CS621/CSL611
Quantum Computing For Computer Scientists

Quantum Search

Dhiman Saha

Winter 2024

IIT Bhilai

Quantum Search

Grover's Algorithm

- Given an unordered array of m elements, find a particular element.
- Classically, in the worst case, this takes m queries.
- On average, we will find the desired element in $m/2$ queries.

Can we do better?

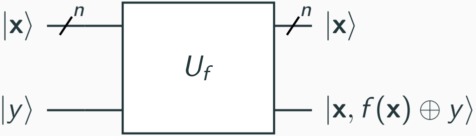
- Lov Grover's search algorithm does the job in $\sqrt{m}$ queries.
- Grover's algorithm has many applications to database theory and other areas.

- Let us look at the search problem from the point of view of functions.
- **Given:** A function $f : \{0,1\}^n \rightarrow \{0,1\} : \exists \mathbf{x_0} \in \{0,1\}^n$

$$f(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} = \mathbf{x_0}, \\ 0, & \text{if } \mathbf{x} \neq \mathbf{x_0}. \end{cases}$$

- **Goal:** To find $\mathbf{x_0}$
- Worst case effort:
  - **Classical Search:** 2^n evaluations of f
  - **Grover's Search:** $\sqrt{2^n} = 2^{\frac{n}{2}}$ evaluations of f

Quantum Circuit for f

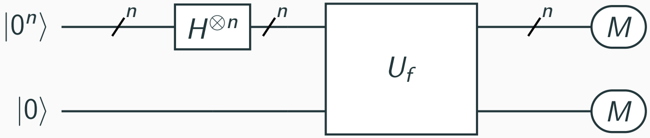


Example (For $n = 2$, if f "picks out" 10, then U_f is)

$$
\begin{array}{c|cccccccc}
 & \mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1} \\
\begin{array}{c}\mathbf{00,0}\\ \mathbf{00,1}\\ \mathbf{01,0}\\ \mathbf{01,1}\\ \mathbf{10,0}\\ \mathbf{10,1}\\ \mathbf{11,0}\\ \mathbf{11,1}\end{array} &
\multicolumn{8}{c}{\begin{bmatrix}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & 1 & & & & \\
 & & & & & 1 & & \\
 & & & & 1 & & & \\
 & & & & & & 1 & \\
 & & & & & & & 1
\end{bmatrix}}
\end{array}
$$

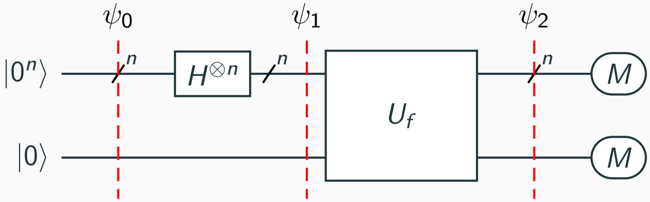
- Find U_f, if f "picks out" 11.

$$
\begin{array}{c c}
 & \begin{array}{cccccccc} \mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1} \end{array} \\
\begin{array}{c} \mathbf{00,0} \\ \mathbf{00,1} \\ \mathbf{01,0} \\ \mathbf{01,1} \\ \mathbf{10,0} \\ \mathbf{10,1} \\ \mathbf{11,0} \\ \mathbf{11,1} \end{array} & \begin{bmatrix} & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{bmatrix}
\end{array}
$$

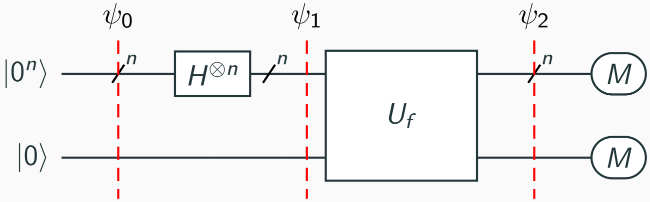


- Try placing $|\mathbf{x}\rangle$ into a superposition of all possible strings
- Then evaluate U_f
- In terms of matrices this becomes

$$U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0\rangle$$

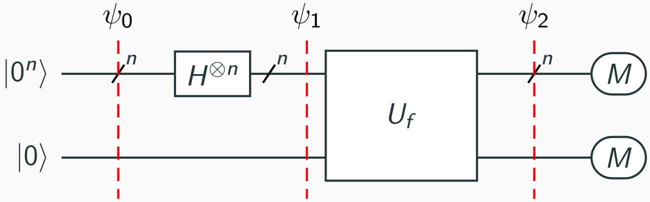


$$U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0\rangle$$



$$U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0\rangle$$

$$|\psi_0\rangle = |0^n\rangle\,|0\rangle$$

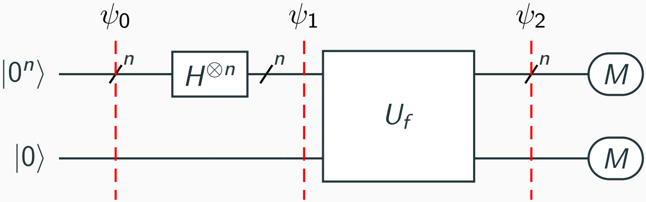


$$U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0\rangle$$

$$|\psi_0\rangle = |0^n\rangle\,|0\rangle$$

$$|\psi_1\rangle = \left(\frac{\sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle}{\sqrt{2^n}}\right)|0\rangle$$

Attempt-1



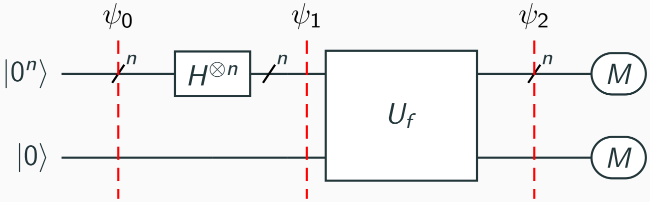
$$U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0\rangle$$

$$|\psi_0\rangle = |0^n\rangle\,|0\rangle$$

$$|\psi_1\rangle = \left(\frac{\sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle}{\sqrt{2^n}}\right)|0\rangle$$

$$|\psi_2\rangle = \left(\frac{\sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle\,|f(\mathbf{x})\rangle}{\sqrt{2^n}}\right)$$

Recall, $|\mathbf{x}, y\rangle \xrightarrow{U_f} |\mathbf{x}, f(\mathbf{x}) \otimes y\rangle$

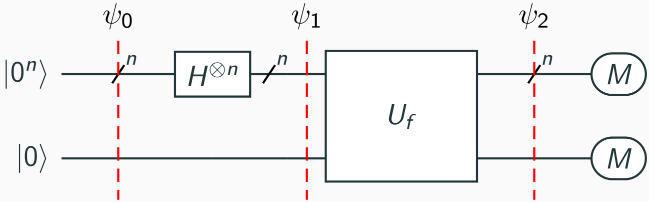


$$|\psi_2\rangle = \left(\frac{\sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle\, |f(\mathbf{x})\rangle}{\sqrt{2^n}} \right)$$

- Measuring the top qubits will, with equal probability, give one of the 2^n binary strings
- Measuring the bottom qubit will give
  - $|0\rangle$ with probability $\frac{2^n-1}{2^n}$
  - $|1\rangle$ with probability $\frac{1}{2^n}$ $\implies$ the top qubit will reveal x_0? How?

Measuring $|1\rangle$ **highly** improbable, Need better solution

Attempt-1 — Measurement Interpretation

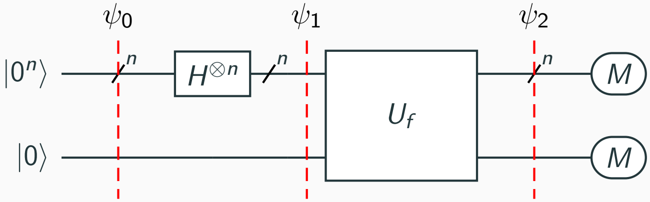


$$|\psi_2\rangle = \left(\frac{\sum_{x \in \{0,1\}^n} |\mathbf{x}\rangle \, |f(\mathbf{x})\rangle}{\sqrt{2^n}} \right)$$

- Measuring the top qubits will, with equal probability, give one of the 2^n binary strings
- Measuring the bottom qubit will give
  - $|0\rangle$ with probability $\frac{2^n-1}{2^n}$
  - $|1\rangle$ with probability $\frac{1}{2^n} \implies$ the top qubit will reveal x_0? How?

