The Quantum Complexity of Group Testing

Sebastian Dörn [1] Thomas Thierauf [2]

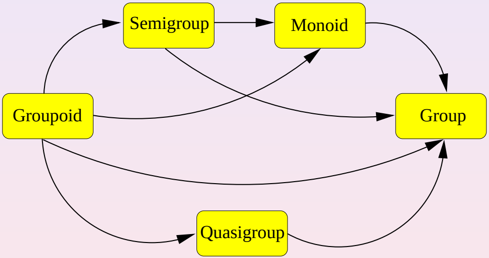
[1] Inst. für Theoretische Informatik, Universität Ulm

[2] Fak. Elektronik und Informatik, HTW Aalen

21. January 2008

Our Work

- Prove quantum complexity lower and upper bounds for algebraic properties.
- Consider decision problems whether a given structure is in fact a group.



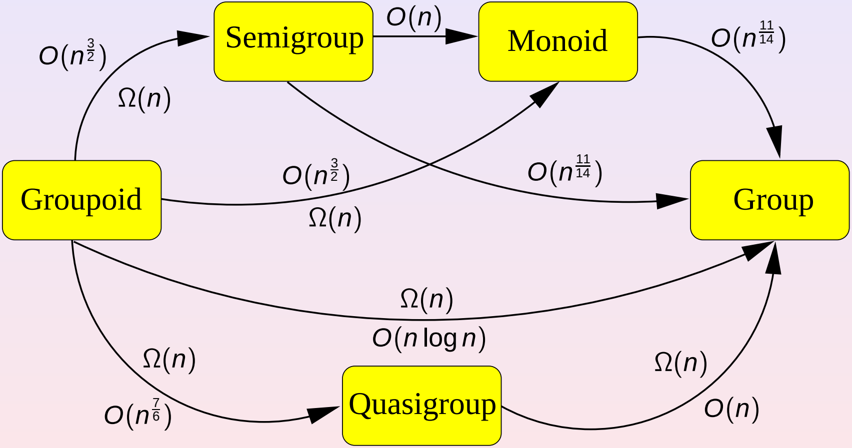
- Give quantum complexity bounds for testing distributivity and commutativity.

Some Algebraic Facts

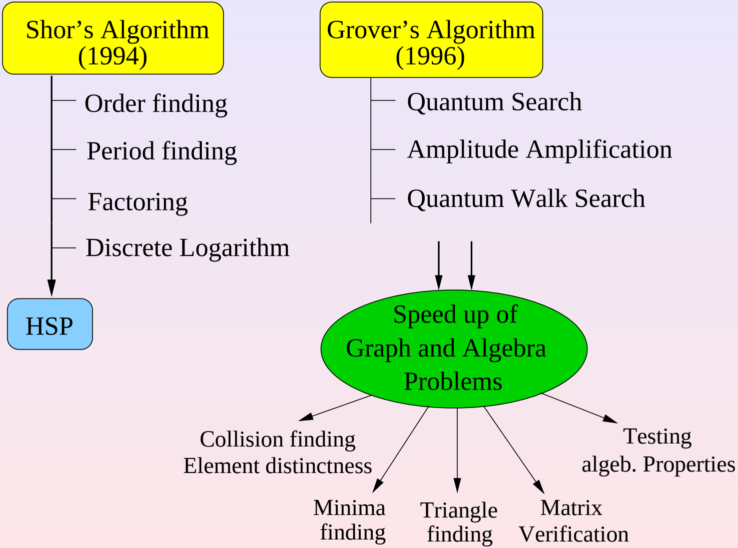
Input: Operation table for set S of size $n \times n$.

- Groupoid: finite set S with a binary operation $\circ$.
- Semigroup: associative groupoid.
- Monoid: semigroup with an identity element e.
- Quasigroup: groupoid where all equations $a \circ x = b$ and $x \circ a = b$ have unique solutions.
- Group: associative quasigroup.

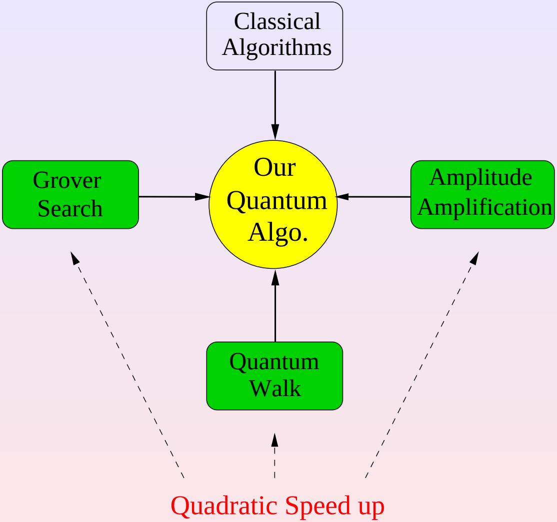
Our Main Results



Quantum Algorithms



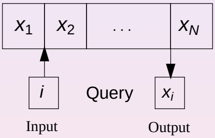
Our Quantum Algorithms



Classical vs. Quantum Query Model

Classical Query Model.

- Pay for access black box:



- Compute Boolean func. on input by minimizing number of queries.

Quantum Query Model.

