On group theory, quantum gates and quantum coherence

Michel Planat (joint work with Philippe Jorrand)

Institut FEMTO-ST, 32 Avenue de l’Observatoire, F-25044 Besançon
(michel.planat@femto-st.fr)

Quantum Information and Graph Theory: emerging connections, Waterloo (PI), April 28- May 2 (2008)

2. Finite group extensions: a natural language for quantum computing: error gates from the Pauli group $\mathcal{P}$, and stabilizing gates within an extension group $\mathcal{C}$.

- Single qubit $C_1$ and ... magic states.
- Two-qubit $C_2$ and ... alt. group $A_6$, the non-coherent group $U_6$ (order 5760), Mathieu group $M_{22}$, alt. group $A_5$, the coherent group $M_{20}$ (order 960)... 
- Three-qubit coherence, $A_5$ and ...$SU(4, 2)$. 

Michel Planat (joint work with Philippe Jorrand) 
On group theory, quantum gates and quantum coherence
On the Pauli graphs on $N$-qudits$^1$

$^1$M. Planat and M. Saniga, Quant Inf Comp 8, 127-146 (2008)
Glossary on finite geometries: 1

- **FINITE GEOMETRY**: a space $S = \{P, L\}$ of points $P$ and lines $L$ such that certain conditions, or axioms, are satisfied.

- **A near linear space/linear space**: a space such that any line has at least two points and two points are at most exactly on one line.

- **A projective plane**: a linear space in which any two lines meet and there exists a set of four points no three of which lie on a line. The projective plane axioms are dual. The smallest one is $PG(2, 2)$: the Fano plane with 7 points and 7 lines.

- **A projective space**: a linear space such that any two-dimensional subspace of it is projective plane. The smallest one is three dimensional and binary: $PG(3, 2)$. 
1. Geometry of the two-qubit system, the generalized quadrangle $GQ(2)$ and its basic factorizations

2. Group theory for quantum gates...

Glossary on finite geometries: 2

- **A generalized quadrangle**: a near linear space such that given a line $L$ and a point $P$ not on the line, there is exactly one line $K$ through $P$ that intersects $L$ (in some point $Q$). A **finite** generalized quadrangle $GQ$ is said to be of order $(s, t)$ if every line contains $s + 1$ points and every point is in exactly $t + 1$ lines$^2$.

- **A geometric hyperplane $H$**: a set of points such that every line of the geometry either contains exactly one point of $H$, or is completely contained in $H$.

- **A polar space $S = \{P, L\}$**: a near-linear space such that for every point $P$ not on a line $L$, the number of points of $L$ joined to $P$ by a line equals either one (as for a generalized quadrangle) or to the total number of points of the line.

---

$^2$Properties: $\#P = (s + 1)(st + 1)$, $\#L = (t + 1)(st + 1)$, the incidence graph is strongly regular and the eigenvalues of the adjacency matrix are $k = s(t + 1)$, $r = s - 1$, $l = t - 1$; moreover $r$ has multiplicity $f = st(s + 1)(t + 1)/(s + t)$. 

Michel Planat (joint work with Philippe Jorrand) On group theory, quantum gates and quantum coherence
1. Geometry of the two-qubit system, the generalized quadrangle $GQ(2)$ and its basic factorizations

2. Group theory for quantum gates...

Geometry of commuting/anti-commuting relations of the two-qubit system

- Fifteen tensor products $\sigma_i \otimes \sigma_j$ of Pauli matrices $\sigma_i = (l_2, \sigma_x, \sigma_y, \sigma_z)$, where $l_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\sigma_y = i\sigma_x\sigma_z$.

