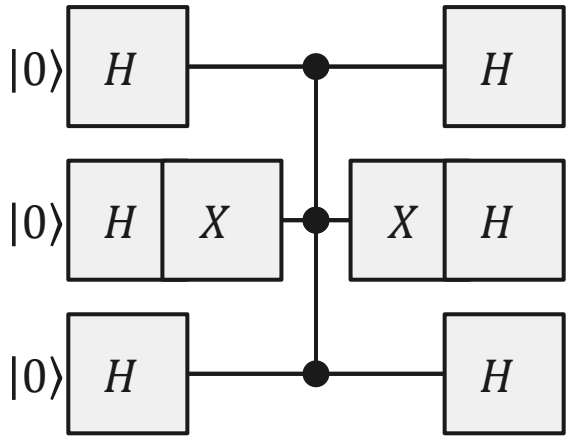
SAJID Lab
Smart & Advanced Junction of Intelligent Devices

EEE 6516 · QUANTUM COMPUTING

Grover Search

Finding a marked item in about √N queries

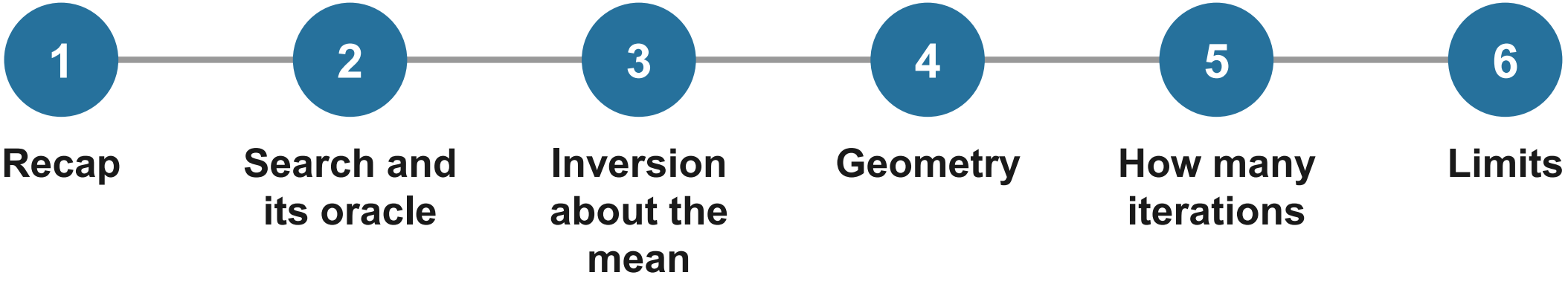


Chapter 5 · Lecture 11

Sajid Muhaimin Choudhury

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Today



By the end of this lecture you can

- build the phase oracle for a marked item and the diffusion circuit
- explain one Grover iteration as two reflections, a rotation by 2θ
- compute θ, $k^* = \lfloor \pi/(4\theta) \rfloor$ and the success probability for given N and M
- state what the quadratic speed-up does and does not give

Two tools from Lecture 10

Phase oracle (Lecture 10)

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle$$

from U_f with the ancilla in $|-\rangle$

Uniform superposition

$$|u\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$$

N = 2^n amplitudes, all equal

The oracle marks an item with a minus sign.

|u⟩ starts the search: every item has amplitude 1/√N.

Measuring |u⟩ finds a given item with probability 1/N: that is guessing.

YOUR TURN · RECALL

Warm-up: the oracle as a matrix

Recall · 45 seconds

N = 4 items, marked item $w = 10$. Write O_f as a diagonal matrix in textbook order (basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$).

A $\mathrm{diag}(1,1,-1,1)$

B $\mathrm{diag}(1,-1,1,1)$

C $\mathrm{diag}(-1,-1,1,-1)$

D $\mathrm{diag}(1,1,1,-1)$

ANSWER

A: diag(1, 1, −1, 1)

Index of $|10\rangle$ is $2q_0 + q_1 = 2$: the third diagonal entry is −1.

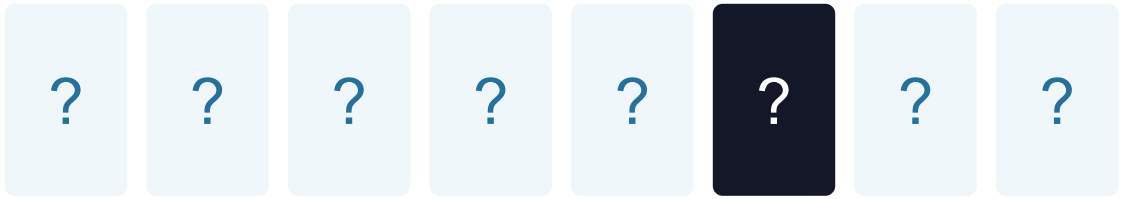
In general $O_f = I - 2|w\rangle\langle w|$: minus sign on the marked item only.

B is Qiskit's order (qubit 0 rightmost); C differs from A by a global sign but negates the unmarked items.

1 Unstructured search

How fast can we find a marked item in a list with no order?

