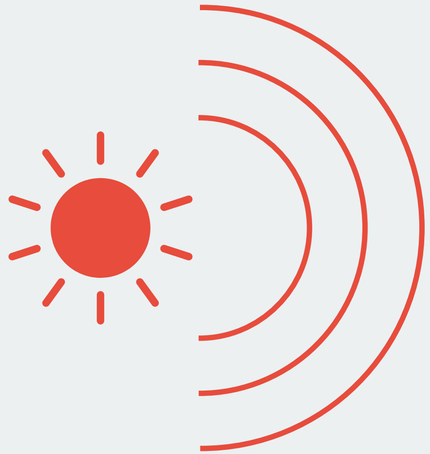
UVOD V
KVANTNO RAČUNALNIŠTVO

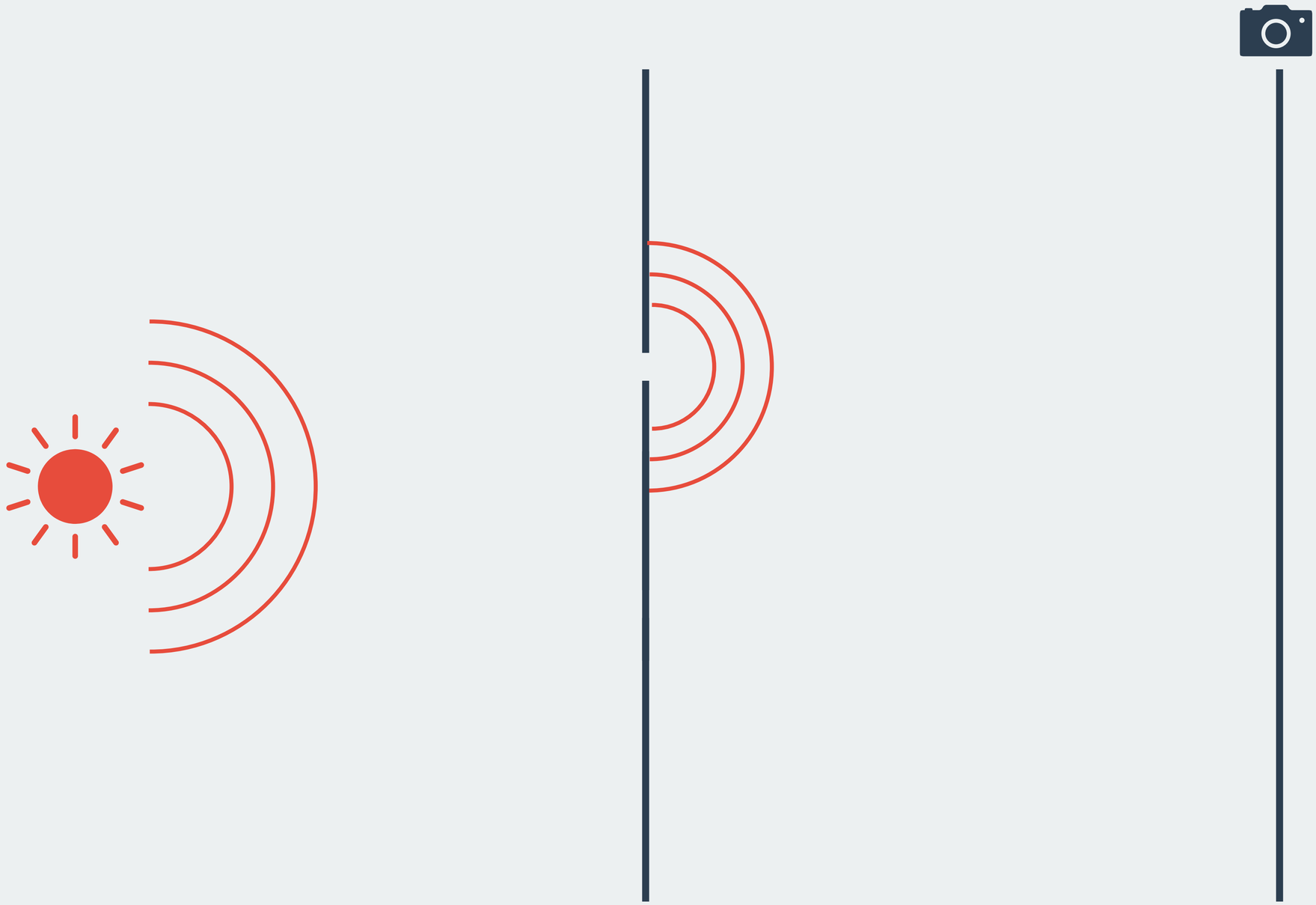
Matija Pretnar

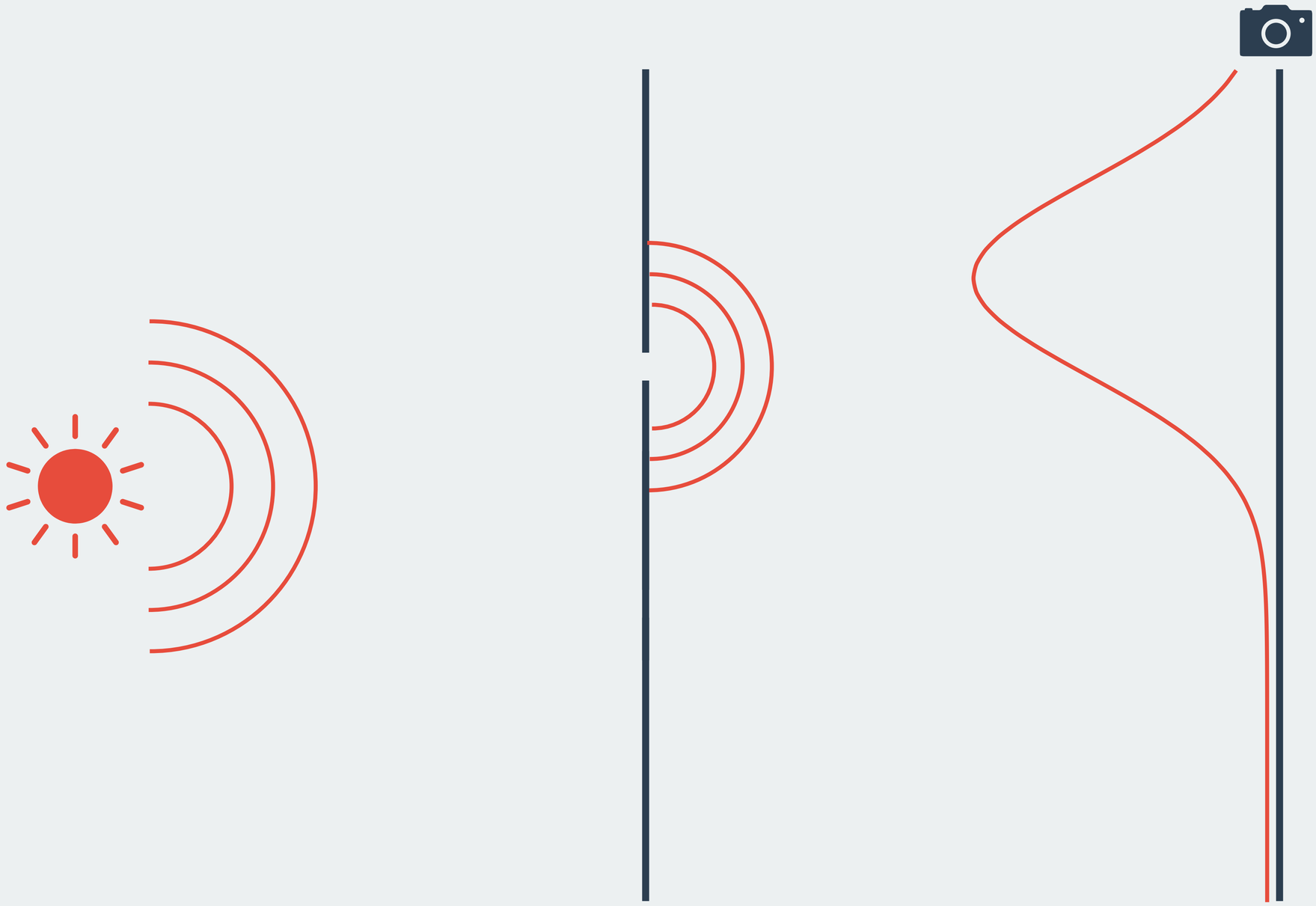
FMF
UNIVERZA V LJUBLJANI
Fakulteta za matematiko in fiziko

