Group theory for quantum gates and quantum coherence

IOP FTC ▶▶▶

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **41** (2008) 182001 (8pp) doi:10.1088/1751-8113/41/18/182001

FAST TRACK COMMUNICATION

Group theory for quantum gates and quantum coherence

Michel Planat[1] **and Philippe Jorrand**[2]

[1] Institut FEMTO-ST, CNRS, 32 Avenue de l'Observatoire, F-25044 Besançon, France
[2] Laboratoire d'Informatique de Grenoble, 46 avenue Felix Viallet, 38000 Grenoble, France

Received 14 March 2008, in final form 2 April 2008
Published 18 April 2008
Online at stacks.iop.org/JPhysA/41/182001

Abstract

Finite group extensions offer a natural language to quantum computing. In a nutshell, one roughly describes the action of a quantum computer as consisting of two finite groups of gates: error gates from the general Pauli group $\mathcal{P}$ and stabilizing gates within an extension group $\mathcal{C}$. In this communication we explore the nice adequacy between group theoretical concepts such as commutators, normal subgroups, groups of automorphisms, short exact sequences, wreath products etc. and the coherent quantum computational primitives. The structure of the single-qubit and two-qubit Clifford groups is analyzed in detail. As a byproduct, we discover that M_{20}, the smallest perfect group for which the commutator subgroup departs from the set of commutators, underlies quantum coherence of the two-qubit system. We recover similar results by looking at the automorphisms of a complete set of mutually unbiased bases.

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

1. Introduction

The promises of quantum information processing are to solve computational problems and to achieve communication security with quantitative and qualitative performances that are beyond the reach of classical information processing. One of the main obstacles facing the design of a quantum computer is the extreme sensitivity of quantum systems to their classical environment, which induces the decoherence of quantum state preparations. To overcome this limitation, many designs have been proposed for correcting the unavoidable errors, or for preventing them occurring. Since the inception of the field, fault-tolerant procedures such as universal bases of gates [1], quantum codes [2] or quantum teleportation based protocols [3] have been proposed. Other approaches relate to topological quantum computation [4, 5], decoherence free subspaces [6] or are based on sequences of measurements [7].

Despite the number of seemingly different proposals some of them are related: there is a close relation between the 'old fashioned' quantum gate circuitry, fault tolerant quantum codes and measurements, already apparent in the stabilizer formalism [8, 11]. It was shown that a few building block gates are enough to simulate any unitary evolution [2] and a few minimal resources are required for measurement-only quantum computation [12]. This communication explores the fresh view that the geometry of commutation relations [13–15] between the error operators, their corresponding group of symmetries (i.e. the automorphisms), and the splitting of the stabilizer group in terms of maximal normal subgroups [16], sustain the explanation of quantum (de)coherence. Although the approach is performed for a reduced number of qubits, novel pieces of the puzzle appear such as perfect groups with special group theoretical or geometrical properties, and new links are established, such as the relevance of mutually unbiased bases to quantum coherence, or the embedding of quantum topological concepts within the Clifford group. Several recent papers concern closely related topics, see for example [9–19].

Following an outline of useful group theoretical concepts in section 2, the structure of one- and two-qubit Clifford groups is unraveled in section 3 in terms of split short exact sequences, which makes use of permutation groups acting on five or six letters. Calculations are performed using GAP [20] and MAGMA [21].

2. An outline of group commutators, group extensions and groups of automorphisms

For an introduction to group theory one may use the web page [22]. A subgroup N of a group G is called a normal subgroup if it is invariant under conjugation: that is, for each n in N and each g in G, the conjugate element gng^{-1} still belongs to N. In particular, the center $Z(G)$ of a group G (the set of all elements in G which commute with each element of G) is a normal subgroup of G. The group $\tilde{G} = G/Z(G)$ is called the central quotient of G. A second important example of a normal subgroup of G is provided by the subgroup G' of commutators (also called the derived subgroup of G). It is defined as the subgroup generated by all the commutators $[g, h] = ghg^{-1}h^{-1}$ of elements of G. The quotient group $H^{\mathrm{ab}} = G/G'$ is an Abelian group called the Abelianization of G and corresponds to its first homology group. The set $K(G)$ of all commutators of a group G may depart from G' [23].