The search problem and the classical cost



N items, one marked; only the oracle can tell

$$\frac{1}{N}\left(\sum_{j=1}^{N-1} j + (N-1)\right) = \frac{(N-1)(N+2)}{2N} \approx \frac{N}{2}$$

classical average, random order (N = 4: 2.25)

N = 2^n items; $f(x) = 1$ for the M marked ones; no order to exploit.

Classical, M = 1: N − 1 queries in the worst case.

Random order, stop when found or one item is left: about N/2 on average.

Grover (1996): about (π/4)√N queries.

DERIVATION

The classical average, step by step

$\Pr(\text{marked item at position } j) = 1/N, \qquad j = 1,2,\dots,N$ — random order of testing

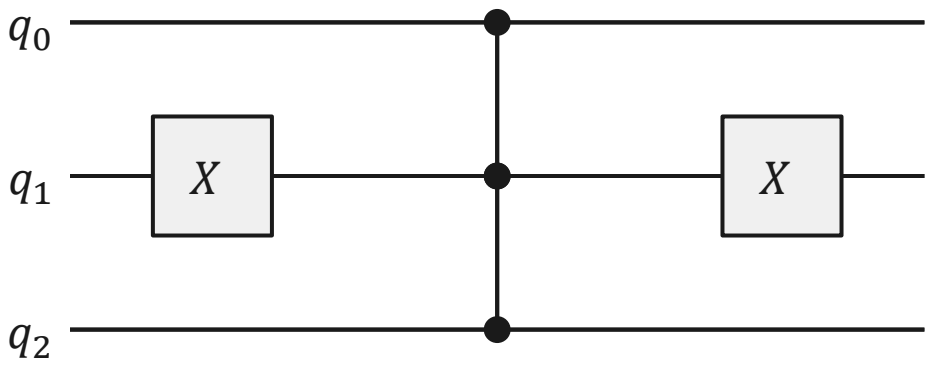
$j \le N-1$: j queries; $\quad j = N$: $N-1$ queries — the last item needs no test

$$\text{average} = \frac{1}{N}\left(\sum_{j=1}^{N-1} j + (N-1)\right)$$ — average over the positions

$$= \frac{1}{N}\left(\frac{N(N-1)}{2} + N - 1\right) = \frac{(N-1)(N+2)}{2N}$$ — arithmetic series

N = 4: 3·6/8 = 2.25 queries on average; for large N about N/2, and N − 1 in the worst case.

The oracle for a marked item



w = 101: X on the zero bit, MCZ, X

$$O_f = I - 2|w\rangle\langle w|$$

MCZ multiplies $|1^n\rangle$ by −1; the X gates move w onto 1^n and back.

MCZ = H, a multi-controlled NOT, H on one qubit (Chapter 3: CZ from CNOT).

Caveat 1: a real oracle checks a candidate; it does not contain the answer.

Caveat 2: Grover searches a function's inputs, not a stored database.

2 Inversion about the mean

How do we move amplitude onto the marked item?

DERIVATION

The diffusion operator reflects about the mean

$D = 2|u\rangle\langle u| - I$ — the diffusion operator

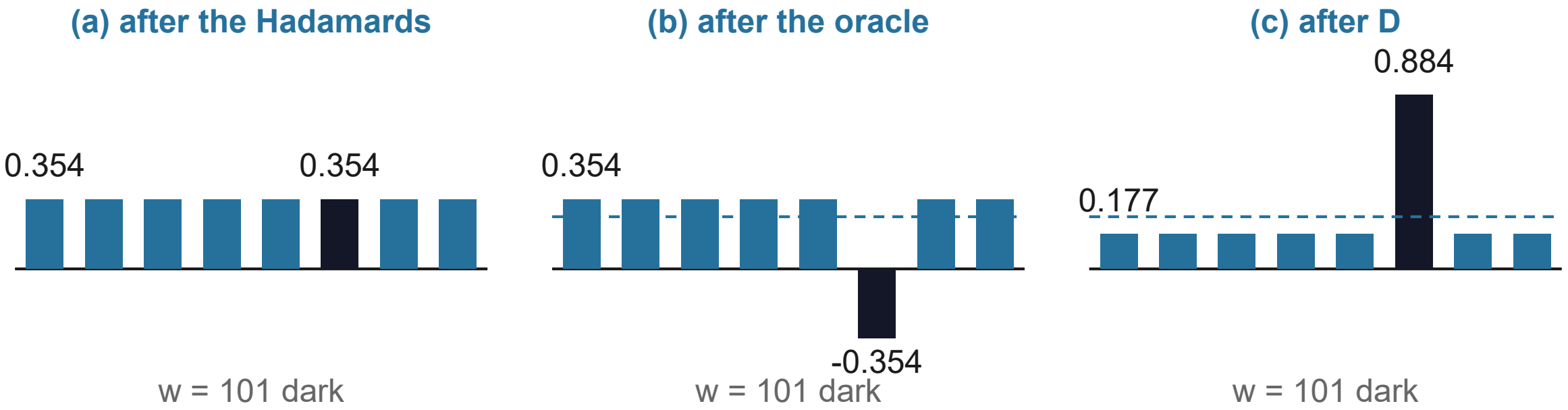
$\langle u|\psi\rangle = \sum_x a_x / \sqrt{N} = \sqrt{N}\,\overline{a}$ — $\overline{a}$ = mean amplitude of $|\psi\rangle = \sum_x a_x |x\rangle$

$D|\psi\rangle = 2\sqrt{N}\,\overline{a}|u\rangle - |\psi\rangle$ — apply D

$= \sum_x (2\overline{a} - a_x)|x\rangle$ — $|u\rangle = \Sigma_x |x\rangle/\sqrt{N}$

Each amplitude a_x goes to $2\overline{a} - a_x$: a reflection about the mean.

