Computing with Infinite Groups

with Applications to Quantum Computation

Emmanuel Jeandel

LIP, École Normale Supérieure de Lyon (France)

emmanuel.jeandel@ens-lyon.fr

CONTENTS

- Definitions : Gates, completeness.
- Algorithm to test for completeness.
  - Problem in terms of algebraic groups;
  - Previously known algorithms for infinite groups;
  - The algorithm.

- A qubit is a vector of norm 1 in $\mathbb{C}^2$.

  The canonical basis of $\mathbb{C}^2$ is denoted by $|0\rangle$, $|1\rangle$.

  The qubit $\phi = \alpha|0\rangle + \beta|1\rangle$ represents a system which is simultaneously in the states 0 and 1, with respective amplitudes α and β. If the system is observed, it becomes the constant qubit $|0\rangle$ with probability $|\alpha|^2$ and the constant qubit $|1\rangle$ with probability $|\beta|^2$.

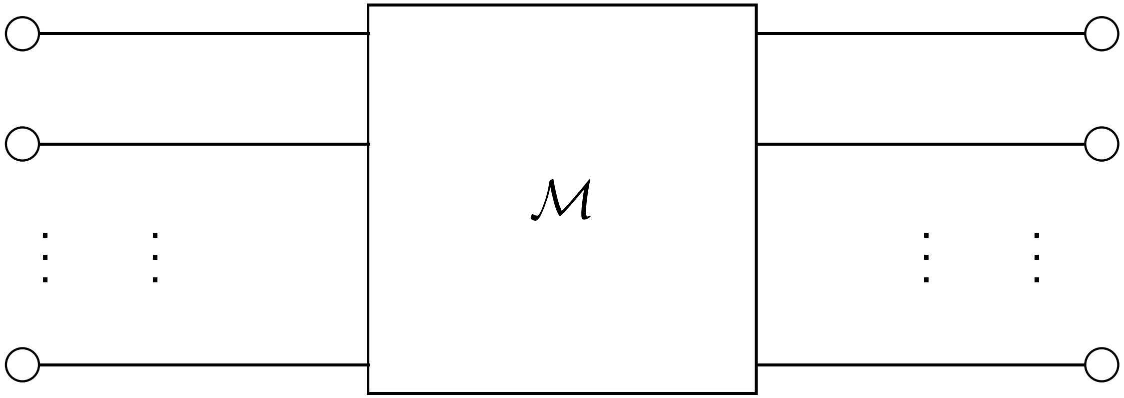
- A quantum state is a vector of norm 1 in $(\mathbb{C}^2)^{\otimes n}$. The canonical basis of $(\mathbb{C}^2)^{\otimes n}$ will be denoted by $|\omega\rangle$ where ω is a word over $\{0,1\}$ of length n .

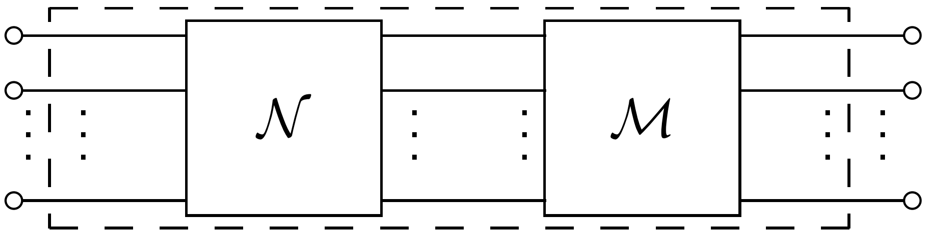
- A quantum state is then a vector $\phi = \sum_\omega \alpha_\omega |\omega\rangle$ with $\sum |\alpha_\omega|^2 = 1$.