Our third example relates to group extensions. Let $\mathcal{P}$ and $\mathcal{C}$ be two groups such that $\mathcal{P}$ is a normal subgroup of $\mathcal{C}$. The group $\mathcal{C}$ is an extension of $\mathcal{P}$ by H if there exists a short exact sequence of groups

$$1 \rightarrow \mathcal{P} \overset{f_1}{\rightarrow} \mathcal{C} \overset{f_2}{\rightarrow} H \rightarrow 1,$$

in which 1 is the trivial (single element) group. The above definition can be reformulated as follows:

(i) $\mathcal{P}$ is isomorphic to a normal subgroup N of $\mathcal{C}$,
(ii) H is isomorphic to the quotient group $\mathcal{C}/N$.

Because in an exact sequence the image of f_1 is equal to the kernel of f_2, the map f_1 is injective and f_2 is surjective.

* Given any groups $\mathcal{P}$ and H the direct product of $\mathcal{P}$ and H is an extension of $\mathcal{P}$ by H.

* The semidirect product $\mathcal{P} \rtimes H$ of $\mathcal{P}$ and H is defined as follows. The group $\mathcal{C}$ is an extension of $\mathcal{P}$ by H (one identifies $\mathcal{P}$ with a normal subgroup of $\mathcal{C}$) and

(i) H is isomorphic to a subgroup of $\mathcal{C}$,
(ii) $\mathcal{C} = \mathcal{P}H$ and
(iii) $\mathcal{P} \cap H = \langle 1 \rangle$.

One says that the short exact sequence splits.

The wreath product $M \wr H$ of a group M with a permutation group H acting on n points is the semidirect product of the normal subgroup M^n with the group H, which acts on M^n by permuting its components.

* Let $G = \mathcal{Z}_2 \wr A_5$, in which A_5 is the alternating group on five letters, then G' is a perfect group with order 960 and one has $G' \neq K(G)$. Let $H = Z_2^5 \rtimes A_5$, one can think of A_5 having a wreath action on Z_2^5. The group $G' = \tilde{H} = M_{20}$ [27] is the smallest perfect group having its commutator subgroup distinct from the set of the commutators [23]. One easily checks that M_{20} also corresponds to the derived subgroup W' of the Weyl group (also called hyperoctahedral group) $W = \mathcal{Z}_2 \wr S_5$ for the Lie algebra of type B_5. For a quantum version, see [24].

Group of automorphisms

Given the group operation $*$ of a group G, a group endomorphism is a function ϕ from G to itself such that $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$, for all $g_1, g_2 \in G$. If it is bijective, it is called an automorphism. An automorphism of G that is induced by conjugation of some $g \in G$ is called inner. Otherwise it is called an outer automorphism. Under composition the set of all automorphisms defines a group denoted $\mathrm{Aut}(G)$. The inner automorphisms form a normal subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$, that is isomorphic to the central quotient of G. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the outer automorphism group.

3. Quantum computing and the Clifford group

Compared to group theory, the science of quantum computing is in its infancy [11]. In quantum codes and in quantum computing, one is interested in preventing or correcting errors that may affect one or many physical qubits [10–26]. A frequently used error group is the general Pauli group $\mathcal{P}_n$. It consists of tensor products of the Pauli matrices [13]

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

and the unit matrix σ_0. Pauli matrices generate the single-qubit Pauli group $\mathcal{P}_1$ of order 16 and center $Z(\mathcal{P}_1) = \{\pm 1, \pm i\}$. More generally the n-qubit Pauli group $\mathcal{P}_n$, of order 4^{n+1}, is generated by the tensor product of n Pauli matrices.

