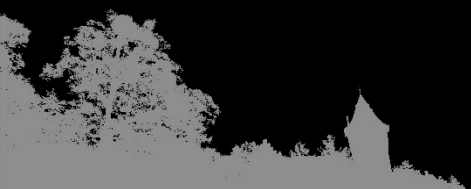
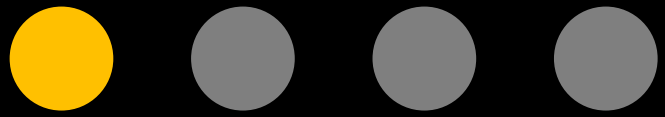
kvantové počítanie

čo počítače budúcnosti (ne)dokážu

daniel nagaj
fyzikálny ústav SAV

Quantum Rendezvous
Smolenice, 6/2022

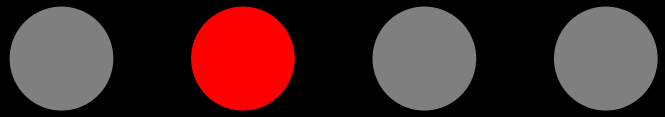




hlavolamy

zložitosť

počítače sú veľmi užitočné
nie všetky úlohy sú si rovné



kvantová hra

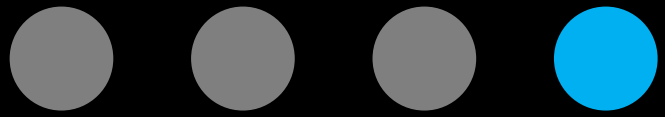
nové nápady

mnoho ciest naraz (superpozícia)
šikovne prepojených (interferencia)

kam ideme

aplikácie QC

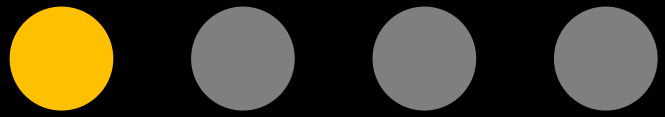
načo to je vlastne dobré
a kde sa nám „darí“



obmedzenia

a limity QC

škálovanie a oprava chýb
nie je to všeliek



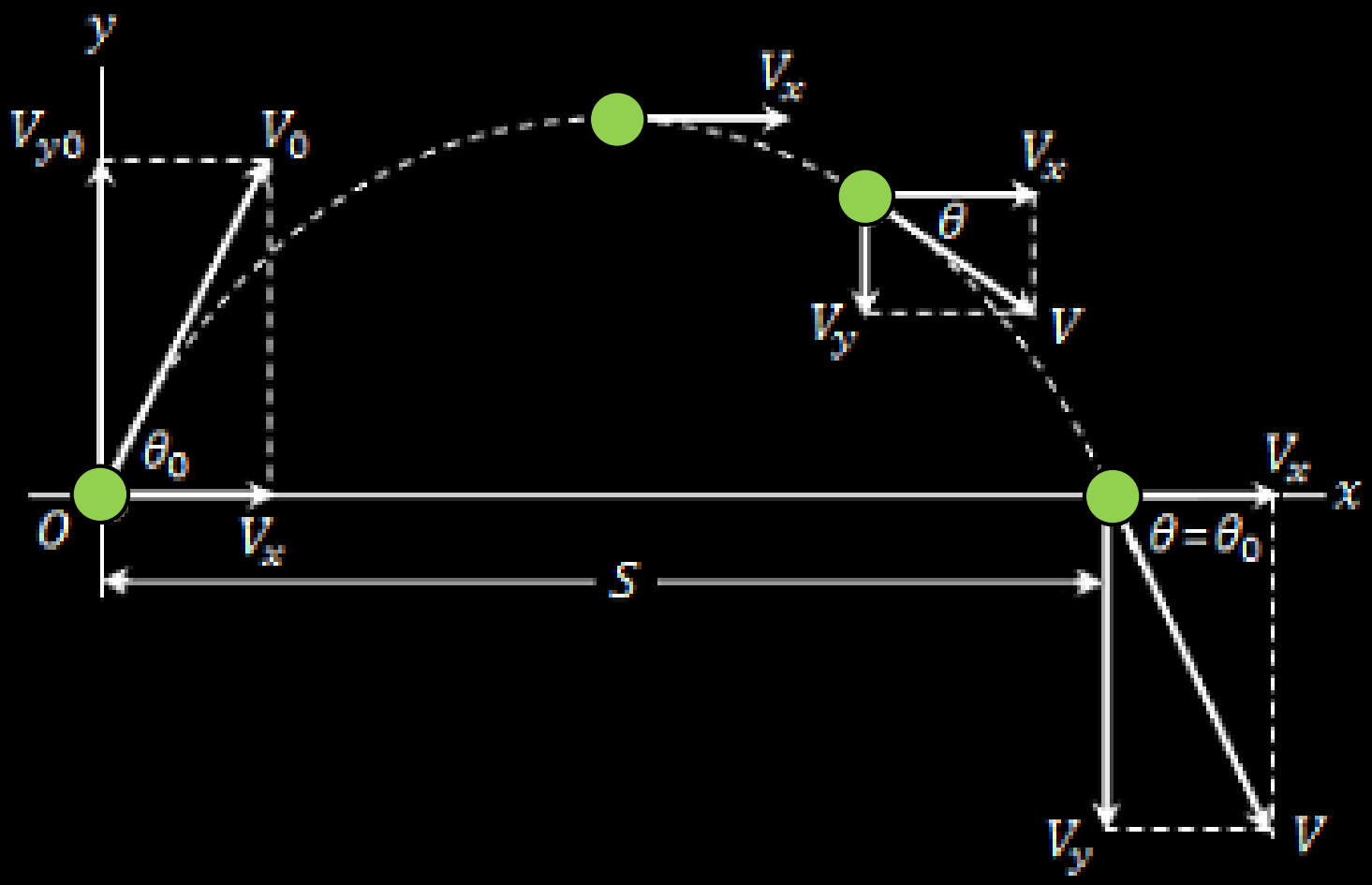
hlavolamy

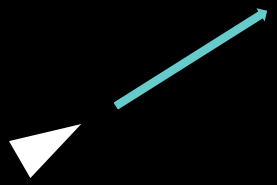
zložitosť

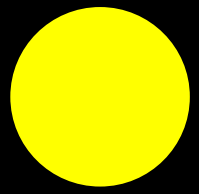
počítače sú veľmi užitočné
nie všetky úlohy sú si rovné

