrak{e}_{ijk}=[\mathfrak{e}_{ijkl},\mathfrak{e}_l]$ (and so any element of third and fourth order).

(vii) Analogously, if we have an element of order $2k+2$, it is possible to generate some element of order $2k+1$ [and so any element with the order $2k+1$ or $2k+2$, as in the steps (iii) and (v)].

(viii) We have all elements with order less than or equal to $2k$, $k\geqslant 2$ due to steps (i), (ii), and (iv) and we can prove the theorem by recursion: by using a commutator of an element with order $2k-1$ and an element with order 3, it is possible to generate an element of order $2k+2$ and so any elements of order $2k+1$ or $2k+2$, as in the step (vii).

Note 1. Instead of elements $\mathfrak{e}_0,\ldots,\mathfrak{e}_{n-1}$, it is possible to use $\mathfrak{e}_0$ together with $n-1$ elements $\mathfrak{e}_{l-1,l}$: $[\mathfrak{e}_0,\mathfrak{e}_{01}]=2\mathfrak{e}_1,\ldots,[\mathfrak{e}_{l-1},\mathfrak{e}_{l-1,l}]=2\mathfrak{e}_l$.

Note 2. If n is odd, it is impossible to generate only an element with the order n, because due to step (vii) of recursion it would be generated only from an even element with the order $n+1$, but there are no such elements. So in this case we need $n+2$ elements, the extra one being $\mathfrak{e}_{0,\ldots,n-1}$.

Note 3. If we use only n generators $\mathfrak{e}_i$, then together with $n(n-1)/2$ commutators $[\mathfrak{e}_k,\mathfrak{e}_j]=2\mathfrak{e}_{kj}$, $k\neq j$, it is possible to generate $n+n(n-1)/2=n(n+1)/2$ elements, because, as may be checked directly, any new commutators may not generate an element with order more than 2. It is the Lie algebra of the spoin(n) group, because products of $\exp(\epsilon\mathfrak{e}_k)\approx\mathbb{1}+\epsilon\mathfrak{e}_k$ belong to that group and the dimension of the group is the same, $\dim\mathrm{Spoin}(n)=\dim\mathrm{SO}(n+1)=n(n+1)/2$. Despite the fact that only elements $\mathfrak{e}_I$, $\mathcal{N}(I)\leqslant 2$ belong to the *Lie algebra*, all 4^n elements $\mathfrak{e}_I$, $\mathcal{N}(I)\leqslant n$ of $\mathfrak{Cl}(n)$ belong to the *Lie group* Spoin(n) by definition and so a linear span of these elements is the full Clifford algebra.

Note 4. The theorem was proved rather for the more general case of the Lie algebra of the complex Lie group $\mathrm{GL}(N,\mathbb{C})$, $N=2^{n/2}$ of all matrices M, $\det(M)\neq 0$, than for the unitary group $\mathrm{U}(N)\subset\mathrm{GL}(N,\mathbb{C})$. The proof for the Lie algebra $\mathfrak{u}(N)$ of the unitary group $\mathrm{U}(N)$ is directly implied. It is sufficient to choose the initial matrices in $\mathfrak{u}(N)$ for a given representation, after which the Lie brackets may produce only matrices in $\mathfrak{u}(N)$ for each step of the proof.

It should be mentioned that there are two traditions for representations of $\mathfrak{u}(N)$. In physical applications, Hermitian matrices H are used, the Lie brackets are $i[a,b]$, and the unitary matrices are represented as $U=\exp(-i\tau H)$ due to relations with Hamiltonians and a quantum version of Poisson brackets [12]. In Eq. (2.4), elements $\mathfrak{e}_l=\Gamma_l$, $i\mathfrak{e}_{012}$, and $\mathfrak{e}_{0123}$ (and $i\mathfrak{e}_{kl}$, see *Note 1*), i.e., all $\mathfrak{e}_I^\sigma$, are Hermitian. In more general mathematical applications, $\mathfrak{u}(N)$ are skew-Hermitian matrices $A^\dagger=-A$ and "i" multipliers are not present in the expressions for the commutators and the exponents [4], because $A\triangleq iH$.

III. APPLICATION TO QUANTUM GATES

A. Universal set of quantum gates

Now let us discuss the construction of universal gates more directly. Instead of Lie algebra $\mathfrak{u}(2^n)$, we should work with Lie group $\mathrm{U}(2^n)$. Then an element $\mathfrak{e}_I^\sigma$ corresponds to a unitary gate $U_I^\tau\equiv\exp(i\tau\mathfrak{e}_I^\sigma)$. One of the advantages of elements $\mathfrak{e}_I^\sigma$ is the analytical expression for the exponent:

$$U_I^\tau=e^{i\tau\mathfrak{e}_I^\sigma}=\cos(\tau)+i\sin(\tau)\mathfrak{e}_I^\sigma. \tag{3.1}$$

Equation (3.1) is valid for any operator with the property $\mathfrak{e}^2=\mathbb{1}$ and it is true for all 4^n basis elements $\mathfrak{e}_I^\sigma$.