Let us assume a quantum system in a state $|\psi\rangle$, and apply to it an error g belonging to the Pauli group $\mathcal{P}$ so that the new state of the system is $g|\psi\rangle$. One allows unitary evolutions U so that the new state evolves as $Ug|\psi\rangle = UgU^{\dagger}U|\psi\rangle$. For stabilizing the error within the Pauli group $\mathcal{P}$, one requires that $UgU^{\dagger} \in \mathcal{P}$. The set of operators leaving $\mathcal{P}$ invariant under conjugation is the normalizer $\mathcal{C}$ in the unitary group U, also known as the Clifford group [8–10][3]. Within a unitary group one has the equality $U^{\dagger} = U^{-1}$. As a result, the group $\mathcal{P}$ is a normal subgroup of $\mathcal{C}$ and one vectors and one may use the powerful formalism of group extensions to report on it. Additionally some subgroups of $\mathcal{C}$, which have the error group $\mathcal{P}$ as a normal subgroup, will play a role for displaying the quantum coherence.

The Clifford group, stabilizing the (error) Pauli group $\mathcal{P}_n$ on n-qubits, will be denoted $\mathcal{C}_n$. One learned from Gottesman–Knill theorem that the Hadamard gate $H = 1/\sqrt{2}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and

[3] The Clifford group (also known as the Jacobi group) was introduced in the context of quantum stabilizer codes by D Gottesman. It does not explicitly refer to Clifford algebras in which the Clifford group means 'the set of invertible elements in the Clifford algebra that stabilizes under twisted conjugation'. In the context of an n-qubit system, a Clifford algebra may be obtained by selecting a set of mutually anti-commuting observables as for the Dirac relativistic equation.

the phase gate $P = \mathrm{Diag}(1, i)$ are in the one-qubit Clifford group $\mathcal{C}_1$, and that the controlled-Z gate $CZ = \mathrm{Diag}(1, 1, 1, -1)$ is in the two-qubit Clifford group $\mathcal{C}_2$. Any gate in $\mathcal{C}_n$ may be generated from the application of gates from $\mathcal{C}_1$ and $\mathcal{C}_2$ [8, 9]. Clifford group $\mathcal{C}_n$ on n-qubits has order $|\mathcal{C}_n| = 2^{n^2+2n+3} \prod_{j=1}^{n} 4^j - 1$ [10].

Below we will concentrate on the properties of the Clifford group related to one and two qubits, using the group theoretical package GAP4 [20]. Generation of the gates will be ensured by the use of cyclotomic numbers, as described in Sec 18 of the GAP4 reference manual. For example, the elements $1, -1, i$ and $2^{1/2}$ will be modeled as the roots of unity $E(1)$, $E(2)$, $E(4)$ and as $ER(2)$, respectively.

3.1. The Clifford group on a single qubit

The one-qubit Clifford group is generated by H and P as $\mathcal{C}_1 = \langle H, P\rangle$. It has order $|\mathcal{C}_1| = 192$, its center is $Z(\mathcal{C}_1) = \mathcal{Z}_8$ and the derived subgroup $\mathcal{C}_1'$ equals the special linear group $SL(2, 3)$. The central quotient is $\tilde{\mathcal{C}_1} = S_4$ and one obtains the Abelianization as the direct product $\mathcal{C}_1^{\mathrm{ab}} = \mathcal{Z}_4 \times \mathcal{Z}_2$.

Using the method described in section 2 two split extensions follow. The first one is attached to $\mathcal{C}_1' = SL(2, 3)$ as follows:

$$1 \rightarrow SL(2,3) \rightarrow \mathcal{C}_1 \rightarrow \mathcal{Z}_2 \times \mathcal{Z}_3 \rightarrow 1.$$

The second one is attached to the Pauli group

$$1 \rightarrow \mathcal{P}_1 \rightarrow \mathcal{C}_1 \rightarrow D_{12} \rightarrow 1,$$

in which $D_{12} = \mathcal{Z}_2 \times S_3$ is the dihedral symmetry group of a regular hexagon.