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

VDV (veda o dosadzovaní do vzorca)

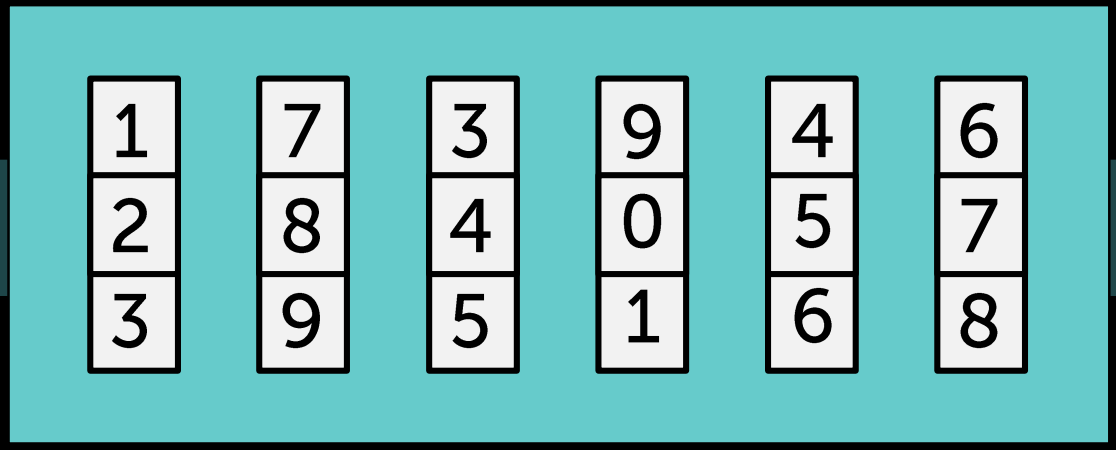

y
V_{y0}
V_0
V_x
V_x
θ
V_y
V
