UNIVERSITY
OF COLOGNE

HIDDEN SUBGROUP PROBLEM

Why are quantum algorithms faster?

Contents

01

MOTIVATION

The root of the exponential speedup

- Many exponentially faster quantum algorithms are a special case of the Hidden Subgroup Problem
- It's the 'framework' behind many exponential speedups, i.e. generalization of a large class of quantum algorithms
- Finding period of a periodic function –> Shor's factoring algorithm, discrete logarithm, order of permutations, …

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest

02

SOME GROUP THEORY TO CATCH UP & HSP

What is an Abelian Group?
A set G with a binary operation $\otimes$

G

e.g. $(\mathbb{Z}, +)$, $(\{0,1,2,3,4,5\}, \text{sum mod} 6)$, ...

Associativity

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

Identity element

$$\exists\, \mathbb{I} \in G \quad s.t. \quad a \otimes \mathbb{I} = a$$

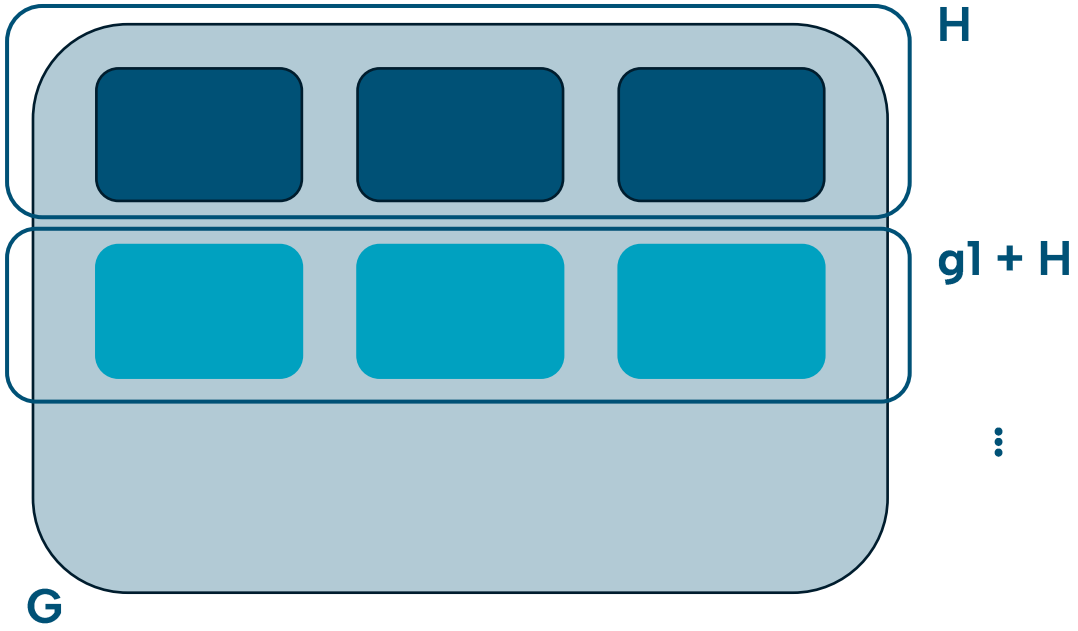
Inverse element

$$\forall\, a \in G\ \exists\, a^{-1} \quad s.t. \quad a \otimes a^{-1} = \mathbb{I}$$