- Labels: $1 = l_2 \otimes \sigma_x$, $2 = l_2 \otimes \sigma_y$, $3 = l_2 \otimes \sigma_z$, $a = \sigma_x \otimes l_2$, $4 = \sigma_x \otimes \sigma_x \ldots$, $b = \sigma_y \otimes l_2 \ldots$, $c = \sigma_z \otimes l_2 \ldots$

Embedding of the generalized quadrangle $GQ(2)$ (and thus of the Pauli graph $G_2$ into the projective space $PG(3,2)$).
GQ(2) as the *unique* underlying geometry of the two-qubit system. The Pauli operators correspond to the points and the base/maximally commuting subsets of them to the lines of the quadrangle.
1. Geometry of the two-qubit system, the generalized quadrangle \( GQ(2) \) and its basic factorizations

2. Group theory for quantum gates...

Miscellaneous properties of the generalized quadrangle \( GQ(2) \)

- Two-qubit geometry \( GQ(2) \), graph \( G_2 \), group \( P_2 \)
- \( GQ(2) \) as the two-qubit Pauli graph \( G_2 \)
- \( \text{Aut}(GQ(2)) = S_6 \)
- \( G_2 = \hat{L}(K_6) \) generalizes Petersen graph \( PG = \hat{L}(K_5) \)
- There exists 6 maximal sets of 5 disjoint lines (MUBs)
- \( \text{Out}(S_6) = \mathbb{Z}_2 \times \mathbb{Z}_2 \)
- Later, I define \( \mathbb{Z}_2 \wr A_6 \) as \( \text{Aut}(P_2) \)
1. Geometry of the two-qubit system, the generalized quadrangle $GQ(2)$ and its basic factorizations

2. Group theory for quantum gates...

Basic partitionings: FP+CB

Partitioning of $G_2$ into a pencil of lines in the Fano plane (FP) and a cube (CB).
Partitioning of $G_2$ into an unentangled bipartite graph ($BP$) and a fully entangled Mermin square ($MS$). Operators on all six lines carry a base of entangled states. The graph is polarized.
The partitioning of $G_2$ into a maximum independent set (I) and the Petersen graph (PG), aka its minimum vertex cover. )
A geometric hyperplane $H$: a set of points such that every line of the geometry either contains exactly one point of $H$, or is completely contained in $H$.

- A perp-set $(H_{cl}(X))$, i.e., a set of points collinear with a given point $X$, the point itself inclusive (there are 15 such hyperplanes). It corresponds to the pencil of lines in the Fano plane.

- A grid $(H_{gr})$ of nine points on six lines (there are 10 such hyperplanes). It is a Mermin square.

- An ovoid $(H_{ov})$, i.e., a set of (five) points that has exactly one point in common with every line (there are six such hyperplanes). An ovoid corresponds to a maximum independent set.
Group theory, quantum gates and quantum coherence

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 $N$.

e.g. 1: the **center** $Z(G)$ of a group of $G$. The group $\tilde{G} = G/Z(G)$ is called the **central quotient** of $G$.

e.g. 2: the subgroup $G'$ of **commutators** (generated by all the commutators $[g, h] = ghg^{-1}h^{-1}$ of elements of $G$). The quotient group $H^{ab} = G/G'$ 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 $G'$.
e.g. 3: **group extensions.** Let $\mathcal{P}$ and $\mathcal{C}$ be two groups such that $\mathcal{P}$ is 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

$$1 \to \mathcal{P} \xrightarrow{f_1} \mathcal{C} \xrightarrow{f_2} H \to 1,$$

i.e.

(i) $\mathcal{P} \cong$ a normal subgroup $N$ of $\mathcal{C}$,

(ii) $H \cong \mathcal{C}/N$.

In an exact sequence $\text{Im}(f_1) = \text{Ker}(f_2)$, then the map $f_1$ is injective and $f_2$ is surjective.
Given any groups $P$ and $H$ the **direct product** of $P$ and $H$ is an extension of $P$ by $H$,

The **semidirect product** $P \rtimes H$ of $P$ and $H$:
The group $C$ is an extension of $P$ by $H$ and
(i) $H$ is isomorphic to a subgroup of $C$,
(ii) $C = PH$ and
(iii) $P \cap H = \langle 1 \rangle$.
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.
Icosahedral symmetry and the "Mathieu group" $M_{20}$:

Let $G = \mathbb{Z}_2 \wr A_5$, then $G$ is a perfect group with order $2^5 \cdot 60$. 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 $G' = \tilde{H} = M_{20}$ is the smallest perfect group having its commutator subgroup distinct from the set of the commutators $^4$.