θ_0
O
V_x
S
V_x
x
$\theta=\theta_0$
V_y
V

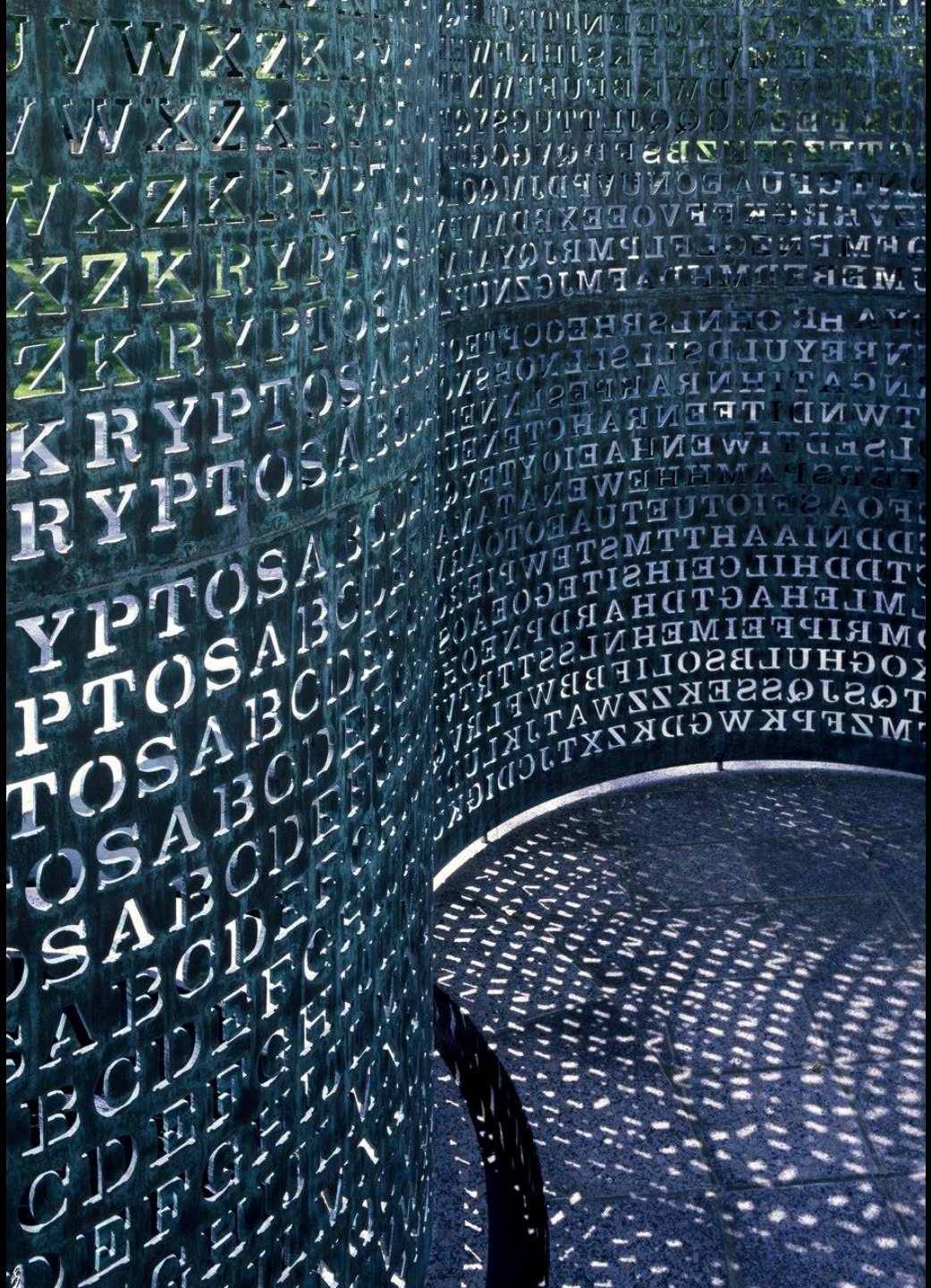




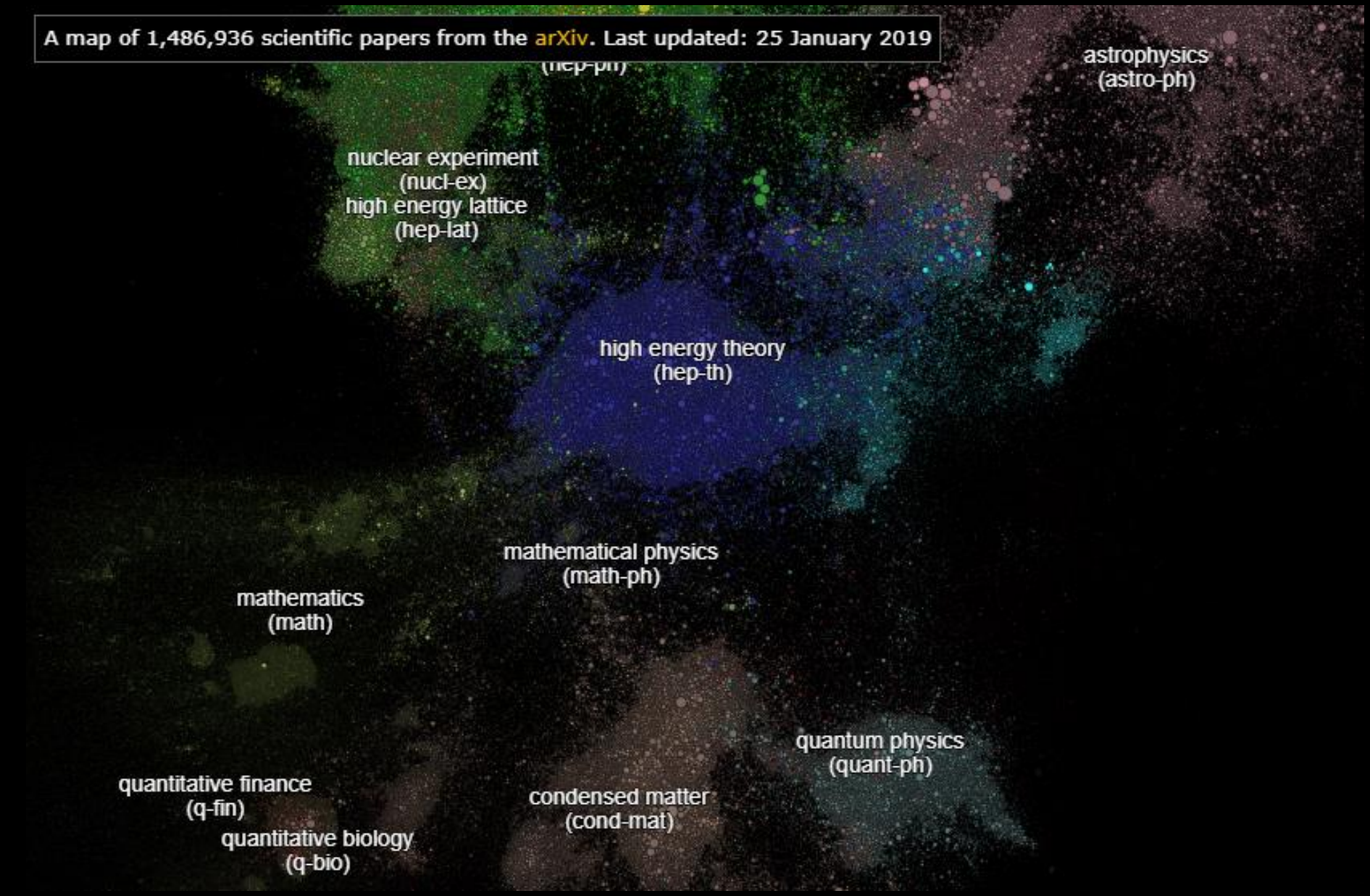
Opustí táto raketa slnečnú sústavu?

