Fearful Symmetries: Factoring, Graph Isomorphism, and Quantum Computing

Cristopher Moore, University of New Mexico and the Santa Fe Institute

Joint work with
Alexander Russell, University of Connecticut
Daniel Rockmore, Dartmouth
Leonard J. Schulman, Caltech
Physics

Problems:
- come from Nature
- have solutions that are as simple, symmetric, and beautiful as possible (far more so than we have any right to expect)

Fig. 1: Nature
Computer Science

Problems:

- are artificial
- are maliciously designed to be the worst possible
- may or may not have elegant solutions...
- ...or proofs (cf. Erdős)

Fig. 2: The Adversary
In 1928, Dirac saw that the simplest, most beautiful equation for the electron has \textit{two} solutions.

Four years later, the positron was found in the laboratory.
Conservation is Symmetry

\[ \frac{dx}{dt} = \frac{\partial H}{\partial p}, \quad \frac{dp}{dt} = -\frac{\partial H}{\partial x} \]

perhaps you are more familiar with \( p = mv \)
and \( F = ma \); try with \( H = (1/2)mv^2 + V(x) \)

Conservation of momentum follows from translation invariance:

moving entire world by \( dx \) \( \frac{dp}{dt} = -\frac{\partial H}{\partial x} = 0 \)
doesn’t change energy
Conservation is Symmetry

Noether’s Theorem: symmetry implies conservation

\[
\frac{d\theta}{dt} = \frac{\partial H}{\partial J} \quad , \quad \frac{dJ}{dt} = -\frac{\partial H}{\partial \theta}
\]

Conservation of angular momentum follows from symmetry under rotation!
In classical and quantum mechanics, *all* conservation laws are of this form.
Relativity is Symmetry

Physics is invariant under changes of coordinates to a moving frame:

$$\begin{pmatrix} x \\ ct \end{pmatrix} \rightarrow \gamma \begin{pmatrix} 1 & -v/c \\ -v/c & 1 \end{pmatrix} \begin{pmatrix} x \\ ct \end{pmatrix}$$

at small velocities, Galileo:

$$x \rightarrow x - vt \ , \ t \rightarrow t$$
Symmetry in Computer Science?

- In Physics, finding the right symmetry often solves the problem.

- In Computer Science, we are used to a different notion of
  - instance (arbitrary graphs vs. lattices)
  - answer (algorithm vs. closed form)

- But in Quantum Computing, symmetry plays a key role.
Symmetry Groups

A *group* is a mathematical structure with:

- **associativity**: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **identity**: $a \cdot 1 = 1 \cdot a = a$
- **inverses**: $a \cdot a^{-1} = a^{-1} \cdot a = 1$
- **but not necessarily** $a \cdot b \neq b \cdot a$

(These are *non-Abelian* groups)
Some Common Groups

- cyclic: $\mathbb{Z}_n$ (addition mod n), $\mathbb{Z}_n^*$ (multiplication)
- symmetric group (permutations): $S_n$, $A_n$
- invertible matrices
- rotations: $O(3)$
- $O(3)$ contains $A_5$!
Symmetry Groups

Transformations that leave an object fixed:

\[ \mathbb{Z} \times \mathbb{Z} \quad D_8 \quad S_5 \]
Symmetries of Functions

Given a function on a group $f : G \to X$, we can ask for which elements $h$ we have

$$\forall g : f(g) = f(gh)$$

E.g. if $G = \mathbb{Z}_n$, find $h$ s.t.

$$\forall x : f(x) = f(x + h)$$

These $h$ form a subgroup $H \subseteq G$, multiples of the periodicity of $f$. 
Periodicity Gives Factoring!

To factor $n$, let $f(x) = c^x \mod n$.

Find smallest $r$ such that $f(x) = f(x + r)$, i.e., $c^r \equiv 1 \mod n$. Suppose $r$ is even:

$$c^r - 1 = kn = \left(\frac{c^r}{2} + 1\right)\left(\frac{c^r}{2} - 1\right)$$

Now take g.c.d. of $n$ with both factors.

Works at least 1/2 the time with random $c$!
Factoring: An Example

Let’s factor 15. Choose $c=2$:

\[
x : \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \\
2^x : \quad 1 \quad 2 \quad 4 \quad 8 \quad 1 \quad 2 \quad 4 \quad 8 \quad 1
\]

\[
2^4 - 1 = 15 = (2^2 - 1)(2^2 + 1) = 3 \times 5
\]

Bad news: in general $r$ could be as large as $n$, i.e., exponentially big.
Quantum Measurements

We measure the function $f(x)$. We “collapse” onto a superposition of the $x$ with that $f(x)$:

\[
\begin{array}{cccccccc}
  x : & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
  2^x : & 4 & 4 &   &   &   &   &   &   &   \\
\end{array}
\]

This is a random coset of the subgroup $H$.