It is also possible due to Eq. (3.1) to combine the approach with *infinitesimal* parameters τ [1,2] and an approach with *irrational* parameters [5,6]. The smaller τ is, the higher is the precision in the generation of arbitrary unitary gates in [1,2]. Due to Eq. (3.1), accuracy may be arbitrarily high if we use gates $U_I=e^{i\varpi\mathfrak{e}_I^\sigma}$ with irrational ϖ/π because for any τ there exists the natural number N and $\varepsilon<\tau$: $U_I^\varepsilon=(U_I)^N$. It should be mentioned that the unitary gates do not necessarily have irrational coefficients even if ϖ/π is irrational, for example $U_I=0.8+0.6\mathfrak{e}_I^\sigma$.

Yet another advantage of the elements $\mathfrak{e}_I^\sigma$ is a simpler expression for "commutator gate." In the usual case [1,2], it is generated as

$$e^{i\tau i[H_k,H_l]}\approx e^{i\sqrt{\tau}H_k}e^{i\sqrt{\tau}H_l}e^{i\sqrt{\tau}H_k}e^{-i\sqrt{\tau}H_l},$$

and the expression has precision $O(\tau^{1.5})$. For elements $\mathfrak{e}_I^\sigma$, there is an exact construction. If $H_I=\mathfrak{e}_I^\sigma$ and $H_J=\mathfrak{e}_J^\sigma$, then either $[H_I,H_J]=0$ or $[H_I,H_J]=2H_IH_J$. The first case is trivial and for the second case due to Eq. (3.1),

$$e^{i\tau i[H_I,H_J]/2}=e^{-\tau H_IH_J}=e^{i(\pi/2)H_I}e^{i\tau H_J}e^{-i(\pi/2)H_I}.$$

After construction of the basis of Hermitian matrices $H_I=\mathfrak{e}_I^\sigma$, it is possible to use an expression

$$e^{\Sigma_I\alpha_IH_I}=(e^{(1/N)\Sigma_I\alpha_IH_I})^N\approx\left(\prod e^{(1/N)\alpha_IH_I}\right)^N$$

$$\equiv\left(\prod U_I^{\alpha_I/N}\right)^N.$$

The expression has accuracy $O(\Sigma\alpha_I^2/N)$.

The approach to a universal set of gates U is more convenient and constructive if we know the Hermitian matrix H, $U^\tau=e^{i\tau H}$. It is not a principal limitation, because for physical realizations we should know the Hamiltonian to construct the gates. It is also related to the universal quantum simulation [9] in which H is the Hamiltonian and τ is a real continuous parameter, the time of "application."

The description with an exponent may be even more complete, because by using H it is possible to find a unique $U=\exp(iH)$, but by using U it is not always possible to restore H because there are many H's for the same U. A simple example is $U=i\sigma_\alpha\otimes\sigma_\beta$ with two arbitrary two Pauli matrices: $U=e^{i\pi(\sigma_\alpha\otimes 1+1\otimes\sigma_\beta)}=e^{i\pi\sigma_\alpha\otimes\sigma_\beta}$.

B. Two-qubit quantum gates

Let us show how to build a universal set of one- and two-qubit gates using Eq. (2.4). For example, it may be $2n+1$ gates $\exp(i\tau\mathfrak{e}_I)$, where $\mathfrak{e}_I$ are $\mathfrak{e}_0$, $i\mathfrak{e}_{l-1,l}$ with $l=1,\ldots,2n-1$, and $i\mathfrak{e}_{012}$:

$$\mathfrak{e}_0=\mathbb{1}^{\otimes(n-1)}\otimes\sigma_x, \tag{3.2a}$$

$$\frac{1}{i}\mathfrak{e}_{2k,2k+1}=\mathbb{1}^{\otimes(n-k-1)}\otimes\sigma_z\otimes\mathbb{1}^{\otimes k}, \tag{3.2b}$$

$$\frac{1}{i}\mathfrak{e}_{2k+1,2k+2}=\mathbb{1}^{\otimes(n-k-2)}\otimes\sigma_x\otimes\sigma_x\otimes\mathbb{1}^{\otimes k}, \tag{3.2c}$$

$$\frac{1}{i}\mathfrak{e}_{012}=\mathbb{1}^{\otimes(n-2)}\otimes\sigma_x\otimes\mathbb{1} \tag{3.2d}$$

with $k=0,\ldots,n-1$ or $n-2$. The elements were discussed in *Note 1*, and it was shown that they generate the full Lie algebra $\mathfrak{u}(2^n)$.

C. Nonuniversal set of quantum gates

In [2], an interesting question was raised, asking which sets of gates are *not* universal (and why).