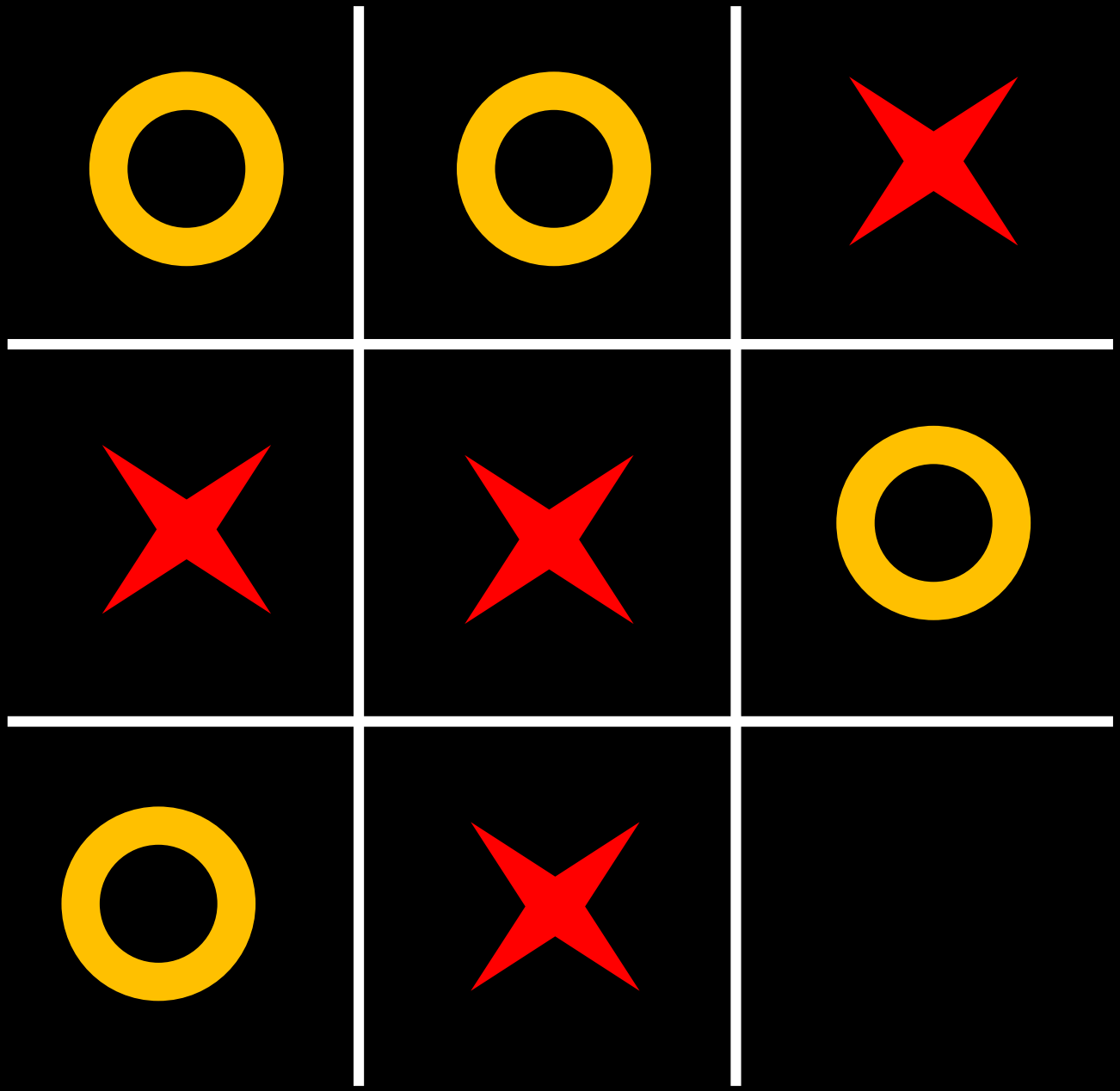
ESA/Rosetta/NAVCAM (2014)


1
2
3
7
8
9
3
4
5
9
0
1
4
5
6
6
7
8



Kryptos statue
CIA headquartes
Carol M. Higsmith

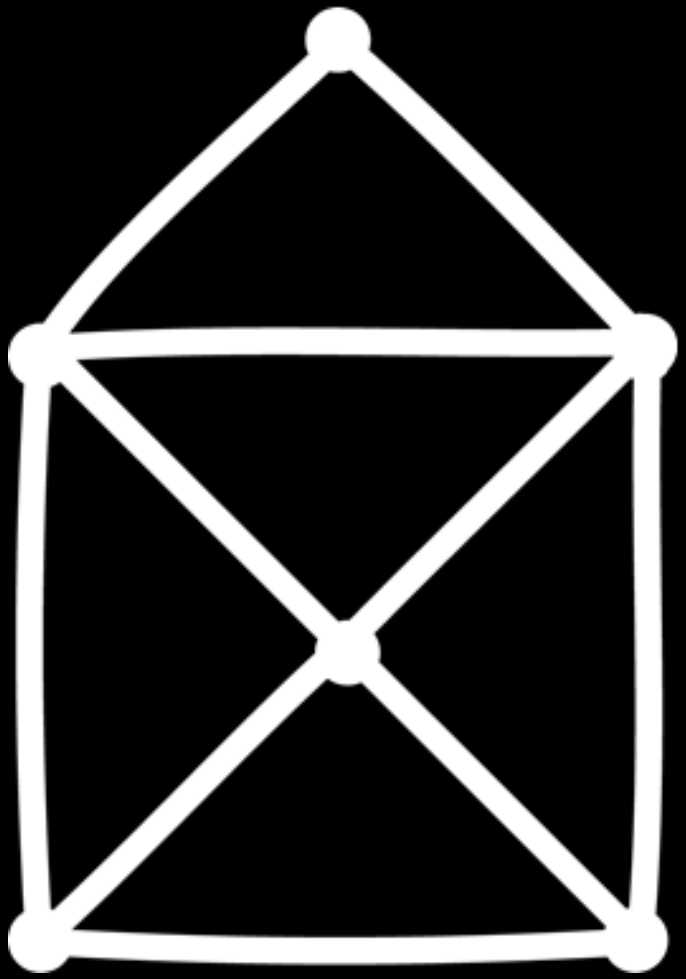




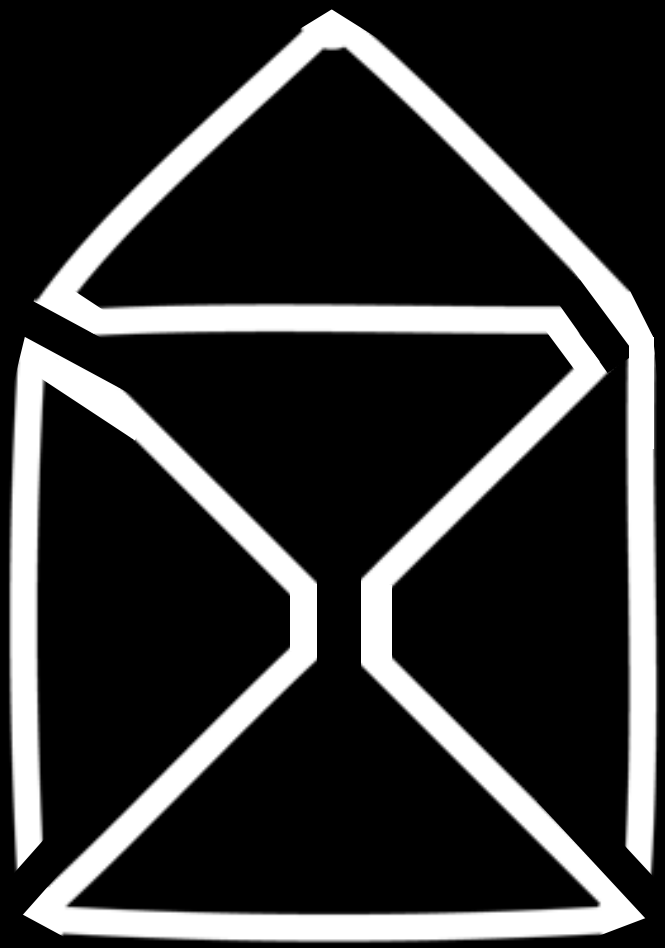
www.alphagomovie.com, Lee Sedol vs. AlphaGo 1:4 (2016)