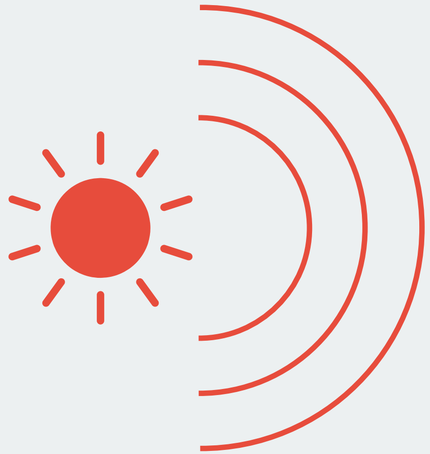
KVANTNO

RAČUNALNIŠTVO

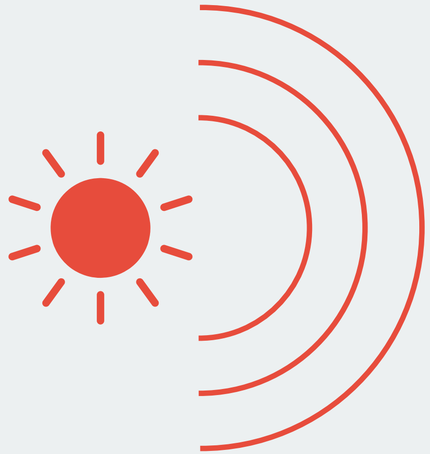


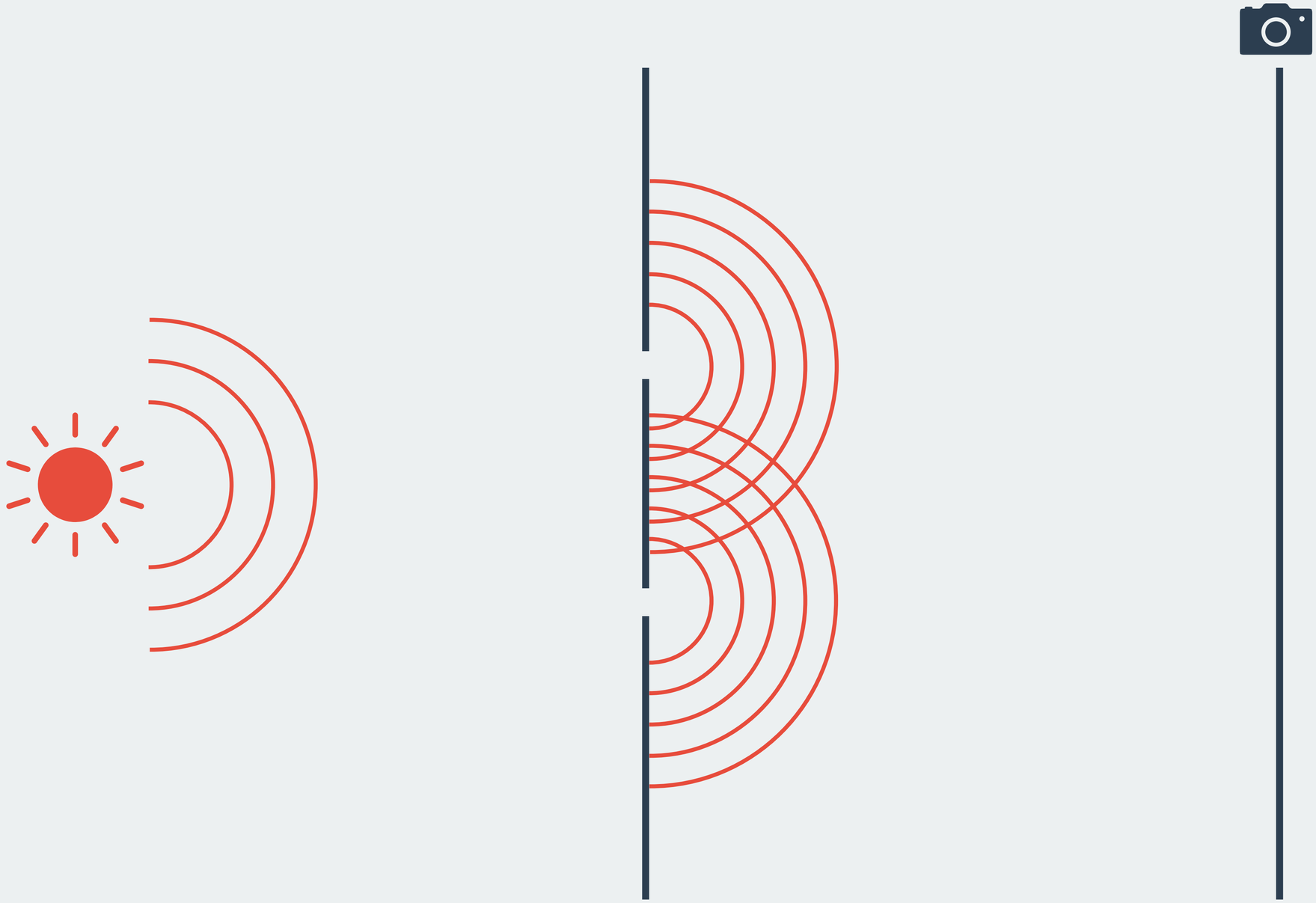


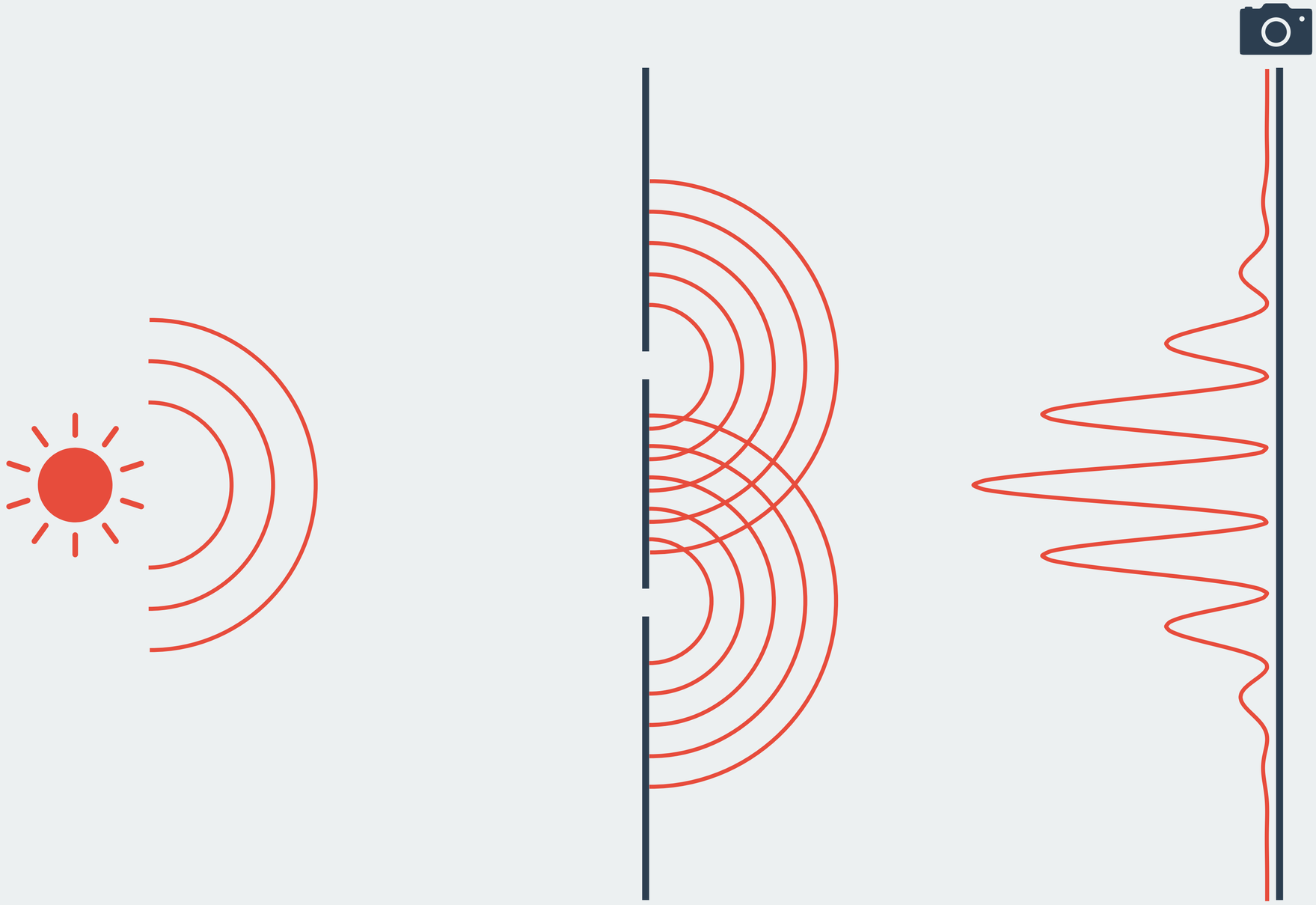


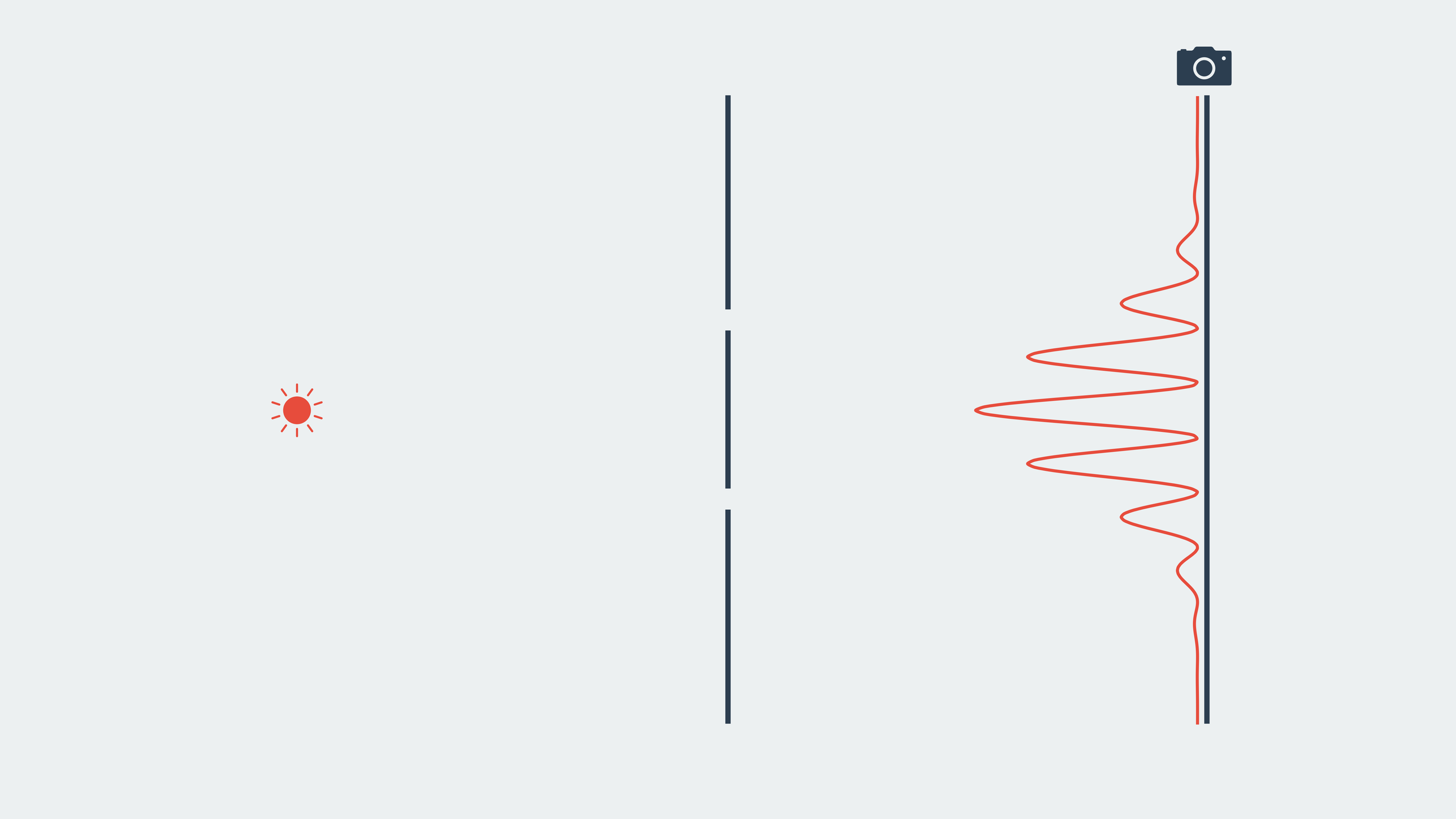


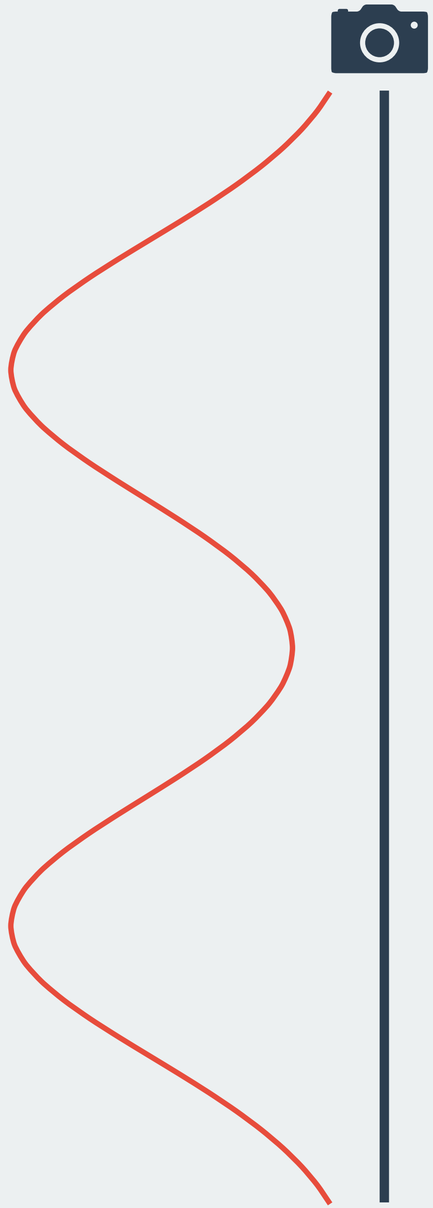

Jay E. Newman









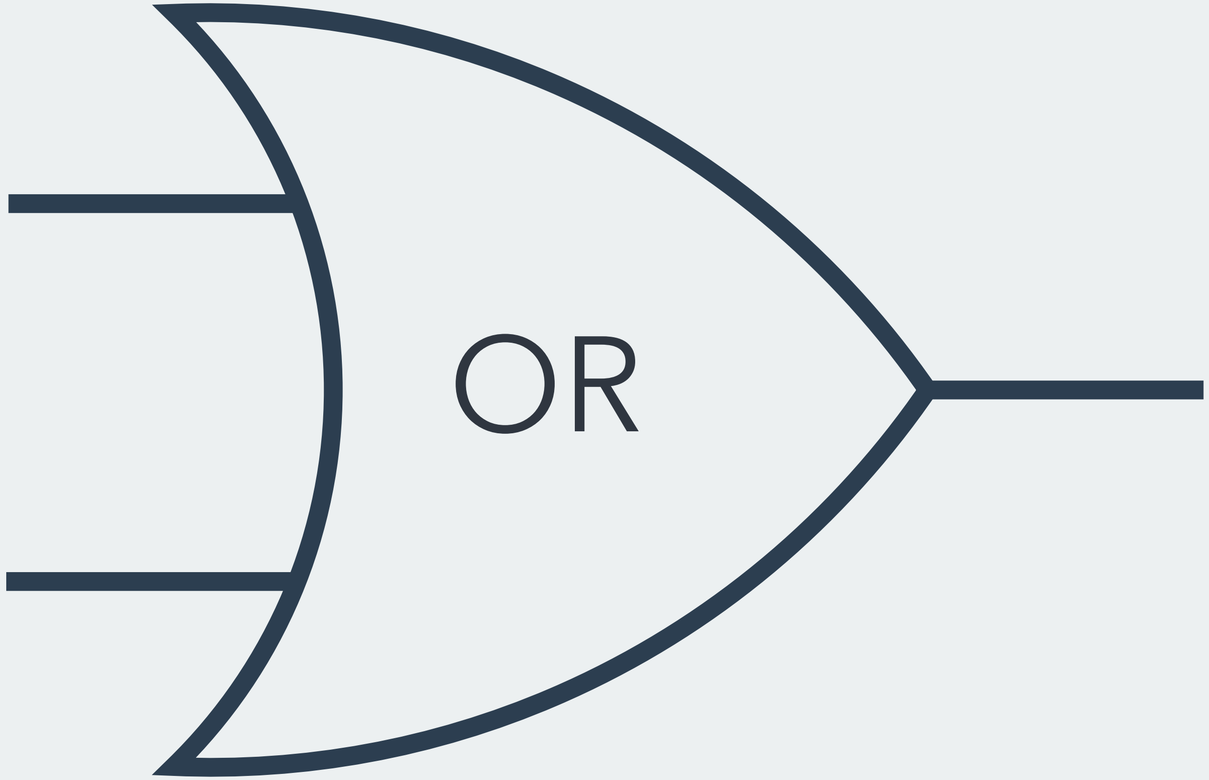


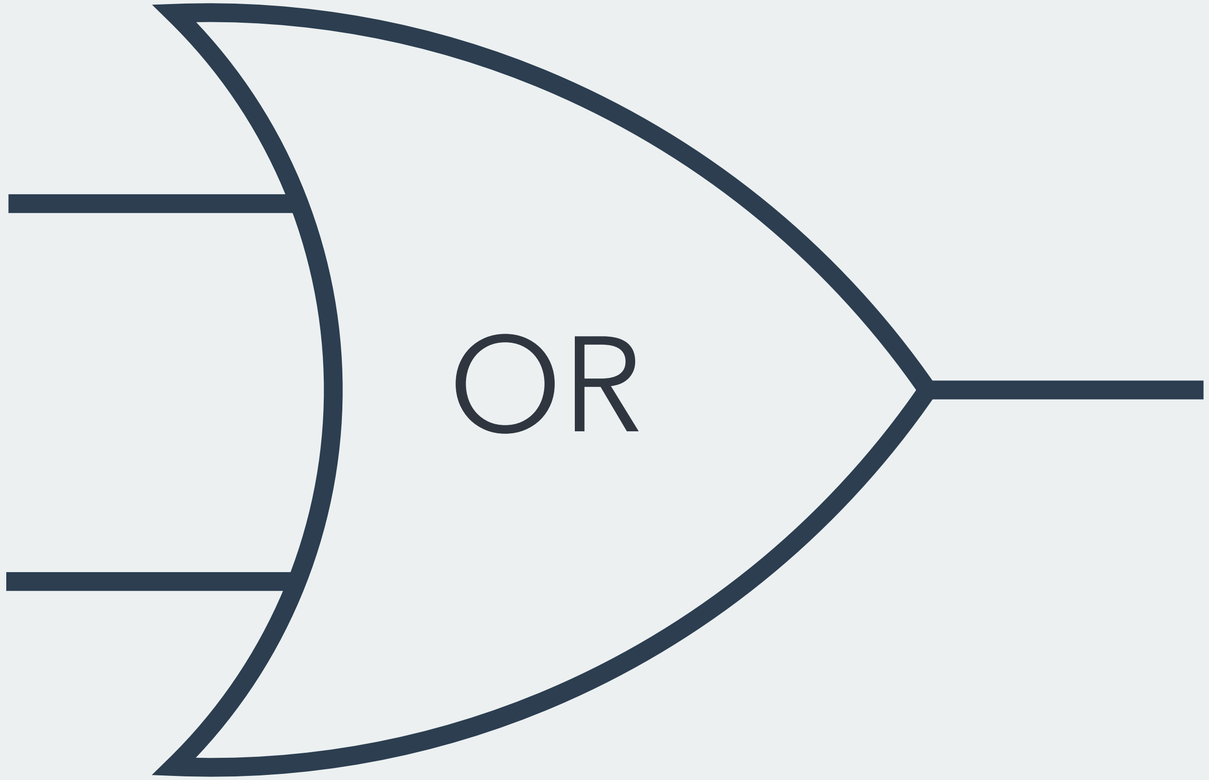
KVANTNO

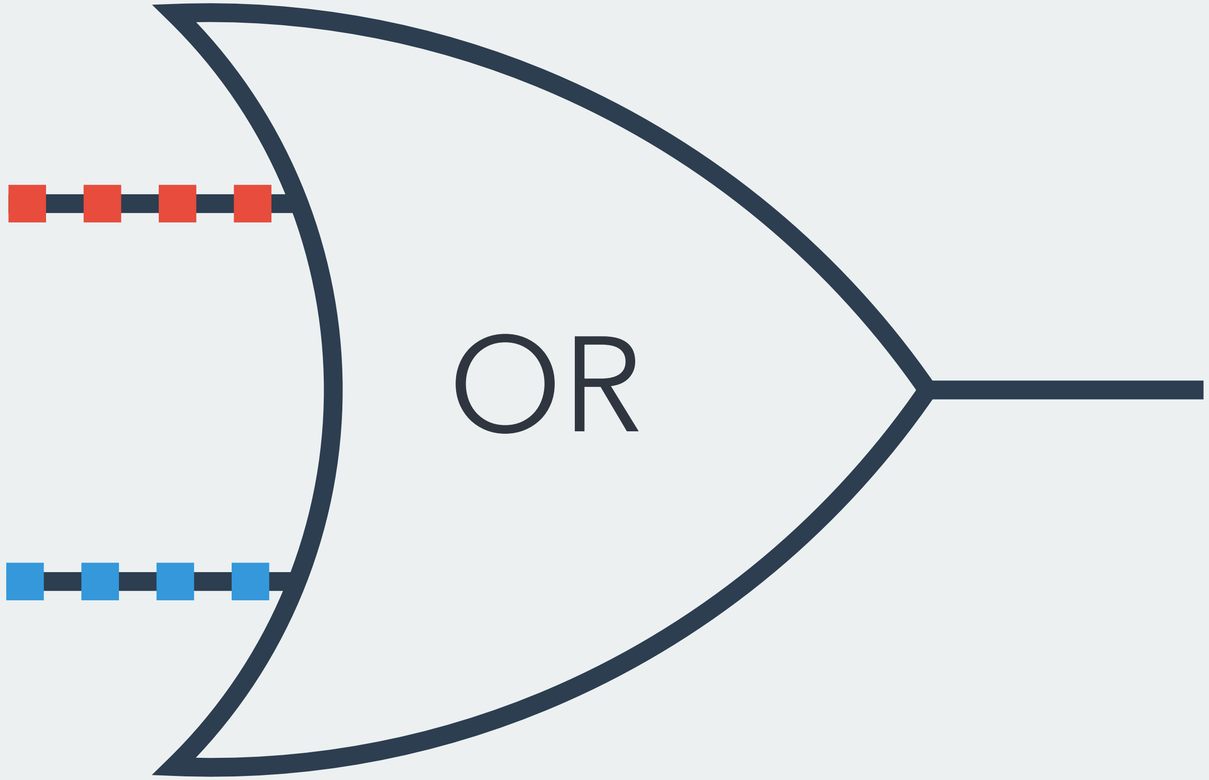
RAČUNALNIŠTVO

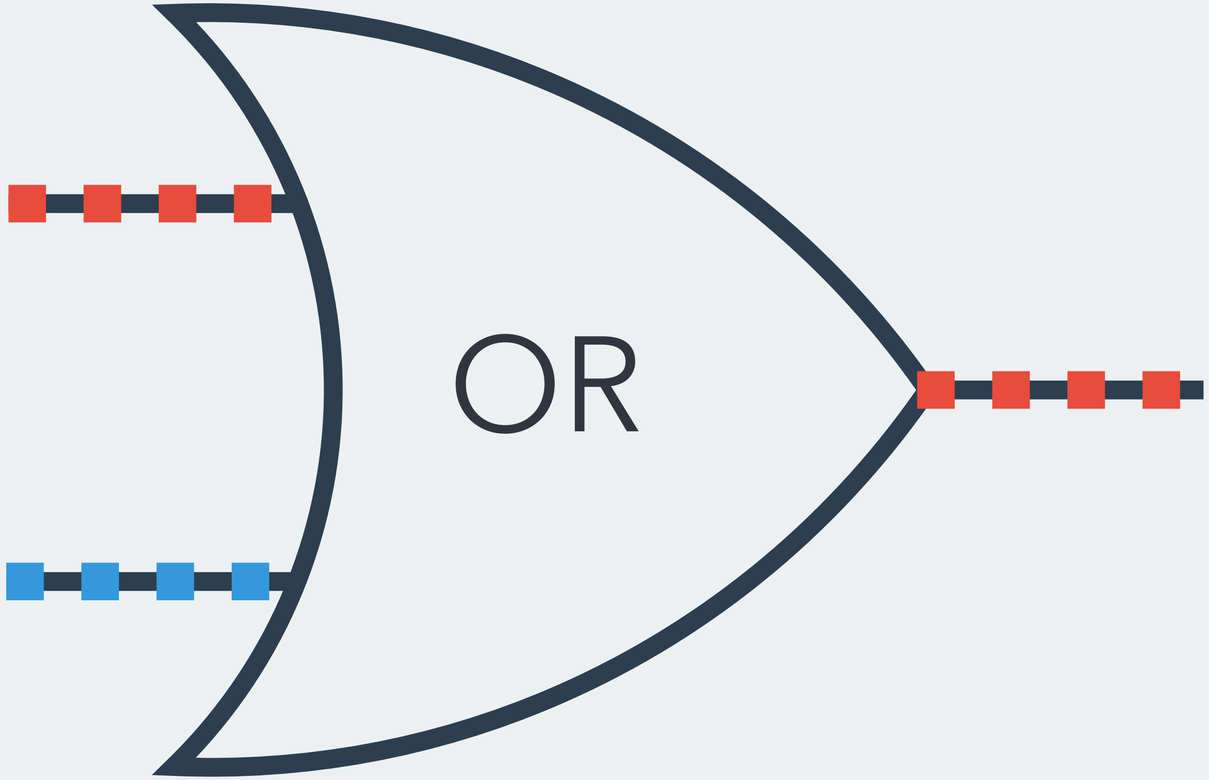
KVANTNO

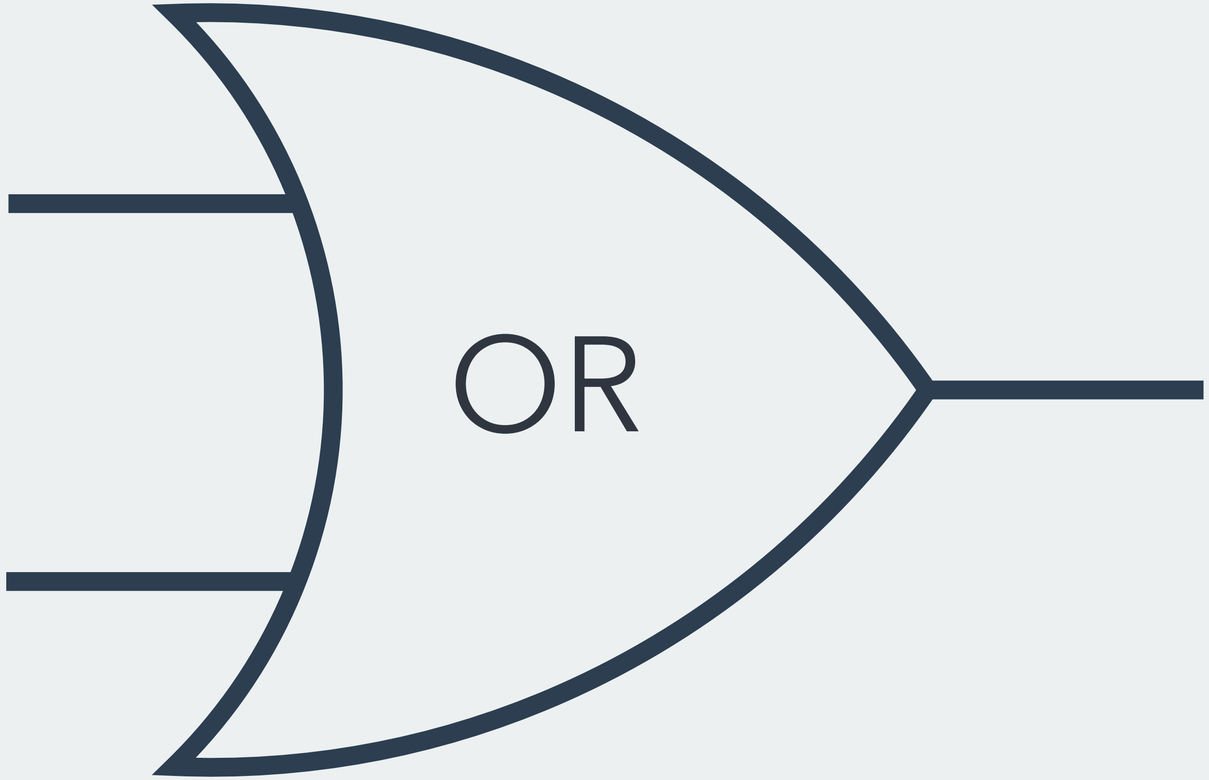
RAČUNALNIŠTVO

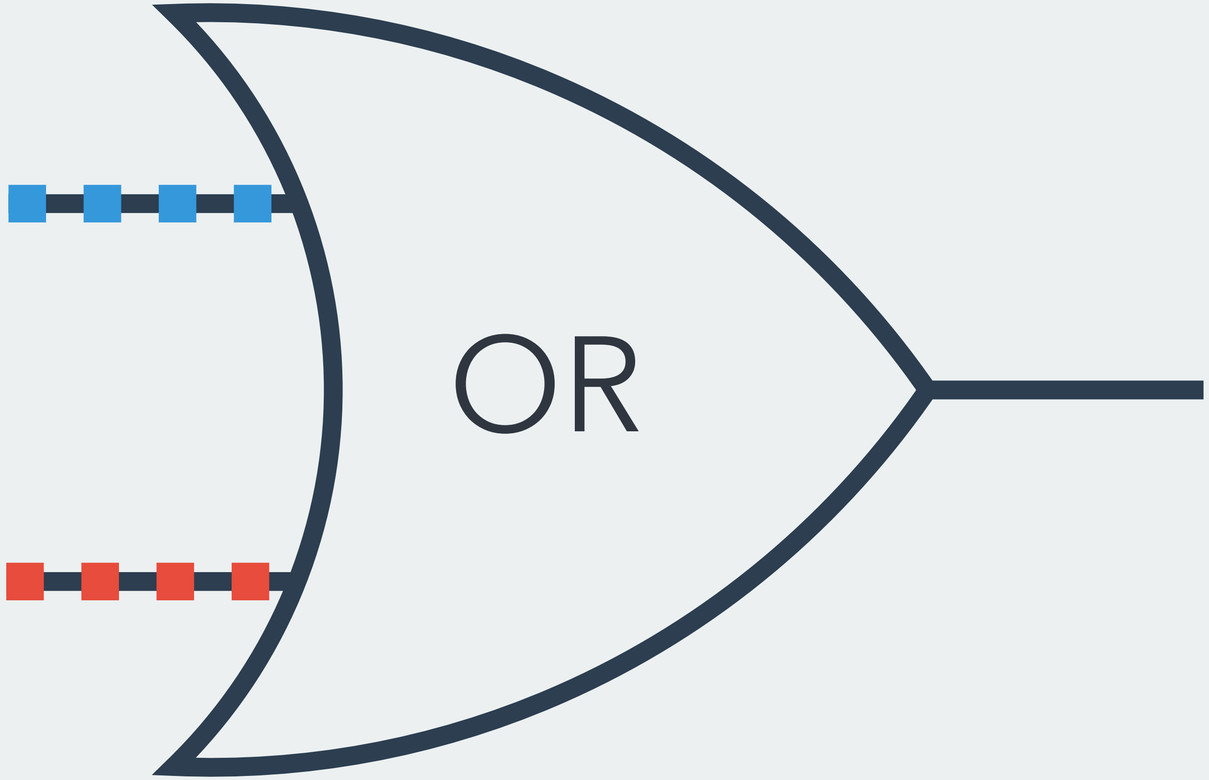

OR

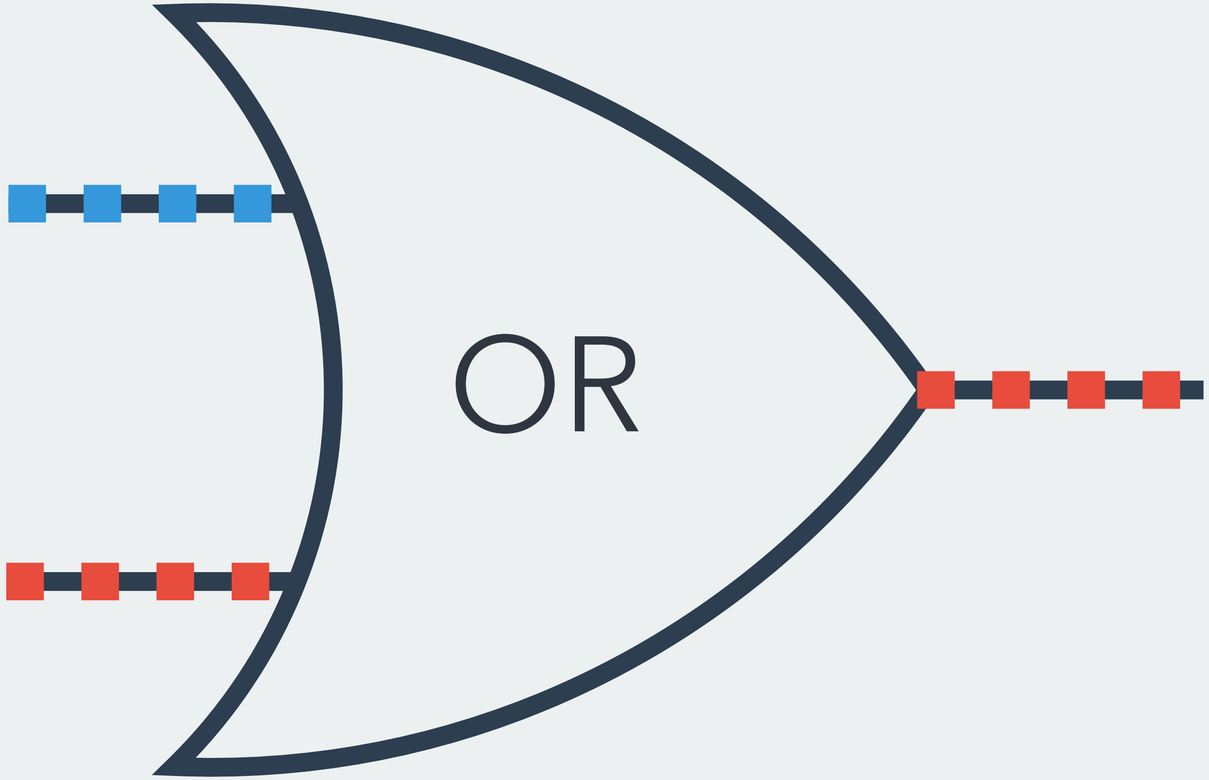

OR

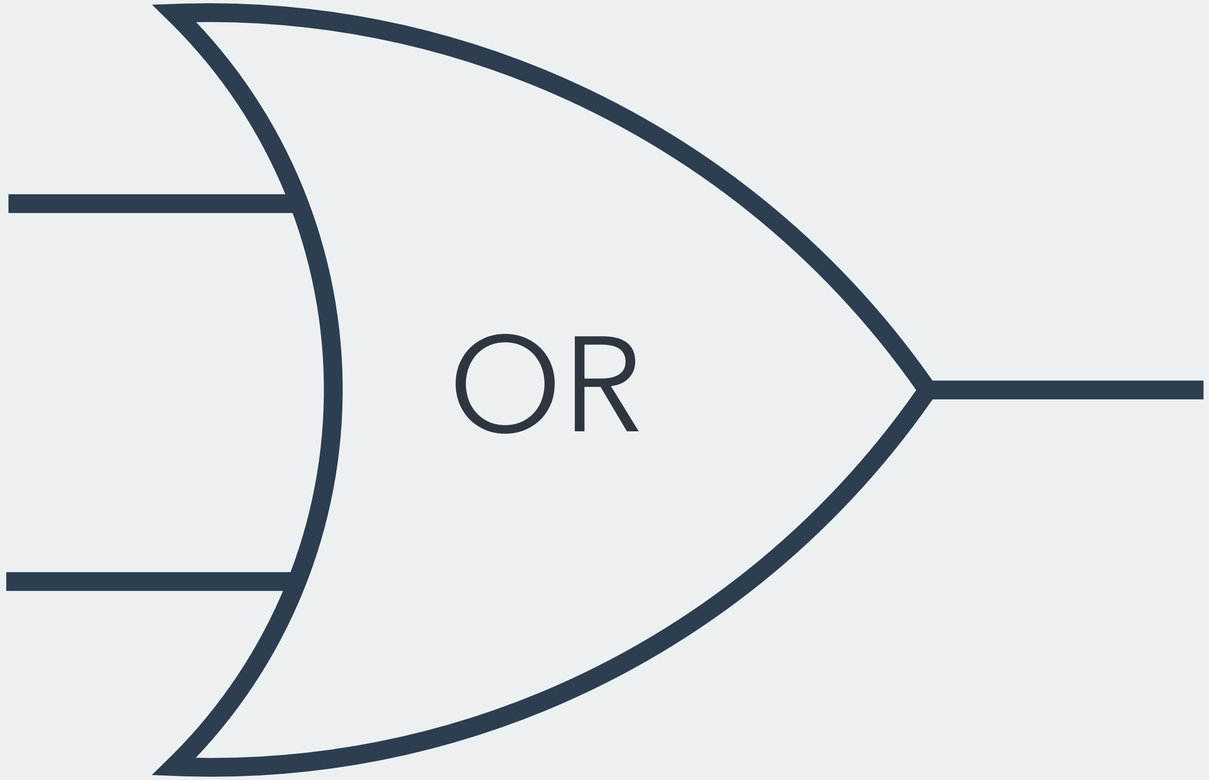

OR

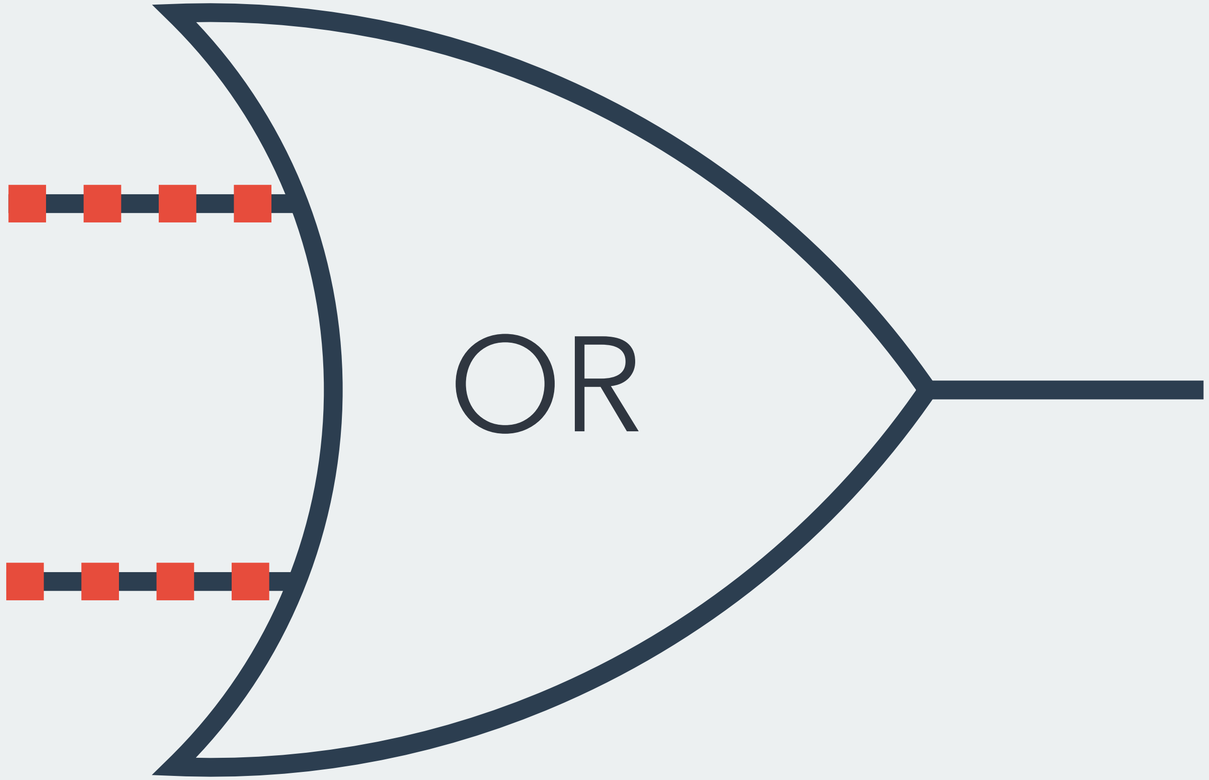

OR

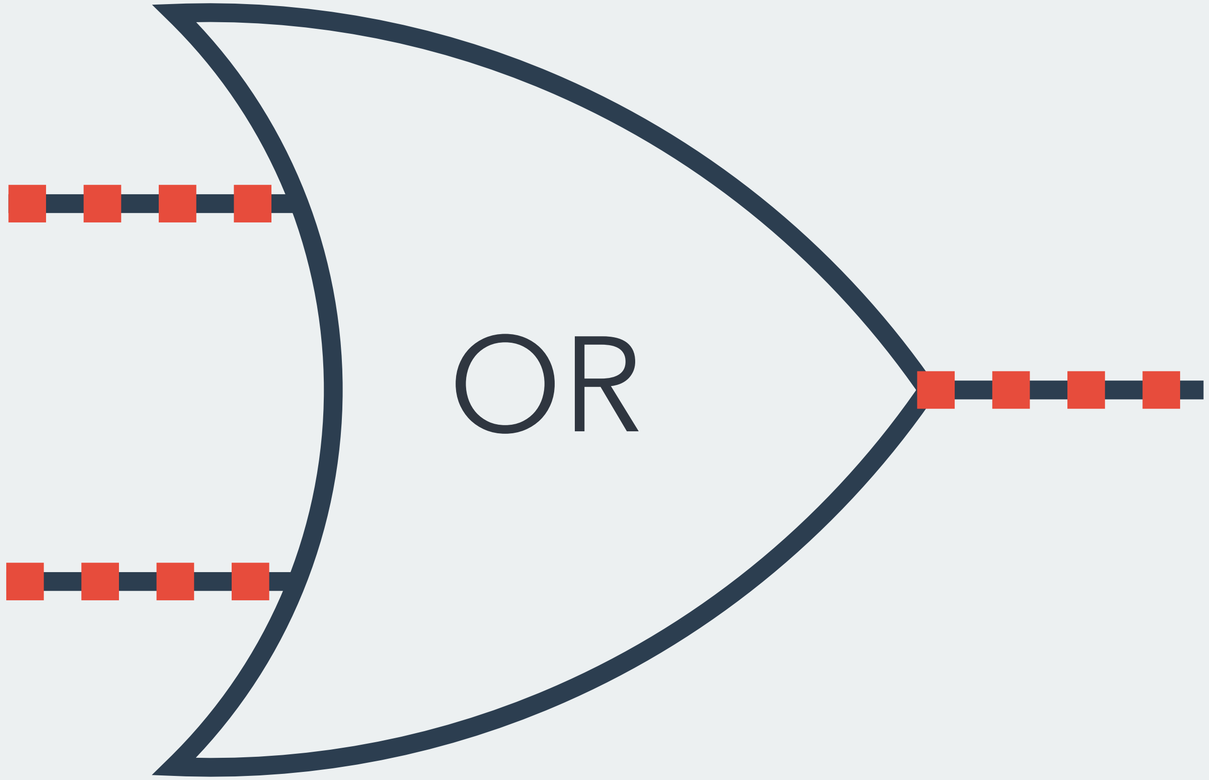

OR

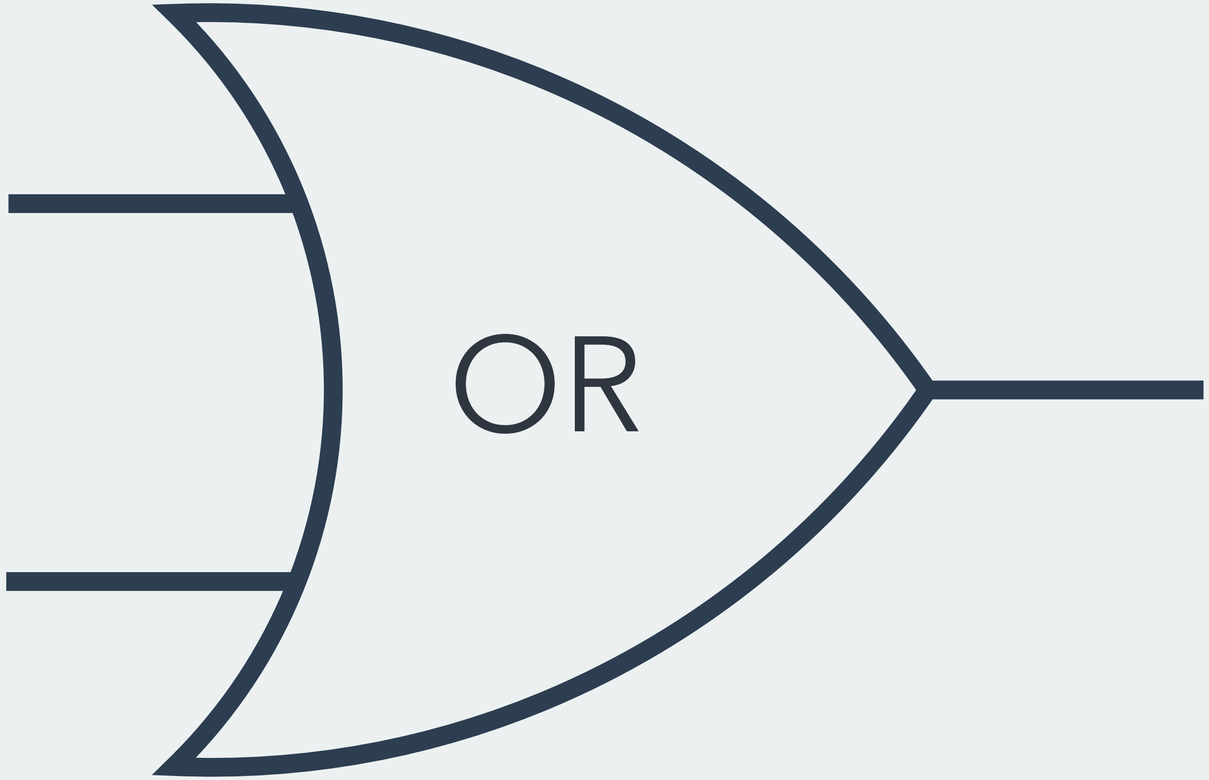

OR

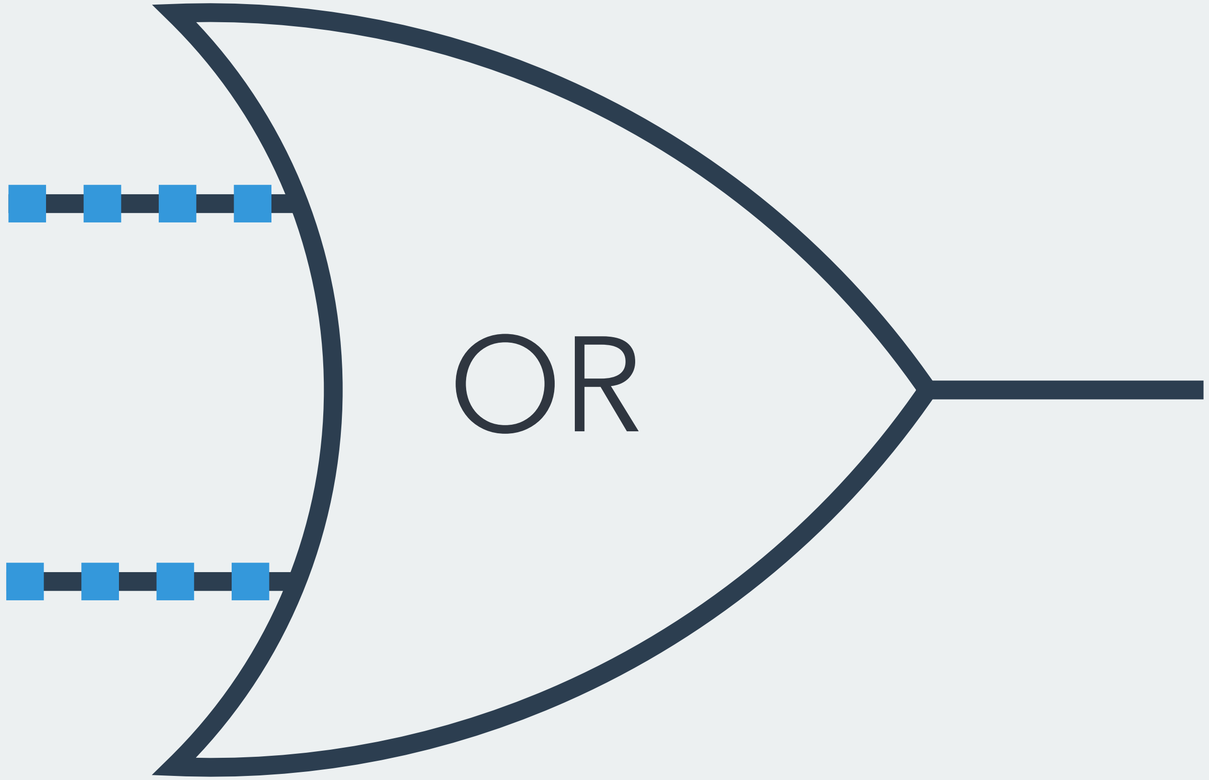

OR

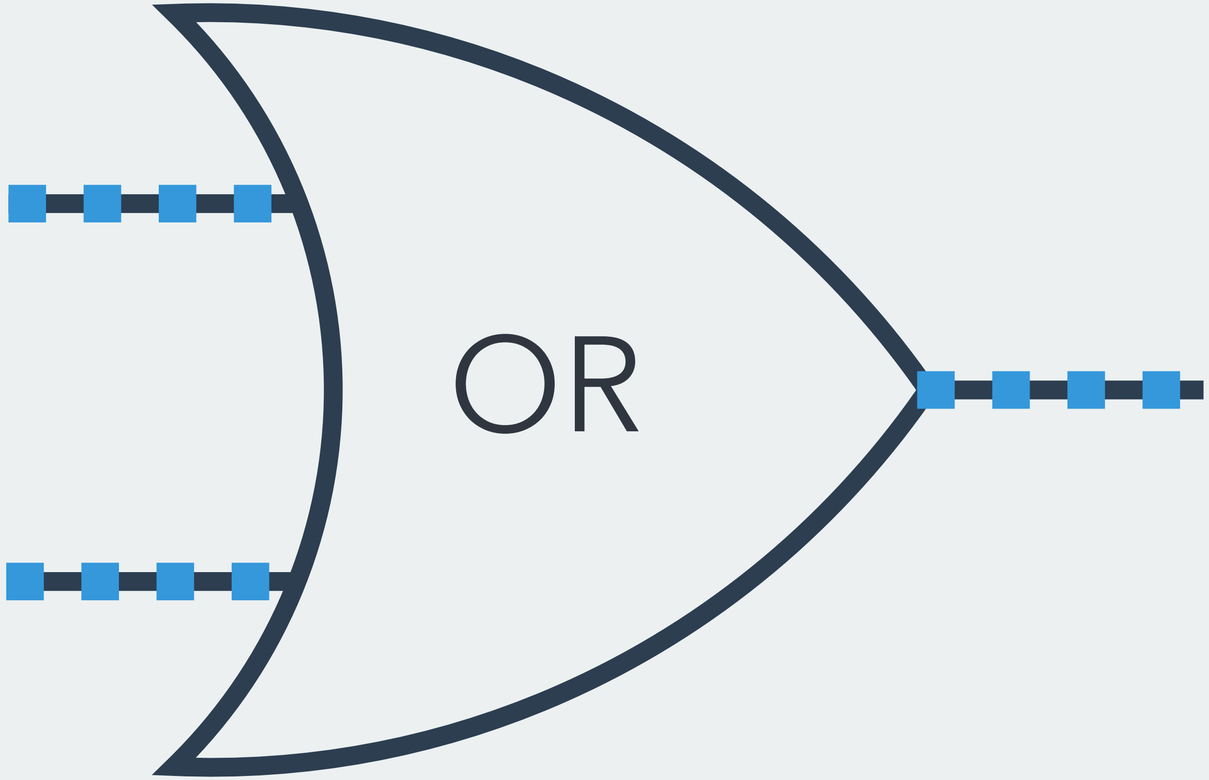

OR

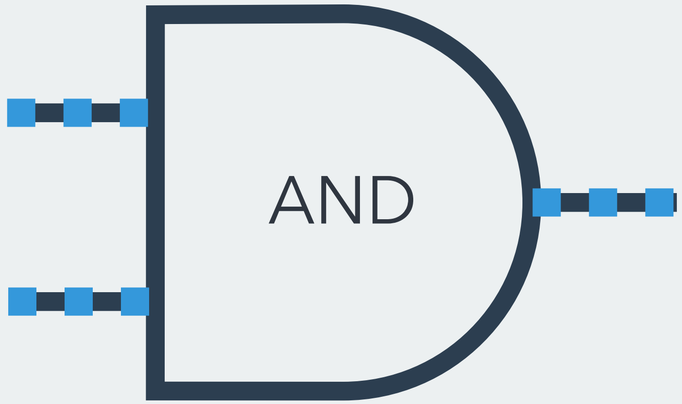

OR

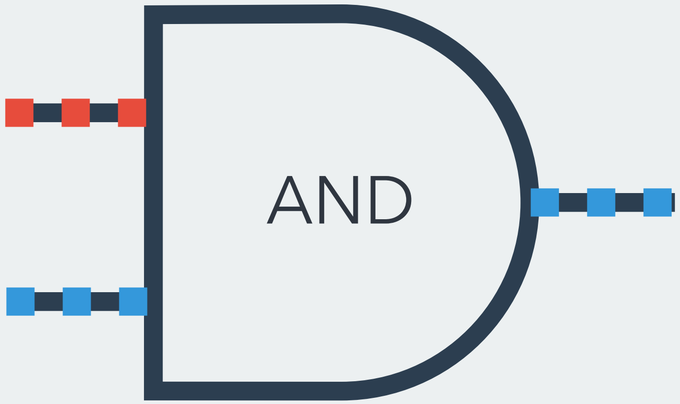

OR

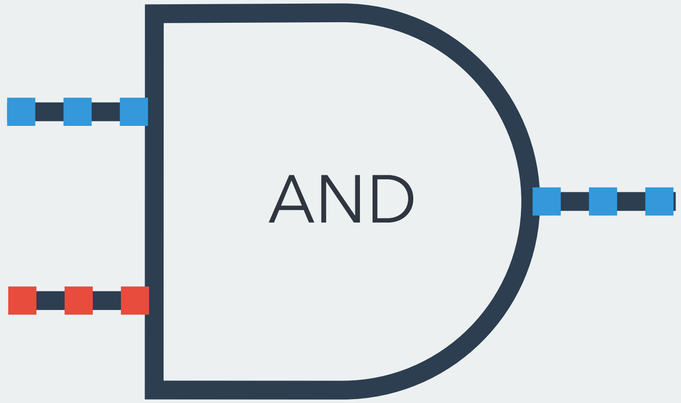

OR

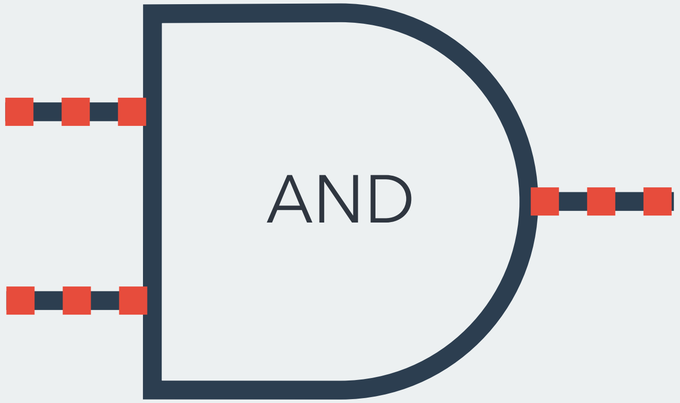

OR

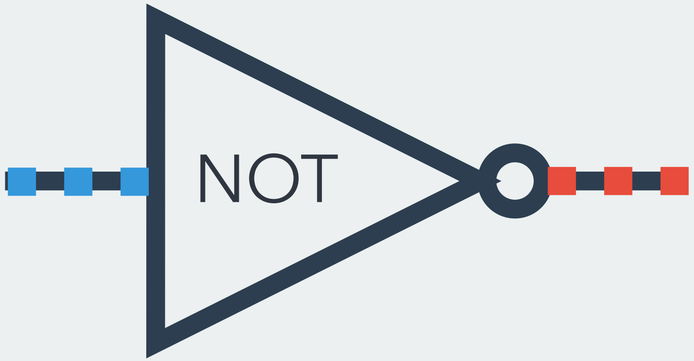

OR

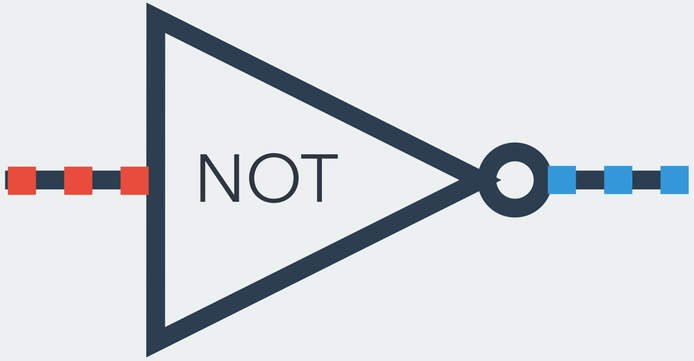

AND

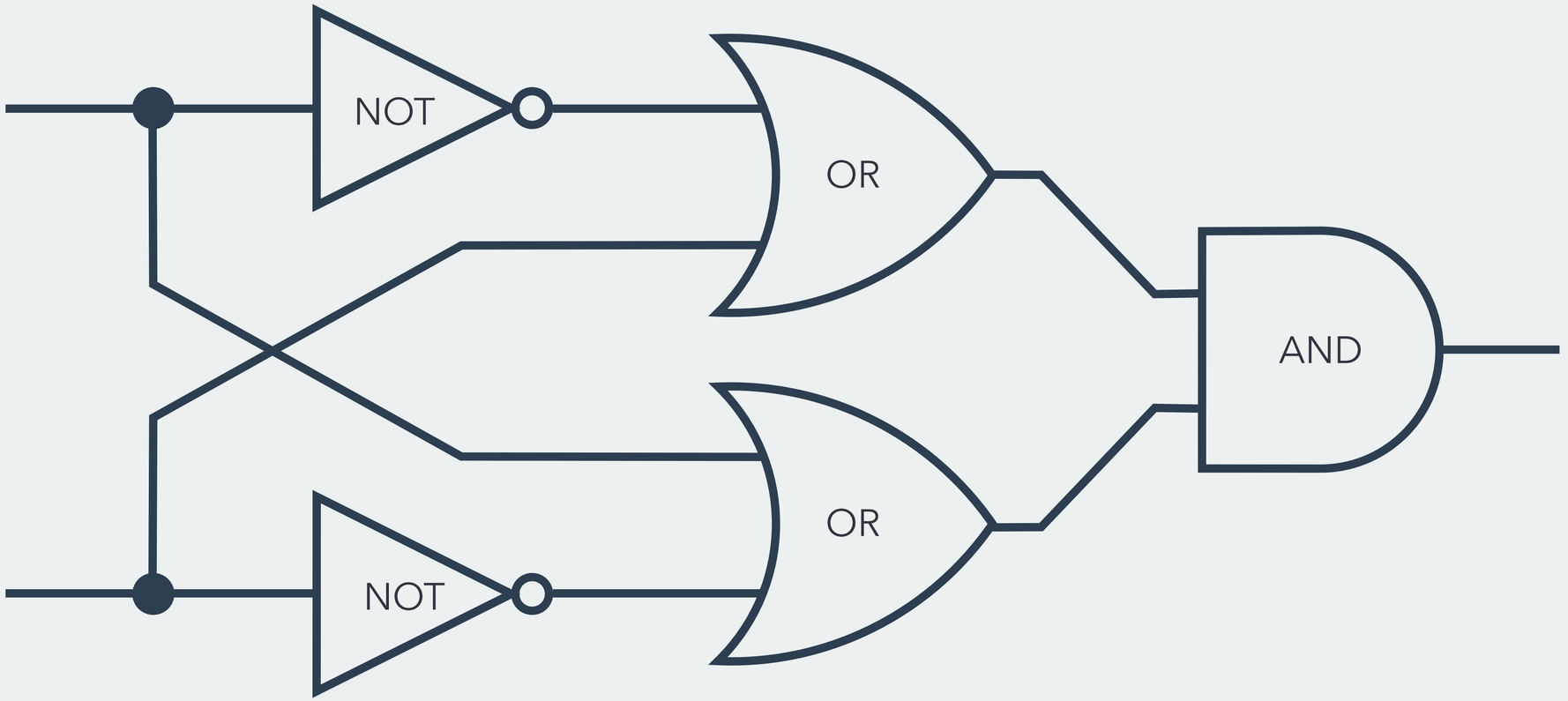

AND

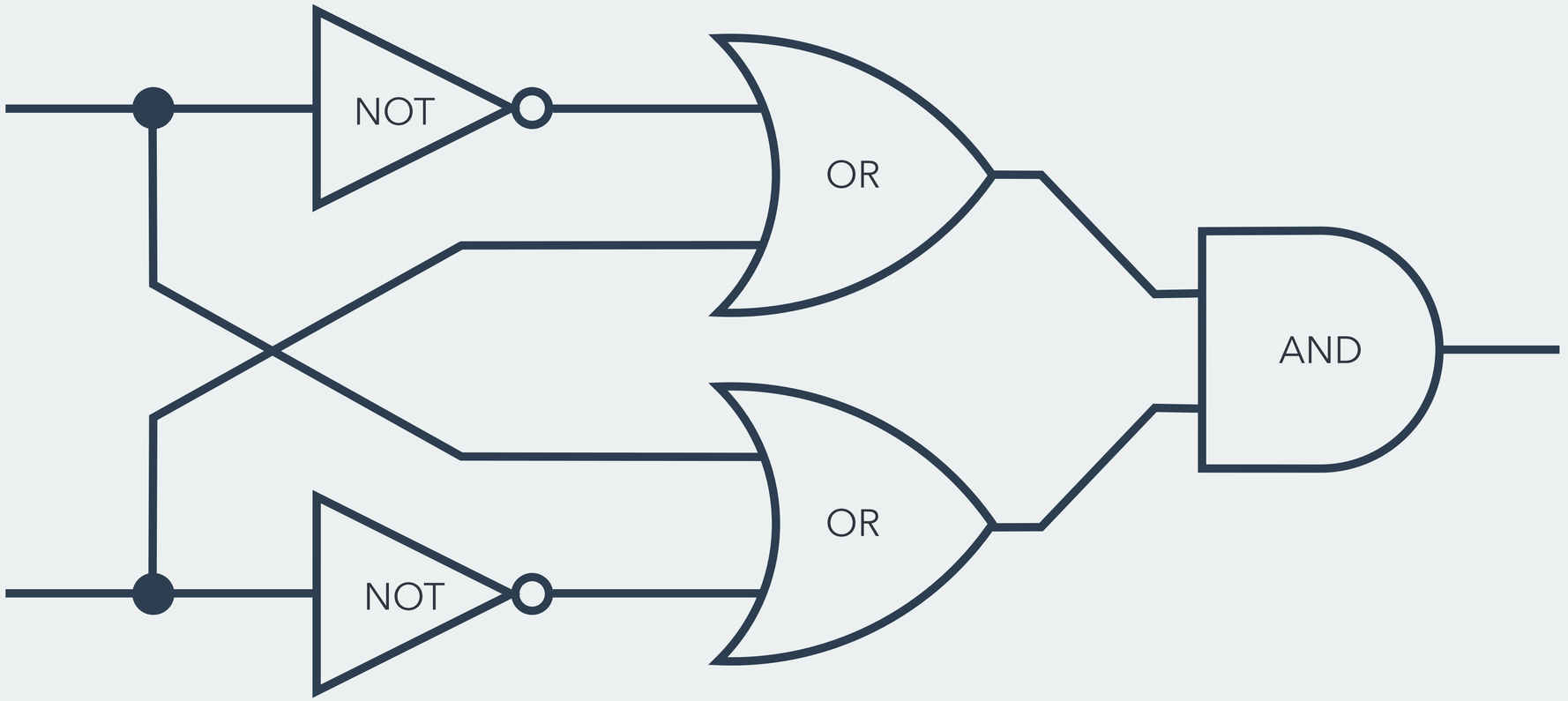

AND

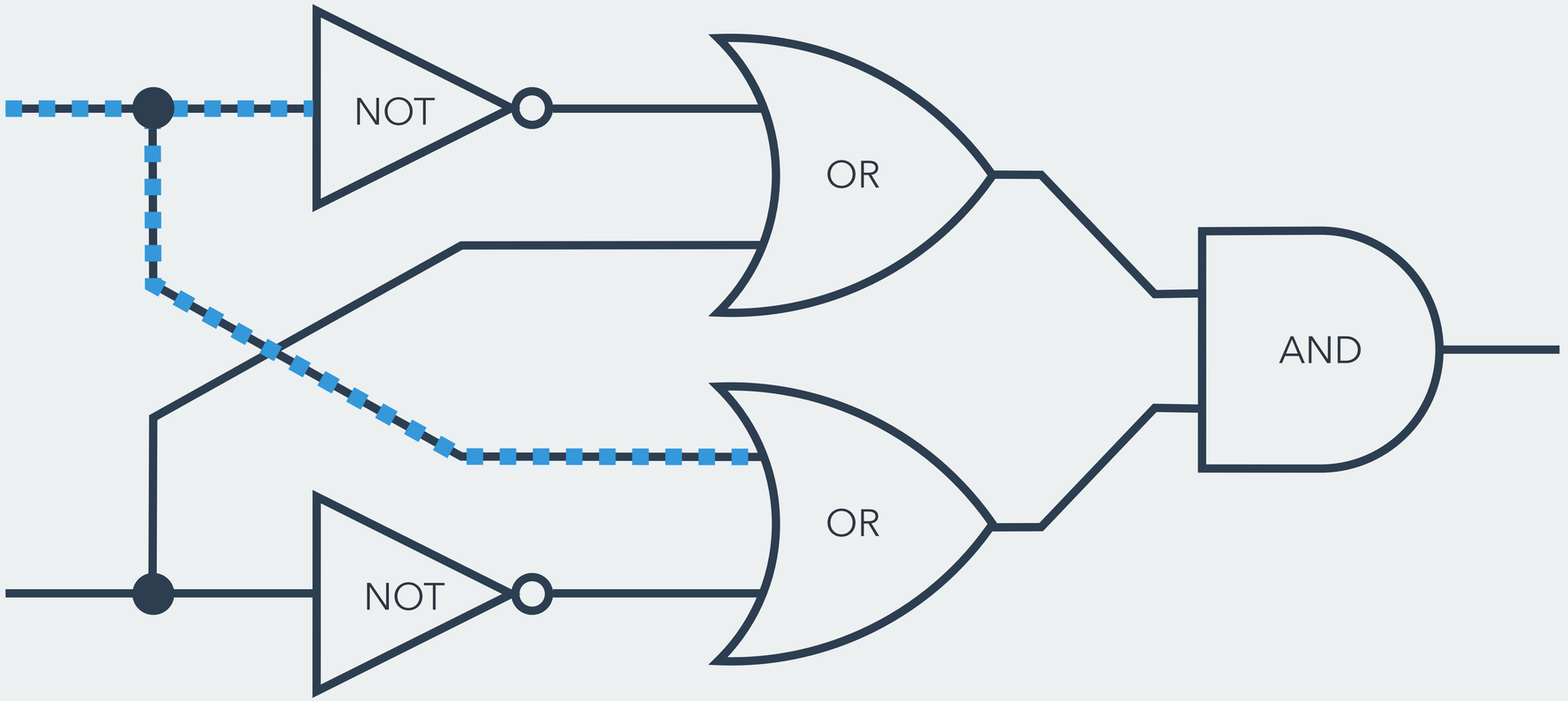

AND

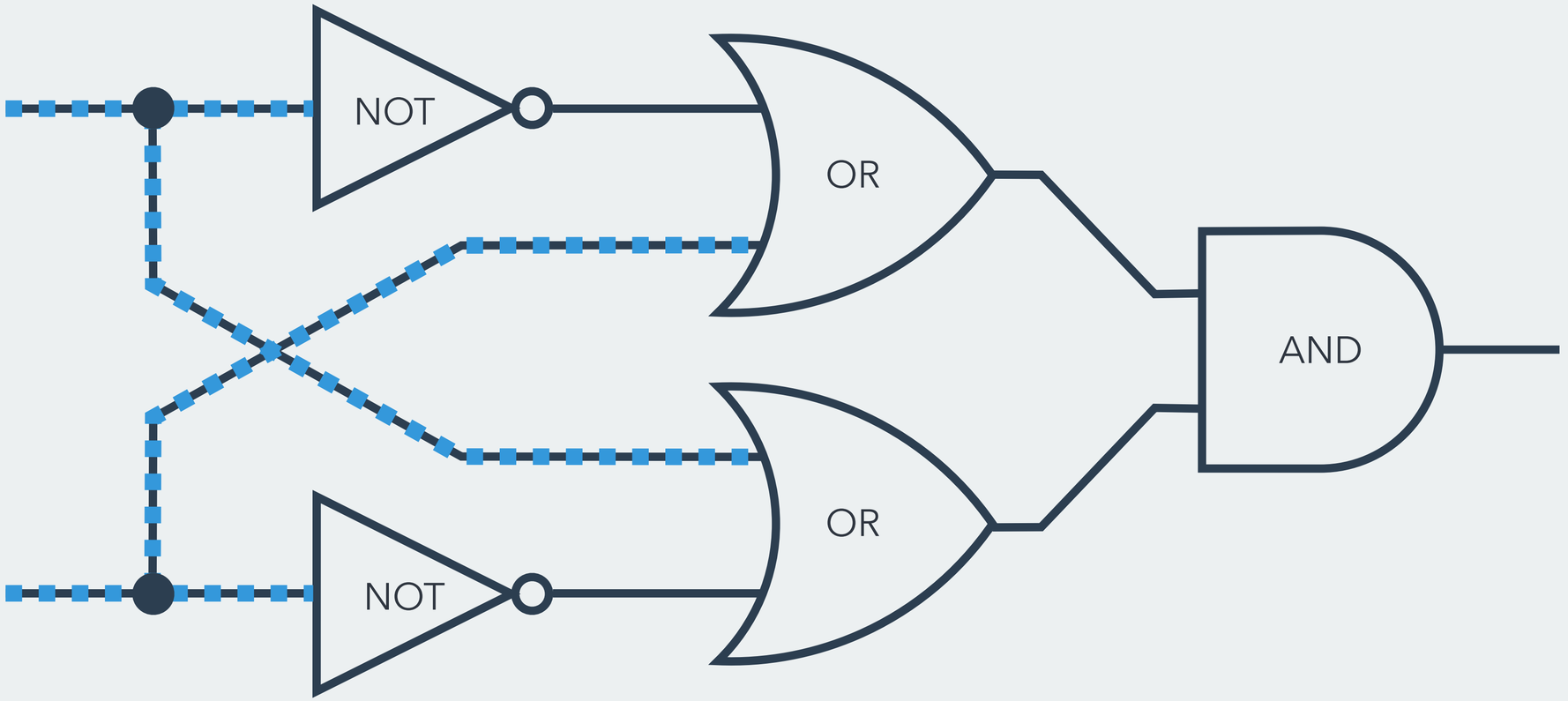

NOT

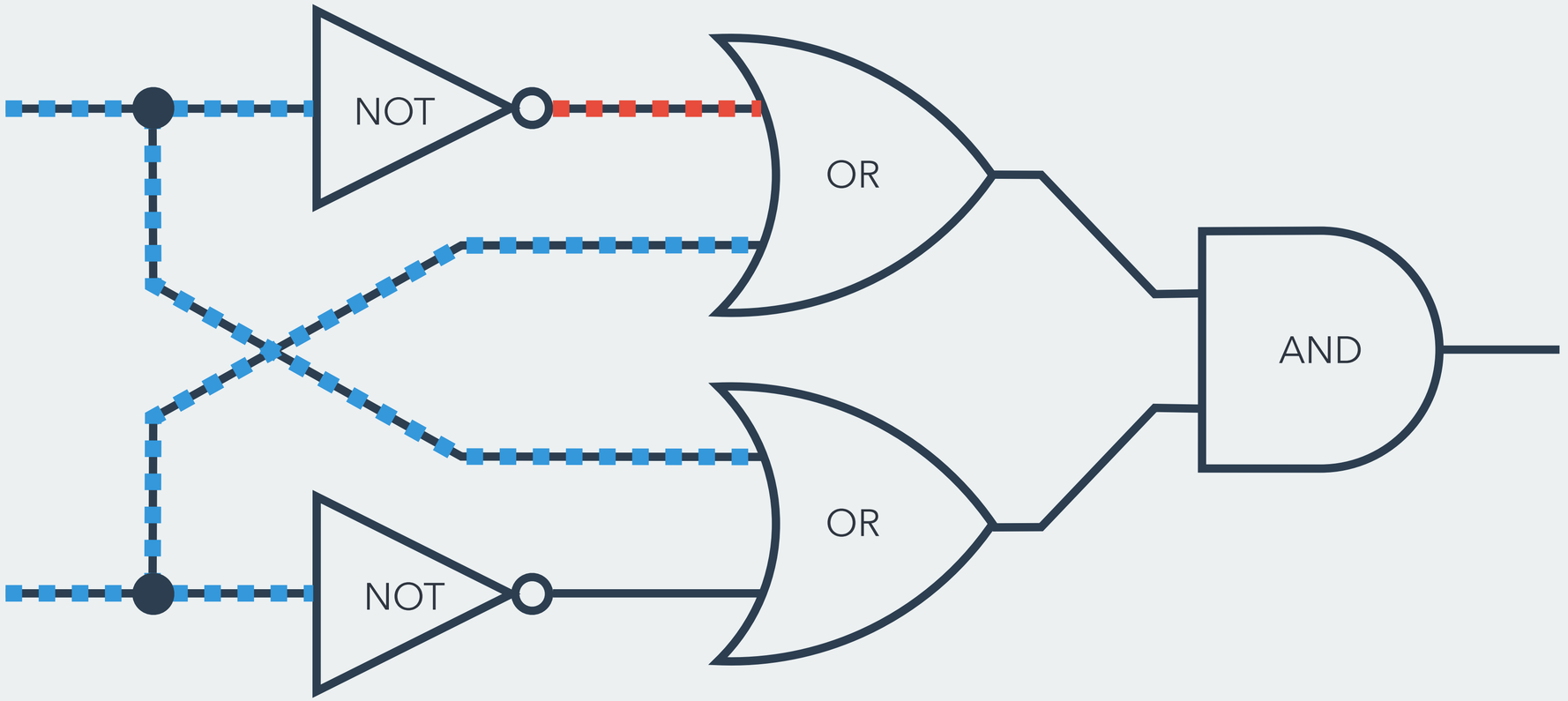

NOT

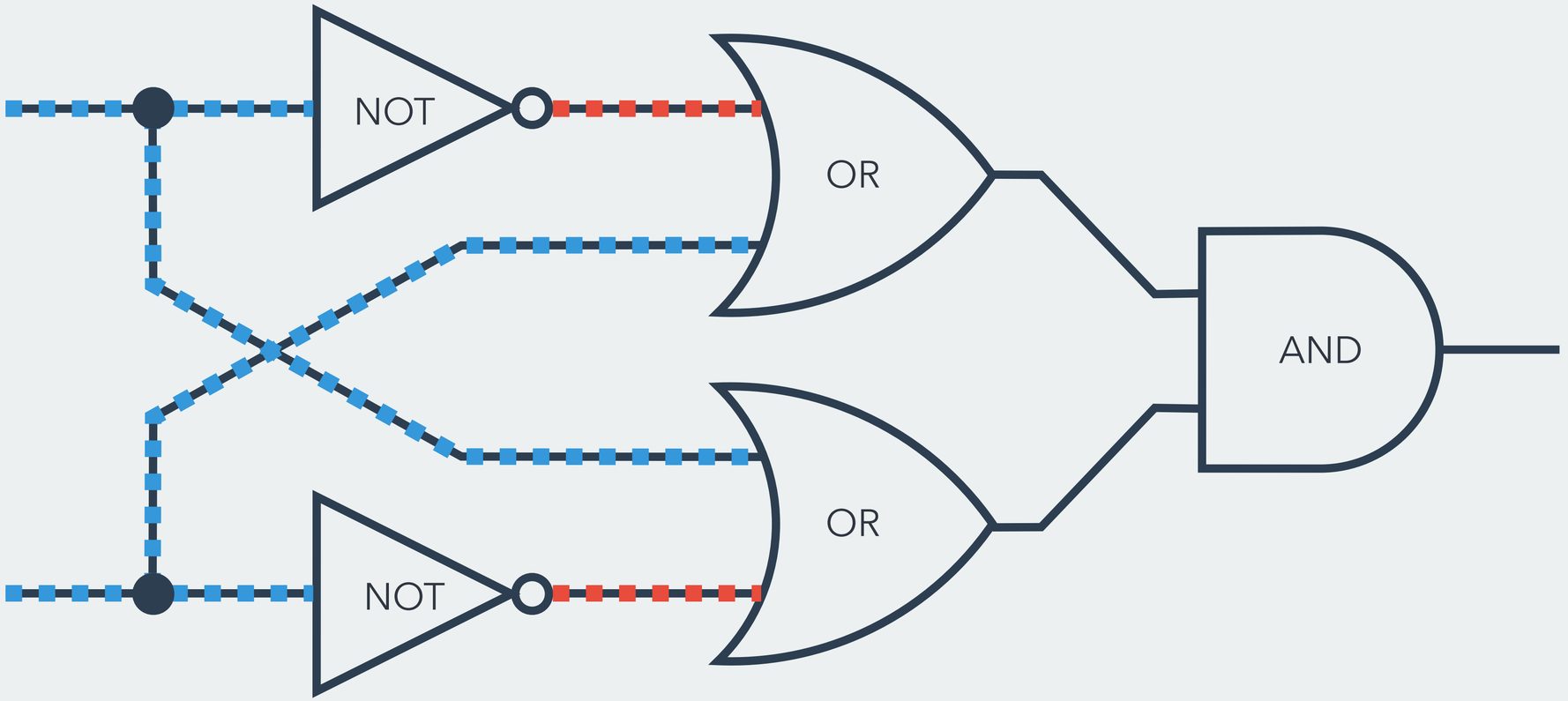

NOT
OR
AND
OR
NOT

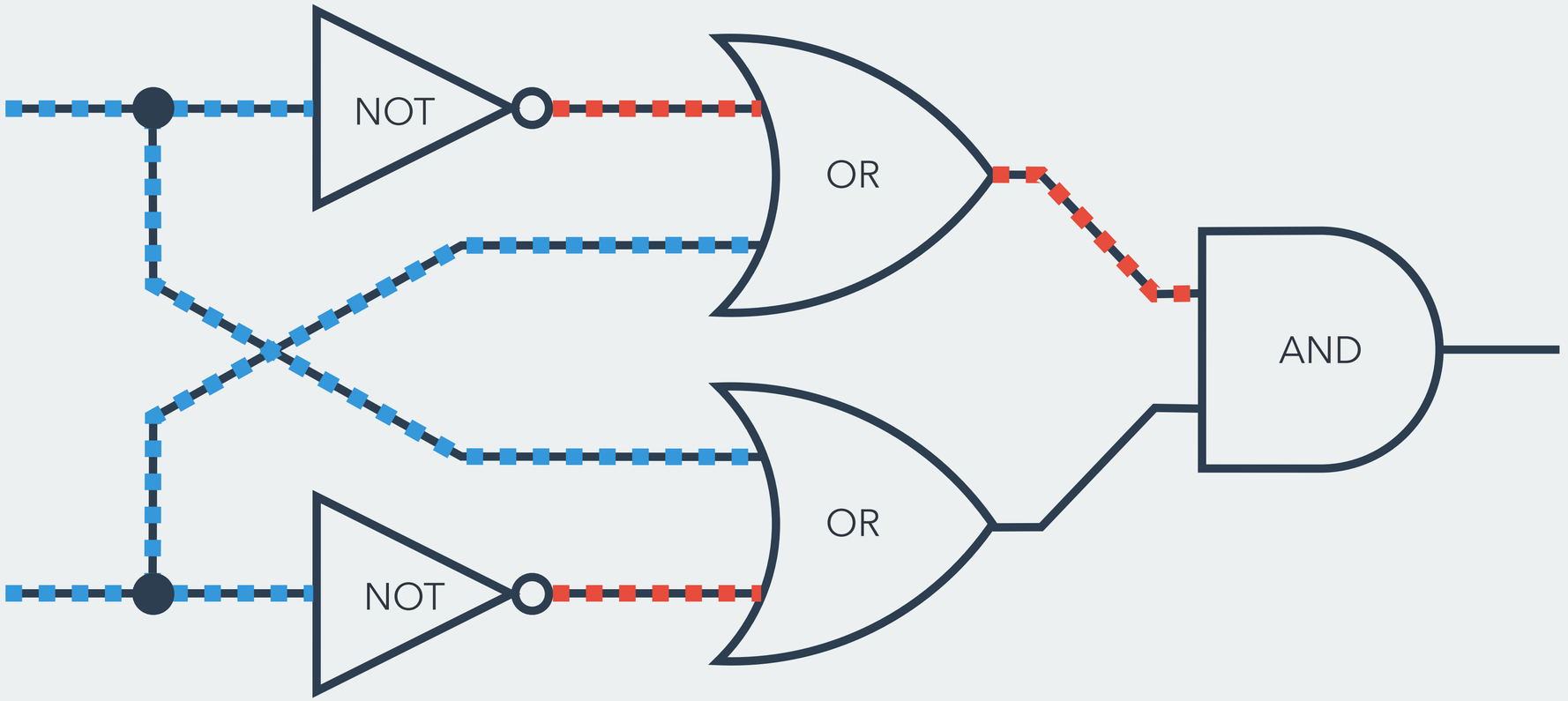

NOT
OR
AND
OR
NOT

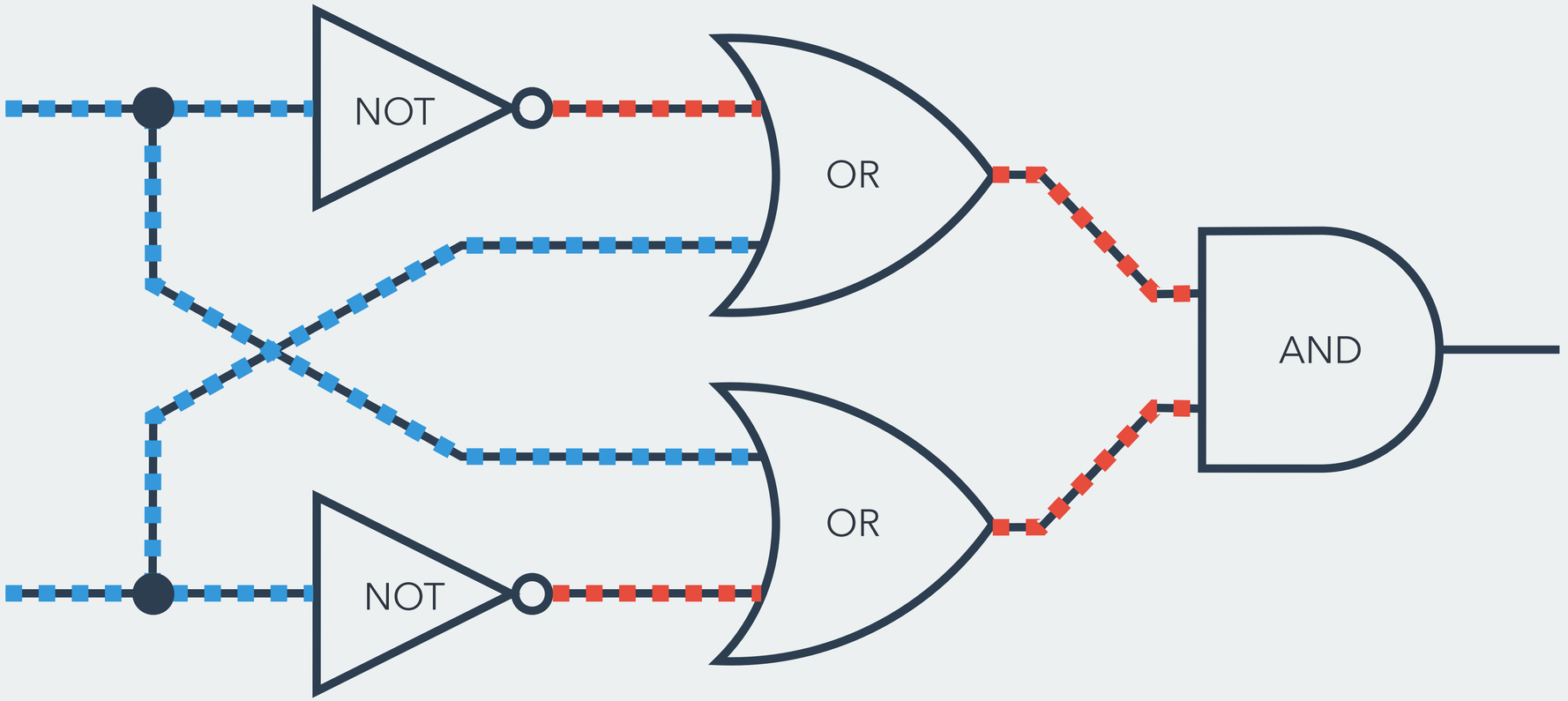

NOT
OR
AND
OR
NOT

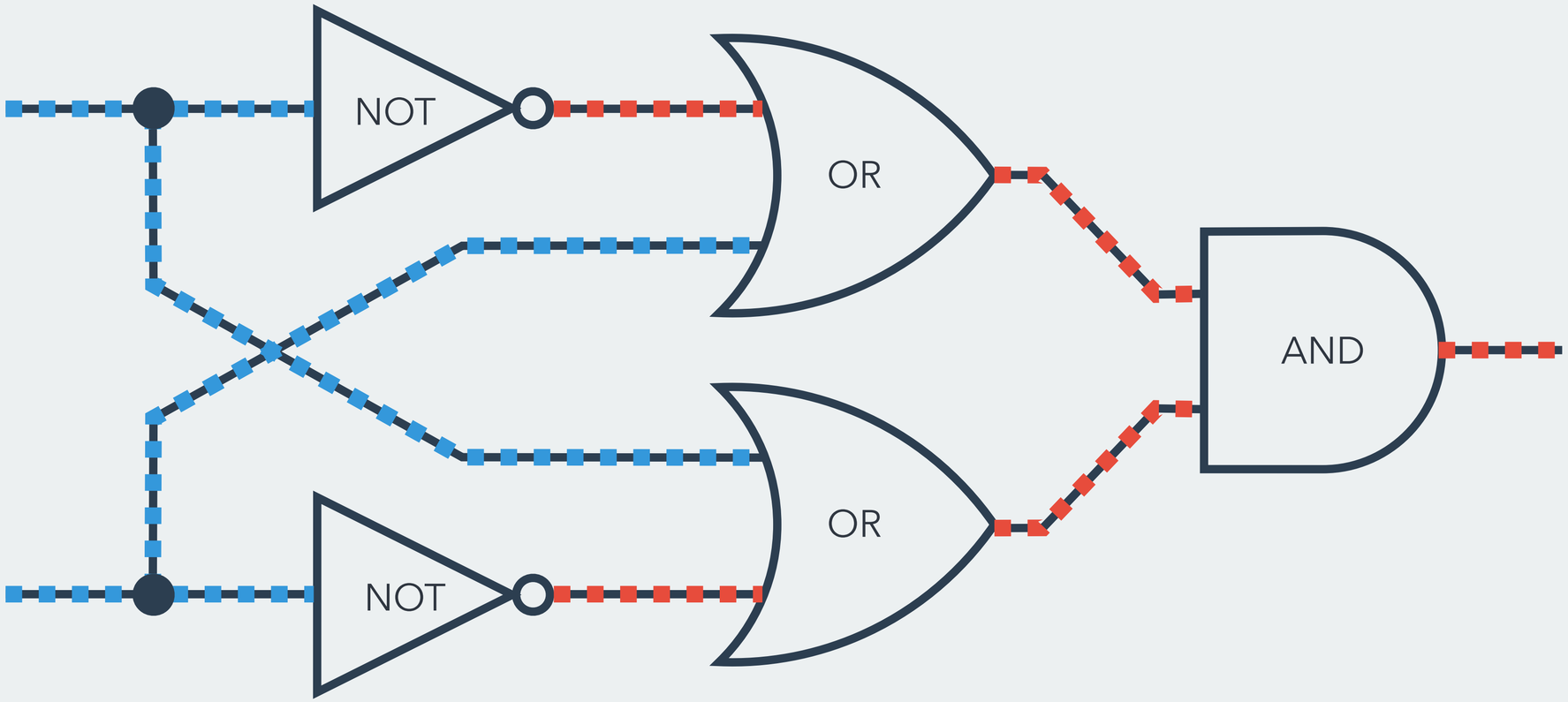

NOT
NOT
OR
OR
AND

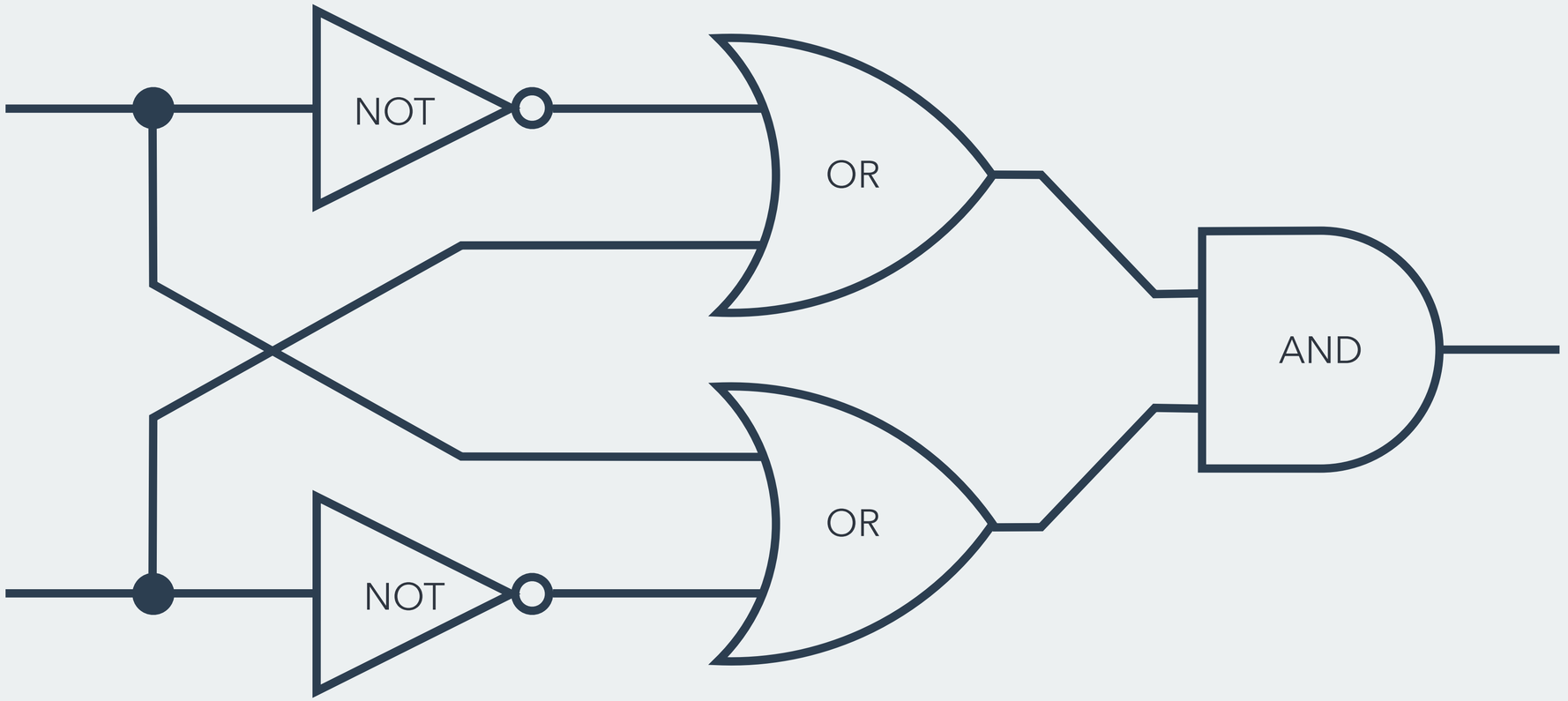

NOT
NOT
OR
OR
AND

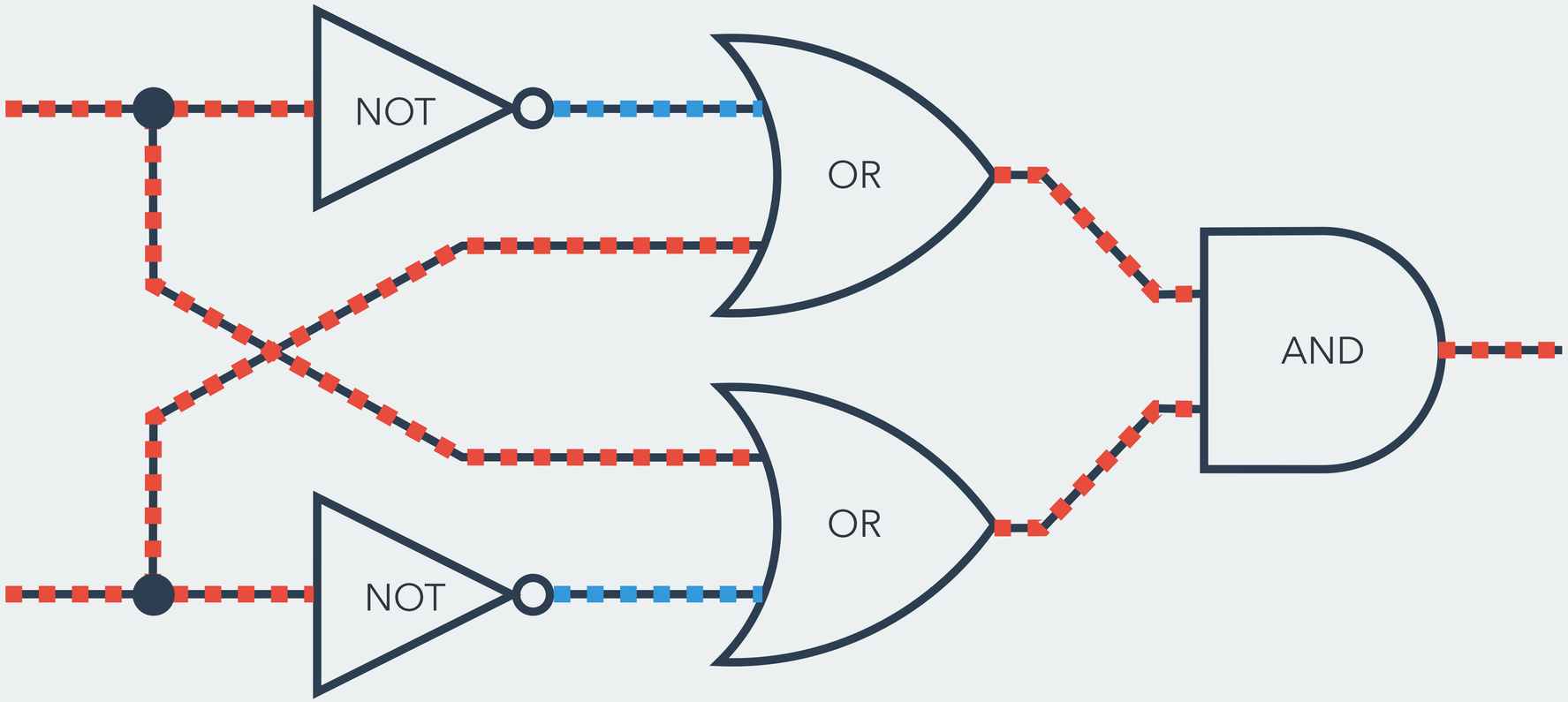

NOT
NOT
OR
OR
AND

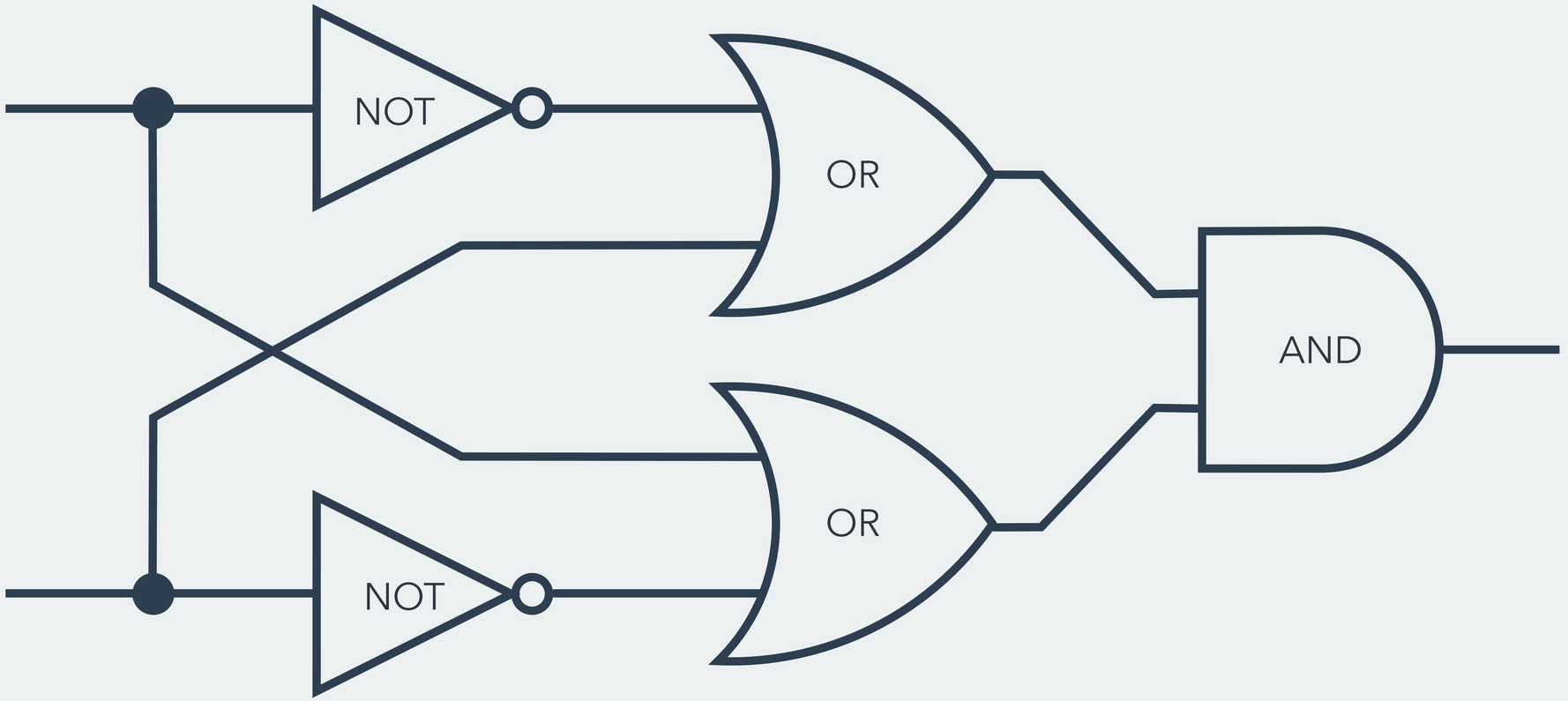

NOT
OR
AND
OR
NOT

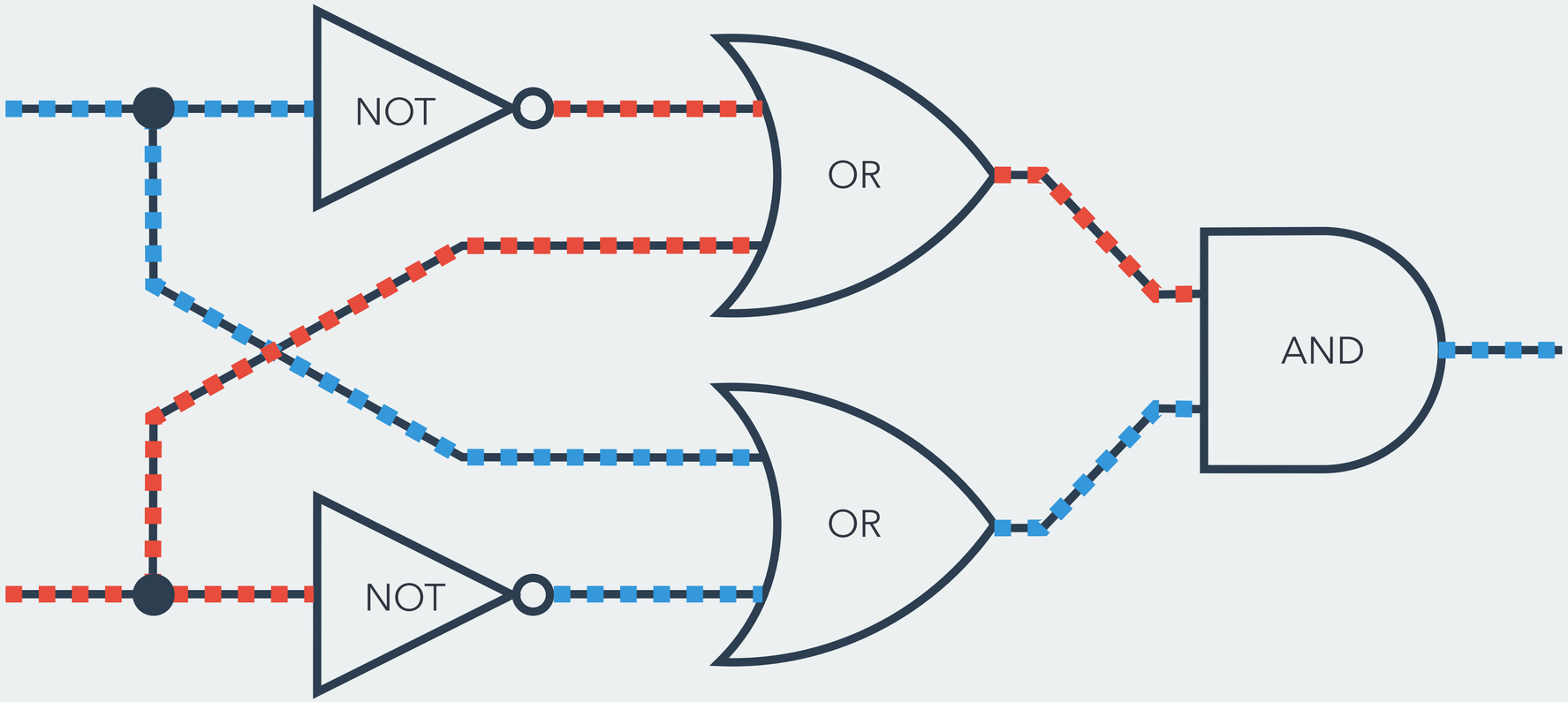

NOT
NOT
OR
OR
AND

