Hidden Subgroup Problems

Connect hidden XOR periods, cyclic periods and discrete logarithms through cosets and Fourier constraints.

Undergraduate 22 min lesson Dr. Charith Jayasekara

By the end, you'll be able to

- State the hidden-subgroup coset promise.
- Calculate Fourier support for a modulo-eight coset state.
- Explain the assumptions and boundaries of the Abelian Fourier-sampling framework.

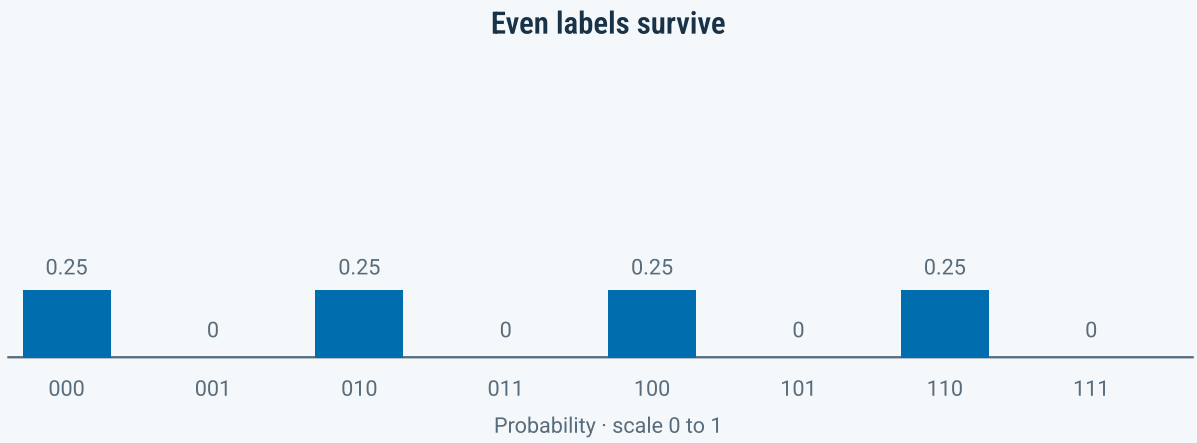
A shared language for hidden regularity

The hidden subgroup problem, or HSP, describes functions whose repeated values reveal a group symmetry. It unifies several quantum algorithms without making them identical. Simon hides an XOR symmetry. Order finding hides repetition in modular powers. Discrete logarithms can be expressed through a hidden relation between two exponents. Fourier sampling is especially effective when the group is Abelian, meaning its operation commutes.

Review Simon's algorithm, the QFT and order finding. This chapter introduces group vocabulary through finite examples. A group is a set with an associative composition, an identity and inverses; a subgroup is a subset that remains a group under the same operation.

WORKED DIAGRAM · A15

A coset pair reveals its subgroup constraint



Label	000	001	010	011	100	101	110	111
Amplitude	1/2	0	i/2	0	−1/2	0	−i/2	0

The coset state (|1⟩+|5⟩)/√2 has a separation of four. Its positive-exponent QFT cancels odd y and keeps even y at probability 1/4. The surviving amplitudes have different phases despite equal magnitudes.

The promise

Let G be a finite group and H an unknown subgroup. The function is constant on each coset of H and takes different values on different cosets. In an additive Abelian group, a coset is a set x plus H. The task is to identify H, typically by returning a compact set of generators rather than listing every element.

The function is supplied through coherent reversible access. The group representation and arithmetic also need efficient implementations for an efficient algorithmic result. Merely calling an enormous set a group does not supply a cheap Fourier transform, uniform preparation or oracle. State those resources alongside the promise.

A function with occasional accidental collisions does not satisfy this task description. The equal-output classes must be exactly the promised cosets. Like other promise problems, a circuit can still run on an invalid input, but its subgroup interpretation then lacks the stated guarantee.

For an additive group, equal function values mean that the inputs differ by an element of the hidden subgroup.

$$f(x) = f(y) \iff x - y \in H, \qquad |g + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |g + h\rangle.$$

The group is G, its hidden subgroup is H, and $g + H$ is one coset. The ket is the conditional input state obtained after selecting a function value.