two-minute papers

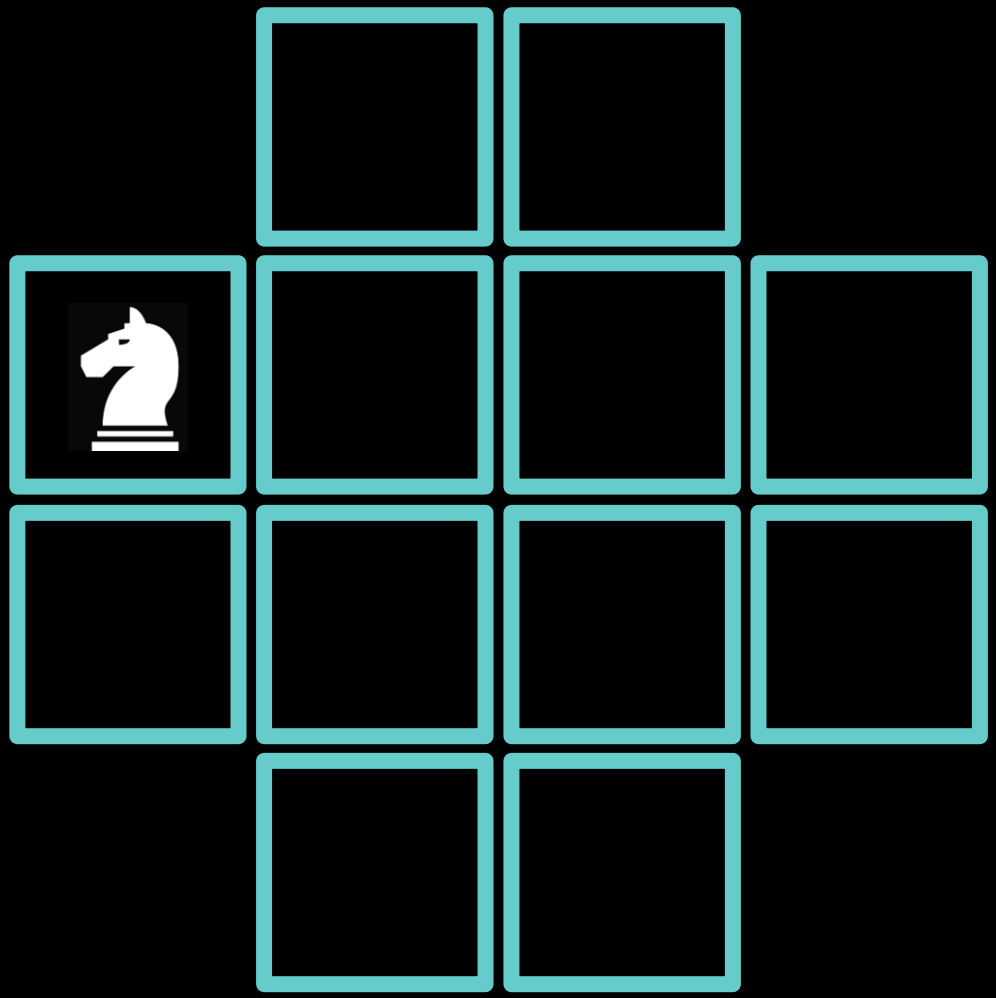
with dr. Károlyi Zsolnai-Fehér



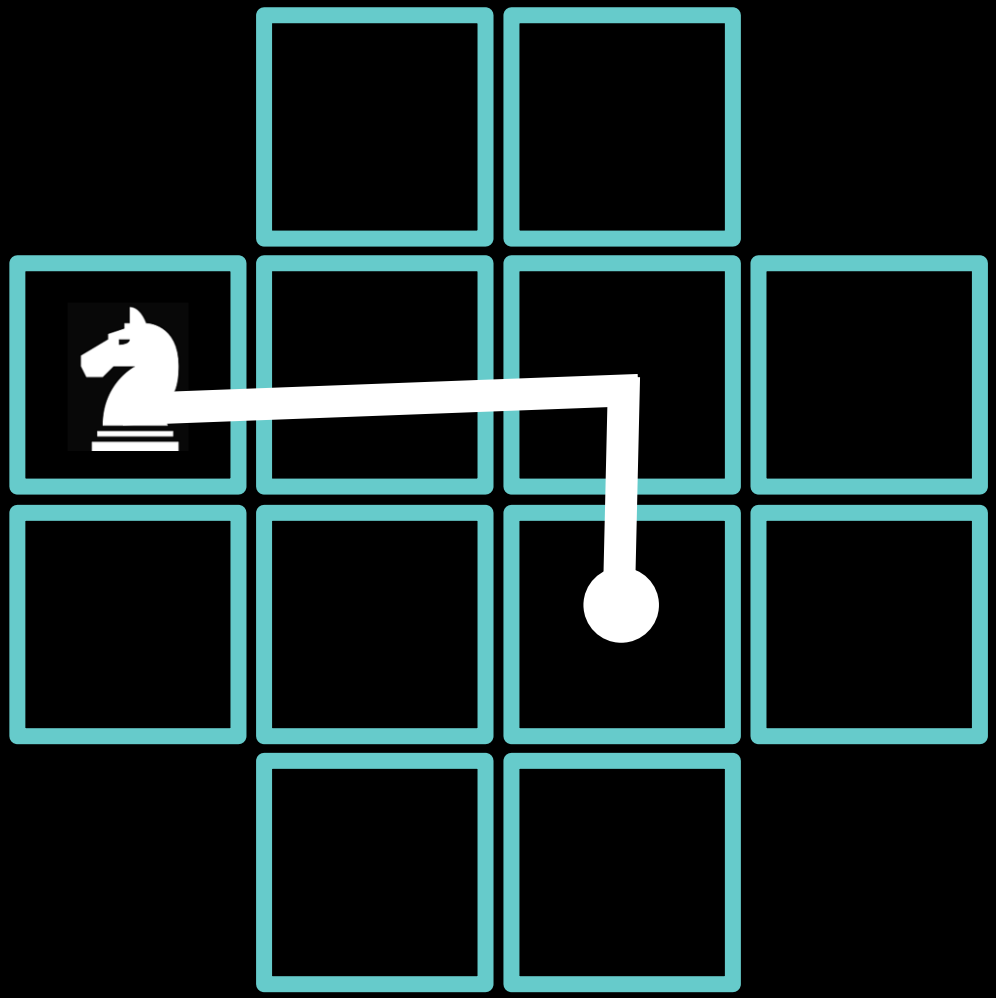
Nakresli jedným ťahom.



