Clifford groups of quantum gates, BN-pairs and smooth cubic surfaces

2009 J. Phys. A: Math. Theor. 42 042003

(http://iopscience.iop.org/1751-8121/42/4/042003)

IOP PUBLISHING
JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **42** (2009) 042003 (6pp)
doi:10.1088/1751-8113/42/4/042003

FAST TRACK COMMUNICATION

Clifford groups of quantum gates, BN-pairs and smooth cubic surfaces

Michel Planat[1] **and Patrick Solé**[2]

[1] Institut FEMTO-ST, CNRS, 32 Avenue de l'Observatoire, F-25044 Besançon, France
[2] CNRS I3S, Les Algorithmes, Euclide B, 2000 route des Lucioles, BP 121, 06903 Sophia Antipolis, France

Received 19 November 2008, in final form 3 December 2008
Published 19 December 2008
Online at stacks.iop.org/JPhysA/42/042003

Abstract

The recent proposal (Planat and Kibler 2008 arXiv:0807.3650 [quant-ph]) of representing Clifford quantum gates in terms of unitary reflections is revisited. In this communication, the geometry of a Clifford group G is expressed as a BN-pair, i.e. a pair of subgroups B and N that generate G, is such that intersection $H = B \cap N$ is normal in G, the group $W = N/H$ is a Coxeter group and two extra axioms are satisfied by the double cosets acting on B. The BN-pair used in this decomposition relies on the *swap* and *match* gates already introduced for classically simulating quantum circuits (Jozsa and Miyake 2008 arXiv:0804.4050 [quant-ph]). The two- and three-qubit cases are related to the configuration with 27 lines on a smooth cubic surface.

PACS numbers: 03.67.Pp, 03.67.Lx, 02.20.−a, 03.65.Vf, 02.40.Dr

1. Introduction

Euclidean real reflection groups (Coxeter groups) are an important ingredient for representing quantum computations [1]. Coxeter groups are finite sets of involutions and specific pairwise relations. As a result, they provide a distinguished class of quantum Boolean functions [2] possessing inherent crystallographic properties. But complex reflections are more appropriate for modeling the Clifford unitaries. For instance, the single qubit Pauli group $\mathcal{P}_1$ (generated by the ordinary Pauli spin matrices σ_x, σ_y and σ_z) is the imprimitive reflection group $G(4, 2, 2)$. Its normalizer in the unitary group $U(2)$, the so-called Clifford group $\mathcal{C}_1$, is isomorphic (but is not the same as) to the reflection group number 9 in the Shephard–Todd list [3]. The n-qubit Clifford group $\mathcal{C}_n$ is the normalizer in $U(2^n)$ of the tensor product of n Pauli spin matrices [4]. It originally appeared in the context of doubly-even self-dual classical codes [5], where it was discovered that the space of homogeneous invariants of $\mathcal{C}_n$ is spanned by the complex weight enumerators of the codes. Group $\mathcal{C}_2$ contains a maximal subgroup (of half its size) which is the Shephard–Todd group number 31, but the connection to unitary reflection groups becomes more tenuous as far as $n \geqslant 3$.

In this communication, we show that Clifford groups may be seen as aggregates of Coxeter groups with the structure of BN-pairs, also named Tits systems. There is a compelling physical connection of the BN-pair decomposition to *swap* and *match* gates introduced in the context of classical simulations of quantum circuits [13]. The B group relies on the *swap* gates and the local component of the n-qubit Clifford group $\mathcal{C}_n$, while the N group relies on the *match* gates and the topological component of $\mathcal{C}_n$. It is also noticeable that such a construction also vindicates a connection of the Clifford group geometry to smooth cubic surfaces, already pointed out in our earlier work [1].

2. BN-pairs

Henceforth, G is a finite group, B and N two subgroups of G generating G, $H = B \cap N$ is a normal subgroup of G and the quotient group $W = N/H$ is generated by a set $S \subset W$ of order 2 elements (involutions). In the following section, we shall observe that such a pairing easily follows from the structure of the Clifford group $G \equiv \mathcal{C}_n$, when it is divided into its *local* component, the local Clifford group $B \equiv \mathcal{C}_n^L$, and its *topological* component $N \equiv \mathcal{B}_n$.