One iteration as amplitudes, N = 8



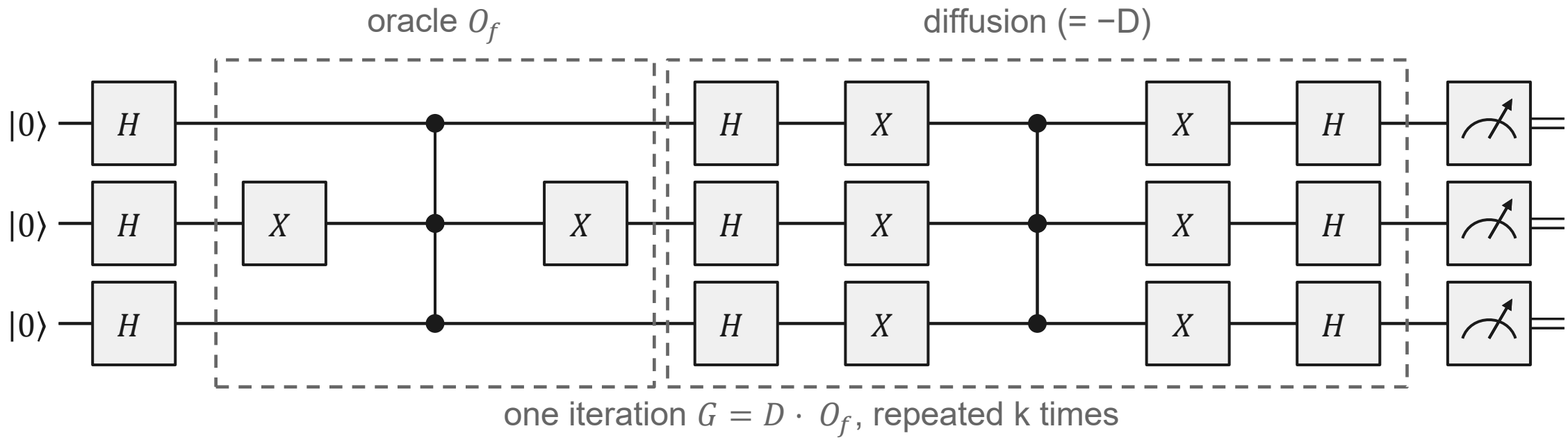
The oracle flips the marked amplitude; the mean drops to $6/(8\sqrt{8}) \approx 0.265$.

D reflects about that mean: unmarked $0.354 \rightarrow 0.177$, marked $-0.354 \rightarrow 0.884$.

Probability of w: $0.884^2 \approx 0.781$ after one iteration (1/8 before).

DERIVATION

The Grover iterate and its circuit



$$X^{\otimes n}\,\mathrm{MCZ}\,X^{\otimes n} = I - 2|0^n\rangle\langle 0^n|$$

X gates move $|1^n\rangle$ to $|0^n\rangle$

$$H^{\otimes n}X^{\otimes n}\,\mathrm{MCZ}\,X^{\otimes n}H^{\otimes n} = I - 2|u\rangle\langle u| = -D$$

Hadamards move $|0^n\rangle$ to $|u\rangle$

COMMON MISTAKE

“The circuit gives −D, so it is a different algorithm”

✗ A different operator

the circuit is −D, not D

so it computes something else

and the analysis must be redone

Treats a global phase as physical.

✓ The same algorithm

−1 multiplies the whole iteration

a global phase: no probability changes

it matters only under control (Ch. 6)

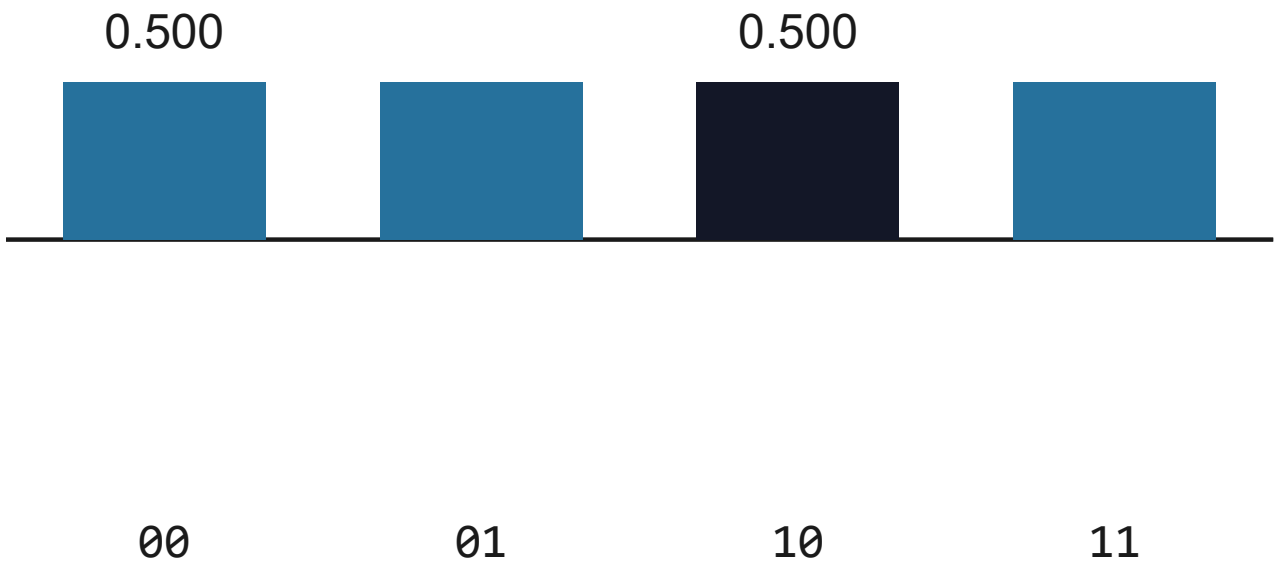
Track the sign when G is controlled.