3.2. The Clifford group on two qubits

The two-qubit Pauli group may be generated as $\mathcal{P}_2 = \langle \sigma_x \otimes \sigma_x, \sigma_z \otimes \sigma_z, \sigma_x \otimes \sigma_y, \sigma_y \otimes \sigma_z, \sigma_z \otimes \sigma_x\rangle$. It is of order 64 and has center $\mathcal{Z}(\mathcal{P}_2) = \mathcal{Z}(\mathcal{P}_1)$. The two-qubit Clifford group, of order 92160, may be generated from H, P and CZ as $\mathcal{C}_2 = \langle H \otimes H, H \otimes P, CZ\rangle$. Its center is $Z(\mathcal{C}_2) = Z(\mathcal{C}_1)$ and the central quotient $\tilde{\mathcal{C}_2}$ is found to satisfy the exact sequence

$$1 \rightarrow U_6 \rightarrow \tilde{\mathcal{C}_2} \rightarrow \mathcal{Z}_2 \rightarrow 1,$$

in which we introduced the notation $U_6 = \tilde{\mathcal{C}_2'} = \mathcal{Z}_2^{\times 4} \rtimes A_6$. Another important relationship is $U_6 = \mathrm{Aut}(\mathcal{P}_2)'$, i.e. U_6 encodes the commutators of the Pauli group automorphisms. It turns out that the group $\tilde{\mathcal{C}_2}$ only contains two normal subgroups $\mathcal{Z}_2^{\times 4}$ and U_6. The group U_6, of order 5760, is a perfect group. It can be seen as a parent of the six element alternating group A_6. Its outer automorphism group $\mathrm{Out}(U_6)$ is the same, equal to the Klein group $\mathcal{Z}_2 \times \mathcal{Z}_2$.

The group U_6 is an important maximal subgroup of several sporadic groups. The group of smallest size where it appears is the Mathieu group M_{22}. Mathieu groups are sporadic simple groups, so that U_6 is not normal in M_{22}. It appears in the context of a subgeometry of M_{22} known as an *hexad*. Let us recall the definition of Steiner systems. A Steiner system $S(a, b, c)$ with parameters a, b, c, is a c-element set together with a set of b-element subsets of S (called *blocks*) with the property that each a-element subset of S is contained in exactly one block. A finite projective plane of order q, with the lines as blocks, is an $S(2, q+1, q^2+q+1)$, because it has q^2+q+1 points, each line passes through $q+1$ points, and each pair of distinct points lies on exactly one line. Any large Mathieu group can be defined as the automorphism (symmetry) group of a Steiner system [28]. The group M_{22} stabilizes the Steiner system $S(3, 6, 22)$ comprising 22 points and six blocks, each set of three points being contained exactly in one block[4]. Any block in $S(3, 6, 22)$ is a Mathieu hexad, i.e. it is stabilized by the *general* alternating group U_6.

There is a relationship between the two-qubit Clifford and Pauli groups

$$\mathcal{C}_2/\mathcal{P}_2 = \mathcal{Z}_2 \times S_6,$$

which features the important role of the six-letter symmetric group S_6. The latter governs the Pauli graph attached to the two-qubit system, being the automorphism group of generalized quadrangle of order 2 $W(2)$ [13]. The group S_6 is peculiar among the symmetric permutation groups as having an outer automorphism group $\mathcal{Z}_2$.

3.3. Quantum coherence within the two-qubit system

Topological quantum computing based on anions has been proposed as a way of encoding quantum bits in nonlocal observables that are immune of decoherence [4, 29]. The basic idea is to use pairs $|v, v^{-1}\rangle$ of 'magnetic fluxes' playing the roles of the qubits and permuting them within some large enough non-Abelian finite group G such as A_5. The 'magnetic flux' carried by the (anyonic) quantum particle is labeled by an element of G, and 'electric charges' are labeled by irreducible representation of G [30].

The exchange within G modifies the quantum numbers of the fluxons according to the fundamental logical operation

$$|v_1, v_2\rangle \rightarrow \left|v_2, v_2^{-1} v_1 v_2\right\rangle,$$

a form of Aharonov–Bohm interactions, which is nontrivial in a non-Abelian group. This process can be shown to produce universal quantum computation. It is intimately related to topological entanglement, the braid group and unitary solutions of the Yang–Baxter equation [31]