Measuring $|1\rangle$ **highly** improbable, Need better solution

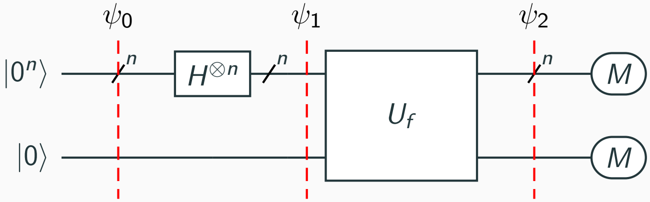
Measurement Interpretation



$$|\psi_2\rangle = \left(\frac{\sum_{x \in \{0,1\}^n} |\mathbf{x}\rangle \, |f(\mathbf{x})\rangle}{\sqrt{2^n}} \right)$$

- Measuring the top qubits will, with equal probability, give one of the 2^n binary strings
- Measuring the bottom qubit will give
  - $|0\rangle$ with probability $\frac{2^n-1}{2^n}$
  - $|1\rangle$ with probability $\frac{1}{2^n}$ $\Longrightarrow$ the top qubit will reveal x_0? How?

Measuring $|1\rangle$ **highly** improbable, Need better solution



$$|\psi_2\rangle = \left(\frac{\sum_{x \in \{0,1\}^n} |\mathbf{x}\rangle\, |f(\mathbf{x})\rangle}{\sqrt{2^n}} \right)$$

- Measuring the top qubits will, with equal probability, give one of the 2^n binary strings
- Measuring the bottom qubit will give
  - $|0\rangle$ with probability $\frac{2^n-1}{2^n}$
  - $|1\rangle$ with probability $\frac{1}{2^n} \implies$ the top qubit will reveal x_0? How?

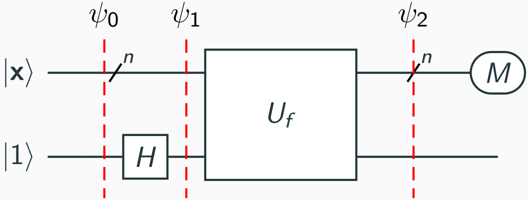
Measuring $|1\rangle$ **highly** improbable, Need better solution

- **Trick-1: Phase Inversion**:
  - Changes the phase of the desired state
- **Trick-2: Inversion About The Mean/Average**:
  - This is a way of boosting the separation of the phases.

Idea

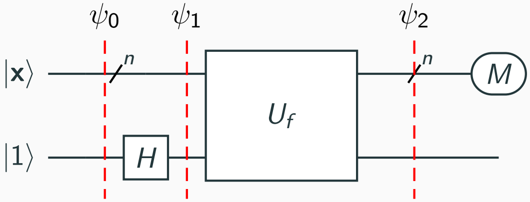
Take U_f and place the bottom qubit in the superposition $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

- Corresponding quantum circuit for an arbitrary $\mathbf{x}$

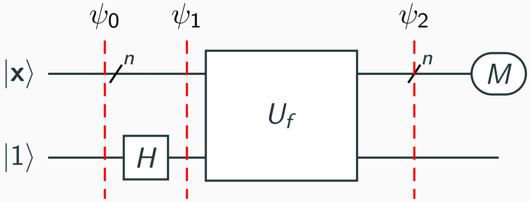


$$U_f(I_n \otimes H)\,|\mathbf{x}\rangle\,|1\rangle$$

- **Note:** Phase inversion, by construction, is a unitary operation.

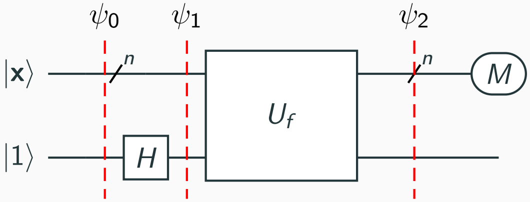


$$|\psi_0\rangle = |\mathbf{x}\rangle\,|1\rangle$$



$$|\psi_0\rangle = |\mathbf{x}\rangle\,|1\rangle$$

$$|\psi_1\rangle = |\mathbf{x}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|\mathbf{x}\rangle\,|0\rangle - |\mathbf{x}\rangle\,|1\rangle}{\sqrt{2}}\right)$$

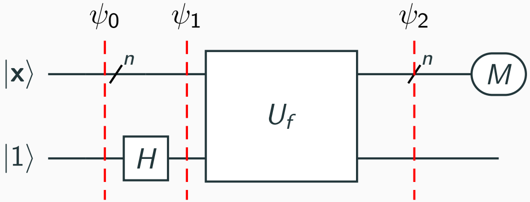


$$|\psi_0\rangle = |\mathbf{x}\rangle\,|1\rangle$$

$$|\psi_1\rangle = |\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|\mathbf{x}\rangle\,|0\rangle - |\mathbf{x}\rangle\,|1\rangle}{\sqrt{2}}\right)$$

$$|\psi_2\rangle = |\mathbf{x}\rangle\left(\frac{|f(\mathbf{x}) \oplus 0\rangle - |f(\mathbf{x}) \oplus 1\rangle}{\sqrt{2}}\right) = |\mathbf{x}\rangle\left(\frac{|f(\mathbf{x})\rangle - |\overline{f(\mathbf{x})}\rangle}{\sqrt{2}}\right)$$

Phase Inversion



$$|\psi_0\rangle = |\mathbf{x}\rangle\,|1\rangle$$

$$|\psi_1\rangle = |\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|\mathbf{x}\rangle\,|0\rangle - |\mathbf{x}\rangle\,|1\rangle}{\sqrt{2}}\right)$$

$$|\psi_2\rangle = |\mathbf{x}\rangle\left(\frac{|f(\mathbf{x}) \oplus 0\rangle - |f(\mathbf{x}) \oplus 1\rangle}{\sqrt{2}}\right) = |\mathbf{x}\rangle\left(\frac{|f(\mathbf{x})\rangle - \overline{|f(\mathbf{x})\rangle}}{\sqrt{2}}\right)$$

$$= (-1)^{f(\mathbf{x})}\,|\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \begin{cases} -1\,|\mathbf{x}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), & \text{if } \mathbf{x} = \mathbf{x_0} \\ +1\,|\mathbf{x}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), & \text{if } \mathbf{x} \neq \mathbf{x_0} \end{cases}$$

Effect of Phase Inversion

- Let $|\mathbf{x}\rangle$ start in a equal superposition of four different states:

$$|\mathbf{x}\rangle \rightarrow \left[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right]^T$$

- Let f be the function that uniformly chooses "10"
- After phase inversion state looks like:

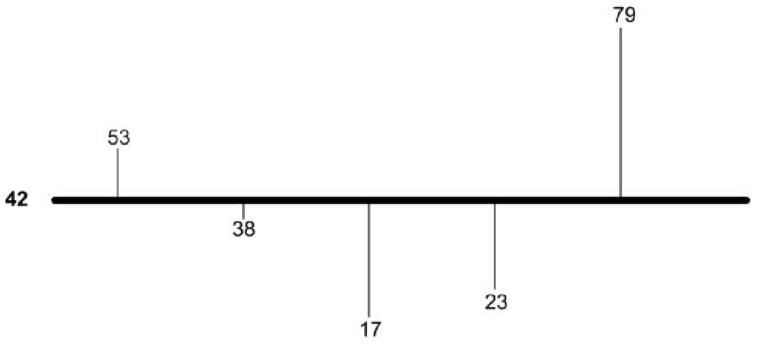
$$\left[\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right]^T$$

- Measurement does not help since $\left|\frac{1}{2}\right|^2 = \left|-\frac{1}{2}\right|^2 = \frac{1}{4}$
- **Implication:** Just separating phases is **not** enough

What next?