The factor −1 is a global phase: the circuit implements Grover exactly. Only a controlled G would see it.

WORKED EXAMPLE · STEP 1 OF 3

Worked example: Grover search with four items

1 After H⊗H: every amplitude ½.

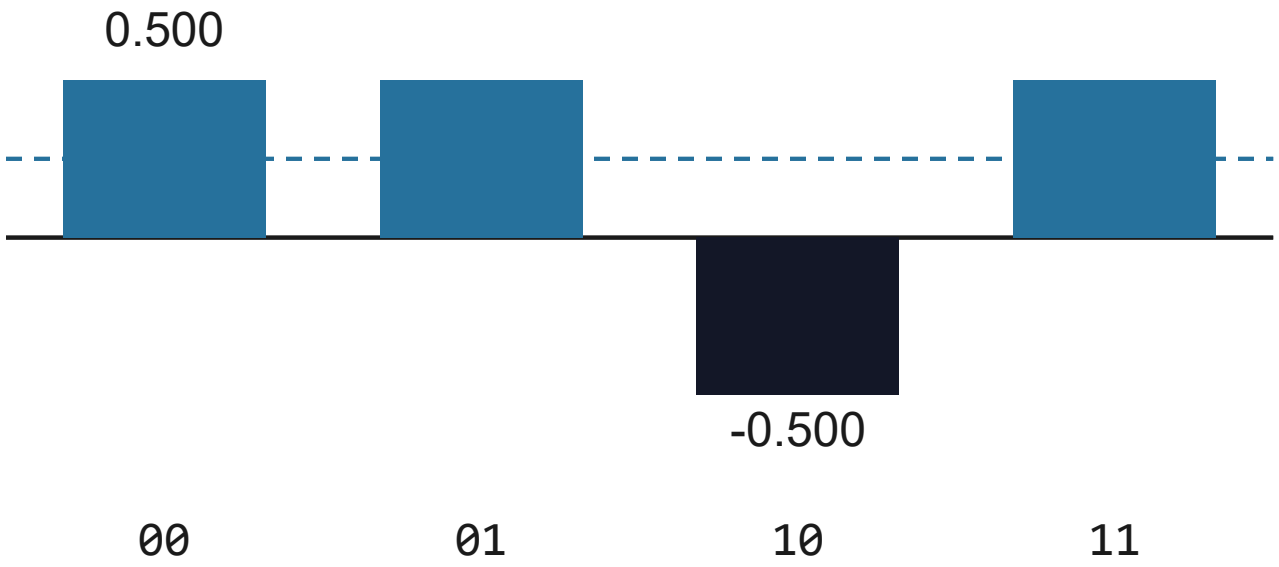


$$|u\rangle = \frac{1}{2}(1,1,1,1)$$

Before the next slide

What does the oracle for w = 10 do?