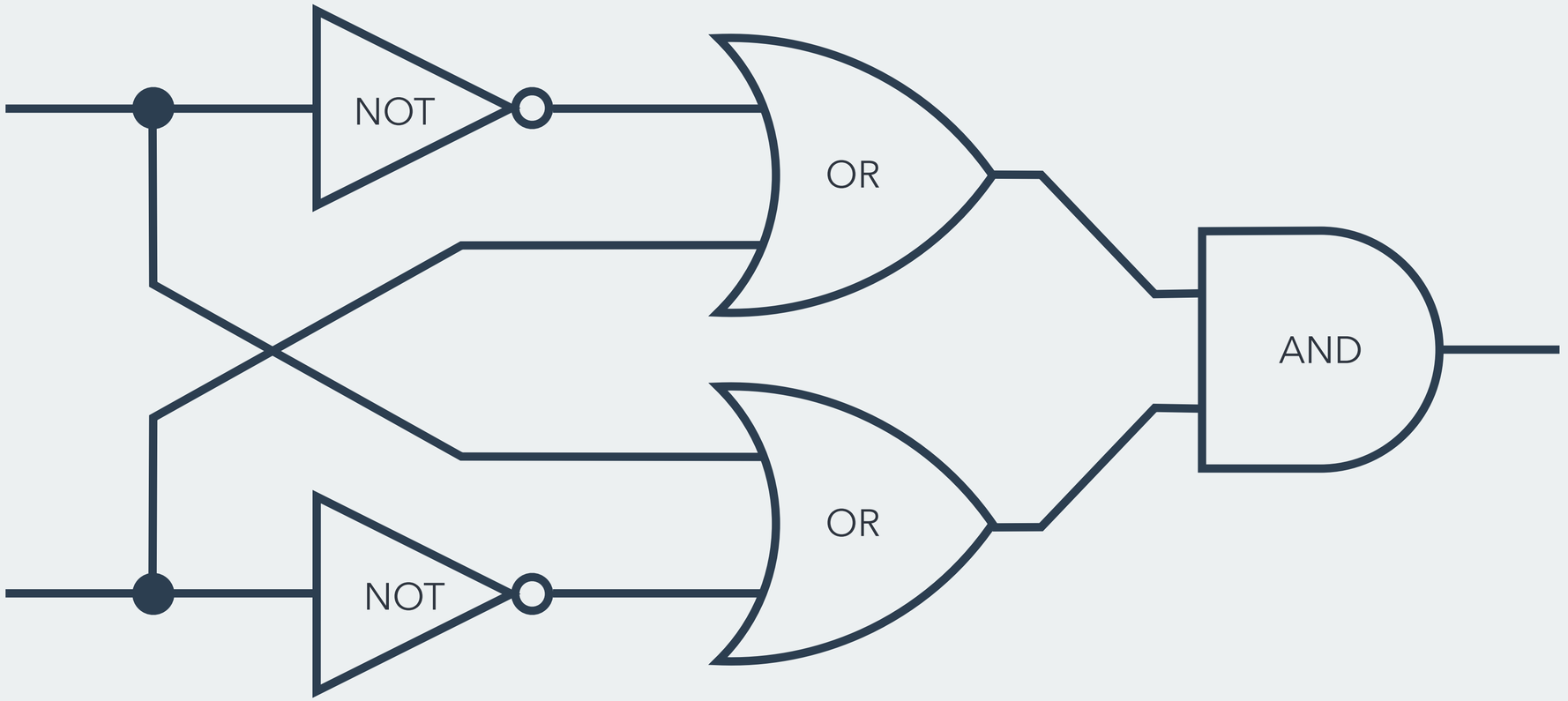

NOT
OR
AND
OR
NOT

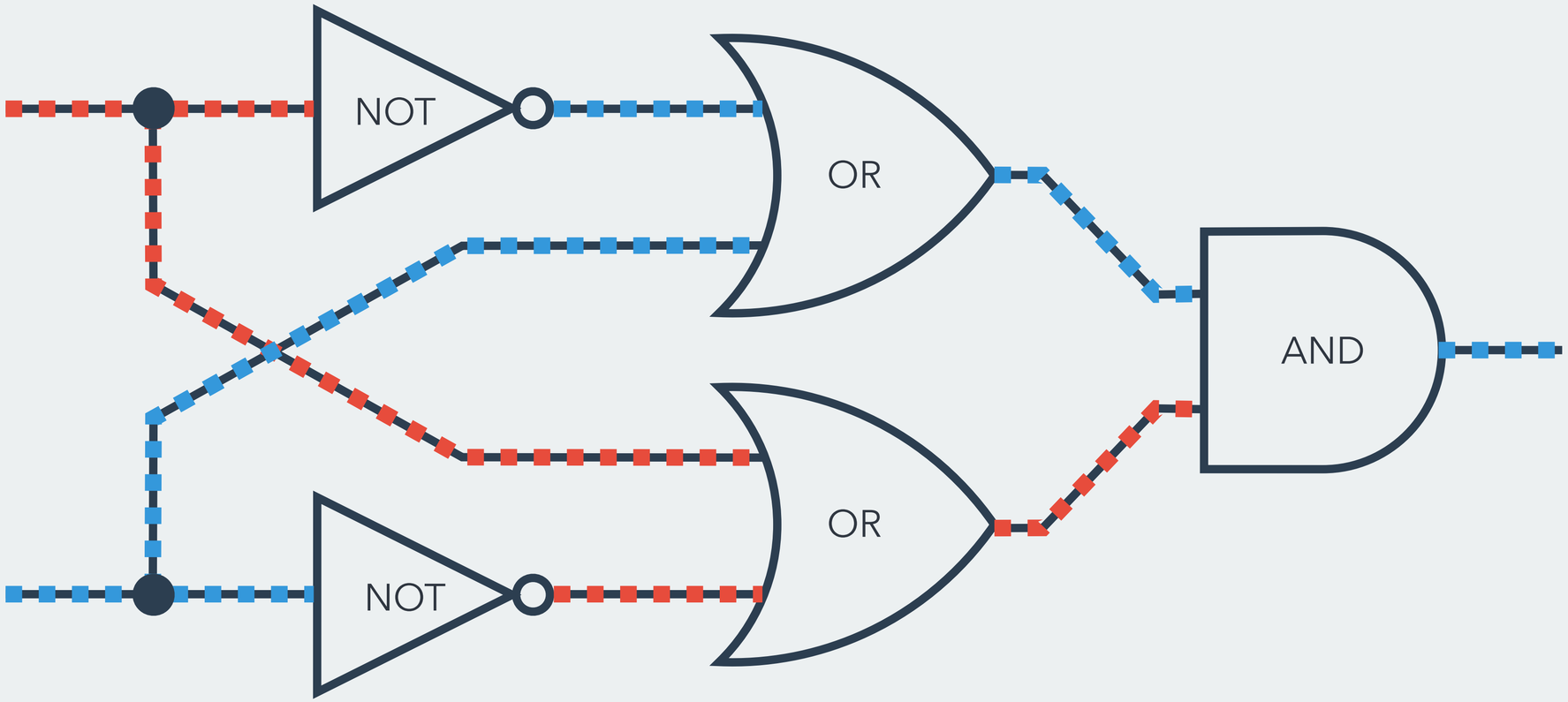

NOT
OR
AND
OR
NOT

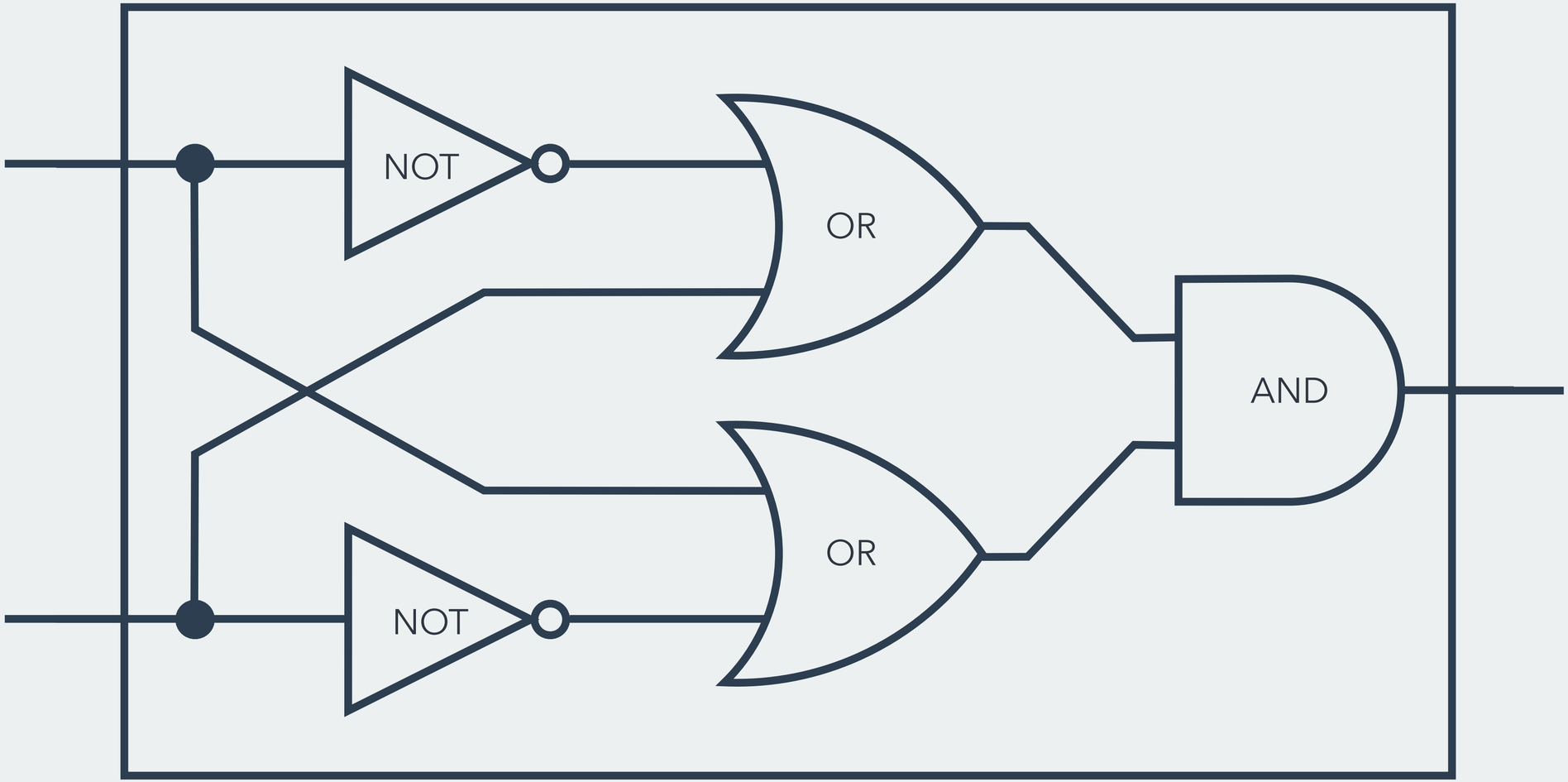

NOT
OR
AND
OR
NOT

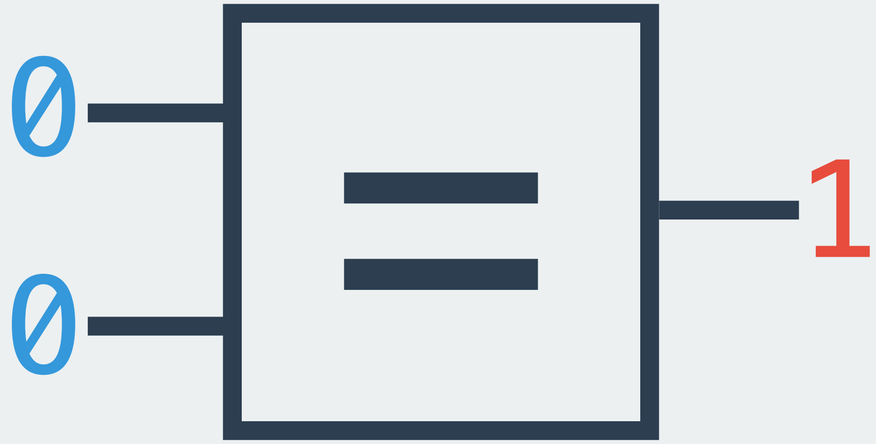

NOT
OR
AND
OR
NOT

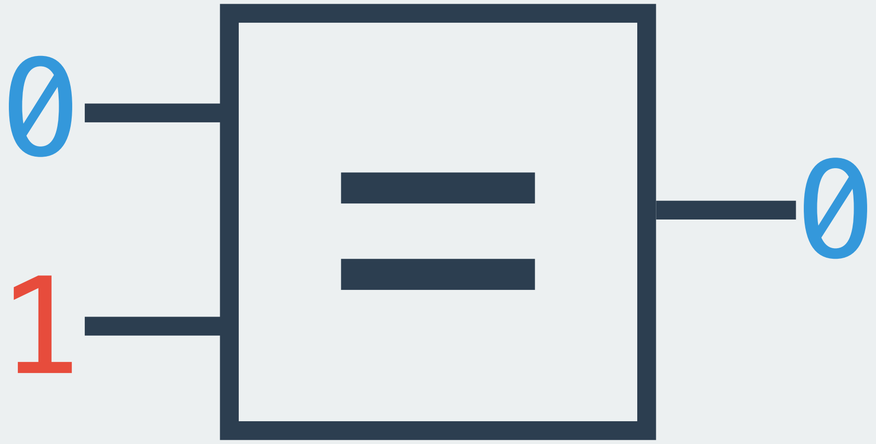

NOT
OR
AND
OR
NOT

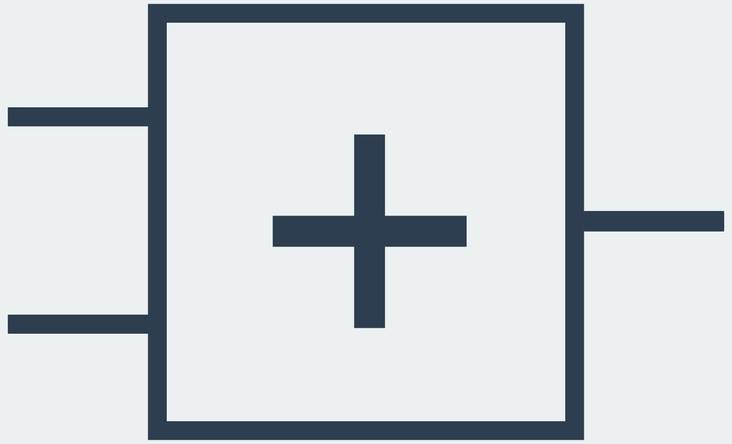

NOT
OR
AND
OR
NOT

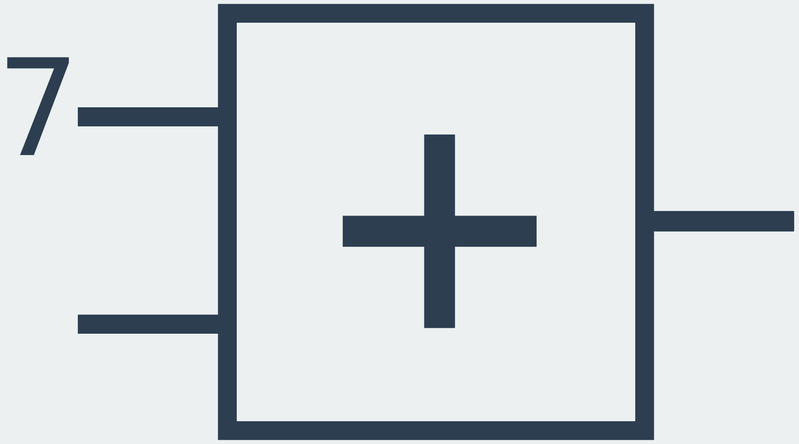

NOT
OR
AND
OR
NOT

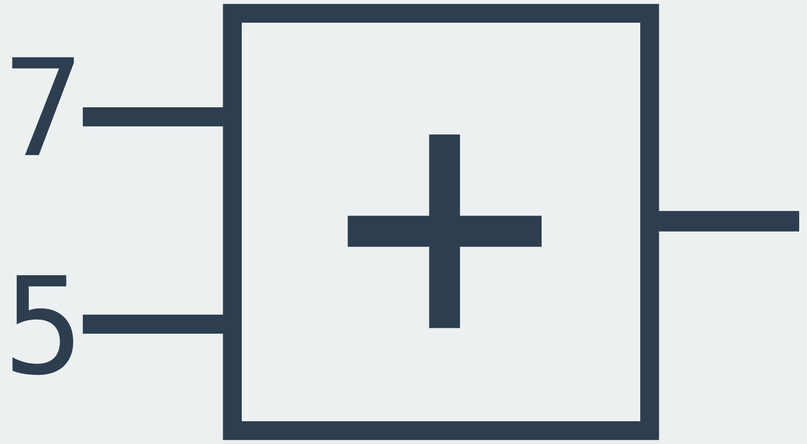

NOT
OR
AND
OR
NOT

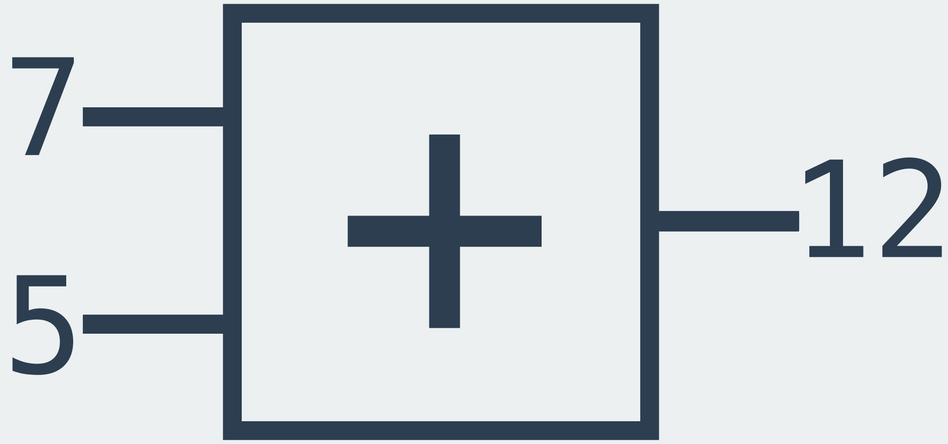

0
0
1

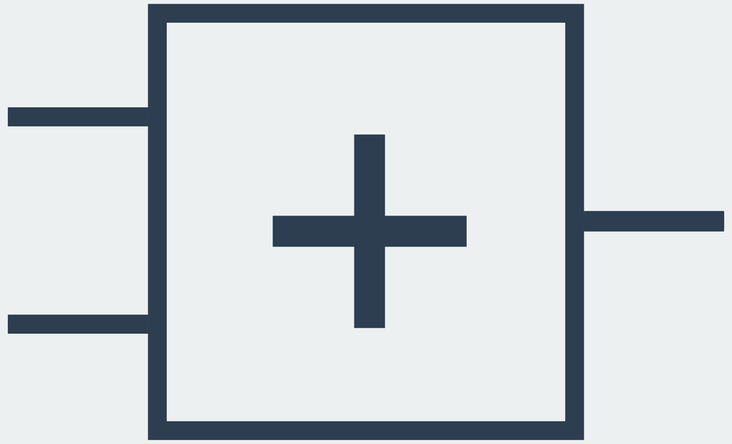

0
1
=
0




7


7
5
+

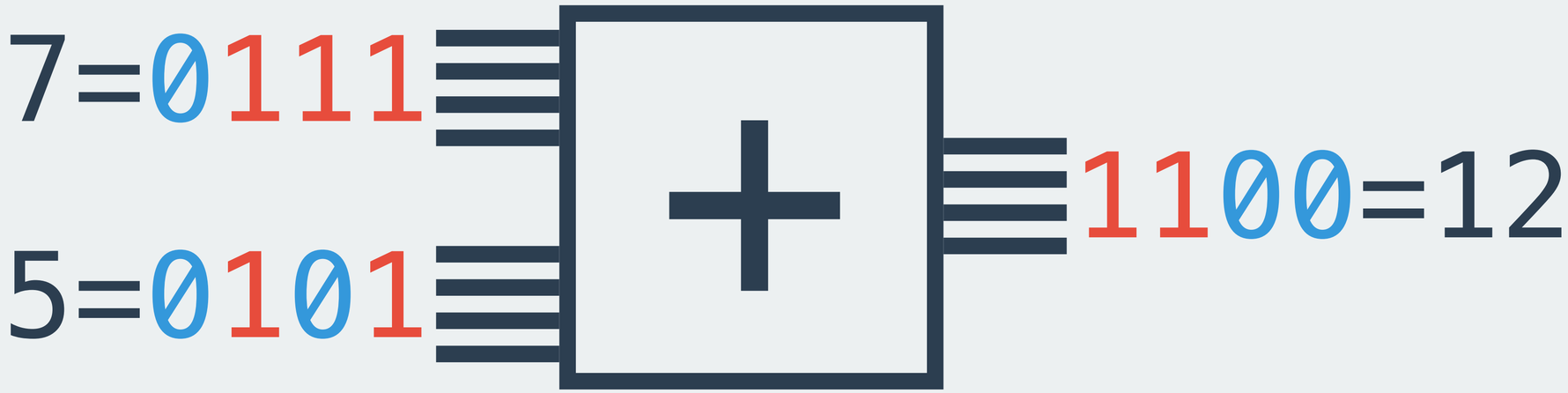

7
5
+
12



7=0111

7=0111

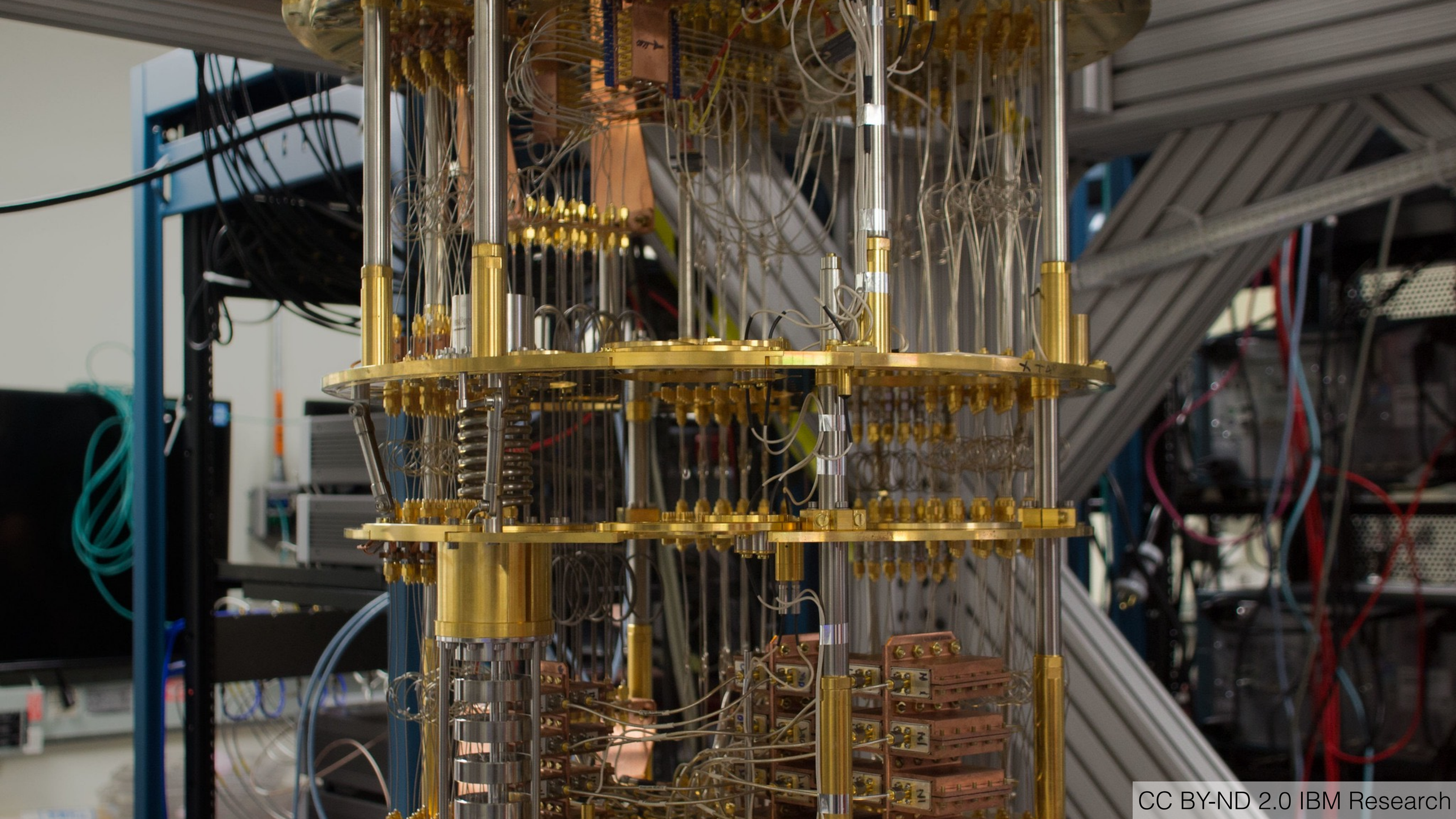
5=0101

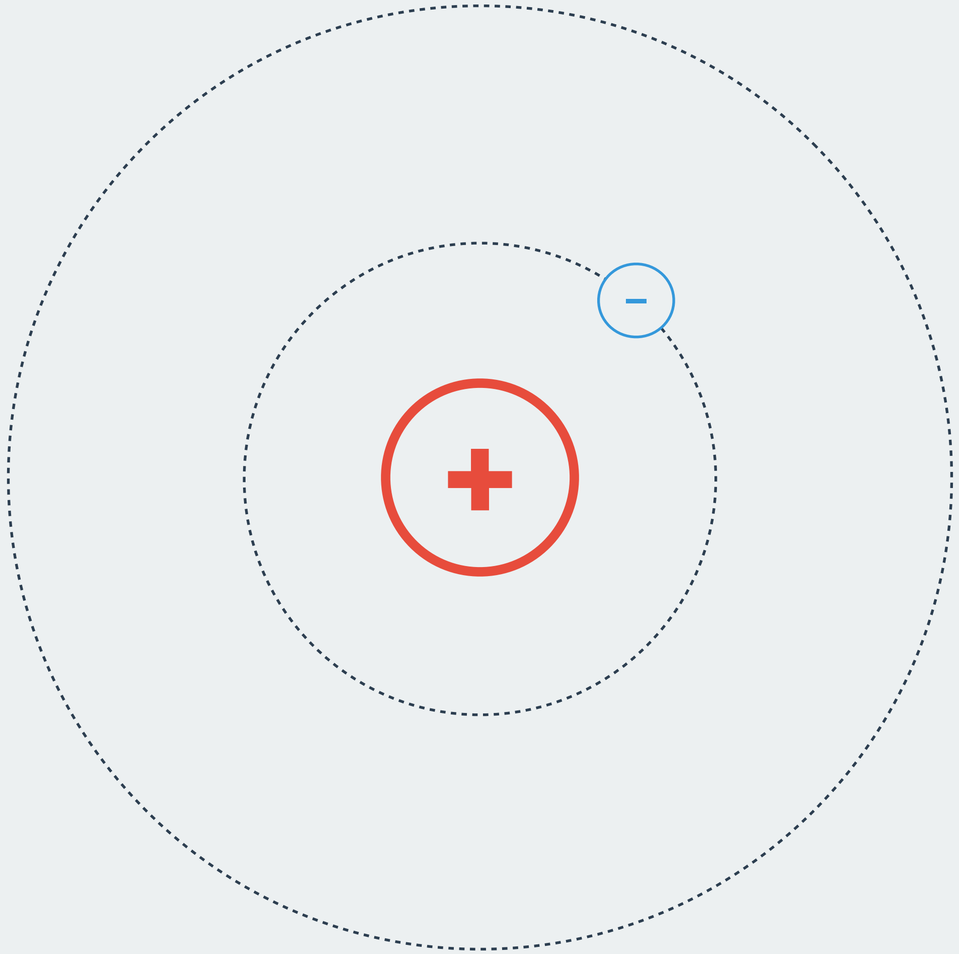

7=0111
5=0101
+
1100=12

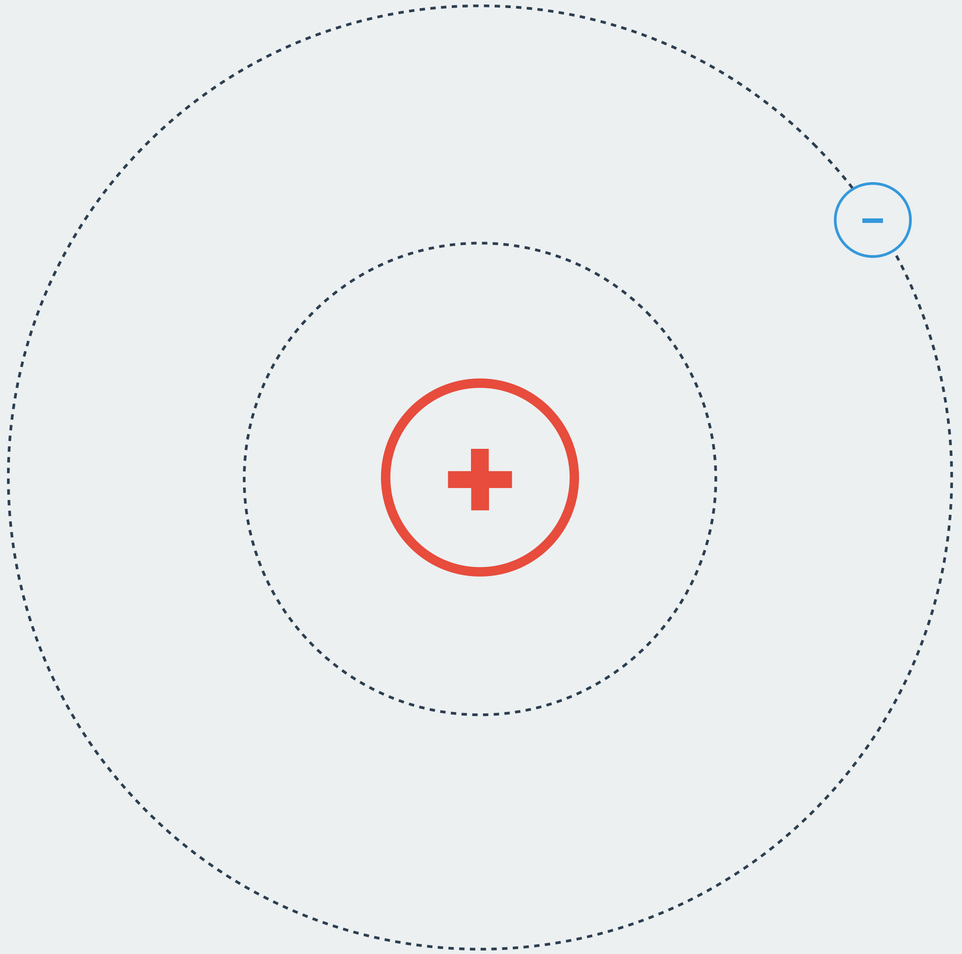
KVANTNO

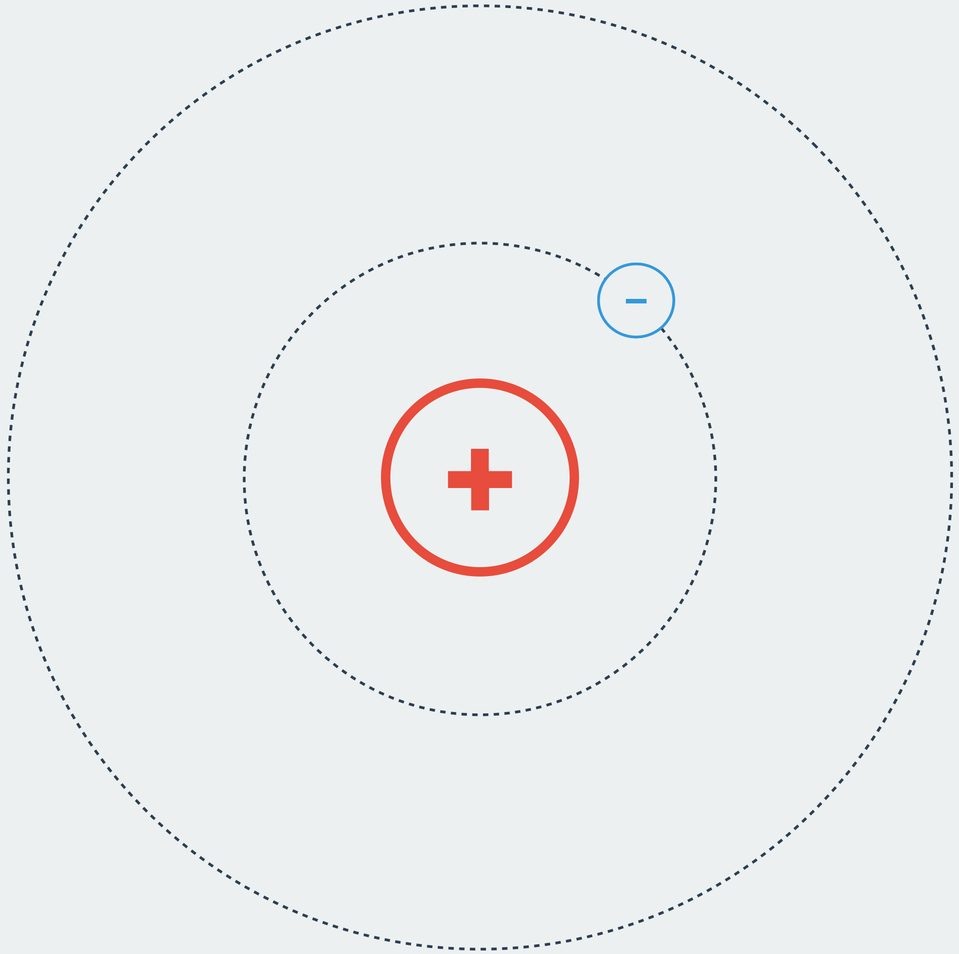
RAČUNALNIŠTVO

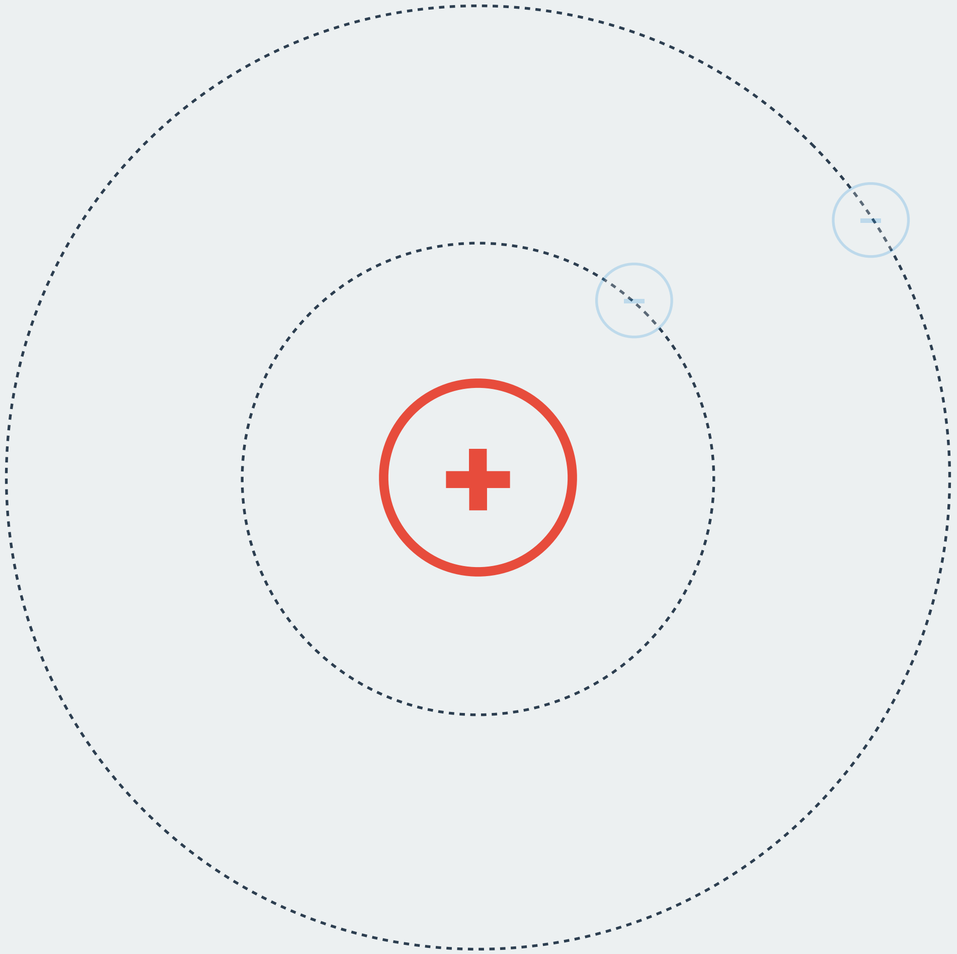
KVANTNO RAČUNALNIŠTVO

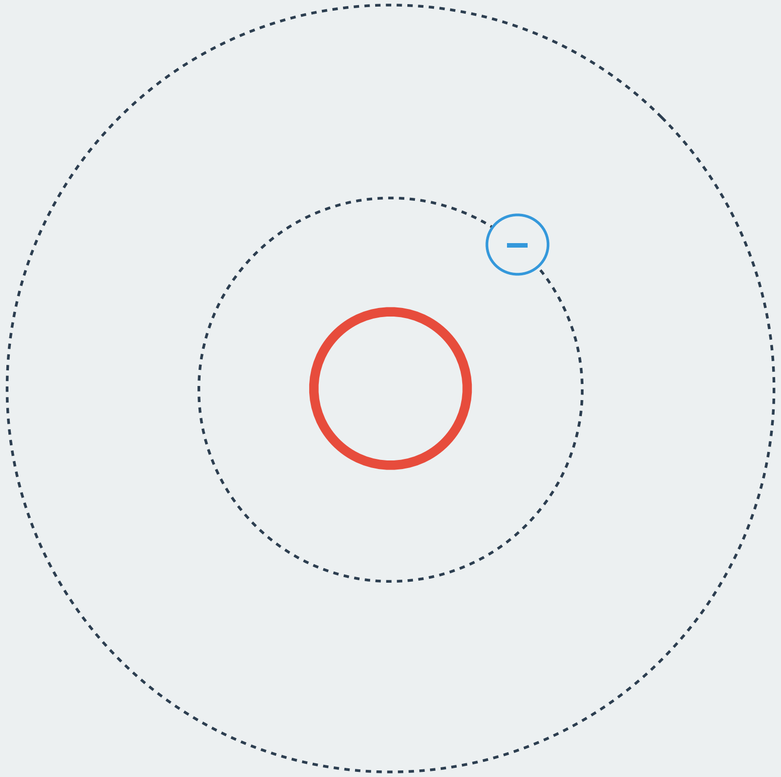


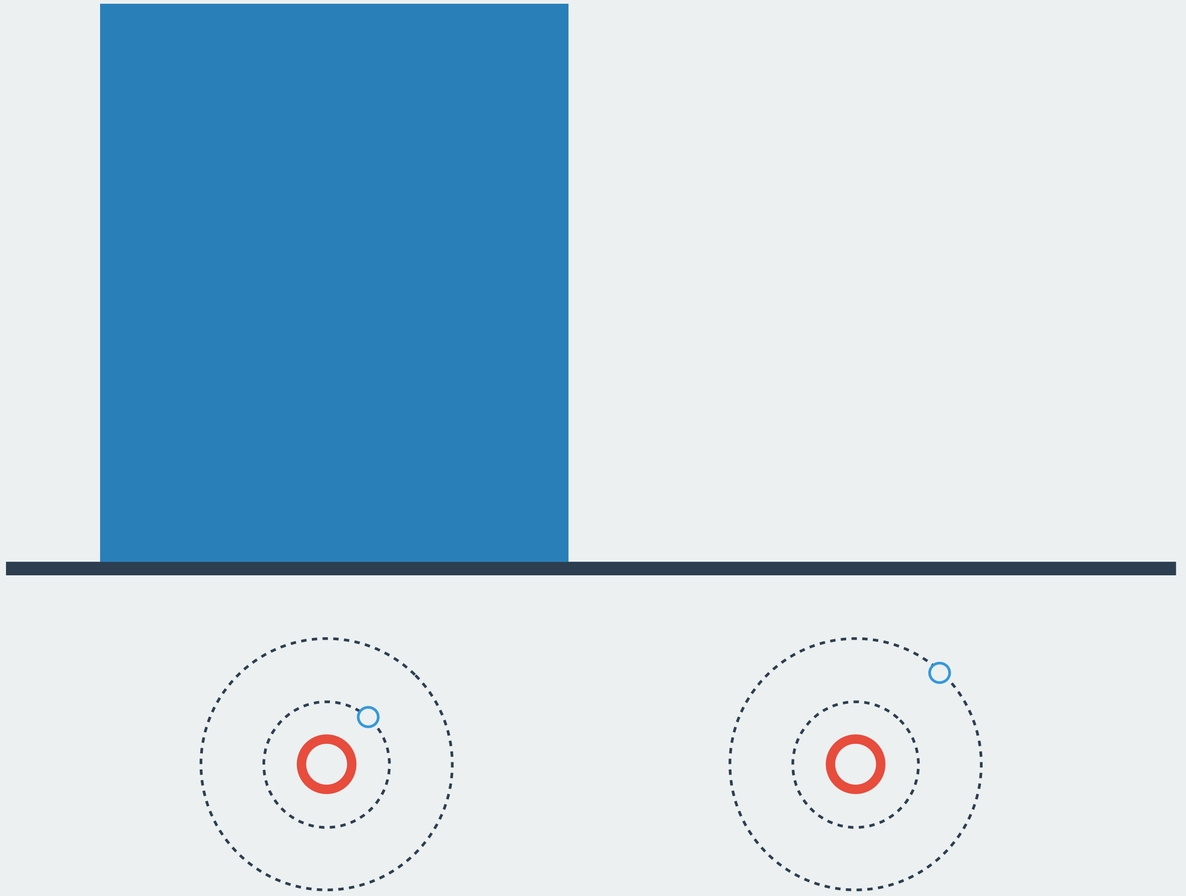


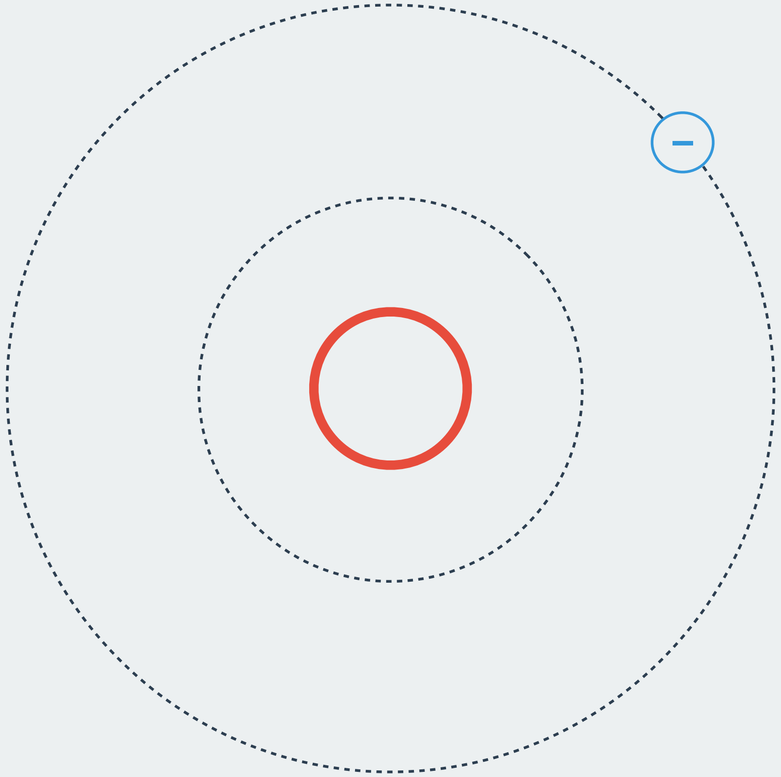


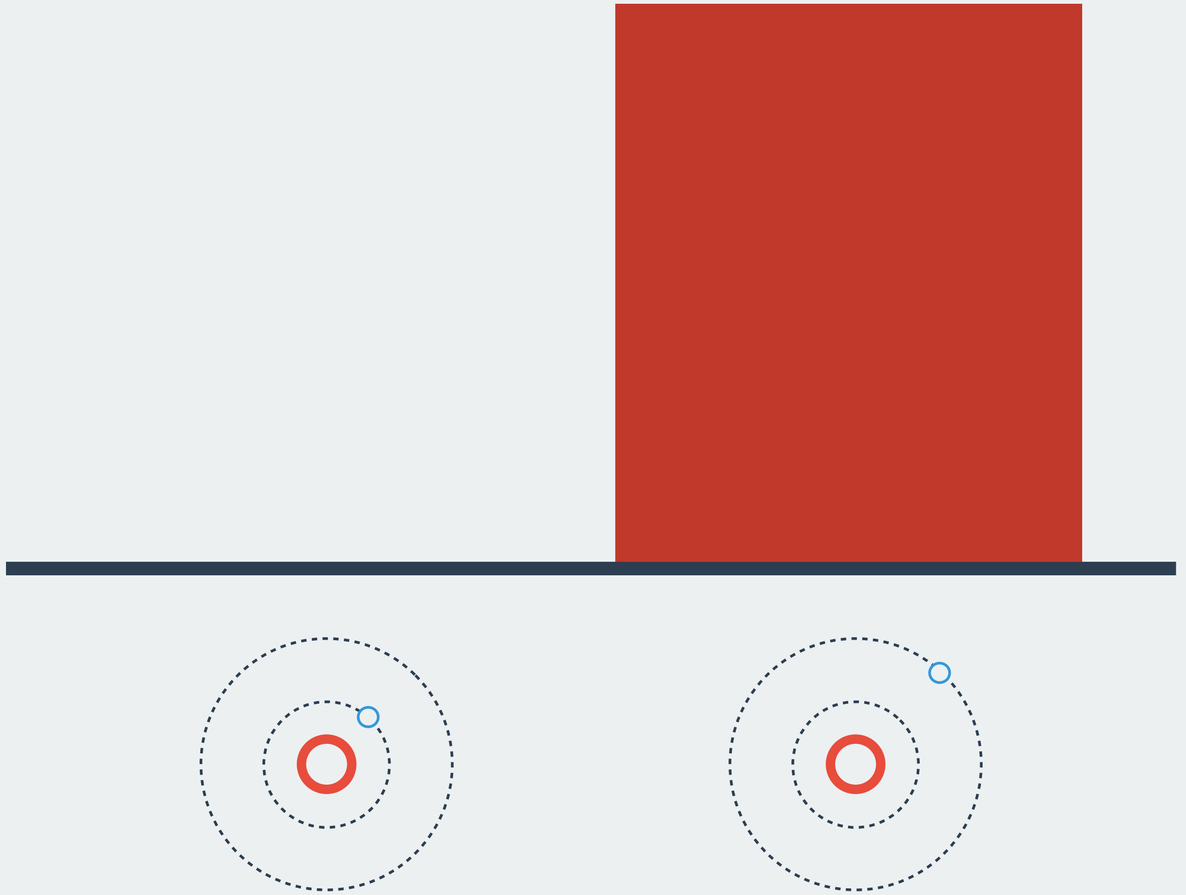


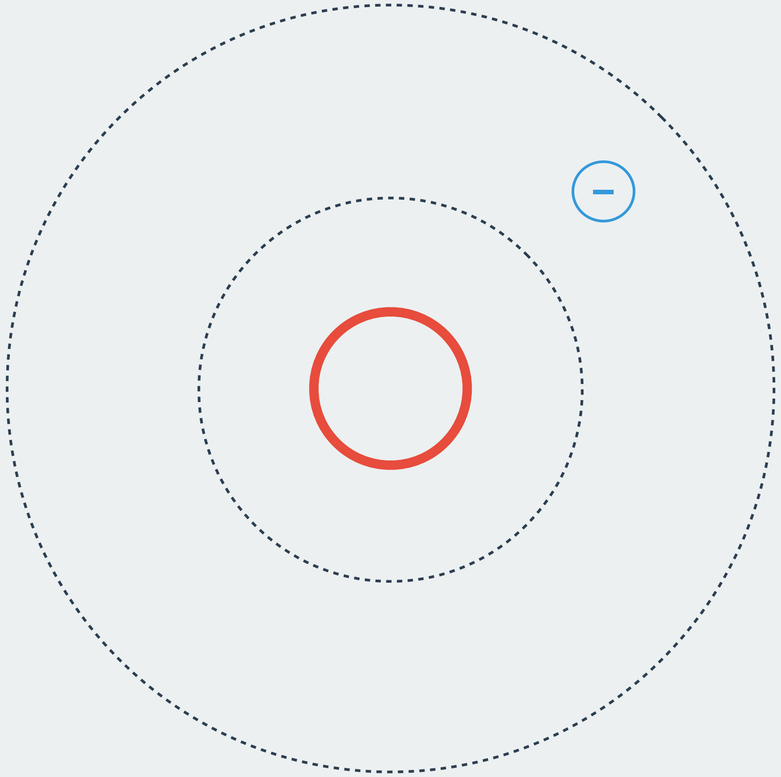


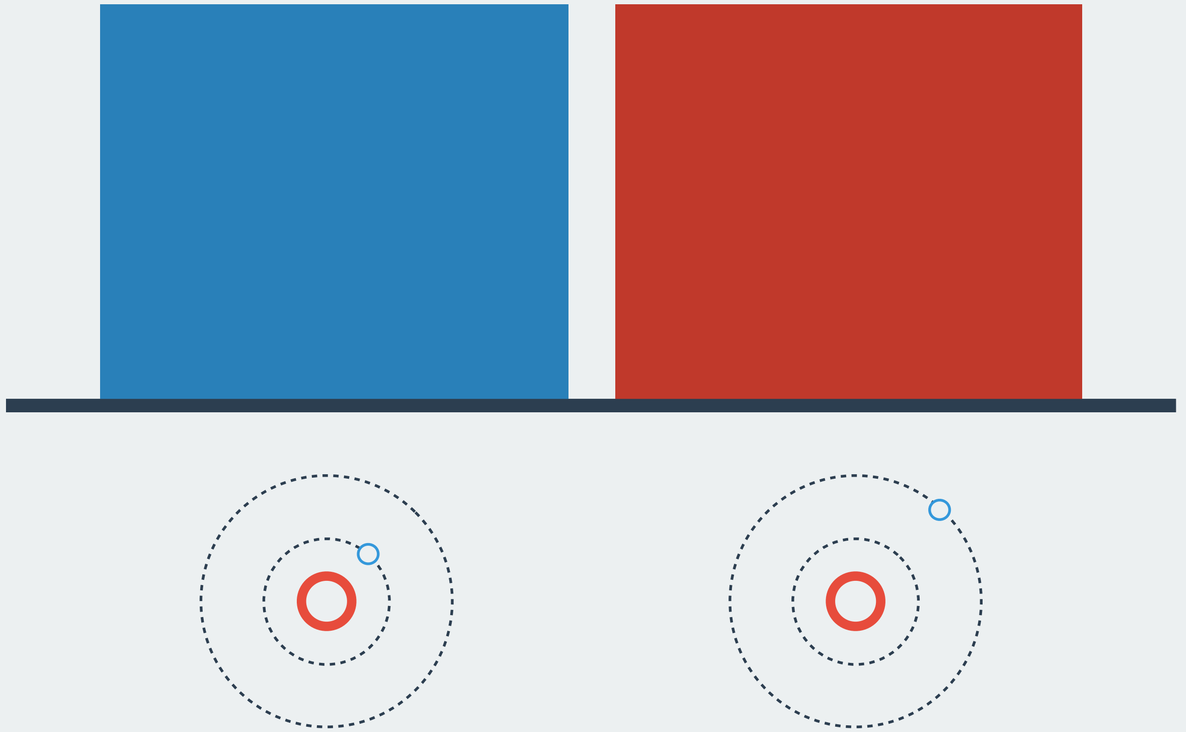


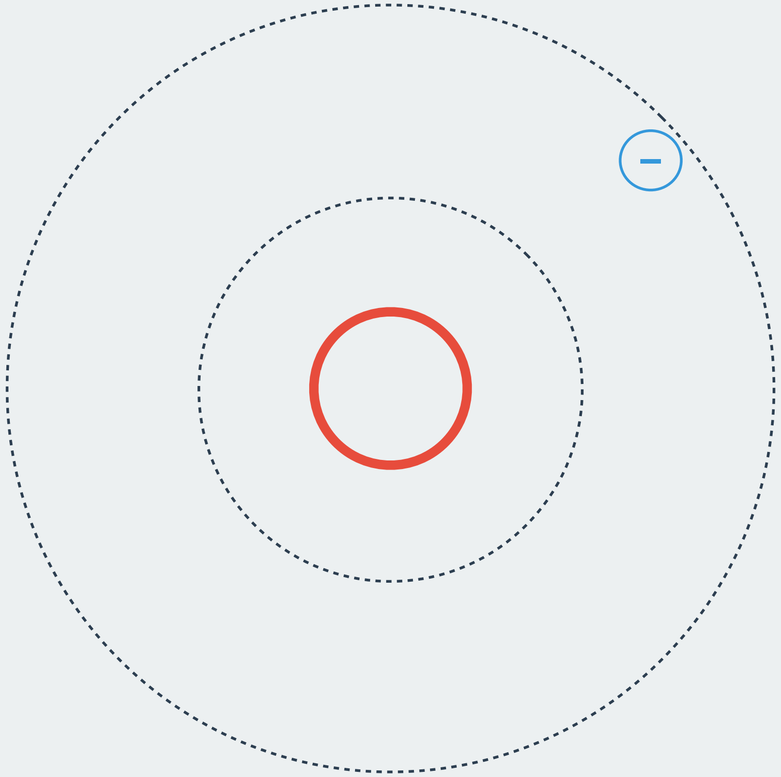


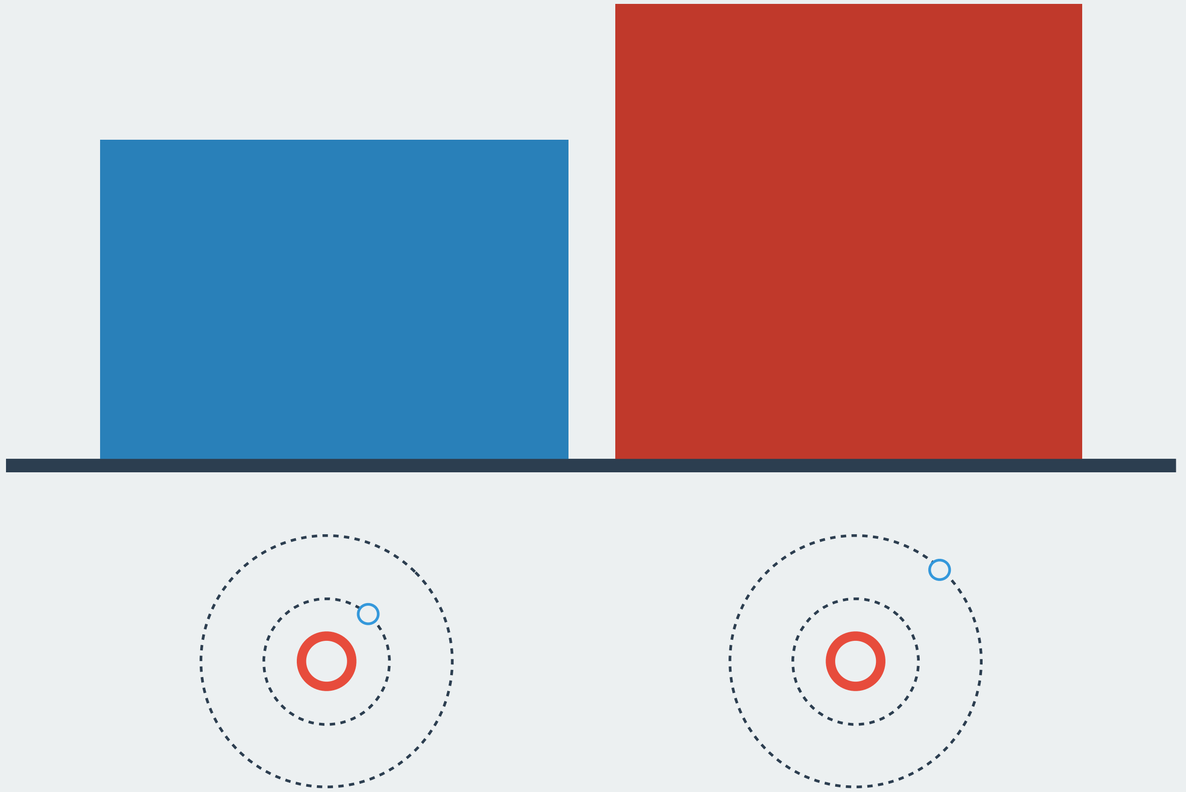


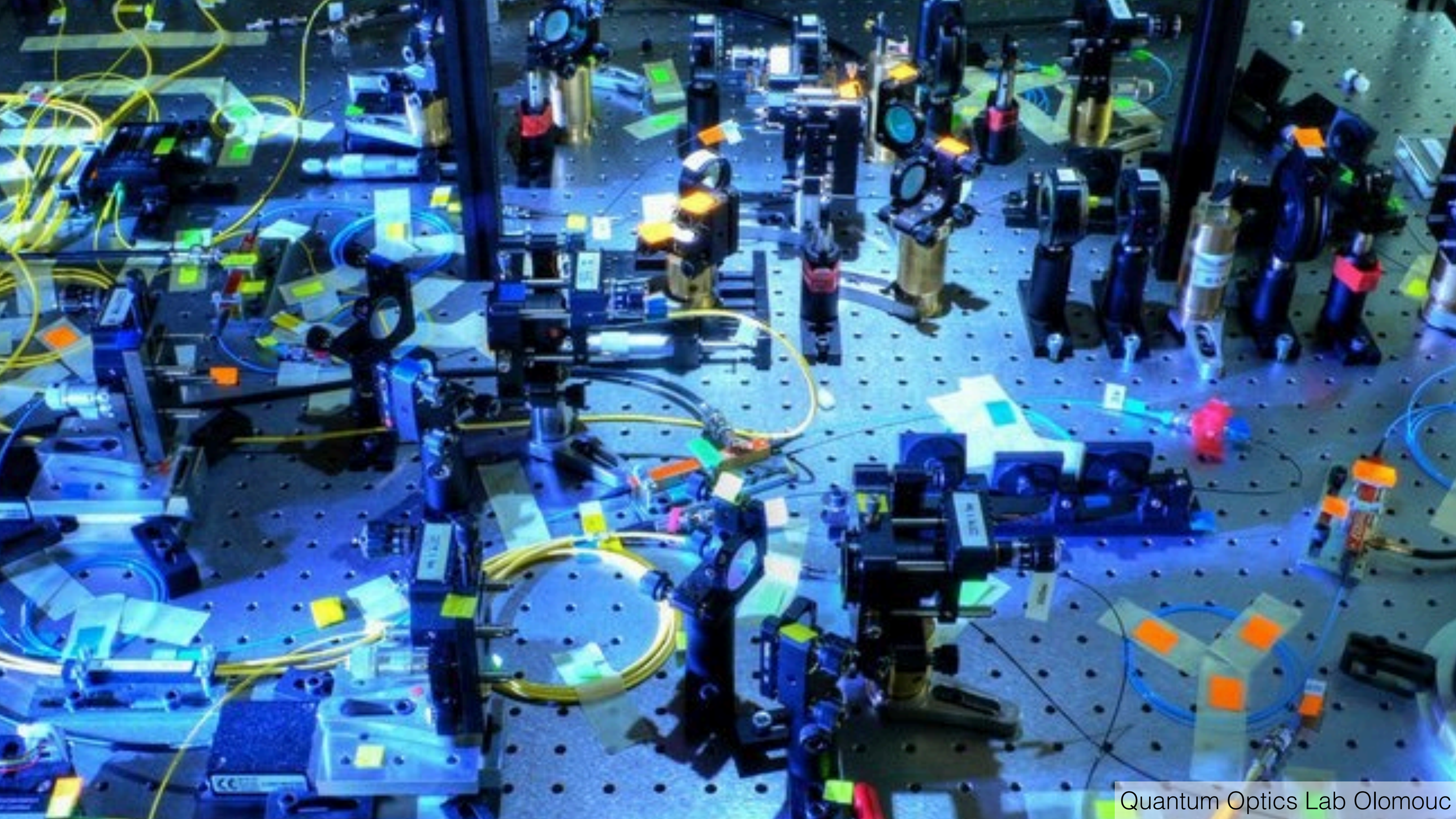




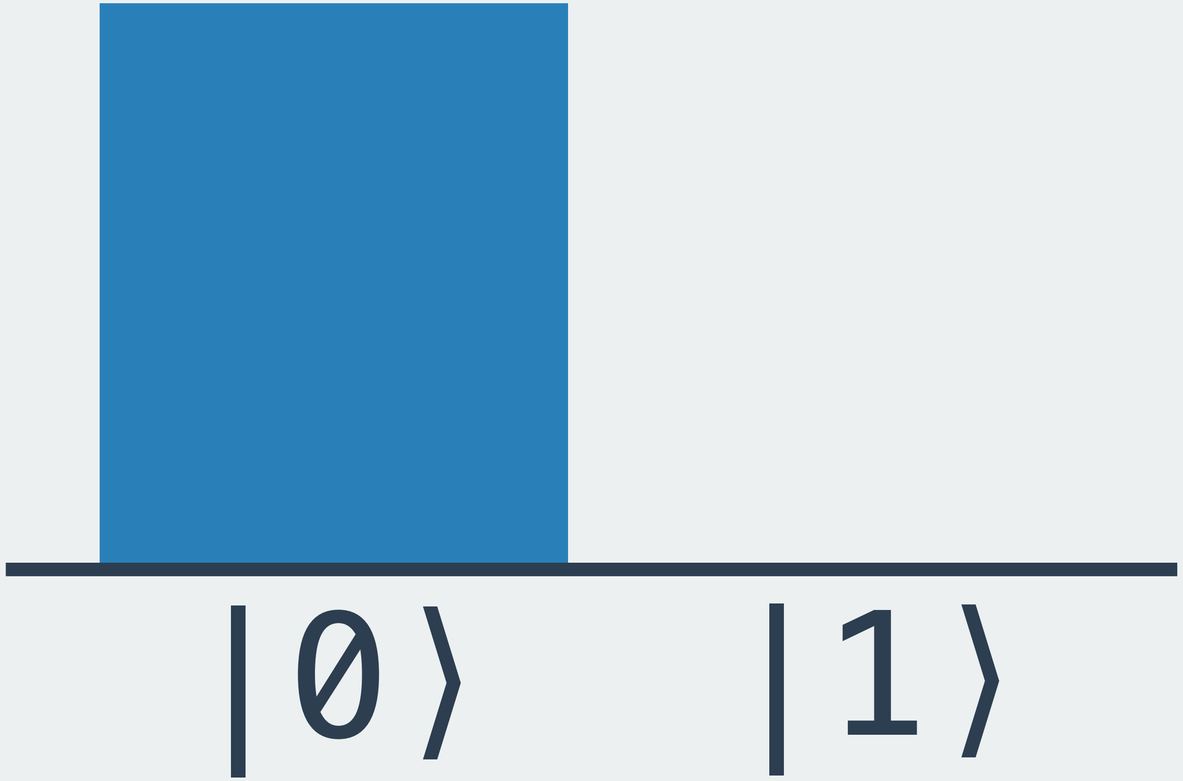


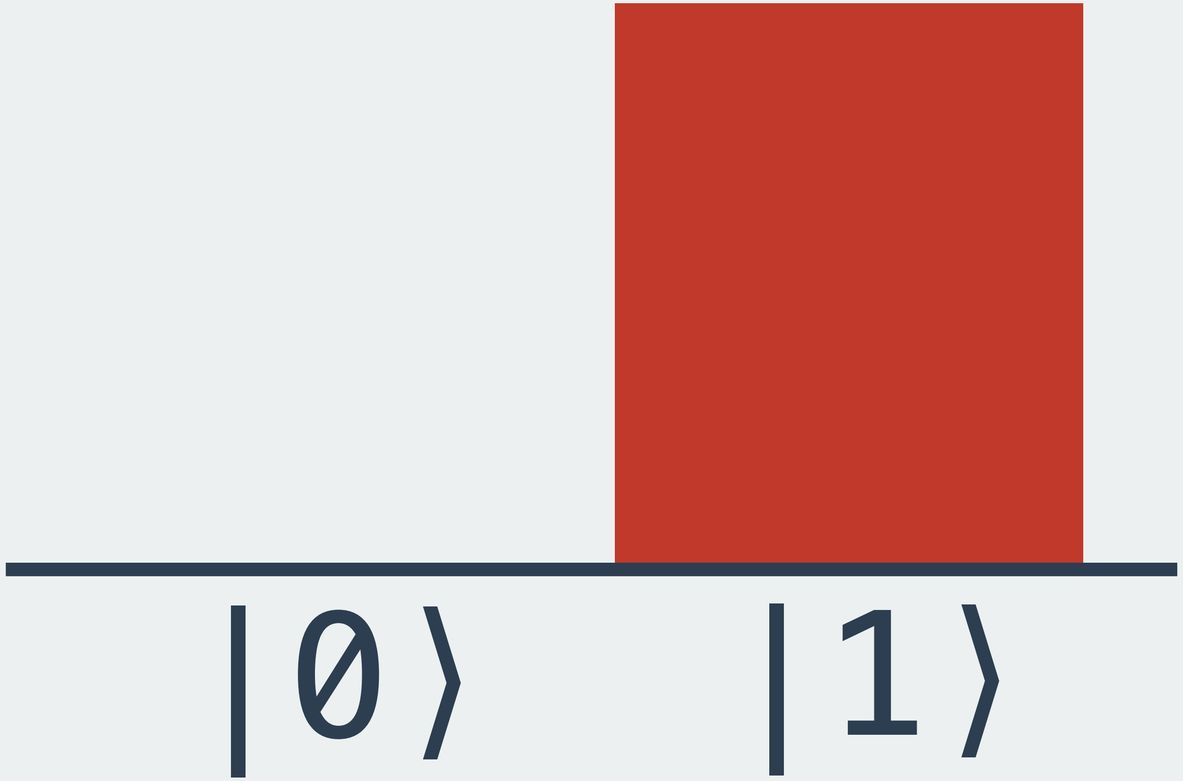


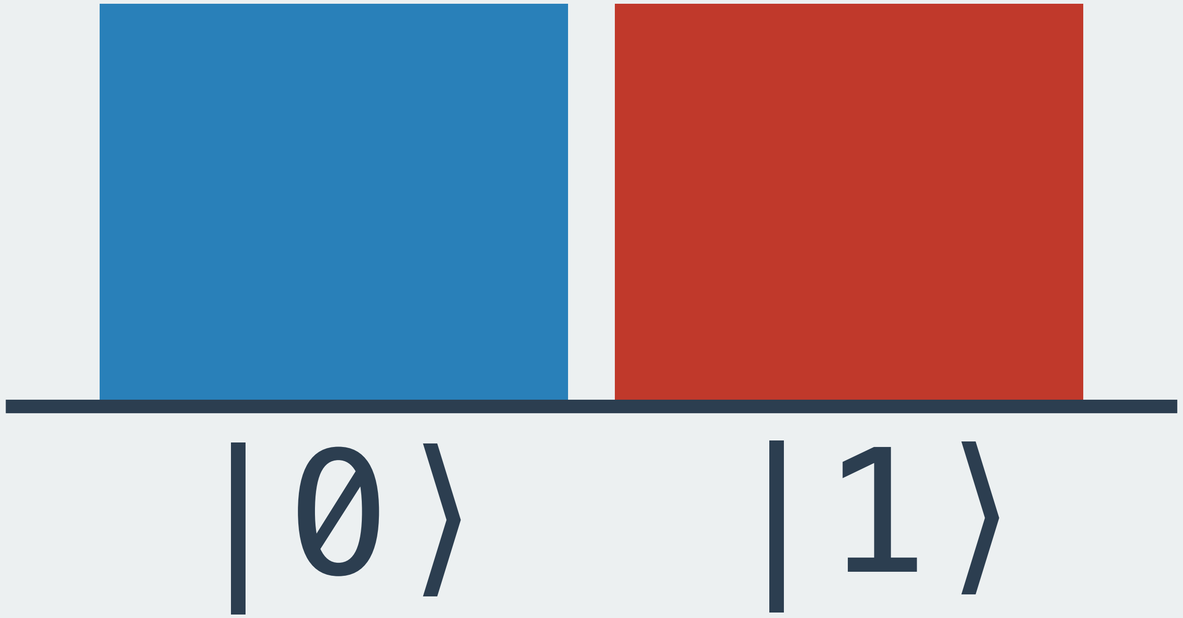


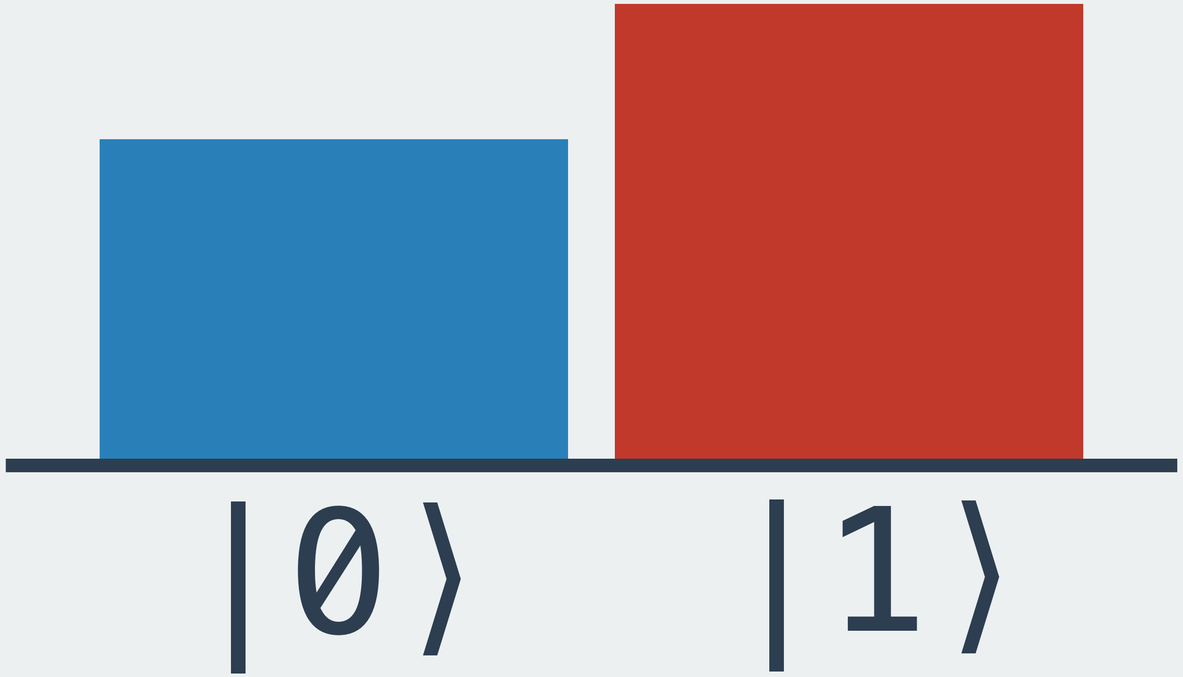

Quantum Optics Lab Olomouc

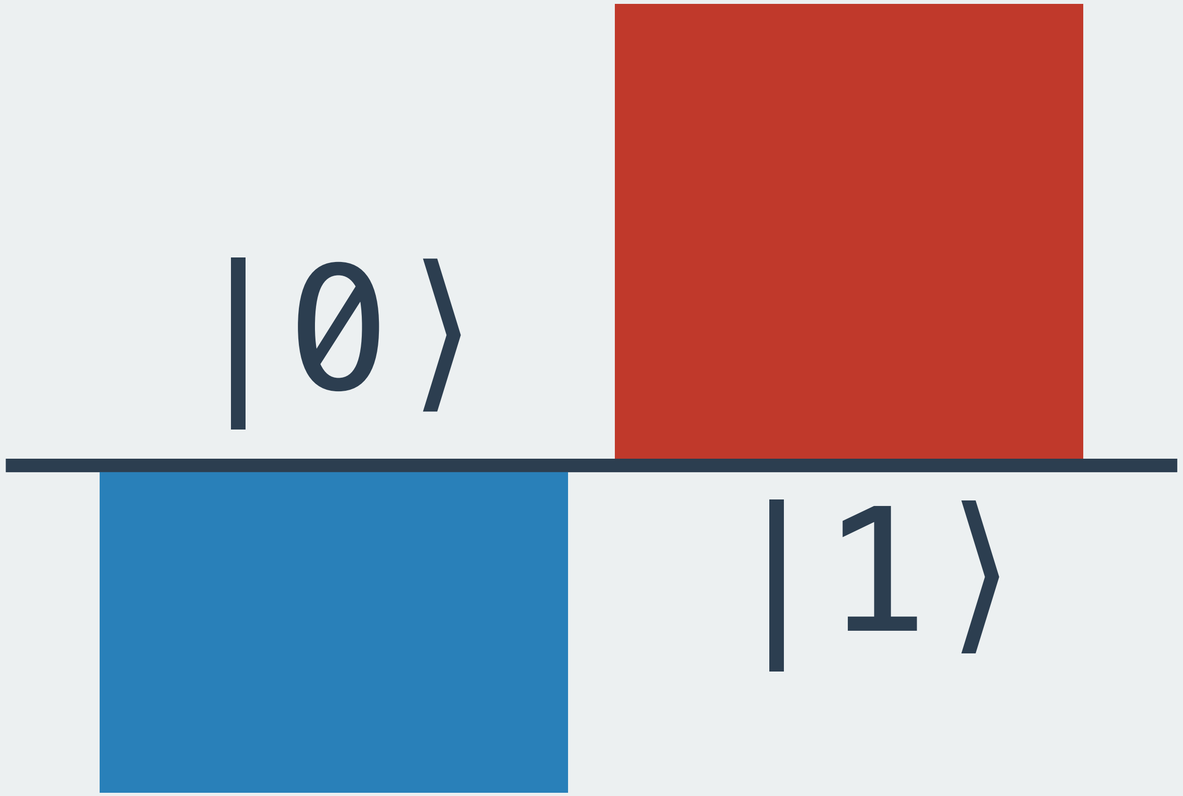
simulacija žarka

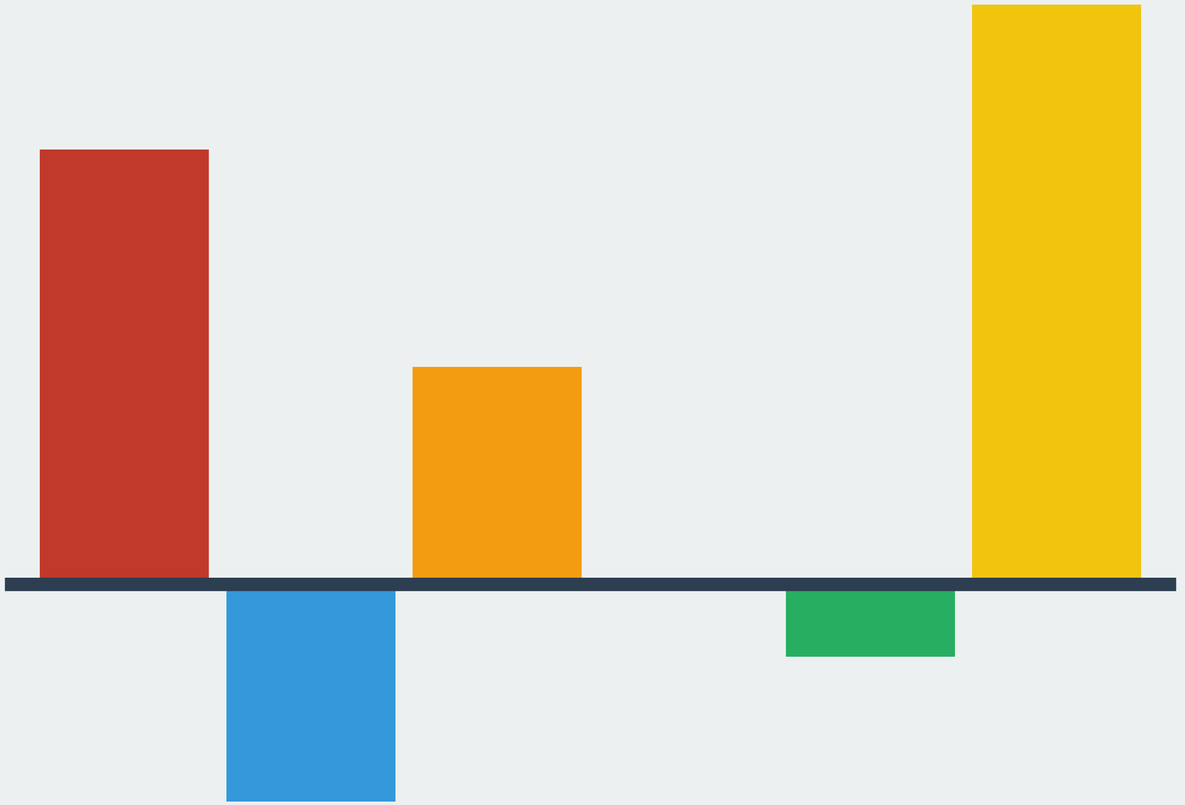

|0⟩
|1⟩

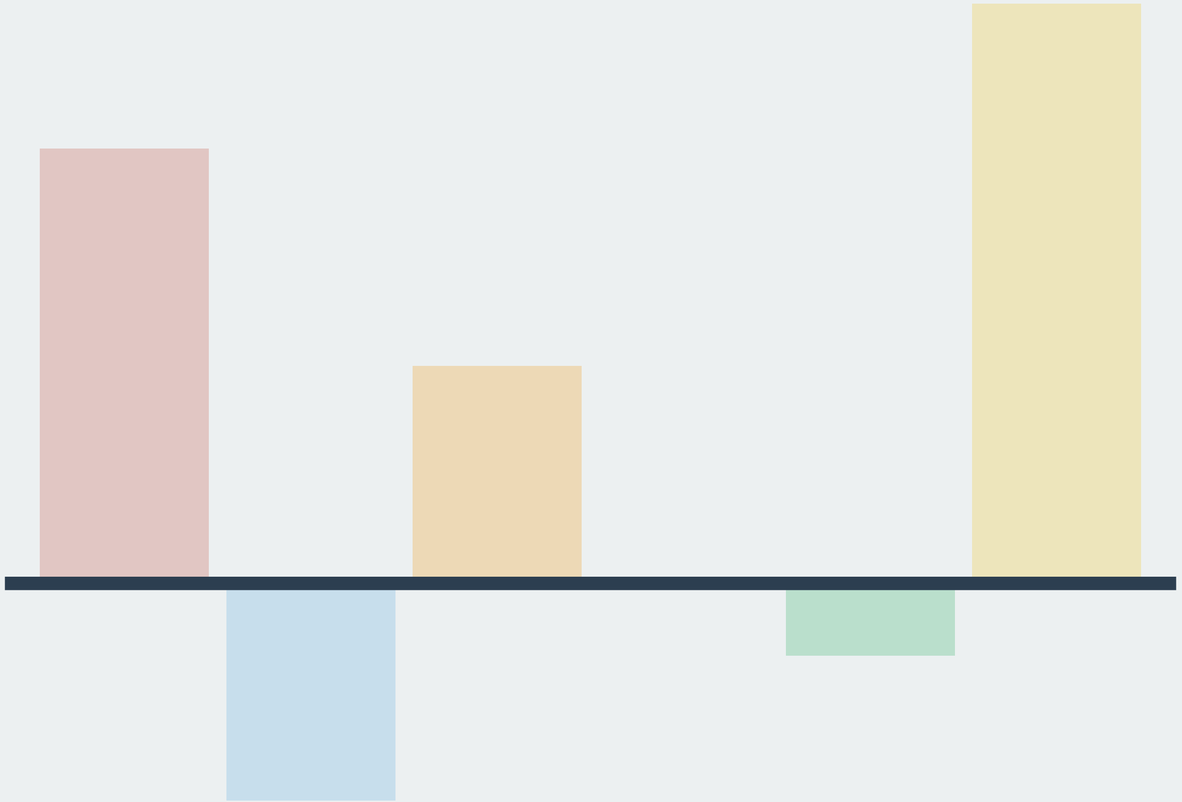

|0⟩
|1⟩

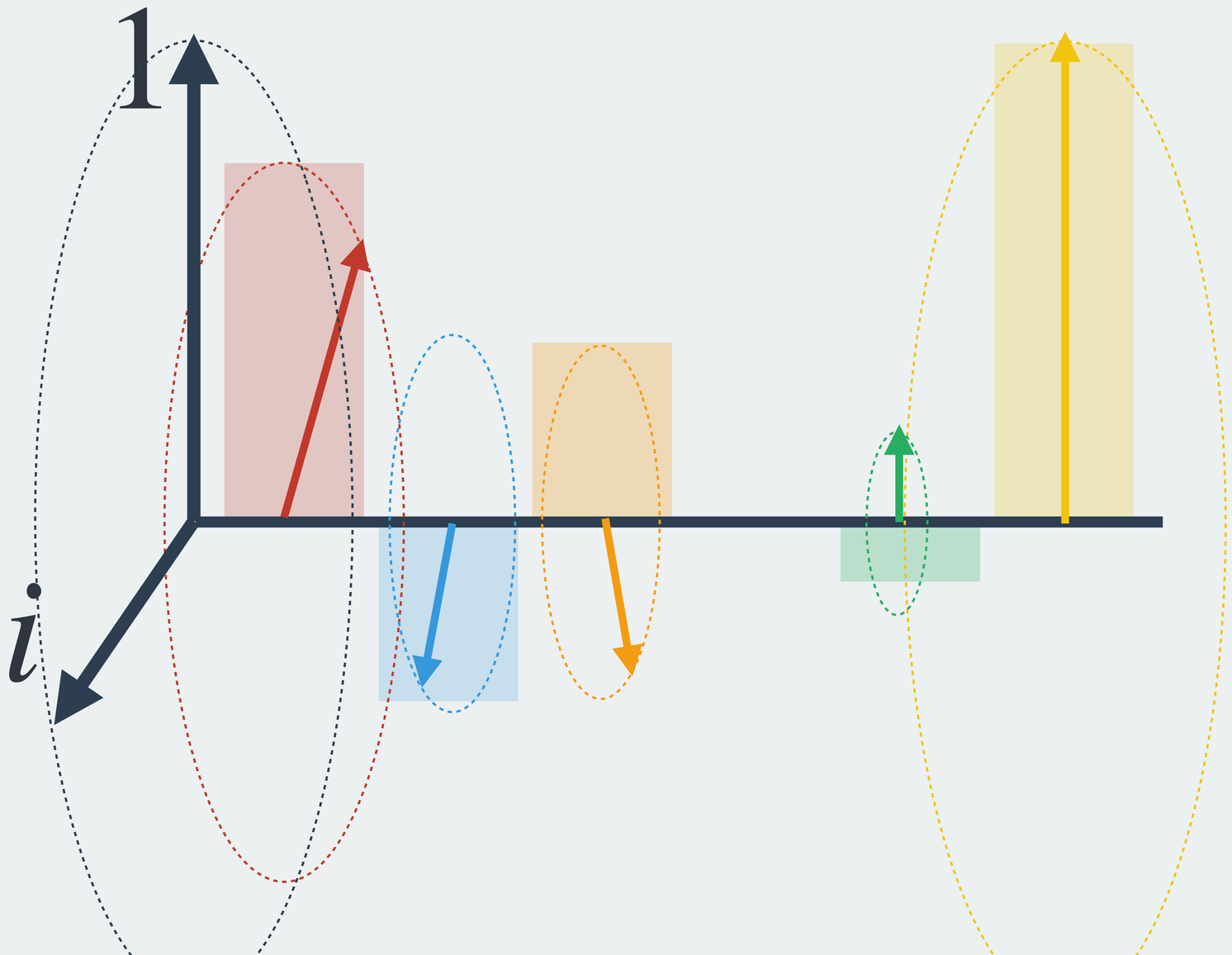

|0⟩
|1⟩


|0⟩
|1⟩

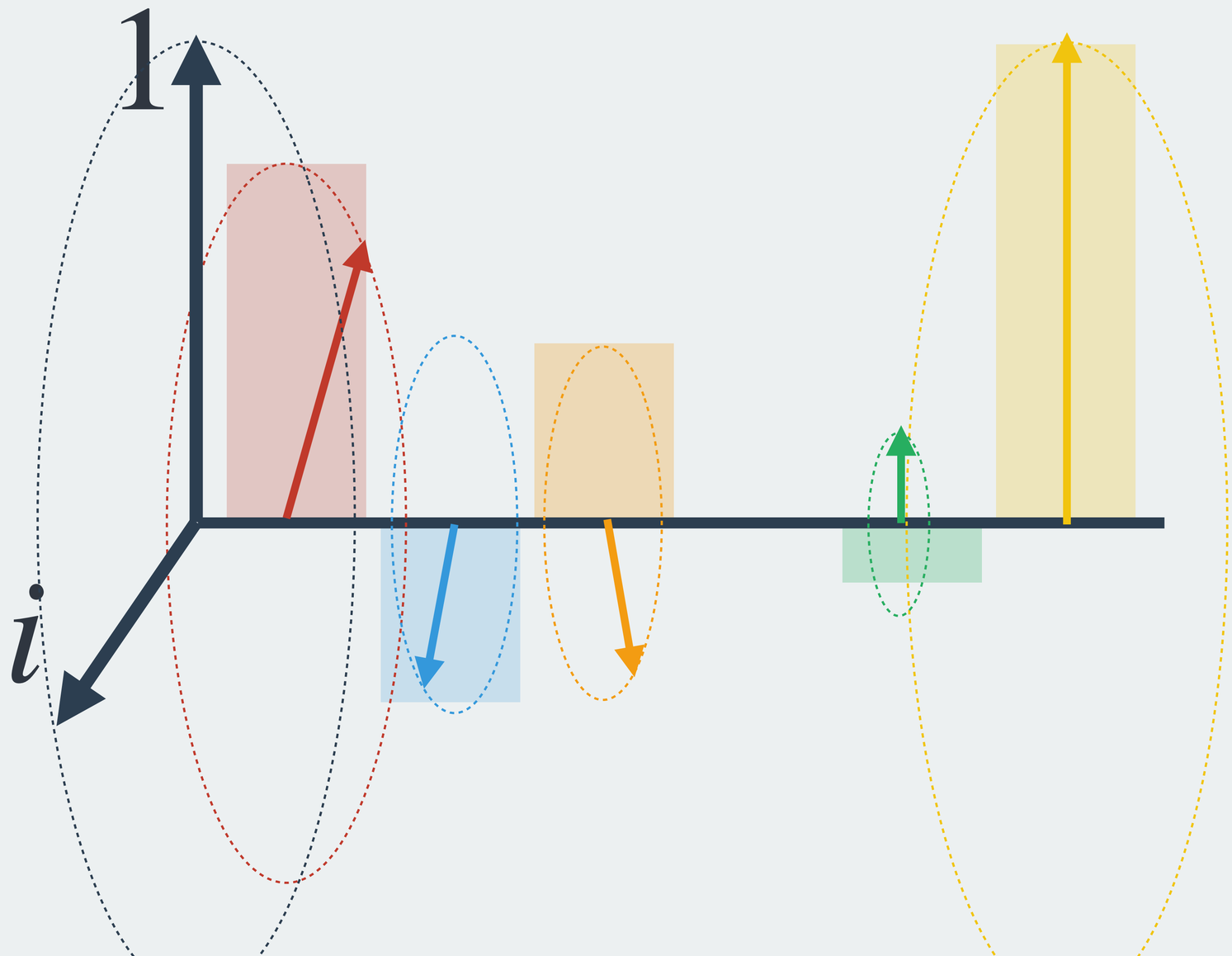

|0⟩
|1⟩

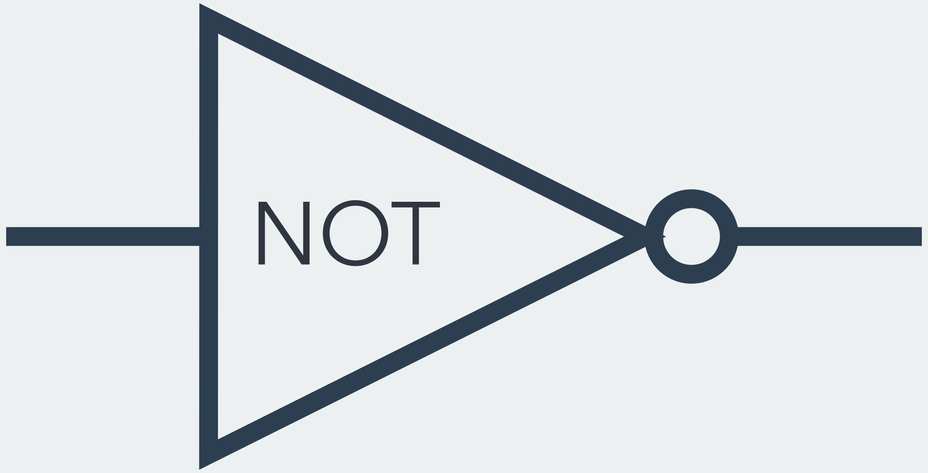


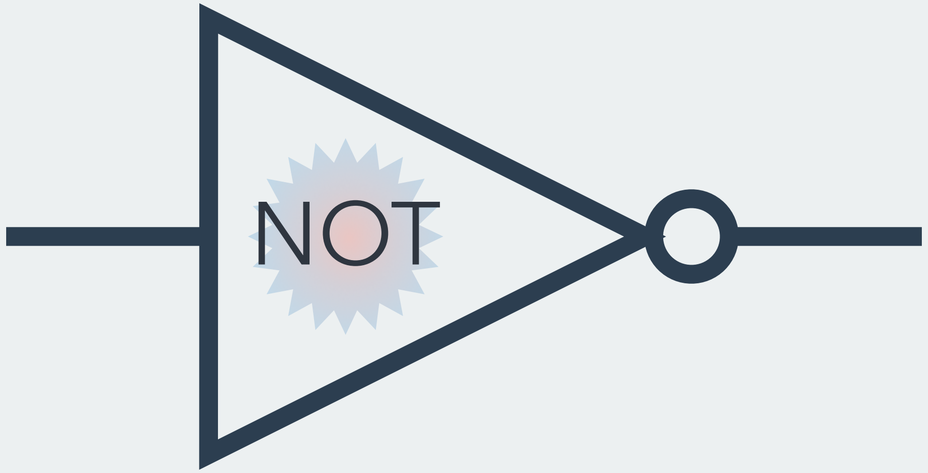


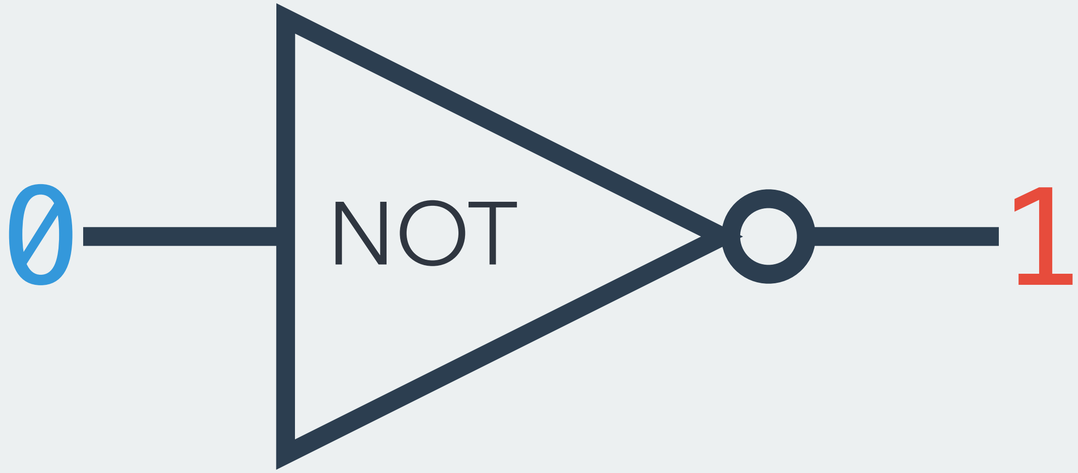

1
i

