19. Grover's algorithm

Grover’s algorithm

Deutsch’s algorithm and teleportation are impressive demonstrations, but still aren’t exactly useful tasks.

Grover’s algorithm is one of the first quantum algorithms that were shown that quantum computers are faster than classical computers AND it is useful.

Together with Shor’s algorithm for factoring numbers, it is two of the most famous quantum algorithms.

It is also provably faster than classical algorithms, so shows the power of quantum computing.

L.K. **Grover**,
“A Fast Quantum Mechanical **Algorithm** for Database Search”, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Pennsylvania, 212-219 (1996).

Searching a database

Suppose we have the task that we would like to search a large database of N entries.

In many databases that we use, the entries are sorted (e.g. by alphabetical order).

If the database is already sorted, then we can very quickly find any entry.

But if the database is unsorted, then we have to search through each entry until we find it.

Classically, the typical time scaling is

$$t \propto N$$

Or to use complexity theory notation the complexity is $O(N)$

index	License Number	Name	Address	City
1	F298-6588	Anderson, Roger David	77 Sunset Strip	Miami
2	L781-9586	Babcock, George Hale	1000 College Blvd	Pensacola
3	T585-7121	Brewer, Larry Mitchell	4801 E Fowler Ave	Tampa
4	L998-5456	Castle, Frederick Evan	8581 Navarre Pkwy	Navarre
5	F742-5421	Cantrell, Carolyn Elise	1500 Miracle Strip Pkwy	Ft Walton Beach
6	T626-3357	Dixon, Cynthia Louise	366 13th St	Santa Rosa Beach
7	T929-8985	Evans, Susan Elaine	301 Hollywood Blvd E	Mary Esther
8	L303-2621	Garrett, Patrick Sean	44 Bayshore Point	Valparaiso
9	R881-9881	Hartley, Matthew Paul	500 Wonderwood Dr	Jacksonville
10	R754-6523	Kensington, Carrie Ann	17000 Emerald Coast Pkwy	Destin
11	S755-6921	Lanouette, Phil	Margaritaville 500 Duval St	Key West
12	S181-1615	Mason, Daniel D	4607 State Park Lane	Panama City
13	L991-0220	Naylor, John T	900 N Birch Rd	Ft Lauderdale
14	R132-1895	Nicholas, Paul	6000 Universal Blvd	Orlando

The Oracle

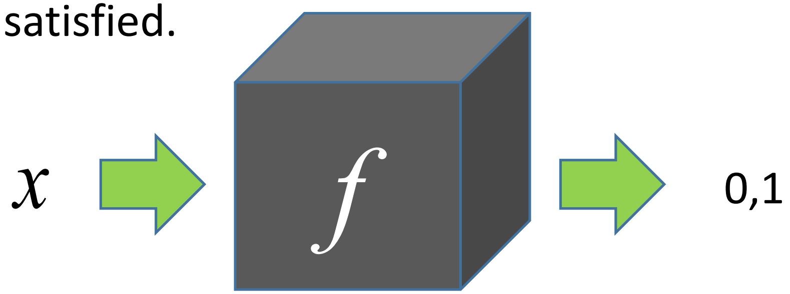
To mathematically frame this, let's define a function such that

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution} \\ 0 & \text{otherwise} \end{cases}$$

Here x is the index of the database

Then the task is to find $x = f^{-1}(1)$

We can think of f(x) as a black-box that tells us when the search criterion is satisfied.



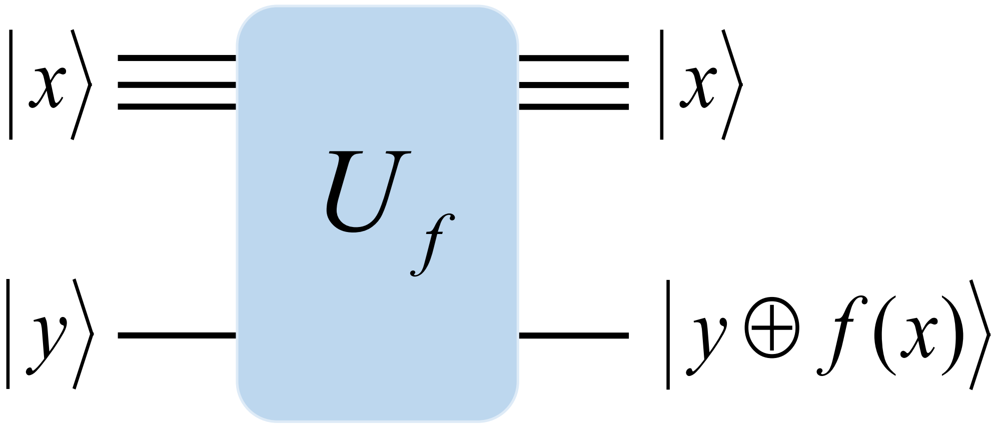
Such a setup where it is easy to calculate a function but difficult to invert is quite common. E.g. factoring numbers 36019=181x199