Work a subgroup of integers modulo eight

Take G to be the integers zero through seven under addition modulo eight. Let H contain zero and four. Its cosets are the pairs zero/four, one/five, two/six and three/seven. A valid oracle gives one output label to each pair and different labels to different pairs.

Prepare a uniform superposition over G and query. If measuring the output selects the one/five label, the input becomes the equal superposition of one and five. Apply the eight-point QFT. The contribution from five differs from the contribution from one by a factor of negative one raised to the output label y. Odd y values cancel; even y values survive.

The possible Fourier samples are therefore zero, two, four and six, each with probability one quarter. These labels are exactly the characters that are trivial on the hidden subgroup. Several samples reveal constraints consistent with H. The oracle's arbitrary output names are irrelevant; the repeated-value structure is what matters.

The input pair contributes an explicit even/odd cancellation factor.

$$F_8 \frac{|1\rangle + |5\rangle}{\sqrt{2}} = \sum_{y=0}^{7} \frac{e^{2\pi i y/8}}{4} \left(1 + (-1)^y\right) |y\rangle = \frac{|0\rangle + i|2\rangle - |4\rangle - i|6\rangle}{2}.$$

All four surviving labels have probability $1/4$. Their relative phases depend on the chosen coset; the even-label support identifies the hidden subgroup's constraint.

Checkpoint 1

PAUSE & THINK

For H={0,4} in Z8, which output label can occur after the QFT of a coset state?

- ☐ 3
- ☐ 6
- ☐ 7

Answer: 6. The annihilator consists of even labels 0,2,4,6, because exp(2πi·4y/8)=1 exactly when y is even.

Characters explain the cancellation

For an Abelian group, a character assigns a unit complex phase to each group element while turning group composition into phase multiplication. On integers modulo N, the characters are the familiar Fourier phase factors. A character is trivial on H if it assigns phase one to every element of H.

The Fourier amplitude of a coset state contains a sum of character values over H. For a character trivial on H, the terms reinforce. For a nontrivial restriction, symmetry forces cancellation. The measured support is therefore the annihilator of H: the set of characters that are trivial on it. Classical group arithmetic then reconstructs H from those constraints.

This is the group-theoretic version of Simon's orthogonality equation. In the XOR group, characters are signs determined by binary dot products, and being trivial on the two-element subgroup generated by s means y dot s equals zero. The language is more general, but the interference mechanism is the same pairing or symmetry cancellation you already know.

The annihilator collects the characters that assign phase one to every hidden-subgroup element.

$$H^{\perp} = \{\chi \in \widehat{G} : \chi(h) = 1 \text{ for every } h \in H\}, \qquad F_G|g + H\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{\chi \in H^{\perp}} \chi(g)|\chi\rangle.$$

Here $\widehat{G}$ is the character set and this formula uses a positive-character Fourier convention. Measurement is uniform on $H^{\perp}$; changing the coset changes phases rather than this support.

Connection to order finding

Modular powers repeat with a period. In a finite cyclic setting where the domain length is compatible with that period, the repeated-value classes form cosets of a subgroup. Fourier sampling returns reciprocal-period information. Practical order finding handles a power-of-two approximation grid and uses rational reconstruction, so it should not be reduced to the oversimplified claim that every period divides the chosen register length.

The HSP perspective identifies the shared structure while the order-finding chapter supplies the precision, arithmetic and reconstruction details. A unifying abstraction is useful only when it preserves the application-specific assumptions that make the algorithm implementable.

A discrete-logarithm example

Suppose a cyclic group has prime order q, generator g, and an element h equal to g raised to an unknown x. Define a function of two exponents by g to the power a times h to the power b. Its value depends on a plus x times b modulo q. The hidden subgroup consists of pairs satisfying that expression equal to zero.

Fourier samples supply relations between the two output coordinates. With the convention used here, a sample k, l satisfies l equal to k times x modulo q. When k is nonzero, invert k and recover x. For q five and x three, sample k two and l one gives x equal to three, because the inverse of two modulo five is three.

