Group Order is in QCMA

Joint work with François Le Gall and Harumichi Nishimura

To appear in FOCS 2025

Dhara Thakkar
Graduate School of Mathematics, Nagoya University

September 24th, 2025

Shenzhen-Nagoya Workshop on Quantum Science 2025

Groups

A finite group G is a finite set of elements together with a binary operation $(\cdot)$ that satisfy following group axioms:

- Closure : For all x, y in $G, (x \cdot y) \in G$.
- Associativity : For all x, y and z in G, $(x \cdot (y \cdot z)) = ((x \cdot y) \cdot z)$.
- Identity : There exists an element e in G such that, for every element a in G, the equation $(a \cdot e) = (e \cdot a) = a$ holds.
- Inverse : For each x in G, there exists an element y in G such that $(x \cdot y) = (y \cdot x) = e$.

Group Representations

- Cayley Table representation:

*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

- Permutation Group representation: $G = \langle \pi_1, \ldots, \pi_t \rangle \leq S_n$
- Matrix Group representation: $G = \langle M_1, \ldots, M_t \rangle \leq \mathrm{GL}(d, q)$
- Black-box Group Representation

One of the most general ways to work with finite groups

□ Depending on what representation is used a computational problem can become very easy or extremely challenging.

Black-box Representation:

- $G = \langle g_1, \ldots, g_t \rangle$
- Each element of G is represented by a binary string of length $O(\log|G|)$ bits.
- We have two oracles available at unit cost:
  - String representing g and g' $\rightarrow$ [Multiplication Oracle] $\rightarrow$ String representing gg'.
  - String representing g $\rightarrow$ [Inverse Oracle] $\rightarrow$ String representing g^{-1}.

☐ In the quantum setting,

- we can feed quantum superpositions of elements to the oracles
- we assume that each element is encoded by a unique binary string (as in all prior works).

☐ Since the group is generated by $O(\log|G|)$ elements, the input size is $O(\log|G|)^2$ bits.

Group Order

Input: A group G as a black-box representation.

Question: Compute $|G|$

Group Order Verification

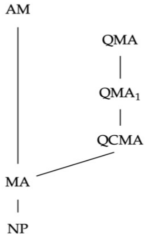
Input: A group G as a black-box representation and an integer m.

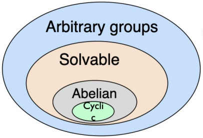
Question: Decide if $|G| = m$

- One of the most fundamental problem over groups

Prior Work

- Classical bounds:
  - Requires exponential time (in $\log|G|$), even for cyclic groups
  - Best upper bound on its complexity is the class AM. [Babai 1992]
- Quantum polynomial time algorithms:
  - Cyclic groups [Shor 1994]
  - Abelian groups [Kitaev 1995]
  - Solvable groups [Watrous 2000]





An Open Question:

What about arbitrary groups? Is it in QMA [Watrous 2000]?

Our Result: Group Order Verification is in QCMA!

Group Membership

Input: A group G as a black-box representation, $H \leq G$, and $g \in G$.

Question: Decide if $g \in H$

Group Non-Membership

Input: A group G as a black-box representation $H \leq G$, and $g \in G$.

Question: Decide if $g \notin H$

- Group Membership is in NP [Babai and Szemerédi, 1984]
- Group Non-Membership is in QMA [Watrous, 2000]
- Group Non-Membership is in QCMA under some group-theoretic assumptions [Aaronson and Kuperberg, 2007]
- **Conjecture**: Group Non-Membership is in QCMA
- Solved!
  Algorithm for Group Order gives a way to check Membership

$$g \in H \text{ if and only if } |\langle H, g\rangle| = |H|$$

Proof Strategy

Group Order Verification: A group G as a black-box representation and an integer m. Decide if $|G| = m$.

- ☐ Group Order **Divisor** Verification: Decide if m divides $|G|$.
- ☐ Group Order **Multiple** Verification: Decide if $|G|$ divides m.

Theorem 1 Group Order Divisor Verification is in QCMA.

Proof Idea:

- Let $m = p_1^{a_1} \cdots p_r^{a_r}$ be the prime decomposition of m.
- Claim: m divides $|G|$ iff G has a subgroup H_i if order $p_i^{a_i}$, for each i.
- A group of order p^a, for a prime p and integer a is solvable.
- The prover sends a set of generators for each H_i.
- The verifier checks that H_i solvable, and then check if $|H_i| = p_i^{a_i}$ using Watrous' algorithm for solvable groups.

Theorem 2 Group Order Multiple Verification is in QCMA.

⋆ Remaining part of the talk.