$$|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$$

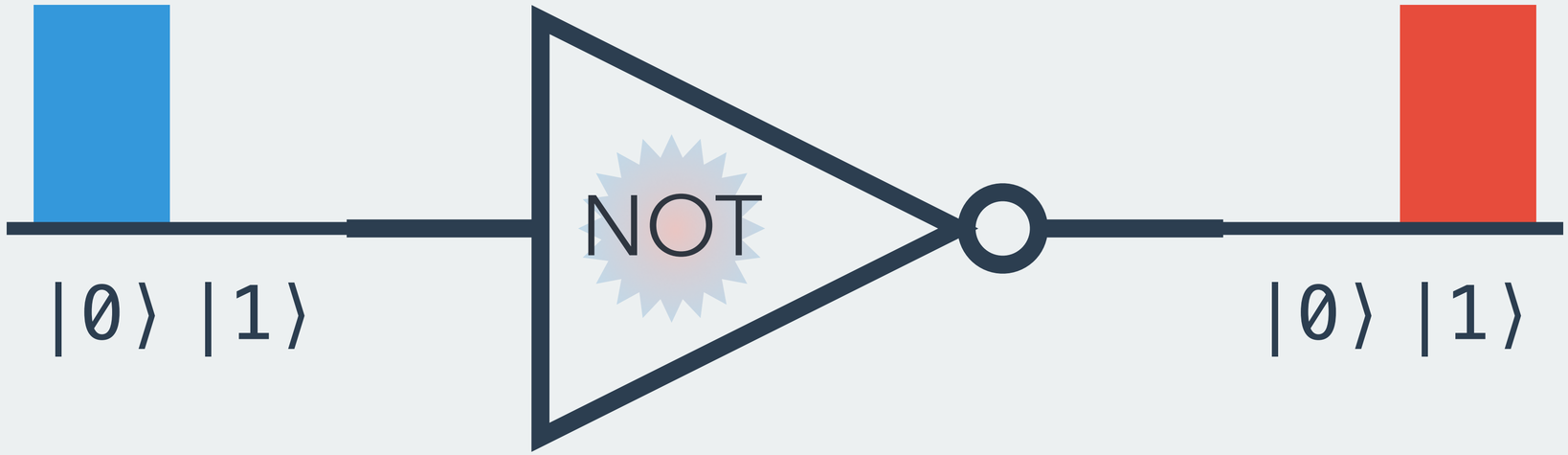


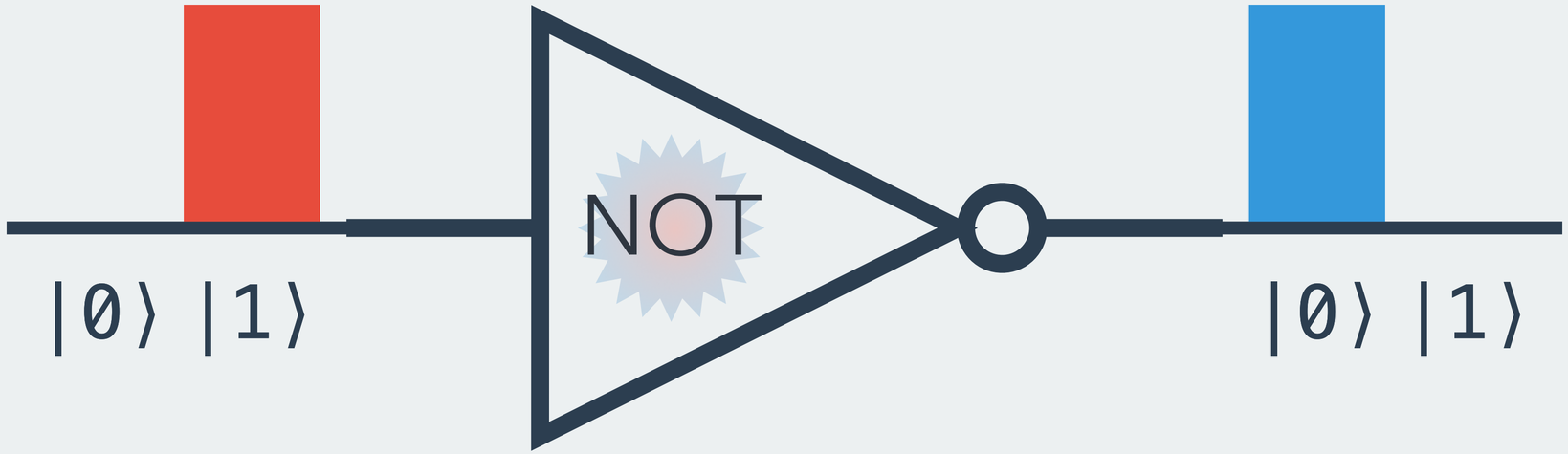

NOT

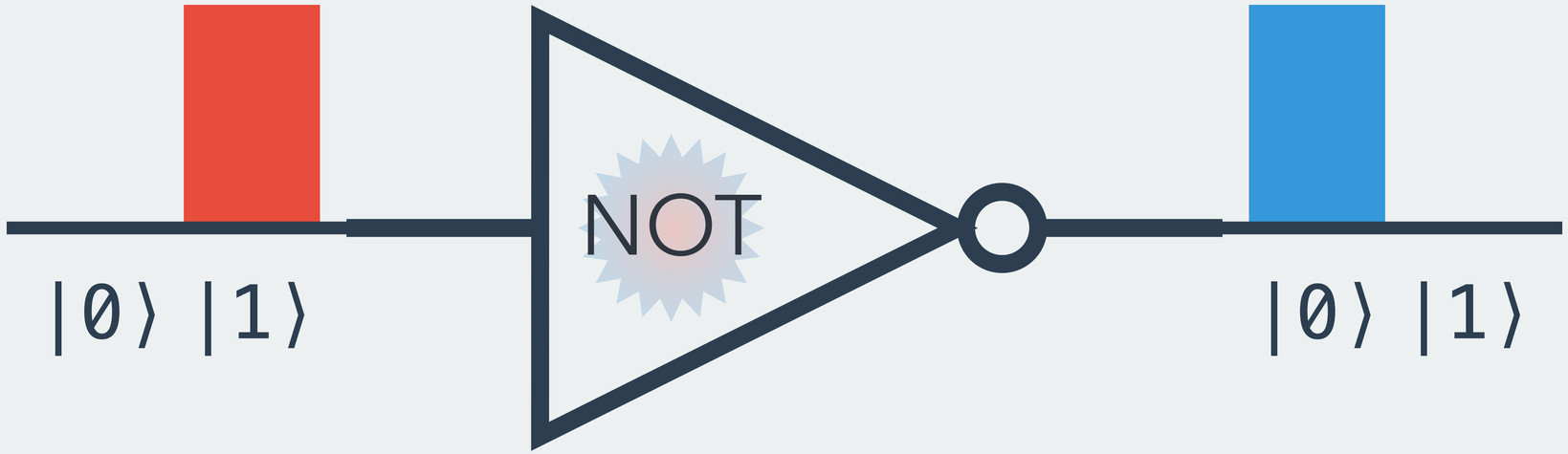

NOT

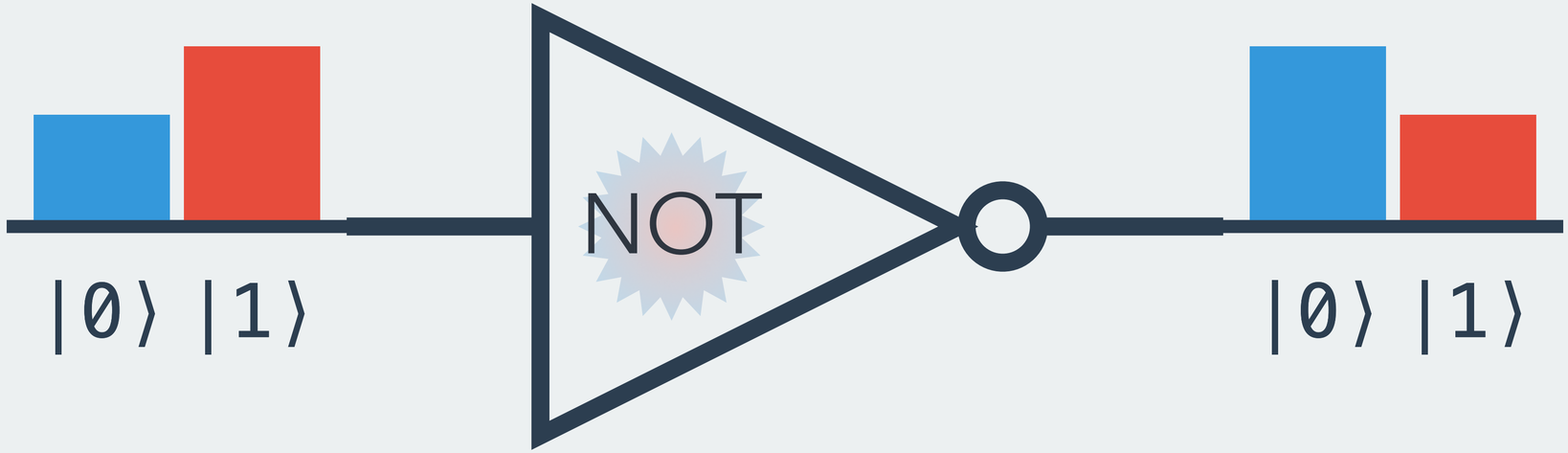

0
NOT
1

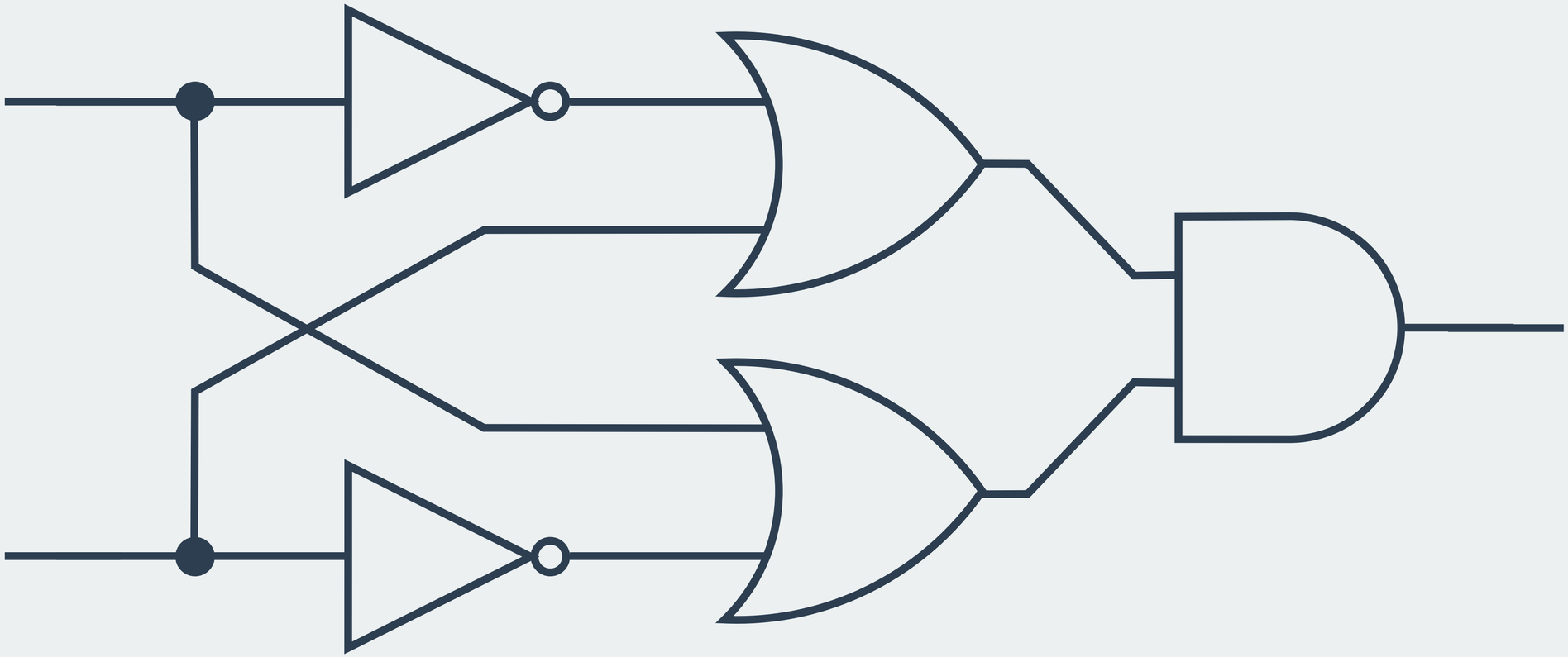
simulacija vrat

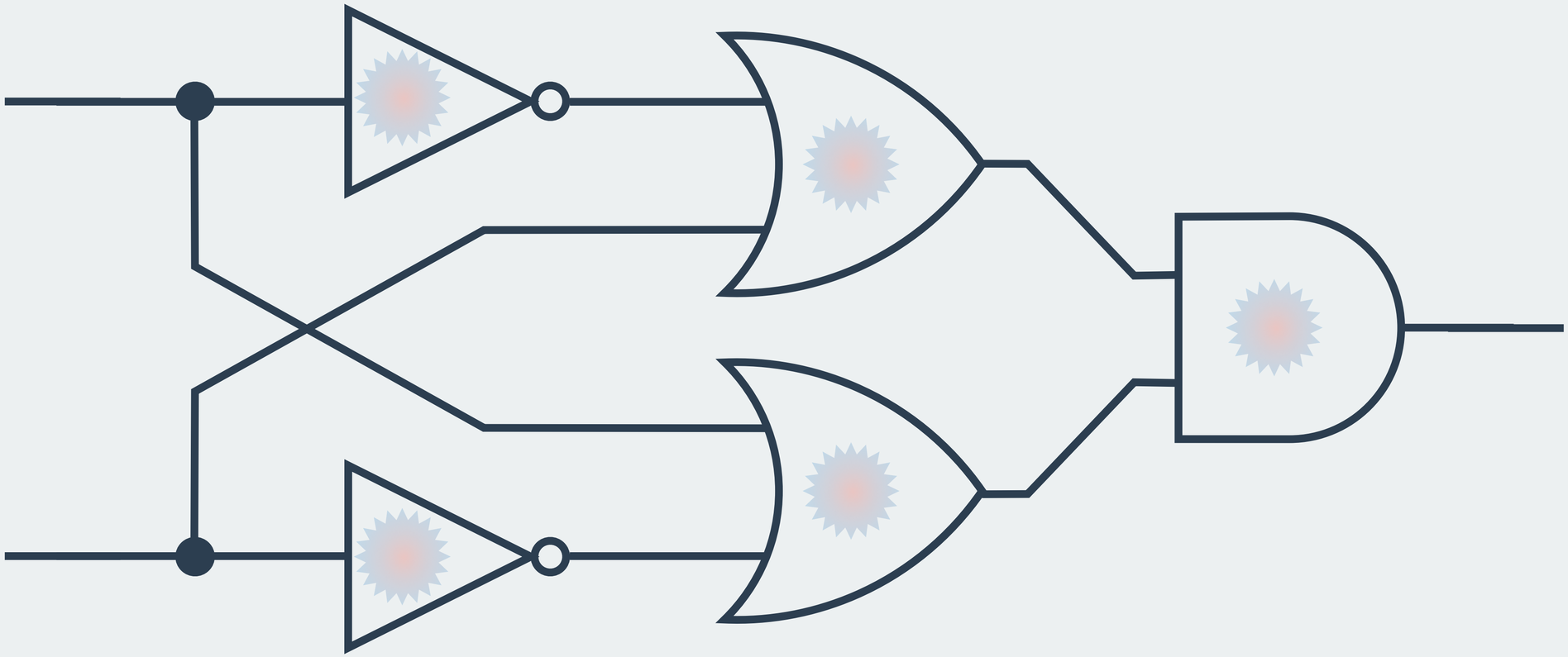

NOT
|0⟩ |1⟩
|0⟩ |1⟩

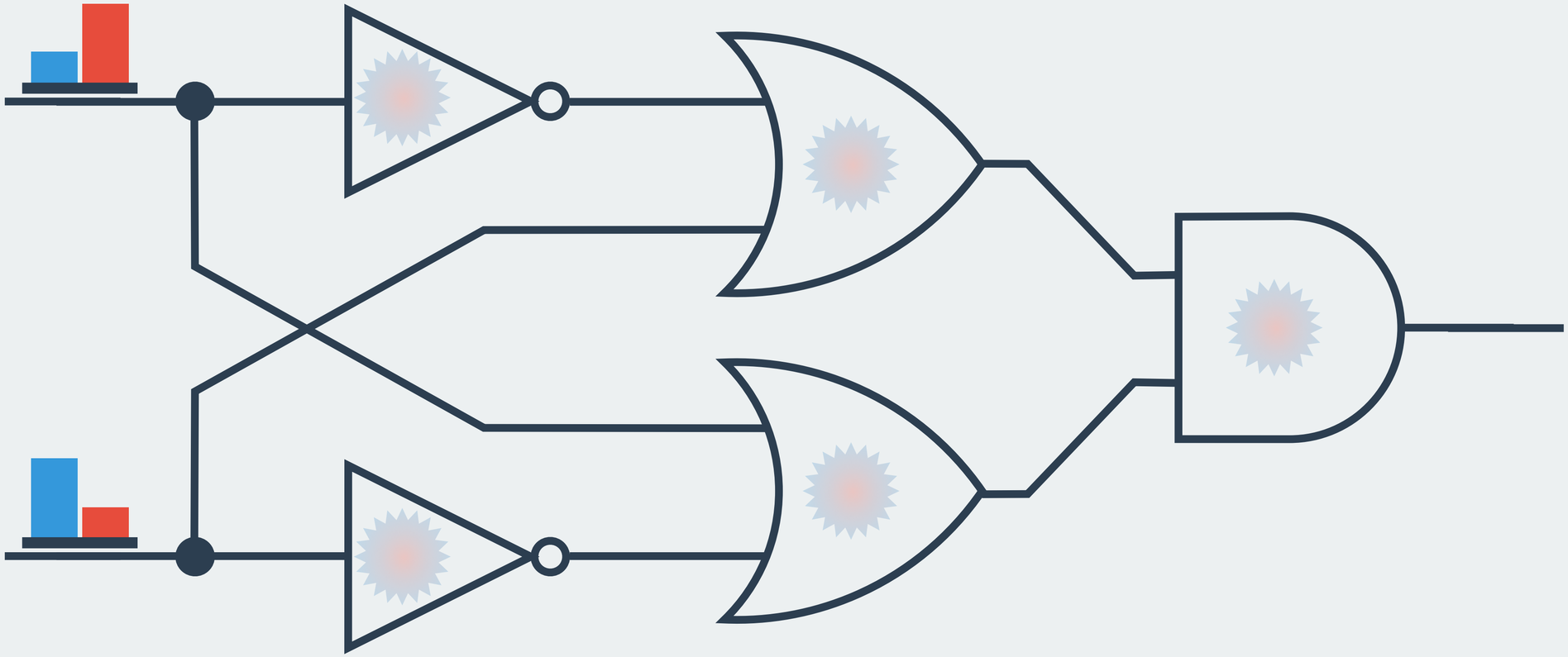

NOT
|0⟩ |1⟩
|0⟩ |1⟩

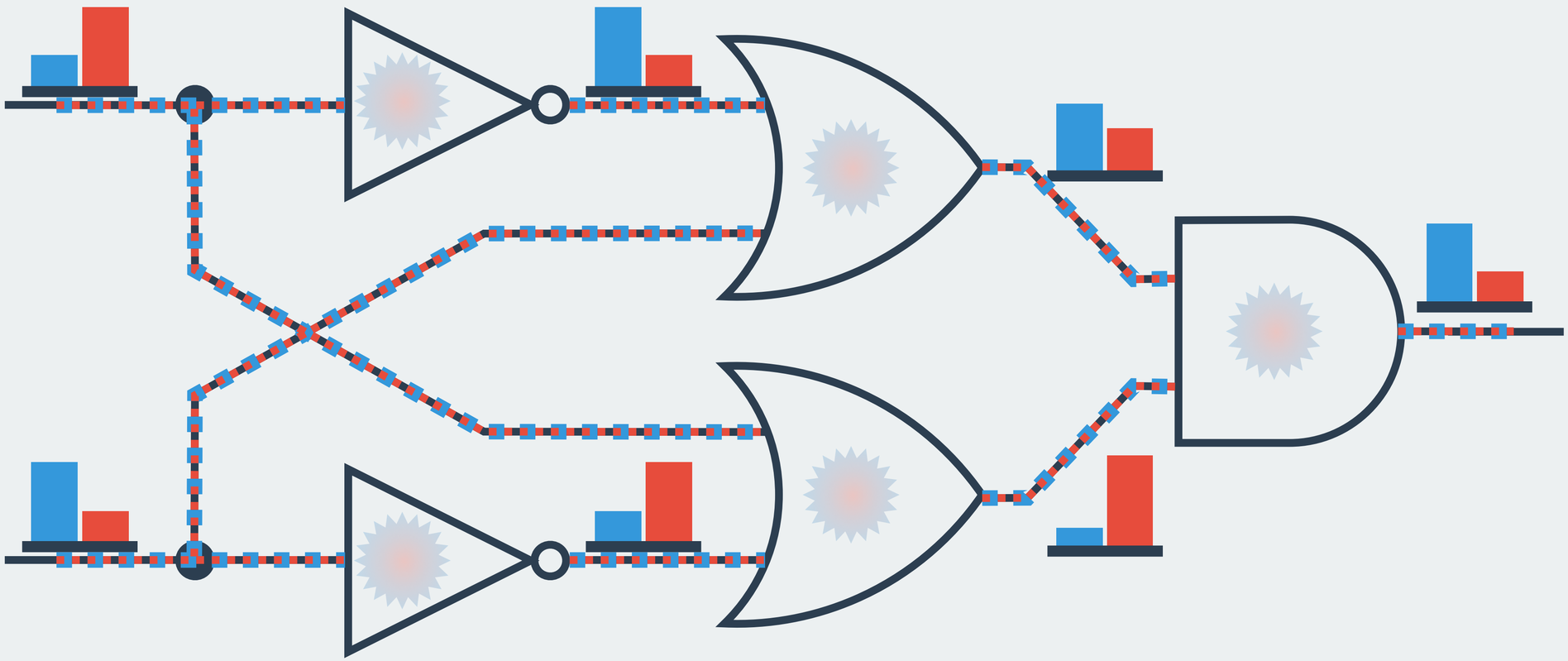

NOT
|0⟩ |1⟩
|0⟩ |1⟩

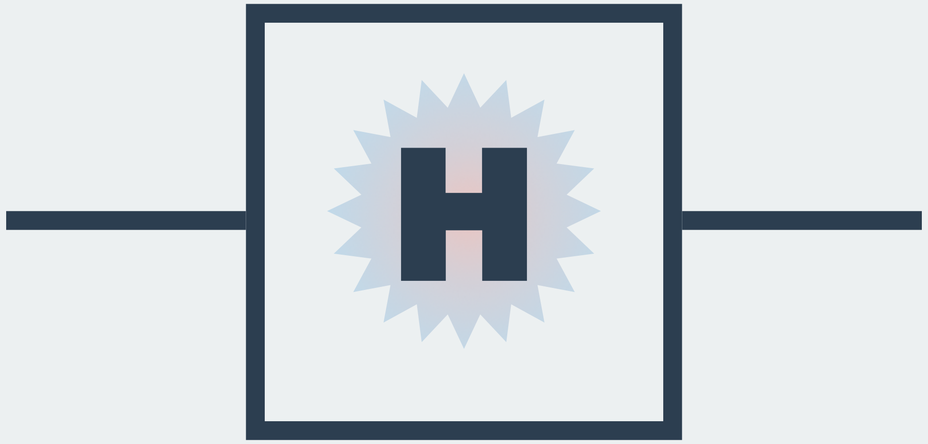

NOT
|0⟩ |1⟩
|0⟩ |1⟩

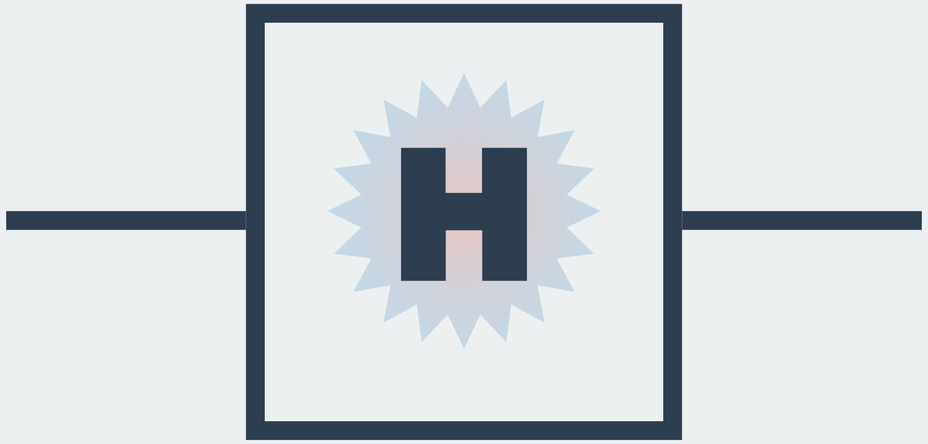




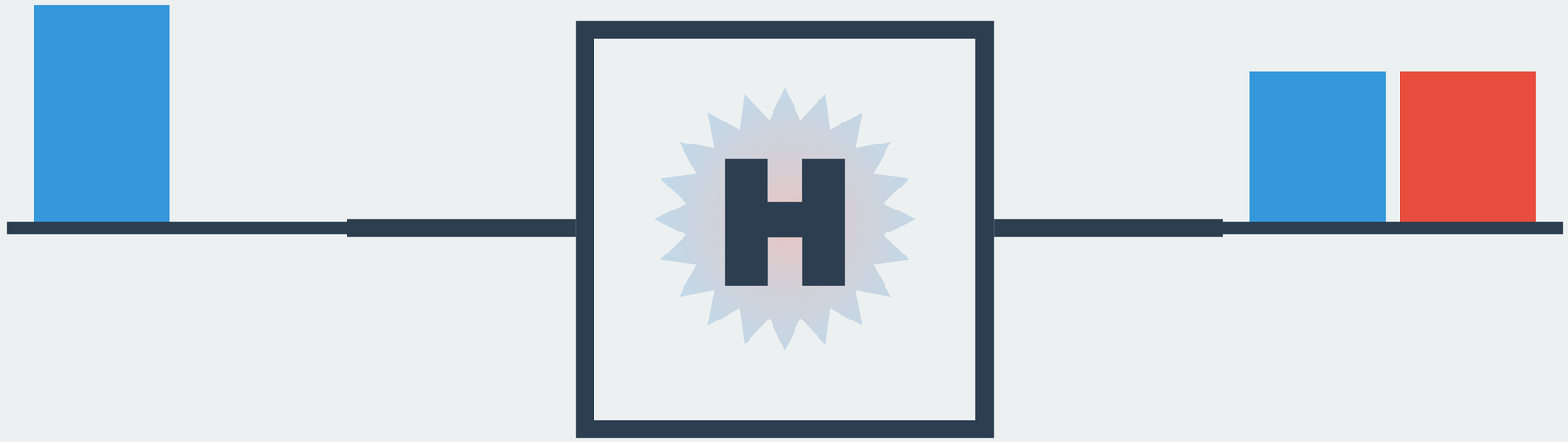


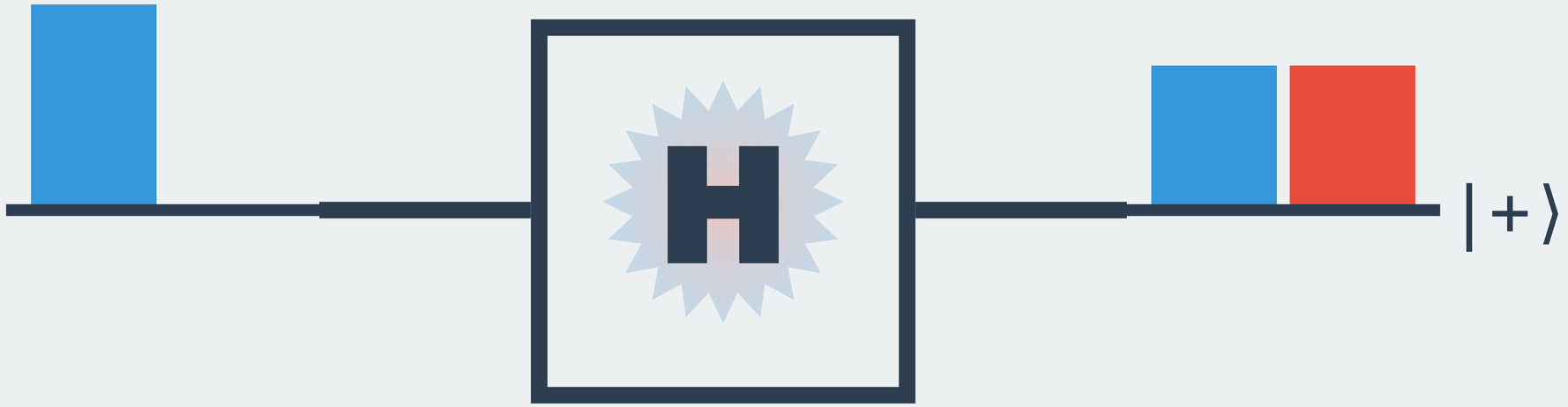


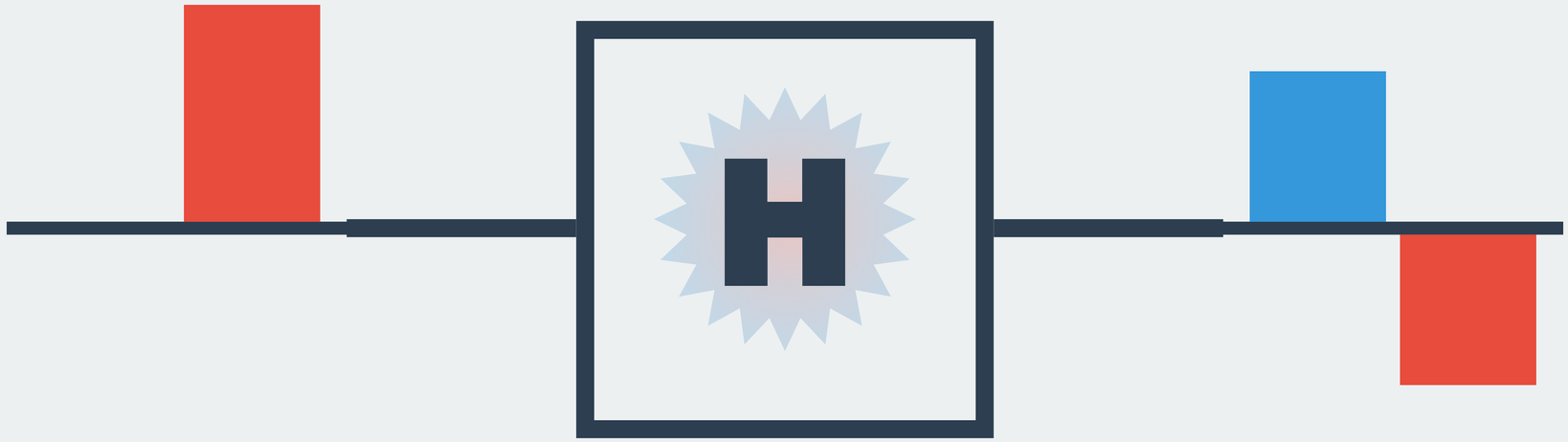


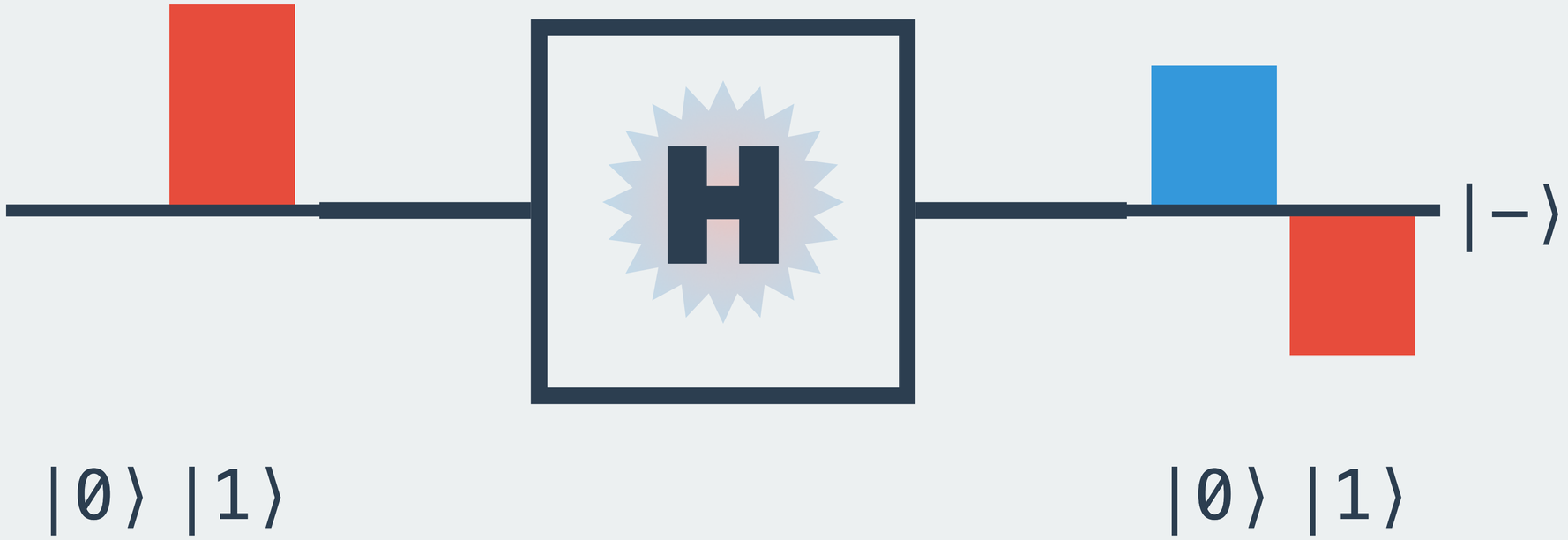


Jacques Hadamard

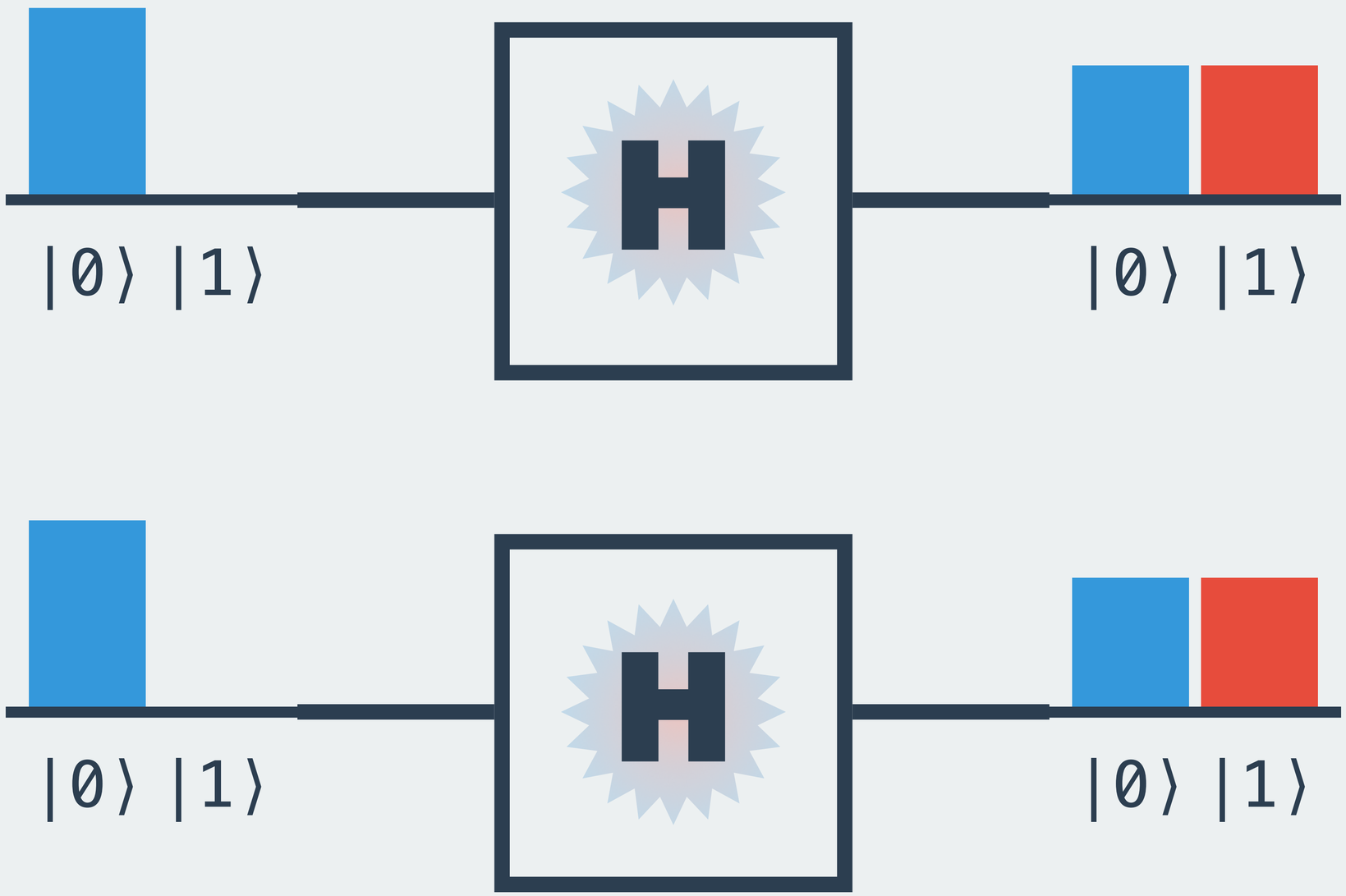

H
|0⟩ |1⟩
|0⟩ |1⟩

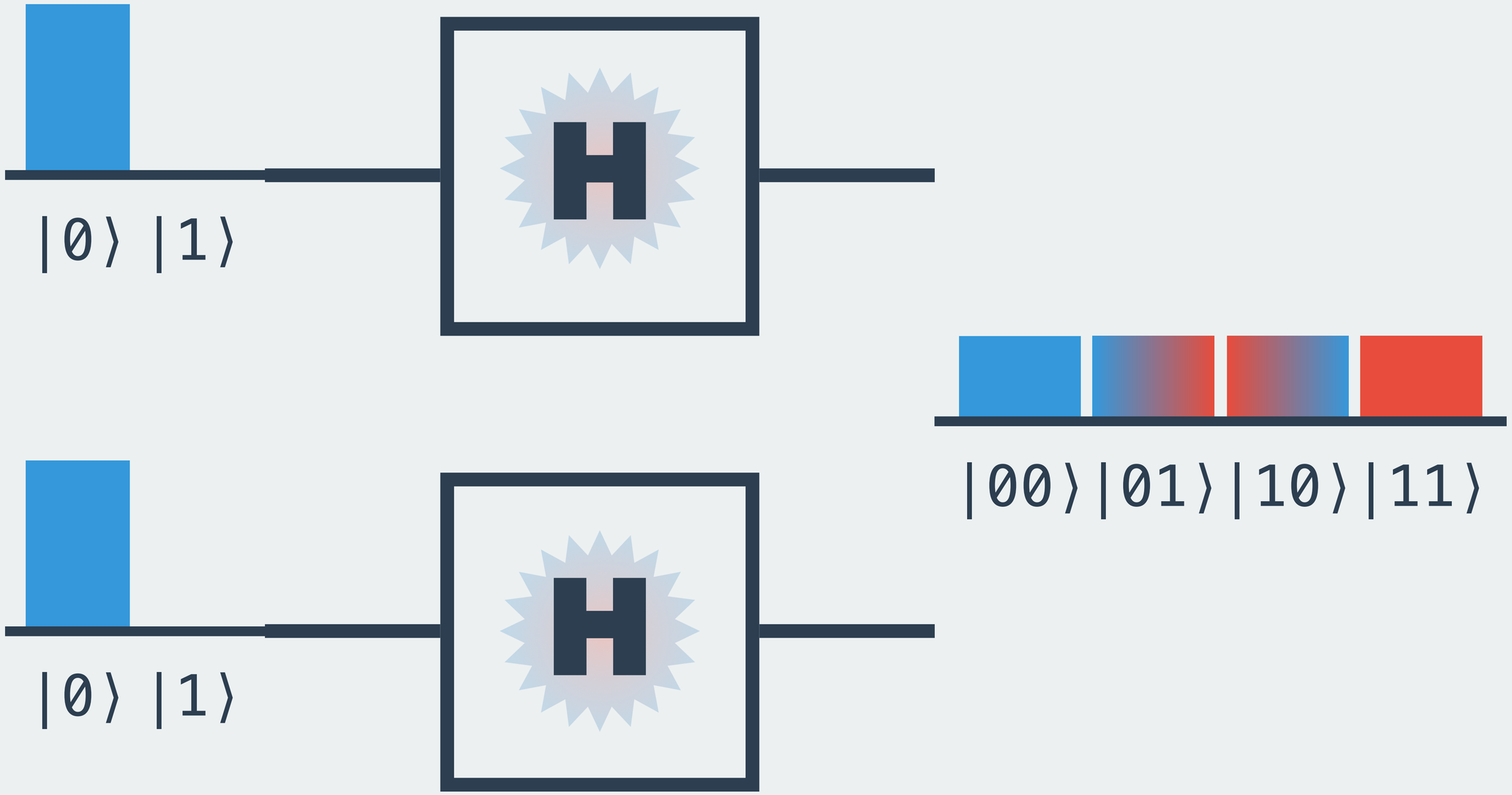

H
|+⟩
|0⟩ |1⟩
|0⟩ |1⟩

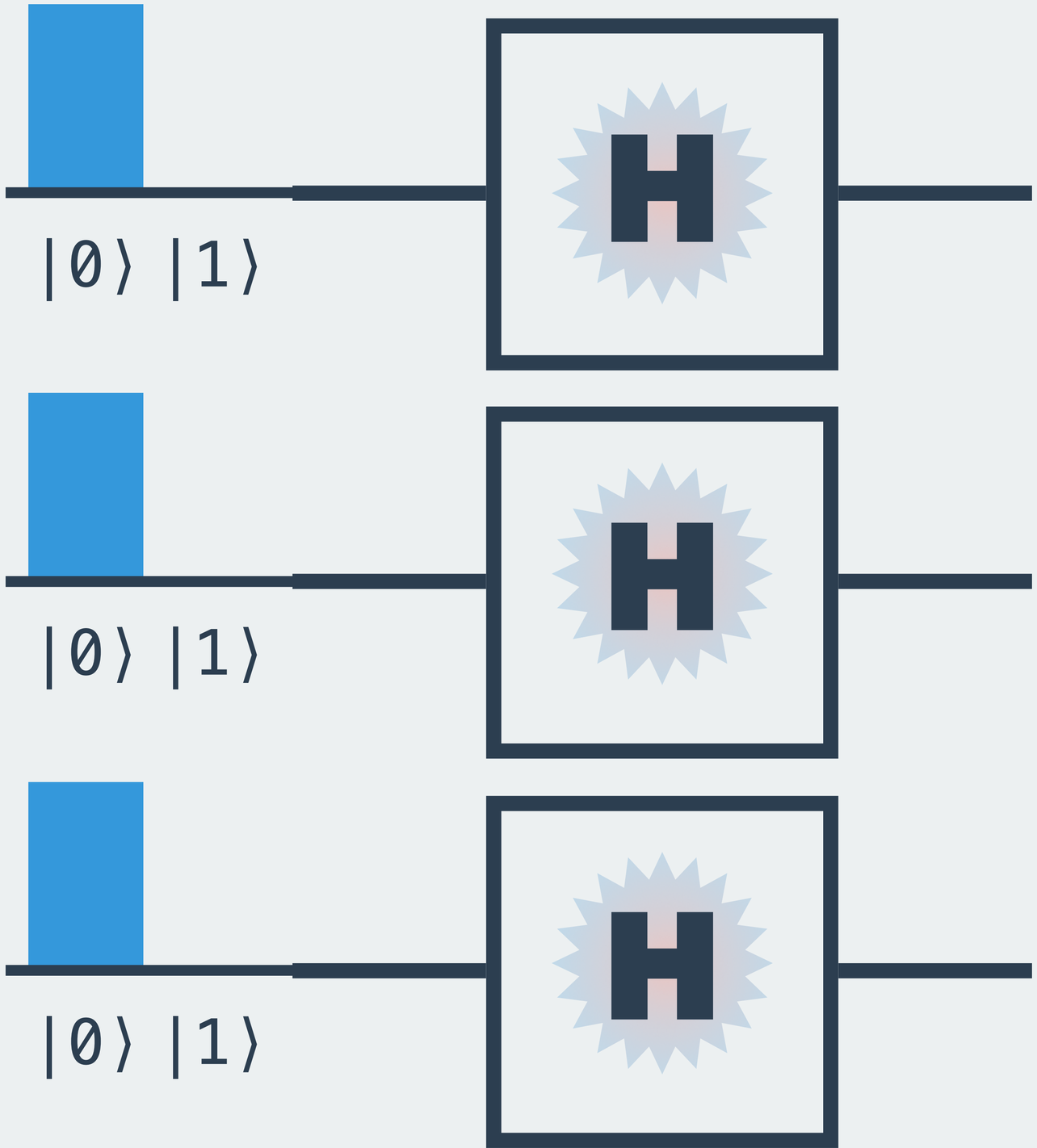

H
|0⟩ |1⟩
|0⟩ |1⟩

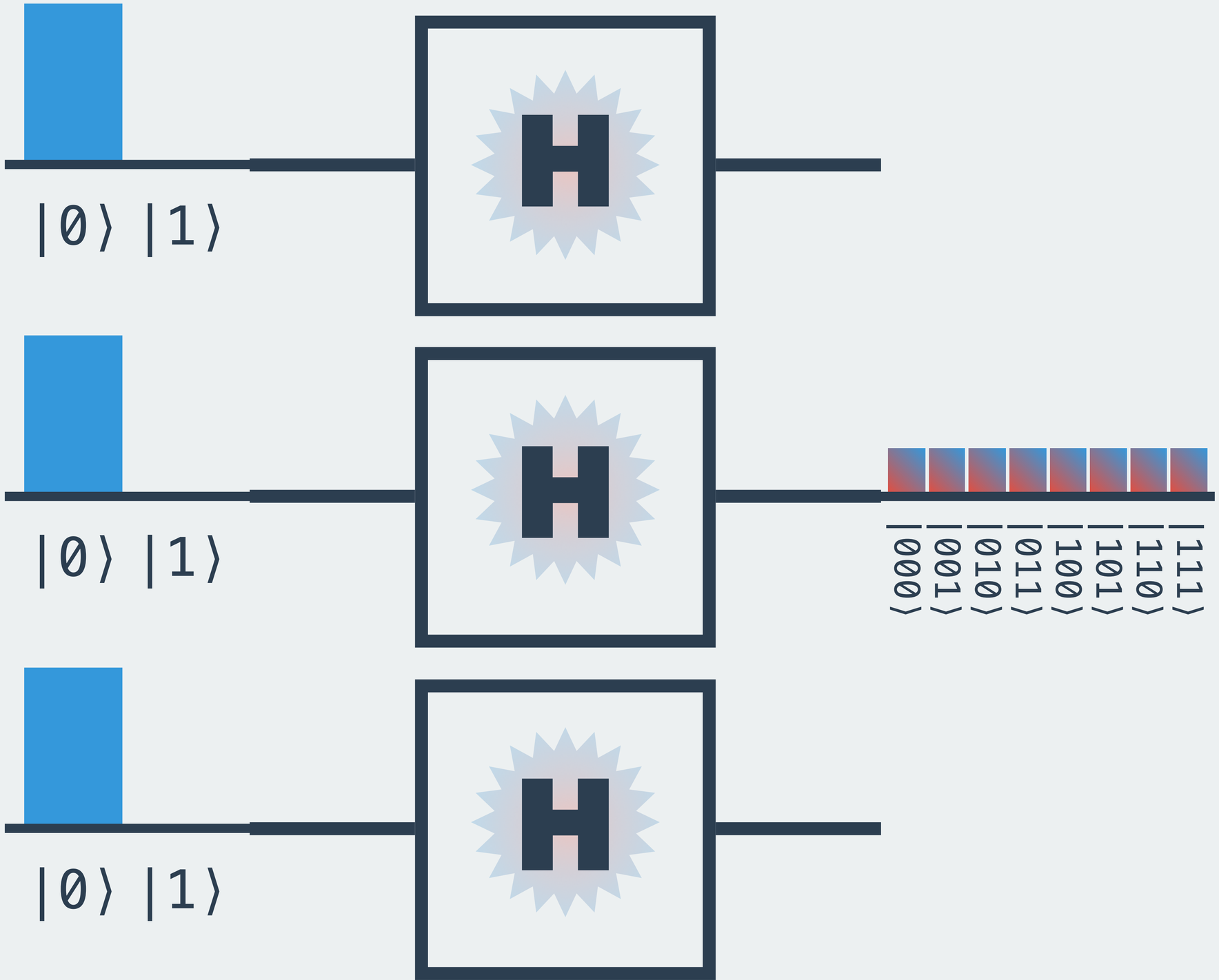

H
|−⟩
|0⟩ |1⟩
|0⟩ |1⟩

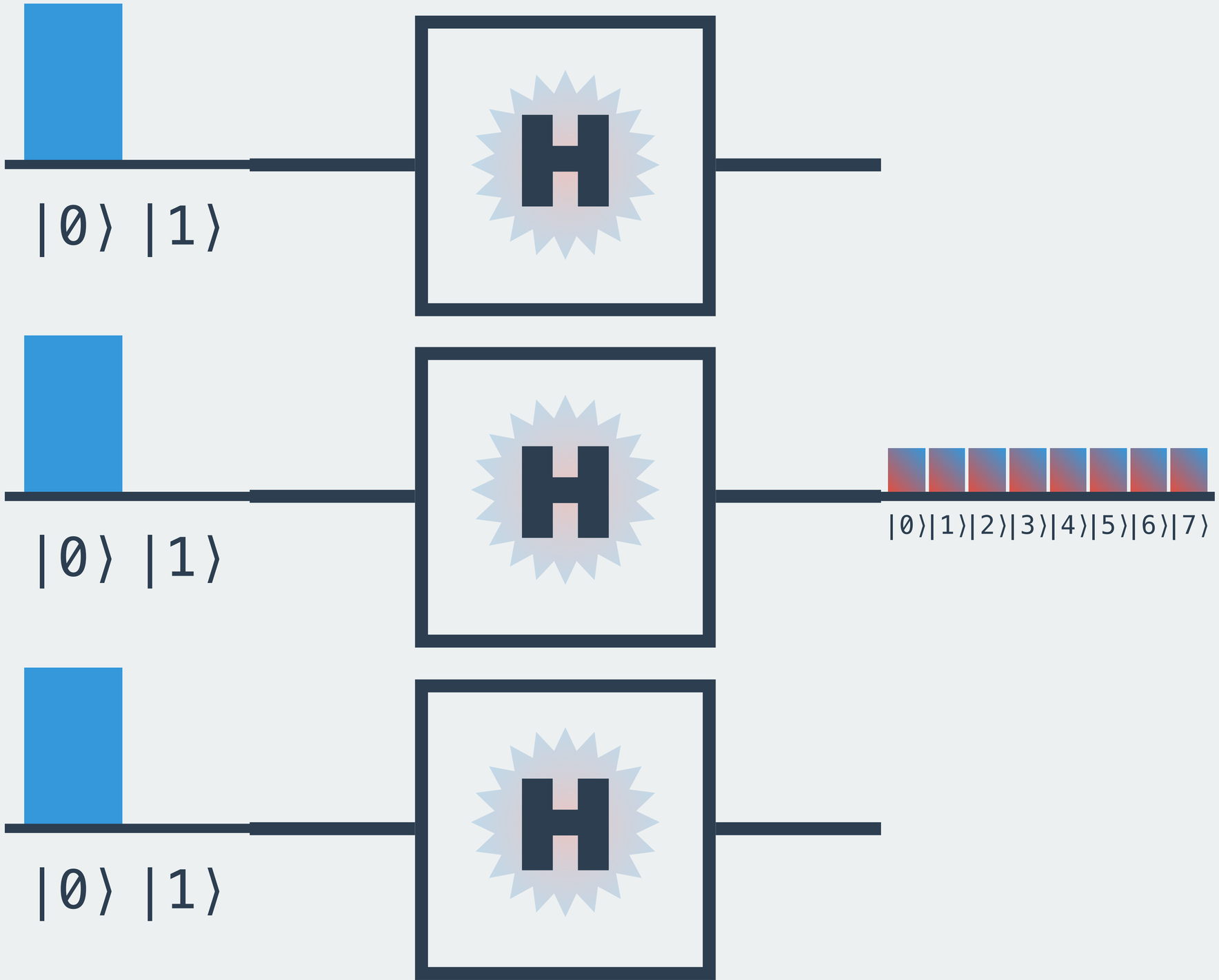
simulacija vrat

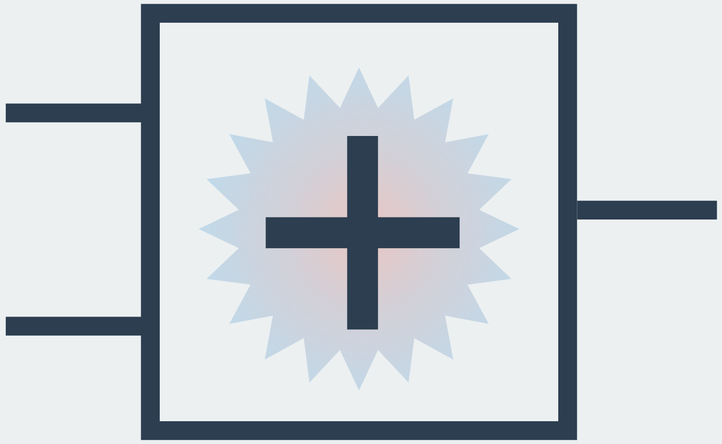

H
|0⟩ |1⟩
|0⟩ |1⟩
H
|0⟩ |1⟩
|0⟩ |1⟩

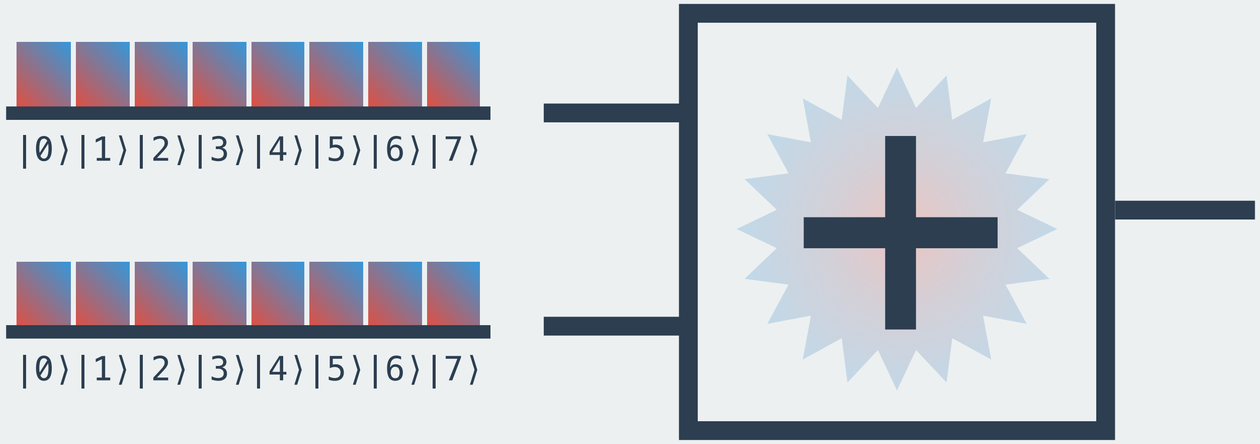

|0⟩ |1⟩
H
|0⟩ |1⟩
H
|00⟩|01⟩|10⟩|11⟩

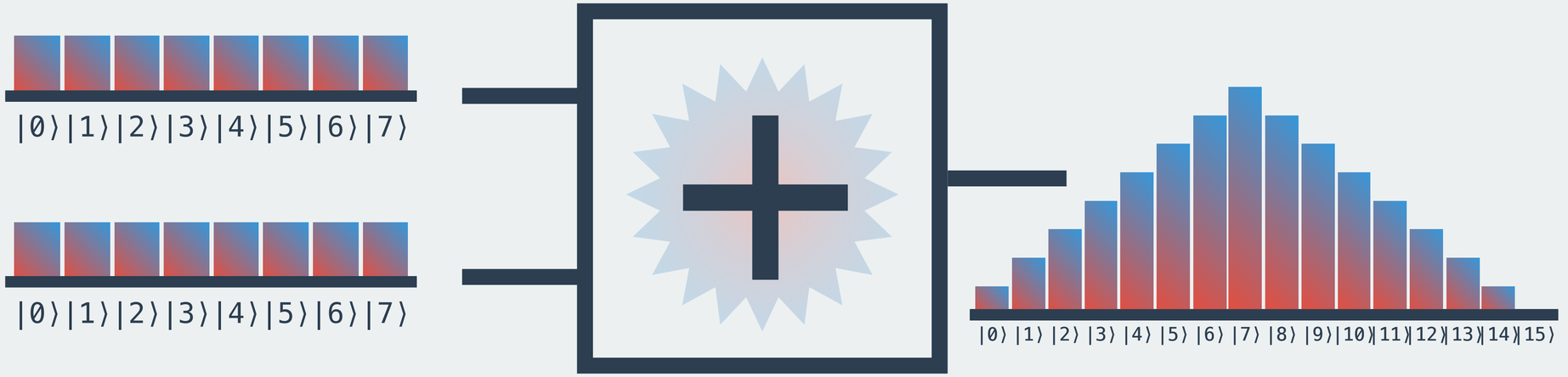

|0⟩ |1⟩
H
|0⟩ |1⟩
H
|0⟩ |1⟩
H

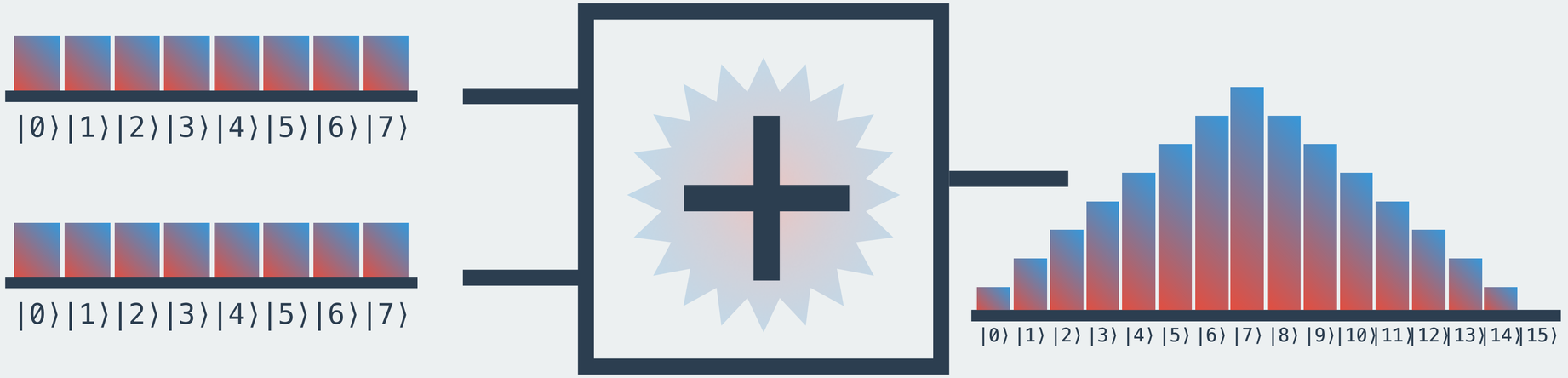

|0⟩ |1⟩
H
|0⟩ |1⟩
H
|0⟩ |1⟩
H
|000⟩
|001⟩
|010⟩
|011⟩
|100⟩
|101⟩
|110⟩
|111⟩


|0⟩ |1⟩
|0⟩ |1⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩ |1⟩

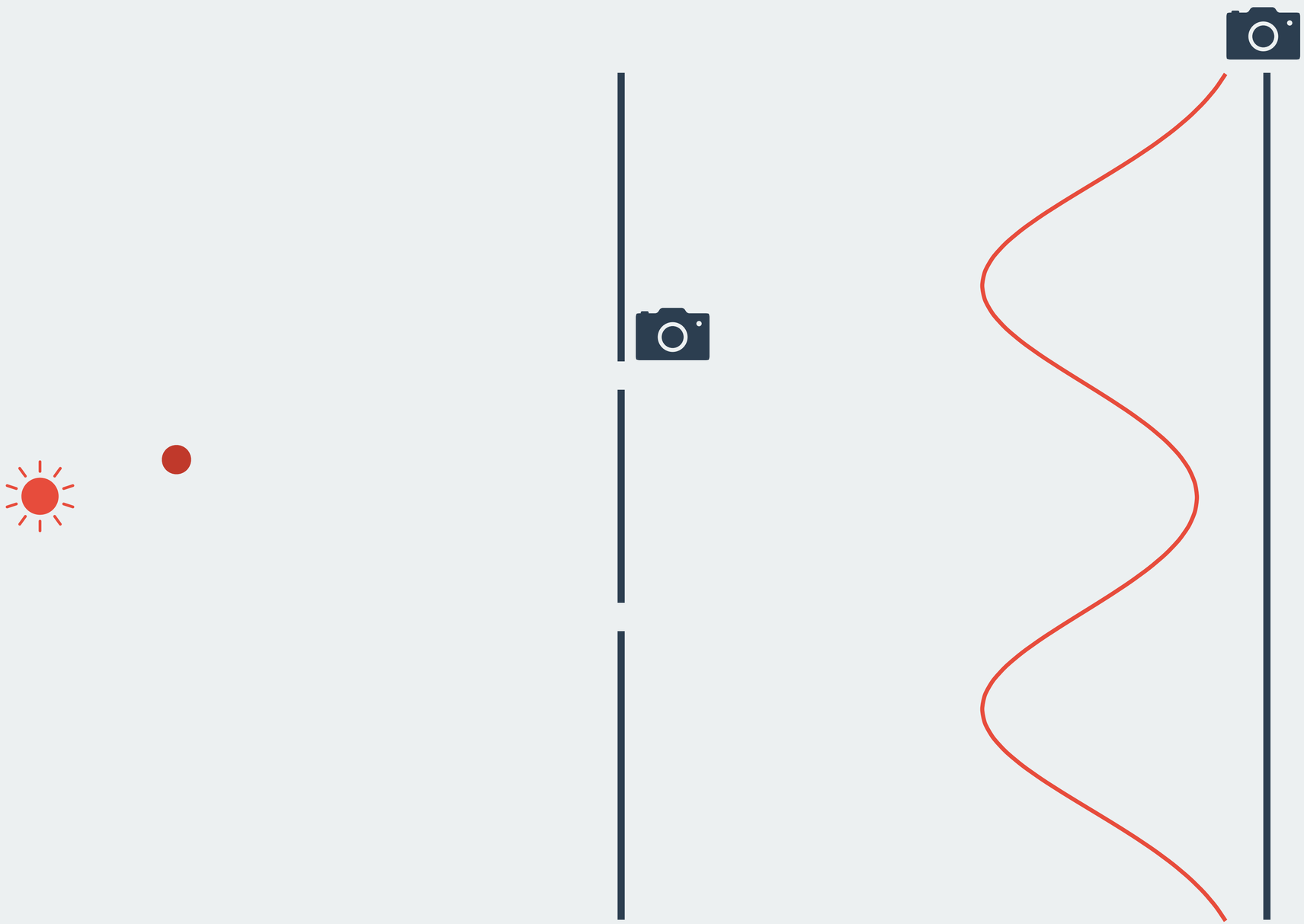


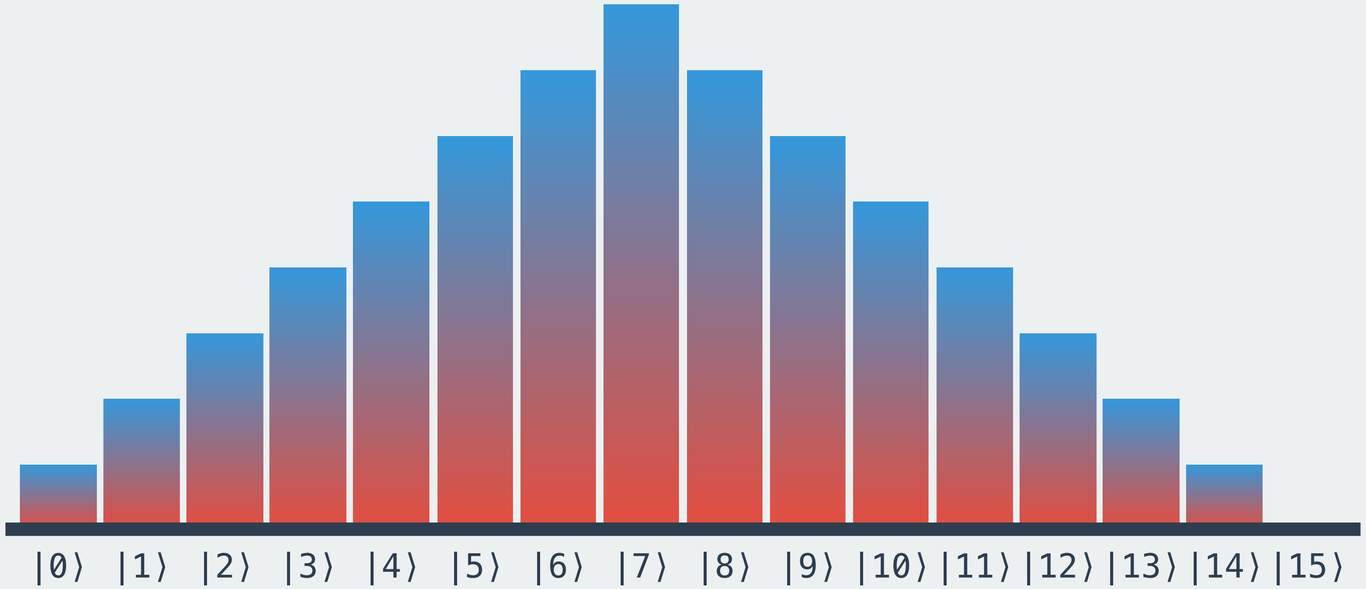

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

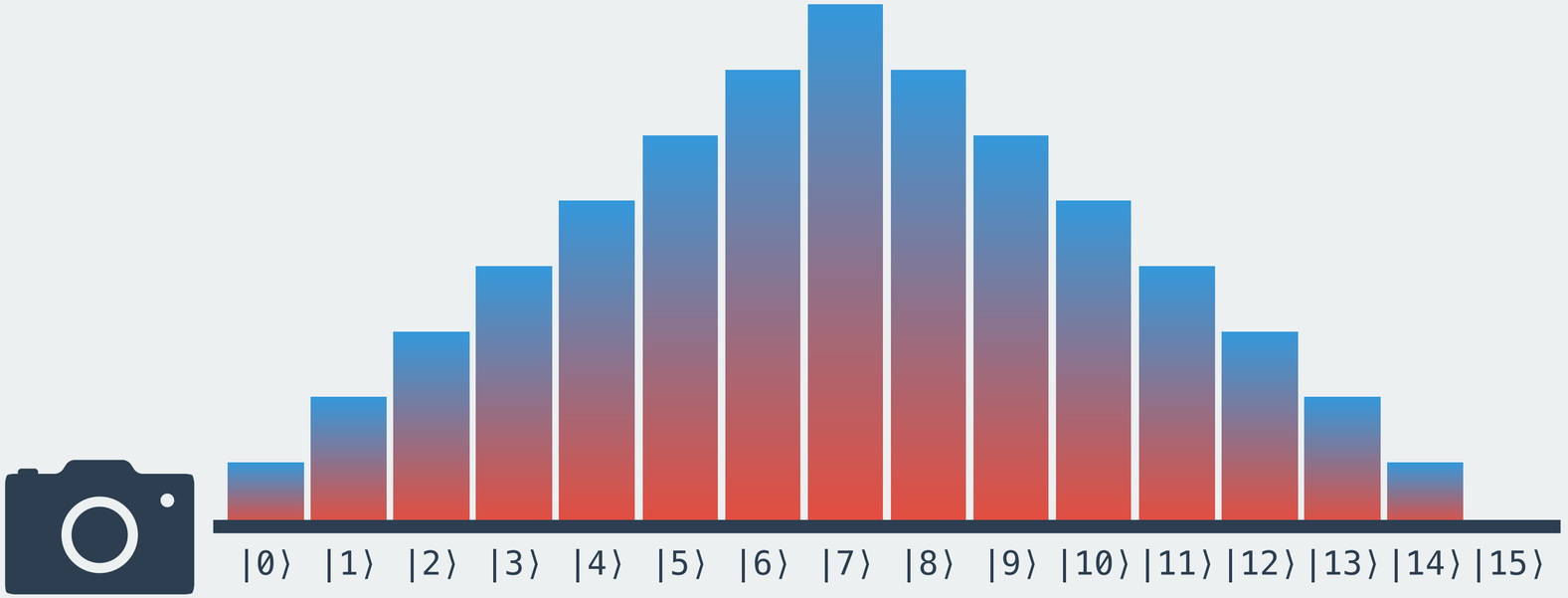

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩

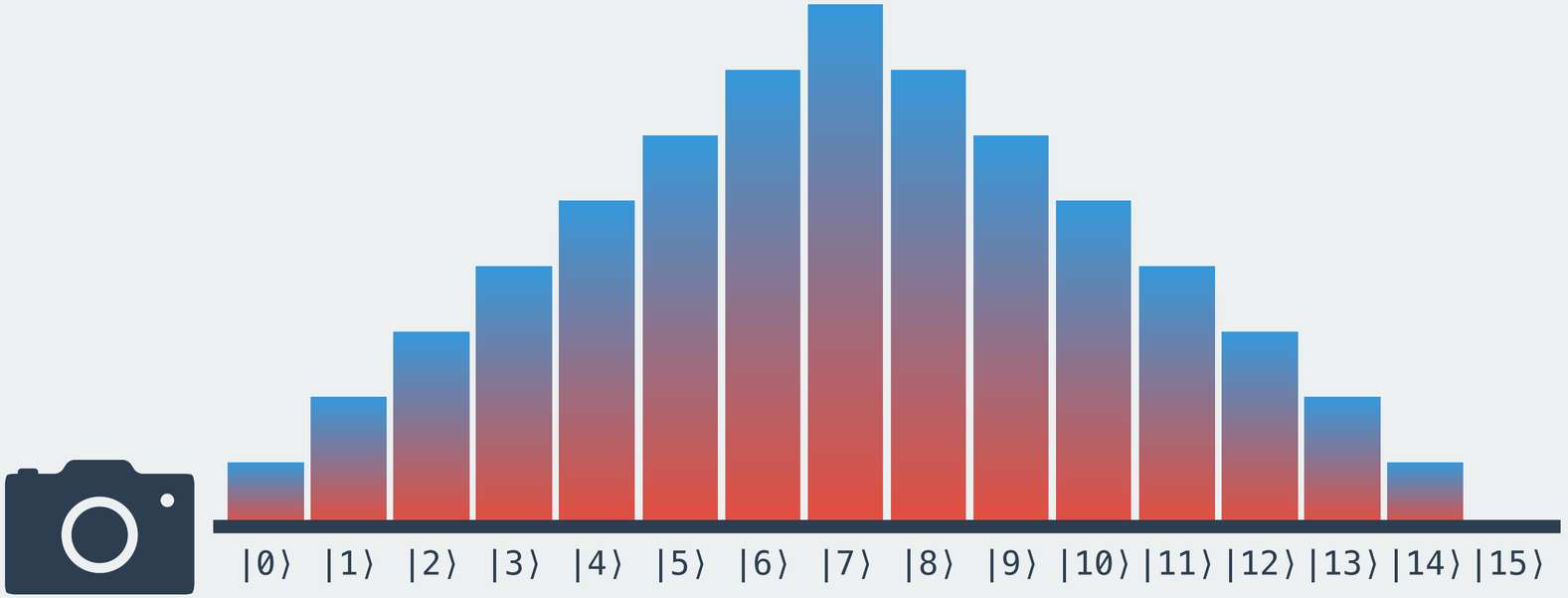

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩|10⟩|11⟩|12⟩|13⟩|14⟩|15⟩

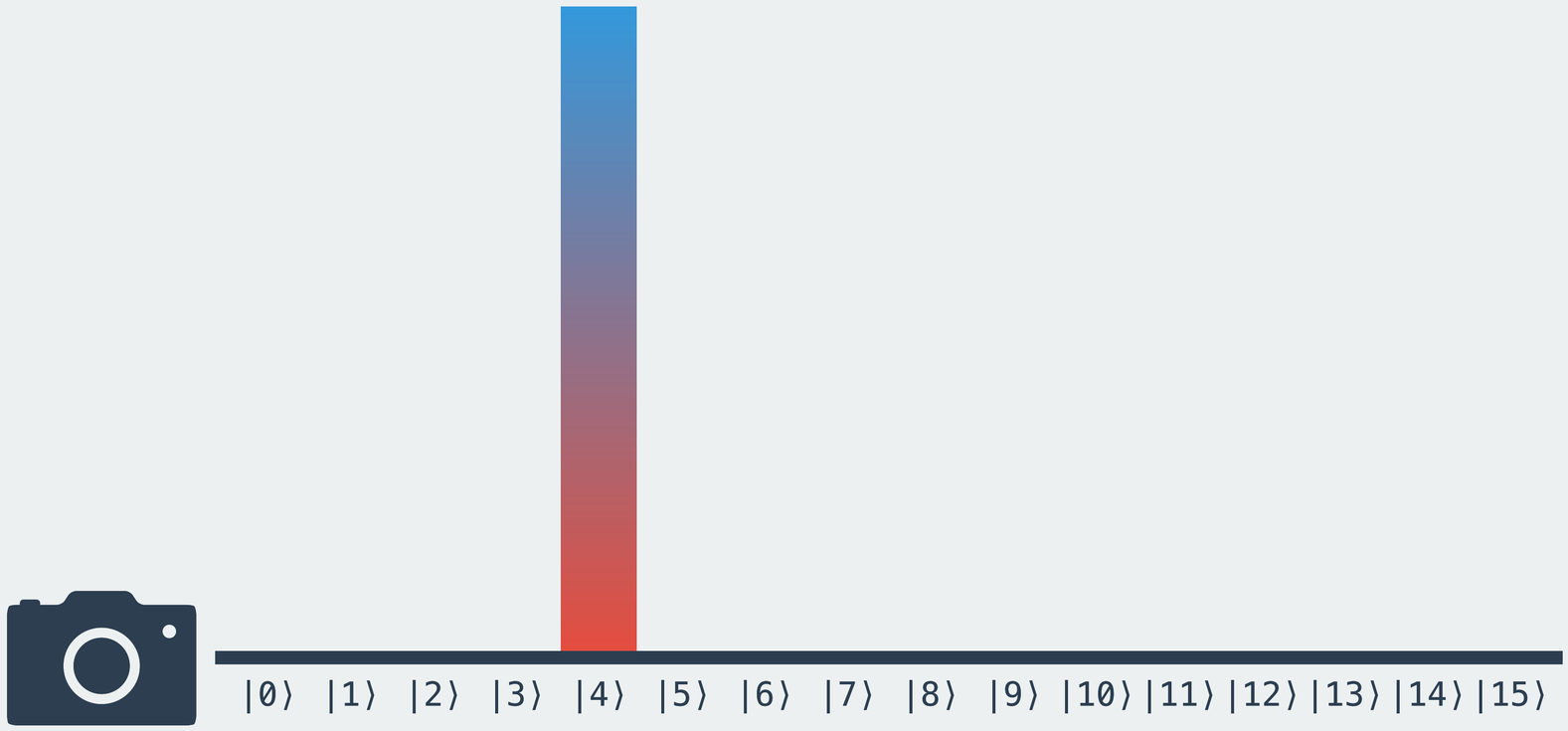
TODA...