This demonstrates why discrete logarithms fit the same hidden-relation framework, but its oracle arithmetic differs from factoring. An application must implement the chosen group's operations and ensure the encoding supports the required coherent evaluation. Group theory describes the structure; it does not erase arithmetic costs.

The unknown exponent defines a linear hidden relation between two input coordinates.

$$h = g^{x}, \quad f(a,b) = g^{a}h^{b} = g^{a+xb}, \qquad H = \{(-xb, b) : b \in \mathbb{Z}_q\}, \qquad \ell - kx \equiv 0 \pmod{q}.$$

The group generated by g has prime order q. A Fourier sample (k, ℓ) is trivial on the hidden subgroup exactly when it satisfies the last relation. Exponent arithmetic is modulo q.

A nonzero first coordinate can be inverted modulo the prime group order.

$$x \equiv \ell k^{-1} \pmod{q}, \qquad q = 5,\ (k,\ell) = (2,1): \quad k^{-1} = 3, \quad x \equiv 1 \cdot 3 = 3 \pmod{5}.$$

The sample $(0, 0)$ supplies no direct division step. Other samples can provide the missing information.

Checkpoint 2

PAUSE & THINK

For q=7 and Fourier sample (k,ℓ)=(2,6), what hidden exponent follows?

- ☐ 3
- ☐ 4
- ☐ 6

Answer: 3. Multiply the equation 2x≡6 by 2^−1=4 modulo seven to obtain x≡24≡3.

Abelian and non-Abelian boundaries

In finite Abelian groups, one-dimensional characters make Fourier sampling particularly clean. Non-Abelian groups have higher-dimensional representations and additional choices about what information to measure. The Abelian cancellation proof does not automatically produce an efficient general non-Abelian algorithm. Any claim for a specific non-Abelian family needs its own access assumptions, reconstruction procedure and complexity analysis.

This boundary is pedagogically important. A framework can connect solved tasks and still contain difficult families. Learning the HSP does not mean that every problem with a hidden symmetry is now efficiently solved. Ask which group, which oracle, which measurements and which classical reconstruction are actually available.

Chapter summary

- The hidden-subgroup promise makes equal-output classes exactly the cosets.
- Abelian Fourier sampling returns characters that are trivial on the subgroup.
- Simon, cyclic order finding and discrete logarithms share this mechanism with different arithmetic and reconstruction steps.

A common misconception

The Abelian HSP argument solves every hidden-symmetry problem efficiently. The Fourier transform, group operations and reconstruction must be efficient for the chosen representation. Non-Abelian groups require additional analysis and do not inherit a general efficient solution from this proof.

Exercises

1. In the modulo-eight example, why can Fourier label three not occur for the coset one/five? Calculate the relative phase of the two contributions.
2. For a prime-order discrete-logarithm instance with q seven, a Fourier sample satisfies k two and l six. Recover x under the stated relation. Why is k zero unhelpful for that division step?

Worked answers

1. The inputs differ by four, so their relative Fourier phase at y three is exp of two pi i times four times three over eight, which is negative one. Equal-magnitude contributions cancel.
2. The inverse of two modulo seven is four. Multiplying six by four gives twenty-four, congruent to three, so x is three. Zero has no multiplicative inverse modulo seven, so a zero first coordinate does not support this direct reconstruction.

Check your understanding

PAUSE & THINK

In the modulo-eight coset example, why is Fourier label three absent?

- [ ] Its two contributions have relative phase −1 and cancel
- [ ] It is outside the register
- [ ] Every odd number is forbidden in every QFT

Answer: Its two contributions have relative phase −1 and cancel. The input separation is four, so the relative phase at label three is exp(2πi·4·3/8)=−1. This cancellation depends on the particular hidden subgroup.

Sources

Quantum factoring, discrete logarithms and the hidden subgroup problem develops the algebraic framework. The QFT and extensions of the Abelian HSP is a primary treatment of related Fourier methods and access issues.