- **Boosting Phase Separation** between desired binary string from the other binary strings
- Inversion About The Mean/Average
- A way of boosting the separation of the phases.
- How? Let us see an example

- Consider a sequence of integers: $53, 38, 17, 23$, and 79.

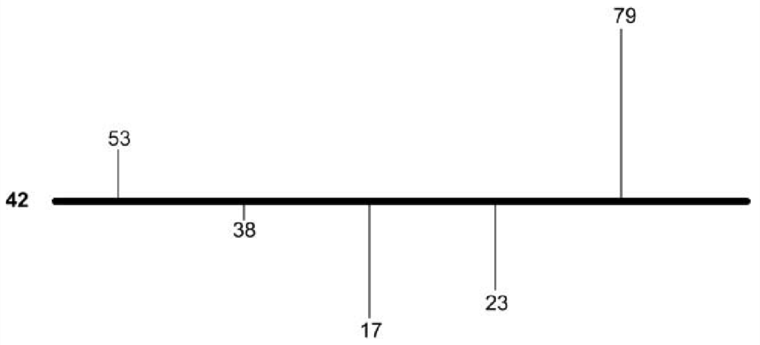


Interpreting the Average **Average is $a = 42$**

The average is the number such that the *sum of the lengths of the lines above the average* is the same as the *sum of the lengths of the lines below.*

Example — Inversion About The Mean/Average

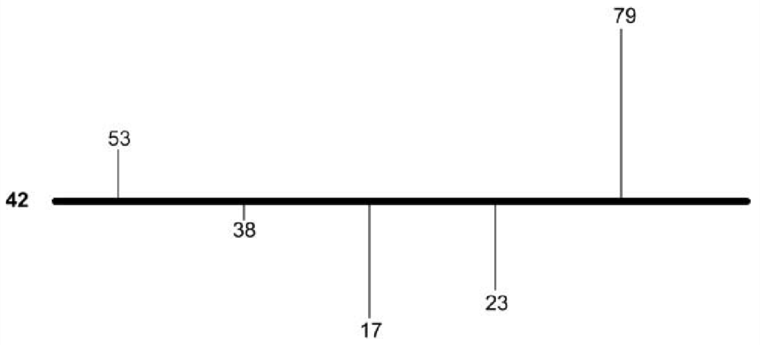
- Consider a sequence of integers: $53, 38, 17, 23$, and 79.



Target — Change The Sequence

- Invert elements around the average
  - Above $\leftrightarrow$ Below
  - **Absolute** distance of from average is preserved

- Consider a sequence of integers: $53, 38, 17, 23$, and 79.

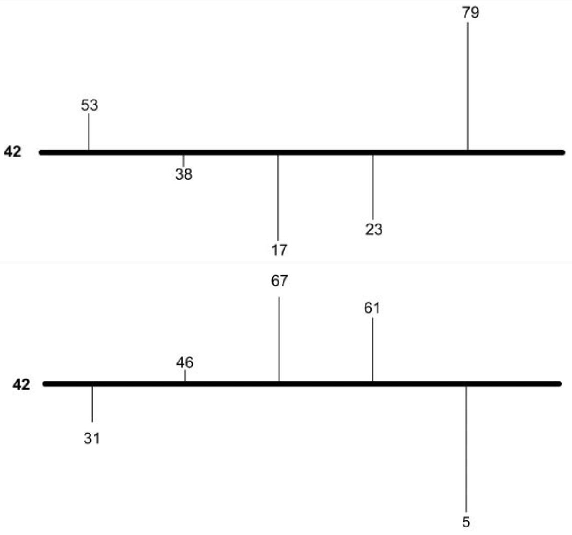


Example ($v' = a + (a - v) \implies v' = -v + 2a$)

53 (Above) $\rightarrow$ 31 (Below) $[a + (a - 53) = 31]$

38 (Below) $\rightarrow$ 46 (Above) $[a + (a - 38) = 46]$

Example — Inversion About The Mean/Average



$$\{53, 38, 17, 23, 79\} \xrightarrow{\text{Average, a} = 42} \{31, 46, 67, 61, 5\}$$

Exercise

- Consider the following numbers: 5, 38, 62, 58, 21, and 35. Invert these numbers around their mean.

Unitary Matrix For Inversion About The Mean

- Continuing with the example: $V = [53, 38, 17, 23, 79]^T$
- Consider the following operation: AV

$$\begin{bmatrix} \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \end{bmatrix} \begin{bmatrix} 53 \\ 38 \\ 17 \\ 23 \\ 79 \end{bmatrix} = \begin{bmatrix} 42 \\ 42 \\ 42 \\ 42 \\ 42 \end{bmatrix}$$

- So matrix A finds the **average** of a sequence.
- In terms of matrices, the formula $v' = -v + 2a$ becomes

$$V' = -V + 2AV = (-I + 2A)V$$

Unitary Matrix For Inversion About The Mean

$$(-I+2A) = \begin{bmatrix} (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) \end{bmatrix}$$

- In our case:

$$(-I+2A)[53, 38, 17, 23, 79]^T = [31, 46, 67, 61, 5]^T$$

$$A = \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} & \frac{1}{2^n} \end{bmatrix}$$

$(-I + 2A)$

$$\begin{bmatrix} \left(-1 + \frac{2}{2^n}\right) & \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} \\ \frac{2}{2^n} & \left(-1 + \frac{2}{2^n}\right) & \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} & \left(-1 + \frac{2}{2^n}\right) & \frac{2}{2^n} & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} & \left(-1 + \frac{2}{2^n}\right) & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} & \left(-1 + \frac{2}{2^n}\right) \end{bmatrix}$$

Exercise

- Prove that $-I + 2A$ is a unitary matrix.

Combining Trick-1 and Trick-2

- When considered separately, **phase inversion** and **inversion about the mean** are each innocuous operations.
- However, when combined, they are a very powerful operation that separates the amplitude of the desired state from those of all the other states.
- Let us do an example to understand this interplay of Trick-1 and Trick-2

- Consider the vector $[10, 10, 10, 10, 10]^T$.
- Target the fourth element:
- State after phase inversion:

$$[\quad,\quad,\quad,\quad,\quad]$$

- Average is:
- State after inversion about mean:

$$[\quad,\quad,\quad,\quad,\quad]$$

- The difference between the fourth element and all the others is:

- State after phase inversion:

$$[\quad,\quad,\quad,\quad,\quad]$$

- Average is:
- State after inversion about mean:

$$[\quad,\quad,\quad,\quad,\quad]$$

- The difference between the fourth element and all the others is:

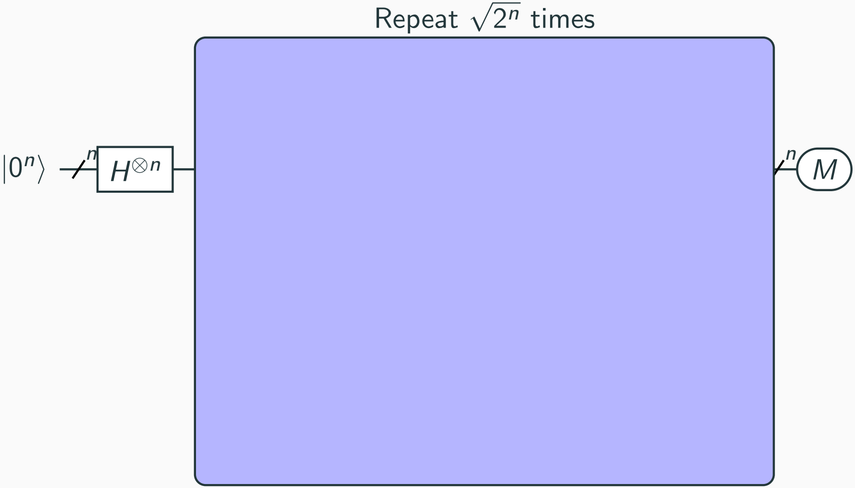
- **Step 1.** Start with a state $|0^n\rangle$
- **Step 2.** Apply $H^{\otimes n}|0^n\rangle$
- **Step 3.** Repeat $\sqrt{2^n}$ times:
  - **Step 3a.** Apply the phase inversion operation:

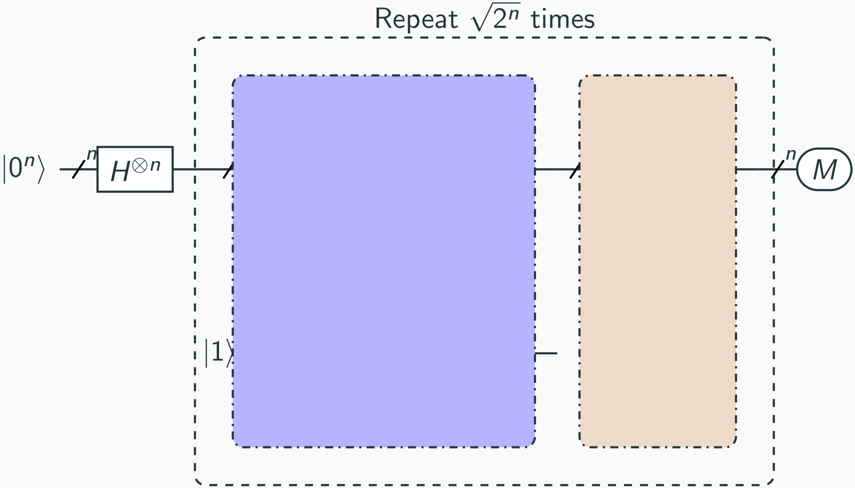
$$U_f(I \otimes H)$$

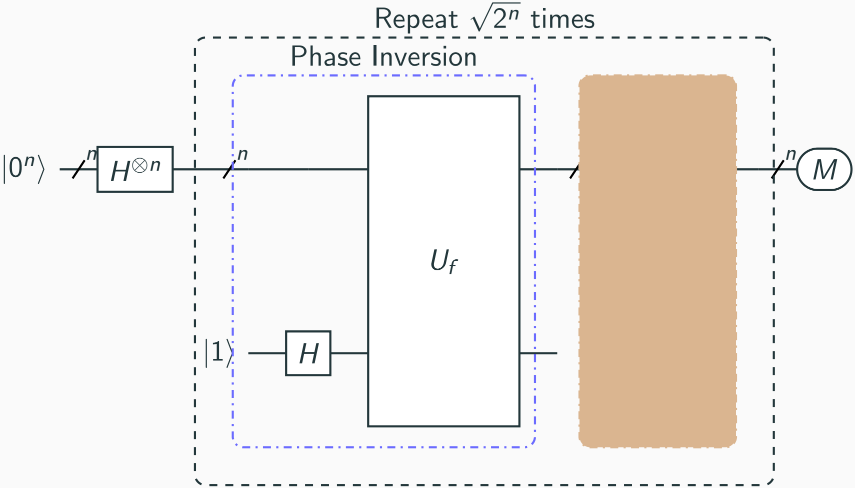
  - **Step 3b.** Apply the inversion about the mean operation:

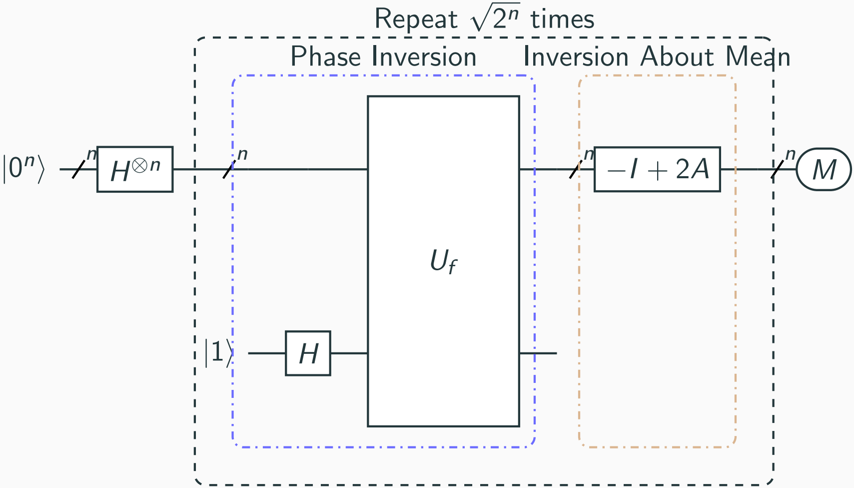
$$-I + 2A$$

- **Step 4.** Measure the qubits


Repeat $\sqrt{2^n}$ times
$|0^n\rangle$
n
$H^{\otimes n}$
n
M


Repeat $\sqrt{2^n}$ times
$|0^n\rangle$
n
$H^{\otimes n}$
$|1\rangle$
n
M


Repeat $\sqrt{2^n}$ times
Phase Inversion
$|0^n\rangle$
n
$H^{\otimes n}$
n
U_f
$|1\rangle$
H
n
M


Repeat $\sqrt{2^n}$ times
Phase Inversion
Inversion About Mean
$|0^n\rangle$
n
$H^{\otimes n}$
n
U_f
$|1\rangle$
H
n
$-I + 2A$
n
M

- Let f be a function that picks out the string "101".
- Initial state:

$$|\phi_1\rangle = \left[\overbrace{1}^{000}, \overbrace{0}^{001}, \overbrace{0}^{010}, \overbrace{0}^{011}, \overbrace{0}^{100}, \overbrace{0}^{101}, \overbrace{0}^{110}, \overbrace{0}^{111} \right]^T$$

- After $H^{\otimes n}$

$$|\phi_2\rangle = \left[\overbrace{\frac{1}{\sqrt{8}}}^{000}, \overbrace{\frac{1}{\sqrt{8}}}^{001}, \overbrace{\frac{1}{\sqrt{8}}}^{010}, \overbrace{\frac{1}{\sqrt{8}}}^{011}, \overbrace{\frac{1}{\sqrt{8}}}^{100}, \overbrace{\frac{1}{\sqrt{8}}}^{101}, \overbrace{\frac{1}{\sqrt{8}}}^{110}, \overbrace{\frac{1}{\sqrt{8}}}^{111} \right]^T$$

- After Phase Inversion

$$|\phi_{3a}\rangle = \left[\overbrace{\frac{1}{\sqrt{8}}}^{000}, \overbrace{\frac{1}{\sqrt{8}}}^{001}, \overbrace{\frac{1}{\sqrt{8}}}^{010}, \overbrace{\frac{1}{\sqrt{8}}}^{011}, \overbrace{\frac{1}{\sqrt{8}}}^{100}, \overbrace{\boxed{-\frac{1}{\sqrt{8}}}}^{101}, \overbrace{\frac{1}{\sqrt{8}}}^{110}, \overbrace{\frac{1}{\sqrt{8}}}^{111} \right]^T$$

- Average of the numbers:

$$a = \frac{}{} =$$

Example (f picks "101")

- Calculating the inversion about the mean:

$$For,\ \frac{1}{\sqrt{8}}, -v + 2a =$$

$$For,\ -\frac{1}{\sqrt{8}}, -v + 2a =$$

- After this step,

$$|\phi_{3b}\rangle = \left[\overbrace{\qquad}^{000}, \overbrace{\qquad}^{001}, \overbrace{\qquad}^{010}, \overbrace{\qquad}^{011}, \overbrace{\qquad}^{100}, \overbrace{\qquad}^{101}, \overbrace{\qquad}^{110}, \overbrace{\qquad}^{111} \right]^T$$