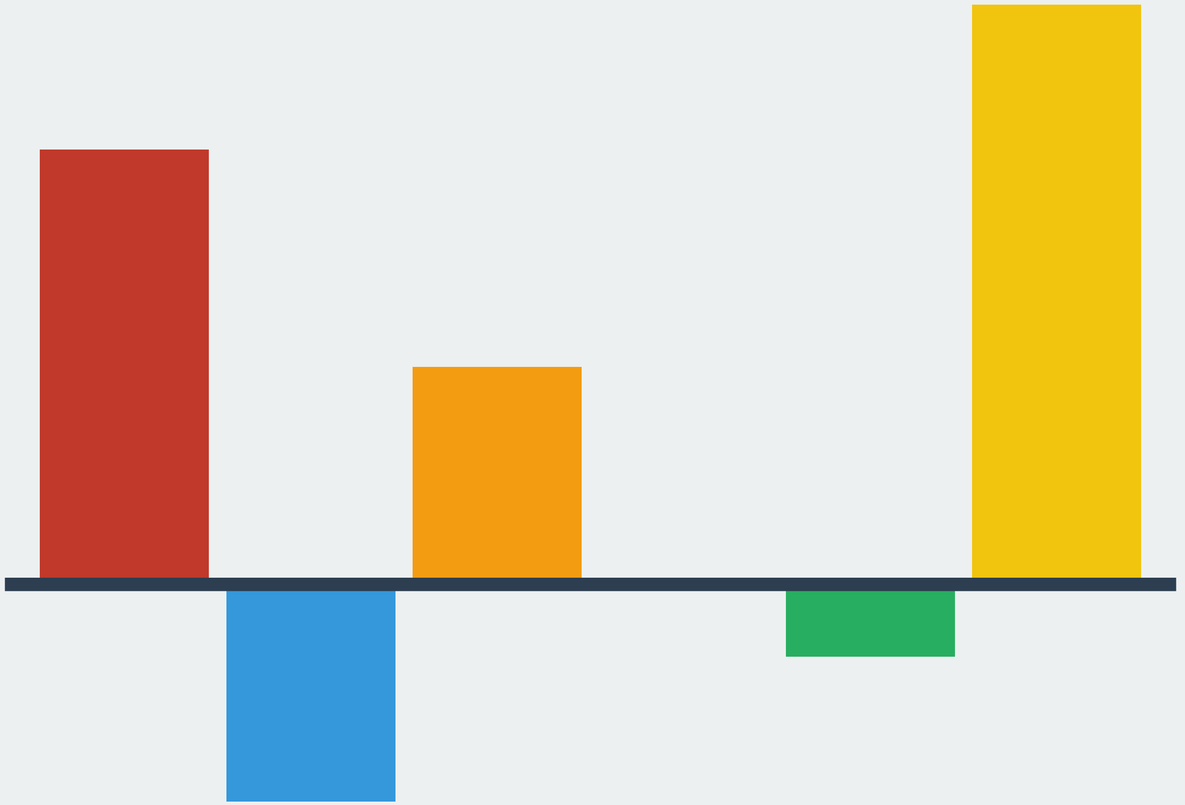

|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩

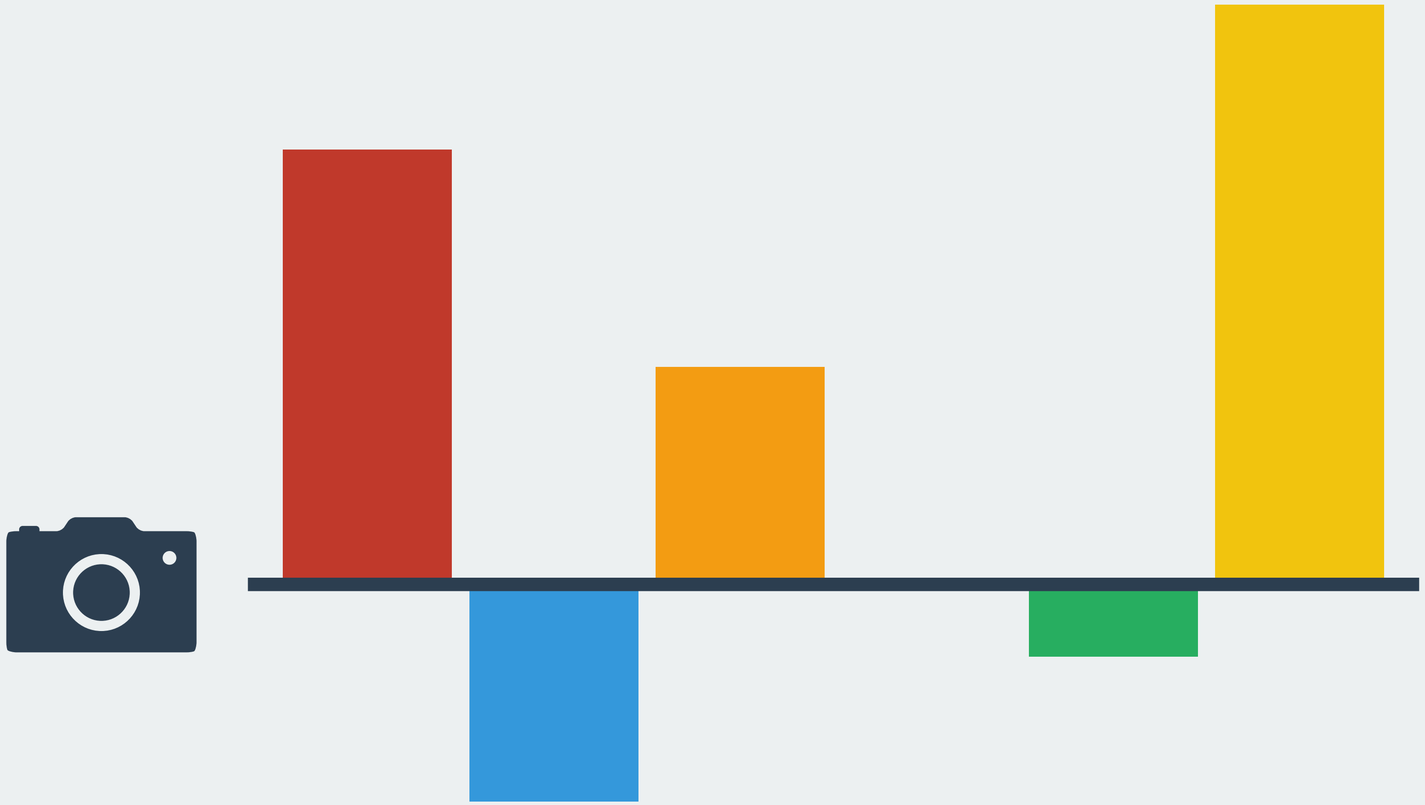

|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩

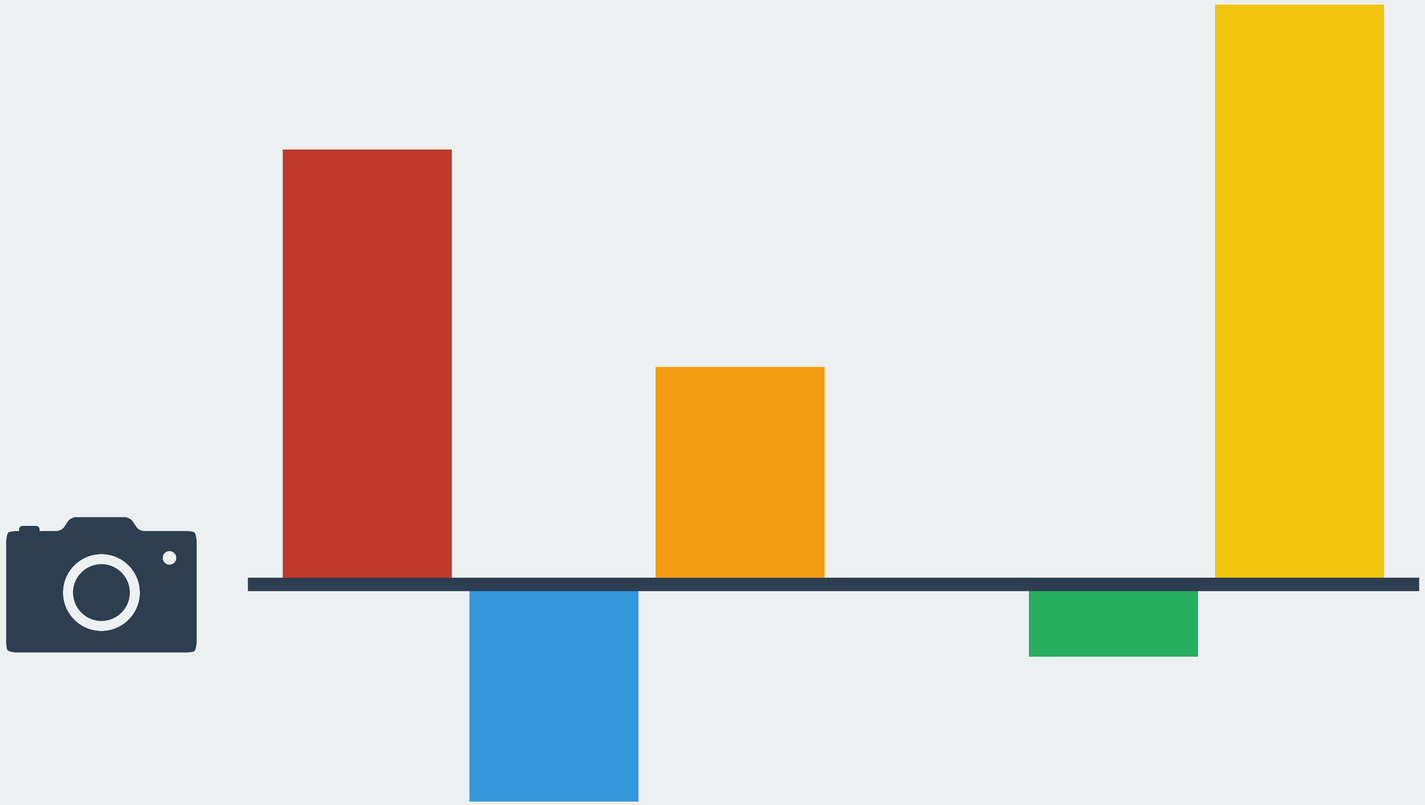

|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩


|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩


&$!#%



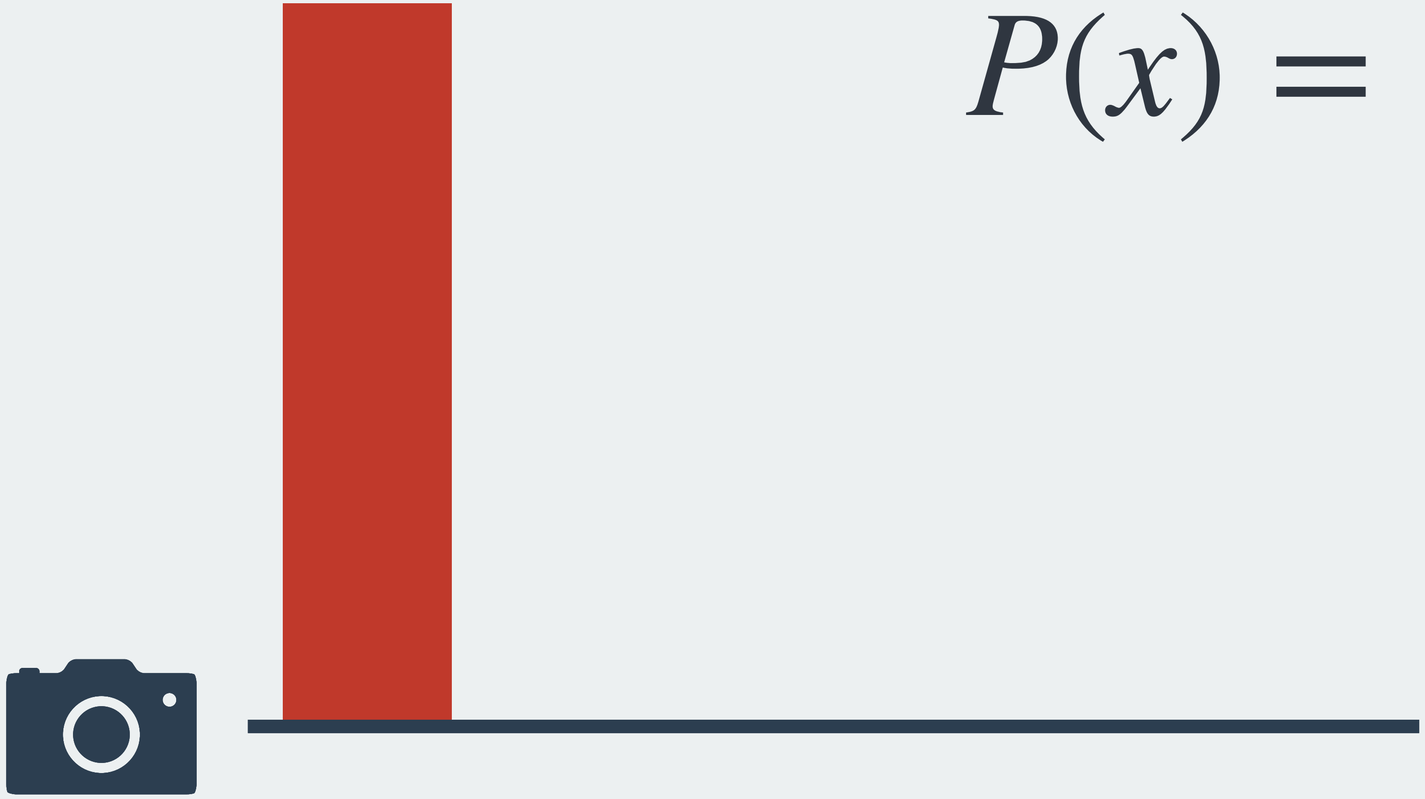


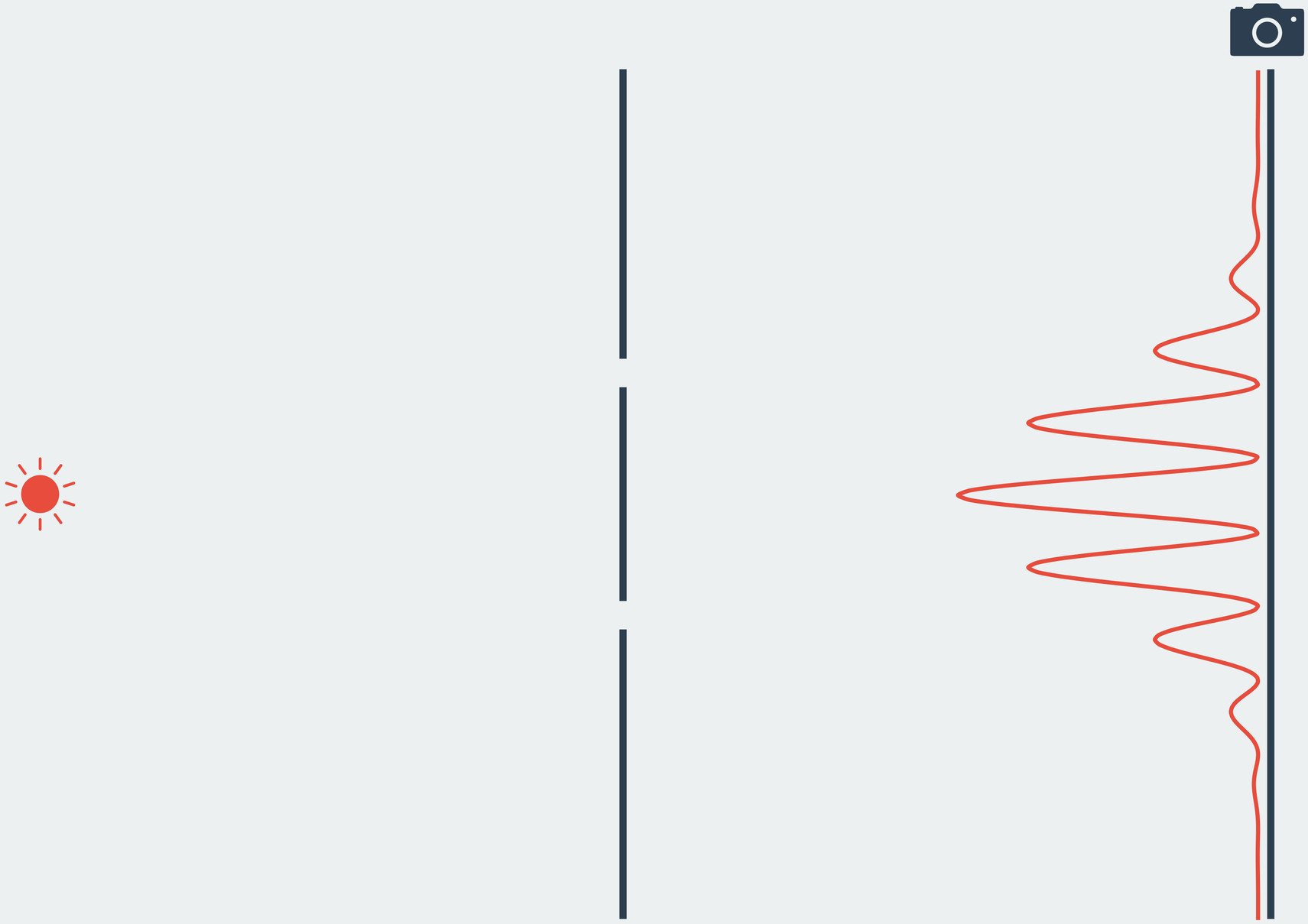


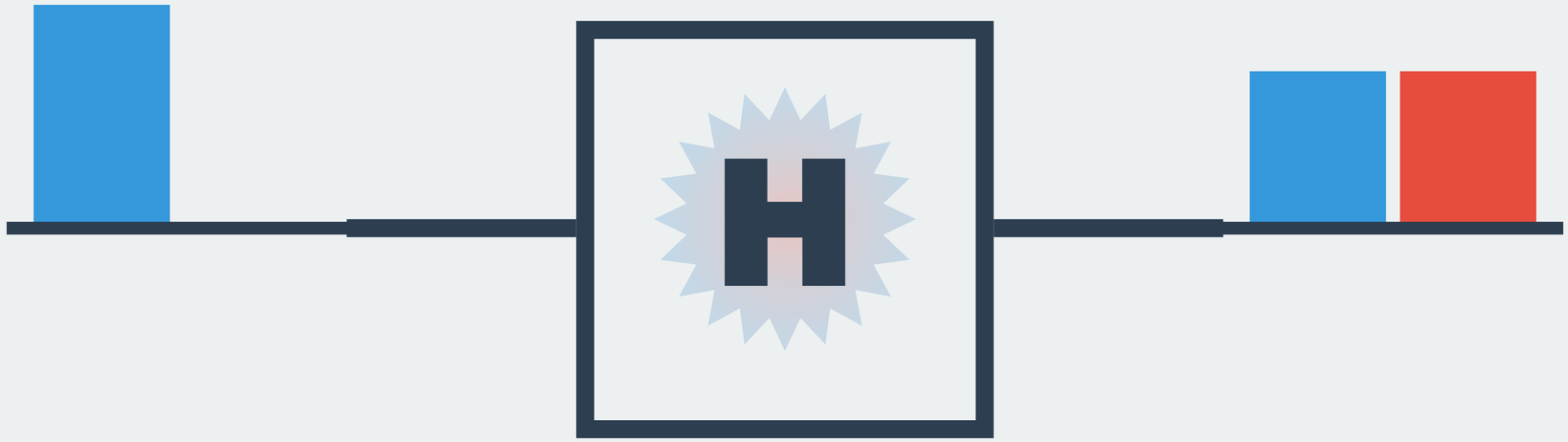
$$|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$$

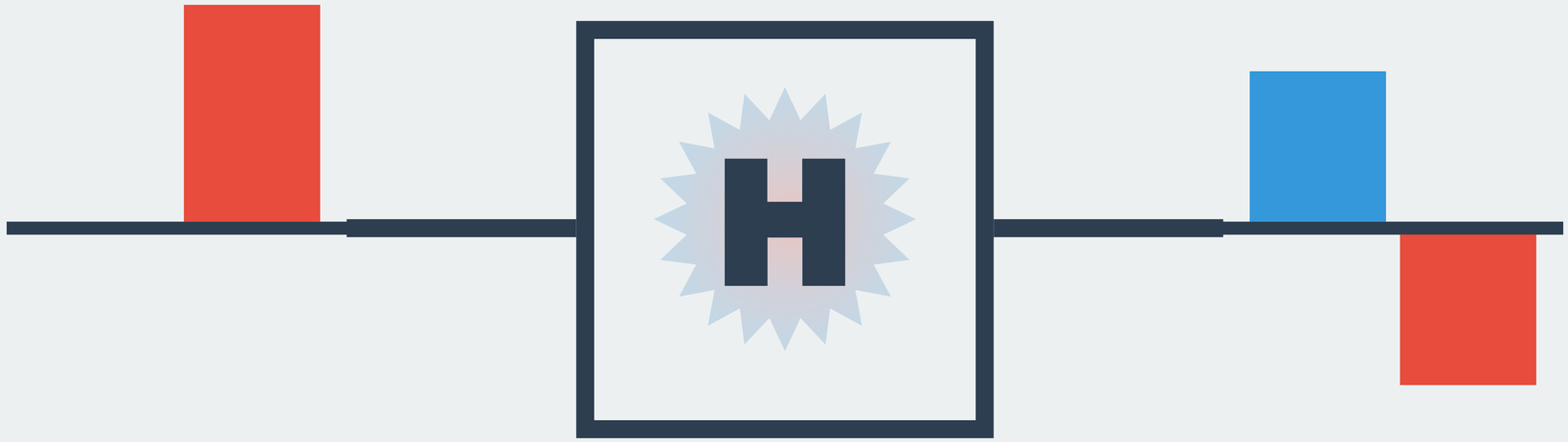
$$|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$$