Worked example: Grover search with four items



$$O_f|u\rangle = \frac{1}{2}(1,1,-1,1), \overline{a} = \frac{1}{4}$$

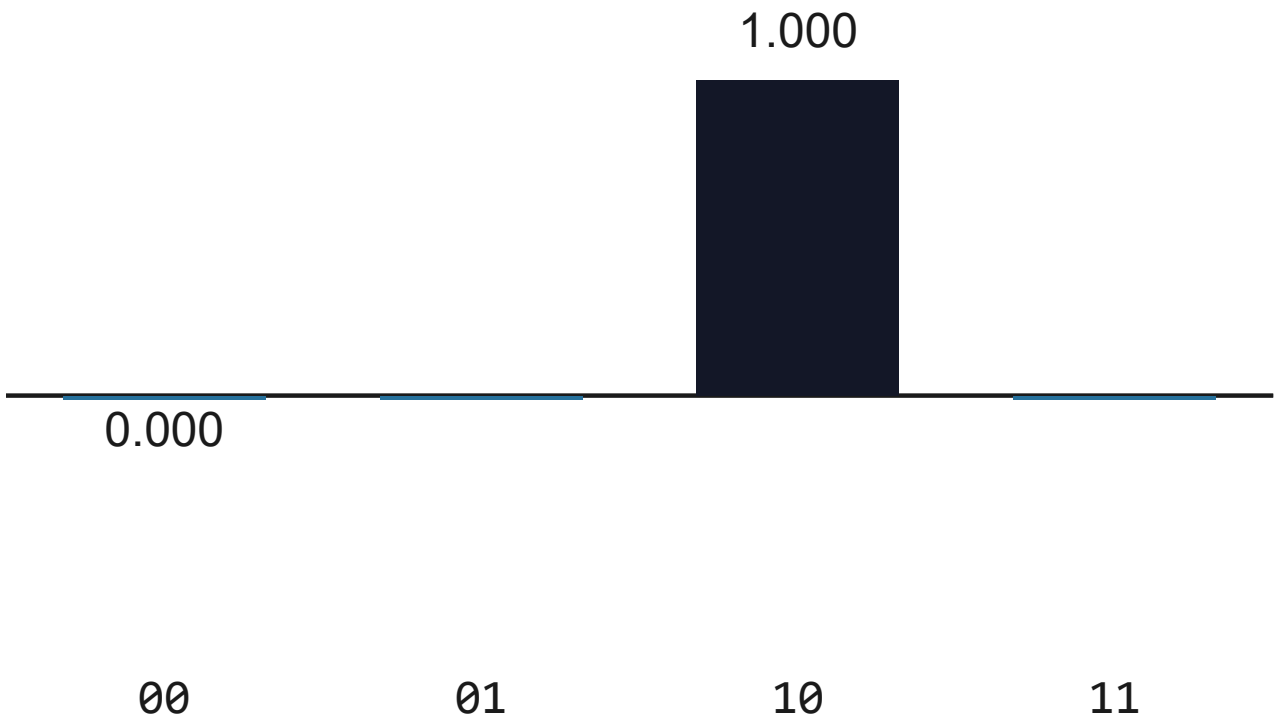
1 After H⊗H: every amplitude ½.

2 Oracle: the amplitude of 10 becomes −½; the mean is ¼.

Before the next slide

Reflect each bar about ¼.

Worked example: Grover search with four items



$$D\,O_f|u\rangle = (0,0,1,0)$$

1 After H⊗H: every amplitude ½.

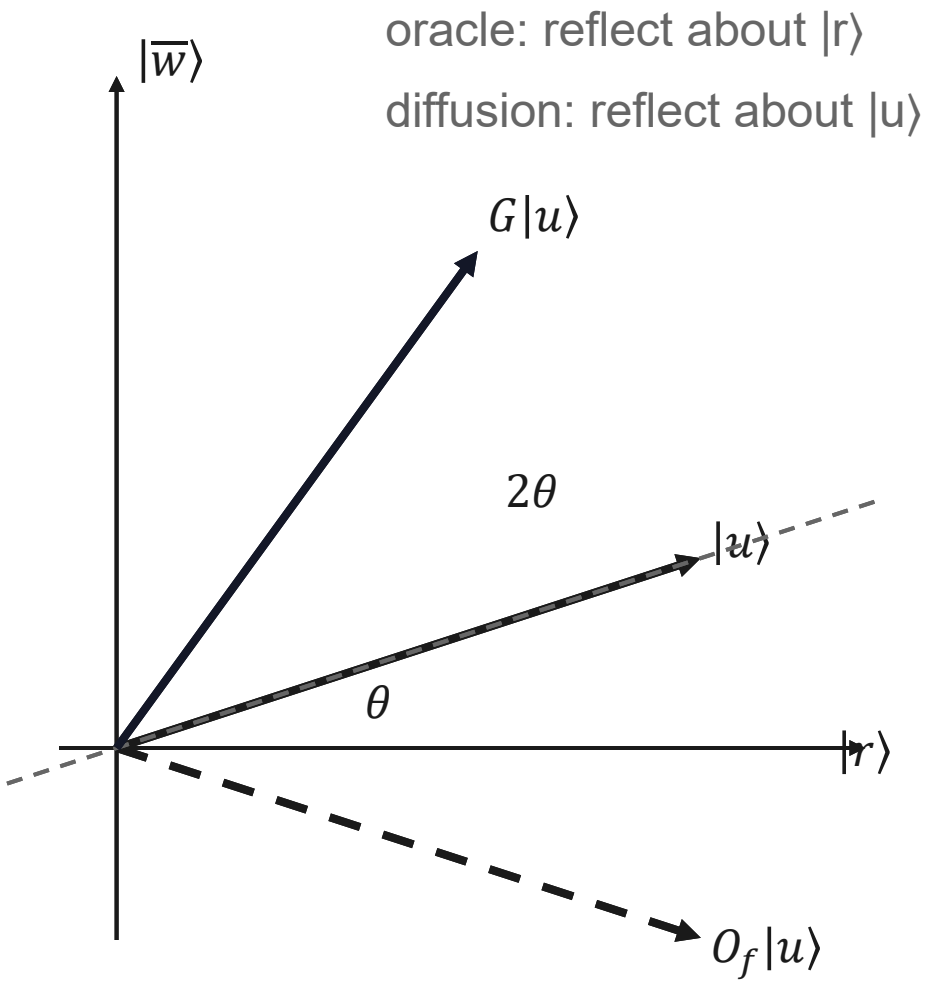
2 Oracle: the amplitude of 10 becomes −½; the mean is ¼.