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R),$$

in which I denotes the identity transformation and the operator R: $V \otimes V \rightarrow V \otimes V$ acts on the tensor product of the bi-dimensional vector space V. One elegant unitary solution of the Yang–Baxter equation is a universal quantum gate known as the Bell basis change matrix

$$R = 1/\sqrt{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}.$$

It is straightforward to see two-qubit topological quantum computing as another group extension of the Pauli group. One may introduce a subgroup of the Clifford group, of order 15360, that we denote the Bell group as follows:

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

The Bell group has center $\mathcal{Z}_8$ and its central quotient only contains two normal subgroups $\mathcal{Z}_2^{\times 4}$ and $M_{20} = \mathcal{Z}_2^{\times 4} \rtimes A_5$. The group M_{20} was already quoted in section 2 as being the smallest perfect group having the set of commutators departing from the commutator subgroup. The relationship between the Bell and Pauli groups

$$\mathcal{B}_2/\mathcal{P}_2 = \mathcal{Z}_2 \times S_5$$

displays the important role of the five letters symmetric group S_5. At this point, it may be useful to mention that A_5 is the automorphism group of the icosahedron. Icosahedral symmetry and quantum coherence seems to be related in recent fullerene experiments [32].

[4] There exists up to equivalence a unique S(5,8,24) Steiner system called a Witt geometry. The group $M(24)$ is the automorphism group of this Steiner system, that is, the set of permutations which map every block to some other block. The subgroups $M(23)$ and $M(22)$ are defined to be the stabilizers of a single point and two points respectively.

Table 1. Group structure of an independent set of the two-qubit (g_2 to g_4) and three-qubit systems (g_2 to g_6). G denotes the identified group and Aut(G) the corresponding automorphism group. $\mathcal{Q}_8$ and $\mathcal{D}_8$ are the eight-element quaternion and dihedral groups.

g_i	g_2	g_3	g_4	g_5	g_6
G	$\mathcal{Z}_2^{\times 2}$	$(\mathcal{Z}_4 \times \mathcal{Z}_2) \rtimes \mathcal{Z}_2$	$(\mathcal{Z}_2 \times \mathcal{Q}_8) \rtimes \mathcal{Z}_2$	$\mathcal{Z}_2 \times ((\mathcal{Z}_2 \times \mathcal{Q}_8) \rtimes \mathcal{Z}_2)$	g_6
Aut(G)	$\mathcal{D}_8$	$\mathcal{Z}_2 \times S_4$	$\mathcal{Z}_2 \wr A_5$	$\mathcal{Z}_2^{\times 2} \wr A_5$	$\mathcal{Z}_2^{\times 3} \wr A_5$
$\lvert$Aut$(G)\rvert$	8	48	1920	61 440	196 6080

3.4. *Quantum coherence within mutually unbiased bases*

To our knowledge, the relationship between mutually unbiased bases (MUBs) of the Pauli group and the Clifford group has not yet been established. Two orthonormal bases are said to be mutually unbiased if each common state of one basis gives rise to the same probability distribution when measured with respect to the other basis. For prime power dimensions p^m, complete sets of MUBs have cardinality $p^m + 1$ and can be determined using different techniques such as the additive characters over a Galois field [33] [5]. In composite dimensions, MUBs strongly rely on projective lines over finite rings [36]. In addition, the continuous variable case was addressed recently [37].

Commuting/non-commuting relations between the Pauli operators of the two-qubit system have been determined [13]. The Pauli graph admits several decompositions: one of them is based on its minimum vertex cover (the Petersen graph) and a maximal independent set (of size five). If one uses a geometrical representation, operators correspond to the points of the geometry, maximal sets of mutually commuting operators, i.e. MUBs, correspond to the lines of the geometry, and a complete set of MUBs corresponds to an ovoid (the maximum number of mutually disjoint lines). The geometry of the two-qubit system is the smallest nontrivial generalized quadrangle. Due to the perfect duality between the 15 points and 15 lines of the quadrangle, the cardinality of a maximal independent set and the one of the ovoid is the same.