Commutativity

$$a \otimes b = b \otimes a \qquad \forall\, a, b \in G$$

What is a coset?
Cosets tile a group in subgroups



Subgroup shifted by element of G

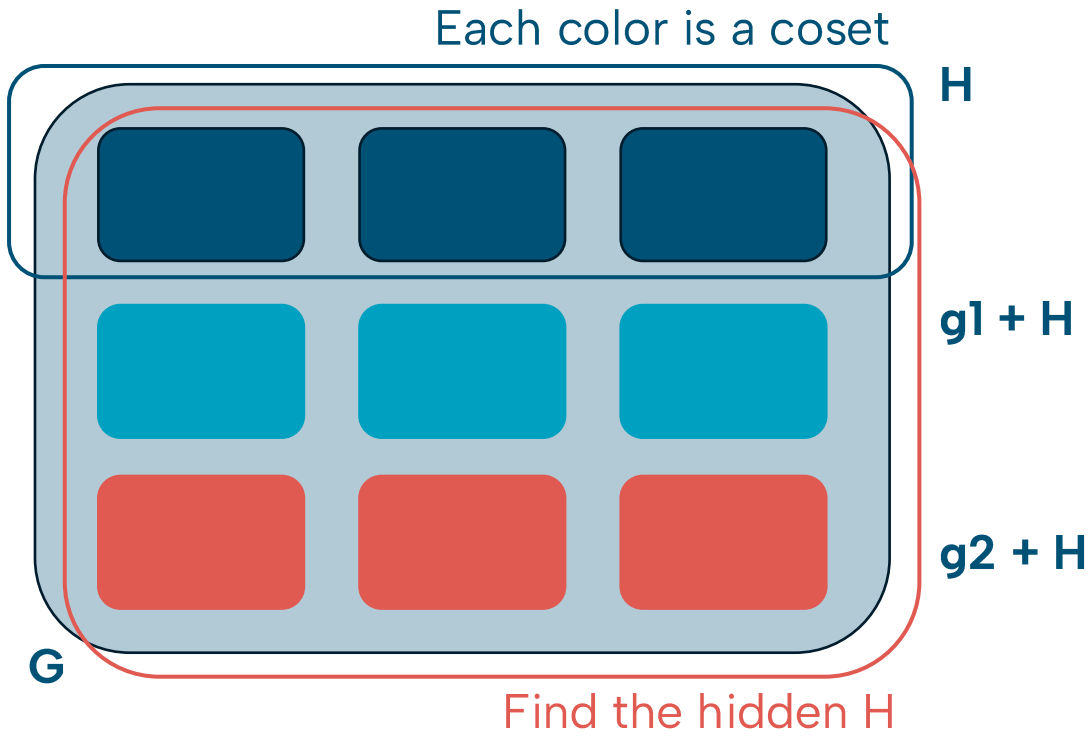
e.g. the right coset is defined as:

$$gH \equiv \{ g \otimes h \mid h \in H \} \quad for \ g \in G$$

For Abelian groups, the right and left cosets are the same

Distinct / non-overlapping cosets of a subgroup

The Hidden Subgroup Problem



Let G be a finite abelian group and X be a finite set. Suppose that there exists a function **f : G □ X that is distinct and constant on each coset of a subgroup H of G**.
Thus **f (g) = f (g□) if and only if g□ = hg for some h □ H**.
Suppose that we possess a unitary operator U that performs the operation |g□|x□ □ |g□|x □ f (g)□, where g □ G, x □ X and □ is an appropriately chosen binary operation on X.
Find (the generating set of) the subgroup H.

Classical vs. quantum

Classical run time	Quantum run time
$\mathcal{O}(\lvert G\rvert)$	$\mathcal{O}(\text{poly log}\lvert G\rvert)$

*Where $|G|$ refers to the number of elements in the group

e.g. for 2048-bit RSA: $2^{2048}$is astronomical but $poly \cdot 2048 \cdot log(2)$ is manageable.

03

THE ROUTINE

The routine I

$$|0\rangle|0\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{G}}\sum_{a\in G}|a\rangle|0\rangle \xrightarrow{f:\ G \to X} \frac{1}{\sqrt{G}}\sum_{a\in G}|a\rangle|f(a)\rangle \xrightarrow{\text{Measure}} \frac{1}{\sqrt{H}}\sum_{h\in H}|gH\rangle$$

- The QFT creates a uniform superposition over all elements of G
- The query evaluates f over all of them and stores in 2nd register
- The measurement collapses everything to a superposition of cosets of G

The routine II

$$\frac{1}{\sqrt{H}}\sum_{h\in H}|gh\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{H_\perp}}\sum_{h'\in H_\perp}|h'\rangle \xrightarrow{\text{sampling}} H_\perp \sim 0.j_i \xrightarrow{\text{Post process}} H$$

- QFT creates a uniform superposition over orthogonal $H_\perp$
- Running it roughly n times gives $n-1$ equations to be solved by Gaussian elimination, e.g. to find a hidden bitstring / order etc.
- We don’t just sample something, we sample valuable information on H!