Desired database entries

x	f(x)
0	0
1	0
2	0
3	1
4	0
5	0
6	0
7	0
8	0
9	1
10	0
11	0

Quantum oracle

Let's use again the same oracle as in Deutsch's algorithm



n qubits, so $N = 2^n$

e.g. $|000\rangle, |001\rangle, \ldots, |111\rangle$

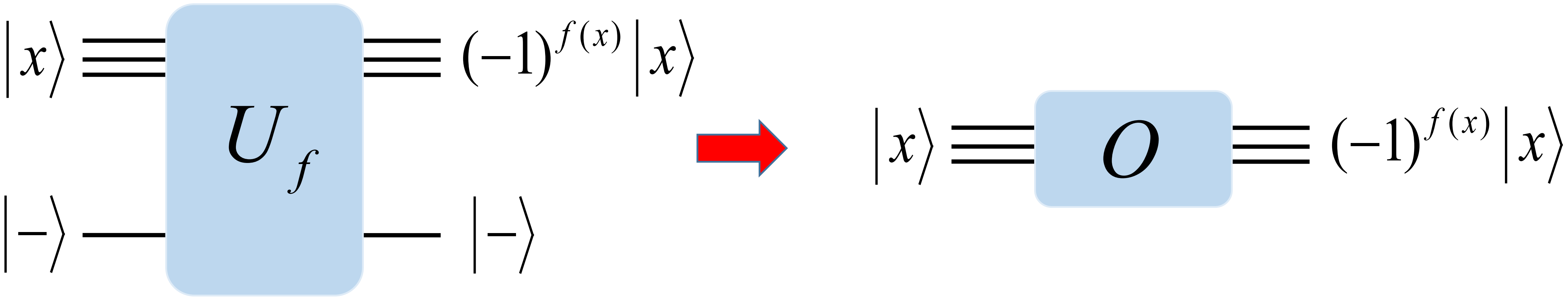
n=3, N=8

1 qubit

Flips y if f(x)=1, nothing otherwise

Quantum oracle

Recall that when $|y\rangle = |-\rangle$

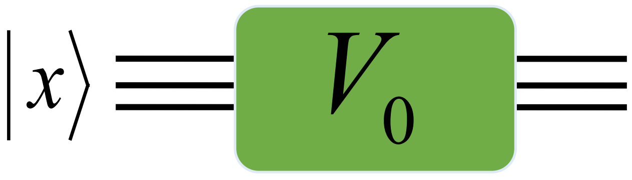


Since nothing happens to the bottom qubit, let's drop it and consider the Oracle operation defined as

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

Phase inversion

Now let’s also define (for reasons that will become clear later) the phase inversion operator

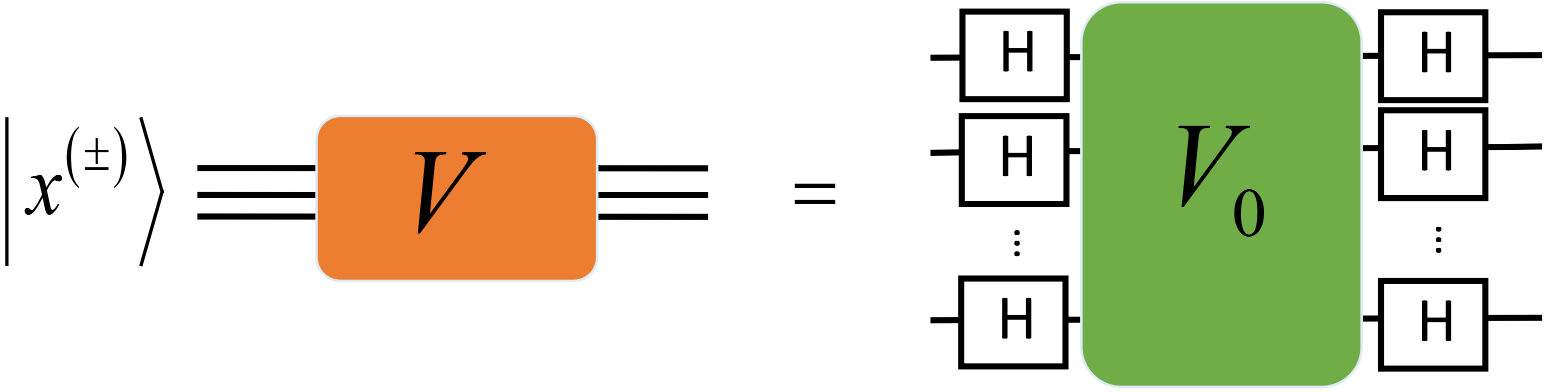


$$= \begin{cases} -|x\rangle & \text{if } x=0 \\ |x\rangle & \text{otherwise} \end{cases}$$

e.g.

