Calcul quantique à partir de Magma

Michel Planat

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

Journée des utilisateurs du Mésocentre, 14/02/2011, Besançon

Les mathématiques de Magma

* The Magma Language and System
* Groups
* Semigroups and Monoids
* Rings and their Fields
* Commutative Rings
* Linear Algebra and Module Theory
* Lattices and Quadratic Forms
* Algebras
* Representation Theory
* Homological Algebra
* Lie Theory
* Algebraic Geometry
* Finite Incidence Geometry
* Differential Galois Theory
* Error-correcting Codes
* Cryptography
* Mathematical Databases

Exemple de théorie des nombre

```
for i in [1000..1010] do
i,MoebiusMu(i),DivisorSigma(0,i),DivisorSigma(1,i);
end for;
1000 0 16 2340
1001 -1 8 1344
1002 -1 8 2016
1003 1 4 1080
1004 0 6 1764
1005 -1 8 1632
1006 1 4 1512
1007 1 4 1080
1008 0 30 3224
1009 -1 2 1010
1010 -1 8 1836
```

L'hypothèse de Riemann

L'hypothèse de Riemann est équivalente à l'inégalité [1]

$$\frac{N_q|\phi_\beta(N_q)|}{\log\log N_q} > \frac{e^\gamma}{\zeta(\beta-1)},\ \beta>2, q>2,$$

où est une primorielle et la fonction KMS de Bost-Connes est

$$\phi_\beta(q) = q^{-\beta} \prod_{p\in\mathcal{P}, p|q} \frac{1-p^{\beta-1}}{1-p^{-1}}.$$

[1] Riemann hypothesis and quantum mechanics, M. Planat and P. Solé, Preprint 1012.4665 [math-ph].

Programme 1

```
// Fonction primorielle
prim:=function(n);
p:=2; pp:=2;
for i in [1..n-1] do
p:=NextPrime(p); pp:=pp*p;
end for;
return (pp);
end function;
time 1.*prim(100000);
1.90960422001273396845930442975E563920 Time: 25.984
//Fonction KMS
b0:=5;
rphi := function(n);
p:=2; phi := (1 − 2^(b0 − 1))/(1 − 1/2);
for i in [1..n-1] do
p:=NextPrime(p); phi := phi ∗ (1 − p^(b0 − 1))/(1 − 1/p);
end for;
return (phi);
```

Résultats

// Un critère quivalent à l'hypothèse de Riemann
t:=b0-1;
Eu:=0.57721566490153286060651209008240243104215933593992359880576723
L := RiemannZeta(: Precision:=50); zeta:=Evaluate(L,t);
k:=Exp(Eu)/zeta;
time for i in [10000..10002] do
$i, 1. * prim(i), 1. * Abs(rphi(i)) * prim(i)^{(1-b0)}/Log(Log(prim(i))) - k;$
end for;
10000 9.063359632921050612922506212 30E45336
0.00092778404848838046715079389994 5
10001 9.493234780310496043493420681 95E45341
0.00092772766941825989298080948097 7
10002 9.945017823505472550203272572 20E45346
0.00092767057872927232206735303937 9
Time: 23.391

Abstract[2, 3]

* **Single qudits**: qubit, qutrit, quartit, quintit, sextit, heptit, octit, 9-dit, 10-dit, 11-dit, 12-dit, 13-dit...

  - Commutation relations between observables of a single q-dit: maximal commuting sets and the **Pauli** group/*graph*/geometry
  - A bijection between the Pauli group observables (modulo the center) and the modular lattice $\mathbb{Z}_q^2$
  - Number/modular theory on $\mathbb{Z}_q^2$: **the Dedekind psi function** and the projective line $\mathbb{P}_1(\mathbb{Z}_q)$

* **Multiple qudits**: 2-qubit, 3-qubit, 2-qutrit...

  - generalized quadrangle $GQ(2,2)$ and symplectic polar spaces

* **Mixtures of qudits**: qubit/ quartit, qubit/octit...

  - multiple copies of $GQ(2,2)$, $GQ(2,2)'$, ...

[2] On the Pauli graphs of N-qudits. *Quant. Inf. Comp.* **8**, 127-146 (2008)

[3] Pauli graphs when the Hilbert space dimension contains a square: why the Dedekind psi function? *J. Phys. A: Math. Theor.* **44**, 045301-16 (2011)

A few multiplicative number theoretical functions

- The **sum of divisors** function

$$\text{if } q = \prod_i p_i^{s_i} \text{ one gets } \sigma(q) = \prod_i \frac{p_i^{s_i+1} - 1}{p_i - 1}$$

- The **Dedekind psi** function

$$\psi(q) = q \prod_{p|q} (1 + \frac{1}{p}) \ (p \text{ prime}) \equiv \prod_i p_i^{s_i} (1 + \frac{1}{p_i})$$

.

One has $\psi(q) \leq \sigma(q)$ where the equality holds if q is square free.

e. g. $\sigma(4) = 1 + 2 + 4 = 7$ and $\psi(4) = 4(1 + \frac{1}{2}) = 6$.