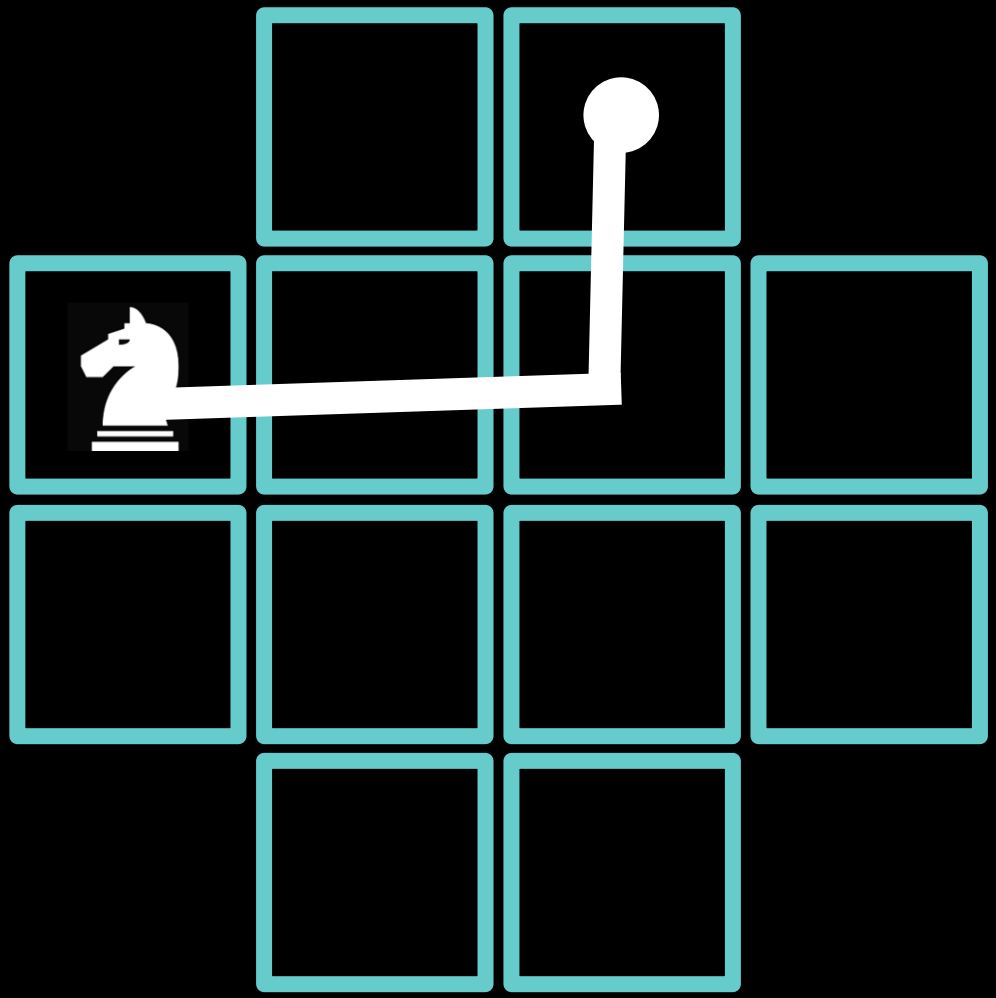
Nakresli jedným ťahom.