- Repeating... After phase inversion:

$$|\phi_{3a}\rangle = \Big[\overbrace{\qquad}^{000}, \overbrace{\qquad}^{001}, \overbrace{\qquad}^{010}, \overbrace{\qquad}^{011}, \overbrace{\qquad}^{100}, \overbrace{\qquad}^{101}, \overbrace{\qquad}^{110}, \overbrace{\qquad}^{111}\Big]^T$$

- Average of the numbers:

$$a = \frac{\qquad\qquad}{\qquad\qquad} =$$

- Calculating the inversion about the mean:

$$For,\ Case-1:, -v+2a=$$

$$For,\ Case-2:, -v+2a=$$

- After this step,

$$|\phi_{3b}\rangle = \left[\overbrace{\quad}^{000}, \overbrace{\quad}^{001}, \overbrace{\quad}^{010}, \overbrace{\quad}^{011}, \overbrace{\quad}^{100}, \overbrace{\quad}^{101}, \overbrace{\quad}^{110}, \overbrace{\quad}^{111}\right]^T$$

- What are the number values of the numbers in $|\phi_{3b}\rangle$?

$$Case - 1 : \qquad\qquad , Case - 2 :$$

- Let us square the numbers in $|\phi_{3b}\rangle$ to get the probabilities.

$$Case - 1 : \qquad\qquad , Case - 2 :$$

- Most probable state after measurement:

$$|\phi_4\rangle = \left[\overbrace{0}^{000}, \overbrace{0}^{001}, \overbrace{0}^{010}, \overbrace{0}^{011}, \overbrace{0}^{100}, \overbrace{\boxed{1}}^{101}, \overbrace{0}^{110}, \overbrace{0}^{111} \right]^T$$

Exercise

- Write a program in your favorite programming language to do a similar analysis for the case where $n = 4$ and f chooses the "1101" string?

- A classical algorithm will search an unordered array of size n in n steps.
- Grover's algorithm will take time $\sqrt{n}$.
- This is what is referred to as a **quadratic speedup**.

What happens if we repeat beyond $\sqrt{n}$

- The phase difference will degrade.
- The **overcooking** effect[1]!
- Let us look at Bernstein's Indocrypt 2021 Example to see a demonstration of this effect.

[1] Proof makes use of geometry. Needs another view of the systems

Quantum Search

Grover's Search Demo

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Grover's algorithm

Assume: unique $s \in \{0,1\}^n$
has $f(s) = 0$.

Goal: Figure out s.

Non-quantum algorithm to find s:
compute f for many inputs,
hope to find output 0.
Success probability is very low
until #tries approaches 2^n.

Grover's algorithm

Assume: unique $s \in \{0,1\}^n$
has $f(s) = 0$.

Goal: Figure out s.

Non-quantum algorithm to find s:
compute f for many inputs,
hope to find output 0.
Success probability is very low
until #tries approaches 2^n.

Grover's algorithm takes only $2^{n/2}$
quantum evaluations of f.
e.g. 2^{64} instead of 2^{128}.

Start from uniform superposition over n-bit strings u: each $a_u = 1$.

Start from uniform superposition over n-bit strings u: each $a_u = 1$.

Step 1: Set $a \leftarrow b$ where
$b_u = -a_u$ if $f(u) = 0$,
$b_u = a_u$ otherwise.
This is fast if f is fast.

Start from uniform superposition over n-bit strings u: each $a_u = 1$.

Step 1: Set $a \leftarrow b$ where
$b_u = -a_u$ if $f(u) = 0$,
$b_u = a_u$ otherwise.
This is fast if f is fast.

Step 2: "Grover diffusion".
Negate a around its average.
This is also fast.

Start from uniform superposition over n-bit strings u: each $a_u = 1$.

Step 1: Set $a \leftarrow b$ where
$b_u = -a_u$ if $f(u) = 0$,
$b_u = a_u$ otherwise.
This is fast if f is fast.

Step 2: "Grover diffusion".
Negate a around its average.
This is also fast.

Repeat Step 1 + Step 2 about $0.58 \cdot 2^{0.5n}$ times.

Start from uniform superposition
over n-bit strings u: each $a_u = 1$.

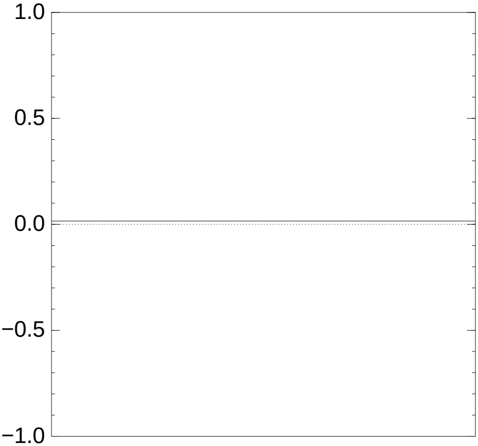
Step 1: Set $a \leftarrow b$ where
$b_u = -a_u$ if $f(u) = 0$,
$b_u = a_u$ otherwise.
This is fast if f is fast.

Step 2: "Grover diffusion".
Negate a around its average.
This is also fast.

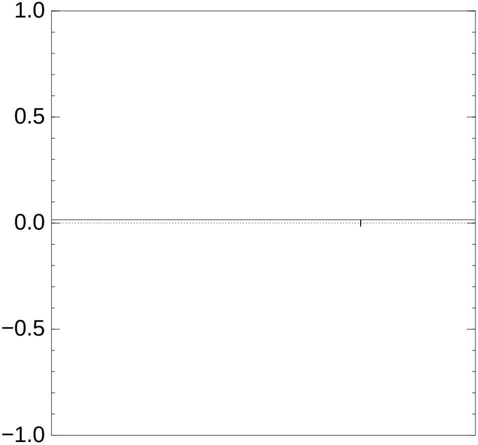
Repeat Step 1 + Step 2
about $0.58 \cdot 2^{0.5n}$ times.

Measure the n qubits.
With high probability this finds s.

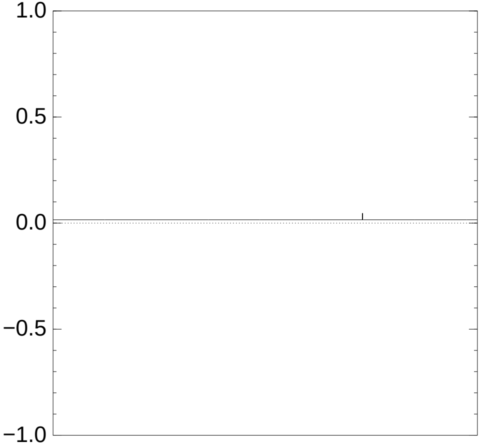
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after 0 steps:



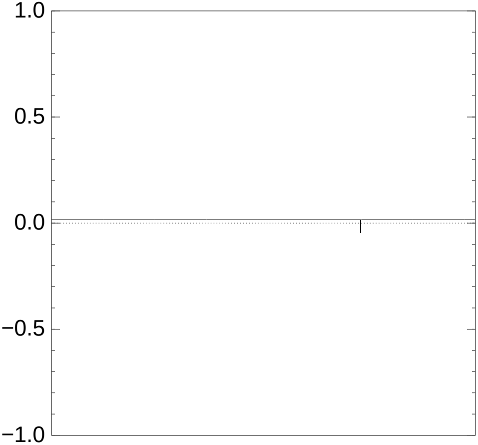
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after Step 1:



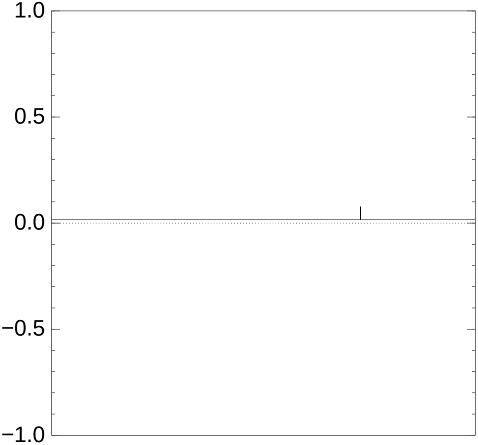
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after Step $1 +$ Step 2:



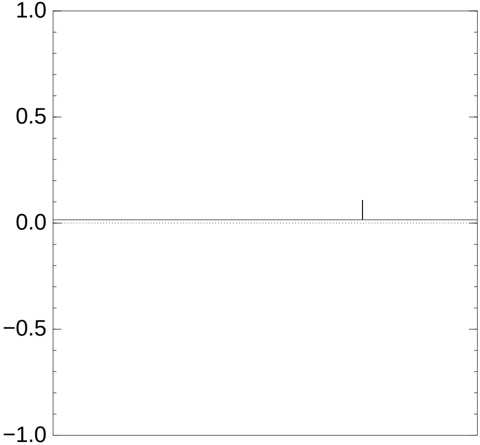
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after Step $1 +$ Step $2 +$ Step 1:



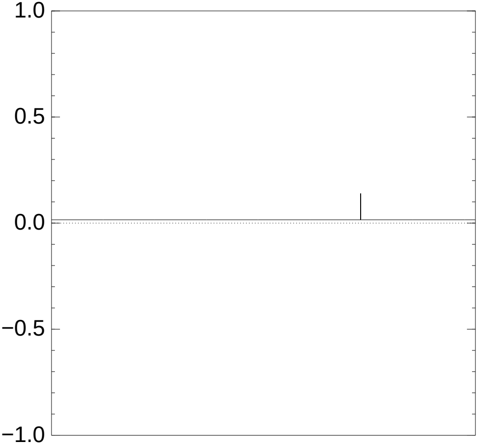
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $2 \times$ (Step $1 +$ Step 2):



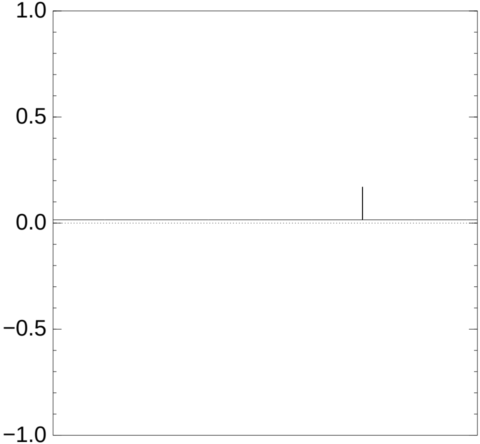
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $3 \times$ (Step 1 + Step 2):



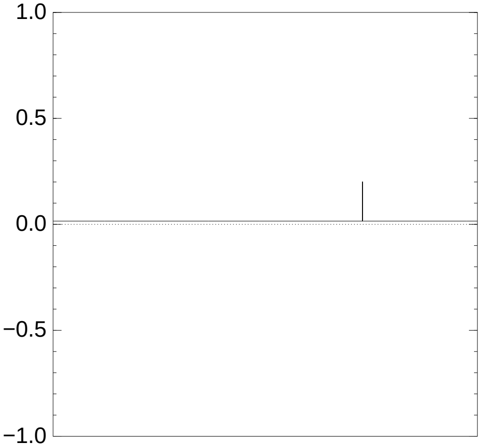
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $4 \times$ (Step 1 + Step 2):



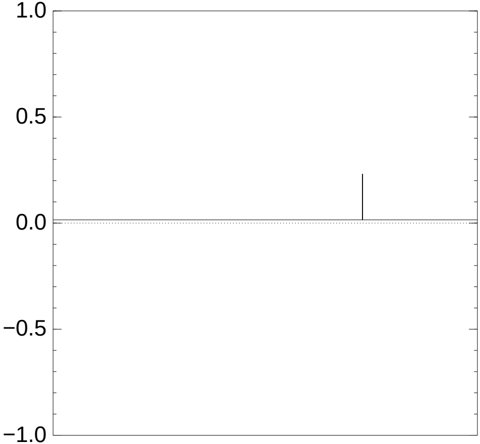
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $5 \times$ (Step 1 + Step 2):



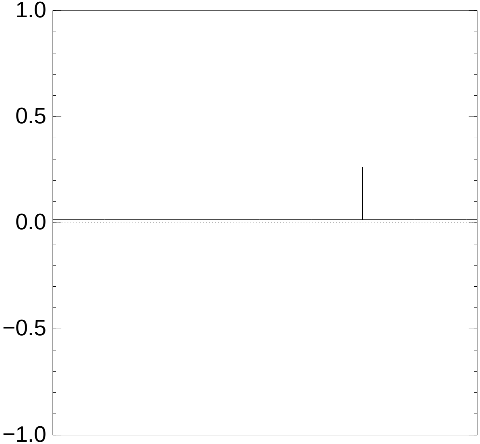
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $6 \times (\text{Step } 1 + \text{Step } 2)$:



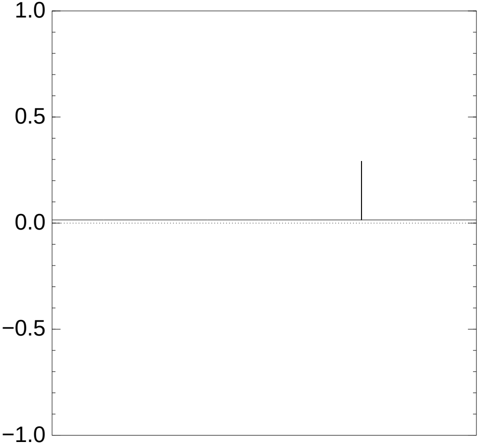
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $7 \times (\text{Step } 1 + \text{Step } 2)$:



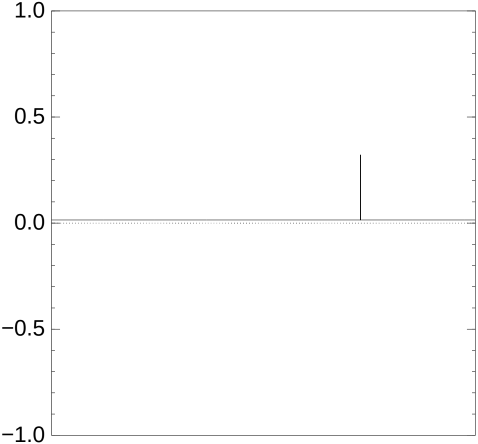
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $8 \times$ (Step 1 + Step 2):



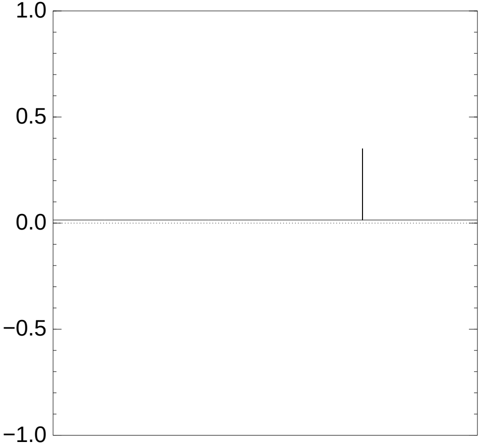
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $9 \times$ (Step 1 + Step 2):