In 1962, Tits coined the concept of a BN-*pair* for characterizing groups resembling the general linear group over a field [6–8]. A group G is said to have a BN-pair iff it is generated as above and two extra relations (i) and (ii) are satisfied by the double cosets[1]

(i) For any $s \in S$ and $w \in W$, $sBw \subseteq (BwB) \cup (BswB)$,

(ii) For any $s \in S$, $sBs \nsubseteq B$.

A particular example is $G = GL_n(K)$ (the general linear group over a field K). One takes B to be the upper triangular matrices, H to be the diagonal matrices and N to be the matrices with exactly one non-zero element in each row and column. There are $n - 1$ generators s, represented by the matrices obtained by swapping two adjacent rows of a diagonal matrix. More generally, any group of Lie type has the structure of a BN-pair, and BN-pairs can be used to prove that most groups of Lie type are simple.

An important consequence of axioms (i) and (ii) is that the group G with a BN-pair may be partitioned into the double cosets as $G = BWB$. The mapping from w to $C(w) = BwB$ is a bijection from W to the set $B\backslash G/B$ of double cosets of G along B [7].

Let us recall that a group W is a *Coxeter group* if it is finitely generated by a subset $S \subset W$ of involutions and pairwise relations

$$W = \langle s \in S | (ss')^{m_{ss'}} = 1\rangle,$$

where $m_{ss} = 1$ and $m_{ss'} \in \{2, 3, \ldots\} \cup \{\infty\}$ if $s \neq s'$. The pair (W, S) is a Coxeter system of rank $|S|$ equal to the number of generators.

The pair (W, S) arising from a BN-pair is a Coxeter system. Denoting $l_s(w)$ for the smallest integer $q \geqslant 0$ such that w is a product of q elements of S, then (i) may be rewritten as (a) if $l_s(sw) > l_s(w)$ then $C(sw) = C(s) \cdot C(w)$, (b) if $l_s(sw) < l_s(w)$ then $C(sw) \cup C(w) = C(s) \cdot C(w)$. Such rules are the cell multiplication rules attached to the Bruhat–Tits cells

[1] For G a group, and subgroups A and B of G, each double coset is of form AxB: it is an equivalence class for the equivalence relation defined on G by

$$x \sim y \quad \text{if there are } a \in A \quad \text{and} \quad b \in B \quad \text{with} \quad axb = y.$$

Then G is partitioned into its (A, B) double cosets. Products of the type sBs in (i) make sense because W is an equivalence class modulo H, and as a result is also a subset of G. More generally, for a subset S of W, the product BSB denotes the coset union $\bigcup_{s \in S} BsB$.

BwB of the Bruhat–Tits decomposition (disjoint union) $G = BWB = \bigcup_{w\in W} BwB$. Axiom (ii) can be rewritten as (c) for any $s \in S$, $C(s) \cdot C(s) = B \cup C(s) \neq B$.

Finally let us give the definition of a *split* BN-*pair*. It satisfies the two additional axioms

$$\text{(iii)} \quad B = UH,$$

where U is a normal nilpotent subgroup of B such that $U \cap H = 1$, and

$$\text{(iv)} \quad H = \bigcap_{n\in\mathbb{N}} nBn^{-1}.$$

3. BN-pairs from the two-qubit Clifford group

Any action of a Pauli operator $g \in \mathcal{P}_n$ on an n-qubit state $|\psi\rangle$ can be stabilized by a unitary gate U such that $(UgU^\dagger)U|\psi\rangle = U|\psi\rangle$, with the condition $UgU^\dagger \in \mathcal{P}_n$. The n-qubit Clifford group (with matrix multiplication for group law) is defined as the normalizer of $\mathcal{P}_n$ in $U(2^n)$

$$\mathcal{C}_n = \{U \in U(2^n) \mid U\mathcal{P}_nU^\dagger = \mathcal{P}_n\}.$$

In view of the relation $U^\dagger = U^{-1}$ in the unitary group $U(2^n)$, normal subgroups of Clifford groups are expected to play a leading role in the quantum error correction [1, 9]. Let us start with the two-qubit Clifford group $\mathcal{C}_2$. The representation

$$\mathcal{C}_2 = \langle \mathcal{C}_1 \otimes \mathcal{C}_1, \mathrm{CZ}\rangle$$