Quantum Fourier Transform

$$
\begin{aligned}
F_N|j\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} |k_1 k_2 \ldots k_n\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \\
&= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)}{\sqrt{N}}
\end{aligned}
$$

Quantum Fourier Transform

- On a coset the QFT maps the subgroup to the dual
- Repeated computation and sampling allows to find H
- Can be implemented via simple gate operations

$$F_N|\mathrm{g}H\rangle = |\mathrm{H}_\perp\rangle$$

Classical FFT operations	Quantum operations
$\mathcal{O}(N \log N)$	$\mathcal{O}(\log^2 \mathrm{N})$

The routine summary

1

Superpose

Hadamard (or F_N gates) on the first register to create a uniform superposition

2

Query

Evaluate oracle and measure the second register, first collapses to cosets of G.

3

Fourier

Applying Fourier transform creates uniform superposition of orthogonal $H_\perp$.

4

Measure

Sample random $H_\perp$ and repeat the process, postprocess to get H.

04

SIMON'S AND SHOR'S ALGORITHM

Simon's algorithm

- $\mathrm{G} = \{0,1\}^n$ and bitwise XOR operation
- $f: G \rightarrow X$

$$\mathrm{f(x)} = \mathrm{f(y)} \quad \text{iff} \quad \mathrm{x} \oplus \mathrm{y} \in \mathrm{H}\ (\mathrm{x} = \mathrm{y} \text{ or } \mathrm{x} \oplus \mathrm{y} = \mathrm{s})$$

$$\mathrm{f(x)} = \mathrm{f(x} \oplus \mathrm{s)}$$

- $\mathrm{H} = \{0^{\mathrm{n}}, \mathrm{s}\},\ \mathrm{s} = \{0,1\}^{\mathrm{n}}$
- Classically it would require exponentially many queries to find the solution (the pairs and s)
  - 2^n different inputs to try
  - Lower bound runtimes of $\mathcal{O}(2^{\frac{\mathrm{n}}{2}})$

x	f(x)
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

solution: $\mathrm{s} = 110$

Shor's algorithm

1. Reduce integer factorization to order finding problem
2. Solve order finding problem as above

1. Pick random integer (a) coprime to N
2. Define $f(x) = a^x \mod N$ on $\mathbb{Z}$
3. $f(x)$ is periodic, i.e. $f(x) = f(x + r)$ so $H = r\mathbb{Z}$, r is periodicity
4. Find r as above, $\gcd(a^{\frac{r}{2}} \pm 1, N)$ gives a factor