3 Diffusion: 2·¼ − ½ = 0 for the others, 2·¼ + ½ = 1 for w. Found with certainty, one query.

3 The geometry of Grover search

Why does a Grover iteration rotate the state?

Everything happens in one plane



$$|\overline{w}\rangle = \frac{1}{\sqrt{M}}\sum_{\text{marked}}|x\rangle,$$

$$|r\rangle = \frac{1}{\sqrt{N-M}}\sum_{\text{unmarked}}|x\rangle$$

$$|u\rangle = \sin\theta|\overline{w}\rangle + \cos\theta|r\rangle, \qquad \sin\theta = \sqrt{M/N}$$

Oracle: reflect about |r⟩. Diffusion: reflect about |u⟩.

Two mirrors at angle θ rotate by 2θ (optics; Householder reflections).

DERIVATION

Where |u⟩ lies in the plane

$$|u\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle = \frac{1}{\sqrt{N}}\left(\sqrt{M}|\overline{w}\rangle + \sqrt{N-M}|r\rangle\right)$$

group marked and unmarked terms

$$\langle \overline{w}|u\rangle = \sqrt{M/N} = \sin\theta, \qquad \langle r|u\rangle = \sqrt{(N-M)/N} = \cos\theta$$

the two coordinates of |u⟩

$$\sin^2\theta + \cos^2\theta = \frac{M}{N} + \frac{N-M}{N} = 1$$

|u⟩ is a unit vector of the plane

$$M = 1, N \text{ large: } \theta \approx \sin\theta = 1/\sqrt{N}$$

a small angle

|u⟩ sits at angle θ above |r⟩, with sin θ = √(M/N): the fraction of marked items fixes θ.

DERIVATION

The diffusion operator as a 2 × 2 matrix

$$|u\rangle\langle u| = \begin{bmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}$$

$|u\rangle = (\cos\theta, \sin\theta)$ in the basis $|r\rangle, |\overline{w}\rangle$

$$2|u\rangle\langle u| - I = \begin{bmatrix} 2\cos^2\theta - 1 & 2\sin\theta\cos\theta \\ 2\sin\theta\cos\theta & 2\sin^2\theta - 1 \end{bmatrix}$$

twice the projector, minus I

$$D = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}$$

double-angle formulas

D keeps |u⟩ and flips the direction perpendicular to it: the reflection about the line through |u⟩.

DERIVATION

One iteration is a rotation by 2θ

$$O_f = \mathrm{diag}(1, -1)$$

basis $|r\rangle, |\overline{w}\rangle$: flips the marked direction

$$D = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}$$

$|u\rangle$ = (cos θ, sin θ): keeps $|u\rangle$

$$D\,O_f = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

a rotation by 2θ

$$P_k = \sin^2\big((2k+1)\theta\big)$$

start at θ; k rotations reach (2k + 1)θ

After k iterations a measurement finds a marked item with probability sin²((2k+1)θ).

YOUR TURN · CALCULATE

Your turn: why does one iteration suffice for N = 4?

Think · 45 seconds

One marked item among $N = 4$. Find θ and the angle of the state after one iteration.

A θ = 30°, angle 90°

B θ = 45°, angle 135°

C θ = 30°, angle 60°

D θ = 15°, angle 45°

ANSWER

A: θ = 30°; 3θ = 90° is the marked axis

$\sin\theta = \sqrt{1/4} = 1/2 \Rightarrow \theta = \pi/6$

$P_1 = \sin^2(3\theta) = \sin^2(\pi/2) = 1$

For N = 4 one rotation hits the target exactly; for larger N it usually does not.

4 How many iterations?

When should we stop, and what does stopping late cost?

DERIVATION

The best number of iterations

$(2k+1)\theta \approx \pi/2 \;\Rightarrow\; k \approx \pi/(4\theta) - 1/2$ — aim at the $|\overline{w}\rangle$ axis

$k^* = \lfloor \pi/(4\theta) \rfloor, \qquad \pi/(4\theta) = k^* + \delta, 0 \le \delta < 1$ — the integer we use

$(2k^*+1)\theta = 2\left(\frac{\pi}{4\theta} - \delta\right)\theta + \theta = \frac{\pi}{2} + (1-2\delta)\theta$ — substitute k* = π/(4θ) − δ

$|(2k^*+1)\theta - \pi/2| = |(1-2\delta)\theta| \le \theta$ — miss the axis by at most θ

$P_{k^*} \ge \cos^2\theta = 1 - M/N, \qquad k^* \le (\pi/4)\sqrt{N/M}$ — θ ≥ sin θ = √(M/N)

One marked item: k* ≈ (π/4)√N queries, the promised square-root speed-up.

YOUR TURN · CALCULATE

Predict: eight items, one marked

Calculate · 1 minute

$N = 8$, one marked item. What is k^*, and what happens if we do $k = 3$ iterations instead?