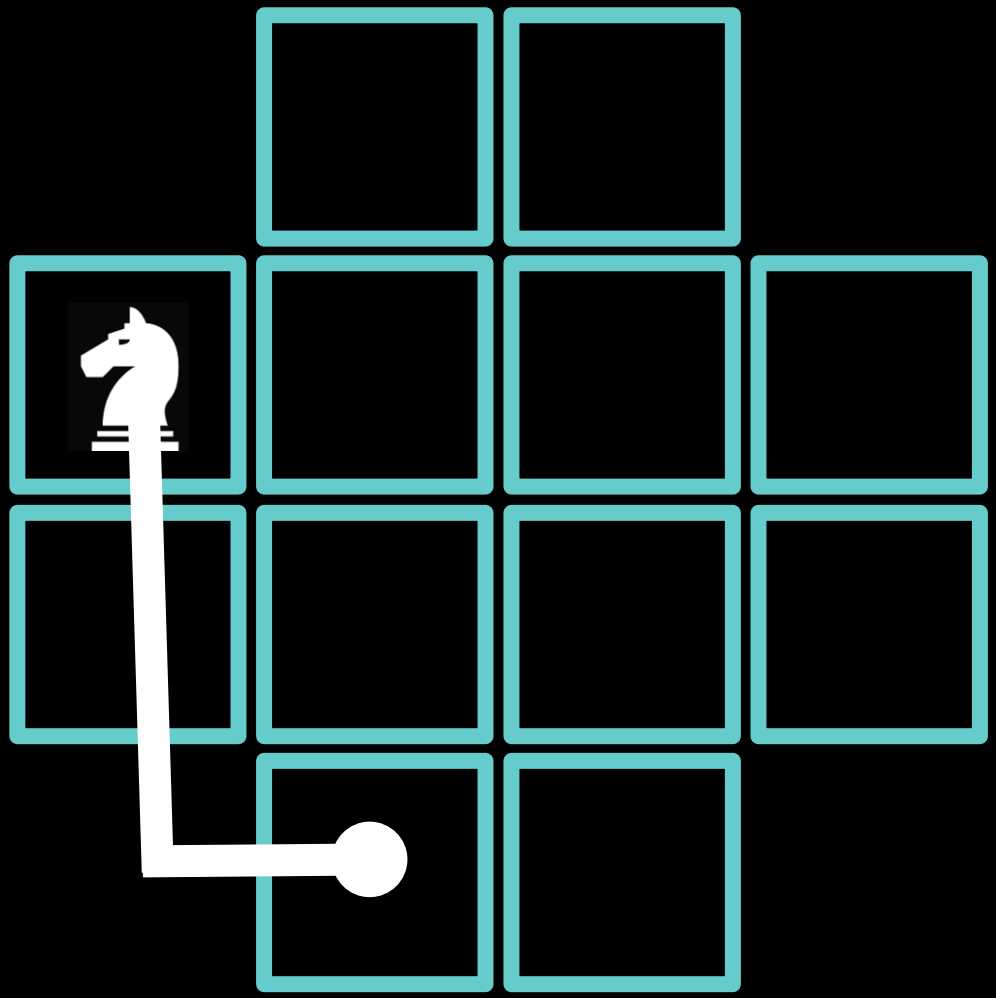
Šachový kôň: poskáč to celé a vráť sa.



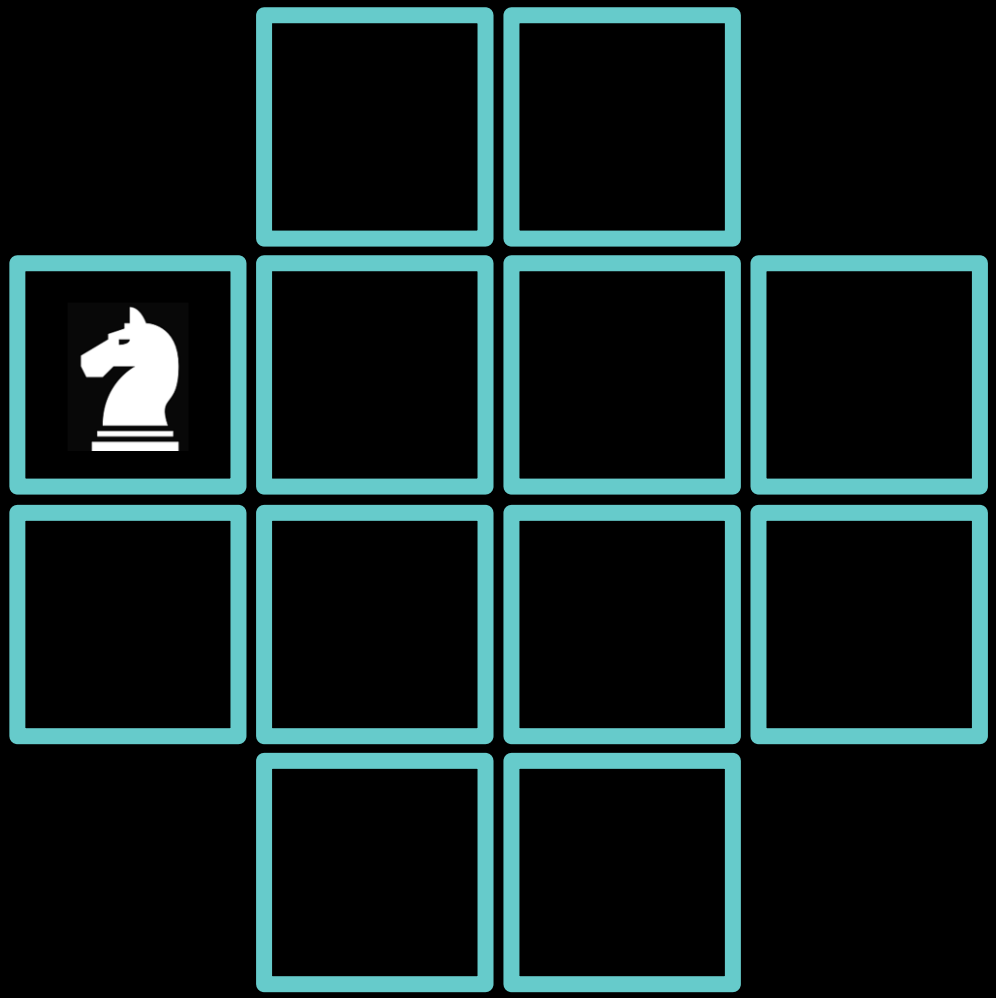
Šachový kôň: poskáč to celé a vráť sa.