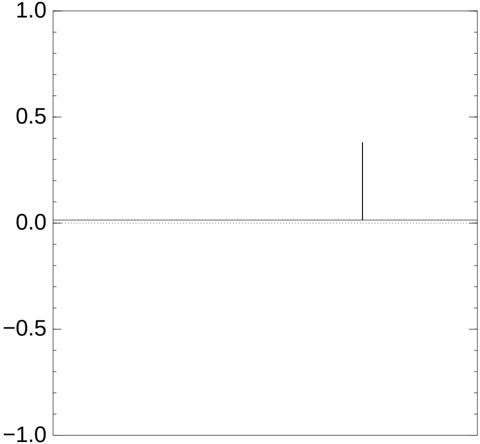
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $10 \times (\text{Step } 1 + \text{Step } 2)$:



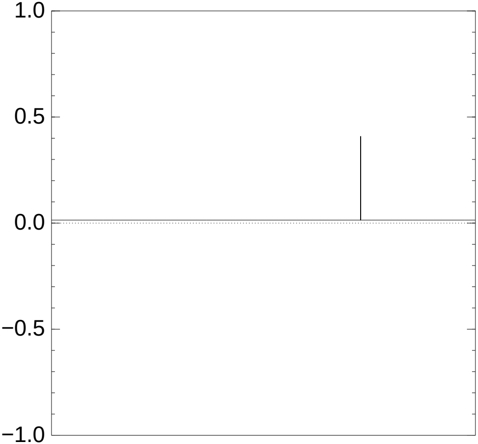
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $11 \times (\text{Step } 1 + \text{Step } 2)$:



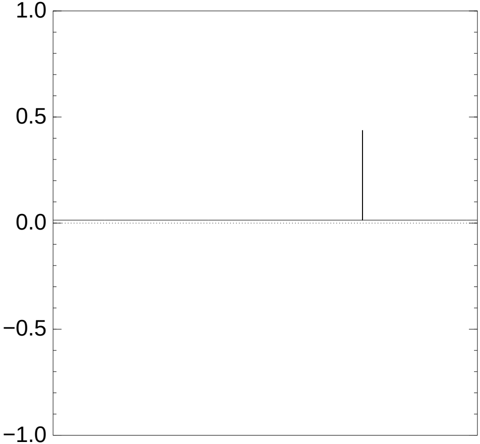
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $12 \times (\text{Step } 1 + \text{Step } 2)$:



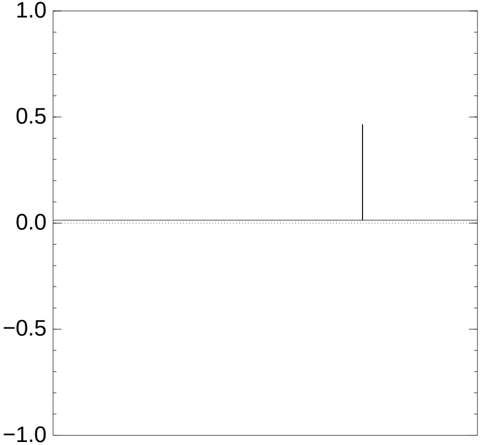
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $13 \times (\text{Step } 1 + \text{Step } 2)$:



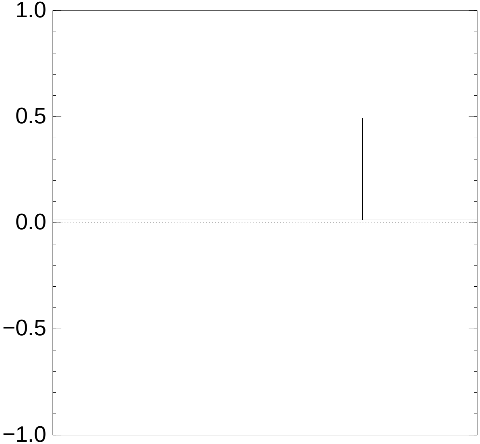
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $14 \times (\text{Step } 1 + \text{Step } 2)$:



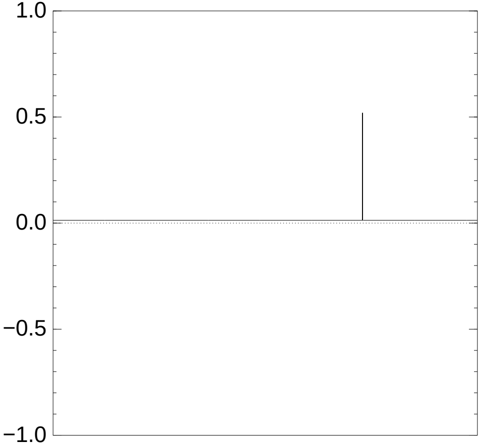
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $15 \times (\text{Step } 1 + \text{Step } 2)$:



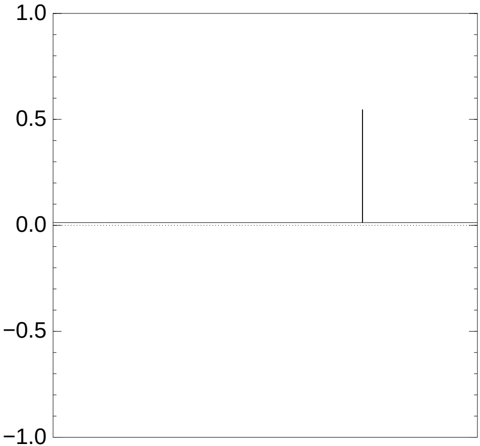
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $16 \times (\text{Step } 1 + \text{Step } 2)$:



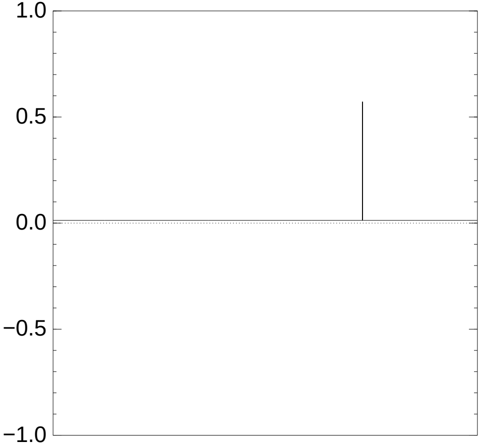
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $17 \times (\text{Step } 1 + \text{Step } 2)$:



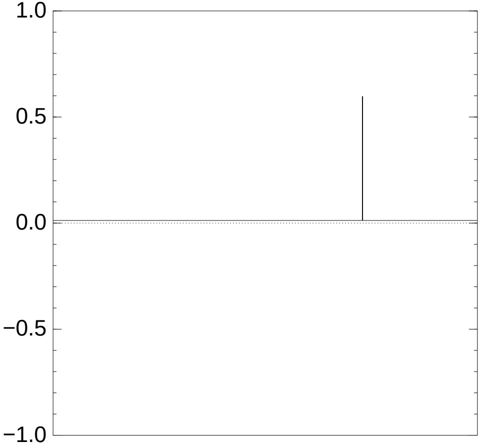
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $18 \times$ (Step 1 + Step 2):



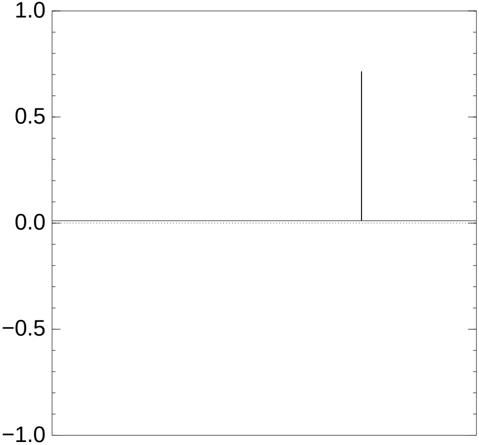
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $19 \times (\text{Step } 1 + \text{Step } 2)$:



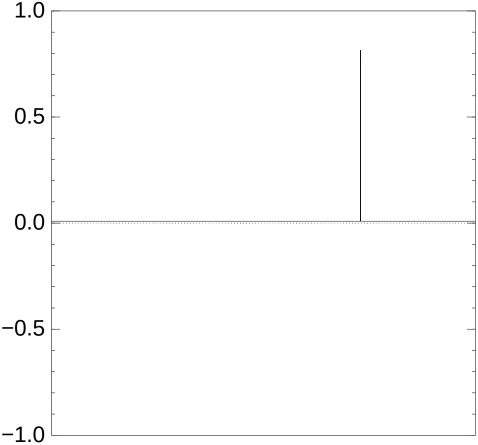
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $20 \times (\text{Step } 1 + \text{Step } 2)$:



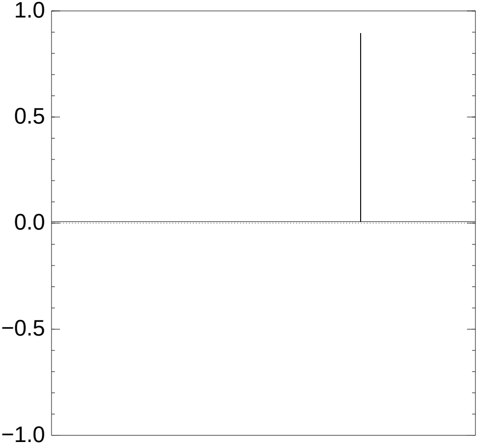
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $25 \times (\text{Step } 1 + \text{Step } 2)$:



Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $30 \times (\text{Step } 1 + \text{Step } 2)$:

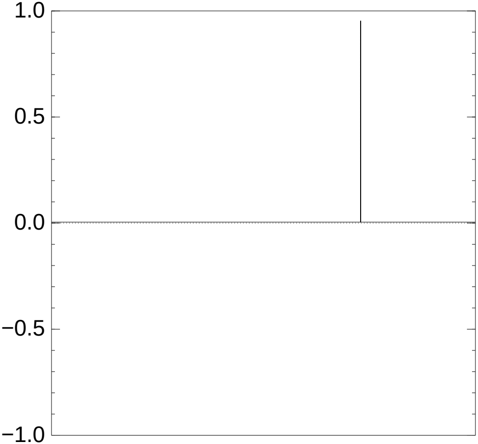


Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $35 \times$ (Step $1 +$ Step 2):

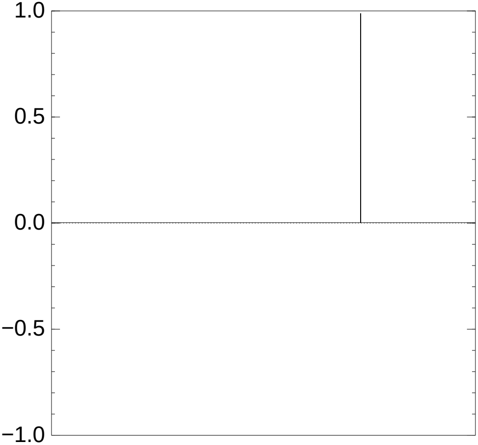


Good moment to stop, measure.

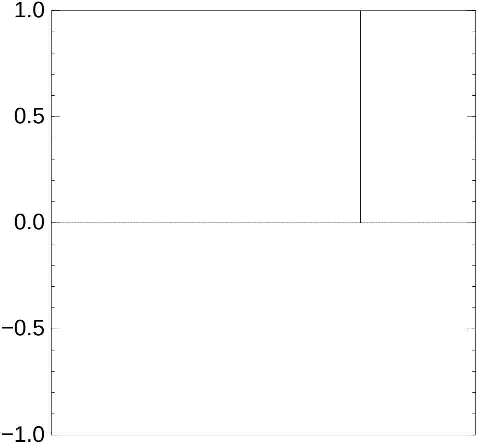
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $40 \times$ (Step $1 +$ Step 2):



Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $45 \times (\text{Step } 1 + \text{Step } 2)$:

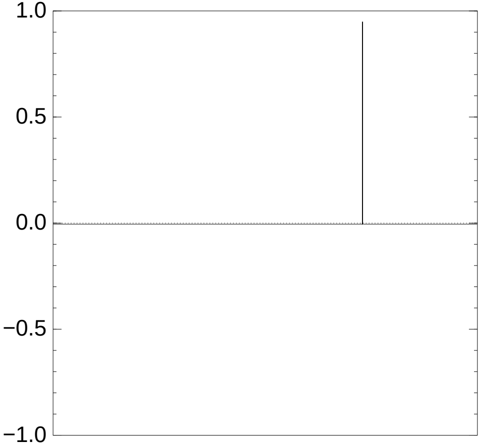


Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $50 \times (\text{Step } 1 + \text{Step } 2)$:

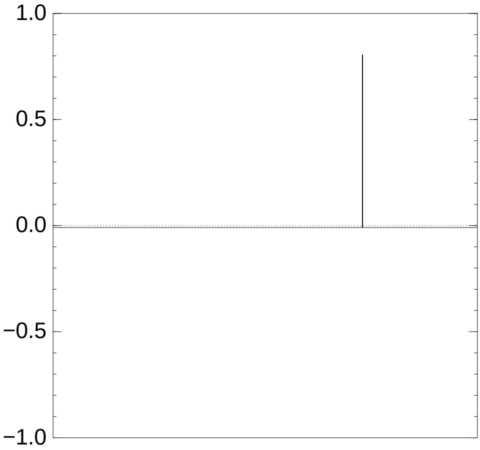


Traditional stopping point.

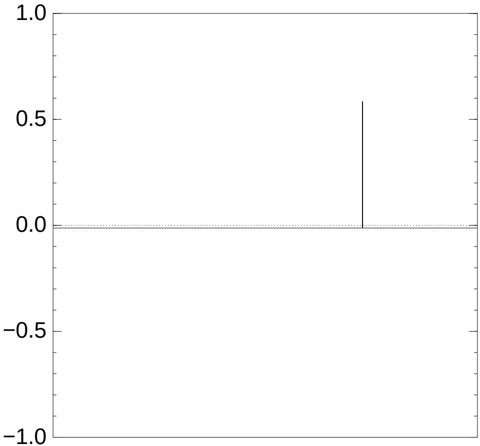
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $60 \times (\text{Step } 1 + \text{Step } 2)$:



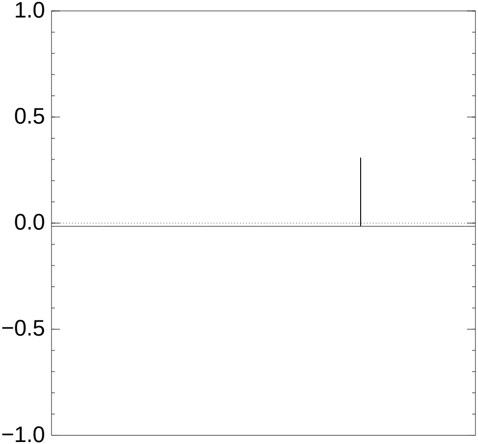
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $70 \times$ (Step $1 +$ Step 2):



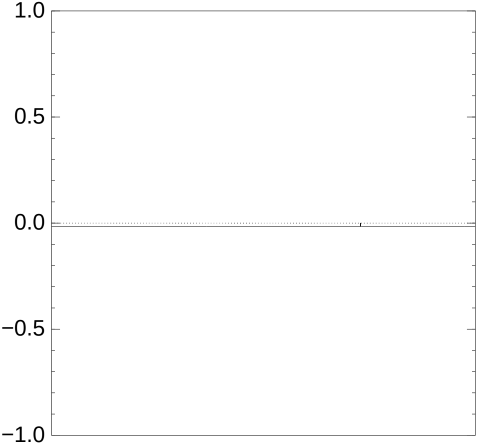
Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $80 \times (\text{Step } 1 + \text{Step } 2)$:



Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $90 \times (\text{Step } 1 + \text{Step } 2)$:



Normalized graph of $u \mapsto a_u$
for an example with $n = 12$
after $100 \times (\text{Step } 1 + \text{Step } 2)$:



Very bad stopping point.