A k* = 2; P_3 is even larger

B k* = 2; P_3 is only about 0.33

C k* = 3; $P_3 \approx 0.96$

D k* = 8, one per item

ANSWER

B: k* = 2 ($P_2 \approx 0.945$); one more iteration over-rotates

$$\theta = \arcsin\left(1/\sqrt{8}\right) \approx 0.3614, \qquad \pi/(4\theta) \approx 2.17, \qquad k^* = 2$$

$$P_2 = \sin^2(5\theta) \approx 0.9453 \geq 1 - 1/8, \qquad P_3 = \sin^2(7\theta) \approx 0.3301$$

2000 shots at k = 2: expect 1890.6 counts of 101, standard deviation 10.2.

YOUR TURN · VOTE

Quick vote: sixty-four items

Vote · 45 seconds

For $N = 64$ and one marked item, the number of Grover iterations $k^* = \lfloor \pi/(4\theta) \rfloor$ is

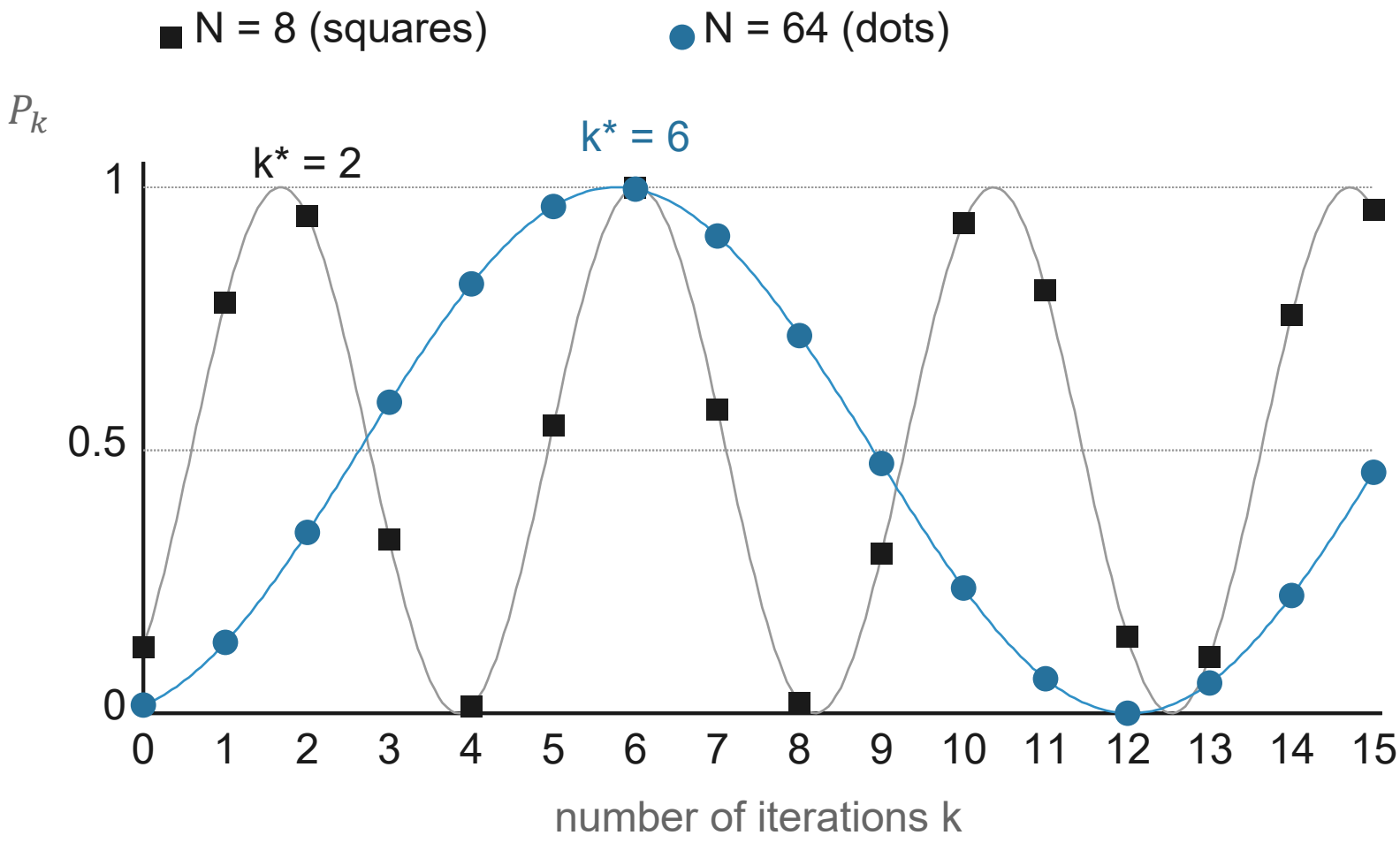
A 6

B 7

C 8

D 32

Success probability against k: N = 8 and N = 64



N = 8: peak $P_2 \approx 0.945$ at k* = 2.

N = 64: peak $P_6 \approx 0.997$ at k* = 6.

Beyond k* the state over-rotates: P_k oscillates with period about π/(2θ) in k.