$$V_0(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) =$$
$$-a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

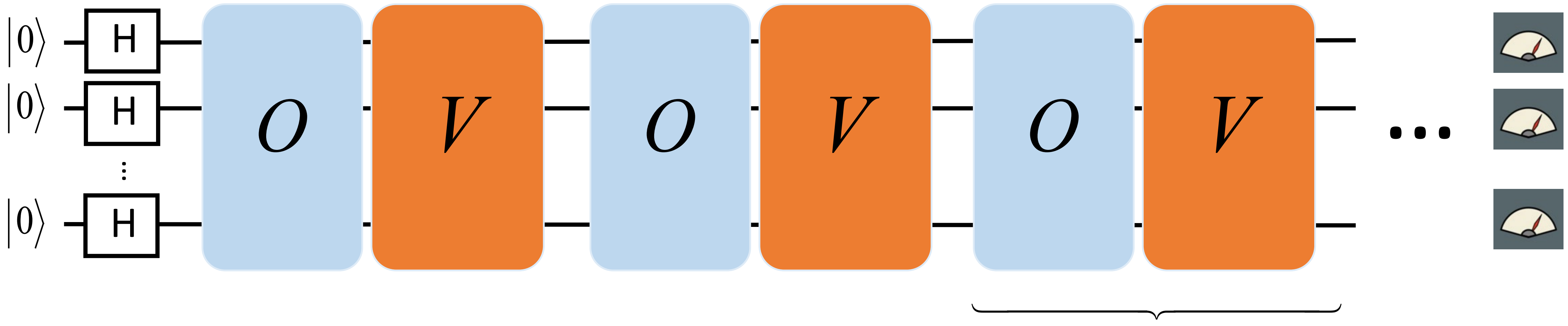
Actually we will use the operator in the |+>,|-> basis, which does



$$= \begin{cases} -|x^{(\pm)}\rangle & \text{if } x=+++++ \\ |x^{(\pm)}\rangle & \text{otherwise} \end{cases}$$

Grover's algorithm

With these elements, Grover's algorithm proceeds like below



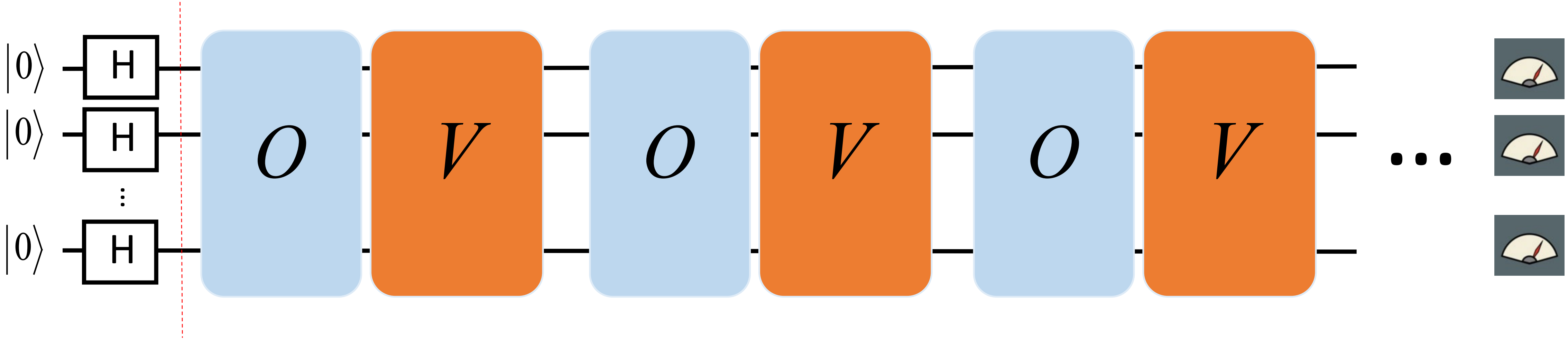
Repeat $\sqrt{N/M}$ times

N = Size of database
M= Number of solutions

After repeating the OV operations $\sqrt{N/M}$ times the state is measured to find the solutions.