$M_{20}$ also corresponds to the derived subgroup $W'$ of the Weyl group (also called hyperoctahedral group) $W = \mathbb{Z}_2 \wr S_5$ for the Lie algebra of type $B_5$.

---

$^4$On commutators in groups. L C Kappe and R F Morse. available on line at http://faculty.evansville.edu/rm43/publications/commutatorsurvey.pdf
Given the group operation $\ast$ of a group $G$, a **group endomorphism** is a function $\phi$ from $G$ to itself such that $\phi(g_1 \ast g_2) = \phi(g_1) \ast \phi(g_2)$, 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 $\text{Aut}(G)$. The **inner automorphisms** form a **normal subgroup** $\text{Inn}(G)$ of $\text{Aut}(G)$, that is isomorphic to the central quotient of $G$. The quotient $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ is called the **outer** automorphism group.
Quantum computing: a few quantum gates

- **The Hadamard gate**: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- **and the phase shift gate** $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

- **superpositions**: $H \ket{0} = \frac{1}{\sqrt{2}}(\ket{0} + \ket{1})$, $H \ket{1} = \frac{1}{\sqrt{2}}(\ket{0} - \ket{1})$.

- **The Controlled not gate** $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

- **entanglement**: $\text{CNOT}(\alpha \ket{0} + \beta \ket{1}) \ket{0} = \alpha \ket{00} + \beta \ket{11}$.

- **The Toffoli gate** $\text{TOF} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. 
1. Geometry of the two-qubit system, the generalized quadrangle $GQ(2)$ and its basic factorizations

2. Group theory for quantum gates...

A quantum computing challenge

- Correcting the errors in **quantum computing**: quantum codes or methods immune of decoherence.

- Error group: the Pauli group $\mathcal{P}$
  
  \[ |\psi\rangle \rightarrow \text{error } g |\psi\rangle \rightarrow \text{unitary evolution } Ug |\psi\rangle = UgU^\dagger U |\psi\rangle. \]
  
  Stabilizing the error $g \in \mathcal{P}$ requires $UgU^\dagger \in \mathcal{P}$.

- Error free operators are in the **Clifford group** $\mathcal{C}$
  
  e.g. $H$, $P$, $CNOT$.

- Since $U^\dagger = U^{-1}$, $\mathcal{P}$ is a **normal subgroup** of $\mathcal{C}$.
For a system of \( n \) qubits one denotes the **Pauli group** as \( \mathcal{P}_n \) and the **Clifford group** as \( C_n \).

\[
C_1 = \langle H, P \rangle, \quad C_2 = \langle C_1 \otimes C_1, CZ \rangle \quad \text{with} \quad CZ = \text{Diag}(1, 1, 1, -1).
\]

Any gate in \( C_n \) is a circuit of gates from \( C_1 \) and \( C_2 \). \(^5\)

Clifford group \( C_n \) on \( n \)-qubits has order

\[
|C_n| = 2^{n^2+2n+3} \prod_{j=1}^n 4^j - 1.
\]

e.g. a **MAGMA program** //Two-qubit Clifford group

\[
K\langle w \rangle := \text{CyclotomicField}(8); \quad r2 := w + \text{ComplexConjugate}(w);
\]

\[
H := \text{Matrix}(K, 2, 2, [1/r2, 1/r2, 1/r2, w^4/r2]);
\]

\[
P := \text{Matrix}(K, 2, 2, [1, 0, 0, w^2]); \quad CZ := \text{DiagonalMatrix}([1, 1, 1, w^4]);
\]

\[
H2 := \text{KroneckerProduct}(H, H); \quad HP := \text{KroneckerProduct}(H, P);
\]

\[
C2 := \text{MatrixGroup}\langle 4, K|H2, HP, CZ \rangle; \quad \text{Order}(C2);
\]

192, 92 160, 743 178 240

The Clifford group on a single qubit

- **One-qubit Clifford group** \( C_1 = \langle H, P \rangle \): \(|C_1| = 192, Z(C_1) \cong \mathbb{Z}_8, C'_1 \cong SL(2,3), \tilde{C}_1 = S_4 \) and \( C_{1 \text{ab}} = \mathbb{Z}_4 \times \mathbb{Z}_2 \).