(where $\mathrm{CZ} = \mathrm{diag}(1, 1, 1, -1)$ is the 'controlled-Z' gate) naturally picks up the local Clifford group

$$\mathcal{C}_2^L = \langle \mathcal{C}_1 \otimes \mathcal{C}_1\rangle = \langle H \otimes I, I \otimes H, P \otimes I, I \otimes P\rangle,$$

where the Hadamard gate $H := 1/\sqrt{2}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$ occurs in coding theory as the matrix of the MacWilliams transform and the phase gate is $P := \left(\begin{smallmatrix}1 & 0\\ 0 & \mathrm{i}\end{smallmatrix}\right)$. The weight enumerator of Type II codes is invariant under the group of order 192 generated by P and H, that is $\mathcal{C}_1$ itself [11]. More generally the weight enumerator of genus n in 2^n variables is invariant under the Clifford group $\mathcal{C}_n$ [5]. The issue of efficient (classical) simulation of quantum circuits [13] as well as the topological approach of quantum computation [13] suggests another decomposition of $\mathcal{C}_2$ in terms of the two-qubit gates

$$T := \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} \quad \text{and} \quad R = 1/\sqrt{2}\begin{pmatrix}1 & 0 & 0 & 1\\ 0 & 1 & -1 & 0\\ 0 & 1 & 1 & 0\\ -1 & 0 & 0 & 1\end{pmatrix}.$$

The action of gate T is a *swap* of the two input qubits. It is straightforward to check another representation of the local Clifford group as

$$\mathcal{C}_2^L = \langle H \otimes H, H \otimes P, T\rangle.$$

The action of gate R is a *maximal entanglement* of the two input qubits. Gate R is a *match* gate [13]. It also satisfies the Yang–Baxter equation $(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$ and plays a leading role in the topological approach of quantum computation [13]. It was used in our earlier work to define the *Bell group*

$$\mathcal{B}_2 = \langle H \otimes H, H \otimes P, R\rangle.$$

Both groups $\mathcal{C}_2^L$ and $\mathcal{B}_2$ are subgroups of order 4608 (with index 20) and 15 360 (with index 6) of the Clifford group. The latter may be represented as $\mathcal{C}_2 = \langle H \otimes H, H \otimes P, \mathrm{CZ}\rangle$.

3.1. The search of the BN-pairs

Clearly, the Clifford group is generated by the local Clifford group $\mathcal{C}_2^L$ and Bell group $\mathcal{B}_2$. Their intersection is the Pauli group $\mathcal{P}_2$, of order 64, that is isomorphic to the central product $E_{32}^+ * \mathbb{Z}_4$ (where E_{32}^+ is the extraspecial 2-group of order 32 and type +). The Pauli group $\mathcal{P}_2$ is normal in the Clifford and Bell groups but neither of the quotient groups $\mathcal{C}_2^L/\mathcal{P}_2$ and $\mathcal{B}_2/\mathcal{P}_2 \cong \mathbb{Z}_2 \times S_5$ is a Coxeter group, so that the pair $\left(\mathcal{C}_2^L, \mathcal{B}_2\right)$ cannot be of the BN-type.

Let us search a BN-pair candidate by selecting the subgroup $N \equiv \mathcal{B}_2$ and reducing the size of $\mathcal{C}_2^L$ to a subgroup B so that the intersection group $H = N \cap B$ is a subgroup of B and N/H is a Coxeter group. One gets

$$B \cong W(F_4), \qquad N \equiv \mathcal{B}_2, \qquad H \equiv Z(\mathcal{B}_2) \cong \mathbb{Z}_8 \qquad \text{and} \qquad W \cong W(D_5),$$

in which B is the unique subgroup of $\mathcal{C}_2^L$ which is both of order 1152 and isomorphic to the Coxeter group $W(F_4)$ of type F_4 (the symmetry group of the 24-cell), N is $\mathcal{B}_2$, H is the center $Z(\mathcal{B}_2)$ and W, of order 1920, is isomorphic to the Coxeter group $W(D_5)$ of type D_5.