How does this work?

Breakdown of Grover's algorithm



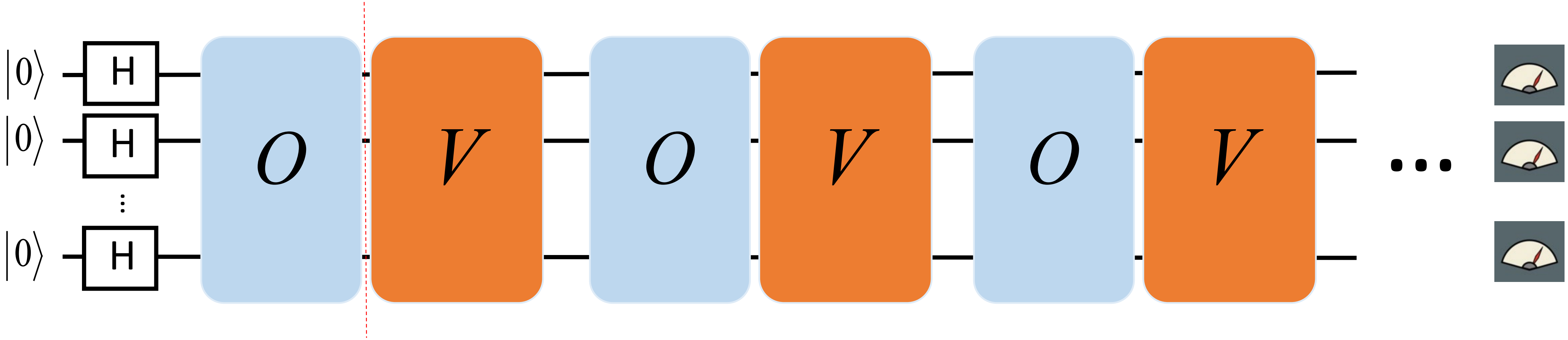
After the first Hadamard gate a superposition of all states is made

$$H_1 \ldots H_n |00\ldots0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\ldots\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\left(|0\ldots00\rangle + |0\ldots01\rangle + \ldots + |1\ldots11\rangle\right)$$

$$= |++\ldots+\rangle$$

Breakdown of Grover's algorithm



Next we will apply the Oracle. Since the Oracle is going to flip the sign of the "solution" states, let's define

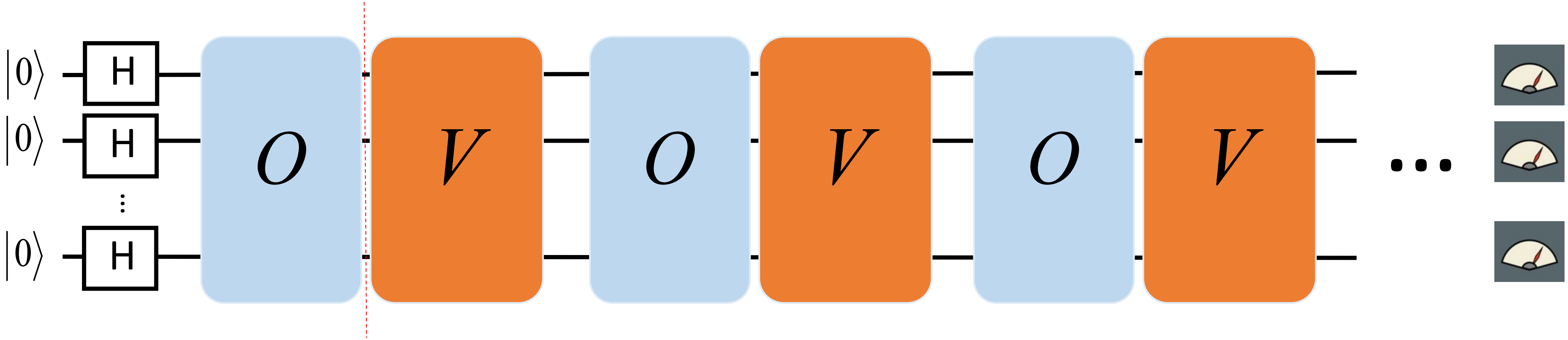
$$|x_{NOTsol}\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \{NOT solution\}} |x\rangle \qquad N = 2^n$$

$$|x_{sol}\rangle = \frac{1}{\sqrt{M}} \sum_{x \in \{solution\}} |x\rangle$$

Then we can write our state before the Oracle is applied as

$$|++\ldots+\rangle = \frac{1}{\sqrt{N}}\left(|0\ldots00\rangle + |0\ldots01\rangle + \ldots + |1\ldots11\rangle\right) = \sqrt{\frac{N-M}{N}}|x_{NOTsol}\rangle + \sqrt{\frac{M}{N}}|x_{sol}\rangle$$