The Pauli group $\mathcal{P}_q$ of a single qudit

- A **Weyl pair** (X, Z) of *shift* and *clock* operators

$$Z^q = X^q = I_q, \quad ZX - \omega XZ = 0,$$

where $\omega = \exp \frac{2i\pi}{q}$ is a primitive q-th root of unity.
In the *computational basis* $\{|s\rangle, s \in \mathbb{Z}_q\}$

$$X = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ . & . & \dots & . & . \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad Z = \mathrm{diag}(1, \omega, \omega^2, \dots, \omega^{q-1})$$

- In the **single qudit Pauli group** $\mathcal{P}_q = \langle X, Z \rangle$, of order q^3, each element may be written as $\omega^a X^b Z^c$, with $a, b, c \in \mathbb{Z}_q$.

Isotropic lines of the lattice $\mathbb{Z}_q^2$

- Isotropic line[4]: as a set of q points on $\mathbb{Z}_q^2$ such that the symplectic product of any two of them is $0 (\mathrm{mod}\ q)$. It corresponds a *maximal commuting set* in $\mathcal{P}_q/Z(\mathcal{P}_q)$.

  Taking the Hilbert space dimension as $q = \prod_i p_i^{s_i}$, the number of isotropic lines of the lattice $\mathbb{Z}_q^2$ reads

$$\eta(q) = \prod_i \frac{p_i^{s_i+1} - 1}{p_i - 1} \equiv \sigma(q)$$

[4] Albouy O. The isotropic lines of $\mathbb{Z}_d^2$. J. Phys. A: Math. Theor. 42,072001.

Projective line $\mathbb{P}_1(\mathbb{Z}_q)$ of the lattice $\mathbb{Z}_q^2$

- A isotropic line of $\mathbb{Z}_q^2$ corresponds to a *Lagrangian submodule*, i.e. a maximal module such that the perpendicular module $M^\perp = M$. For free cyclic submodules[5]

$$\mathbb{Z}_q(b,c) = \{(ub, uc) | u \in \mathbb{Z}_q\}$$

the application $u \longrightarrow (ub, uc)$ is injective.

- A point $x = (b, c)$ such that $\mathbb{Z}_q(b, c)$ is free is called a **admissible point**. Admissible points build the **projective line**

$$\mathbb{P}_1(\mathbb{Z}_q) = \{\mathbb{Z}_q(b,c) | (b,c) \text{ is admissible.}\}$$

Its cardinality is the the **Dedekind psi function** is

$$|\mathbb{P}_1(\mathbb{Z}_q)| = \prod_i (p_i^{s_i} + p_i^{s_i - 1}) \equiv \psi(q)$$

[5] H. Havlicek and M. Saniga. Projective line of an arbitrary single qudit. J. Phys. A: Math. Theor. 41,015302-14 (2008)

name	# cliques	geometry	spectrum	aut. group
quartit	$6+1$	$P_1(\mathbb{Z}_4)$	$\{4^1, 0^{3+1}, -2^2\}$	$G_{48} = \mathbb{Z}_2 \times S_4$
octit	$12+3$	$P_1(\mathbb{Z}_8)$	$\{8^1, 0^{9+3}, -4^2\}$	$\mathbb{Z}_2^6 \rtimes (\mathbb{Z}_3^3 \rtimes G_{48})$
9-dit	$12+1$	$P_1(\mathbb{Z}_9)$	$\{9^1, 0^{8+1}, -3^3\}$	$G_{648} \rtimes G_{48}$
12-dit	$24+4$	$P_1(\mathbb{Z}_{12})$	$\{12^1, 2^6, 0^{12+4}, -4^3, -6^2\}$	$\mathbb{Z}_2^{12} \rtimes G_{144}$
16-dit	$24+7$	$P_1(\mathbb{Z}_{16})$	$\{16^1, 0^{21+7}, -8^2\}$	$A_8^3 \rtimes G_{48}$
18-dit	$36+3$	$P_1(\mathbb{Z}_{18})$	$\{18^1, 3^6, 0^{24+3}, -6^3, -9^2\}$	$\mathbb{Z}_3^{12} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$
24-dit	$48+12$	$P_1(\mathbb{Z}_{24})$	$\{24^1, 4^6, 0^{36+12}, -8^3, -12^2\}$	$G_{2^{24}3^{12}} \rtimes (\mathbb{Z}_2^{12} \rtimes G_{144})$

- e.g. $q = 12 = 2^2 \times 3$, there are $12^2 - 1 = 143$ observables in $\mathcal{G}_{12}$, $\sigma(12) = 28$ max. cliques in $\mathcal{G}_{12}$ and $\mathbb{P}_1(\mathbb{Z}_{12}) = 24$.
  * The 24 max. cliques intersect at $0, 1, 2, 3$, or 5 points,
  $\mathrm{aut}(\mathbb{P}_1(\mathbb{Z}_2^{12})) = \mathbb{Z}_2^{12} \rtimes G_{144}$ with $G_{144} = A_4 \rtimes D_6$.