QUANTUM COMPUTATION (3)

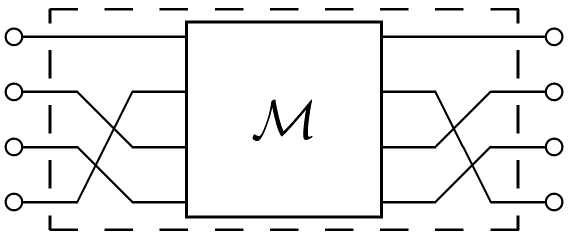
- A quantum gate M represents the basic operation on a quantum state. It is an operation that maps quantum states into quantum states.
- Due to the particular structure of quantum states, a quantum gate M over n qubits is a unitary matrix of dimension 2^n. (More exactly, a quantum gate is an element of U_{2^n}/U_1)
- A quantum circuit over S is a circuit obtained from quantum gates M_i in S by applying a finite set of operations.

A QUANTUM GATE

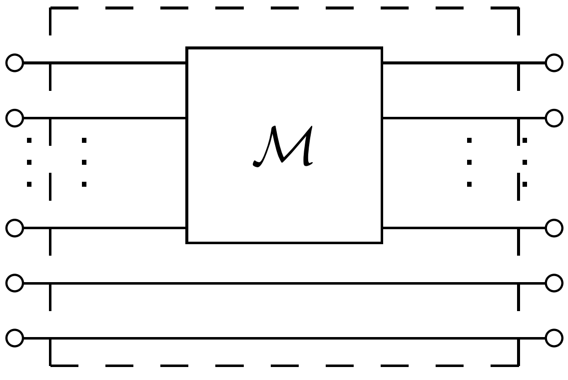




(a) The multiplication $\mathcal{MN}$ (composition of circuits)



(b) $\mathcal{M}[\sigma]$ (permutations of wires)



(c) The operation $\mathcal{M} \otimes \mathcal{I}$

- Let S be a (finite) set of gates over n qubits.
- Denote by $\mathcal{G}_p(S)$ the set of gates over p qubits obtained by circuits over S, and by $\overline{\mathcal{G}}_p(S)$ its euclidean closure (the set of gates we can approximate by circuits over S).
- $\mathcal{G}_p(S)$ is generated by all matrices of the form $(M \otimes \mathcal{I}_{n-p})[\sigma]$, where $M \in S$, hence is finitely generated if S is.
- S is said to be complete if every gate over n qubits can be obtained from S : $\overline{\mathcal{G}}_n(S) = U_{2^n}$ or more accurately $U_1\overline{\mathcal{G}}_n(S) = U_{2^n}$.

- The set of all gates over 2 qubits.
- Barenco, 1995 : The gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

Where ϕ, α, θ are fixed irrational multiples of π and of each other.

How to prove that the set S is complete ?

- Show how to approximate every unitary operation by a quantum circuit in S ;
- Given a complete set S', show how to approximate every operation of S' by quantum circuits ;
- Use specific properties of $\mathcal{G}(S)$, the set of quantum circuits generated by S (object of this talk)

STRUCTURE OF $\mathcal{G}(S)$

- $\mathcal{G}(\mathcal{S})$ is finitely generated, given that S is finite;
- $\overline{\mathcal{G}}(S)$ is always a group (we can approximate the gate A^{-1} by successive iterations of the gate A) ;
- $\overline{\mathcal{G}}(S)$ is even a compact group, hence algebraic : There exists polynomials $p_1 \ldots p_k$ in x_{ij} (entries of the matrix) such that

$$M \in \overline{\mathcal{G}}(S) \iff p_1(M) = p_2(M) = \ldots = p_k(M) = 0$$

- [Derksen, EJ, Koiran, 2003] There exists a general algorithm that compute polynomials p_i for finitely generated algebraic groups. However, the complexity of the algorithm makes him uninteresting for practical purposes;

COMPLETENESS IN TERMS OF GROUPS

- Deciding if a finite set of gates is complete is the same as deciding if a finitely generated subgroup of U_n is dense in U_n
- More generally, how to prove that some finitely generated subgroup of an algebraic group G is dense in G ?