Breakdown of Grover's algorithm



When we apply the Oracle then we have

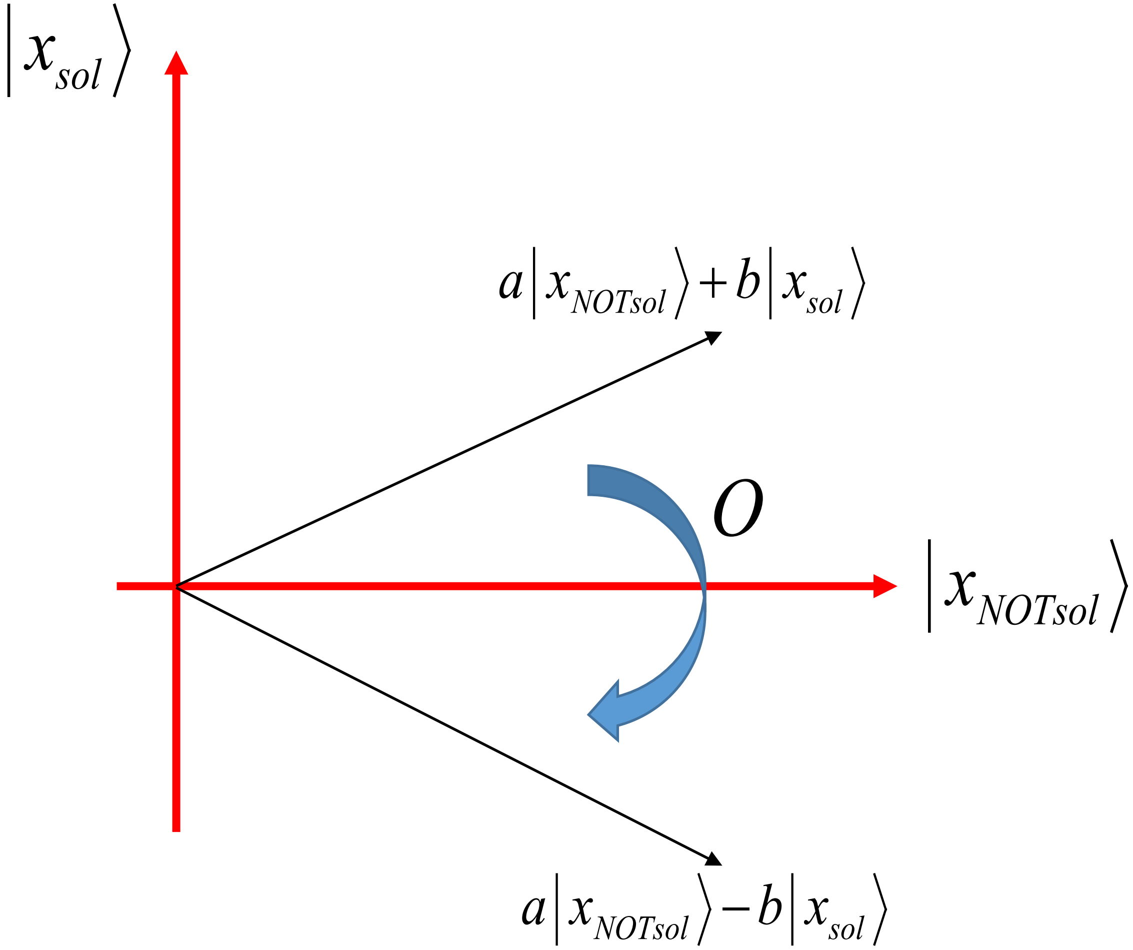
$$O|++\ldots+\rangle = \sqrt{\frac{N-M}{N}}|x_{NOTsol}\rangle - \sqrt{\frac{M}{N}}|x_{sol}\rangle$$

More generally

$$O\left(a|x_{NOTsol}\rangle + b|x_{sol}\rangle\right) = a|x_{NOTsol}\rangle - b|x_{sol}\rangle$$