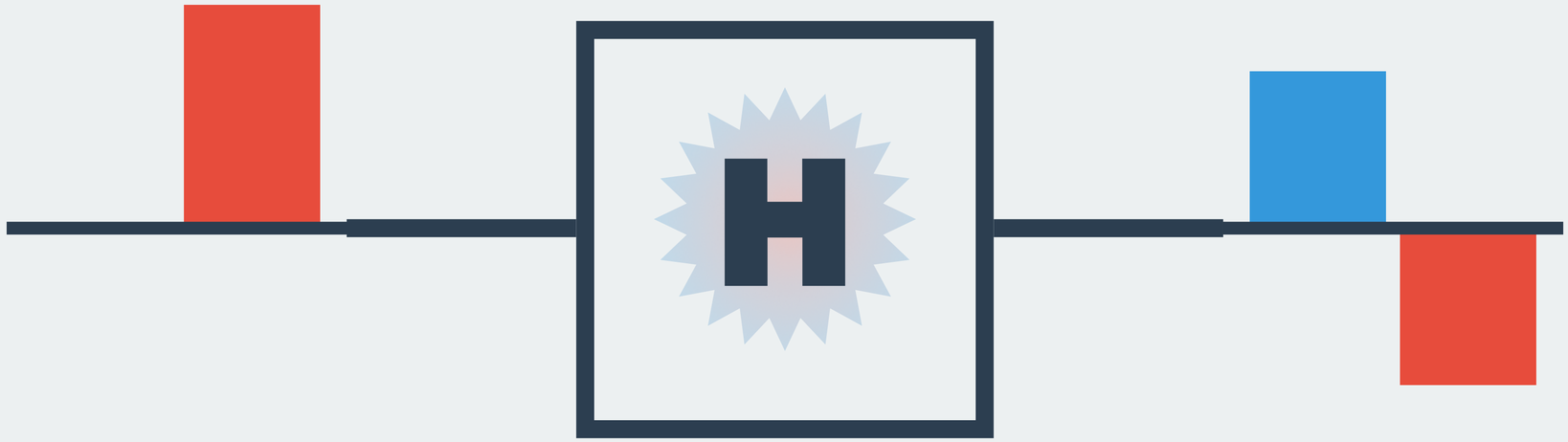
$$P(x) = |\alpha_x|^2$$

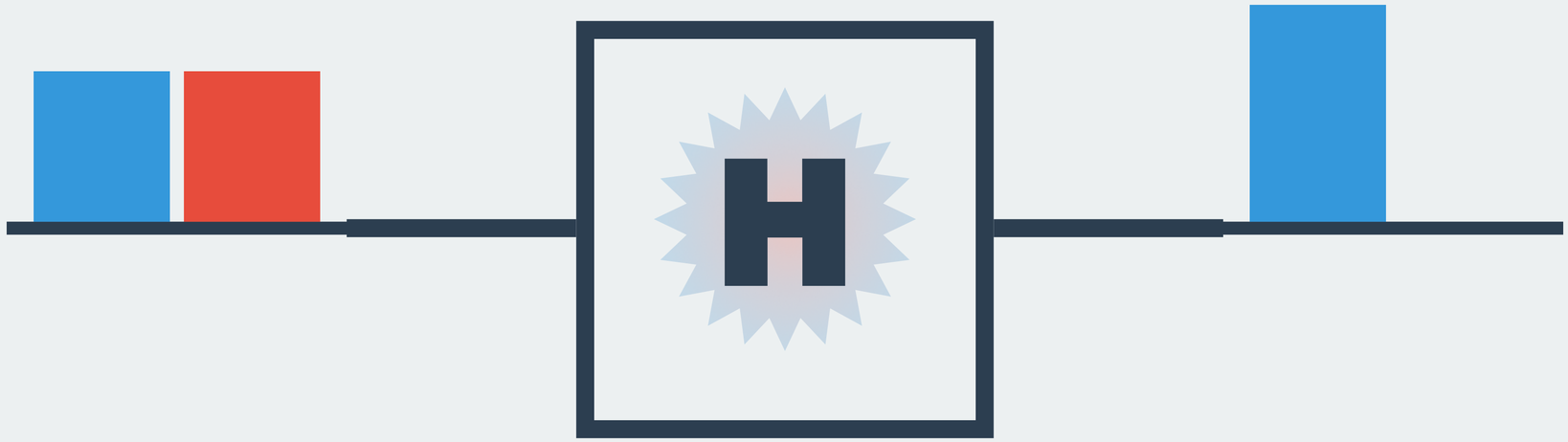


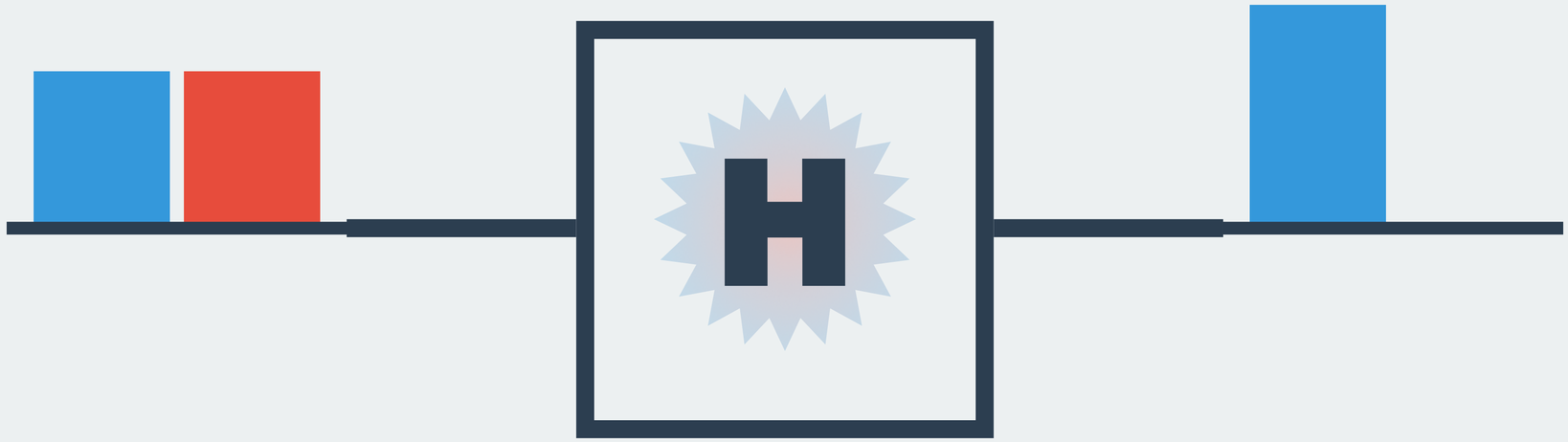


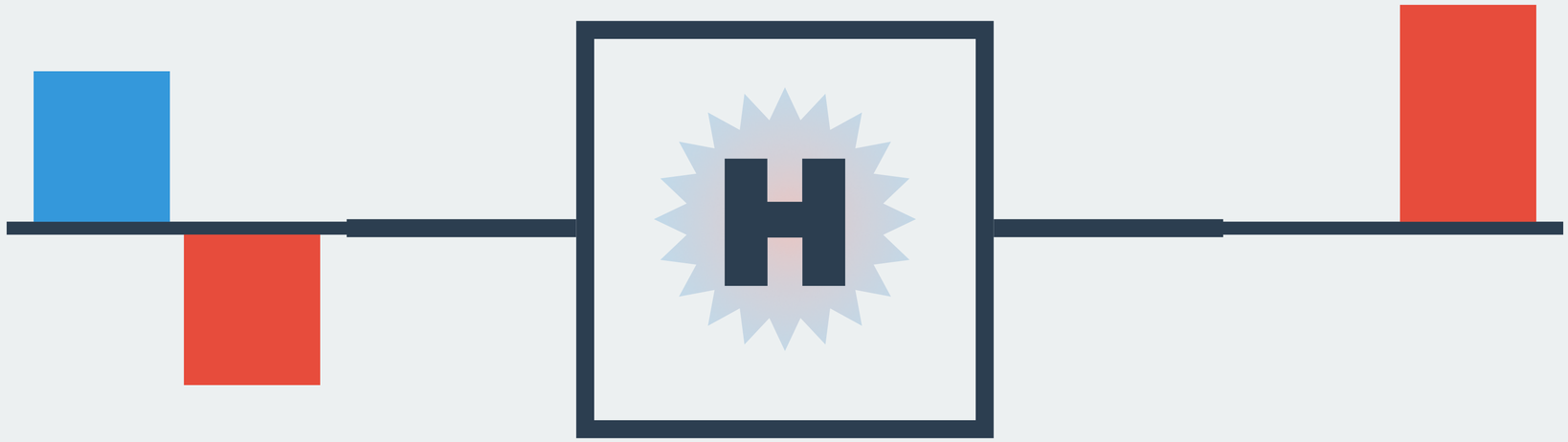

H
|0⟩ |1⟩
|0⟩ |1⟩


H
|0⟩ |1⟩
|0⟩ |1⟩


H
|0⟩ |1⟩
|0⟩ |1⟩


H
|0⟩ |1⟩
|0⟩ |1⟩


H
|0⟩ |1⟩
|0⟩ |1⟩

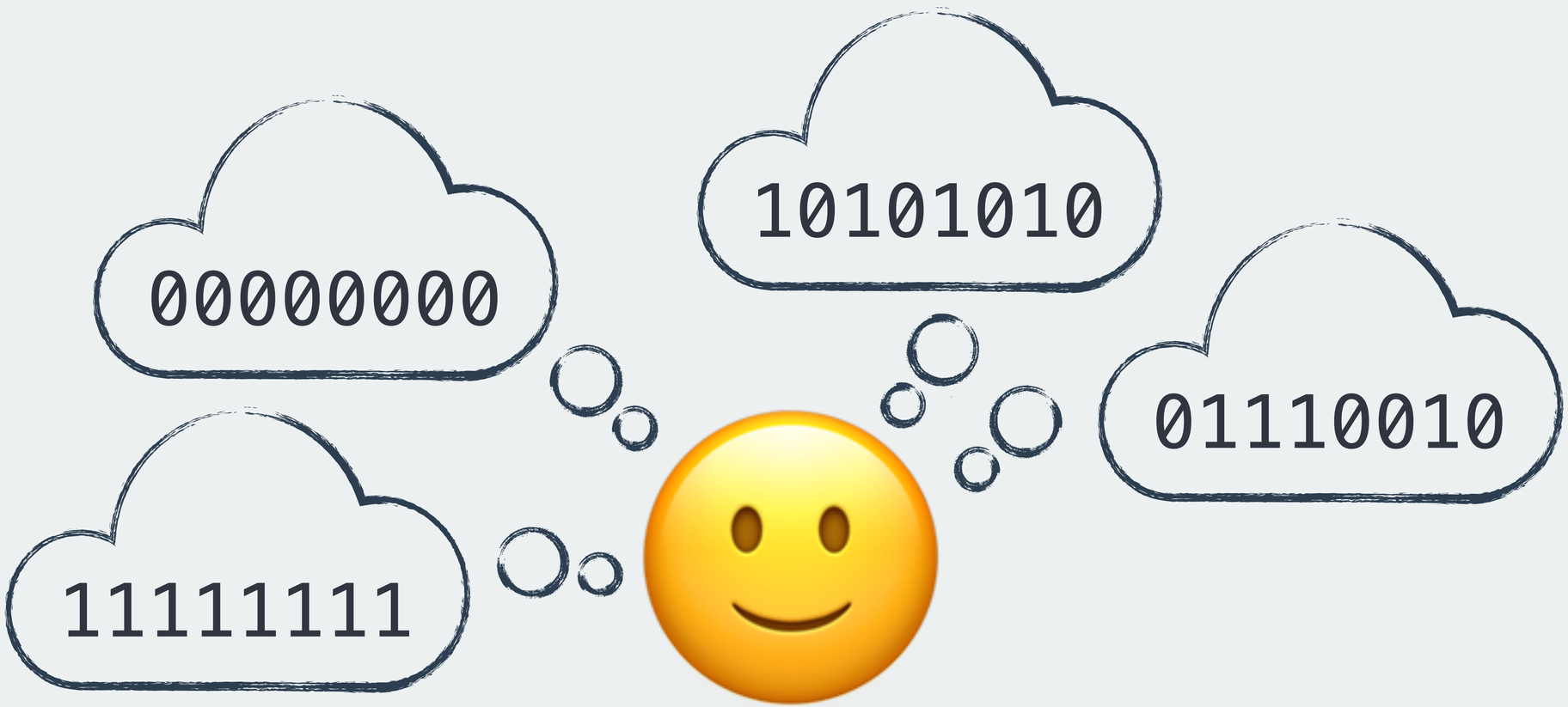

H
|0⟩ |1⟩
|0⟩ |1⟩

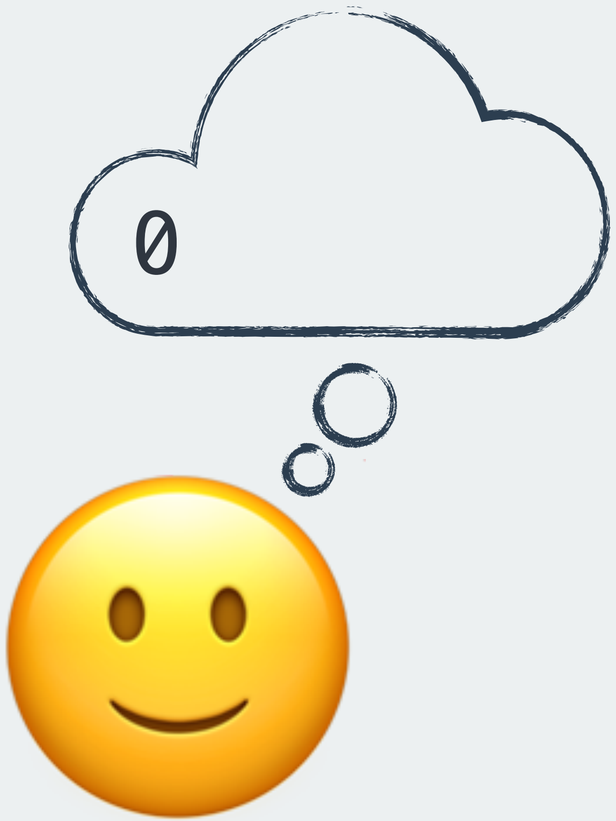
KVANTNO RAČUNALNIŠTVO

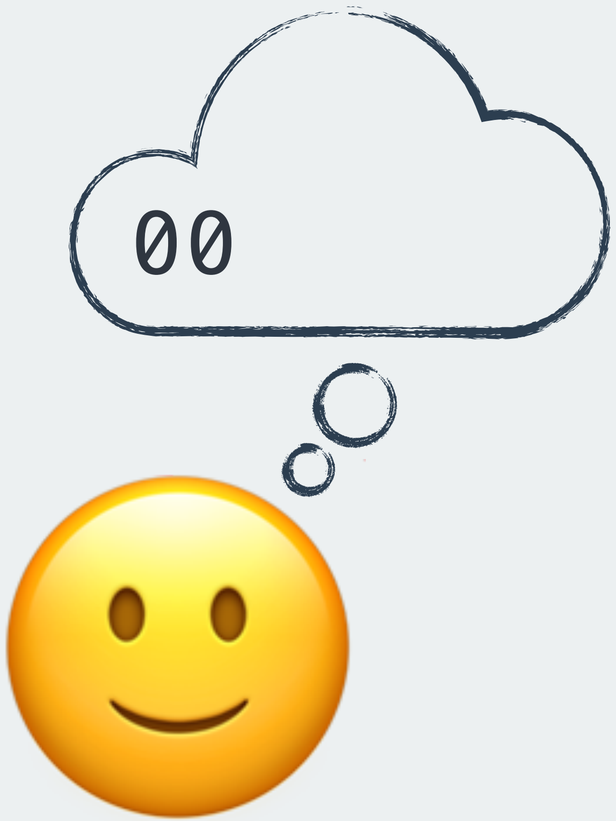
DEUTSCHEV ALGORITEM

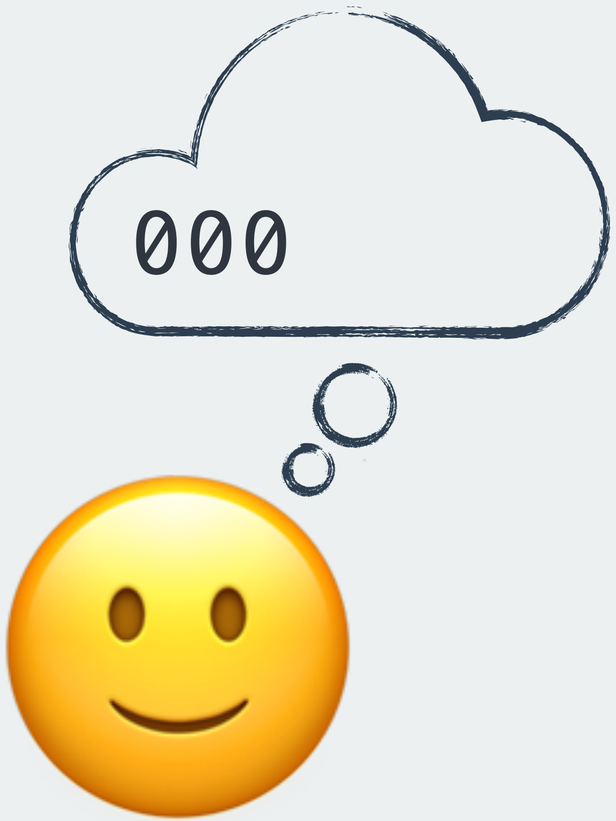
Richard Jozsa
1953-

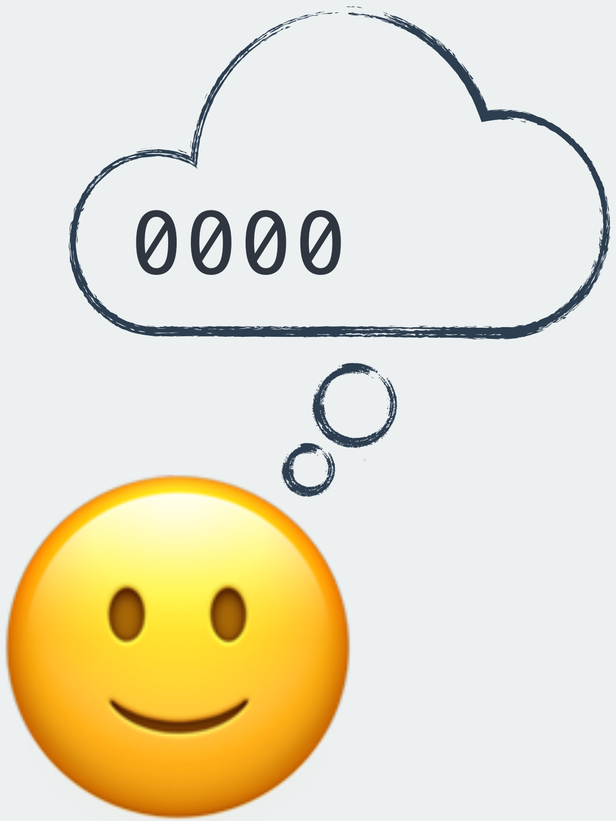
David Deutsch
1953-

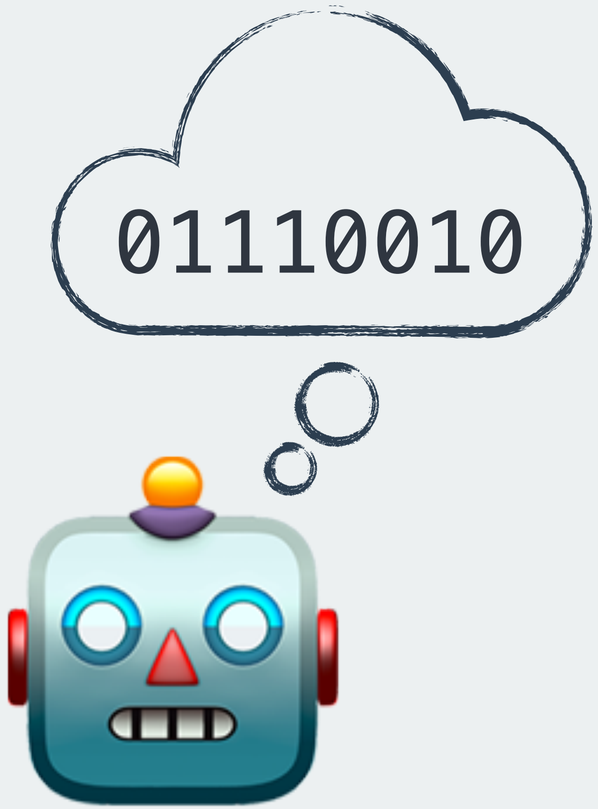

00000000
10101010
01110010
11111111

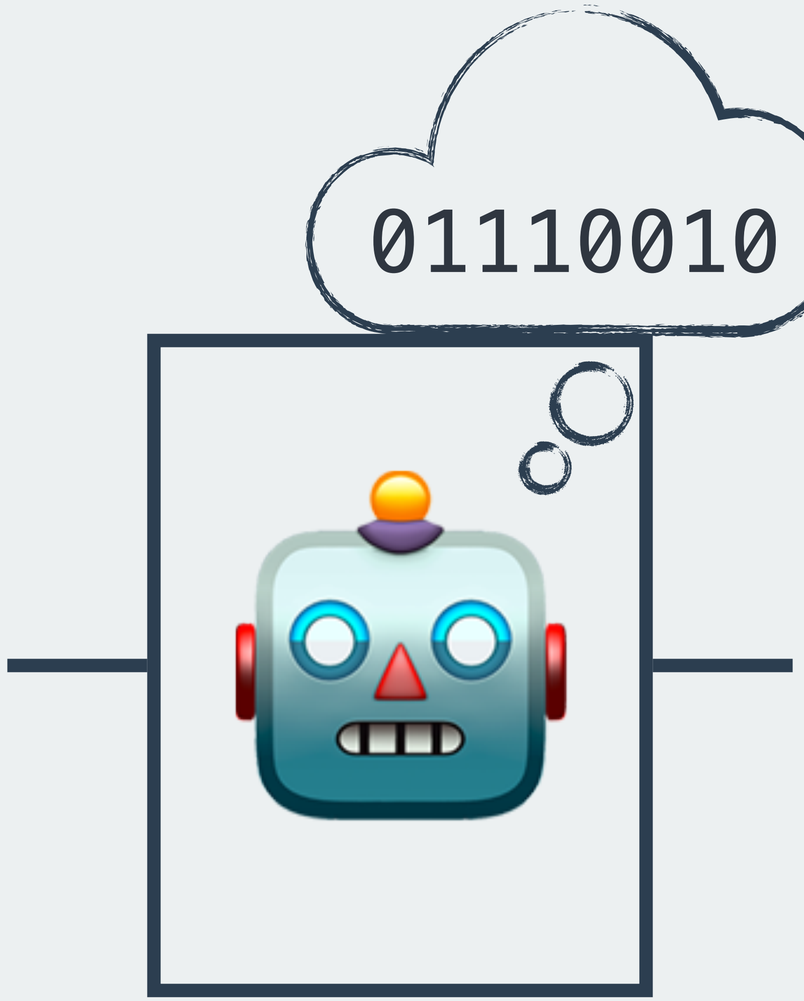

0

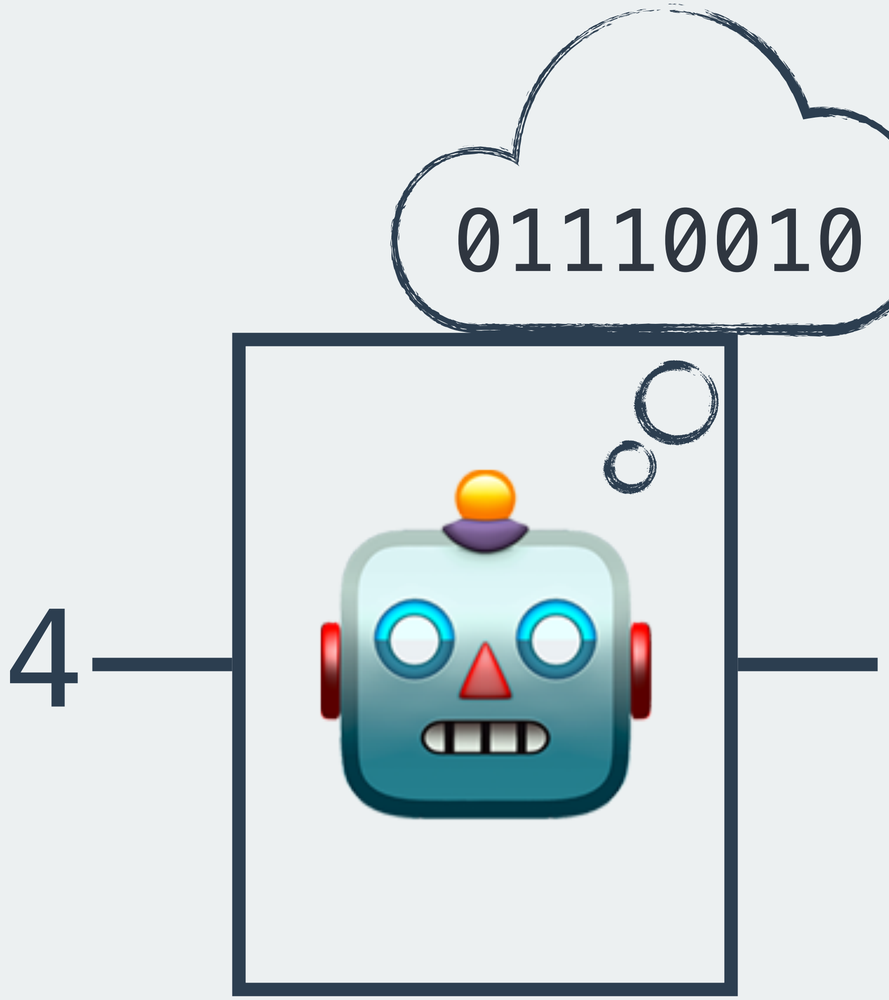

00

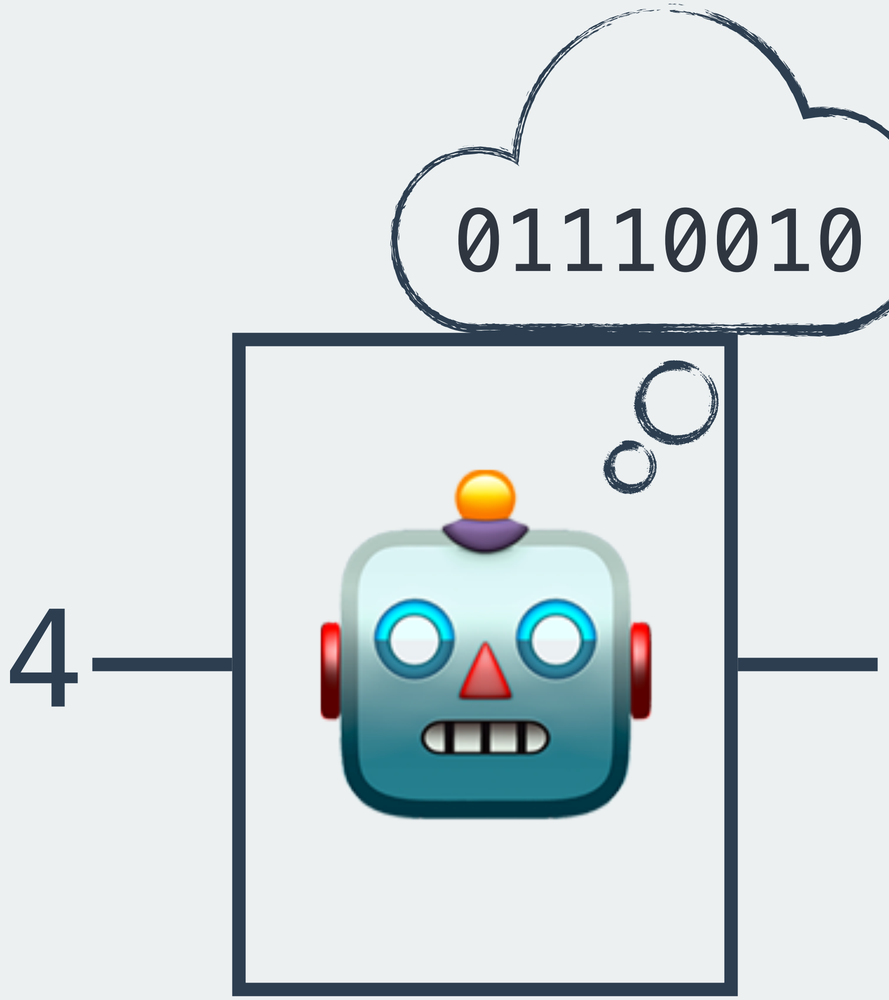

000

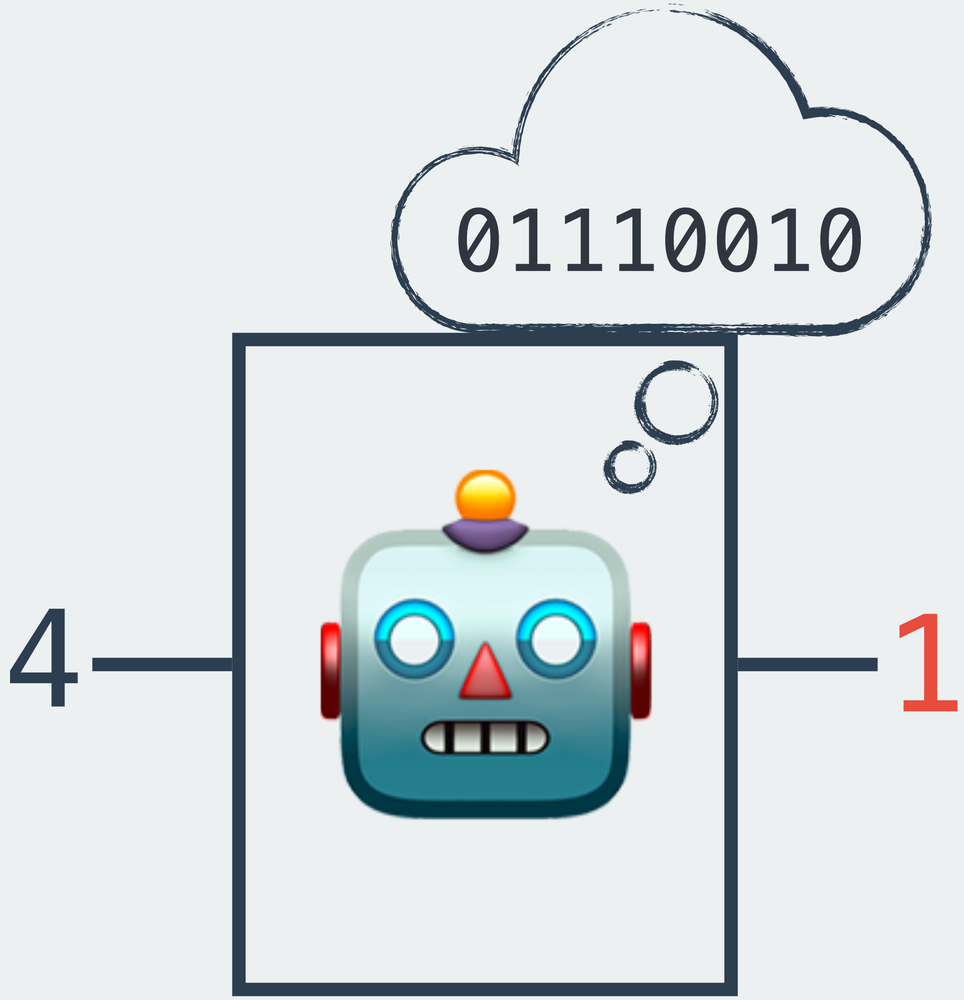

0000

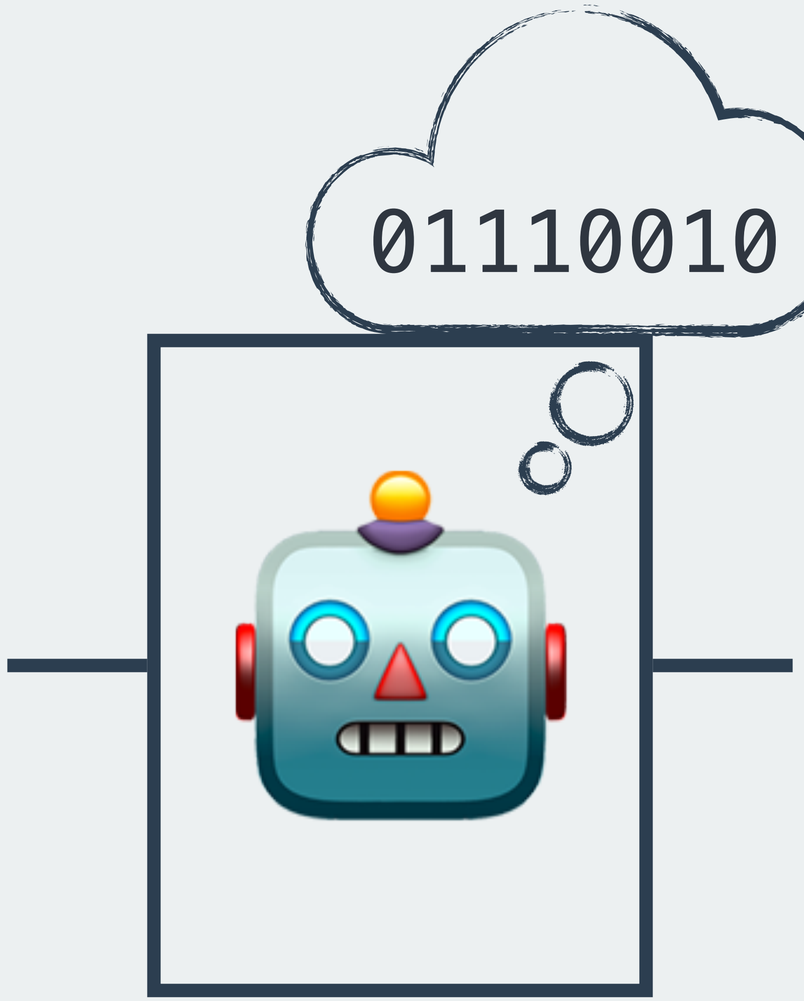

01110010

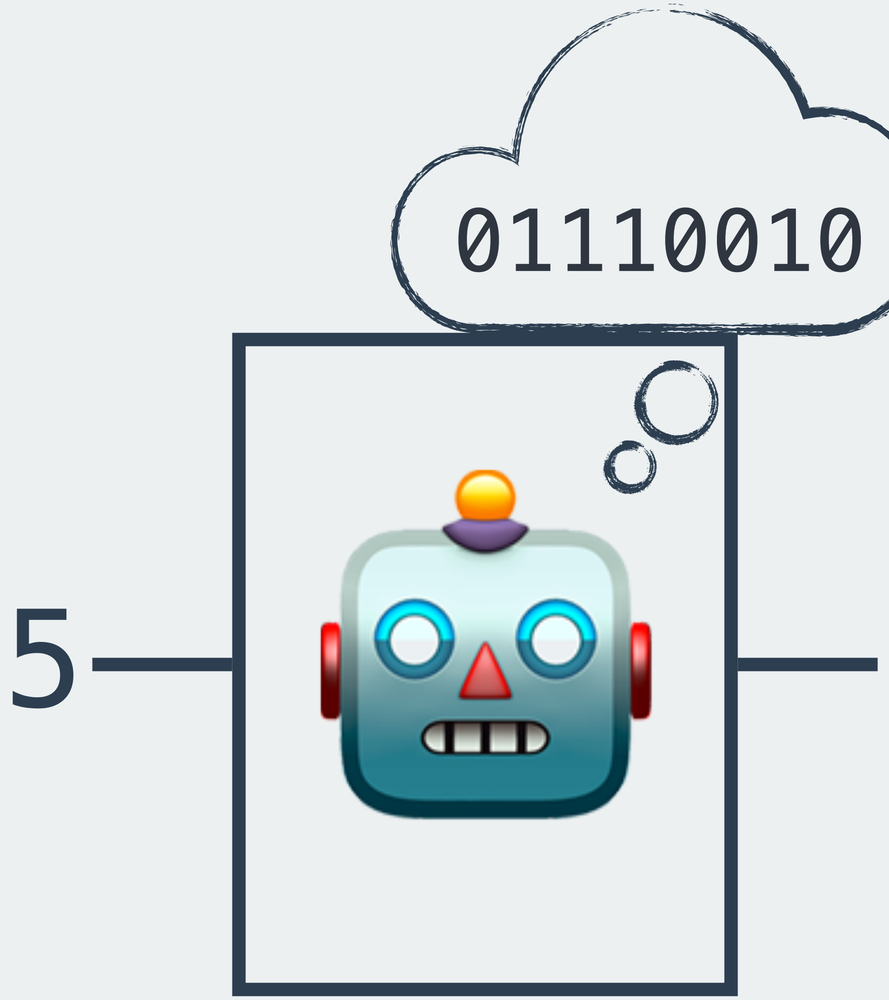

01110010

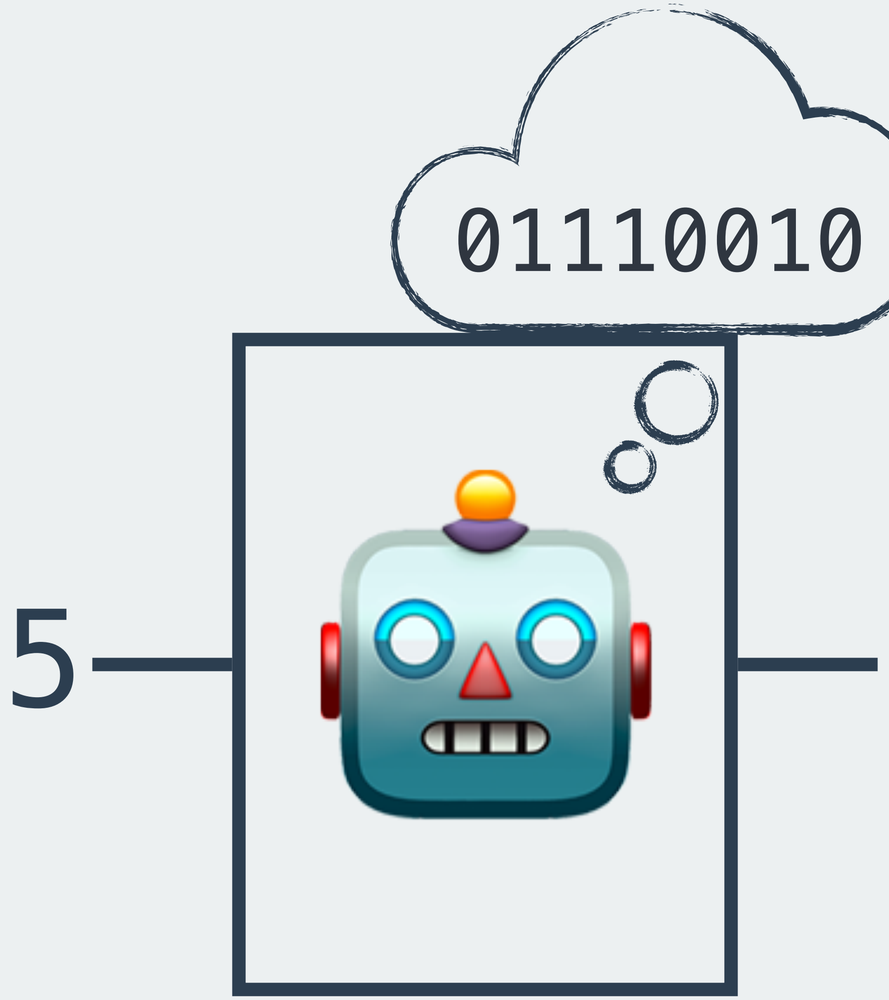

01110010
4

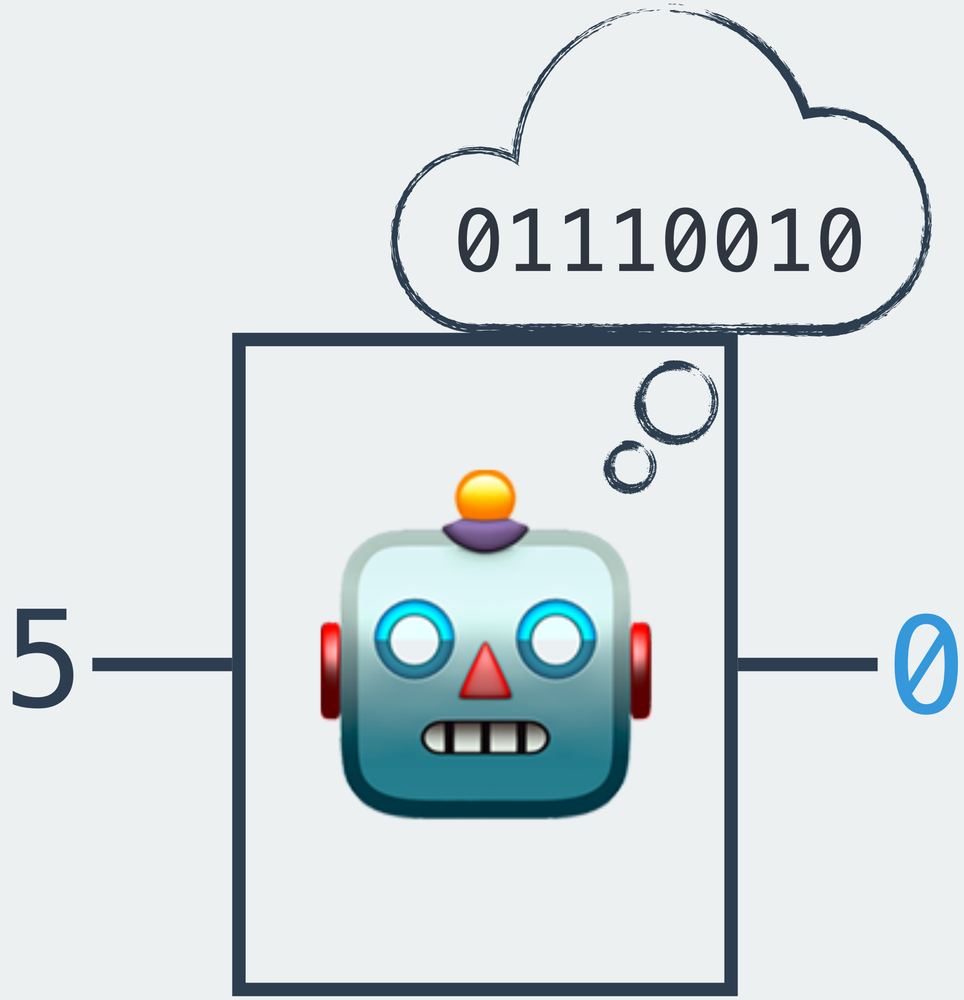

01110010
4

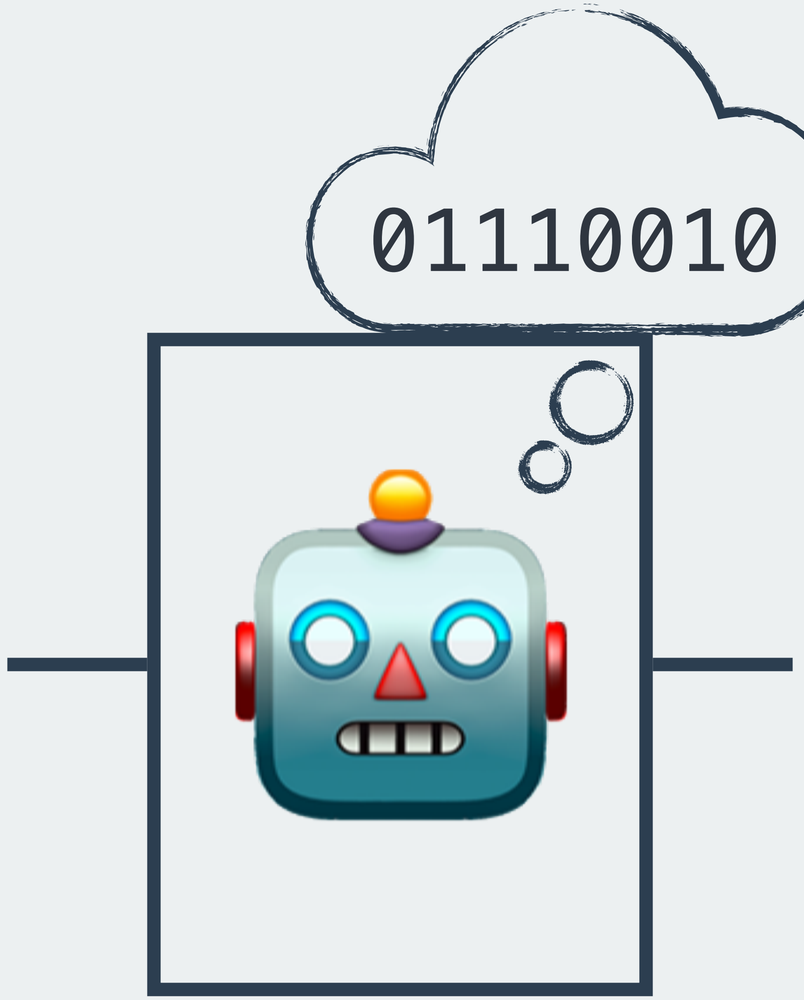

01110010
4
1

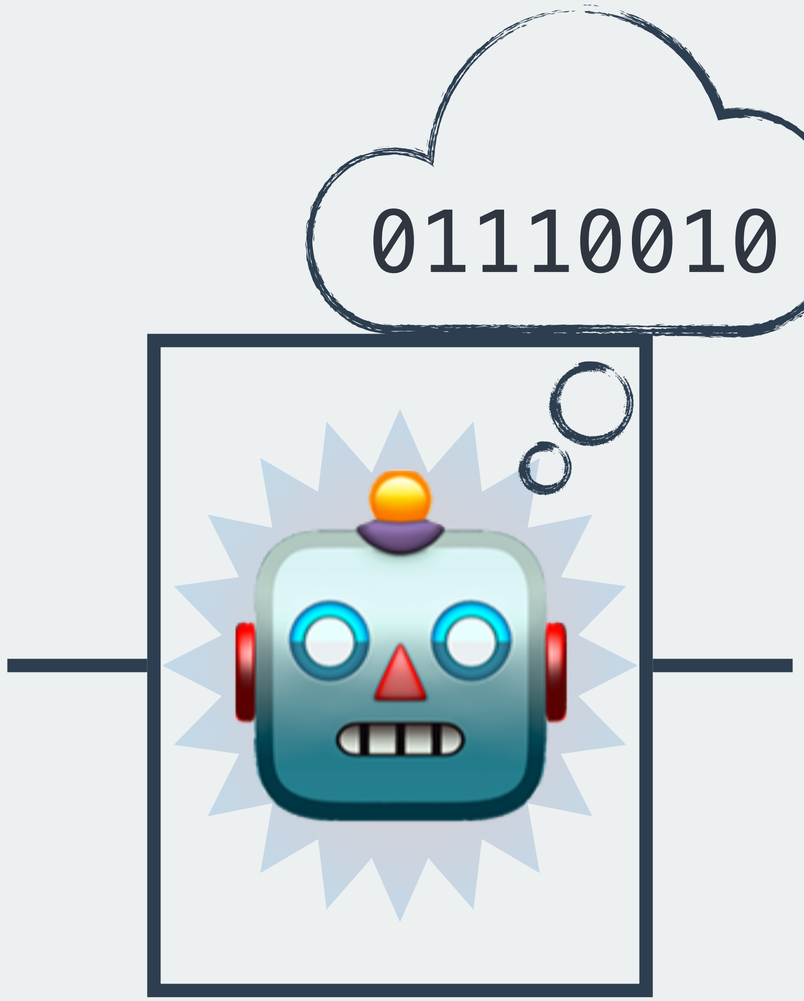

01110010

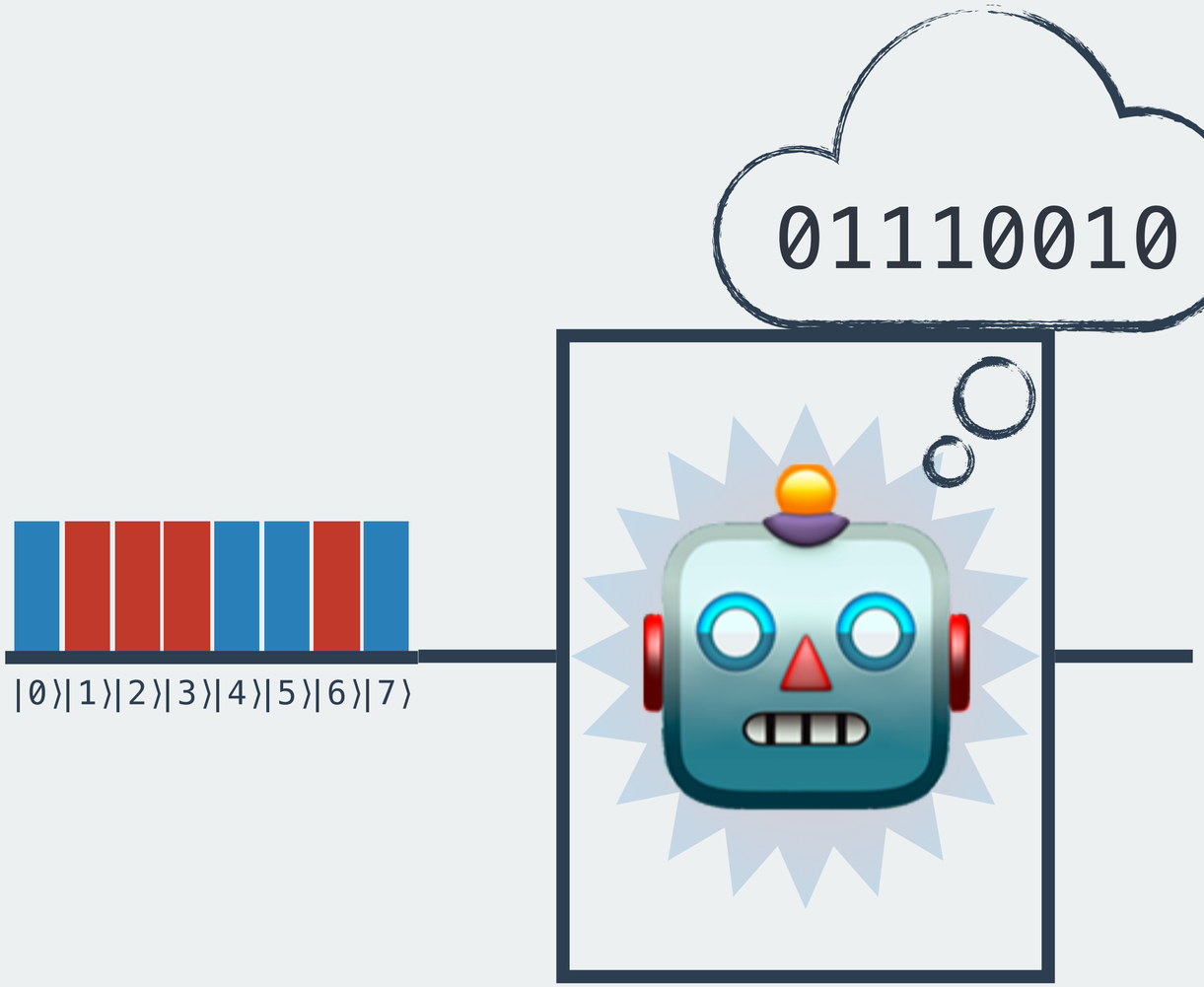

01110010
5

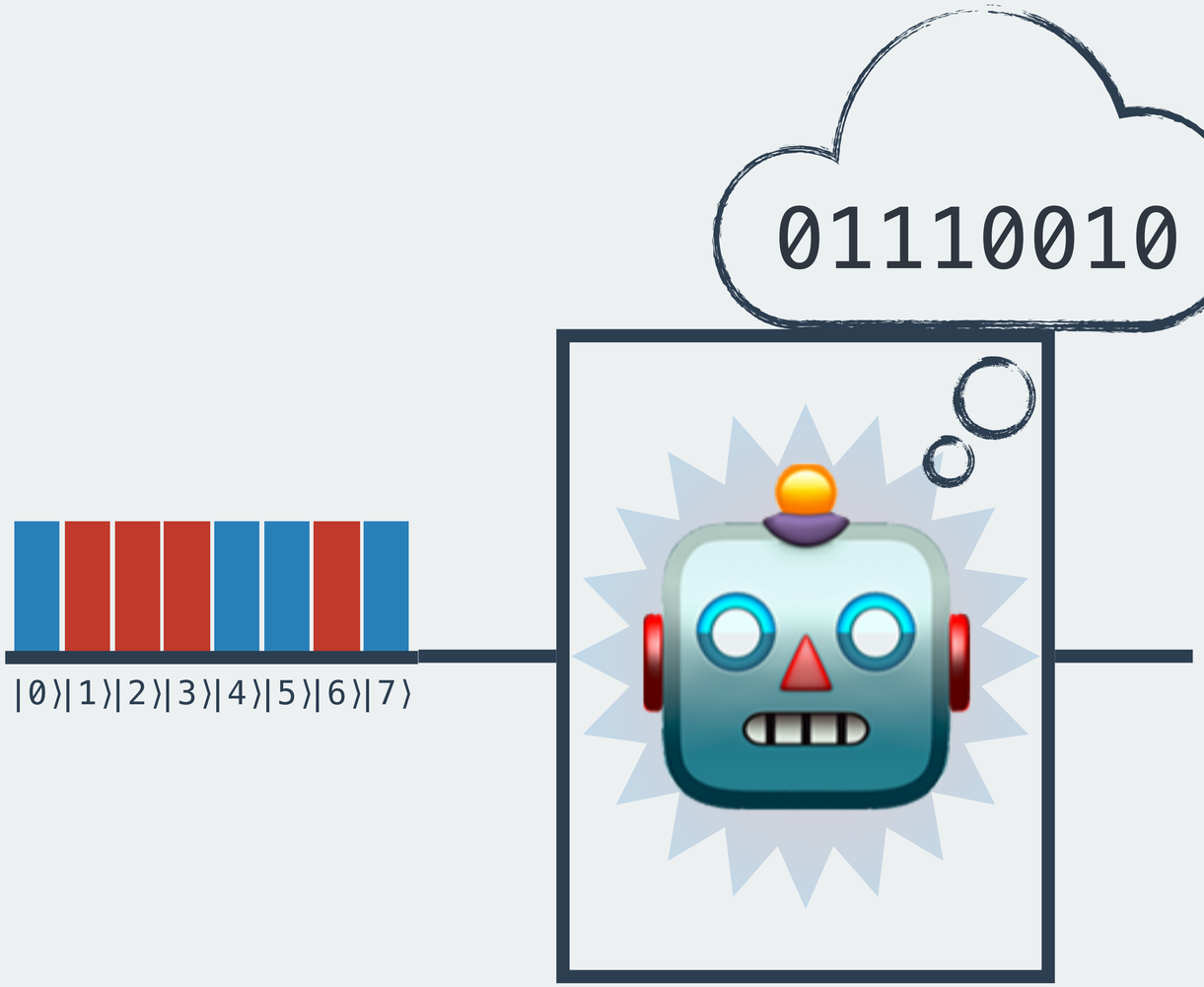

01110010
5

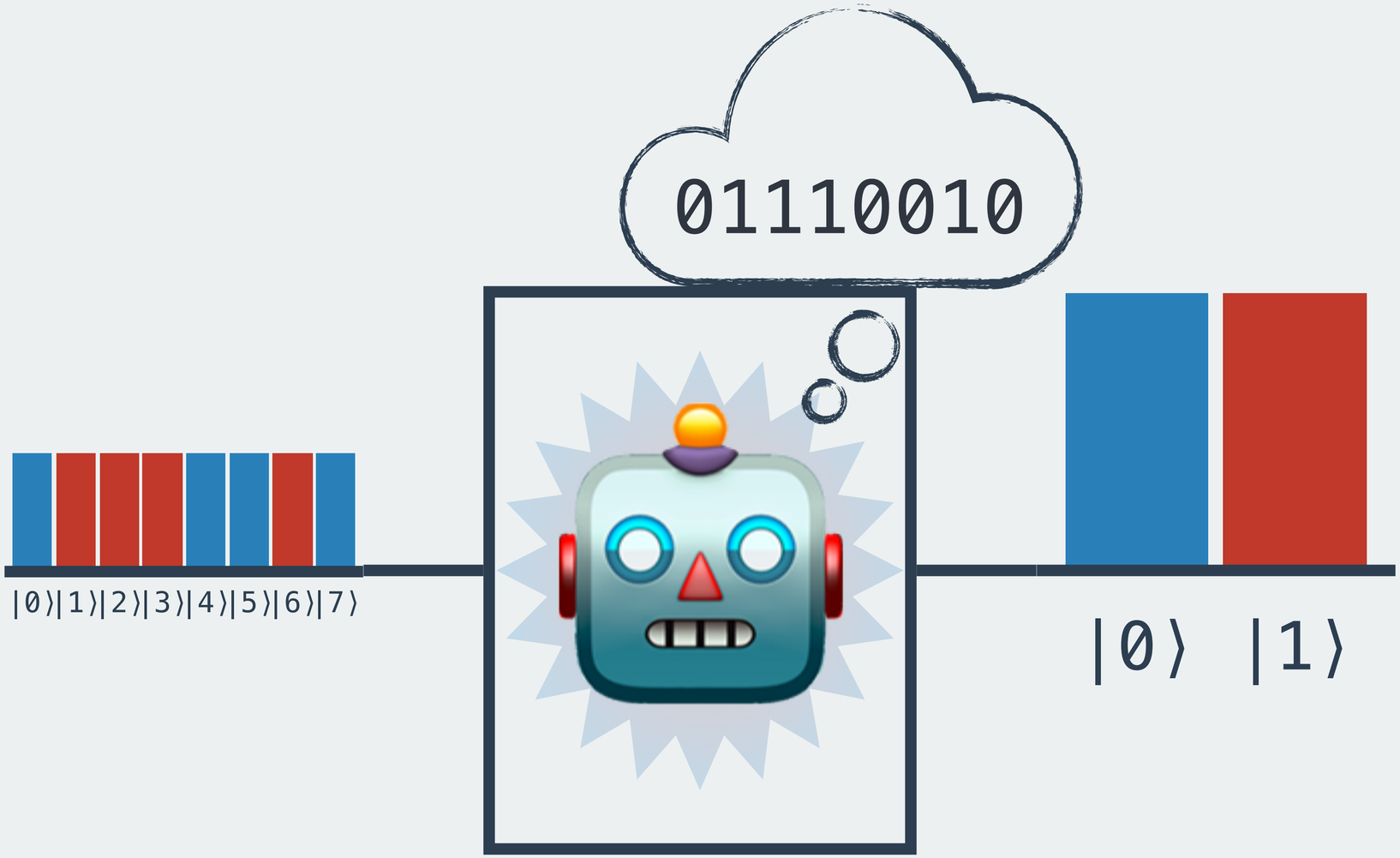

01110010
5
0

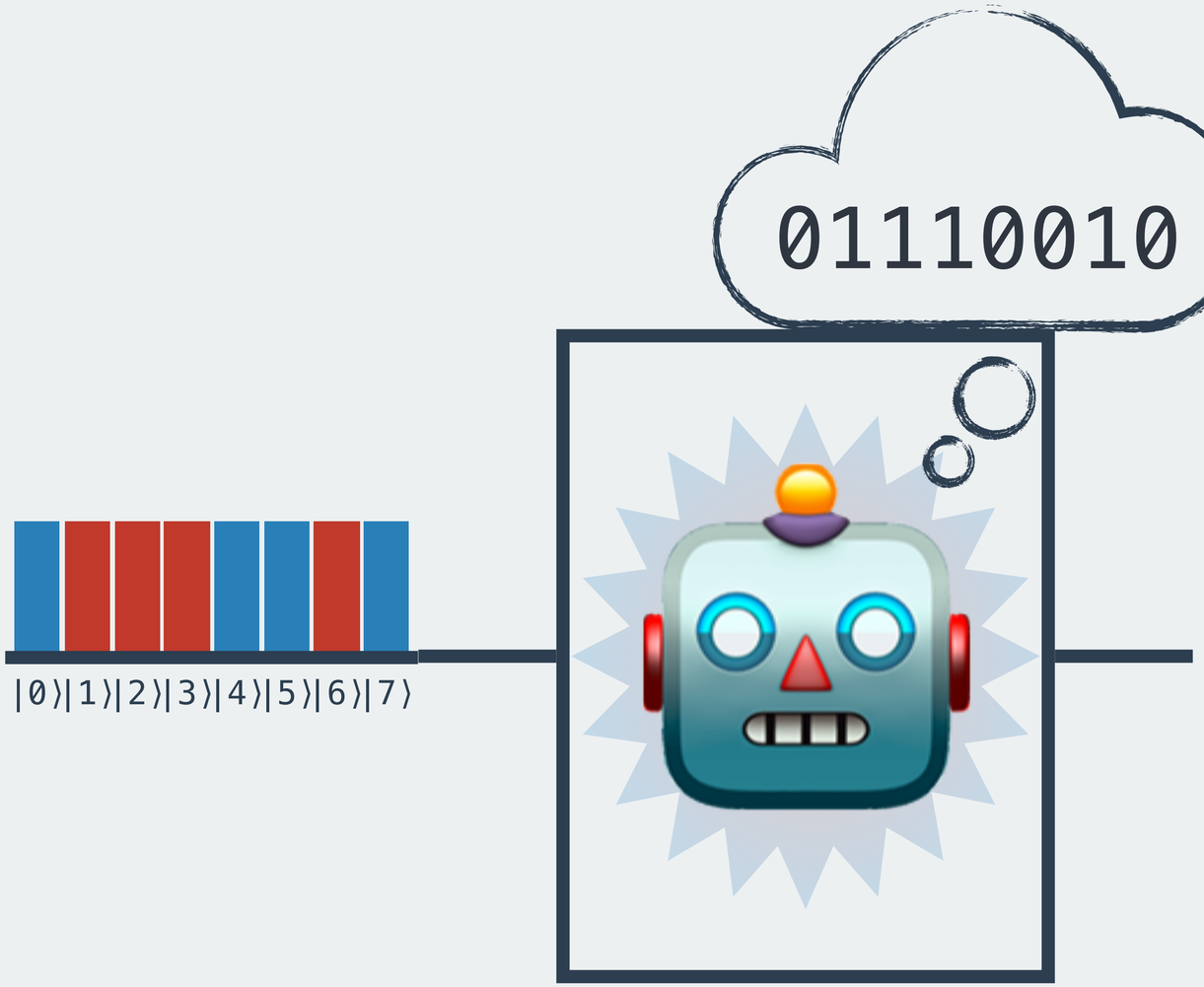

01110010

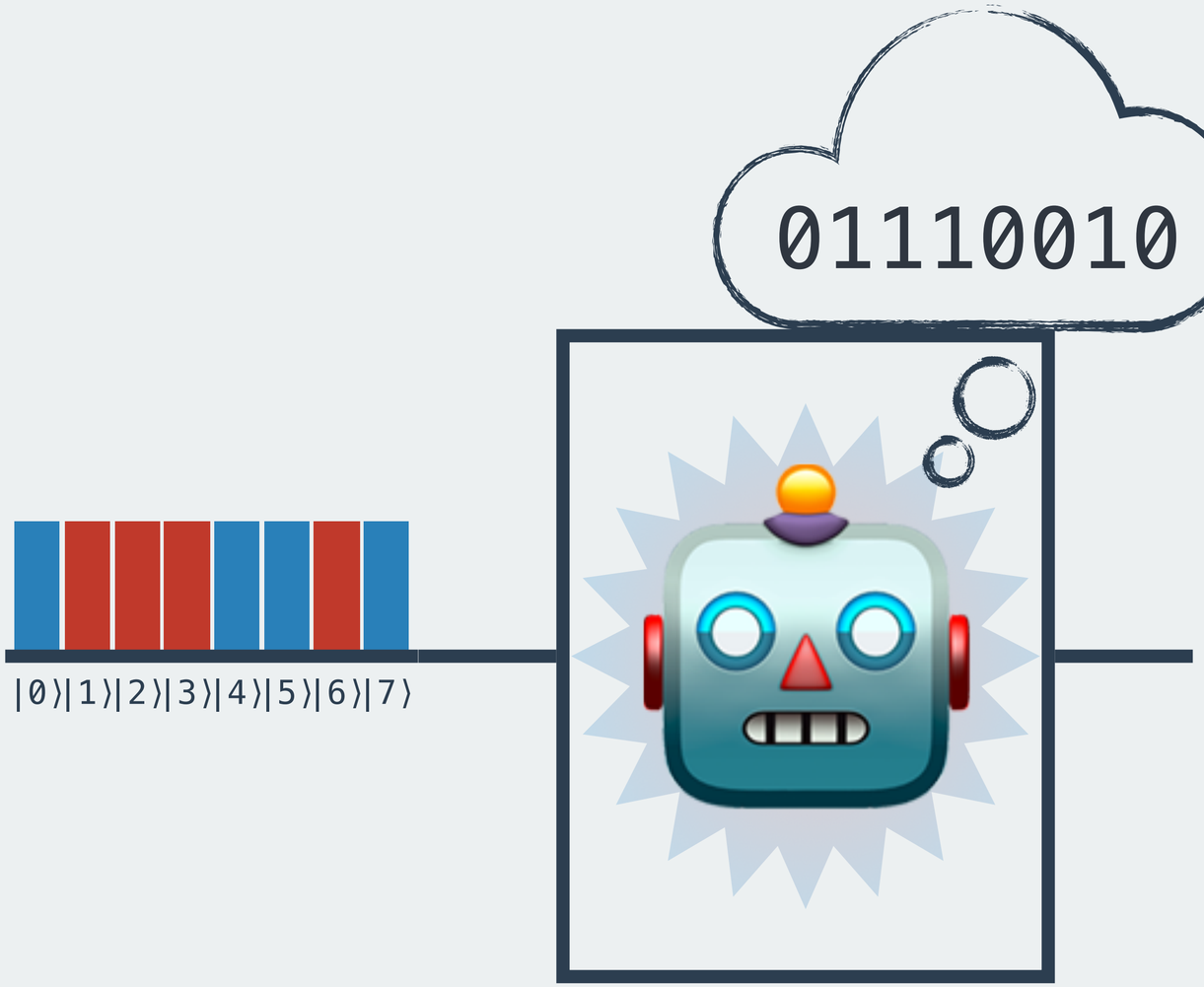

01110010

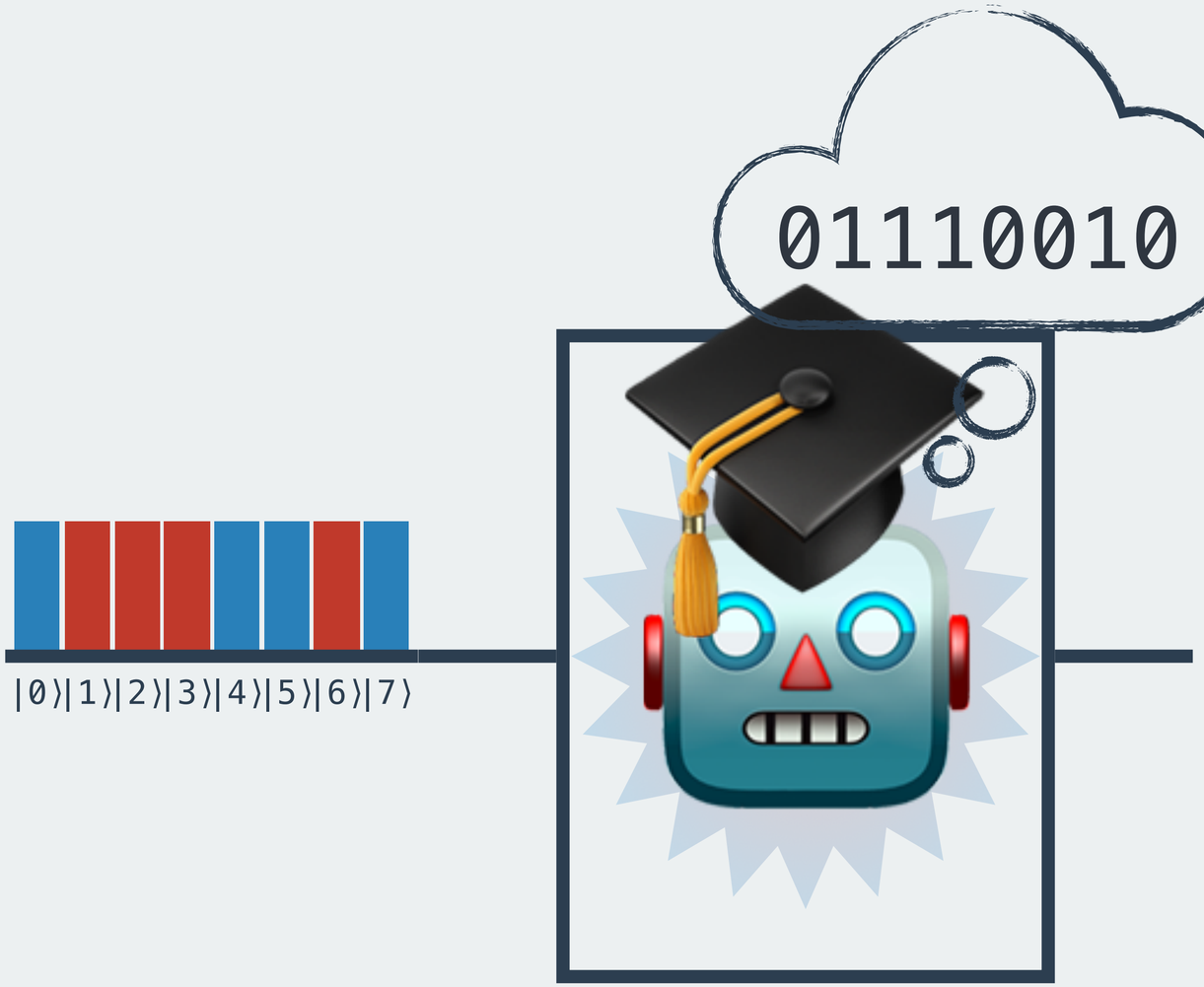

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

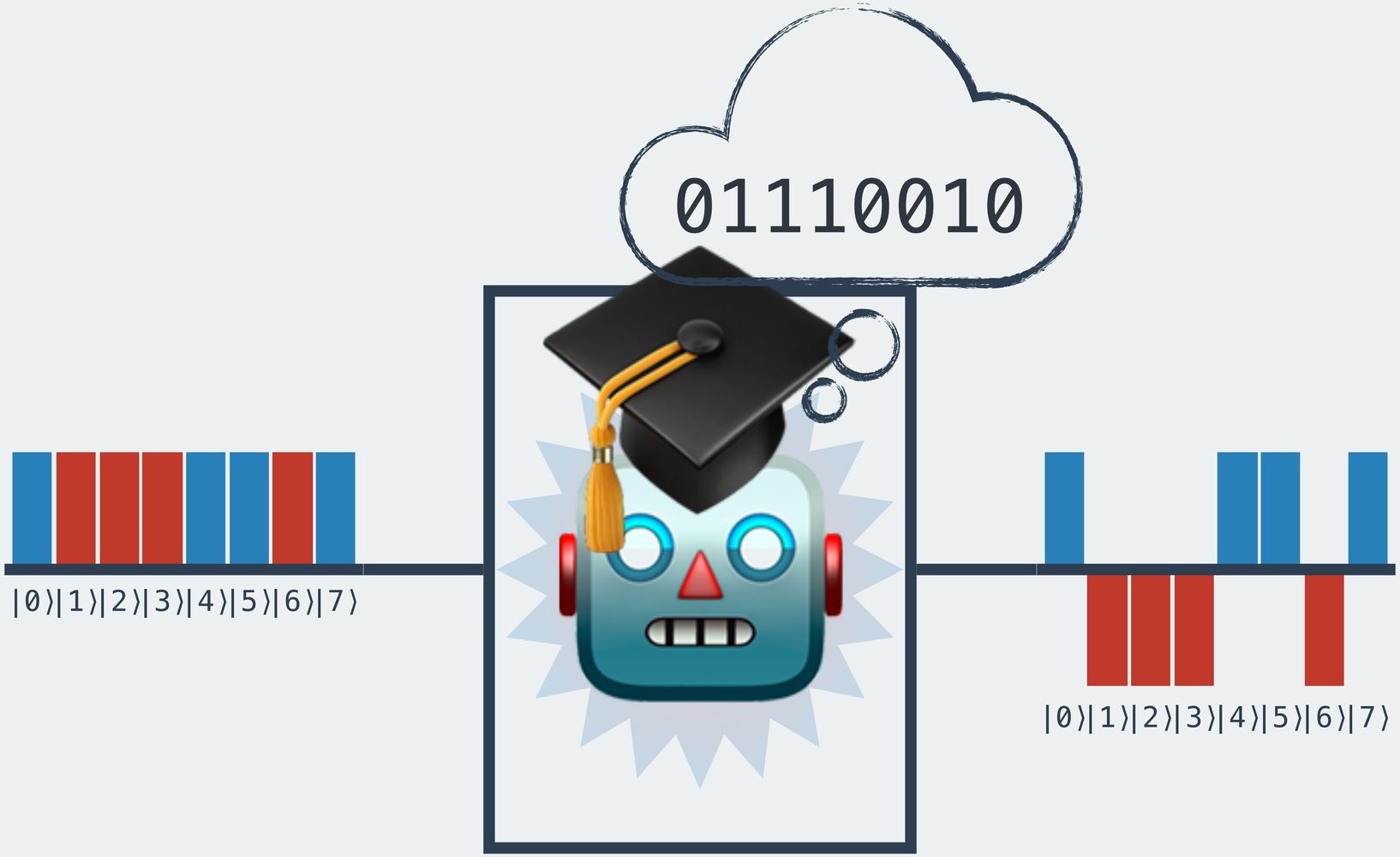

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

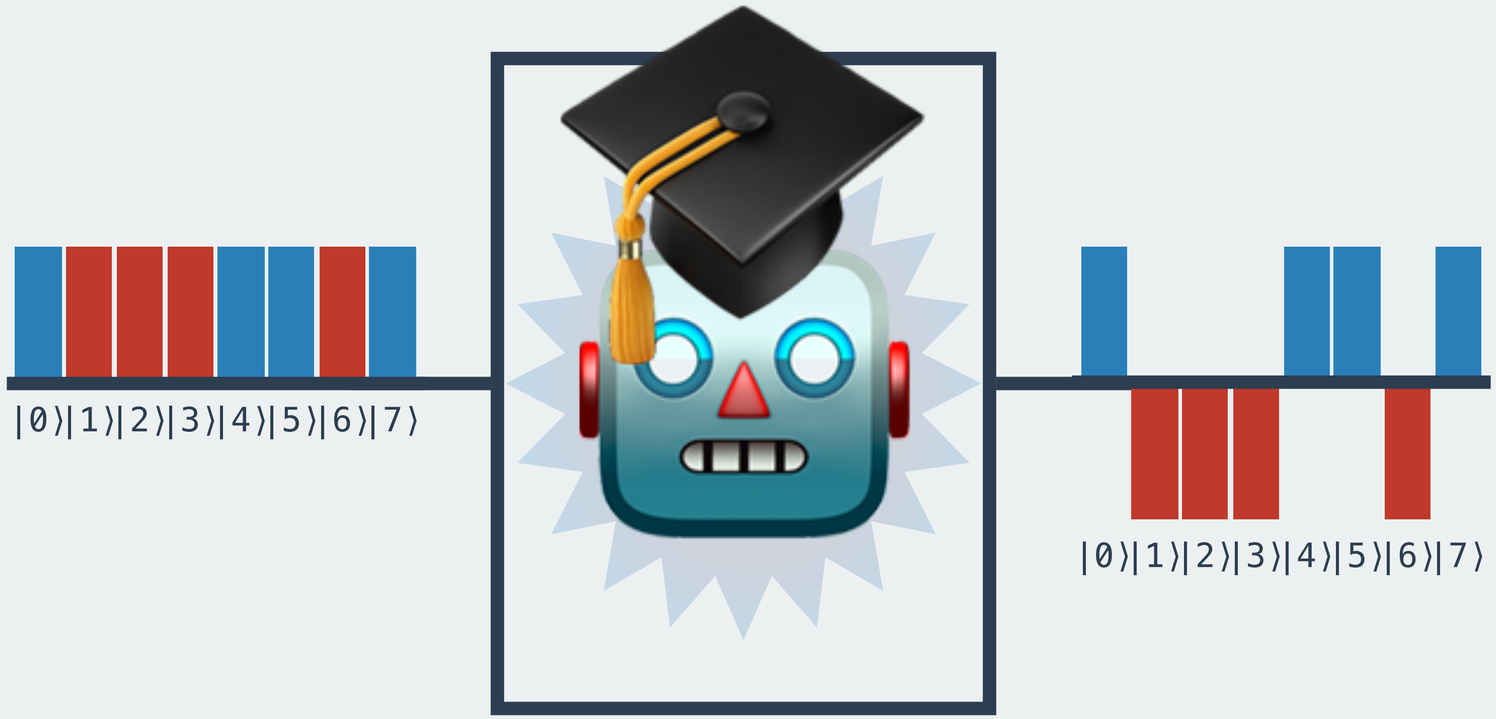

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩ |1⟩

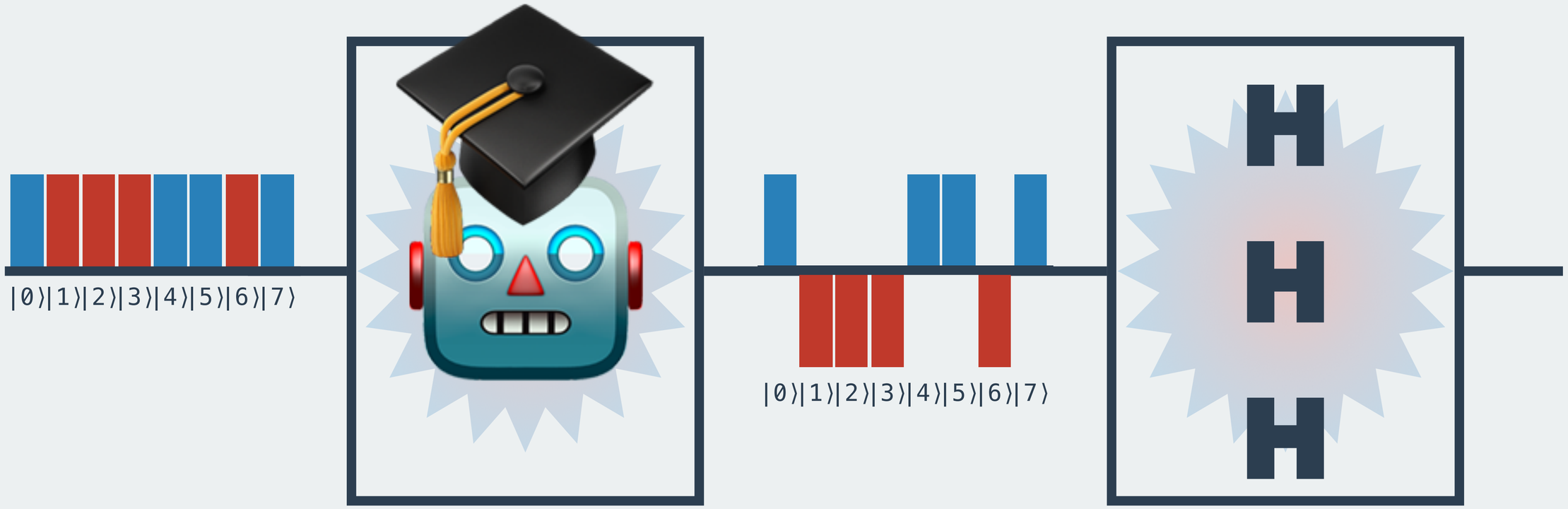

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

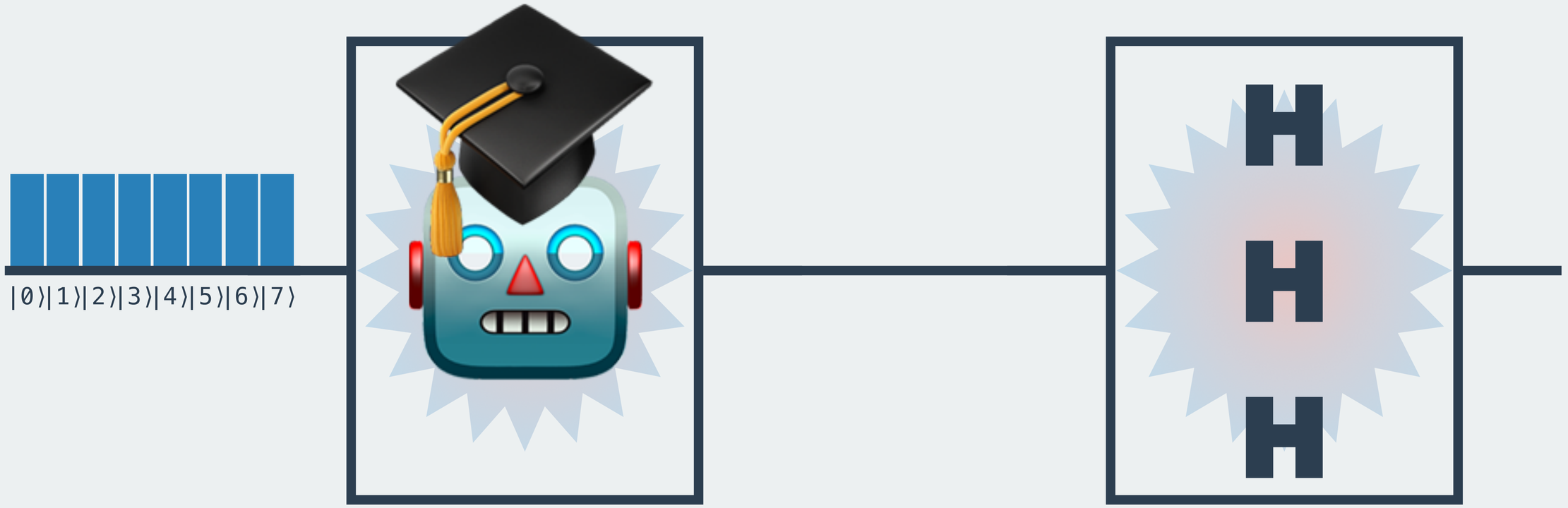

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

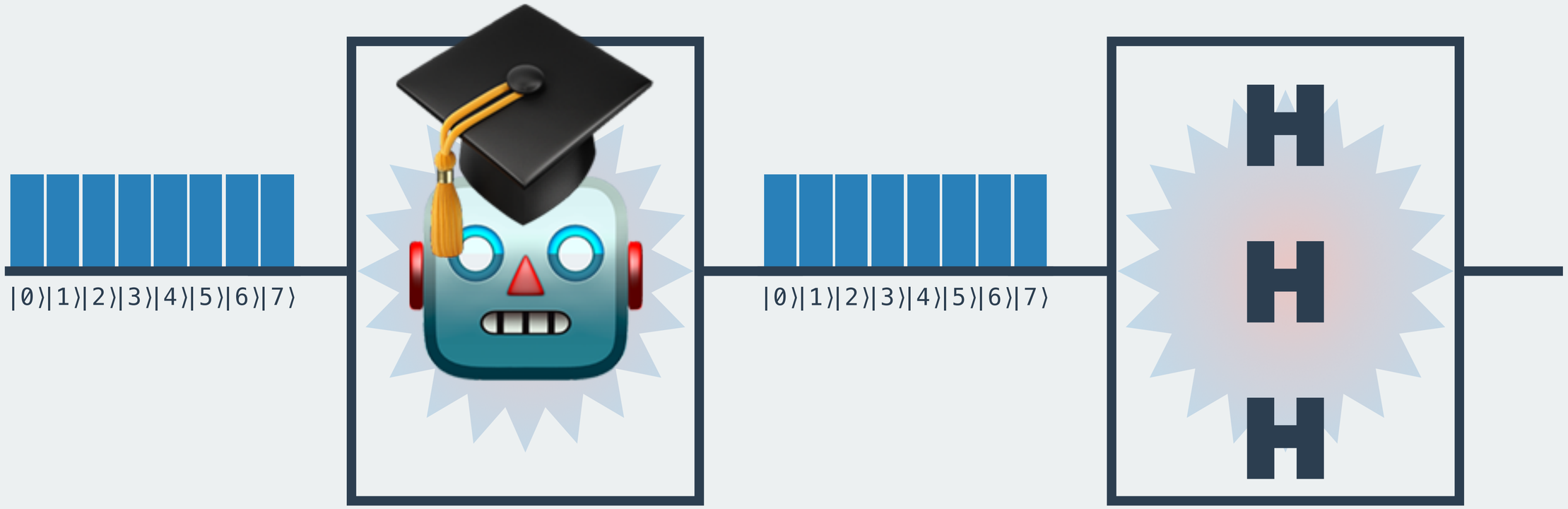

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

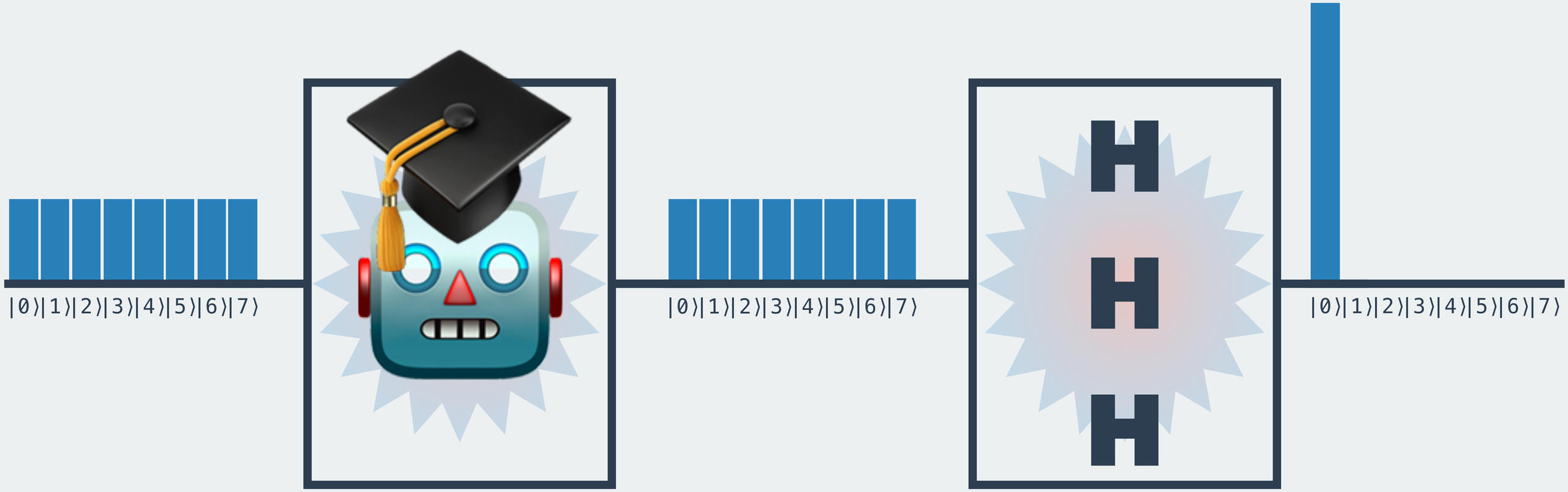

01110010
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

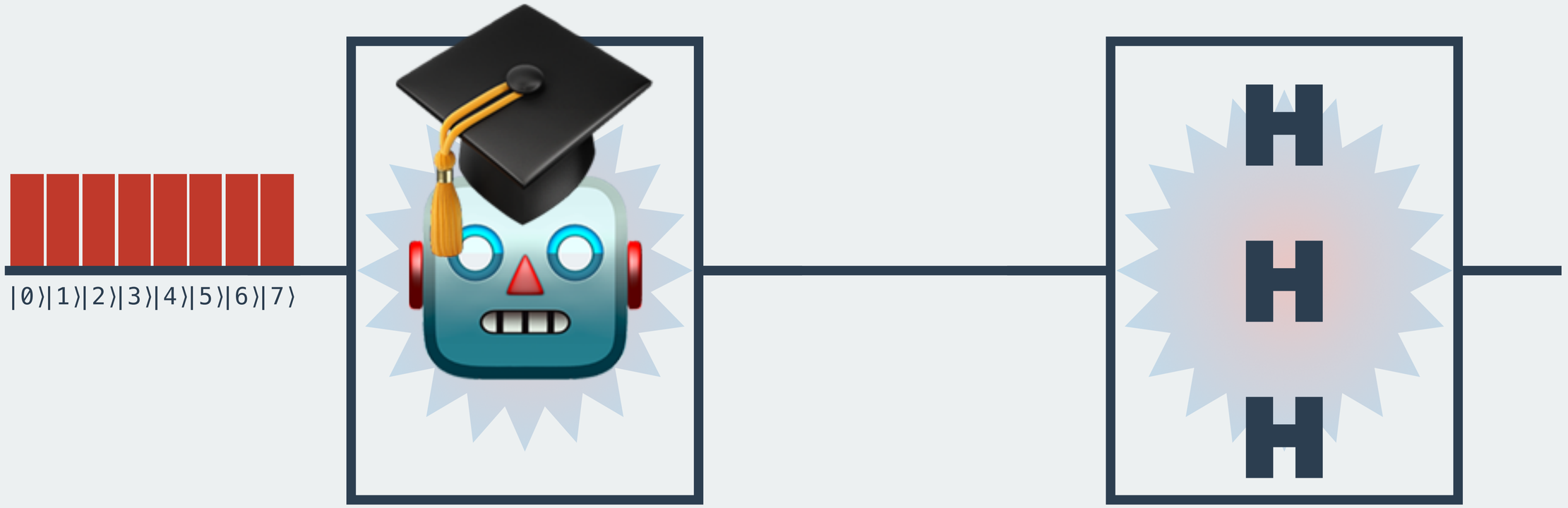

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

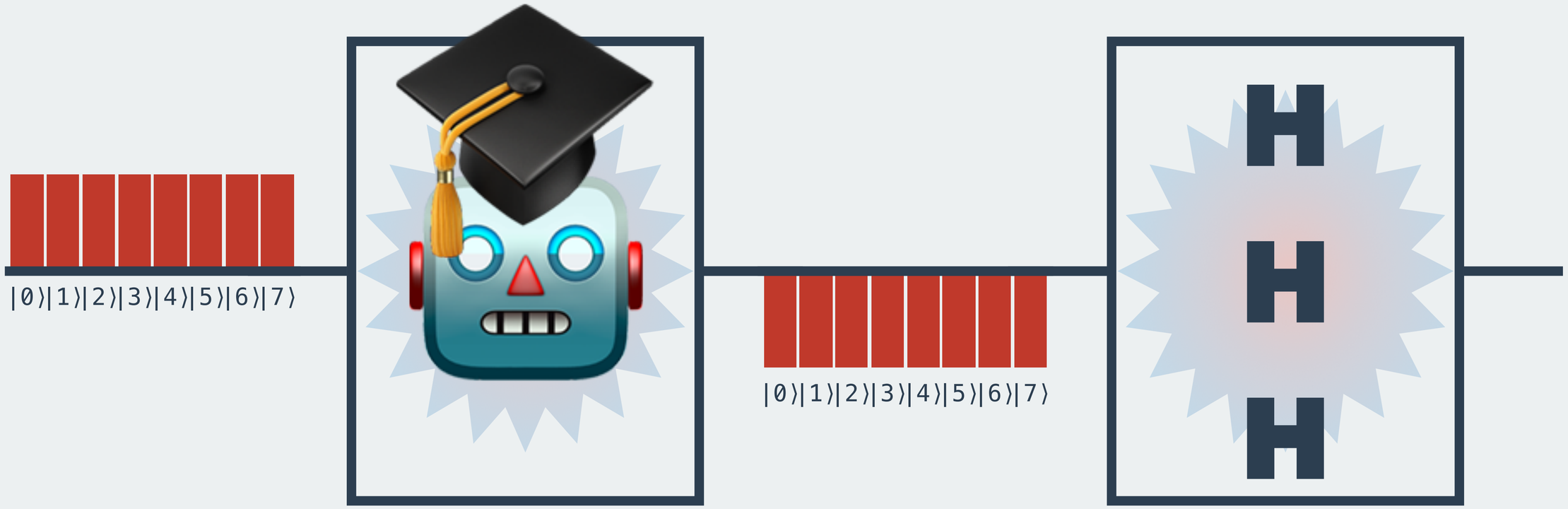

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H

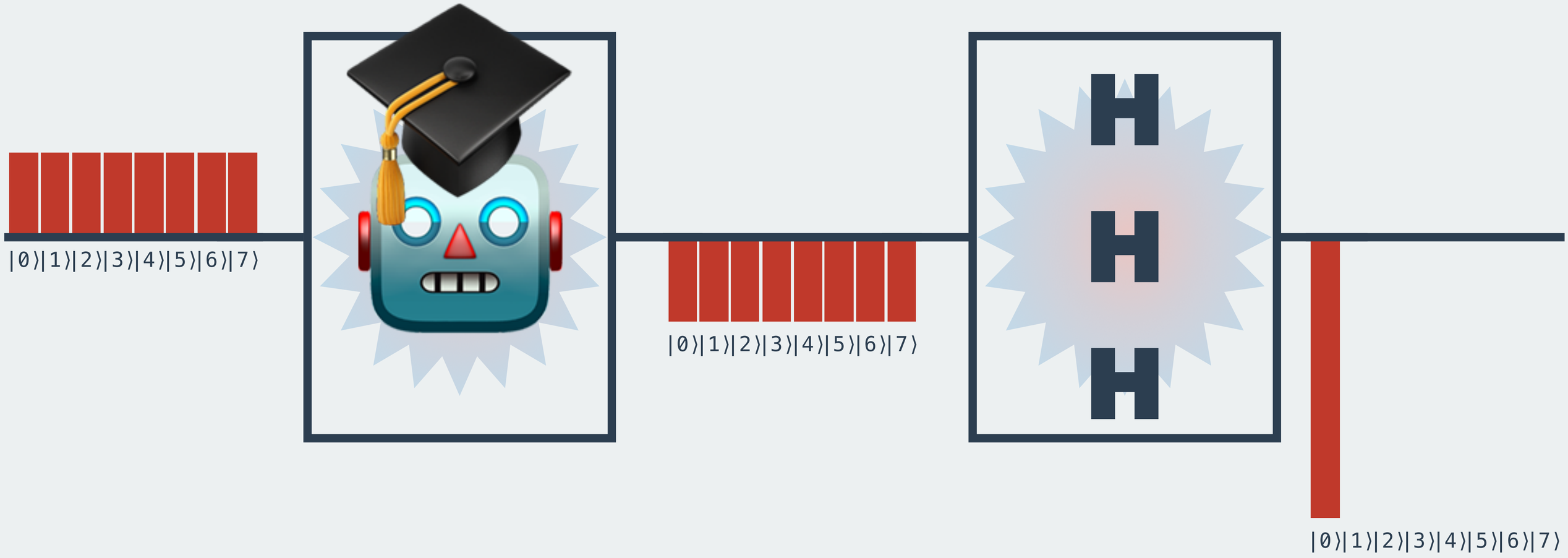

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H

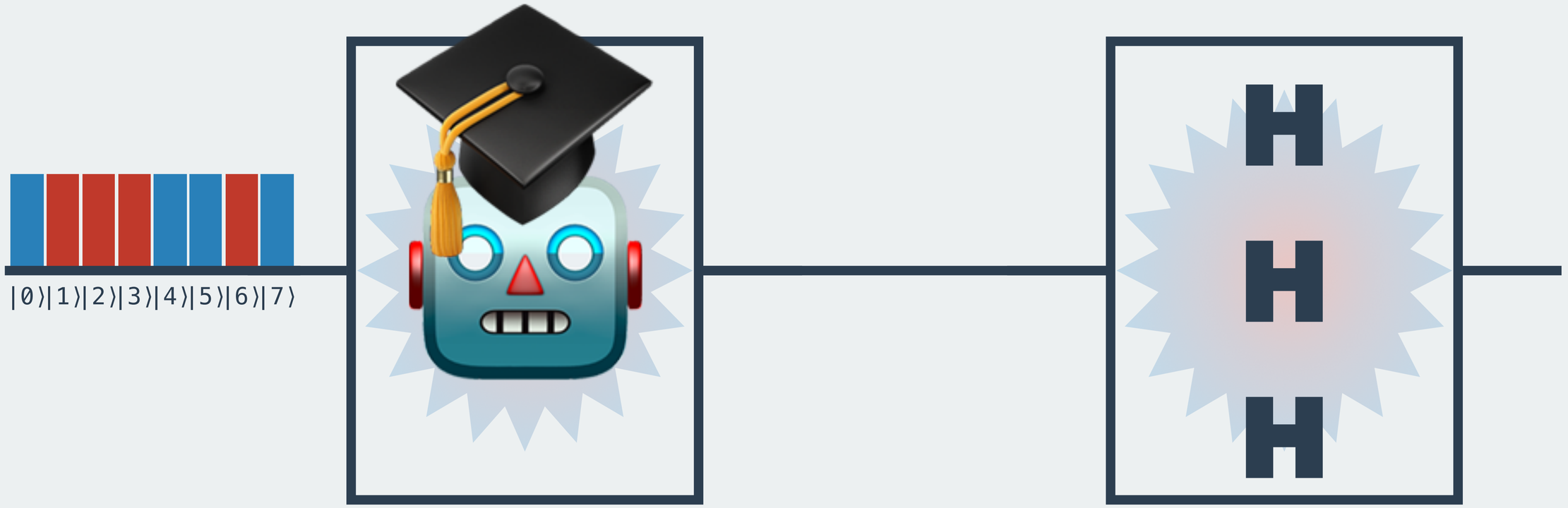

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H

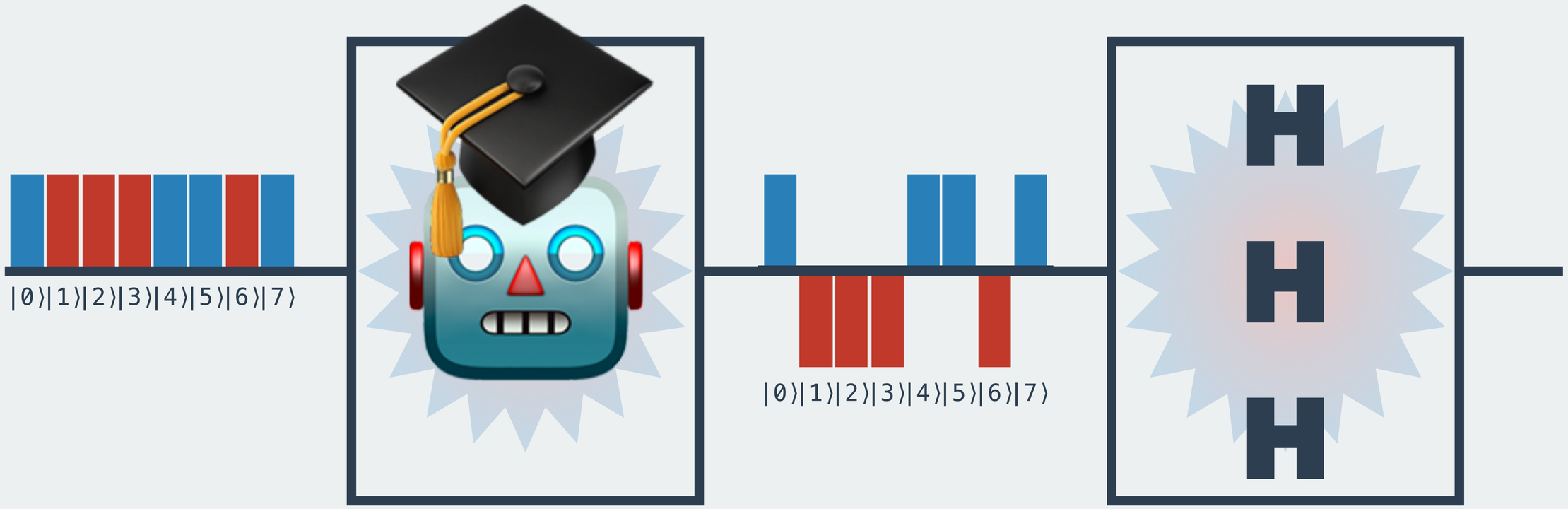

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

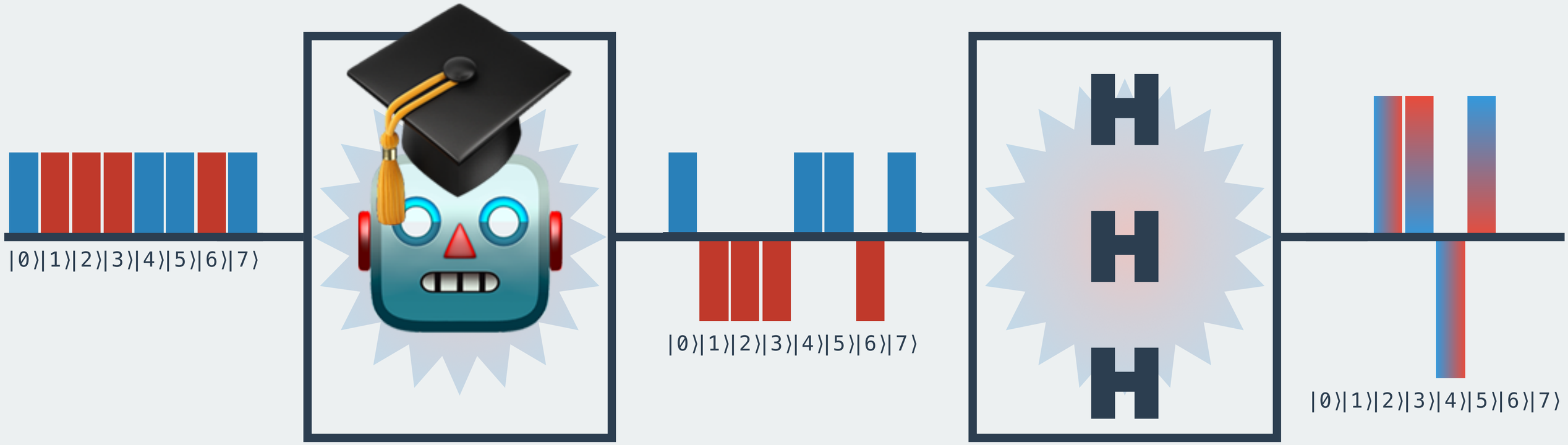

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H


|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H


|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

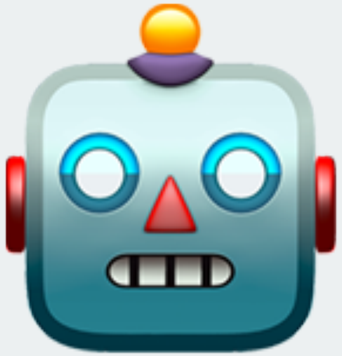

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H


|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H

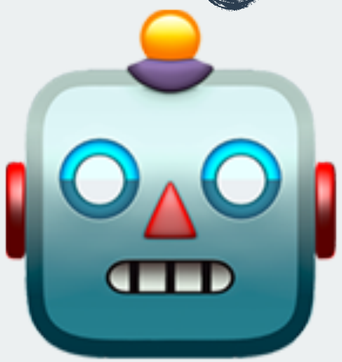

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
H
H
H
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

GROVERJEV
ALGORITEM

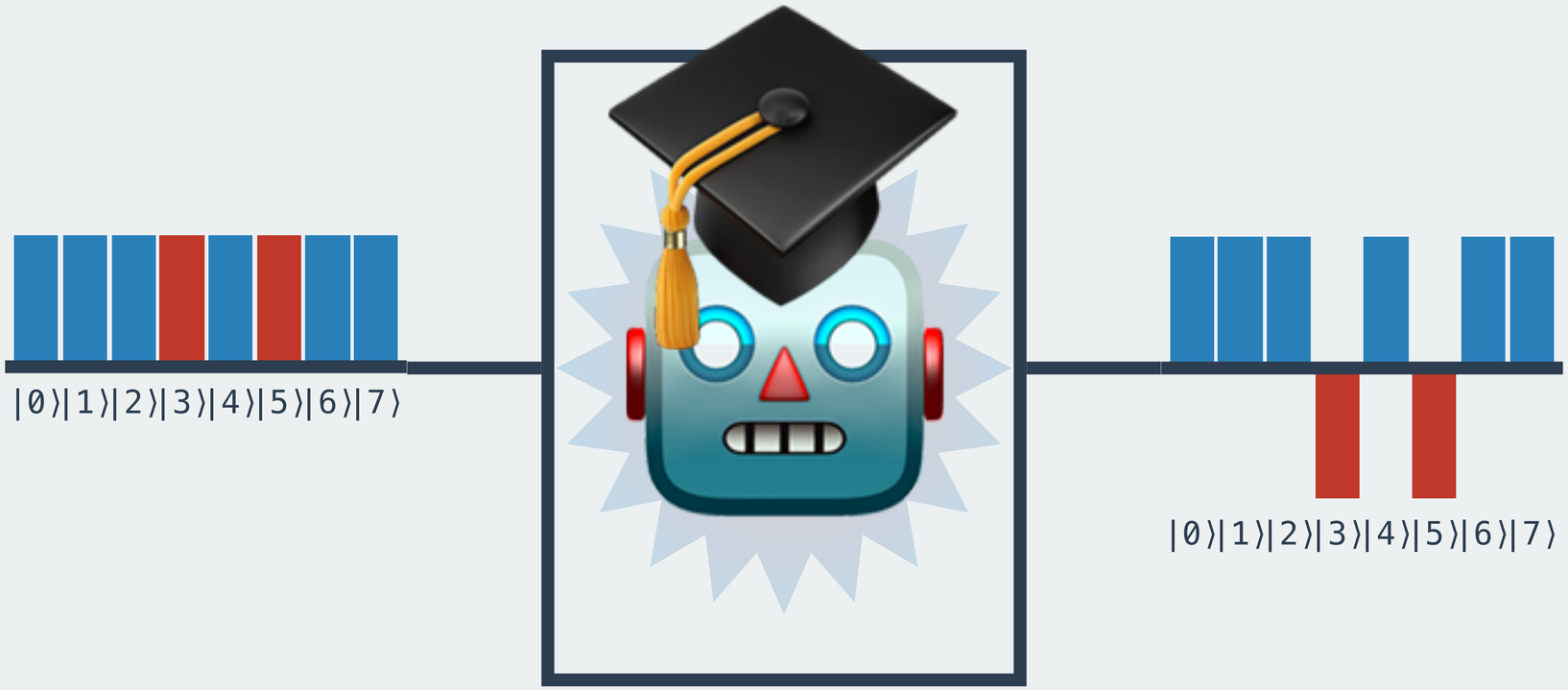
Lov Grover, 1961-

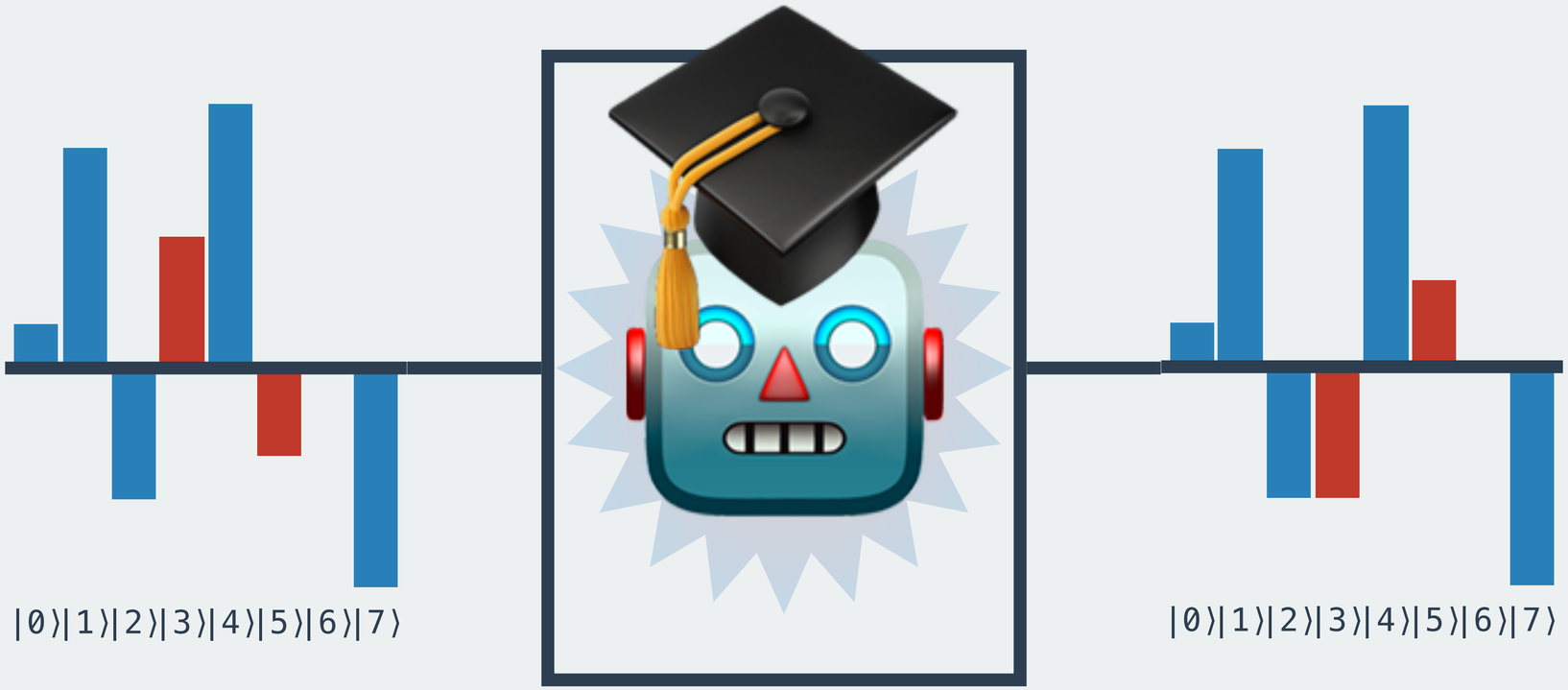


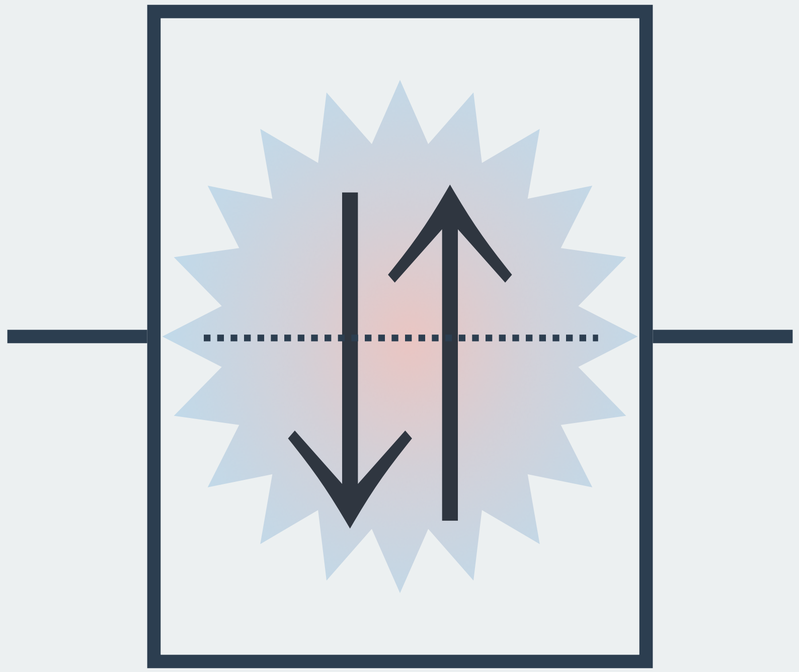
ali je **x**
pravi delitelj **15**?