Density in algebraic groups is defined with the Zariski Topology : H is dense in G if every polynomial which is identically zero on H vanishes on G.

EASY THINGS TO COMPUTE

What are we able to compute about finitely generated matrix groups ?

- [Babai, Beals and Rockmore, 1993] There exists a polynomial time algorithm that decides if such a group is finite ;
- [Beals, 1997] There exists a polynomial time algorithm that decides if such a group is abelian-by-finite, nilpotent-by-finite. . .
- [Ge, 1993] There exists a polynomial time algorithm that decides if two finitely generated groups of diagonal matrices generate the same algebraic group.

Inputs are assumed to be in a finite extension $\mathbb{F}$ of $\mathbb{Q}$, given by an irreducible polynomial.

Our problem, for a given group G and a finite extension $\mathbb{F}$ of $\mathbb{Q}$:

- Input : Matrices $X_1 \dots X_m \in \mathrm{GL}_n(\mathbb{F})$.

  $X_1 \dots X_m$ generate an algebraic group H over $\mathbb{C}$.

- Problem : Is $H = G$?

Is there a polynomial time algorithm to solve this problem ?

As G, $\mathbb{F}$ and n are **not** part of the input, complexity is in terms of the size of the coefficients of the matrices.

- For which group G is there a polynomial time algorithm ?

Due to Ge's algorithm, we know this is true when G is a group of diagonal matrices.

Easy things to compute (2)

- Given generators of G, we can easily compute $\operatorname{env} G$, the vector space generated by the matrices in G.
  - Set $E = \mathbb{R}\mathcal{I}$.
  - While there exists $\mathcal{X}_i$ such that $E \neq \mathcal{X}_i E$, then $E = E + \mathcal{X}_i E$
- We can also easily compute $\operatorname{env} \phi(G)$ for any morphism ϕ.
- We may obtain in this way a representation of $G/Z(G)$: Consider the morphism ψ such that $\psi(M)$ is the matrix that represents the automorphism $\operatorname{env} G : X \mapsto MXM^{-1}$

$$\begin{aligned}
\psi(M) = I \quad &\iff \quad \forall X \in \operatorname{env} G, MXM^{-1} = X \\
&\iff \quad \forall X \in G, MXM^{-1} = X \\
&\iff \quad M \in Z(G)
\end{aligned}$$

Density for simple groups

- Let G be a simple (connected) group, that is G has no normal non trivial subgroup.
- To prove that H is dense in G, it is therefore sufficient to prove that the algebraic group generated by H is a normal subgroup of G and that H is infinite.
- Denote by $\phi(X)$ the automorphism $\mathcal{M} \mapsto \mathcal{X}\mathcal{M}\mathcal{X}^{-1}$. We want to know if $\forall X \in G, \phi(X)H = H$.
- As H is obviously a normal subgroup of H, it is enough to prove $\phi(\overline{H}) = \phi(G)$.

Simple groups (cont'd)

- Idea : Test only if they span the same (linear) subspace.

$\boxed{H \text{ is dense in } G \text{ if and only if } H \text{ is infinite and } \mathrm{env}\ \phi(H) = \mathrm{env}\ \phi(G)}$

- Sketch of Proof : We use the Lie group structure of G : Instead of testing if $\overline{H} = G$, we test if the two groups have the same Lie Algebra.

  The condition ensures that the Lie Algebra $\mathfrak{h}$ of H is an ideal of the Lie Algebra $\mathfrak{g}$ of G, which is a simple Lie Algebra. Hence $\mathfrak{h} = \mathfrak{g}$ or $\mathfrak{h} = 0$. As H is infinite, the latter is not possible.

For every simple group G, there exists a polynomial time algorithm which decides if a finitely generated group H of G is dense in G.