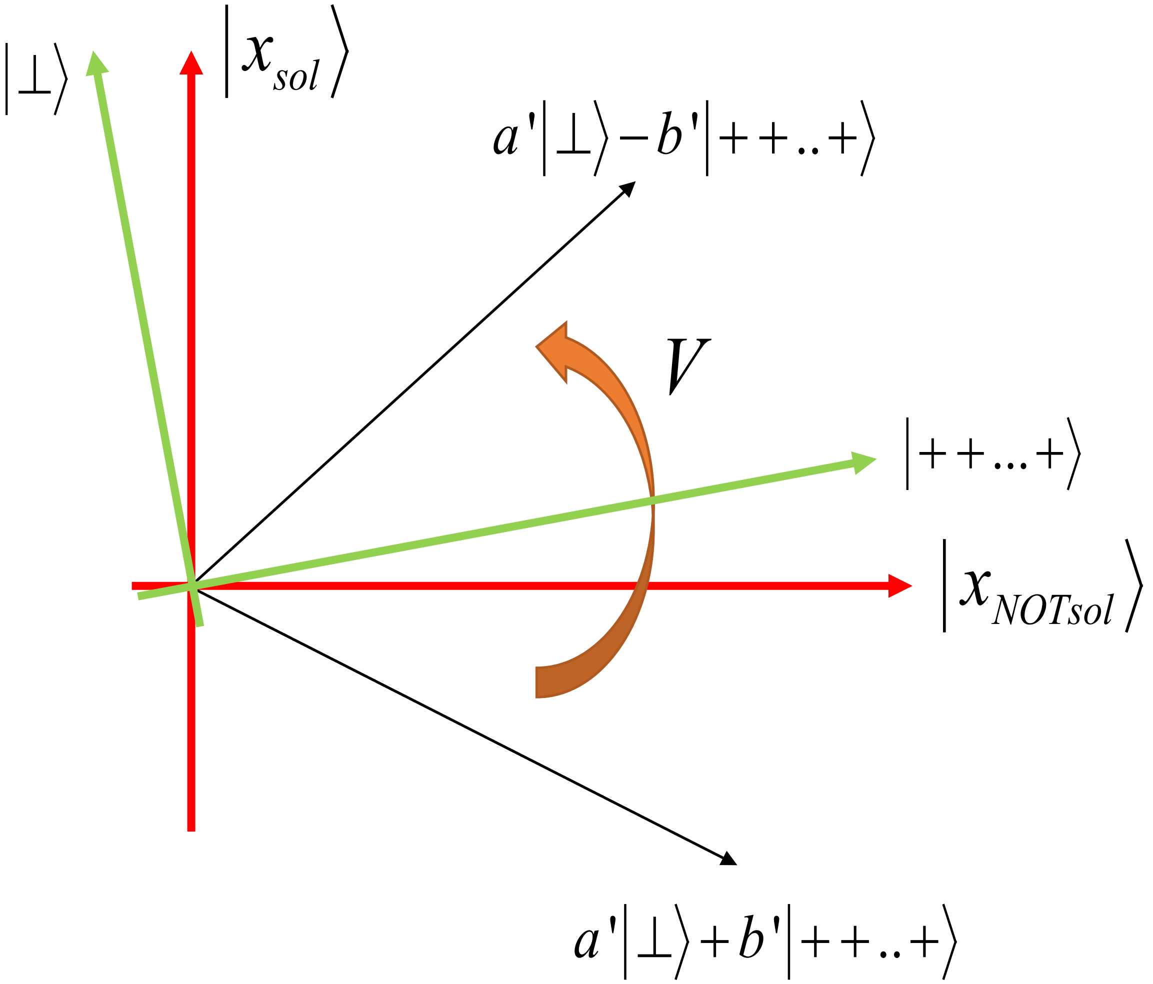
A geometrical way to view this is that the Oracle a reflection of the state about $|x_{sol}\rangle$

$$O\left(a|x_{NOTsol}\rangle + b|x_{sol}\rangle\right) = a|x_{NOTsol}\rangle - b|x_{sol}\rangle$$



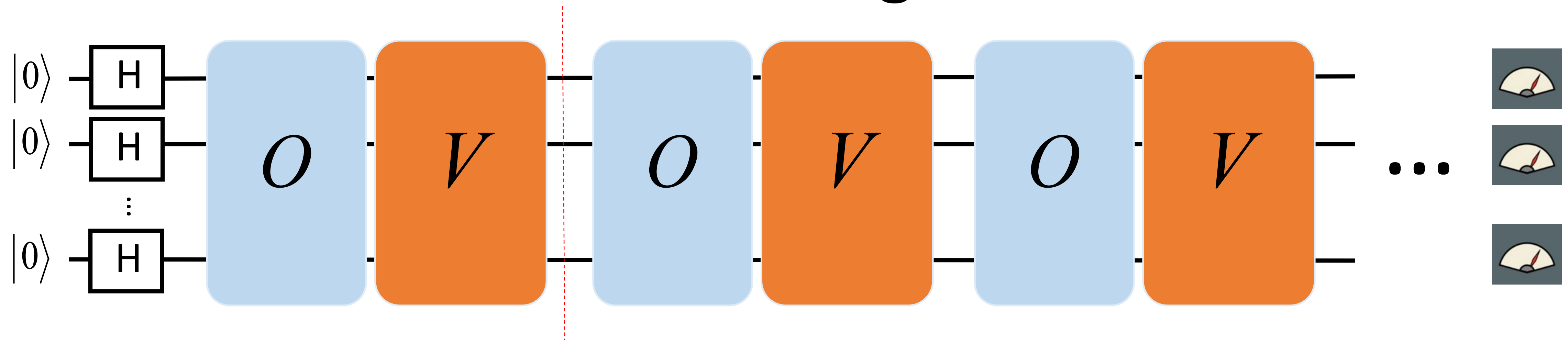
Similarly the V operation reflects around another set of axes