- A split extension attached to the **commutator subgroup** \( C'_1 \)
  
  \[
  1 \rightarrow SL(2,3) \rightarrow C_1 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow 1.
  \]

- ... attached to the **magic group**\(^6\) \( \langle T, H \rangle \), where \( T = \exp(i\pi/4)PH \)
  
  \[
  1 \rightarrow GL(2,3) \rightarrow C_1 \rightarrow \mathbb{Z}_4 \rightarrow 1.
  \]

- ... attached to the **Pauli group**
  
  \[
  1 \rightarrow P_1 \rightarrow C_1 \rightarrow D_{12} \rightarrow 1,
  \]

  in which \( D_{12} = \mathbb{Z}_2 \times S_3 \) is the symmetry group of a **regular hexagon**.

---

Two-qubit Pauli group
\[ \mathcal{P}_2 = \langle \sigma_x \otimes \sigma_x, \sigma_z \otimes \sigma_z, \sigma_x \otimes \sigma_y, \sigma_y \otimes \sigma_z, \sigma_z \otimes \sigma_x \rangle, \text{ order } 64, \]
\[ Z(\mathcal{P}_2) = \{ \pm 1, \pm i \}. \]

Two-qubit Clifford group \( \mathcal{C}_2 = \langle H \otimes H, H \otimes P, CZ \rangle, \text{ order } 92160. \)

\[ Z(\mathcal{C}_2) = \mathbb{Z}_8, \tilde{\mathcal{C}}_2 \text{ such that} \]
\[ 1 \to U_6 \to \tilde{\mathcal{C}}_2 \to \mathbb{Z}_2 \to 1. \]

It turns out that the group \( \tilde{\mathcal{C}}_2 \) only contains two normal subgroups \( \mathbb{Z}_2^\times \times 4 \) and \( \tilde{\mathcal{C}}'_2 = U_6 = \mathbb{Z}_2^\times \times 4 \rtimes A_6 \). The group \( U_6 \), of order 5760, is a perfect group. \( \text{Out}(U_6) = \text{Out}(A_6) = \mathbb{Z}_2 \times \mathbb{Z}_2. \)

\[ \text{Aut}(\mathcal{P}_2) = \mathbb{Z}_2 \rtimes A_6, U_6 = \text{Aut}(\mathcal{P}_2)'. \]

\[ \mathcal{C}_2/\mathcal{P}_2 = \mathbb{Z}_2 \times S_6. \]
- $U_6$ is a maximal subgroup of several sporadic groups. The smallest one is $M_{22}$. It appears in relation to a subgeometry of $M_{22}$ known as an hexad.

- 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.

$M_{22}$ stabilizes the **Steiner system** $S(3, 6, 22)$ comprising 22 points and 6 blocks, each set of 3 points being contained exactly in one block.

Any block in $S(3, 6, 22)$ is a **Mathieu hexad**, stabilized by the *general* alternating group $U_6$. 

Michel Planat (joint work with Philippe Jorrand)
Topological quantum computing based on anyons has been proposed as way of encoding quantum bits in non local observables that are immune of decoherence \(^7\). The basic idea is to use pairs \(|\nu, \nu^{-1}\rangle\) 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 \(G\).