- Pay for access black box.
- Queries in superposition.
- Quantum parallelism.

$$\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i,0\rangle \xrightarrow{O_x} \frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i,x_i\rangle$$

Quantum Query Complexity.

- Number of quantum queries to the black box.

Quantum Time Complexity.

- Number of ”basic” quantum operations.

Group Testing

Input: Operation table of a groupoid S.

Question: Decide whether S is a group.

Classical Algorithm: $\widetilde{O}(n^2)$, Rajagopalan & Schulman, 2000

Theorem

Whether a groupoid is a group requires $\Omega(n)$ quantum queries.

Theorem

Whether a groupoid is a group can be decided with $O(n \log n)$ expected quantum queries.

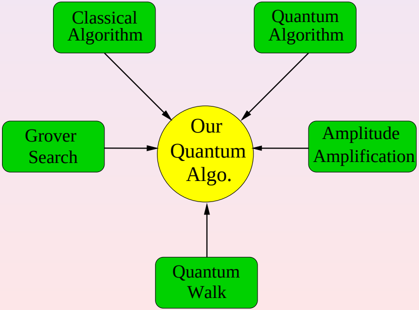
Input: Operation table of a groupoid S.

Question: Decide whether S is a group.

Theorem

Whether a groupoid is a group can be decided by a quantum algorithm within $O(n^{\frac{13}{12}} \log^c n)$ expected steps, for constant c.

Proof.



Definition

Let $(S, \circ)$ be a groupoid represented by its operation table T. A row of T is called cancellative, if it is a permutation of S.

Lemma

Let $\circ$ be cancellative in r rows. If $\circ$ is nonassociative, then it has at least $r/4$ nonassociative triples.

1. Choose $A \subset S$ (size r) and check if $T(A,*)$ is cancellative.
2. If there is noncancellative row $\Rightarrow$ **No Group**.
3. Choose $a, b, c \in S$ and check if triple is associative.
4. Using quantum amplitude amplification.
5. If there is nonassociative triple $\Rightarrow$ **No Group**.
6. Check if semigroup is a group.

Quantum Time Complexity:

$$O\left(\sqrt{r}n^{\frac{2}{3}}\log^c n + \sqrt{\frac{n^3}{r}} + n^{\frac{11}{14}}\log n\right) = O(n^{\frac{13}{12}}\log^c n) \quad \text{for } r = n^{\frac{5}{6}}$$

1. Choose $A \subset S$ (size r) and check if $T(A, *)$ is cancellative.
2. If there is noncancellative row $\Rightarrow$ **No Group**.
3. Choose $a, b, c \in S$ and check if triple is associative.
4. Using quantum amplitude amplification.
5. If there is nonassociative triple $\Rightarrow$ **No Group**.
6. Check if semigroup is a group.

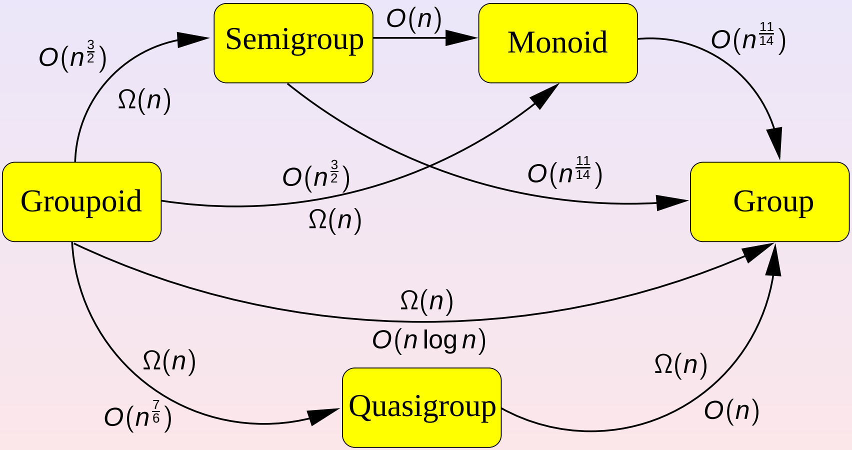
Quantum Time Complexity:

$$O\left(\sqrt{r}n^{\frac{2}{3}}\log^c n + \sqrt{\frac{n^3}{r}} + n^{\frac{11}{14}}\log n\right) = O(n^{\frac{13}{12}}\log^c n) \text{ for } r = n^{\frac{5}{6}}$$

More Results

- Present quantum algorithm to check whether a given semigroup is a group.
- Show that quasigroup is a group can be decided with $\Theta(n)$ quantum queries.
- Improve the quantum query complexity of associativity testing by a more detailed analysis.
- Present quantum complexity bounds for distributivity and commutativity problem.

Conclusion



Semigroup
Monoid
Groupoid
Group
Quasigroup
$O(n)$
$O(n^{\frac{11}{14}})$
$O(n^{\frac{3}{2}})$
$\Omega(n)$
$O(n^{\frac{3}{2}})$
$O(n^{\frac{11}{14}})$
$\Omega(n)$
$\Omega(n)$
$O(n \log n)$
$\Omega(n)$
$O(n^{\frac{7}{6}})$
$\Omega(n)$
$O(n)$