Products of gates $U_k^\tau=e^{i\tau\mathfrak{e}_k}=\cos(\tau)+i\mathfrak{e}_k\sin(\tau)$ generate a group $\mathrm{Spin}(2n+1)\cong\mathrm{Spoin}(2n)\subset U(2^n)$ due to *Note 3*. It is an interesting example of nonuniversality when only one extra gate like $e^{i\tau\overset{\sigma}{\mathfrak{e}}_{012}}$ may produce a universal set with ''an exponential improvement'' from a subgroup $\dim\mathrm{Spoin}(2n)=n(2n+1)$ to a full group $\dim\mathrm{U}(2^n)=2^{2n}$.

This result is more important if the extra gate $e^{i\tau\overset{\sigma}{\mathfrak{e}}_I}$ with $\mathcal{N}(I)=3$ or $\mathcal{N}(I)=4$ has a different physical nature from the gates with $\mathcal{N}(I)=1$ and $\mathcal{N}(I)=2$. It is not clear from Eq. (3.2) why the extra gate Eq. (3.2d) is simply one gate. But this is not so for physical systems with *natural* Clifford and spin structure.

A possible reason is the Schrödinger equation for n particles without interaction [13]: $i\hbar(\partial\psi/\partial t)=\frac{1}{2}\hbar^2\Sigma_{a=1}^n(\Delta_a/m_a)\psi$, or using $m_a=m$ and the Laplacian Δ_N with $N=\nu n$ variables, it is possible to write for stationary solutions with total energy E,

$$(\Delta_N+\lambda^2)\psi(x_0,\ldots,x_{N-1})=0, \tag{3.3}$$

where $\lambda\equiv\sqrt{2mE}/\hbar$. Let the dimension of one particle motion be $\nu=2$ for simplicity, $N=2n$.

Let us consider a full basis $\phi_{\mathbf{p}}(\mathbf{x})\equiv e^{i(\mathbf{p},\mathbf{x})}$ on Hilbert space $\mathcal{L}$ of wave functions $\psi\in\mathcal{L}$. Here $\mathbf{p},\mathbf{x}\in\mathbb{R}^N$ and $(\mathbf{p},\mathbf{x})$ is the scalar product. The plane waves $\phi_{\mathbf{p}}$ correspond to n particles with definite momenta. If $O\in\mathrm{SO}(N)$, then a transformation defined on the basis as $\Sigma_O:\phi_{\mathbf{p}}\to\phi_{O\mathbf{p}}$ is a *symmetry* of Eq. (3.3). It is an analog of the classical transition between two configurations *with the same total kinetic energy* in ''billiard balls'' conservative logic [14].

The general Dirac operator [4] is the first-order differential operator $\mathfrak{D}_N=\Sigma_{i=0}^{N-1}i\mathfrak{e}_k(\partial/\partial x_k)$ with a property $\mathfrak{D}_N^2=-\Delta_N$. If to use the Dirac operator for factorization of Eq. (3.3),

$$(\mathfrak{D}_N-\lambda)(\mathfrak{D}_N+\lambda)\mathbf{\Psi}(x_0,\ldots,x_{N-1})=0, \tag{3.4}$$

then each component of $\mathbf{\Psi}$ is a solution of Eq. (3.3) and the action of the Spin(N) group on $\mathbf{\Psi}$ corresponds [4] to SO(N) symmetry Σ_O described above and it has some analog in the classical physics of billiard balls. A Spoin(N) group is represented less directly, but it can be considered as a symmetry between two stationary solutions with *different* total energies.

The example above shows that it is possible to find some classical correspondence for elements $\mathfrak{e}_I$, $\mathcal{N}(I)=2$ of the Spin group and maybe for generators $\mathcal{N}(I)=1$ of the Spoin group, but the special element with $\mathcal{N}(I)=3$ does not have some allusion with classical physics.

[1] D.P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[2] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[3] A.Yu. Vlasov, e-print quant-ph/9907079 (1999).
[4] J.E. Gilbert and M.A.M. Murray, *Clifford Algebras and Dirac Operators in Harmonic Analysis* (Cambridge University Press, Cambridge, England, 1991).
[5] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
[6] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[7] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[8] R. Cleve, e-print quant-ph/9906111 (1999).
[9] S. Lloyd, Science **273**, 1073 (1996).
[10] S.S. Somaroo, D.G. Cory, and T.F. Havel, Phys. Lett. A **240**, 1 (1998).
[11] T.F. Havel and C.J.L. Doran, e-print quant-ph/0004031 (2000).
[12] P.A.M. Dirac, *The Principles of Quantum Mechanics* (Clarendon Press, Oxford, 1958).
[13] L. D. Landau and E. M. Lifshitz, *Course of Theoretical Physics* (Nauka, Moscow, 1989), Vol. III.
[14] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. **21**, 219 (1982).