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

\[
|\nu_1, \nu_2\rangle \rightarrow |\nu_2, \nu_2^{-1} \nu_1 \nu_2\rangle,
\]

a form of Aharonov-Bohm interactions (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:\(^8\)

\[(R \otimes I_2)(I_2 \otimes R)(R \otimes I_2) = (I_2 \otimes R)(R \otimes I_2)(I_2 \otimes R),\]

in which the operator \(R: V \otimes V \to V \otimes V\) acts on the tensor product of the bidimensional vector space \(V\). One elegant unitary solution of the Yang-Baxter equation is a universal quantum gate known as the Bell basis change matrix

\[
R = \frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 0 & 0 & 1 \\
0 & 1 & -1 & 0 \\
0 & 1 & 1 & 0 \\
-1 & 0 & 0 & 1
\end{pmatrix}.
\]

Two-qubit topological quantum computing and the Bell subgroup of the Clifford group, of order $15360$

$$\mathcal{B}_2 = \langle H \otimes H, H \otimes P, R \rangle. \quad (1)$$

- $Z(\mathcal{B}_2) = \mathbb{Z}_8$, $\mathcal{B}'_2 = \mathbb{Z}_2 \wr A_5$, and

$$1 \to \mathbb{Z}_2 \wr A_5 \to \mathcal{B}_2 \to \mathbb{Z}_2 \to 1.$$ 

- $\tilde{\mathcal{B}}_2$ only contains two normal subgroups $\mathbb{Z}_2^{\times 4}$ and $M_{20} = \mathbb{Z}_2^{\times 4} \rtimes A_5$.

Relation between Bell and Pauli groups

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

$S_5$ is the stabilizer of Petersen graph.
1. Geometry of the two-qubit system, the generalized quadrangle $GQ(2)$ and its basic factorizations

2. Group theory for quantum gates...

Quantum coherence from mutually unbiased bases

<table>
<thead>
<tr>
<th>$G$</th>
<th>$g_2$</th>
<th>$g_3$</th>
<th>$g_4$</th>
<th>$g_5$</th>
<th>$g_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aut($G$)</td>
<td>$D_8$</td>
<td>$\mathbb{Z}_2 \times S_4$</td>
<td>$\mathbb{Z}_2 \wr A_5$</td>
<td>$\mathbb{Z}_2^2 \wr A_5$</td>
<td>$\mathbb{Z}_2^3 \wr A_5$</td>
</tr>
<tr>
<td>$</td>
<td>\text{Aut}(G)</td>
<td>$</td>
<td>8</td>
<td>48</td>
<td>1920</td>
</tr>
</tbody>
</table>

- Group structure of the maximal independent set generating a complete set of MUBs: $g_i = \langle m_1, m_2 \cdots m_i \rangle$.
- The wreath product $\mathbb{Z}_2 \wr S_5$ corresponds to the first known example of a non-additive quantum code.
Three-qubit quantum coherence

- **Two-qubit system**
  \[ \tilde{C}_2 = \mathbb{Z}_2^4 \rtimes S_6, \quad S_6 = Sp(4,2) \text{ (order 720)}, \]
  \[ \tilde{B}_2 = \mathbb{Z}_2^4 \rtimes S_5 \]

- **Tree-qubit system**
  Let \( \tilde{B}_3 = \langle H \otimes H \otimes P, H \otimes R, R \otimes H \rangle \).
  \[ \tilde{C}_3 = \mathbb{Z}_2^6 \rtimes G_1, \quad G_1 := Sp(6,2) \text{ (order 1 451 520)}, \]
  \[ \tilde{B}_3 = \mathbb{Z}_2^6 \rtimes G_2, \]
  with \( G_2 = SU(4,2) \cong PSp(4,3) \text{ (order 25920)}. \)

- **Geometry**: \( G_1 \) (resp \( G_2 \)) are the derived subgroups of the Weyl groups attached to exceptional Lie algebra of type \( E_7 \) (resp \( E_6 \)).
Merging of several concepts?

- Quantum gates and the **Geometry of classical groups**
  * Tits systems (BN pairs) (see D. E. Taylor, 1992)
- Topological quantum computing
- Non-additive quantum codes
- Ring geometry [collaboration with M. Saniga (SK) and H. Havlicek(Austria)]