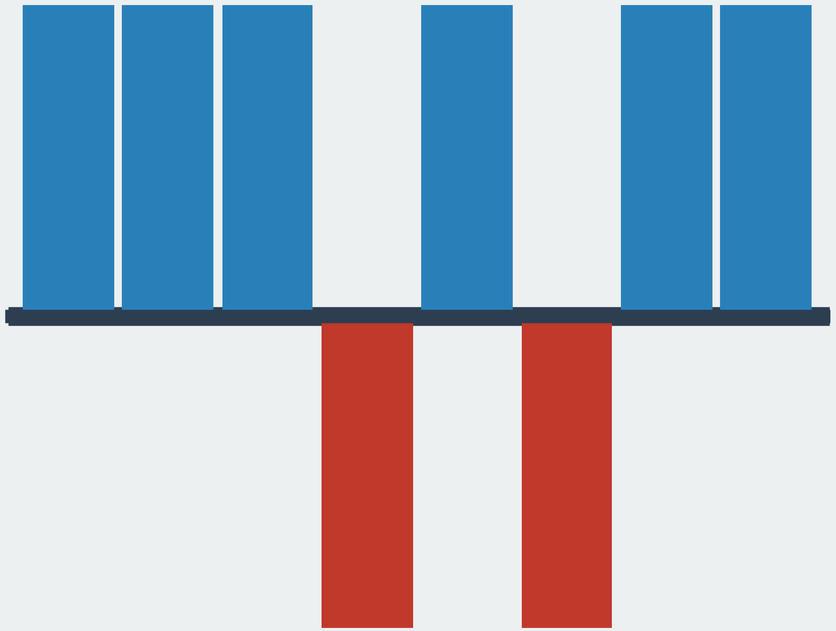


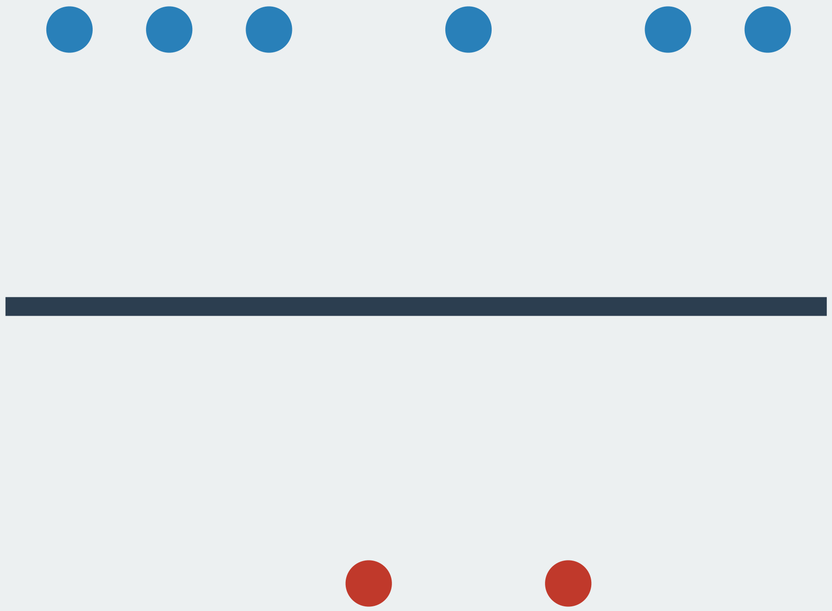
ali je **x**
pravi delitelj
243987329812 79?

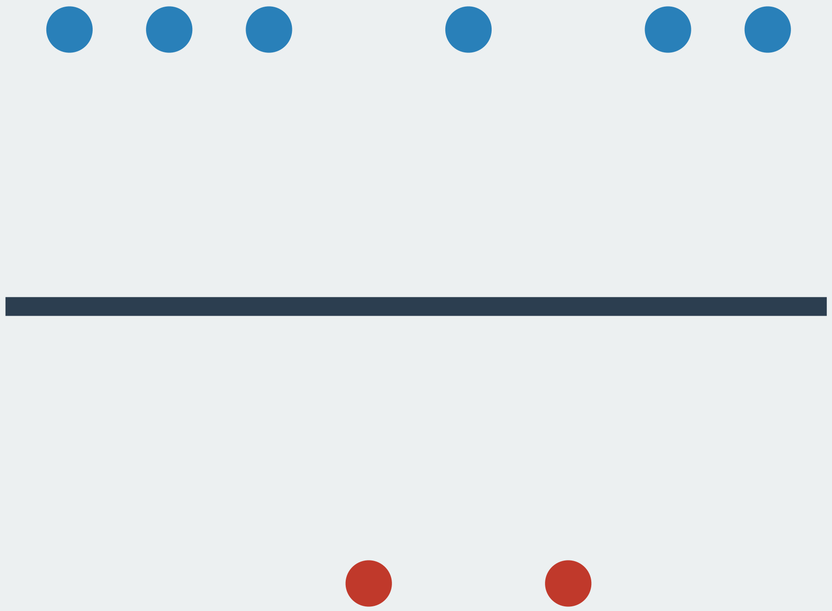

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

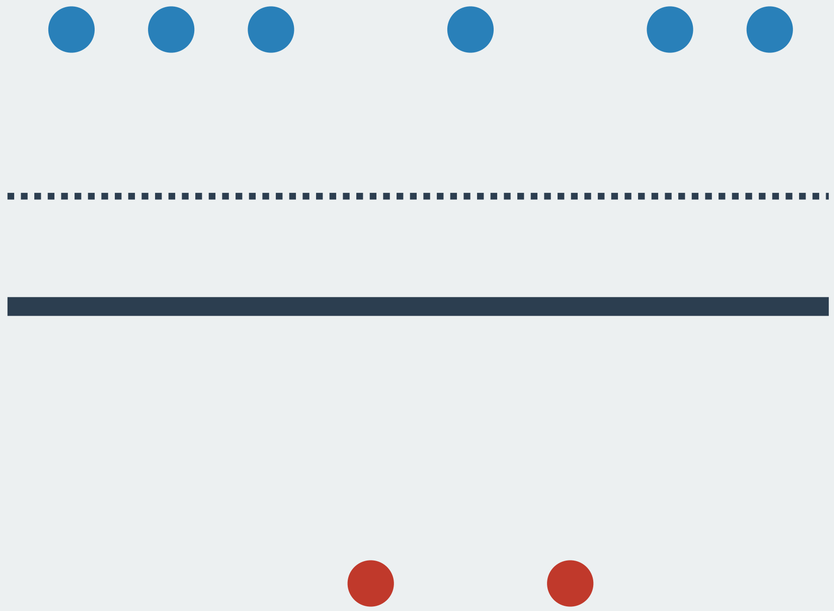

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

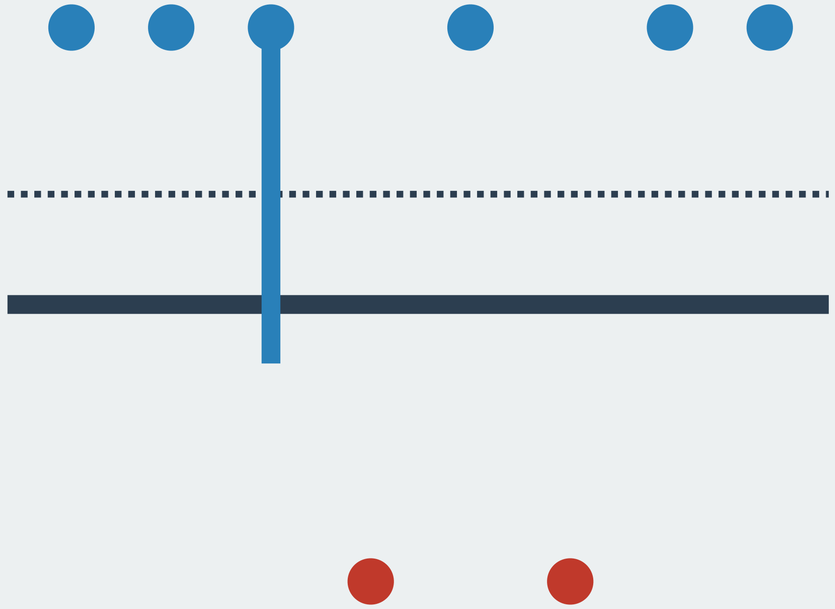


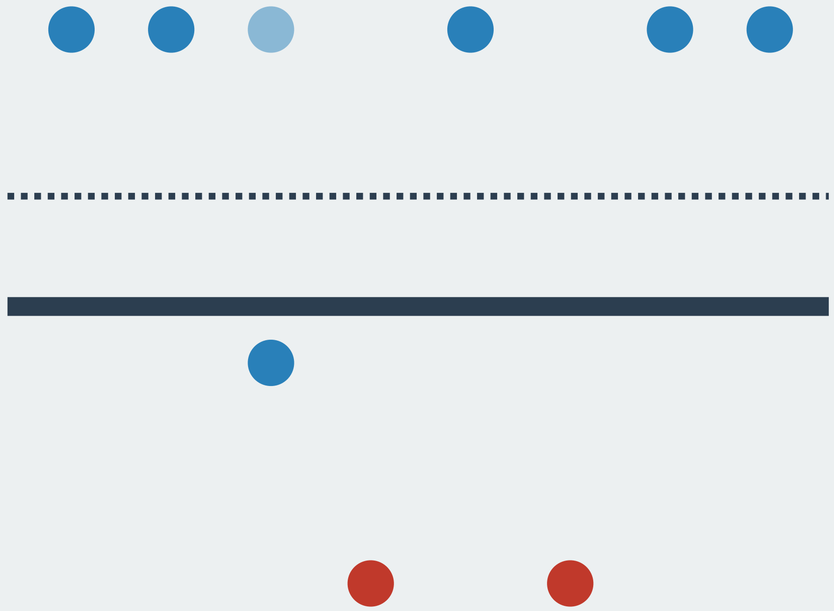


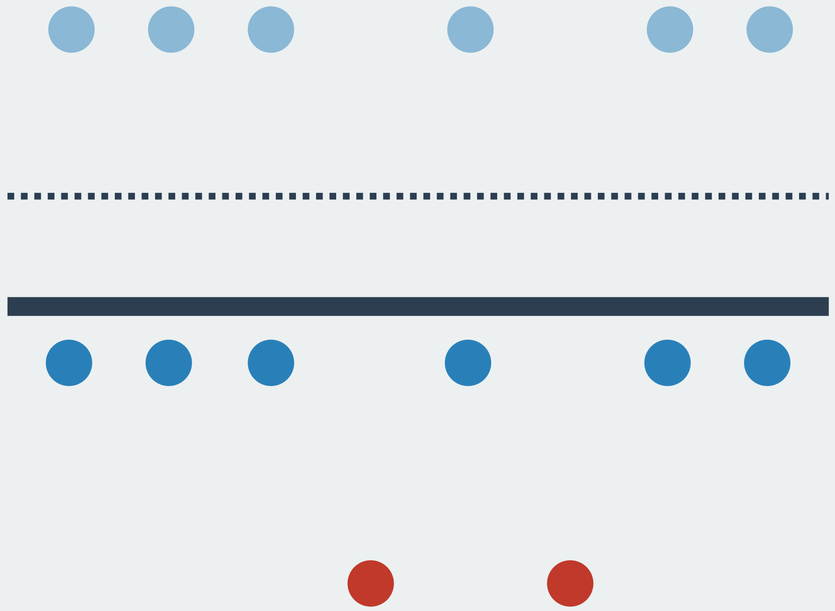


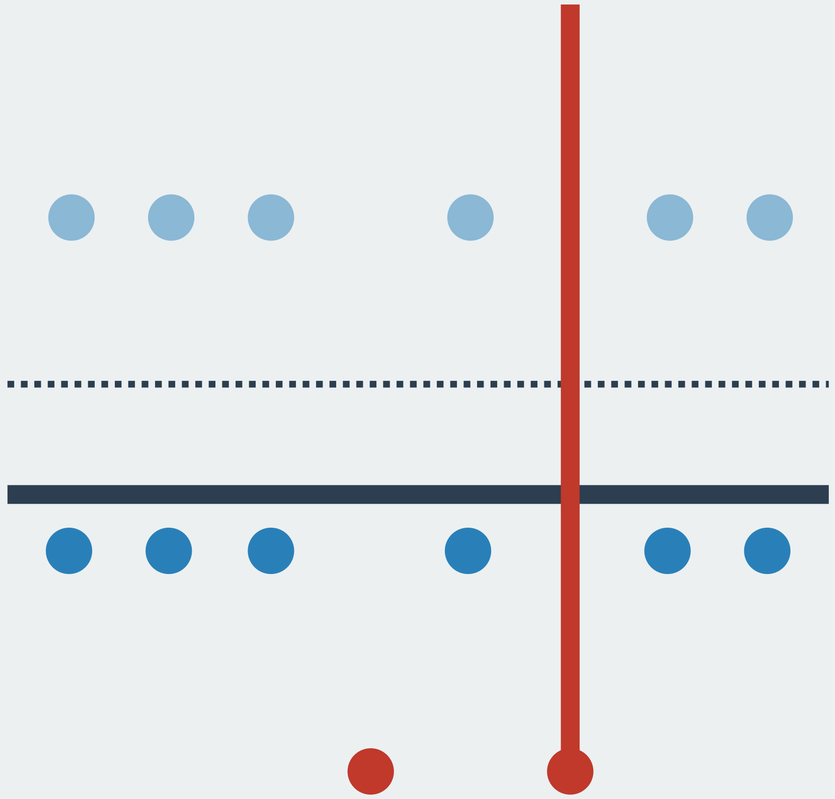


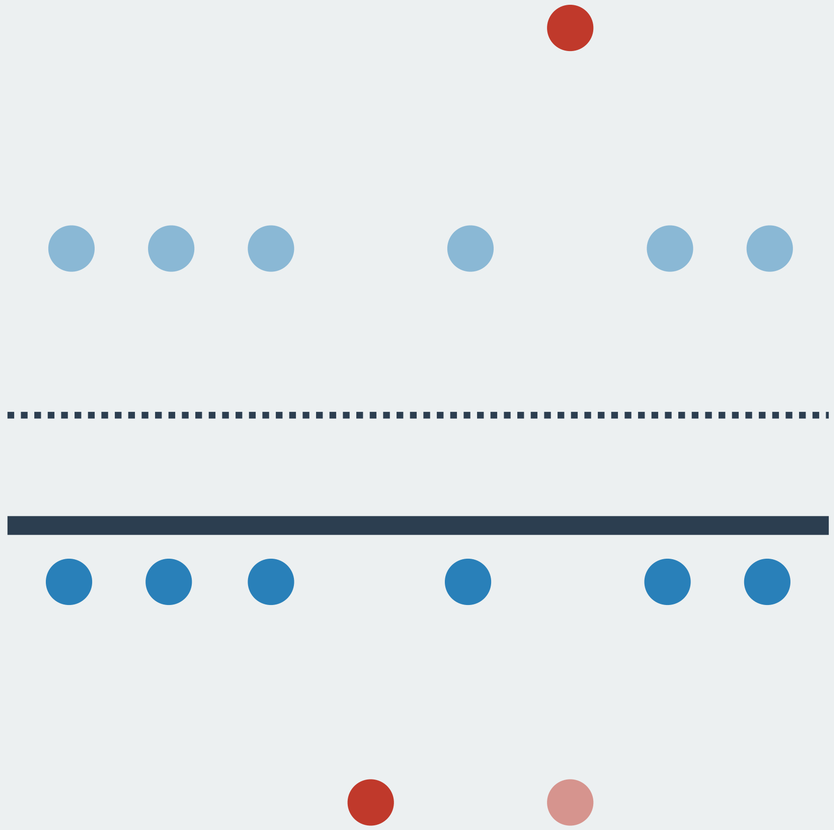


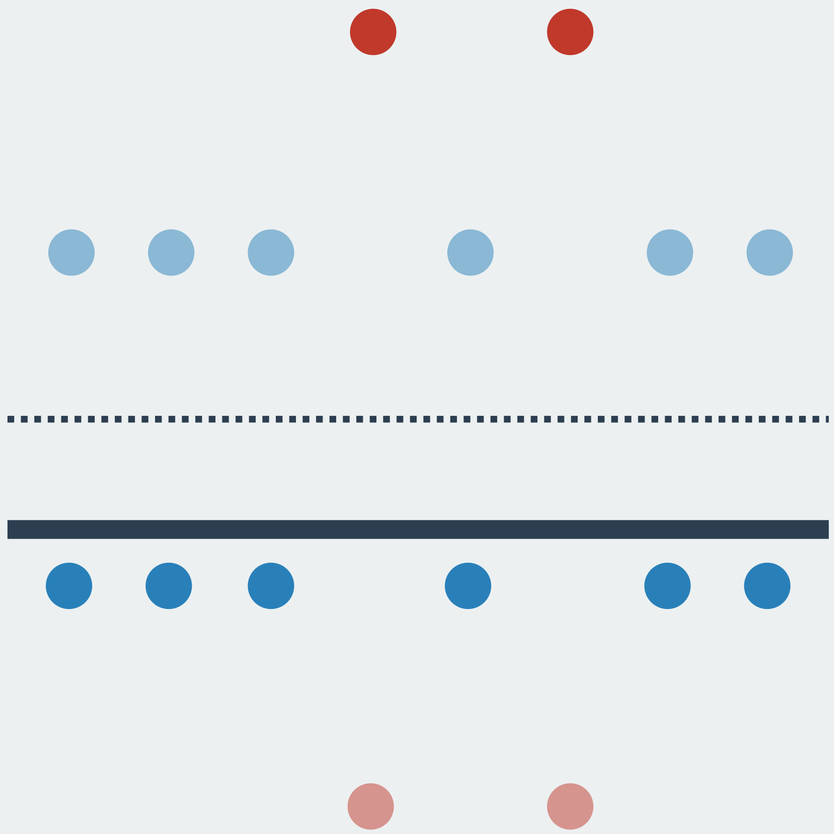


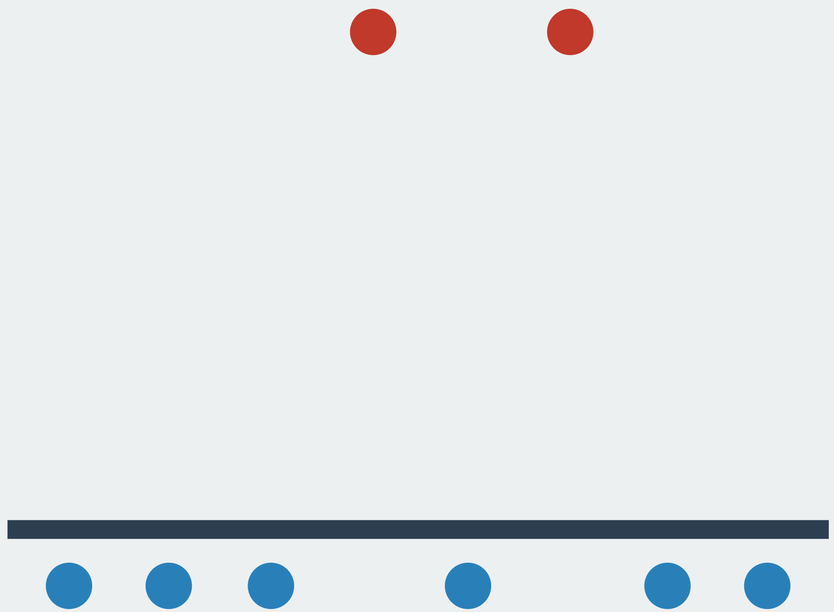


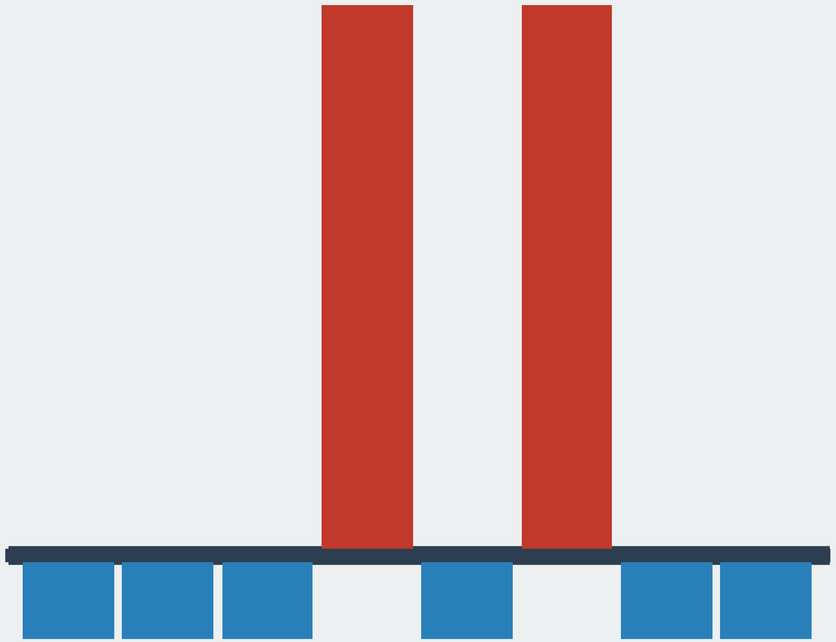


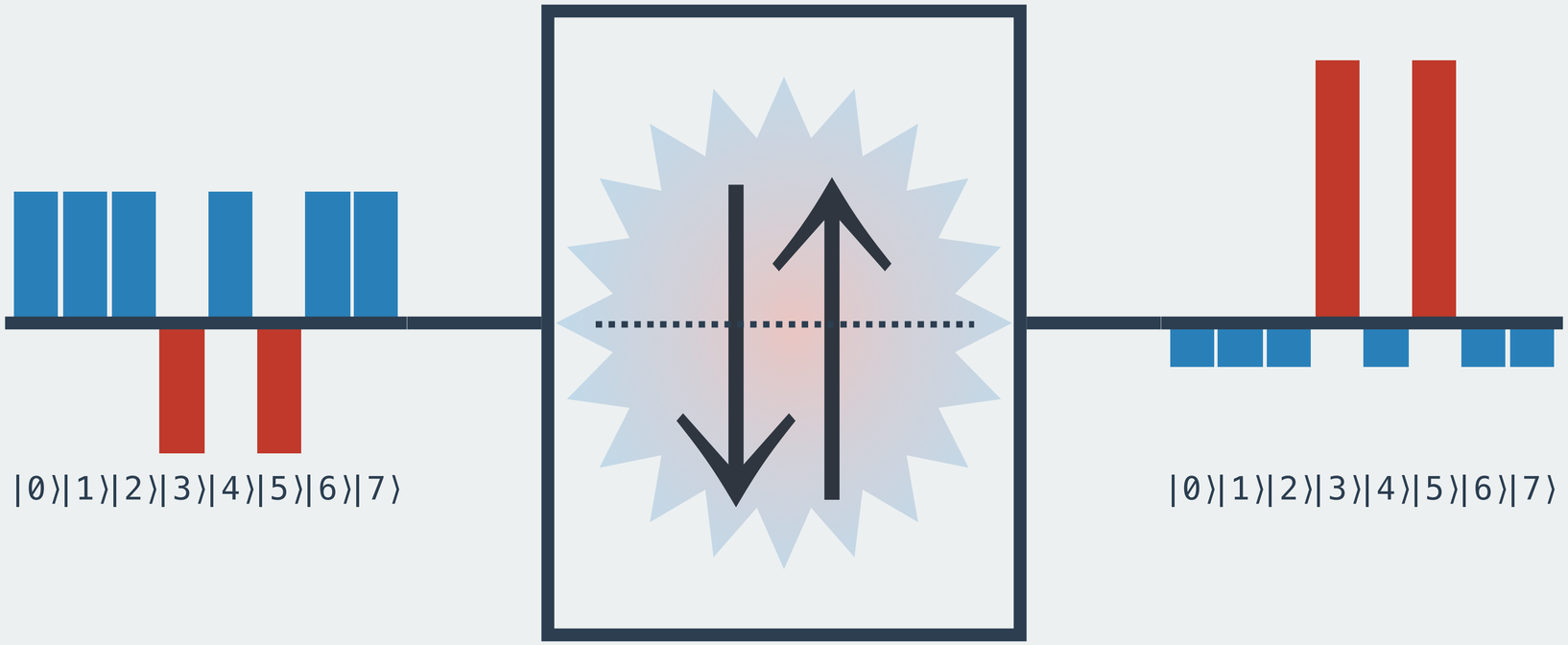


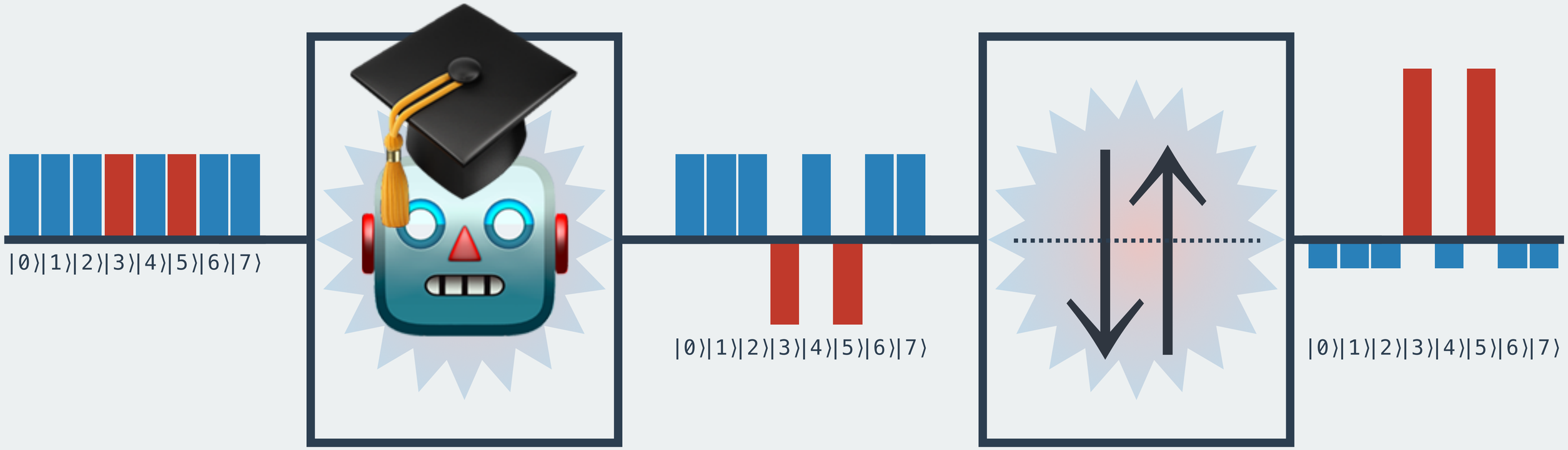


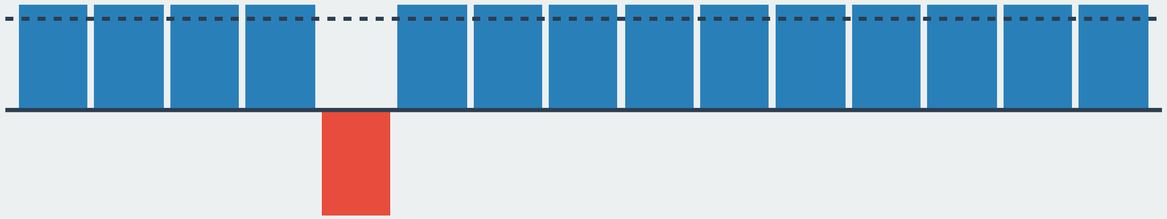


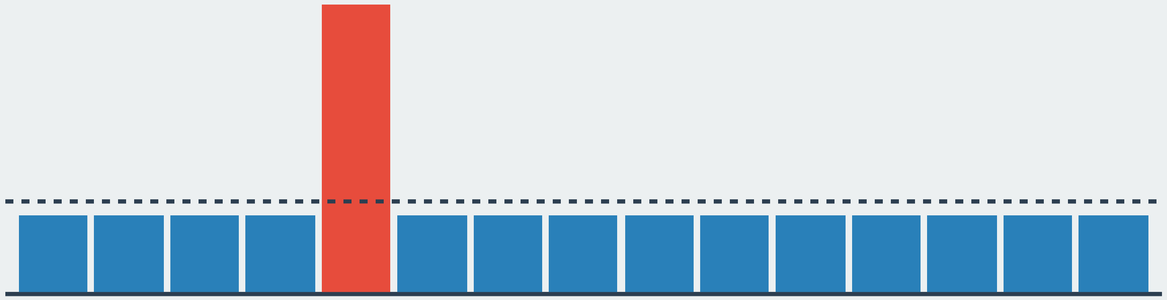


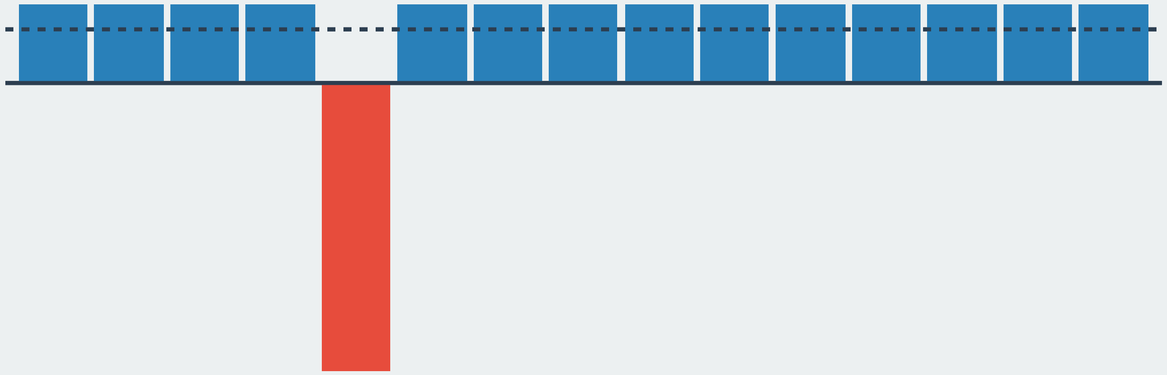


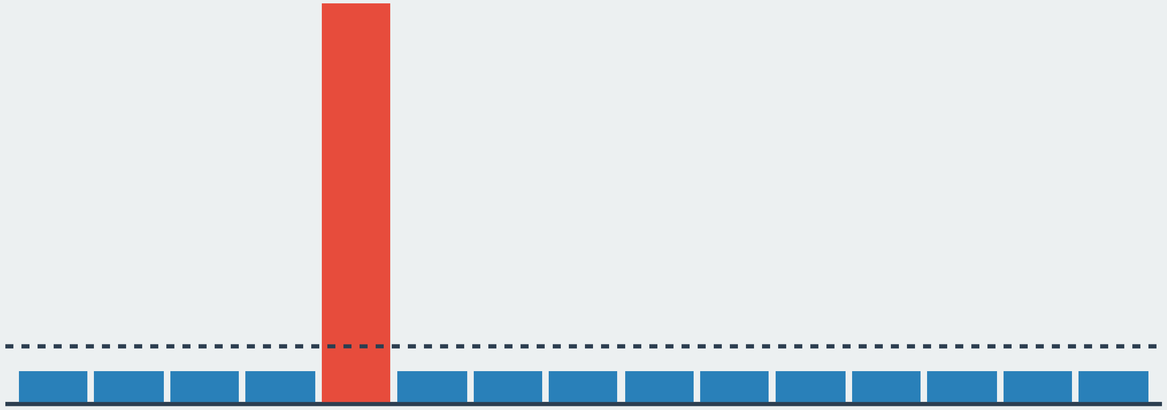

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

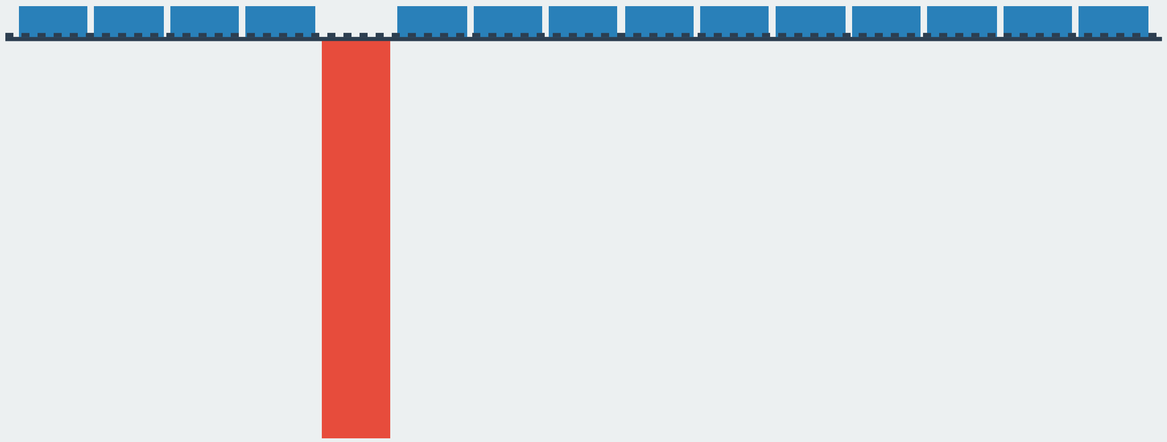

|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩
|0⟩|1⟩|2⟩|3⟩|4⟩|5⟩|6⟩|7⟩

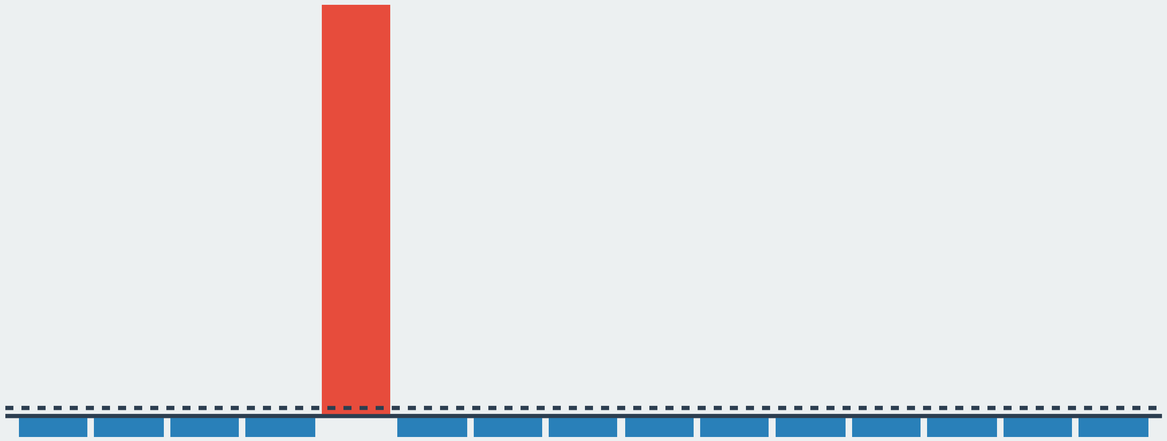


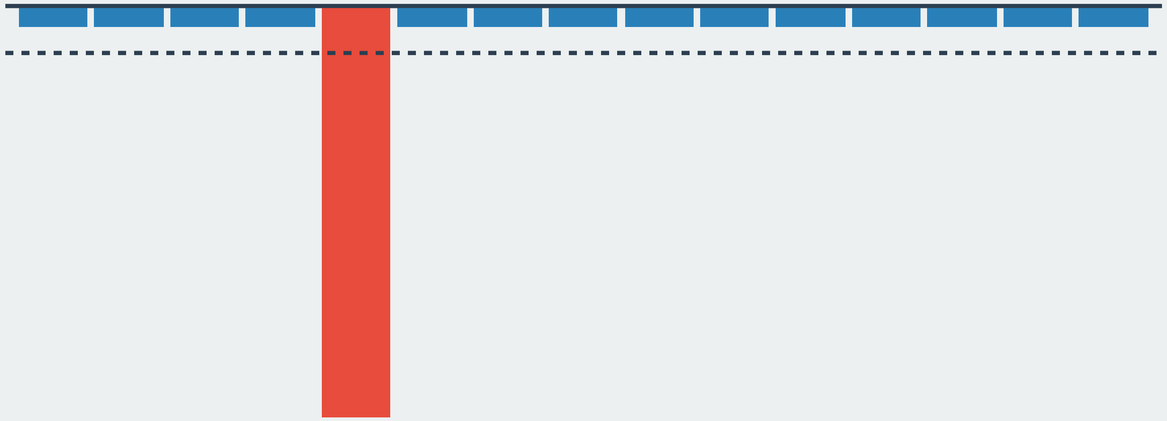


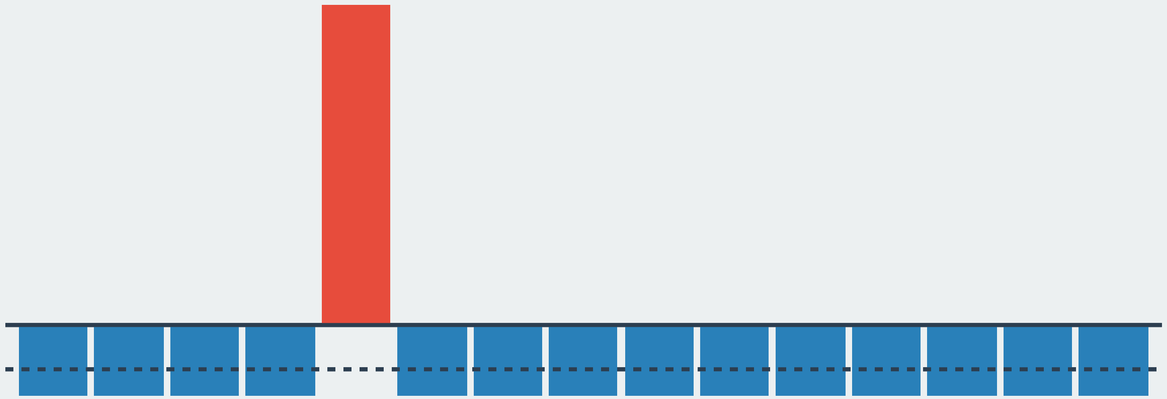


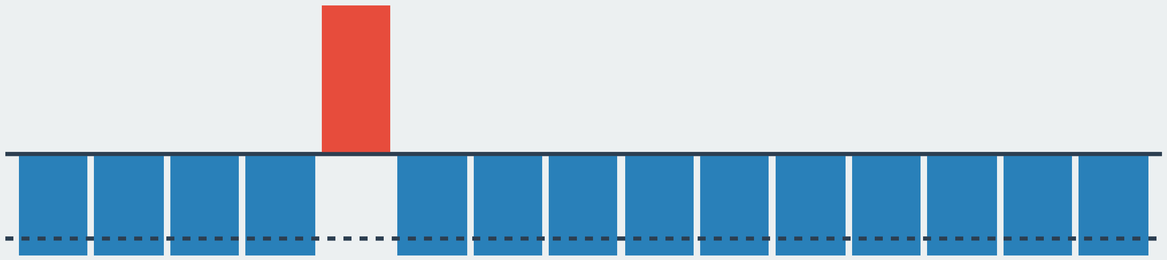


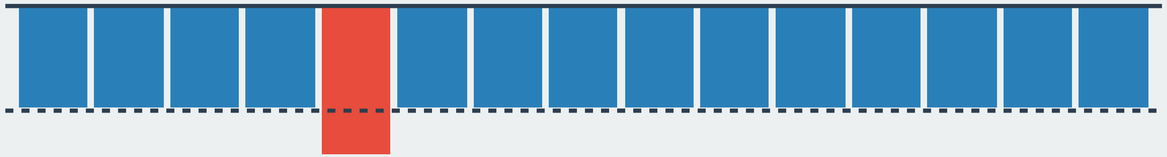


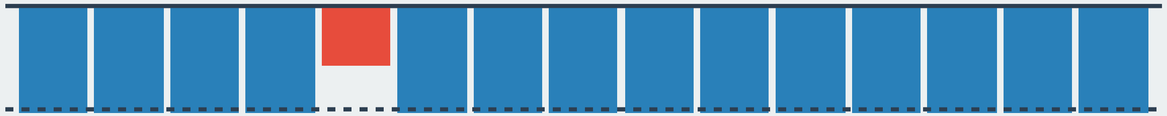




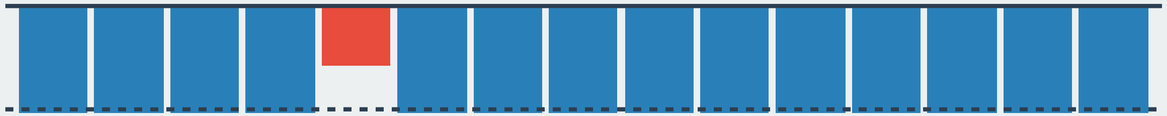








$$\approx \frac{\pi}{4}\sqrt{N/p}$$



naivno iskanje	Groverjev algoritem

naivno iskanje	Groverjev algoritem
N/p	

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	785

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	785
1 000 000 000 000	

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	785
1 000 000 000 000	785 000

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	785
1 000 000 000 000	785 000
12 dni	

naivno iskanje	Groverjev algoritem
N/p	$\approx \frac{\pi}{4}\sqrt{N/p}$
1 000 000	785
1 000 000 000 000	785 000
12 dni	1 sekunda

SHOROV
ALGORITEM

Peter Shor, 1959-

$$21 = ? \cdot ?$$

$$D(21,10) = 1$$

$$10^0 \bmod 21 = 1$$

$$10^0 \bmod 21 = 1$$
$$10^1 \bmod 21 = 10$$

$$10^0 \bmod 21 = 1$$
$$10^1 \bmod 21 = 10$$
$$10^2 \bmod 21 = 16$$

$10^{0} \bmod 21 = 1$

$10^{1} \bmod 21 = 10$

$10^{2} \bmod 21 = 16$

$10^{3} \bmod 21 = 13$

$10^{4} \bmod 21 = 4$

$10^{5} \bmod 21 = 19$

$10^{6} \bmod 21 = 1$

$10^{7} \bmod 21 = 10$

$10^{8} \bmod 21 = 16$

$10^{9} \bmod 21 = 13$

$10^{10} \bmod 21 = 4$

$10^{11} \bmod 21 = 19$

$10^{12} \bmod 21 = 1$

$10^{13} \bmod 21 = 10$

$10^{14} \bmod 21 = 16$

$10^{15} \bmod 21 = 13$

$10^{16} \bmod 21 = 4$

$10^{17} \bmod 21 = 19$

$10^{18} \bmod 21 = 1$

$10^{19} \bmod 21 = 10$

$10^{20} \bmod 21 = 16$

$10^{21} \bmod 21 = 13$

$10^{22} \bmod 21 = 4$

$10^{23} \bmod 21 = 19$

$$10^6 \bmod 21 = 1$$

$$10^6 \bmod 21 = 1$$

$$(10^6 - 1) \bmod 21 = 0$$

$$10^6 \bmod 21 = 1$$

$$(10^6 - 1) \bmod 21 = 0$$

$$(10^3 - 1)(10^3 + 1) \bmod 21 = 0$$

$$D(10^3 - 1, 21) = 3$$

$$D(10^3 - 1, 21) = 7$$

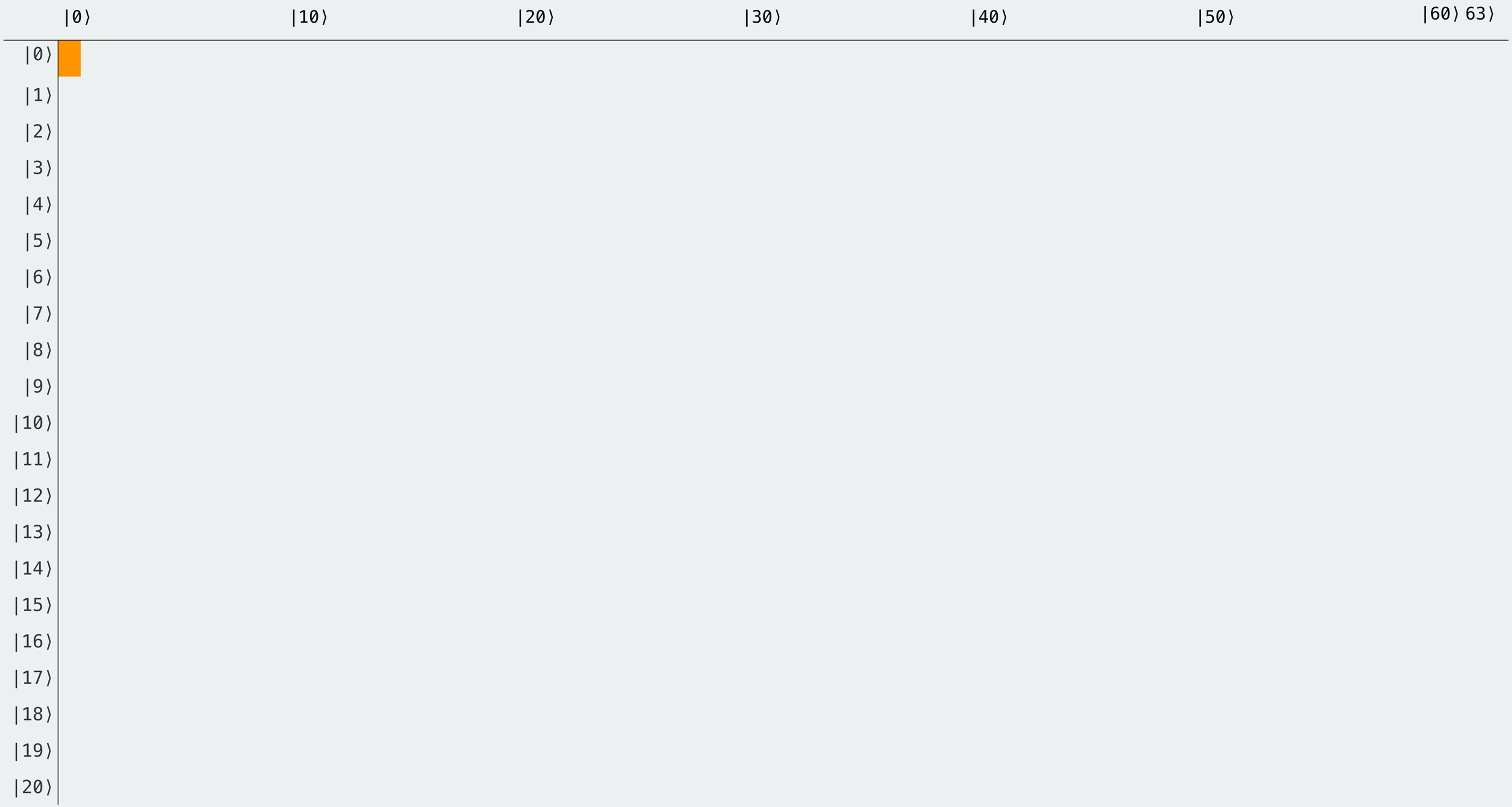
$10^2 \bmod 21 \quad \cdots \quad 10^{64} \bmod 21$

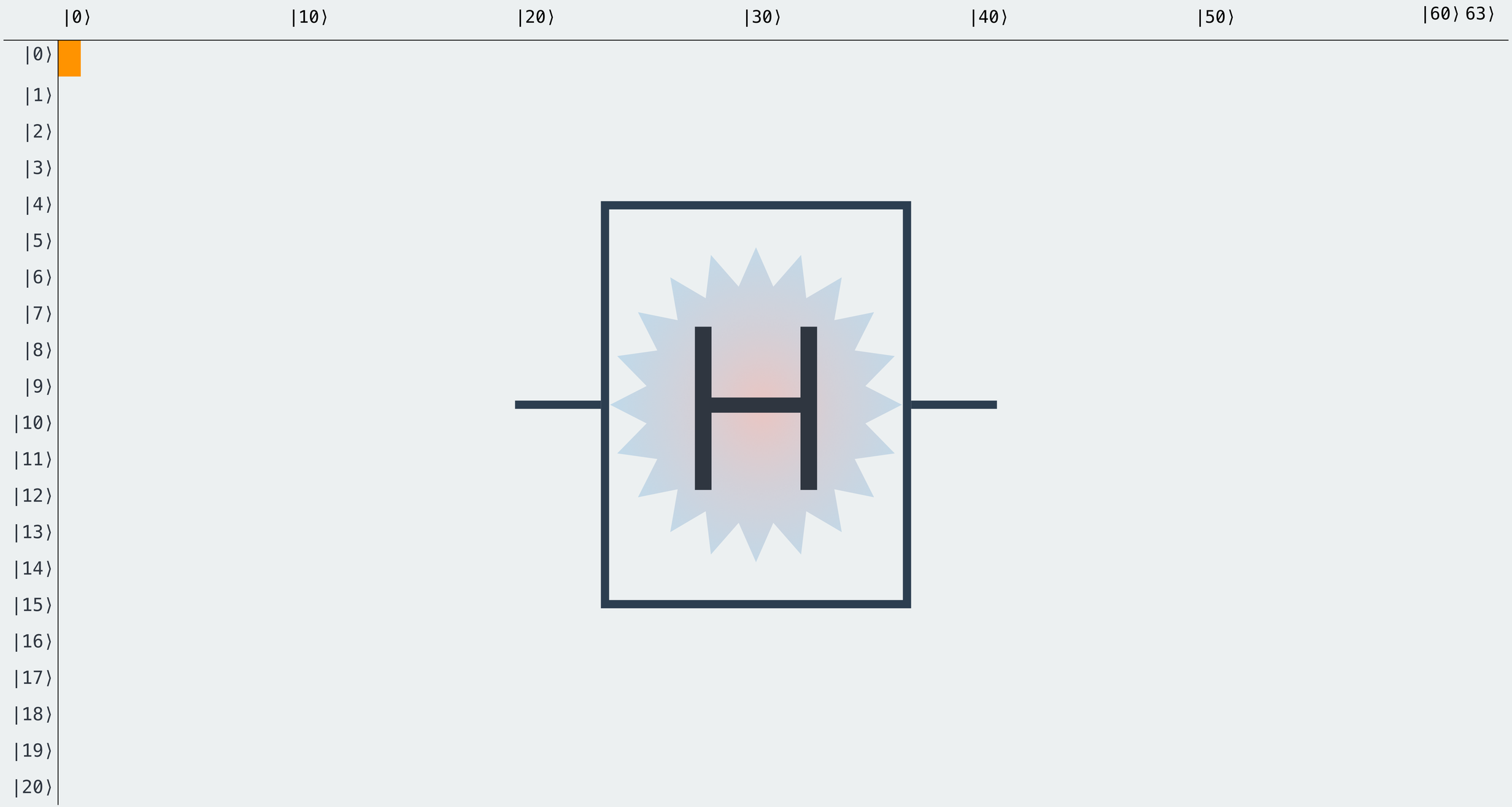
$10^2 \bmod 21 \quad \cdots \quad 10^{64} \bmod 21$

$21 \bmod 2 \quad \cdots \quad 21 \bmod 20$

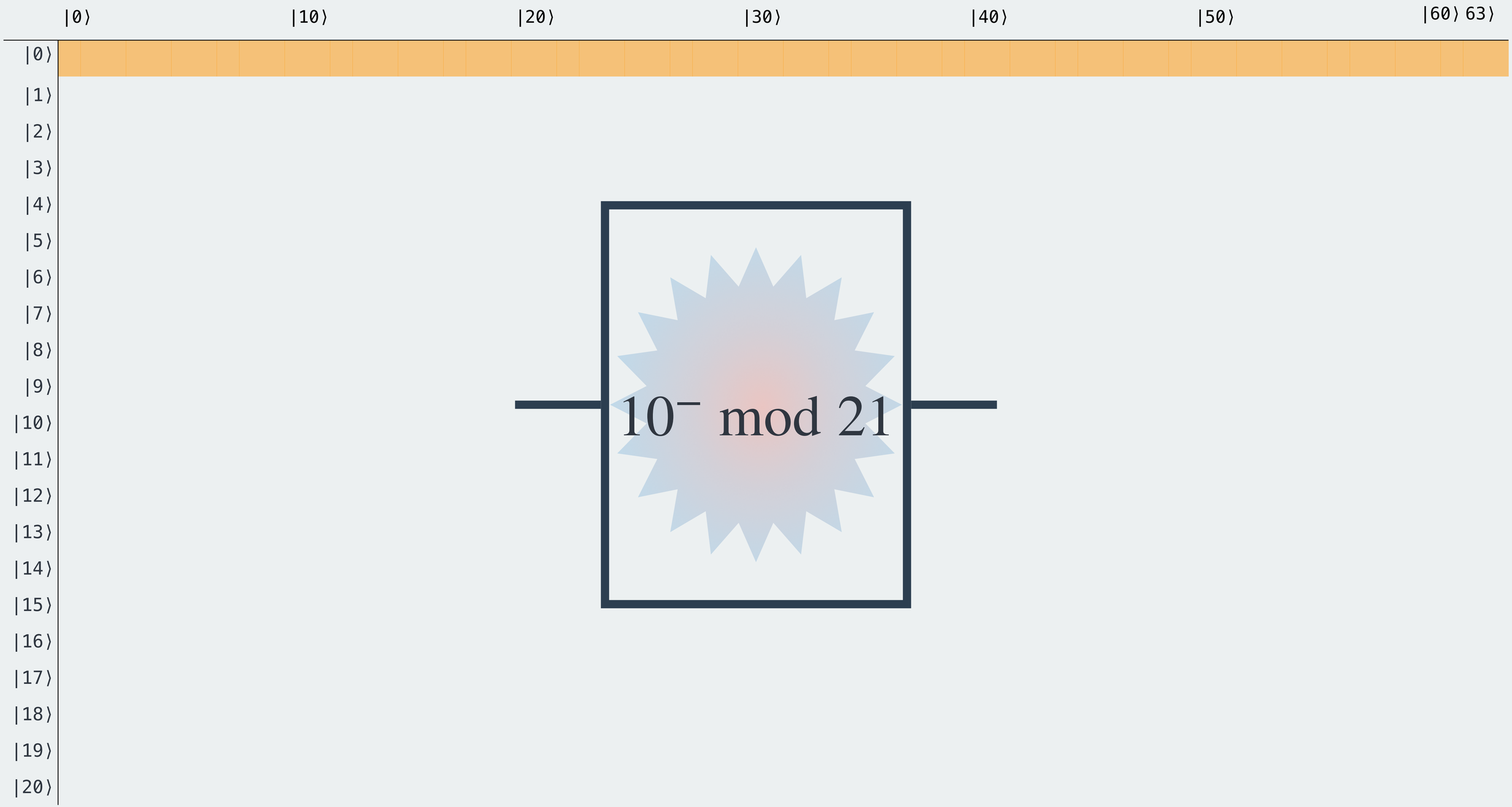
$10^2 \bmod 21 \quad \cdots \quad 10^{64} \bmod 21$

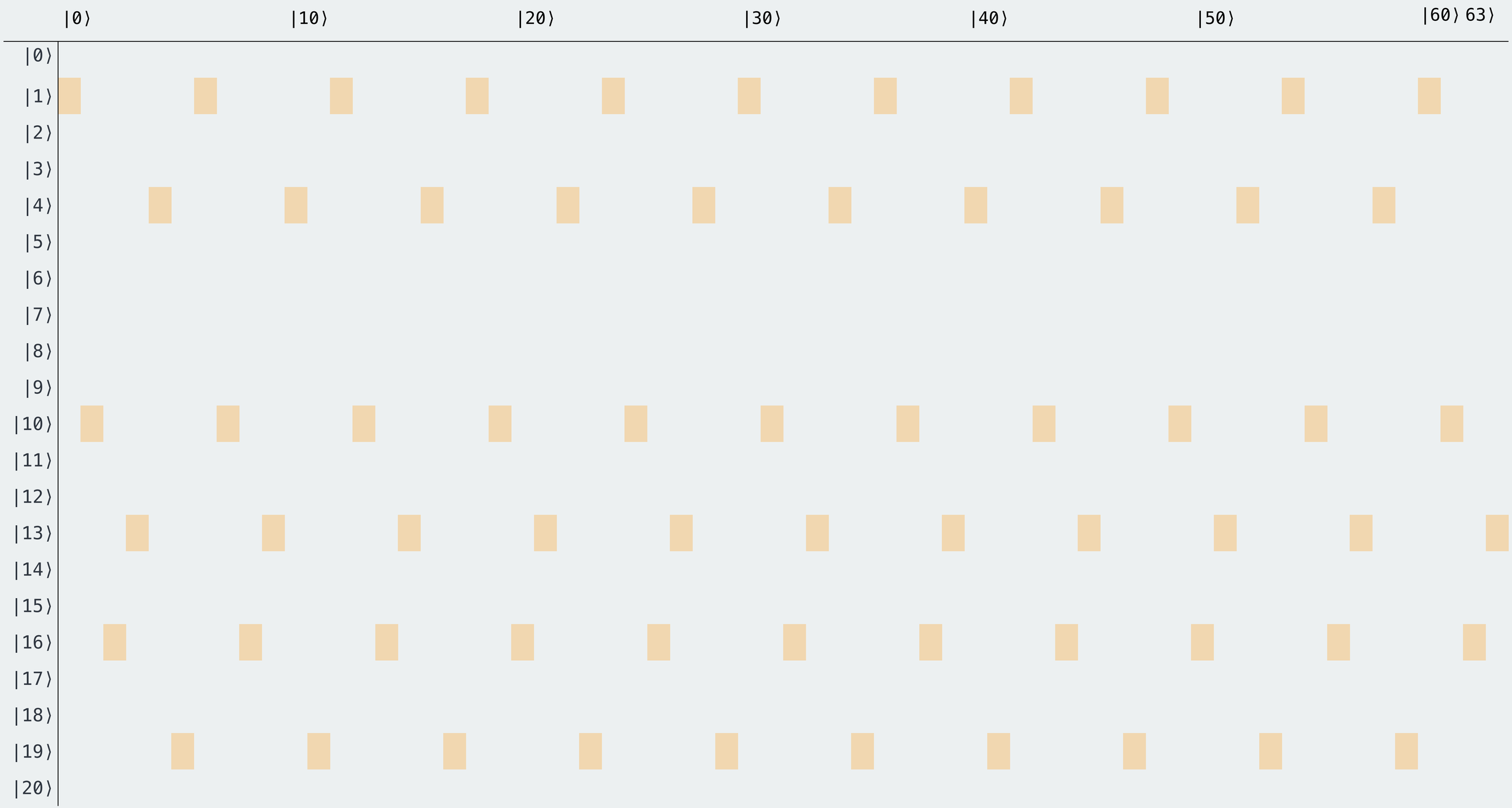
$21 \bmod 2 \quad \cdots \quad 21 \bmod 20$