The above pair of groups is of the BN type seeing that conditions (i) and (ii) are satisfied. Axiom (i) directly follows from the Coxeter group structure of W. For (ii), which is equivalent to (c), it is enough to discover an element in the double coset $C(s)$ which does not lie in group B. Elements of the coset $C(s) = BsB$ arise from elements of the coset $\mathcal{C}_2^L g \mathcal{C}_2^L$, $g \in \mathcal{B}_2$. The latter coset contains the entangling match gate $R' = TRT$, which lies in $\mathcal{B}_2$ but not in $\mathcal{C}_2^L$. Thus (c) is satisfied. The BN pair does not split because there is no normal subgroup of order $|B|/|H| = 144$ within the group B.

3.2. A split BN-pair

A further structure may be displayed in the two-qubit Clifford group. Let us denote $\hat{G}$ the central quotient of the derived subgroup of G. One immediately checks that $\hat{\mathcal{C}}_2 = \left\langle \hat{\mathcal{C}}_2^{(L)}, \hat{\mathcal{B}}_2 \right\rangle \cong U_6$, $\hat{\mathcal{B}}_2 \cong M_{20}$ and $\hat{\mathcal{C}}_2^{(L)} \cong \hat{W}(F_4)$. Group $U_6 = \mathbb{Z}_2^4 \rtimes A_6$, of order 5760, appears in several disguises. The full automorphism group of the Pauli group $\mathcal{P}_2$ possesses a derived subgroup isomorphic to U_6 (see relation (7) in [1]). Geometrically, it corresponds to the stabilizer of a hexad in the Mathieu group M_{22} (see section 4.2 in [1]). Group $M_{20} = \mathbb{Z}_2^4 \rtimes A_5$, of order 960, is isomorphic to the derived subgroup of the imprimitive reflection group $G(2, 2, 5)$ (see section 3.5 in [1]). Incidentally, M_{20} is the smallest perfect group for which the set of commutators departs from the commutator subgroup [9]. Remarkably, the group $\hat{\mathcal{C}}_2$ forms the split BN-pair

$$B \equiv \hat{\mathcal{C}}_2^{(L)}, \qquad N \equiv \hat{\mathcal{B}}_2, \qquad H \equiv \tilde{\mathcal{P}}_2 \cong \mathbb{Z}_2^4, \qquad W \cong A_5, \qquad \text{and} \qquad U \cong \mathbb{Z}_3^2.$$

4. BN-pairs from the three-qubit Clifford group

The local Clifford group

$$\mathcal{C}_3^{(L)} = \{\mathcal{C}_1 \otimes \mathcal{C}_1 \otimes \mathcal{C}_1\}$$

and the three-qubit Bell group

$$\mathcal{B}_3 = \langle H \otimes H \otimes P, H \otimes R, R \otimes H \rangle$$

are subgroups of index 6720 and 56, respectively, of the three-qubit Clifford group (of order 743 178 240). It may be generated as

$$\mathcal{C}_3 = \langle H \otimes H \otimes P, H \otimes \text{CZ}, \text{CZ} \otimes H \rangle.$$

The central quotients $\tilde{\mathcal{C}}_3$ and $\tilde{\mathcal{B}}_3$ may be expressed as semi-direct products

$$\tilde{\mathcal{C}}_3 = \mathbb{Z}_2^6 \rtimes W0'(E_7) \qquad \text{and} \qquad \tilde{\mathcal{B}}_3 = \mathbb{Z}_2^6 \rtimes W'(E_6),$$

in which $W'(E_7) \equiv \mathrm{Sp}(6,2)$ and $W'(E_6)$ are the reflection groups of type E_7 and E_6, respectively [1]. Following the intuition gained from the previous section, one immediately gets the *non-split*[2] BN-pair

$$B \equiv \tilde{\mathcal{C}}_3^{(L)}, \quad N \equiv \tilde{\mathcal{B}}_3, \quad H \equiv \tilde{\mathcal{P}}_3 \cong \mathbb{Z}_2^6, \qquad W \cong W'(E_6) \qquad \text{and} \qquad \tilde{\mathcal{C}}_3^{(L)} \big/ H \equiv V,$$

in which $V \cong S_3^3$ (S_3 is the symmetric group on three letters).