These graph theoretical and geometrical features of MUBs have a group theoretical counterpart that one may find in the group of automorphisms attached to a maximal independent set. Let us denote m_i $(i = 1 \ldots 5)$ the elements of such a maximal set, one may form groups of increasing size $g_2 = \langle m_1, m_2 \rangle, \ldots$ $g_4 = \langle m_1, m_2, m_3, m_4 \rangle$. ($g_1$ is the trivial group and $g_5 = g_4$). The groups g_i and the corresponding groups of automorphisms Aut(g_i) are identified in table 1. One readily observes that the group of automorphisms of the selected maximal independent set/ovoid of the two-qubit system is isomorphic to the wreath product $\mathcal{Z}_2 \wr A_5$ encountered in topological quantum computing. One concludes that some symmetries in a complete set of MUBs also provide a signature of quantum coherence. Let us mention that the hyperoctahedral group $\mathcal{Z}_2 \wr S_5$, of order 3840, corresponds to the automorphism group of the code $((5, 6, 2))$, the first instance of a non-additive quantum code [38].

The same approach can be applied to the three-qubit system and higher-order qubit systems. For the three-qubit system, the size of a maximal independent set is found to be seven (it is different from the size $9 = 2^3 + 1$ of a complete set of MUBs). The corresponding automorphism group encompasses one of the two-qubit systems as shown in table 1. The group Aut(g_n) $(n > 4)$ is found to be isomorphic to the wreath product $\mathcal{Z}_2^{\times m} \wr A_5$, with $m = n - 3$. Its central quotient equals its derived subgroup and may be identified to the

[5] Power of prime dimensions also plays a pivotal role in the number theoretical approach of $1/f$ noise developed by one of us [34, 35].

perfect group $(\mathcal{Z}_2^{\times 4})^{\rtimes m} \rtimes A_5$. These perfect groups of order 960, 15360, 245760 contain some elements, which are not commutators[6].

4. Conclusion

Advanced group theoretical tools may be used to explore fault tolerance in quantum computing. We found some fingerprints of quantum (de)coherence in exceptional groups such as U_6 (the stabilizer of an hexad in M_{22}), in the group M_{20}, and in the automorphism groups of mutually unbiased bases. Using this approach, disparate concepts such as the stabilizer formalism, topological quantum computing [39] and the mathematical approach of quantum complementary, tend to merge. Future work will be devoted to arbitrary n-qudit systems and composite systems, and the link to quantum codes.

Acknowledgments

The authors acknowledge the support of the PEPS program (Projects Exploratoires Pluridisciplinaires) from the ST2I department at CNRS, France (Sciences et Technologies de l'Information et de la Communication).

References

[1] Boykin O, Mor T, Pulver M, Roychowdhury V and Vatan F 1999 On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for Shor's basis 40th Annual Symposium on the Foundations of Computer Science pp 486–94 (*Preprint* quant-ph/9906054)

[2] S Francoise J P, Naber G L and Tsou S T 2006 Quantum error correction and fault tolerance *Encyclopedia of Mathematical Physics* vol 4 ed D Gottesman (Oxford: Elsevier) pp 196–201 (*Preprint* quant-ph/0507174)

[3] Gottesman D and Chuang I L 1999 Quantum teleportation is a universal computational primitive *Nature* **402** 390–2

[4] Kitaev A Yu 1997 Fault-tolerant quantum computation with anions *Preprint* quant-ph/9707021

[5] Raussendorf R, Harrington J and Goyal K 2007 Topological fault-tolerance in cluster state quantum computation *New J. Phys.* **9** 199

[6] Wu L A, Zanardi P and Lidar D A 2005 Holonomic quantum computation in decoherence-free subspaces *Phys. Rev. Lett.* **95** 130501

[7] Perdrix S and Jorrand Ph 2006 Classical-controlled quantum computation *Math. Structures Comp. Sci.* **16** 601–20

[8] Gottesman D 1998 The Heisenberg representation of quantum computers *Preprint* quant-ph/9807006

[9] Clark S, Jozsa R and Linden N 2008 Generalized Clifford groups and simulation of associated quantum circuits *Quant. Inf. Comp.* **8** 106–26

[10] Calderbank A R, Rains E M, Schor P W and Sloane N J A 1998 Quantum error correction via codes over $GF(4)$ *IEEE Trans. Inform. Theory* **44** 1369–87