COMMON MISTAKE

“More iterations are always better”

✗ Iterate until it converges

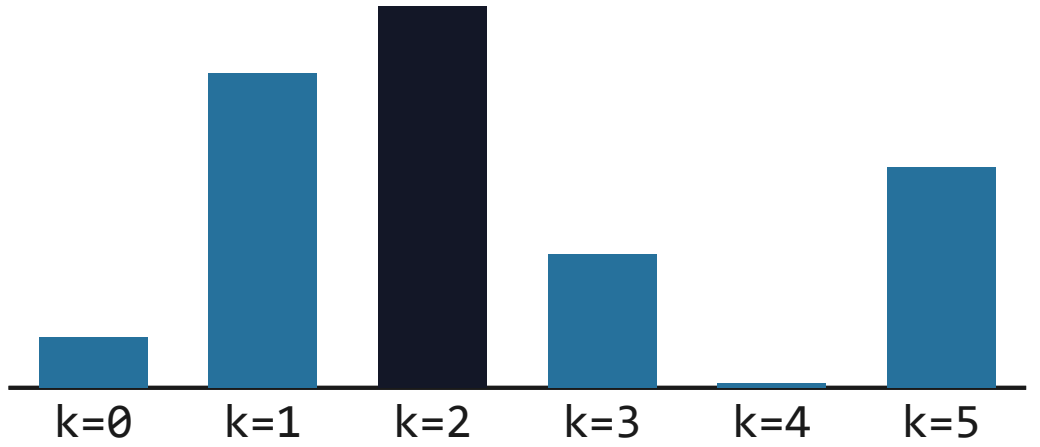
P_k rises towards 1

like Newton's method,

run until it stops changing

Grover is a rotation; it never settles.

✓ Choose k* in advance



P_k for N = 8 (Simulation 5.5): peak at k* = 2, then over-rotation.

P_k oscillates with period about π/(2θ) in k. Choose k* from N and M in advance; for N = 8, $P_4 \approx 0.012$.

SIMULATION · LIVE

Simulation 5.5: Grover search for one item in eight

```
def grover(k):
    qc.h(range(n))
    for _ in range(k):
        qc.x(zeros)
        mcz(qc)
        qc.h(range(n))
theta = np.arcsin(np.sqrt(1 / 2 ** n))
    th = np.sin((2 * k + 1) * theta) ** 2
sim = AerSimulator(seed_simulator=6555)
```

The loop body is one iteration: oracle, then the diffusion circuit (−D).

Exact P_k from Statevector; then 2000 shots at k = 2.

k	P_k (Qiskit)	theory
0	0.125000	0.125000
1	0.781250	0.781250
2	**0.945312**	**0.945312**
3	0.330078	0.330078
4	0.012207	0.012207
5	0.547974	0.547974

k = 2, 2000 shots: 1884 × 101
expected 1890.6 ± 10.2

5 Several marked items, and the limits

What changes with M marked items, and can we do better?

Several marked items

The same formulas with $\sin\theta = \sqrt{M/N}$: a larger angle.

$k^* \approx (\pi/4)\sqrt{N/M}$: more marked items, fewer iterations.

The output is one of the marked items, each with the same probability.

M must be known (or estimated) to choose k*; unknown M: self-study §5.9.

YOUR TURN · CALCULATE

Checkpoint: two of eight items marked

Calculate · 1 minute

Two of eight items are marked. How many iterations should be used, and what is the probability of success?

YOUR TURN · VOTE

Quick vote: how good is the speed-up?

Vote · 30 seconds

The speed-up of Grover's algorithm for unstructured search is

A exponential

B quadratic, and no quantum algorithm can do better

C exponential for NP-complete problems

D quadratic so far; a better quantum algorithm could still need only $O(\log N)$ queries

The limits of the speed-up

$$\Omega\left(\sqrt{N}\right) \text{ queries for one item}$$

no quantum algorithm can do better (Bennett et al. 1997)

n	CNOTs per iteration
2	2
3	12
4	28
5	72
6	168

Qiskit 2.5.2 transpiler counts (self-study §5.9)

Optimal: the square root cannot be improved (Bennett et al. 1997).

Brute force over 2^n candidates: $2^n \rightarrow$ about $2^{n/2}$ queries, still exponential in n.

Not known to solve NP-complete problems efficiently, and Grover alone does not.

√N counts queries, not running time: each query and iteration costs gates.

Recap

1

Oracle and diffusion

$O_f = I - 2|w\rangle\langle w|, D = 2|u\rangle\langle u| - I$: inversion about the mean

2

Geometry

two reflections: a rotation by 2θ, $\sin\theta = \sqrt{M/N}$

3

Iterations

$k^* = \lfloor \pi/(4\theta) \rfloor \approx (\pi/4)\sqrt{N/M}$; more is not better

4

Limits

optimal; quadratic, not exponential; queries, not time

After the break: Lecture 12 (Chapter 6)

The quantum Fourier transform

Read: handout 5.7–5.8; 5.9 is self-study.

Exit ticket

One marked item among $N = 16$: find θ, k^* and P_{k^*}.

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Rights and attributions

Copyright (c) 2026 Sajid Muhaimin Choudhury. All rights reserved.

Public edition of Lecture 11: Grover Search. Release qc-2026-10-15, prepared 2026-10-15 from source revision 3df9449aa6.

This edition omits speaker notes, instructor-only material and every figure whose publication rights are not cleared for public distribution.