- All the classical groups $\mathrm{SO}_n, n \geq 3, \mathrm{SU}_n, n \geq 2$ are standard examples of simple groups, with the remarkable exception of the group SO_4.
- The isometry group of the isocahedron, which may be seen as a finite subgroup of SO_3 provides an example of a finite group H such that $\mathrm{env}\ \phi(H) = \mathrm{env}\ \phi(G)$.

- A semisimple group G has only finitely many normal subgroups G_i.

H is dense in G if and only if $\mathrm{env}\ \phi(H) = \mathrm{env}\ \phi(G)$ and for all normal subgroups G_i, H/G_i is infinite

- To test if H/G_i is infinite, we need a representation of G/G_i that is a morphism $\psi_i : G \mapsto \mathrm{GL}_p$ such that $\psi(X) = I \iff X \in G_i$. The existence of such a morphism is guaranteed by classical theorems.

For every semisimple group G, there exists a polynomial time algorithm which decides if a finitely generated group H of G is dense in G.

The algorithm depends of the given group G, as we need the morphisms ψ_i.

- SO_4 contains two normal subgroups

$$\sigma_1(a,b,c,d) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \sigma_2(a,b,c,d) = \begin{pmatrix} a & b & c & -d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

$G_i = \left\{\sigma_i(a,b,c,d), a^2+b^2+c^2+d^2=1\right\}$ for $i \in \{1,2\}$

- The representation of G/G_1 is given by

$$\begin{array}{llll} \psi_1 : & SO_4 & \mapsto & SO_4 \\ & \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} & \mapsto & \sigma_1(a,b,c,d)^T \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} \end{array}$$

- Testing if H is dense in SO_4 is equivalent to $\mathrm{env}\ \phi(H) = \mathrm{env}\ \phi(G)$ and $\psi_1(H)$ and $\psi_2(H)$ are infinite.

- A connected reductive group G is such that $G = Z(G)D(G)$ where $D(G)$ is the derived group of G. Furthermore, $G/Z(G)$ is semisimple, and $G/D(G)$ is a commutative diagonalisable group.

For every connected reductive group G, there exists a polynomial time algorithm which decides if a finitely generated group H of G is dense in G : Simply decide if $H/Z(G)$ and $H/D(G)$ are dense in $G/Z(G)$ and $G/D(G)$.

The algorithm depends of the given group G, as we need representations of $G/D(G)$ and $G/Z(G)$.

- Denote by G a non-connected group and by G^0 the connected component containing the identity matrix. Choose for each connected component a matrix Y_j.
- Let H be the group generated by the matrices X_i. Choose for each connected component of G a matrix $Y_j \in H$. If no such matrix exists, then H is not dense in G.

  $H \cap G^0$ is generated by the matrices $Y_i X_j Y_k^{-1}$ that belong to G^0.

  (Schreier's Theorem)
- Computing the matrices Y_j is easy as G/G^0 is finite. Deciding if H is dense is then equivalent to decide $H \cap G^0$ is dense.

For every reductive group G, there exists a polynomial time algorithm which decides if a finitely generated group H of G is dense in G. The algorithm depends of the given group G ;

Compact groups are reductive :

For every compact group G, there exists a polynomial time algorithm which decides if a finitely generated group H of G is dense in G. The algorithm depends of the given group G.

- For any n, there exists a polynomial time algorithm which decides if a set of gates over n qubits is complete : Consider it as a problem about compact groups and solve it using the previous algorithm;
- We only need to use the previous algorithms for simple groups ;
- We may even get a better result : there exists a polynomial time algorithm which decides if a set of gates over n qubits is complete.
- Note : The algorithm is polynomial on the size of the input, which is exponential in n.

Summary

- An algorithm which decides if a finitely generated subgroup of a compact group G is dense in G.
- An algorithm which decides if a finite set of gates is complete.
- Generalise the algorithm for any algebraic group ?
- Give an algorithm for other models of computation (black box groups, computation with reals).