$$V\left(a'|\perp\rangle + b'|++..+\rangle\right) = a'|\perp\rangle - b'|++..+\rangle$$



$$|++...+\rangle = \sqrt{\frac{N-M}{N}}|x_{NOTsol}\rangle + \sqrt{\frac{M}{N}}|x_{sol}\rangle$$

Breakdown of Grover's algorithm



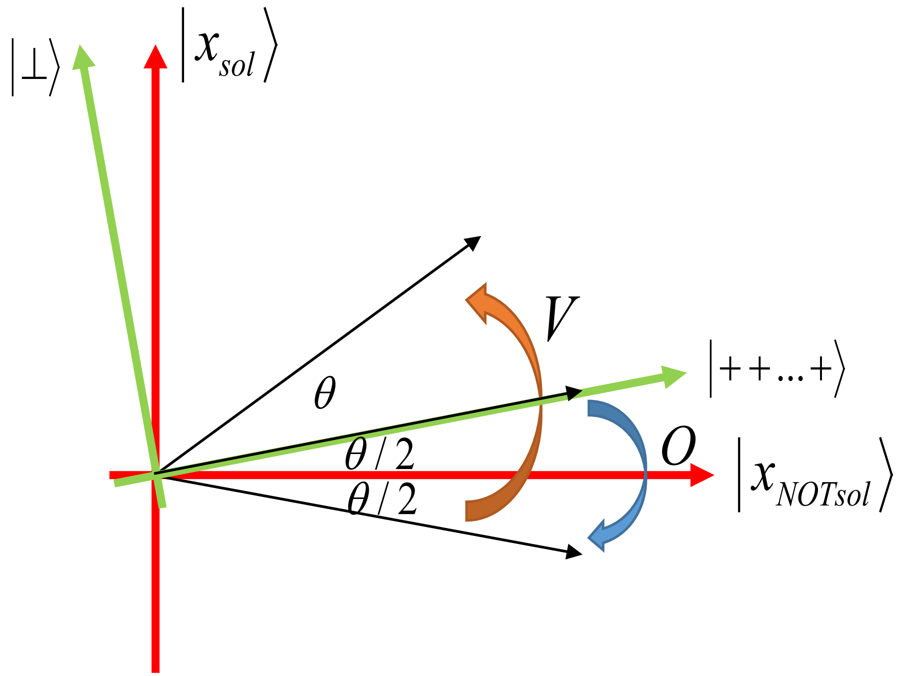
This means that after the first OV pair, the state ends us closer to the solution states!

Defining $\cos(\theta/2)=\sqrt{\frac{N-M}{N}}$ $\sin(\theta/2)=\sqrt{\frac{M}{N}}$