4.1. BN-pairs and a smooth cubic surface

The occurrence of reflection groups $W(F_4)$ and $W(D_5)$ in the decomposition of the two-qubit Clifford group, and of $W(E_6)$ in the decomposition of the three-qubit Clifford group can be grasped in a different perspective from the structure of a *smooth cubic surface* $\mathcal{S}$ embedded into the three-dimensional complex projective space $\mathbb{P}^3(\mathbb{C})$ [14]. The surface contains a maximum of 27 lines in general position and 45 sets of tritangent planes. The group of permutations of the 27 lines is $W(E_6)$, the stabilizer of a line is $W(D_5)$ (observe that $|W(E_6)|/|W(D_5)| = 27$) and the stabilizer of a tritangent plane is $W(F_4)$. Thus the BN-pairs happen to be reflected into the geometry of such a cubic surface.

Other 'coincidences' occur as follows. The number 216 of pairs of skew lines of $\mathcal{S}$ equals the cardinality of the quotient group V entering in the decomposition of $\tilde{\mathcal{C}}_3$. There are 36 double sixes, each one stabilized by the group $g_6 := A_6 \cdot \mathbb{Z}_2^2$ of order 1440 (the symbol . means that the group extension does not split). The latter group can be displayed in the context of the two-qubit Clifford group. Let us observe that the quotients of $\mathcal{C}_2$ and $\mathcal{B}_2$ by the Pauli group $\mathcal{P}_2$ are isomorphic to g_6 and $g_5 := A_5 \cdot \mathbb{Z}_2^2$, respectively. For three-qubits, one checks that the quotients of $\mathcal{C}_3$ and $\mathcal{B}_3$ by the Pauli group $\mathcal{P}_3$ are isomorphic to $W(E_7)$ and $W(E_6)$. Groups $W'(E_6)$, $W(D_5)$, $W(F_4)$ and g_6, which correspond to the permutations of the 27 lines, the stabilizer of a line, a tritangent plane and a double six, respectively, are among the six maximal subgroups of $W(E_6)$. The remaining two are of order 1296 and index 40, corresponding to the size of double cosets BwB, $B \cong W(F_4)$ and $w \in W \cong W(D_5)$, in the BN-pair decomposition of the two-qubit Clifford group.

To conclude, a smooth cubic surface is a particular instance of a K_3 surface, a concept playing a founding role in string theory. Further work is necessary to explore the interface between quantum computing, graded rings and K_3 surfaces [15].

Acknowledgments

The first author warmly acknowledges Richard Jozsa and Noah Linden for the impetus given to this work, following his recent visit at the Department of Computer Science, Bristol. He also received constructive feedback from Maurice Kibler and Metod Saniga.

References

[1] Planat M and Kibler M 2008 arXiv:0807.3650
[2] Montanaro A and Osborne T J 2008 arXiv:0810.2435
[3] Kane R 2001 *Reflection Groups and Invariant Theory* (Berlin: Springer)
[4] Clark S, Jozsa R and Linden N 2008 *Quantum Inf. Comput.* **8** 106

[2] The pair is not split since the quotient group V is not normal in $\tilde{\mathcal{C}}_3^{(L)}$, not nilpotent and $V \cap H \neq 1$.

[5] Nebe G, Rains E M and Sloane N J A 2001 *Des. Codes Cryptogr.* **24** 99
[6] Tits J 1974 *Lecture Notes in Mathematics* vol 386 (Berlin: Springer)
[7] Bourbaki N 1968 *Groupes et algèbres de Lie: Chapitres IV, V and VI* (Paris: Hermann)
[8] Garrett P 1997 *Buildings and Classical Groups* (London: Chapman and Hall)
[9] Planat M and Jorrand P 2008 *J. Phys. A: Math. Theor.* **41** 182001
[10] Jozsa R and Miyake A 2008 *Proc. R. Soc.* **464** 3089 (arXiv:0804.4050)
[11] MacWilliams F J and Sloane N J A 1977 *The Theory of Error-correcting Codes* (Amsterdam: North-Holland)
[12] Carlet C, Danielsen L E, Parker M G and Solé P 2008 Self dual bent functions *BFCA'08 Proc. Int. Conf.* Boolean functions, cryptography and applications
[13] Kauffman L H and Lomonaco S J 2004 *New J. Phys.* **6** 134
[14] Hunt B 1995 arXiv:alg-geom/9503018
[15] Altinok S, Brown G and Reid M 2002 *Contemp. Math.* **314** 25