*coprime: don't share common divisor

Shor's algorithm

N = 15: Number we want to factorize

a = 7: pick as coprime starting point

$f(x) = a^x \mod N$

x	f(x)
0	1
1	7
2	4
3	13
4	1
5	7
6	4

□ r = 4

Other coprimes: 1,2,4,7,8,11,13,14,15

Find $gcd\left(7^{\frac{r}{2}} - 1, 15\right) = gcd(48,15) = 3$

If r is uneven, we pick a new coprime

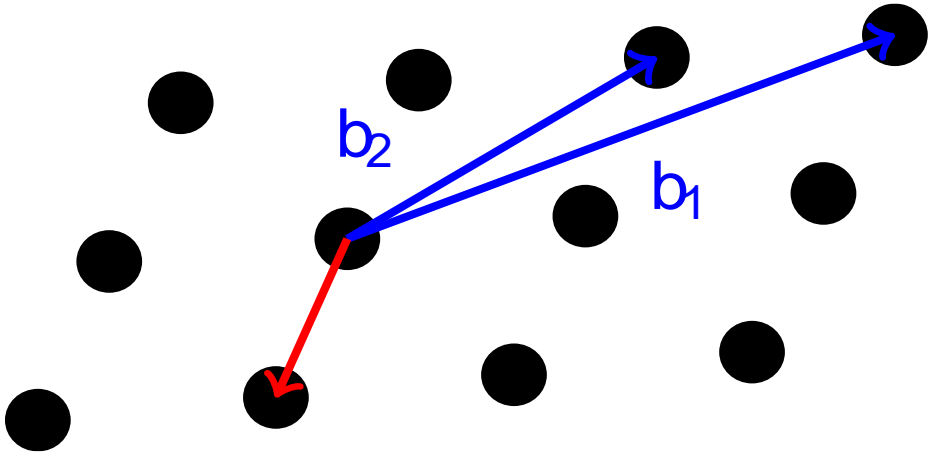
05

THE NON-ABELIAN CASE

Non-abelian groups and problems

Dihedral group D_n

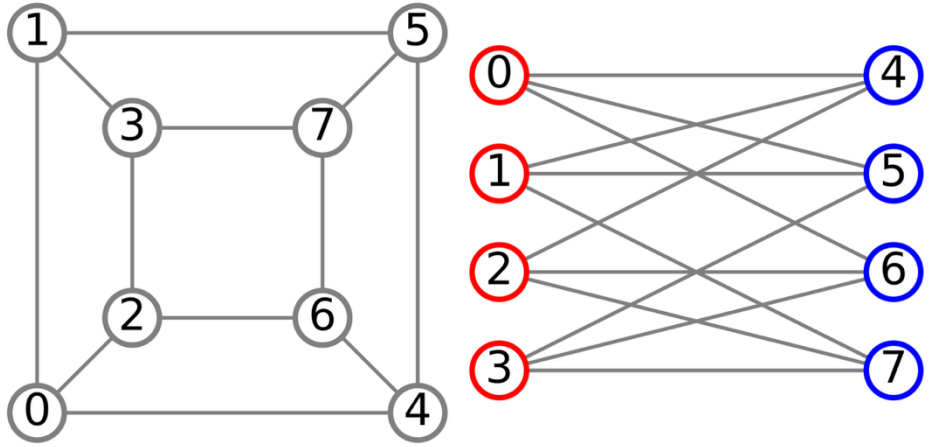
- Find the shortest vector in a lattice



By Sebastian Schmittner – Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=44488873

Symmetric group S_n

- Are two graphs isomorphic?



By BagLuke – Own work, CC0, https://commons.wikimedia.org/w/index.php?curid=162719043

The different efficiencies

1. Fully reconstructable

   HSP can be solved for G with $p > \frac{3}{4}$ by circuit polynomial in $\log|G|$

2. Measurement reconstructable

   HSP can be solved information theoretically using fully measured result of circuit polynomial in $\log|G|$