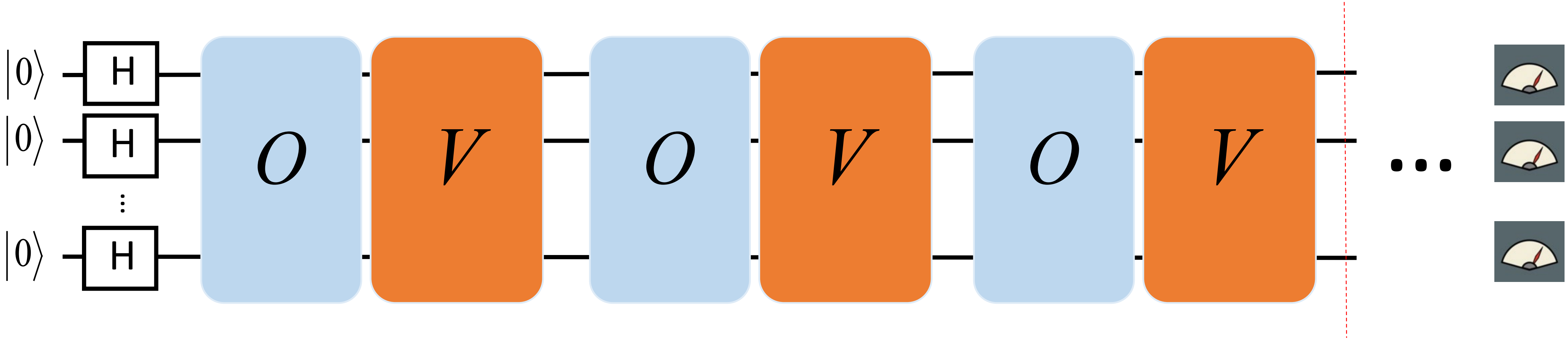
$$|++\ldots+\rangle=\sqrt{\frac{N-M}{N}}|x_{NOTsol}\rangle+\sqrt{\frac{M}{N}}|x_{sol}\rangle=\cos\frac{\theta}{2}|x_{NOTsol}\rangle+\sin\frac{\theta}{2}|x_{sol}\rangle$$

Then

$$VO|++\ldots+\rangle=\cos\frac{3\theta}{2}|x_{NOTsol}\rangle+\sin\frac{3\theta}{2}|x_{sol}\rangle$$



Breakdown of Grover's algorithm



After k applications of VO we have

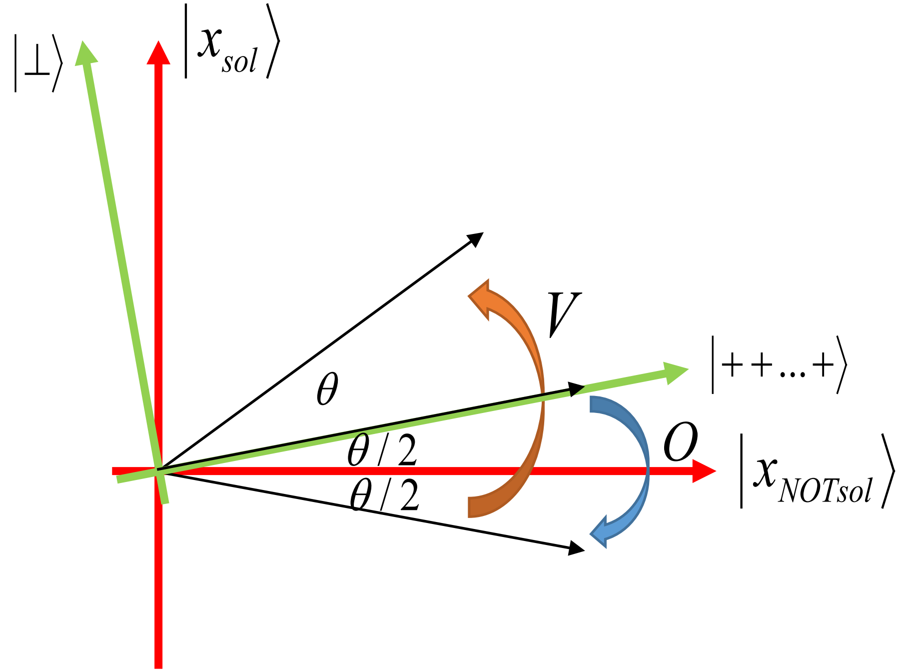
$$(VO)^k |++\ldots+\rangle = \cos\frac{(2k+1)\theta}{2}|x_{NOTsol}\rangle + \sin\frac{(2k+1)\theta}{2}|x_{sol}\rangle$$

If $\dfrac{(2k+1)\theta}{2} = \dfrac{\pi}{2}$ we have a large amplitude of the solutions for

$$k + 1/2 = \frac{\pi}{4\sin^{-1}\sqrt{\frac{M}{N}}}$$

$$\boxed{k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}}$$

Quantum speedup!



Summary

Using the superposition principle in a quantum computer we can perform database search with complexity $O\left(\sqrt{\frac{N}{M}}\right)$

The classical complexity for an unsorted database is $O\left(\frac{N}{M}\right)$

The difference is "only" quadratic, but can be large if N is big. E.g. if $N = 10^{15} \approx 2^{50}, \quad \sqrt{N} = 3 \times 10^{7}$

It is highly versatile, since searching is a generic problem.

e.g. optimization problems, NP-complete problems, etc.

Does not change the complexity class since it is a quadratic speedup, so not always a way to beat classical heuristics.

There exists ways of counting M so that the number of solutions can be calculated ("quantum counting") so that the number of iterations can be known in advance.