Checking that $|G|$ divides m: Strategy

- A group with no nontrivial normal subgroup is called Simple group.
- A composition series of G is a list of subgroups $H_0, H_1, \dots, H_s$ for some integer s, such that
  - $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$;
  - the quotient group H_i/H_{i-1} is **simple group** for each $i \in [s]$.
- Each group has a composition series but it is unknown how to compute it efficiently.
- $|H_0| \cdot |H_1/H_0| \cdot |H_2/H_1| \cdots |H_s/H_{s-1}| = |G|$

This suggests a strategy to compute $|G|$

(i) ask the prover to send a composition series

(ii) check that each H_i/H_{i-1} is simple and compute its order

Remark: The "classification theorem of finite simple groups" (about 15,000-page long proof) states that every finite simple group belongs to one of 18 infinite families of simple groups, or is one of 26 sporadic simple groups. As a consequence, each simple group can be described by a short string called its standard name (its order can be easily obtained from its standard name).

(i) Ask the prover to send a composition series and the standard name w_i of H_i/H_{i-1}

(ii) Check: H_i/H_{i-1} is isomorphic to the simple group with standard name w_i

- For the 26 sporadic simple groups this is trivial (since they have constant order)
- For 17 of the infinite families, this can be done in classical polynomial time using a classical witness using the presentation-test (witness: a short presentation of the simple group in terms of generators and relations)
- We do not know how to do it for the "Ree groups", since it is unknown if Ree groups have a short presentation

Use a randomized homomorphism test.

- The family Ree groups of rank 1 indexed by a positive integer a. Write $q = 3^{2a+1}$. The Ree group of rank one, which we denote by $\mathrm{R}(q)$, is the subgroup of $\mathrm{GL}(7, q)$ generated by the following three matrices:

$$\Gamma_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 1 & 1 & 1 & -1 & 0 & -1 \\ 0 & 0 & 1 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \Gamma_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\Gamma_3 = \begin{bmatrix} \omega^t & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^{1-t} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^{2t-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^{1-2t} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^{t-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega^{-t} \end{bmatrix},$$

where $t = 3^a$ and ω be a primitive element of $\mathbb{F}_q$. The order of $\mathrm{R}(q)$ is $q^3(q^3 + 1)(q - 1)$.

Second Trial: Randomized Homomorphism Test for the Ree Group

Goal: check if a group Σ is isomorphic to a known group S (think of $\Sigma = H_i/H_{i-1}$ and $S = \langle s_1, \ldots, s_k \rangle = \mathrm{R}(q)$).

- We ask Prover to send elements $g_1, \ldots, g_k \in \Sigma$.
- If $\Sigma \cong S$ and Prover is honest, he will send $g_i = \phi(s_i)$ for each $i \in [k]$, for some isomorphism $\phi \colon S \to \Sigma$.
- For the checking procedure, Verifier defines a map $f : S \to \Sigma$ by extending the partial map $s_i \mapsto g_i$ into a map on all S as if it were a homomorphism.
- For instance, for an element $s \in S$ that can be written as $s = s_1 s_2 s_1 s_3$, Verifier will set $f(s) = g_1 g_2 g_1 g_3$.
- Verifier takes two elements s and s' uniformly at random in S and checks if

$$f(ss') = f(s)f(s') \iff f(ss')f(s')^{-1}f(s)^{-1} \in H_{i-1} \qquad (1)$$

To be successful, this approach has to satisfy three important requirements:

A. Verifier needs to be able to efficiently represent an arbitrary element $s \in S$ as a product of elements from the fixed set $\{s_1, \ldots, s_k\}$. This representation should also be unique for f to be well-defined.
   - For $S = \mathrm{R}(q)$ ([Babai, Beals, Seress 2009]+ quantum algorithms)

B. Verifier needs to be able to efficiently check that the homomorphism is actually an isomorphism, i.e., a bijection.
   - "easy" for S = R(q) (since a simple group has no nontrivial normal subgroup)

C. Verifier needs to be able to efficiently check if $f(ss')f(s')^{-1}f(s)^{-1} \in H_{i-1}$ holds.
   - Seems hard for arbitrary H_{i-1}, but Membership testing in Solvable group is in BQP [Watrous, 2000]

(Modified) Babai-Beals filtration [Babai and Beals, 1999]:

For any group G, there exists a solvable subgroup H_0 and elements $\beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_s \in G$ such that when defining $H_i = \langle H_0, \beta_1, \gamma_1, \ldots, \beta_i, \gamma_i \rangle$ for each $i \in [s]$ we have

$$\{e\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s \trianglelefteq \mathrm{Pker}(G) \trianglelefteq G$$

- $G/\mathrm{Pker}(G) \leq Sym(s)$
- $\mathrm{Pker}(G)/H_s$ solvable;
- Each H_i/H_{i-1} is simple;
- $H_i/H_{i-1} \cong \langle H_0, \beta_i, \gamma_i \rangle / H_0$, for all $i \in [s]$

Group Order Verification

Input: A group G as a black-box representation and an integer m.

Question: Decide if $|G| = m$

Open Problem [Watrous, 2000]
Is Group Order Verification in QMA? SOLVED!

Group Non-Membership

Input: A group G as a black-box representation, $H \leq G$, and $g \in G$.

Question: Decide if $g \notin H$

Conjecture [Aaronson and Kuperberg, 2007]
Group Non-Membership is in QCMA. SOLVED!

Thank you! Questions?