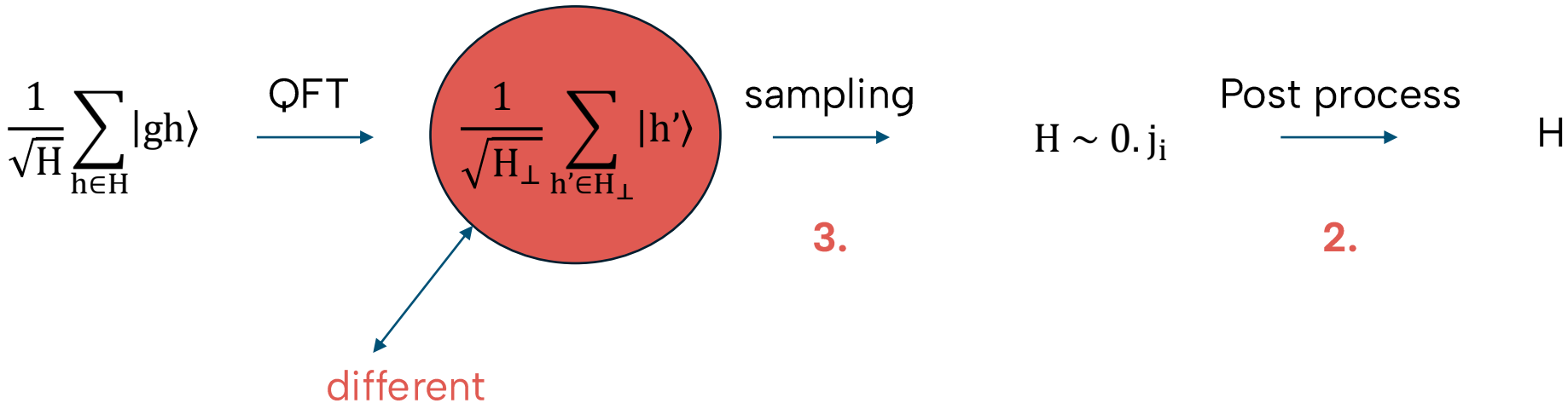
3. Query reconstructable

   HSP can be solved through quantum state resulting from a quantum circuit polynomial in $\log|G|$

   There is a POVM that yields the subgroup H with constant probability

   There is no guarantee that this POVM can be implemented by a small quantum circuit

The routine II



QFT over non-abelian groups

- QFT for non abelian groups -> requires a representation of the group G -> representation theory

$$F_N|x\rangle = \frac{1}{\sqrt{N}} \sum_y e^{\frac{2\pi i x y}{N}} |y\rangle$$

1D

Character: from group to unit circle

Representation: from group to 1D

$$\chi(\mathrm{G}) \cong \mathrm{G} \cong \widehat{\mathrm{G}}$$

$\mathrm{H}_\perp$ through QFT, since $\mathrm{H} \leftrightarrow \mathrm{H}_\perp$

$$F_G|g\rangle = \sum_\rho \sqrt{\frac{d_\rho}{\mathrm{N}}} \sum_{\mathrm{i,j}=1}^{d_\rho} \rho(g)_{ij} |\rho, i, j\rangle$$

matrix

Character: trace of representation

Representation: from group to matrix

Non-commuting group structure can only be represented in matrices of at least 2D

In what basis do we measure ρ?

Why does HSP ‘fail’?

- It does not actually fail but most of the times is no longer efficient
- The one-to-one representation in the dual is ’broken’
- There is no efficient sampling to recover conditions for H
  - Requires entangled measurements
  - Exponential time to classically reconstruct H

06

CONCLUSION

Abelian vs. non-abelian

abelian

- Exponential speedup for order finding / factorization / etc.
- The entire routine (superposition, QFT, readout, postprocess) does not add much to the duration

Non-abelian

- The non-abelian case is still being researched
- No general solution

Requires:

1. Efficient QFT for the groups
2. Choose basis for irreducible representations
3. Efficient reconstruction of H

References and further reading

- Childs, A. M. (n.d.). *Lecture Notes on Quantum Algorithms*.
- Gidney, C. (2025). *How to factor 2048 bit RSA integers with less than a million noisy qubits* (arXiv:2505.15917). arXiv. https://doi.org/10.48550/arXiv.2505.15917
- Kitaev, A. Y. (1995). *Quantum measurements and the Abelian Stabilizer Problem* (arXiv:quant-Ph/9511026). arXiv. https://doi.org/10.48550/arXiv.quant-ph/9511026
- Lomont, C. (2004). *The Hidden Subgroup Problem—Review and Open Problems* (arXiv:quant-Ph/0411037). arXiv. https://doi.org/10.48550/arXiv.quant-ph/0411037
- Martyn, J. M., Rossi, Z. M., Tan, A. K., & Chuang, I. L. (2021). Grand Unification of Quantum Algorithms. *PRX Quantum*, *2*(4), 040203. https://doi.org/10.1103/PRXQuantum.2.040203
- Nielsen, M. A., &; Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press.
- Rizvi, Alina Zainab, Diya Batool, and Hassan Mehmood. *The Hidden Subgroup Problem*. April 2023. https://physlab.org/wp-content/uploads/2023/05/HiddenSubgroup_23100127_Fin.pdf.