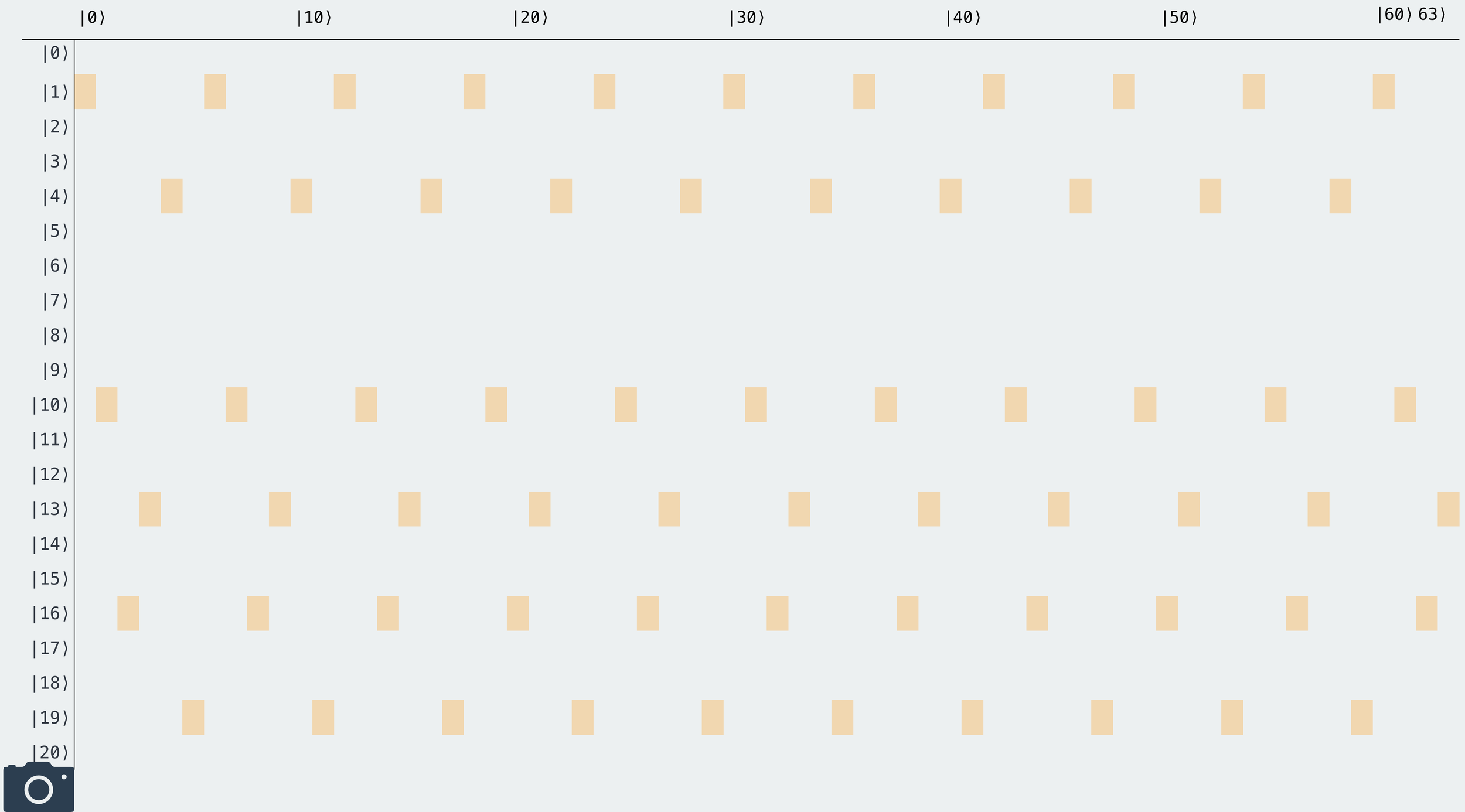

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

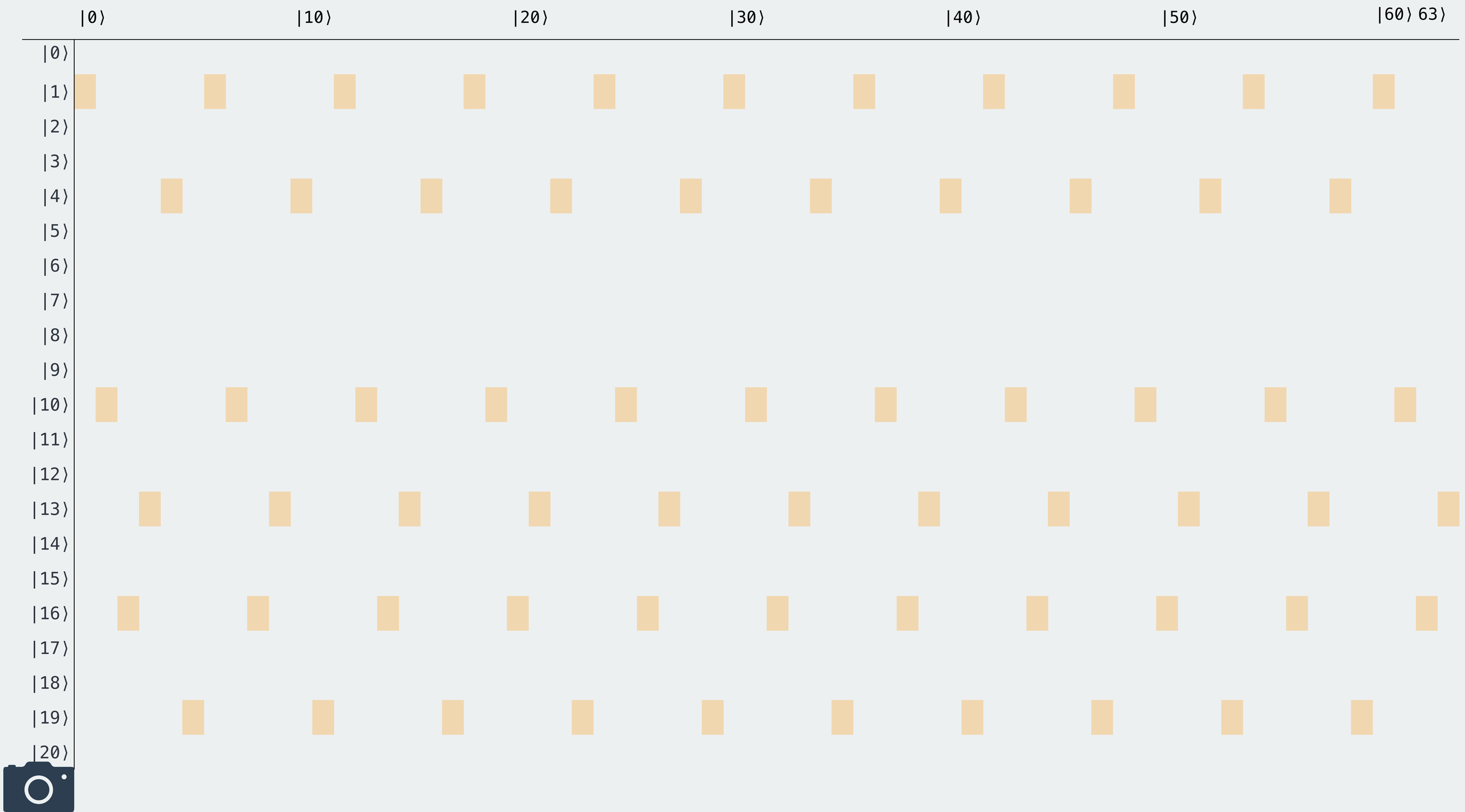

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
H

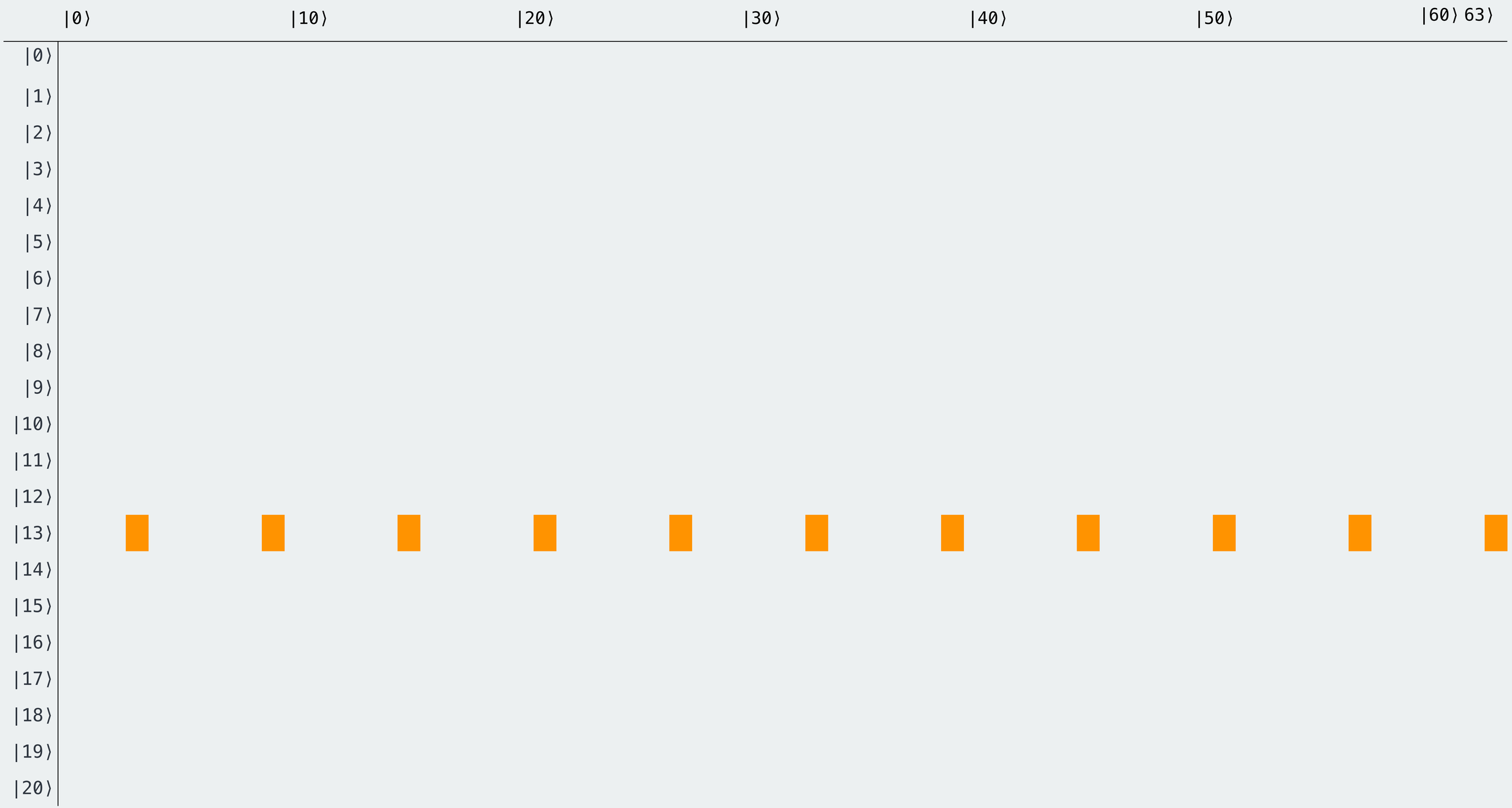

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩
63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

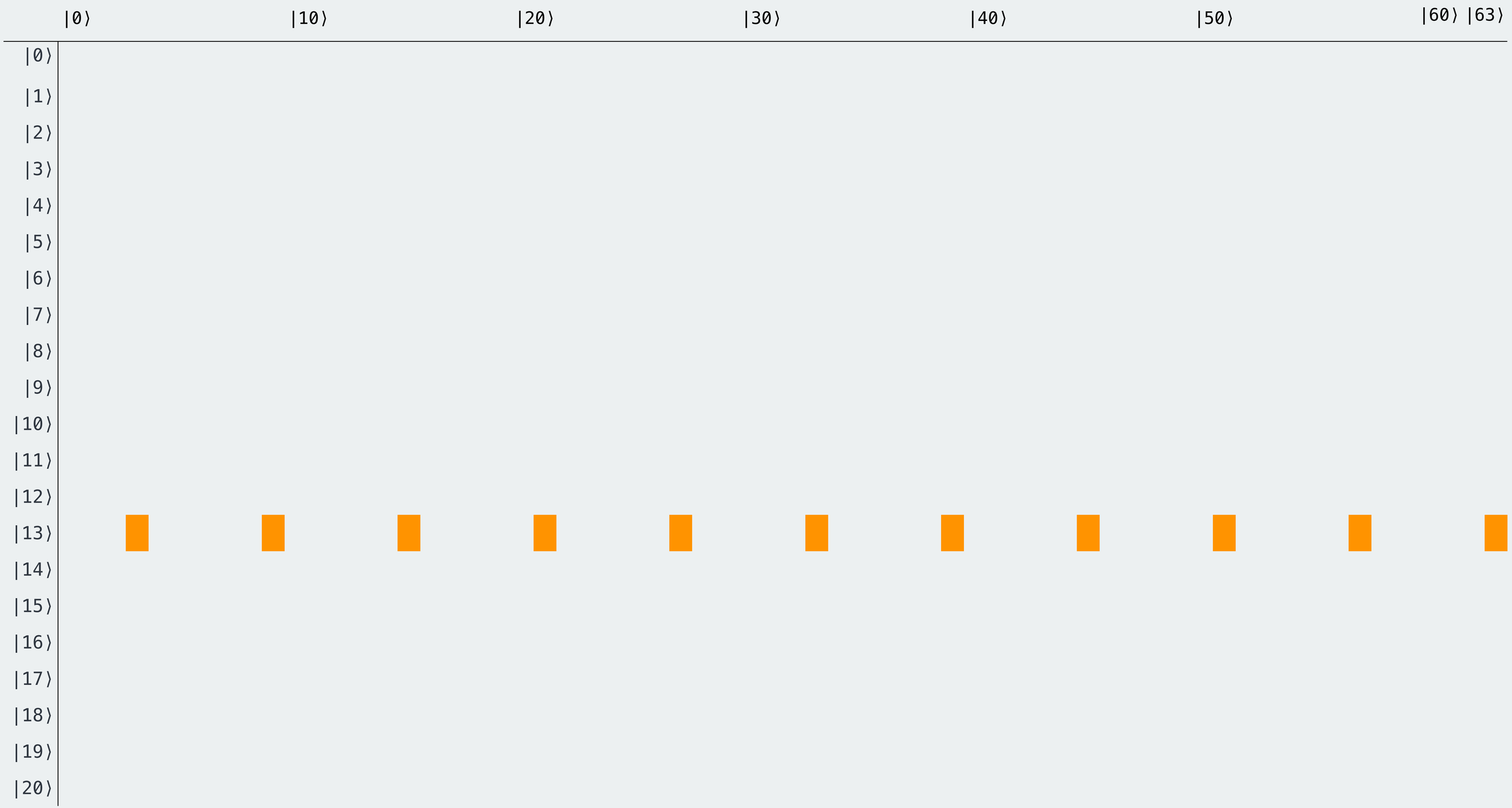

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
10⁻ mod 21

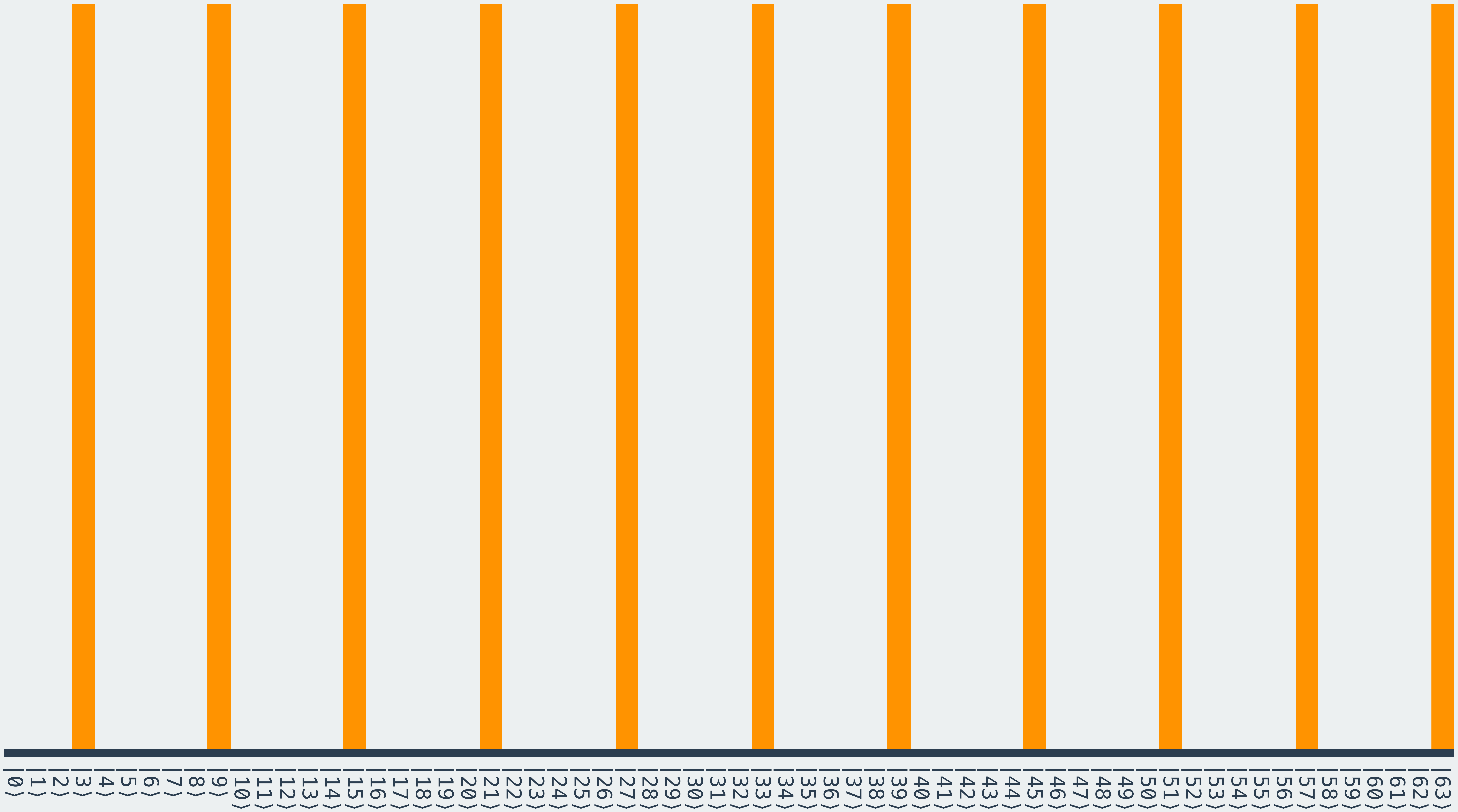

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

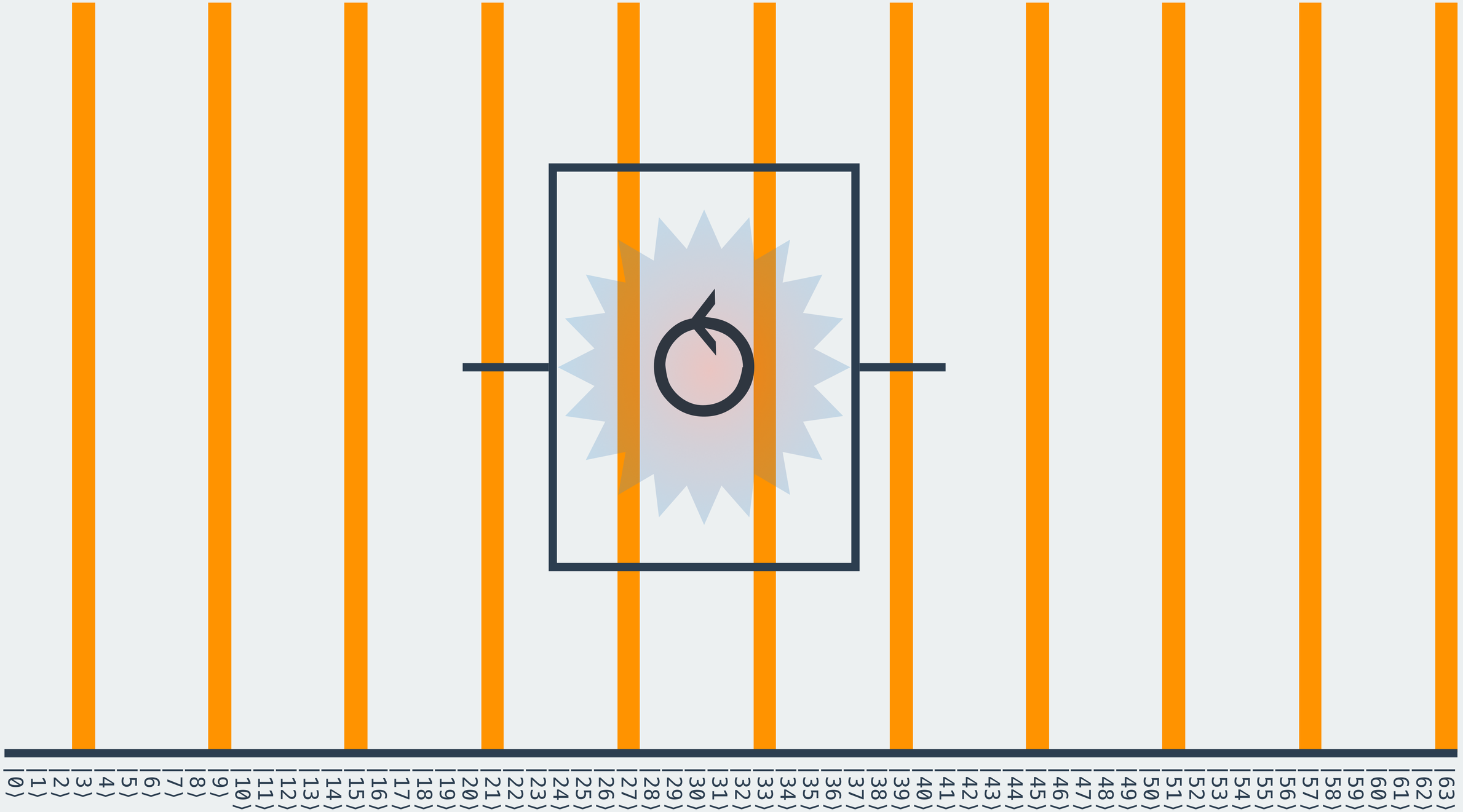

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

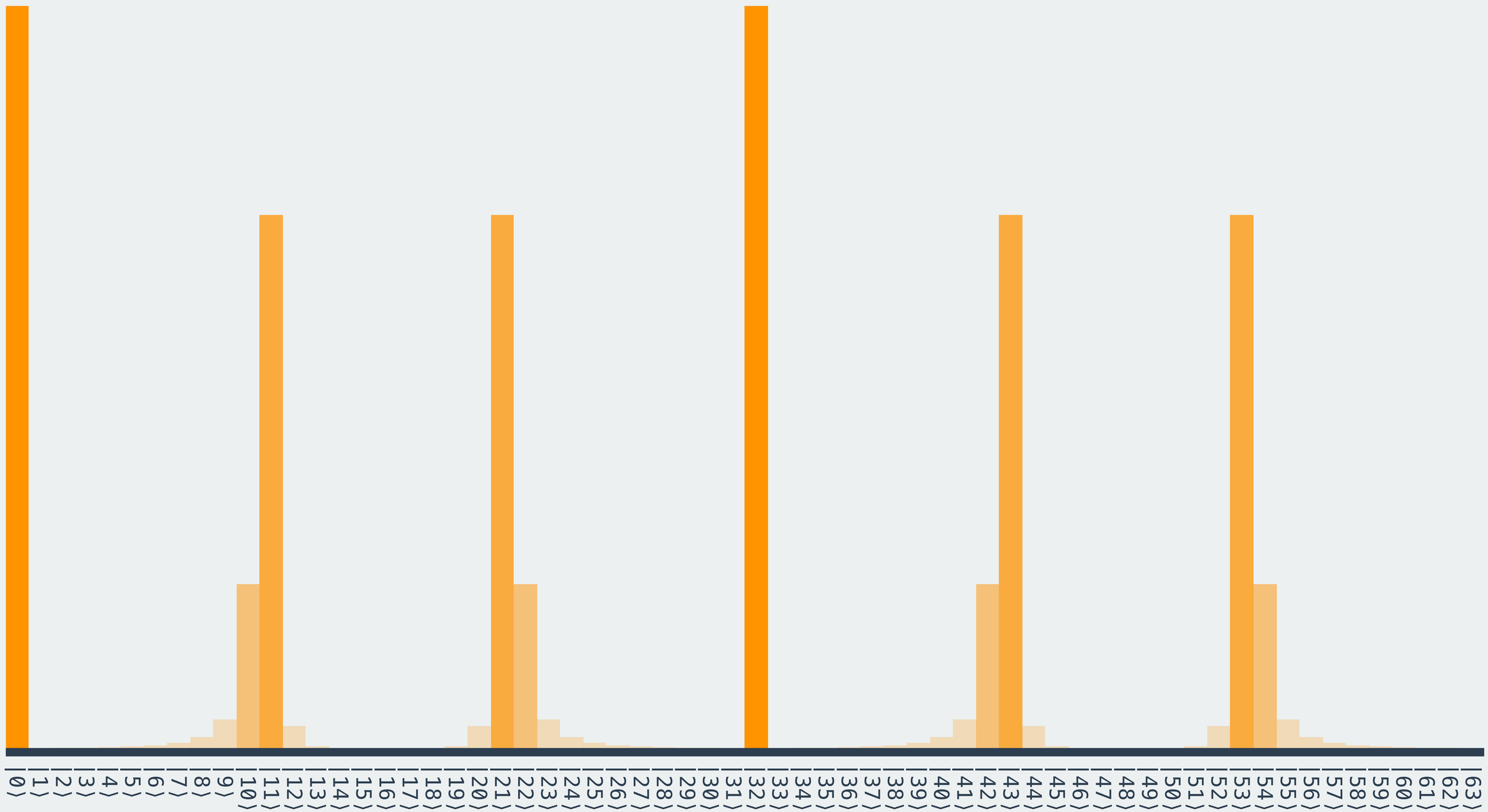

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

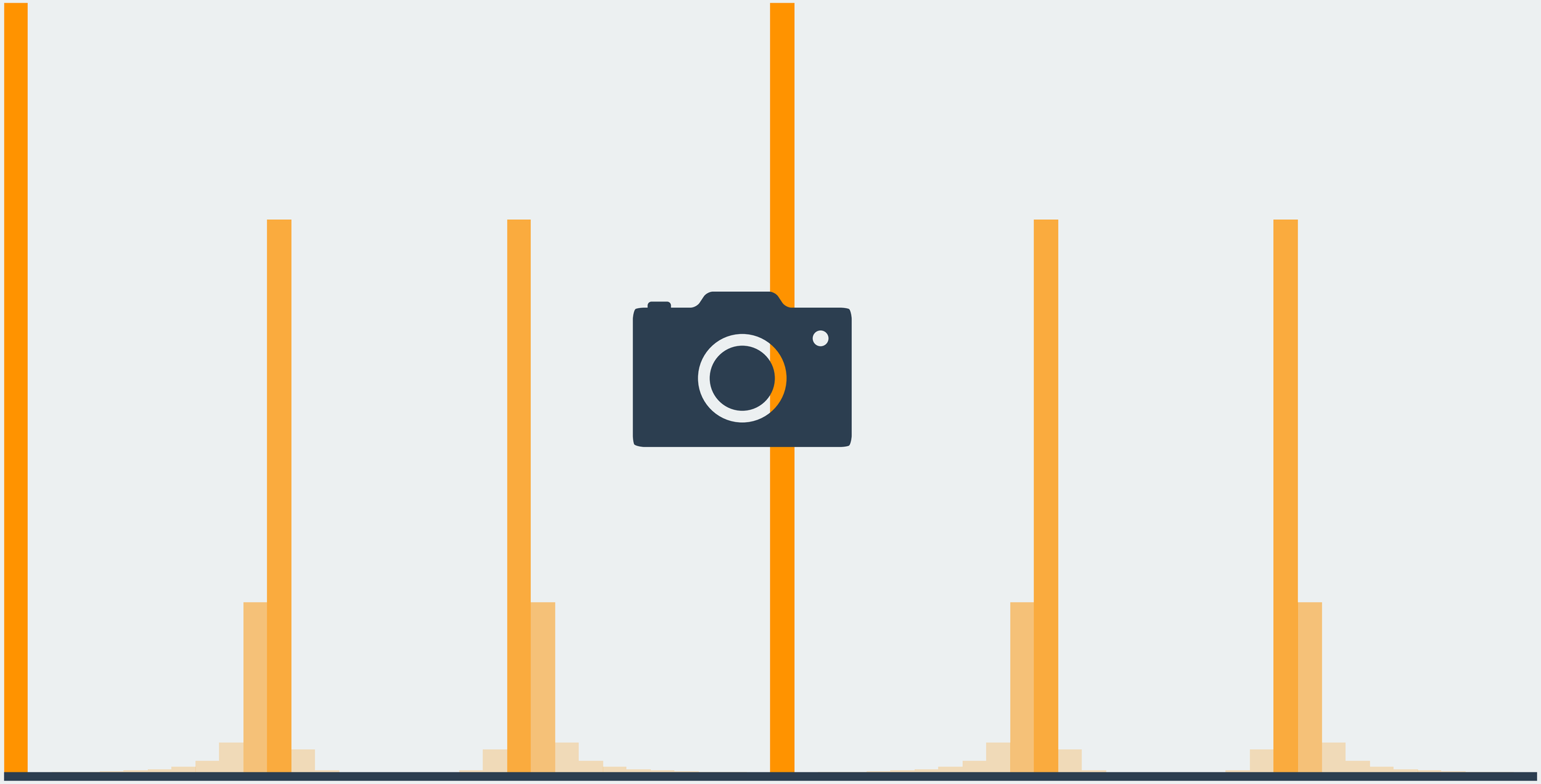

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩ 63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

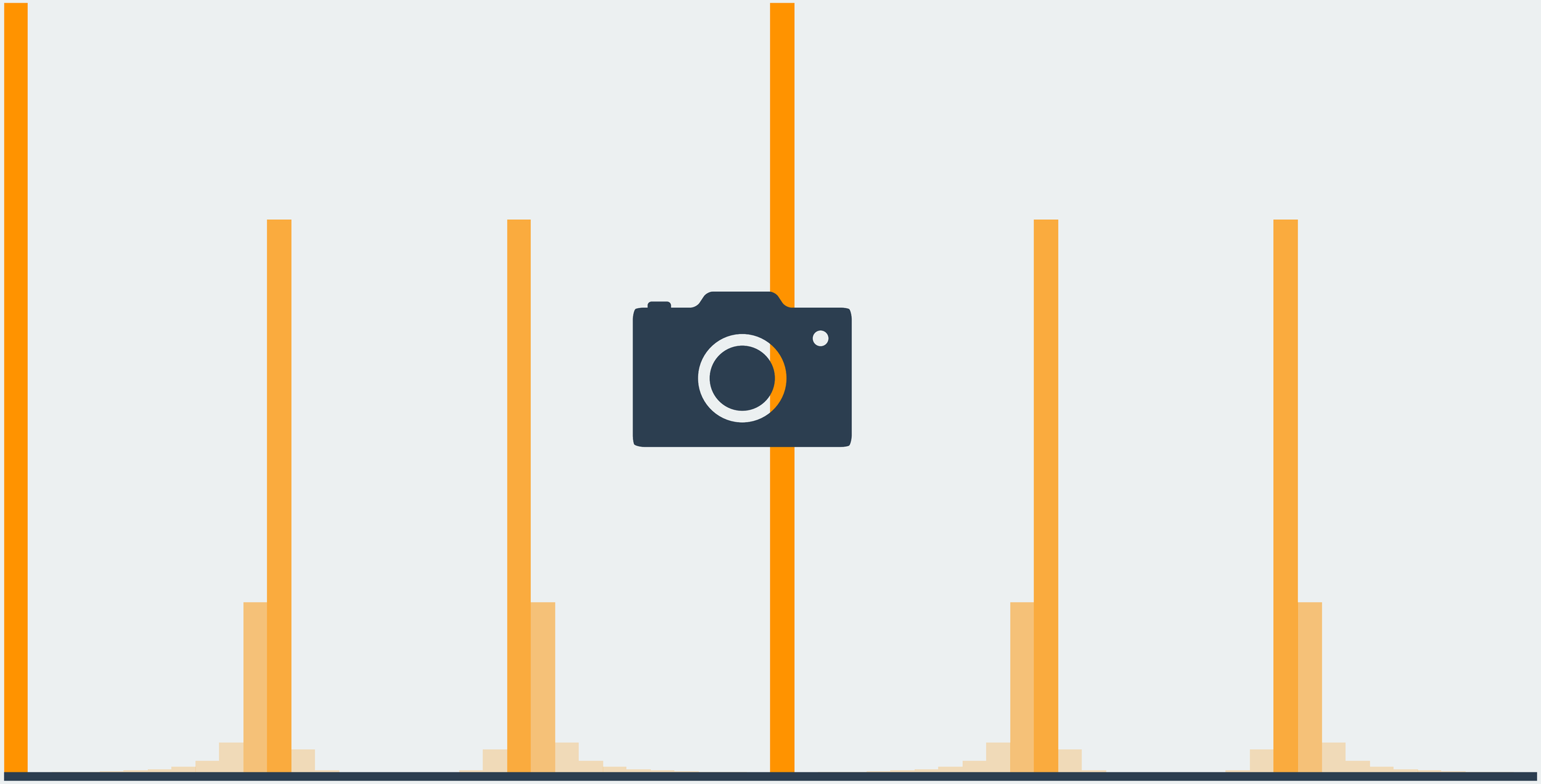

|0⟩
|10⟩
|20⟩
|30⟩
|40⟩
|50⟩
|60⟩
|63⟩
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩

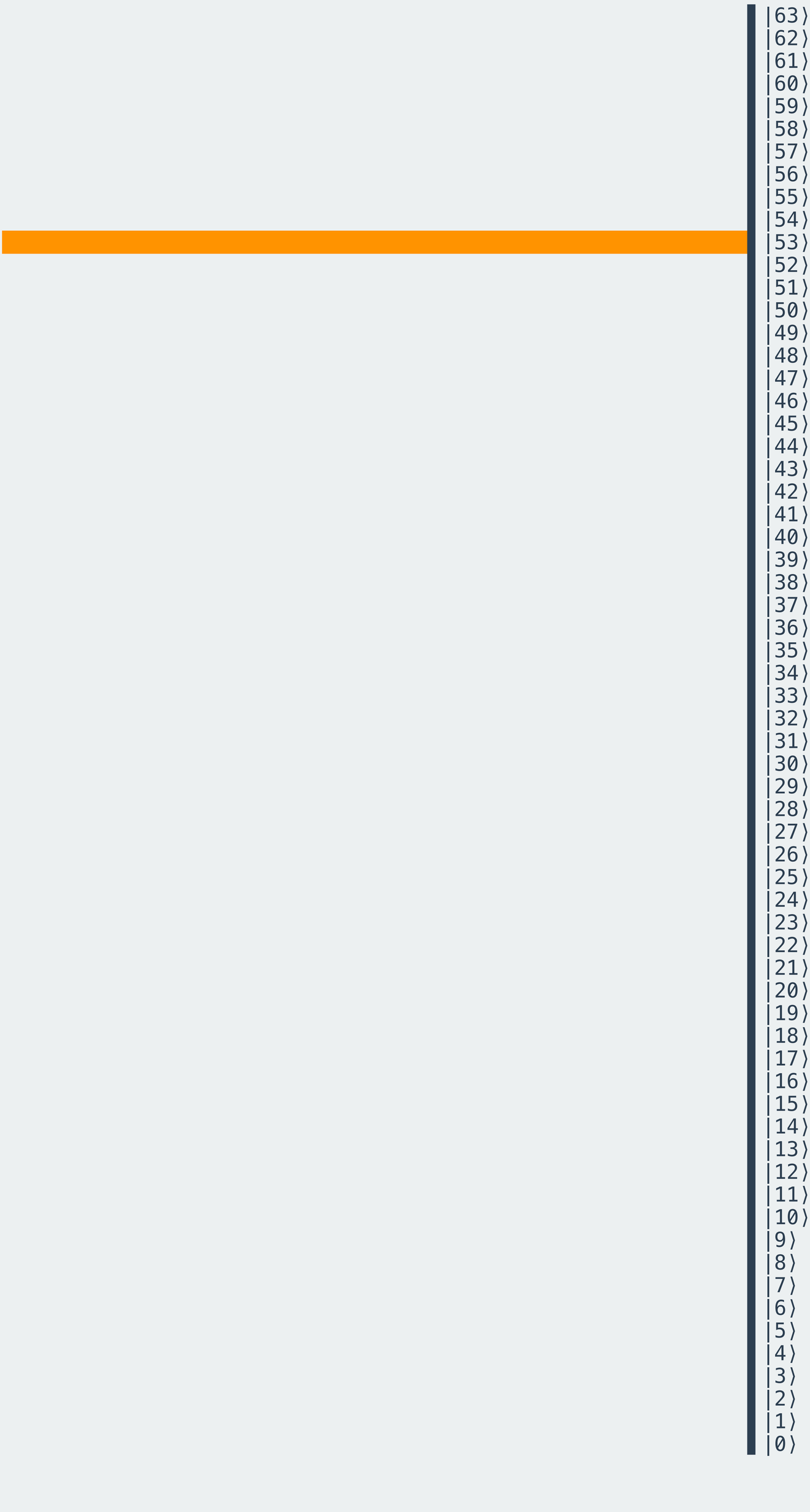

|0⟩ |1⟩ |2⟩ |3⟩ |4⟩ |5⟩ |6⟩ |7⟩ |8⟩ |9⟩ |10⟩ |11⟩ |12⟩ |13⟩ |14⟩ |15⟩ |16⟩ |17⟩ |18⟩ |19⟩ |20⟩ |21⟩ |22⟩ |23⟩ |24⟩ |25⟩ |26⟩ |27⟩ |28⟩ |29⟩ |30⟩ |31⟩ |32⟩ |33⟩ |34⟩ |35⟩ |36⟩ |37⟩ |38⟩ |39⟩ |40⟩ |41⟩ |42⟩ |43⟩ |44⟩ |45⟩ |46⟩ |47⟩ |48⟩ |49⟩ |50⟩ |51⟩ |52⟩ |53⟩ |54⟩ |55⟩ |56⟩ |57⟩ |58⟩ |59⟩ |60⟩ |61⟩ |62⟩ |63⟩


|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
|21⟩
|22⟩
|23⟩
|24⟩
|25⟩
|26⟩
|27⟩
|28⟩
|29⟩
|30⟩
|31⟩
|32⟩
|33⟩
|34⟩
|35⟩
|36⟩
|37⟩
|38⟩
|39⟩
|40⟩
|41⟩
|42⟩
|43⟩
|44⟩
|45⟩
|46⟩
|47⟩
|48⟩
|49⟩
|50⟩
|51⟩
|52⟩
|53⟩
|54⟩
|55⟩
|56⟩
|57⟩
|58⟩
|59⟩
|60⟩
|61⟩
|62⟩
|63⟩


|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
|21⟩
|22⟩
|23⟩
|24⟩
|25⟩
|26⟩
|27⟩
|28⟩
|29⟩
|30⟩
|31⟩
|32⟩
|33⟩
|34⟩
|35⟩
|36⟩
|37⟩
|38⟩
|39⟩
|40⟩
|41⟩
|42⟩
|43⟩
|44⟩
|45⟩
|46⟩
|47⟩
|48⟩
|49⟩
|50⟩
|51⟩
|52⟩
|53⟩
|54⟩
|55⟩
|56⟩
|57⟩
|58⟩
|59⟩
|60⟩
|61⟩
|62⟩
|63⟩


|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
|21⟩
|22⟩
|23⟩
|24⟩
|25⟩
|26⟩
|27⟩
|28⟩
|29⟩
|30⟩
|31⟩
|32⟩
|33⟩
|34⟩
|35⟩
|36⟩
|37⟩
|38⟩
|39⟩
|40⟩
|41⟩
|42⟩
|43⟩
|44⟩
|45⟩
|46⟩
|47⟩
|48⟩
|49⟩
|50⟩
|51⟩
|52⟩
|53⟩
|54⟩
|55⟩
|56⟩
|57⟩
|58⟩
|59⟩
|60⟩
|61⟩
|62⟩
|63⟩


|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩
|16⟩
|17⟩
|18⟩
|19⟩
|20⟩
|21⟩
|22⟩
|23⟩
|24⟩
|25⟩
|26⟩
|27⟩
|28⟩
|29⟩
|30⟩
|31⟩
|32⟩
|33⟩
|34⟩
|35⟩
|36⟩
|37⟩
|38⟩
|39⟩
|40⟩
|41⟩
|42⟩
|43⟩
|44⟩
|45⟩
|46⟩
|47⟩
|48⟩
|49⟩
|50⟩
|51⟩
|52⟩
|53⟩
|54⟩
|55⟩
|56⟩
|57⟩
|58⟩
|59⟩
|60⟩
|61⟩
|62⟩
|63⟩


|63⟩
|62⟩
|61⟩
|60⟩
|59⟩
|58⟩
|57⟩
|56⟩
|55⟩
|54⟩
|53⟩
|52⟩
|51⟩
|50⟩
|49⟩
|48⟩
|47⟩
|46⟩
|45⟩
|44⟩
|43⟩
|42⟩
|41⟩
|40⟩
|39⟩
|38⟩
|37⟩
|36⟩
|35⟩
|34⟩
|33⟩
|32⟩
|31⟩
|30⟩
|29⟩
|28⟩
|27⟩
|26⟩
|25⟩
|24⟩
|23⟩
|22⟩
|21⟩
|20⟩
|19⟩
|18⟩
|17⟩
|16⟩
|15⟩
|14⟩
|13⟩
|12⟩
|11⟩
|10⟩
|9⟩
|8⟩
|7⟩
|6⟩
|5⟩
|4⟩
|3⟩
|2⟩
|1⟩
|0⟩

$$\frac{53}{64}$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}}$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}} \approx \frac{1}{1} = 1$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}} \approx \frac{1}{1} = 1$$

$$= \frac{1}{1 + \frac{1}{4 + \frac{9}{11}}}$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}} \approx \frac{1}{1} = 1$$

$$= \frac{1}{1 + \frac{1}{4 + \frac{9}{11}}} \approx \frac{1}{1 + \frac{1}{4}} = \frac{4}{5}$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}} \approx \frac{1}{1} = 1$$

$$= \frac{1}{1 + \frac{1}{4 + \frac{9}{11}}} \approx \frac{1}{1 + \frac{1}{4}} = \frac{4}{5}$$

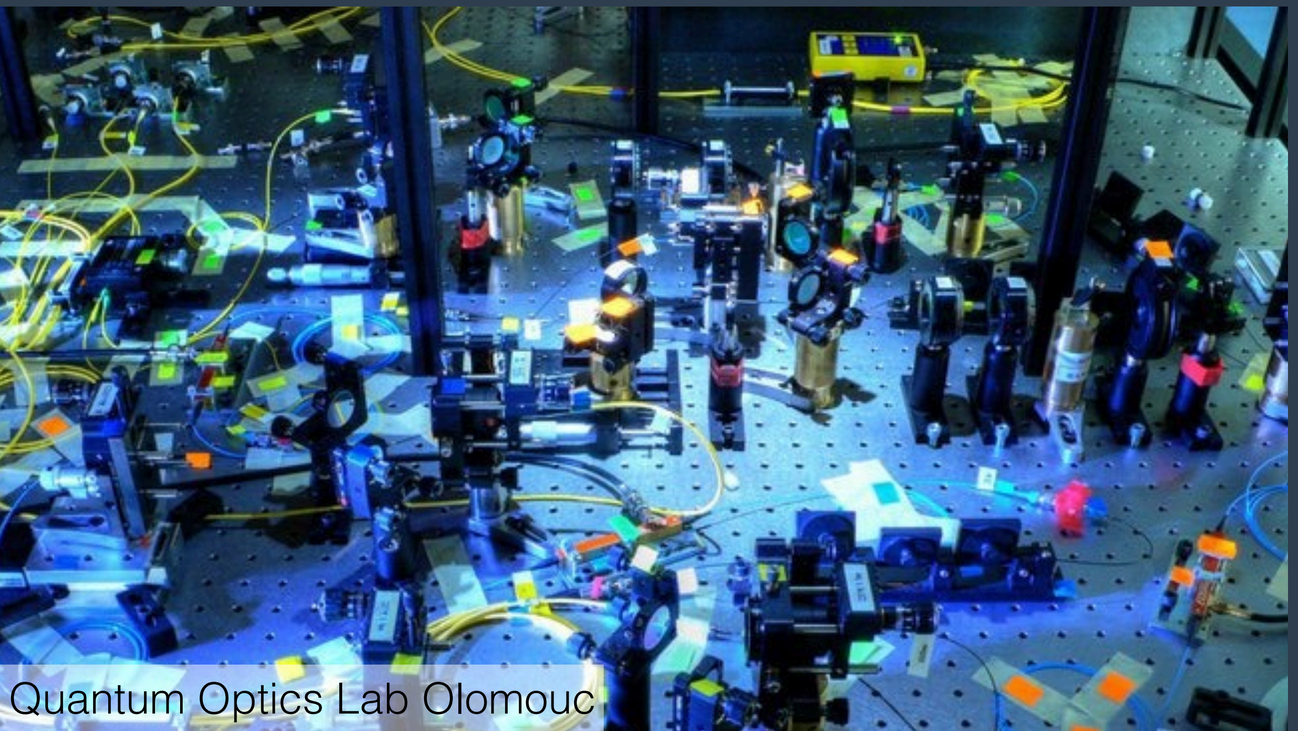
$$= \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{2}{9}}}}$$

$$\frac{53}{64} = \frac{1}{1 + \frac{11}{53}} \approx \frac{1}{1} = 1$$

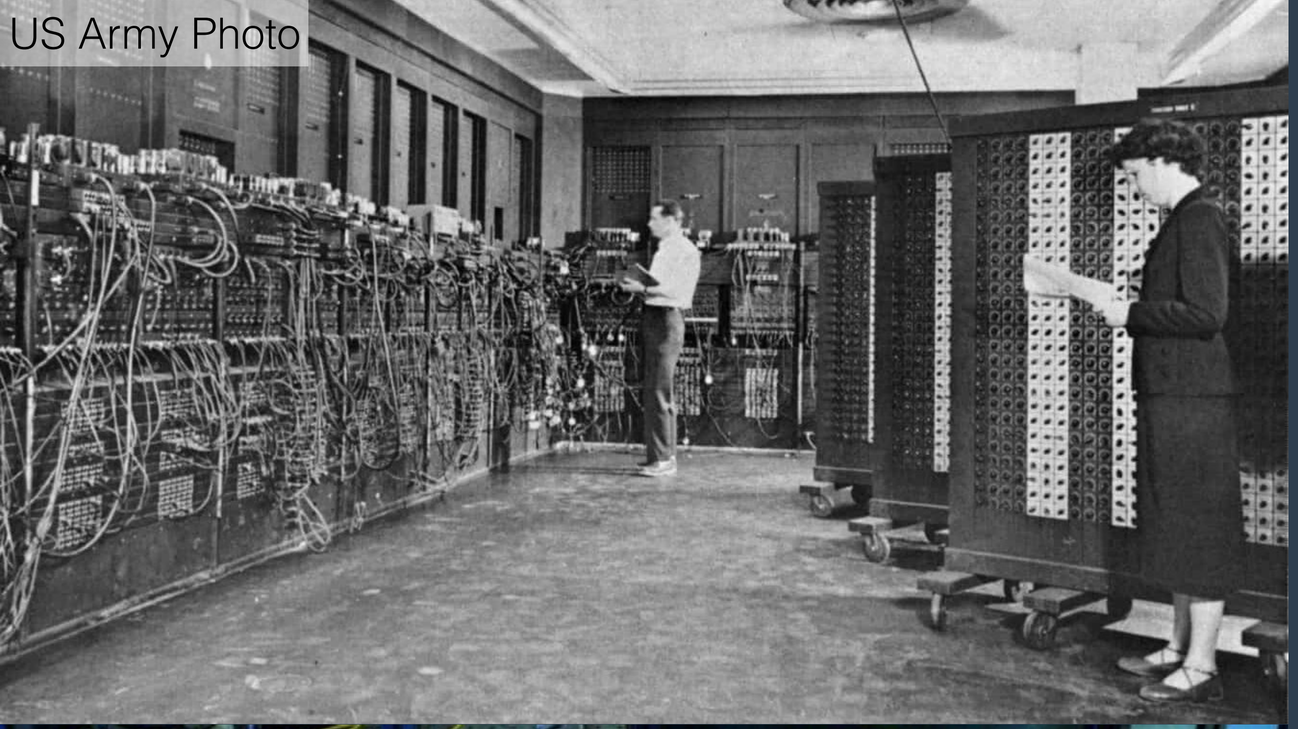
$$= \frac{1}{1 + \frac{1}{4 + \frac{9}{11}}} \approx \frac{1}{1 + \frac{1}{4}} = \frac{4}{5}$$

$$= \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{2}{9}}}} \approx \frac{1}{1 + \frac{1}{4 + \frac{1}{1}}} = \frac{5}{6}$$

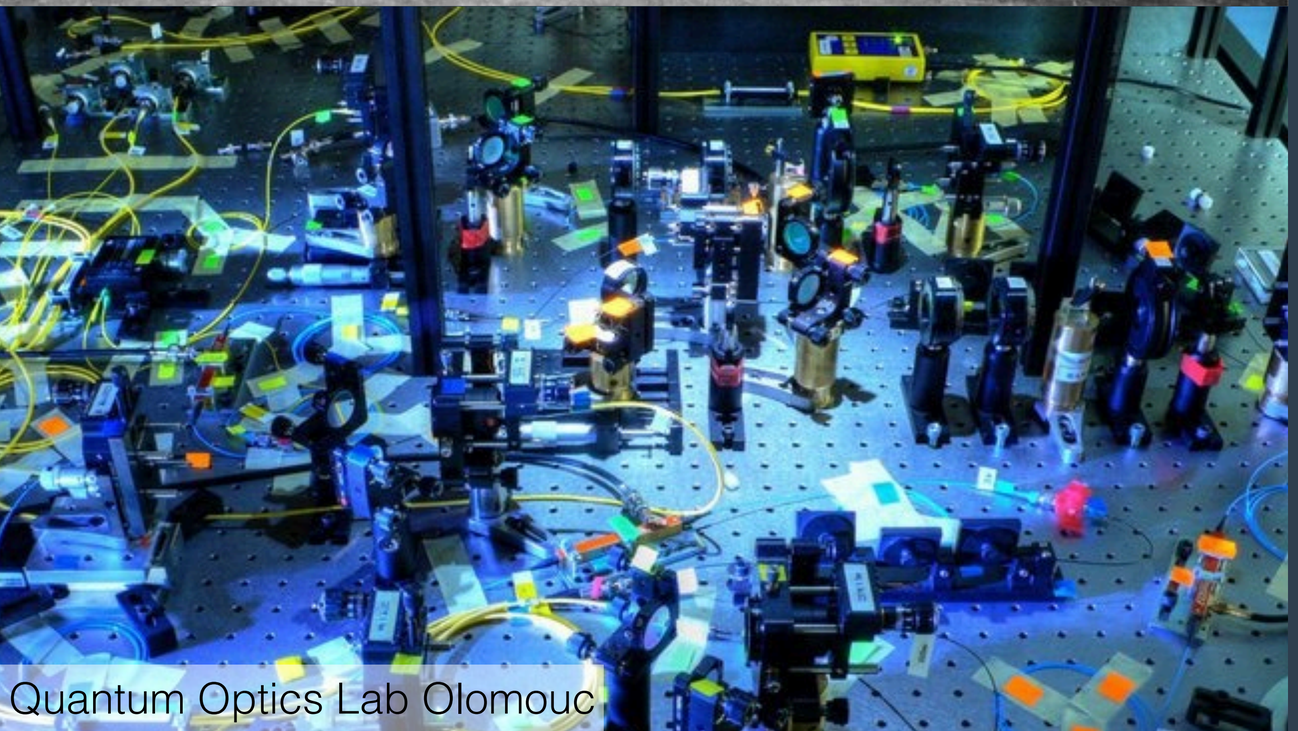
Shorov algoritem



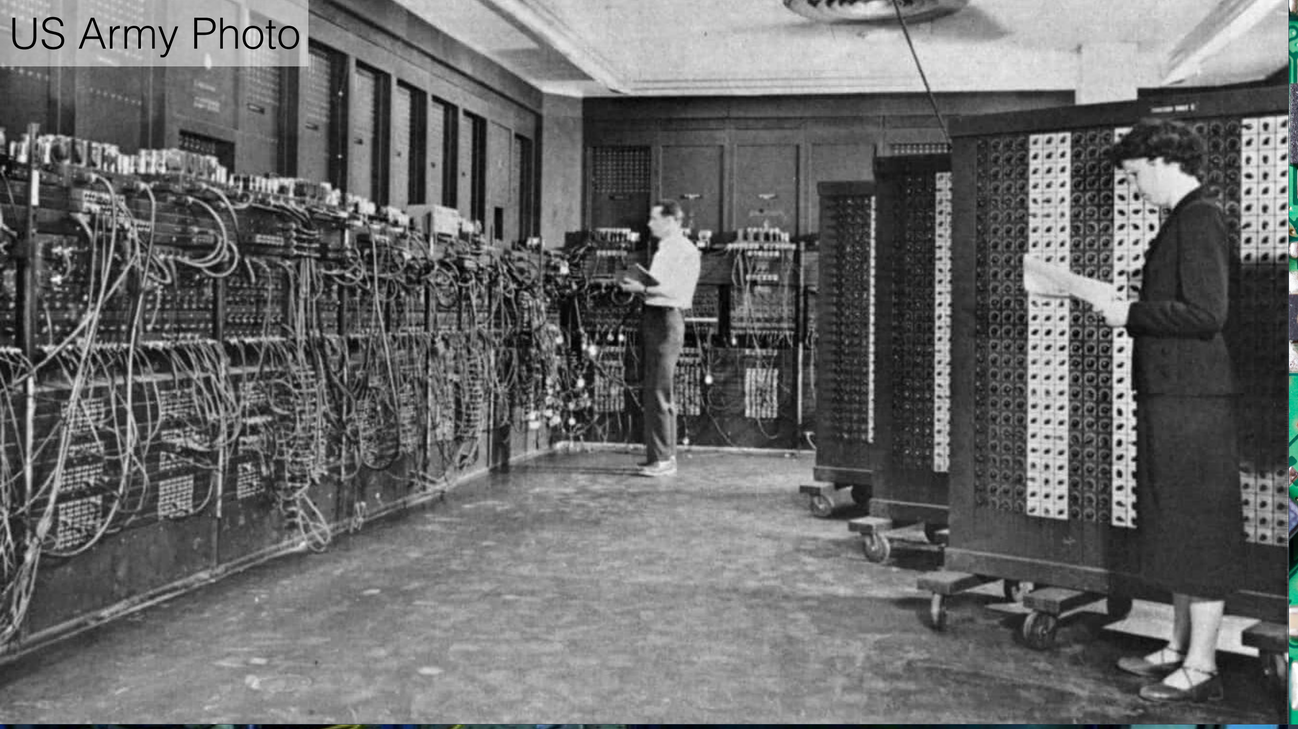
Quantum Optics Lab Olomouc



US Army Photo



Quantum Optics Lab Olomouc



US Army Photo

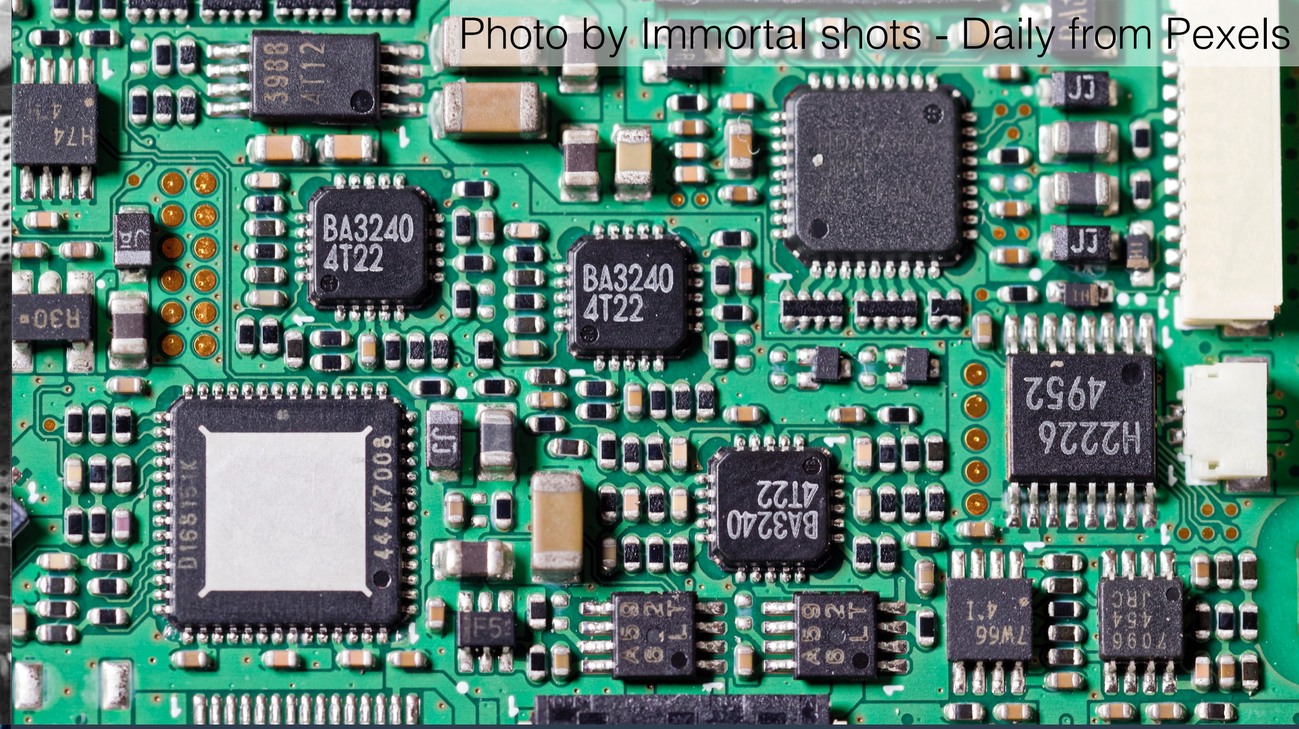
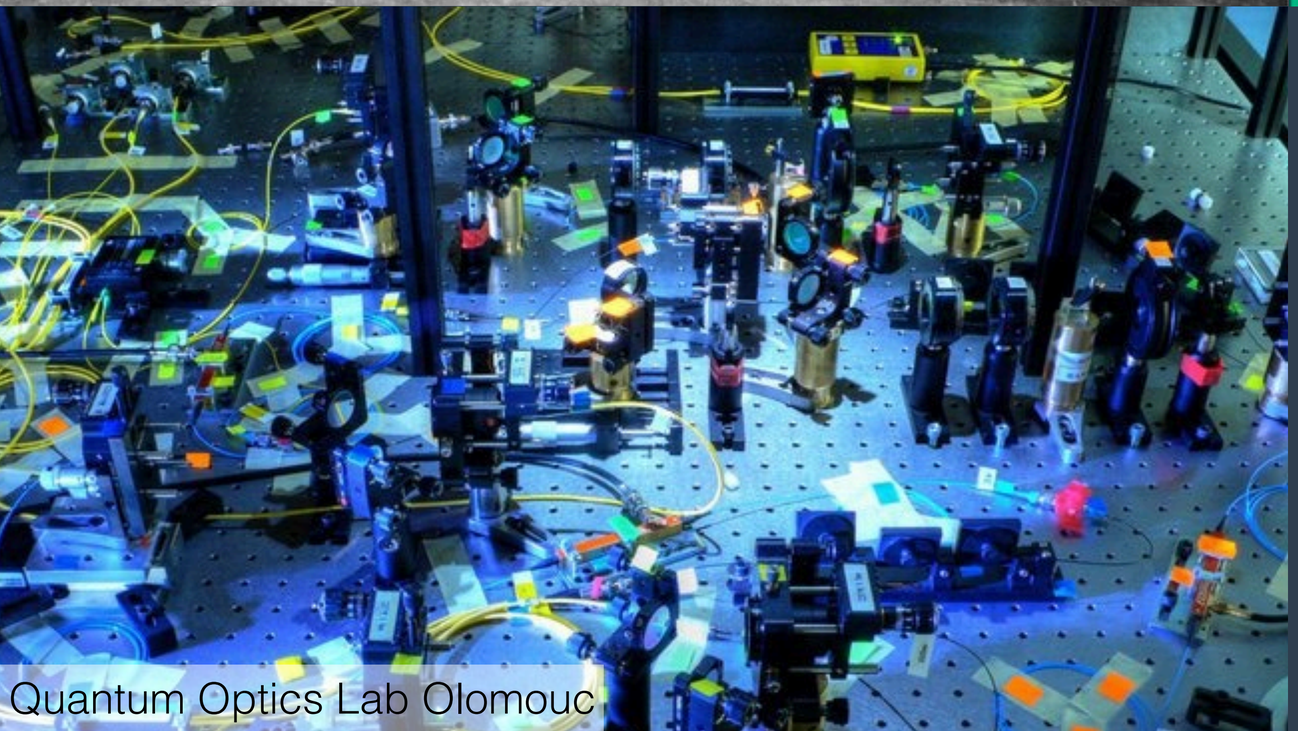
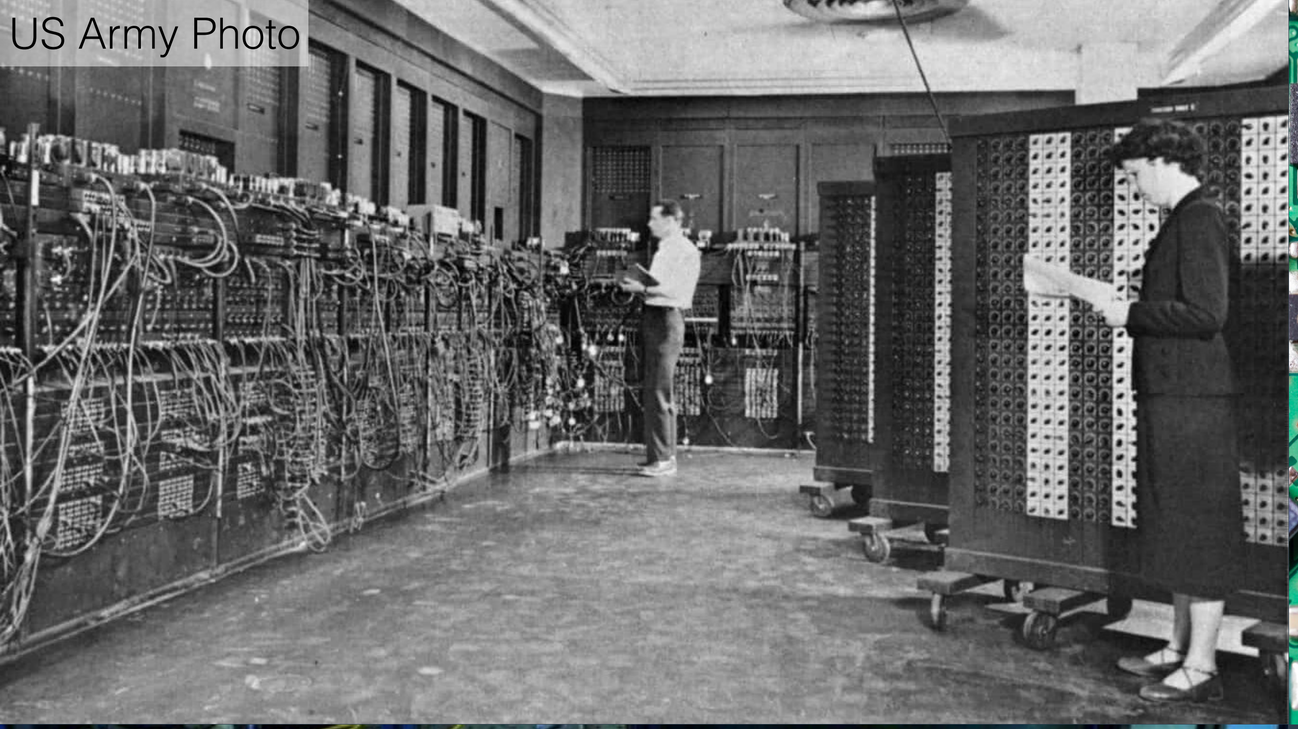


Photo by Immortal shots - Daily from Pexels



Quantum Optics Lab Olomouc



US Army Photo

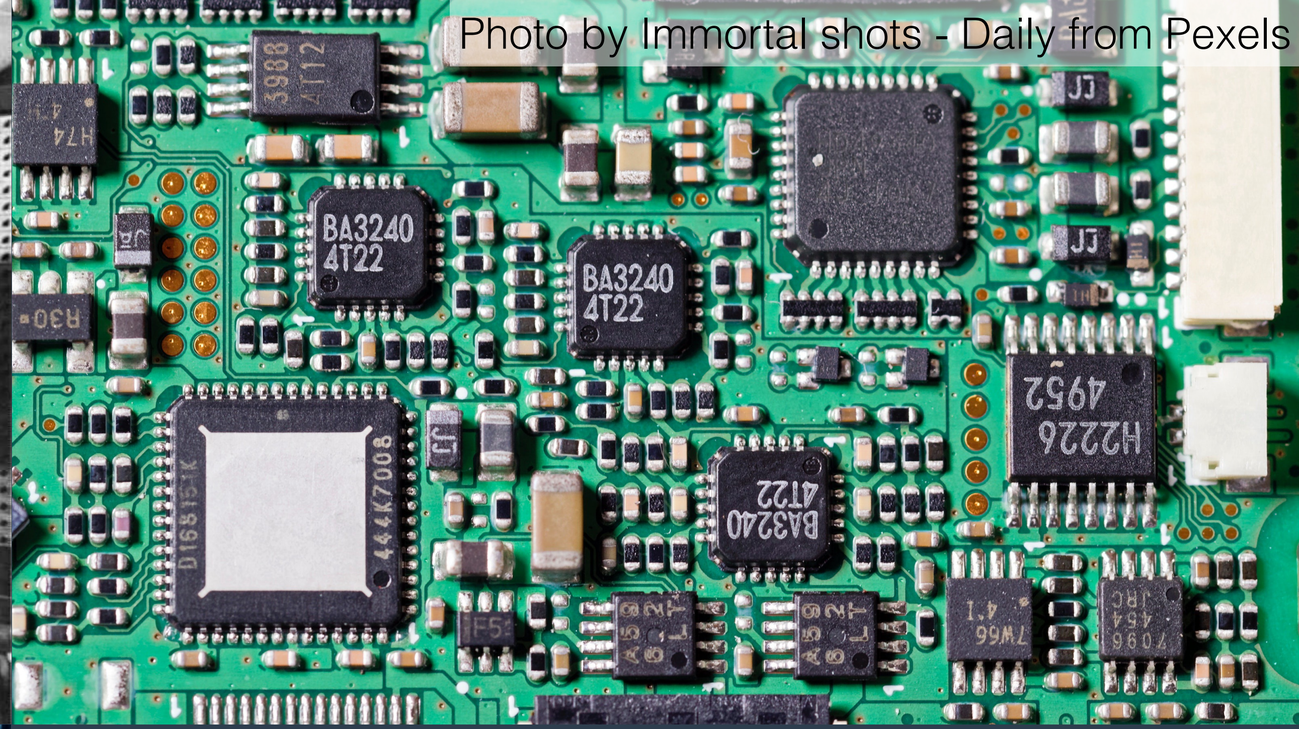
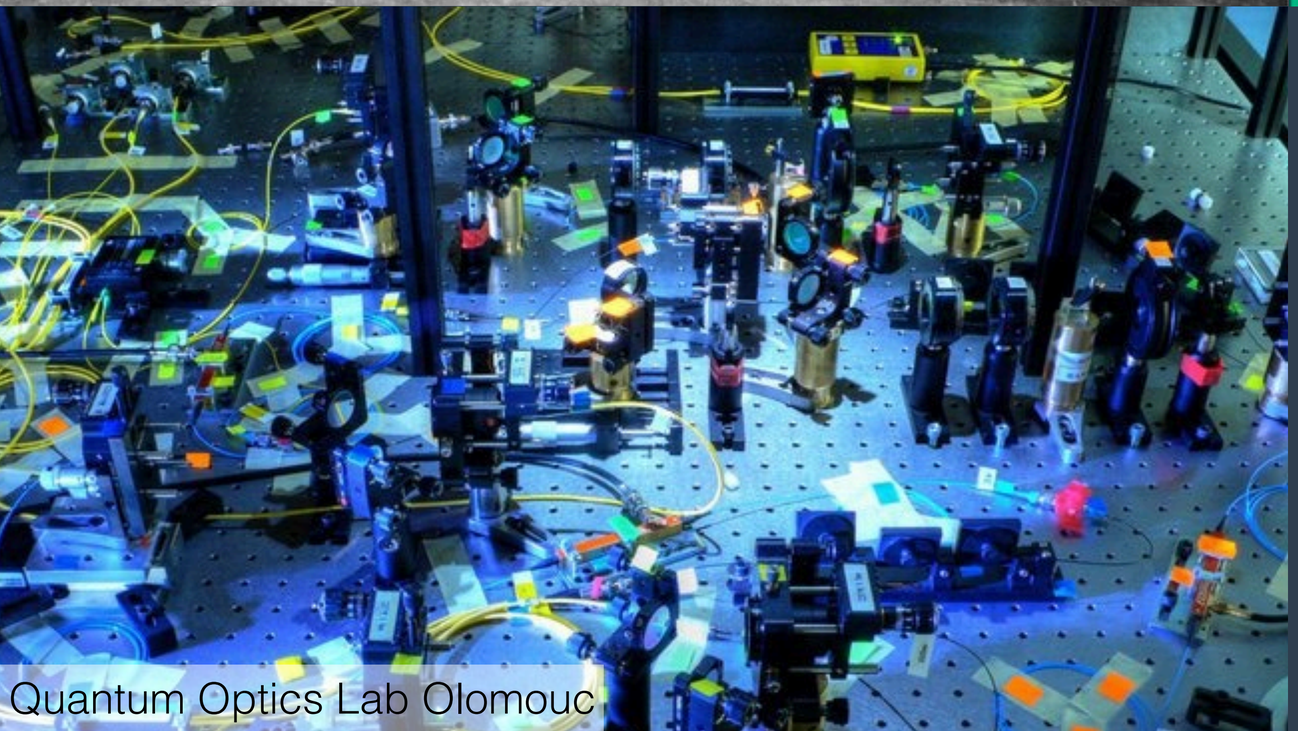


Photo by Immortal shots - Daily from Pexels



Quantum Optics Lab Olomouc

?

OSNOVE KVANTNEGA RAČUNALNIŠTVA

MATIJA PRETNAR

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 68Q12, 81P68

Kvantno računalništvo skuša z izkoriščanjem kvantnih pojavov, kakršni sta superpozicija in prepletenost, učinkoviteje reševati računsko zahtevne probleme. V članku si ogledamo postulate kvantne mehanike, kvantno teleportacijo, Deutschev algoritem, ki je bil prvi kvantni algoritem, ter najznamenitejša kvantna algoritma: Groverjev algoritem za iskanje v neurejeni tabeli in Shorov algoritem za razcep na praštevila.

THE BASICS OF QUANTUM COMPUTING

Quantum computing uses quantum phenomena such as superposition and entanglement in order to efficiently solve computationally hard problems. The paper looks at the quantum mechanics postulates, quantum teleportation, Deutsch's algorithm, which was the first quantum algorithm, and at two most famous quantum algorithms: Grover's search algorithm and Shor's factorization algorithm.

Uvod

V svetu majhnih delcev ne veljajo več pravila klasične Newtonove mehanike, kot smo jih navajeni, temveč nastopijo nenavadna pravila kvantne mehanike. Po teh pravilih se delci obnašajo tako, kot bi bili na več koncih hkrati, vendar le toliko časa, dokler jim ne izmerimo položaja. Ko pa ga enkrat izmerimo, se obnašajo le v skladu z rezultatom meritve. Primer takega vedenja vidimo v poskusu z dvojno režo (slika 1), v katerem streljamo fotone proti zaslonu z dvema ozkima režama, za zaslonom pa postavimo senzor, ki meri, kam so prileteli fotoni, ki jim je uspelo priti mimo.

Če eno od rež zapremo, največ zadetkov po pričakovanjih izmerimo za drugo režo. Če odpremo obe reži, bi tako pričakovali dva vrhova, za vsako režo po enega. V resnici pa dobimo interferenčni vzorec. Lahko bi si ga poskušali razložiti s tem, da fotoni na svoji poti motijo drug drugega, vendar dobimo tako sliko tudi, če poskrbimo, da naenkrat streljamo samo en foton. Torej obe možni poti, po katerih bi lahko potoval foton, motita druga drugo. Še več: če postavimo dodaten senzor, s katerim poskušamo ugotoviti, skozi katero režo je šel foton, interferenca izgine, za zaslonom pa izmerimo vrhova, ki smo ju pričakovali prej.

Kvantno računalništvo poskuša te neobičajne kvantne pojave izkoristiti za učinkovitejše računanje. S kvantnim računalništvom je pričel znani fizik

HVALA ZA
POZORNOST!