But, if we simply measure $x$, all we see is a random value! This is the wrong measurement.
The Fourier Transform

Periodicities are peaks in \( \hat{f} \), where \( \omega = e^{2\pi i / n} \)

\[
    f(x) = \frac{1}{\sqrt{n}} \sum_k \hat{f}(k) \omega^{kx}, \quad \hat{f}(k) = \frac{1}{\sqrt{n}} \sum_x f(x) \omega^{-kx}
\]

Change of basis \( Q_{x,k} = \frac{1}{\sqrt{n}} \omega^{kx} \)

from \( x \) to \( k \). This transformation is unitary:

\[
    Q^{-1} = Q^\dagger
\]
Shor’s Algorithm

- Quantum mechanics allows us to perform unitary transformations.
- We can “do” the Fourier transform mod $n$ with only $O(\log^2 n)$ basic quantum operations.
- Thus $n$ can be exponentially large!
- Measuring the frequency then gives a factor with constant probability.
Graph Isomorphism

- Factoring appears to be outside P, but not NP-complete. (Indeed, we believe that BQP does not contain all of NP.)

- Another candidate problem in this range:
Solving with Symmetry

- Take the union of the two graphs. Permuting the $2n$ vertices defines a function $f$ on $S_{2n}$. What is its symmetry subgroup $H$?

- Assume no internal symmetries. Then either $f$ is 1-1 and $H = \{1\}$, or $f$ is 2-1 and $H = \{1, m\}$ for some matching $m$. 
The Hidden Subgroup Problem

- We have a function $f : G \rightarrow X$
- We want to know its symmetries $H \subseteq G$
- Essentially all quantum algorithms that are exponentially faster than classical are of this form:
  - $\mathbb{Z}_n^*$ = factoring
  - $S_n$ = Graph Isomorphism
  - $D_n$ = Shortest Lattice Vector (some cases)
What We Can Do So Far

- Abelian groups: no problem
- “Slightly” non-Abelian groups:
  - small commutator subgroups [RB 1998, IMS 2003]
  - semidirect products [MRRS 2004, BCvD 2005]
  - “smoothly solvable” groups [FIMSS 2003]
- But these are very far from the symmetric group.
Non-Abelian Fourier Transforms

- The familiar Fourier basis functions $\omega^{kx}$ are homomorphisms $(\mathbb{Z}_n, +) \rightarrow (\mathbb{C}, \times)$
- For non-Abelian groups, we don’t have enough of these!
- For $S_3$, we have just 1 (trivial) and $\pi$ (parity)
- How will we form a basis?
Non-Abelian Fourier Transforms

- For non-Abelian groups, we consider matrix representations $\rho : G \to U(d)$
- For $S_3$, we have $1$ (trivial), $\pi$ (parity), and

  $\rho((12)) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho((123)) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}$

- We can permute three objects by rotating and reflecting the plane!
- Now we have $3! = 6$ basis vectors.
Heartbreaking Beauty

- Any representation is a direct sum of *irreducible* ones (“irreps”)

- Basis functions $\rho_{i,j}(g)$: name $\rho$, row and column $i, j$ in a given basis

- Form an orthogonal basis for $\mathbb{C}[G]$ and so $\sum_\rho d_\rho^2 = |G|

- Convolution = (matrix) product

- Everything beautiful is true...
Shor: Transform and Measure

- Form a superposition over the group
- Measure the value of $f$ (gives a superposition over a random coset)
- Fourier transform: change basis from $G$ to $\rho, i, j$
  [Beals, STOC 1997; Moore, Rockmore, Russell, SODA 2004]
- Measure in this new basis
- How much do we learn?
Levels of Measurement

- **Weak**: just the name $\rho$
- **Strong**: name, row and column $\rho, i, j$ in a basis of our choice (some bases probably much more informative than others, and much more efficient for computing)
- **Random**: strong, but in a random basis
Some Negative Results on $S_n$

- **Weak** sampling fails: only finds normal subgroups
  [Hallgren, Russell, Ta-Shma, STOC 2000]

- **Random** fails: gets lost in high-dimensional representations
  [Grigni, Schulman, Vazirani, Vazirani, STOC 2001]

- **Strong** sampling fails: each measurement gives an exponentially small amount of information
  [Moore, Russell, Schulman, FOCS 2005]

- Indeed, strong sampling is the only thing to do!

- What now?
Before, we queried $f$ once per measurement.

The tensor product of representations can be decomposed into irreducibles: e.g.

$$\rho \otimes \rho \cong 1 \oplus \pi \oplus \rho$$

Measure the irreducible subspace inside

$$G \otimes \cdots \otimes G$$

$k$ times
These are *entangled* measurements, not independent experiments!

**Good news:** $k = O(\log |G|) = \text{poly}(n)$ queries suffice [Ettinger, Høyer, Knill 1999, Moore & Russell 2005]

**The optimal** measurement is known for some groups and subgroups [Bacon, Childs and van Dam 2005, Moore & Russell 2005]

An efficient algorithm still seems difficult...