[11] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[12] Perdrix S 2007 Toward minimal resources of measurement-based quantum computation *New J. Phys.* **9** 206

[13] Planat M and Saniga M 2008 On the Pauli graphs of N-qudits *Quant. Inf. Comp.* **8** 127–46

[14] Planat M, Saniga M and Kibler M 2006 Quantum entanglement and projective ring geometry *Sigma* **2** 66

[15] Saniga M and Planat M 2007 Multiple qubits as symplectic polar spaces of order two *Adv. Stud. Theor. Phys.* **1** 1–4

[16] Planat M 2007 Clifford quantum computer and the Mathieu groups *Preprint* quant-ph/0711.1733

[17] Bombin H and Martin-Delgado M A 2006 Topological quantum distillation *Phys. Rev. Lett.* **97** 180501

[18] Aerts D and Czachor M 2007 Cartoon computation: Quantum-like algorithms without quantum mechanics *J. Phys. A: Math. Theor.* **40** F259–66

[6] The calculation is performed using theorem 6.6 in [23].

[19] Zeier R, Grassl M and Beth T 2004 Gate simulation and lower bounds on the simulation time *Phys. Rev.* A **70** 032319

[20] *The GAP Group 2004 GAP—Groups, Algorithms, and Programming, Version 4.4* (http://www.gap-system.org)

[21] Bosma W, Cannon J and Playoust C 1997 The Magma algebra system. I. The user language *J. Symb. Comput.* **24** 235–65

[22] Milne J S Group theory (available on line at http://www.jmilne.org/math/)

[23] Kappe L C and Morse R F On commutators in groups (available on line at http://faculty.evansville.edu/rm43/publications/commutatorsurvey.pdf)

[24] Banica T, Bichon J and Collins B 2007 The hyperoctahedral quantum group *Preprint* math.RT/0701859

[25] Klappenecker A and Rötteler M 2002 Beyond stabilizer codes: I. Nice error bases *IEEE Trans. Inform. Theory* **48** 2392–5

[26] Klappenecker A and Rötteler M 2002 Beyond stabilizer codes II: Clifford codes *IEEE Trans. Inform. Theory* **48** 2396–9

[27] ATLAS of Finite Group Representations http://brauer.maths.qmul.ac.uk/Atlas/v3/misc/M20/

[28] Wilson R A The finite simple groups (available at http://www.maths.qmul.ac.uk/∼raw/fsgs.html)

[29] Preskill J 1998 Fault tolerant quantum computation *Introduction to Quantum Computation and Information* ed H K Lo, T Spiller and S Popescu (Singapore: World-Scientific) (*Preprint* quant-ph/9712048)

[30] Ogburn R W and Preskill J 1999 *Topological Quantum Computation* (Lecture Notes in Computer Science vol 1509) pp 341–56

[31] Kauffman L H and Lomonaco S J 2004 Braiding operators are universal quantum gates *New J. Phys.* **6** 134

[32] Benjamin S *et al* 2006 Toward a fullerene-based quantum computer *J. Phys.: Condens. Matter* **18** S867–83

[33] Planat M, Rosu H C and Perrine S 2006 A survey of finite algebraic geometrical structures underlying mutually unbiased measurements *Found. Phys.* **36** 1662–80

[34] Planat M 2001 $1/f$ noise, the measurement of time and number theory *Fluc. Noise Lett.* **1** R65–79

[35] Planat M 2000 $1/f$ frequency noise in a communication receiver and the Riemann hypothesis *Lect. Notes Phys.* **550** 265–87

[36] Planat M and Baboin A C 2007 Qudits of composite dimension, mutually unbiased bases and projective ring geometry *J. Phys. A: Math. Theor.* **40** F1–8

[37] Weigert S and Wilkinson M 2008 Mutually unbiased bases for continuous variables (*Preprint* quant-ph/0802.0394)

[38] Rains E M, Hardin R H, Schor P W and Sloane N J A 1997 *Phys. Rev. Lett.* **79** 953–54

[39] Bombin H and Martin-Delgado M A 2007 A family of non-Abelian Kitaev models on a lattice: topological confinement and condensation *Preprint* cond-mat.str-el/0712.0190