Pauli graphs of multiple qudits

$q = p^n$	name	$\mathrm{aut}(\mathcal{G}_{p^n})$	$\mathrm{aut}(\mathcal{G}^*_{p^n})$	$\mathrm{aut}(\mathcal{G}'^*_{p^n})$	$c = \frac{\lvert\mathrm{aut}(\mathcal{G}^*_{p^n})\rvert}{\lvert\mathrm{aut}(\mathcal{G}'^*_{p^n})\rvert}$
2	qubit	S_3	S_3	S_2	$3 \equiv \sigma(2)$
2^2	2-qubit	S_6	S_6	$G_{48} = \mathbb{Z}_2 \times S_4$	$15 \equiv \sigma(2^3)$
2^3	3-qubit	$Sp(6,2)$	$O^+(8,2)$	$\mathbb{Z}_2^6 \rtimes A_8$	$2 \times 135 \neq 63$
3	qutrit	$\mathbb{Z}_2^3 \rtimes G_{48}$	S_4	S_3	$4 \equiv \sigma(3)$
3^2	2-qutrit	$\mathbb{Z}_2^{40}.W(E_6)$	$W(E_6)$	$G_{648} \rtimes \mathbb{Z}_2$	$40 \equiv \sigma(3^3)$
3^3	3-qutrit	$\mathbb{Z}_2^{364}.G$	G	$(E_{243} \rtimes \mathbb{Z}_2).W(E_6)$	$364 \equiv \sigma(3^5)$

- Comparison of the automorphism group of the dual Pauli graph $\mathcal{G}^*_{p^n}$ and that of its *building block* $\mathcal{G}'^*_{p^n}$, defined by removing a perp-set in the symplectic polar space.

Multiple qudit mixtures

q	name	# cliques	geometry	spectrum	aut. group
2^2	2-qubit	15	$GQ(2,2)$	$\{6^1, 1^9, -3^5\}$	S_6
2.2^2	qubit/quartit	$36+3$	$3 \times GQ(2,2)'$	$\{5^1, 1^6, -1^2, -3^3\}^3$	$G_{48}^3 \rtimes S_3$
2^3	3-qubit	135	$W_5(2)$	$\{30^1, 3^{35}, -5^{27}\}$	$Sp(6,2)$
3^2	2-qutrit	40	$GQ(3,3)$	$\{25^1, 5^{24}, -1^{40}, -7^{15}\}$	$\mathbb{Z}_2^{40}.W(E_6)$
3.4	qutrit/quartit	$24+4$	as a 12-dit	as a 12-dit	as a 12-dit
$2^2.3$	2-qubit/qutrit	60	$4 \times GQ(2,2)$	$\{6^1, 1^9, -3^5\}^4$	$S_6^4.S_4$
2.8	qubit/octit	$72+15$	$6 \times GQ(2,2)'$	$\{5^1, 1^6, -1^2, -3^3\}^6$	$G_{48}^6.S_6$
4.4	2-quartit	$120+30+1$	15-cube	$\{-3^1, 3^1, -1^3, 1^3\}^{15}$	$G_{48}^{15} \rtimes S_{15}$
$2^2.4$	2-qubit/quartit	$360+15$	$3 \times W_5(2)'$	$\{13^1, 5^{25}, 3^9, -1^{70}, -5^5, -7^{10}\}^3$	$(\mathbb{Z}_2^5 \rtimes S_6)^3 \rtimes S_3$
2^4	4-qubit	2295	$W_7(2)$	$\{126^1, 7^{135}, -9^{119}\}$	$Sp(8,2)$
2.9	qubit/9-dit	$36+3$	as a 18-dit	as a 18-dit	as a 18-dit
2.3^2	qubit/2-qutrit	120	$3 \times GQ(3,3)$	$\{12^1, 2^{24}, -4^{15}\}^3$	$W'(E_6)^3.G_{48}$
2.3.4	2/3/4-dit	$144+12$			
$2^3.3$	3-qubit/qutrit	540	$4 \times W_5(2)$	$\{56^1, 14^{15}, 2^{35}, -4^{84}\}^4$	$Sp(6,2)^4.S_4$

Abstract [6]

We point out a organic relationship between real entangling n-qubit gates of quantum computation and the group of automorphisms of even Euclidean lattices Λ of the corresponding dimension 2^n. The type of entanglement that is found in the gates/generators of $Aut(\Lambda)$ depends on the lattice. In particular, we investigate $\mathbb{Z}^n$ lattices, Barnes-Wall lattices $D4$, $E8$, 16 (associated to $n = 2$, 3 and 4 qubits), and the Leech lattices $h24$ and 24 (associated to a 3-qubit/qutrit system). Balanced tripartite entanglement is found to be a basic feature of $Aut(\Lambda)$, a finding that bears out our recent work related to the Weyl group of E8.

[6] Preprint 1002.4287 [quant-ph]