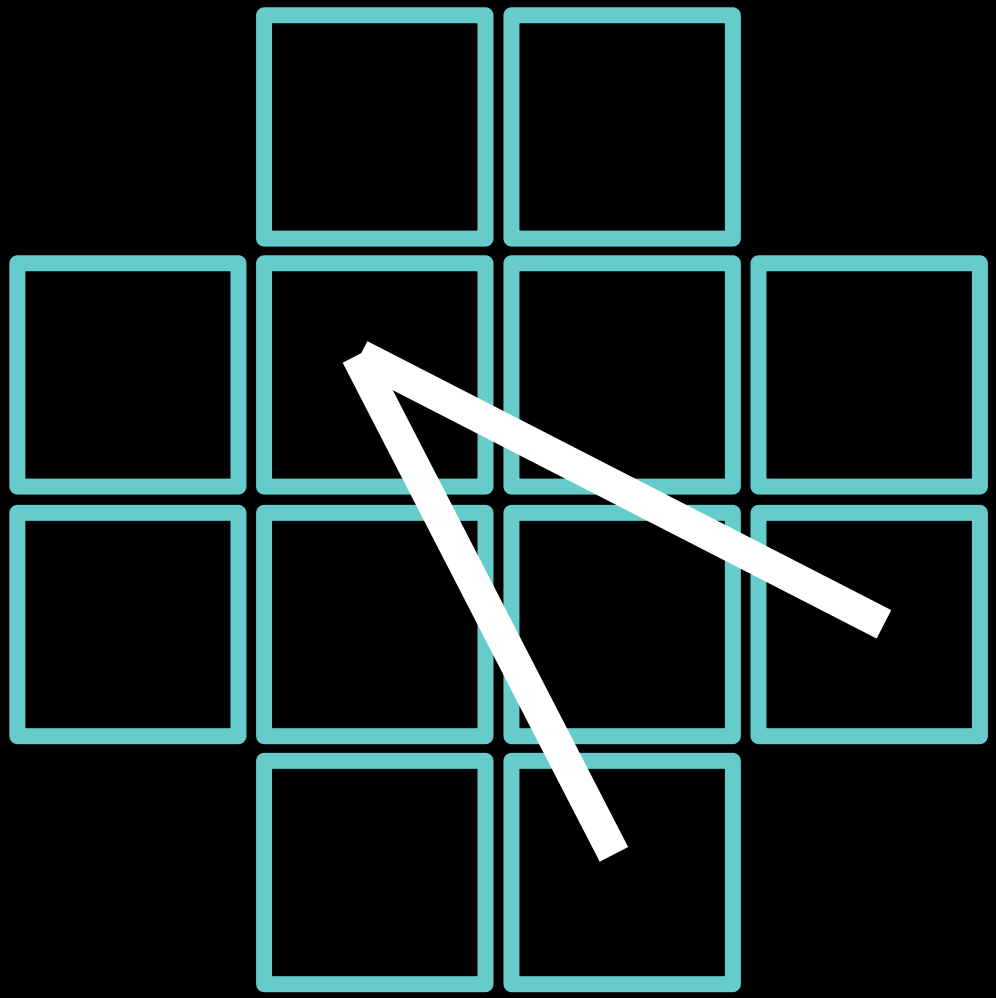
Šachový kôň: poskáč to celé a vráť sa.



Šachový kôň: poskáč to celé a vráť sa.

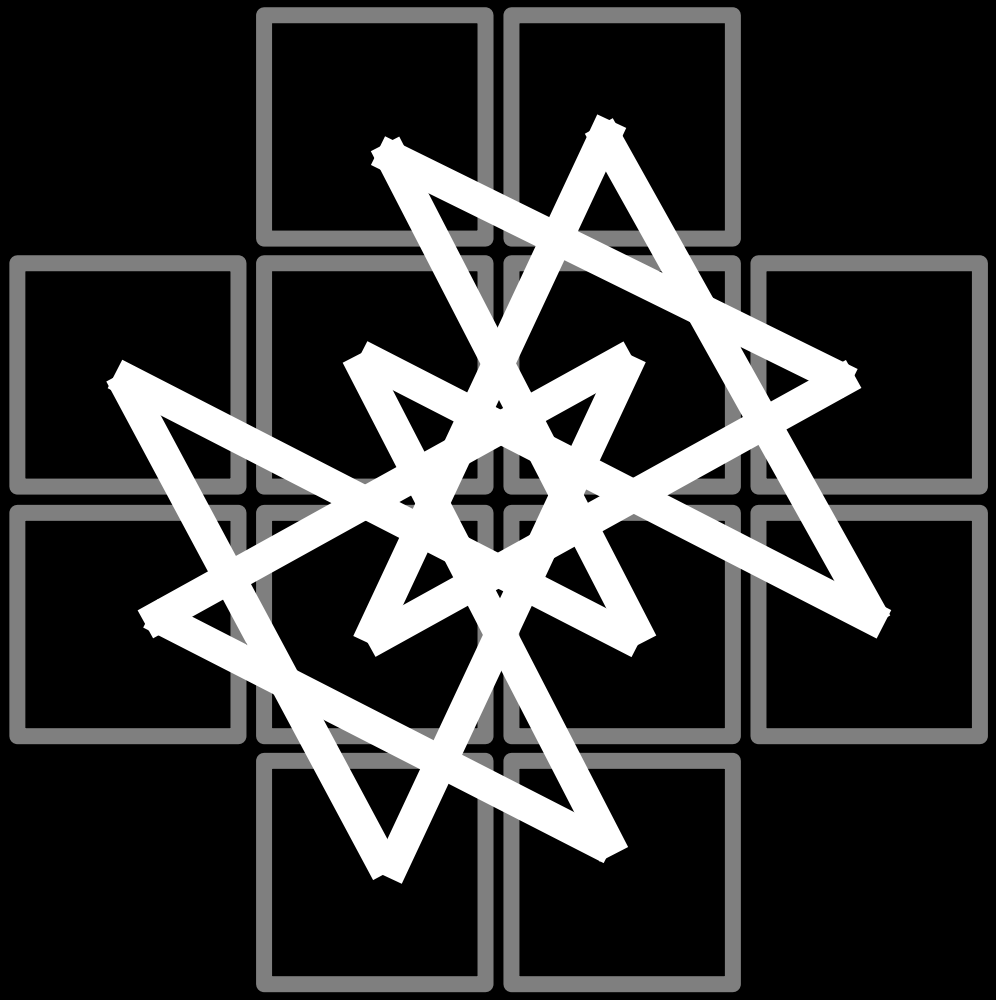


Šachový kôň: poskáč to celé a vráť sa.

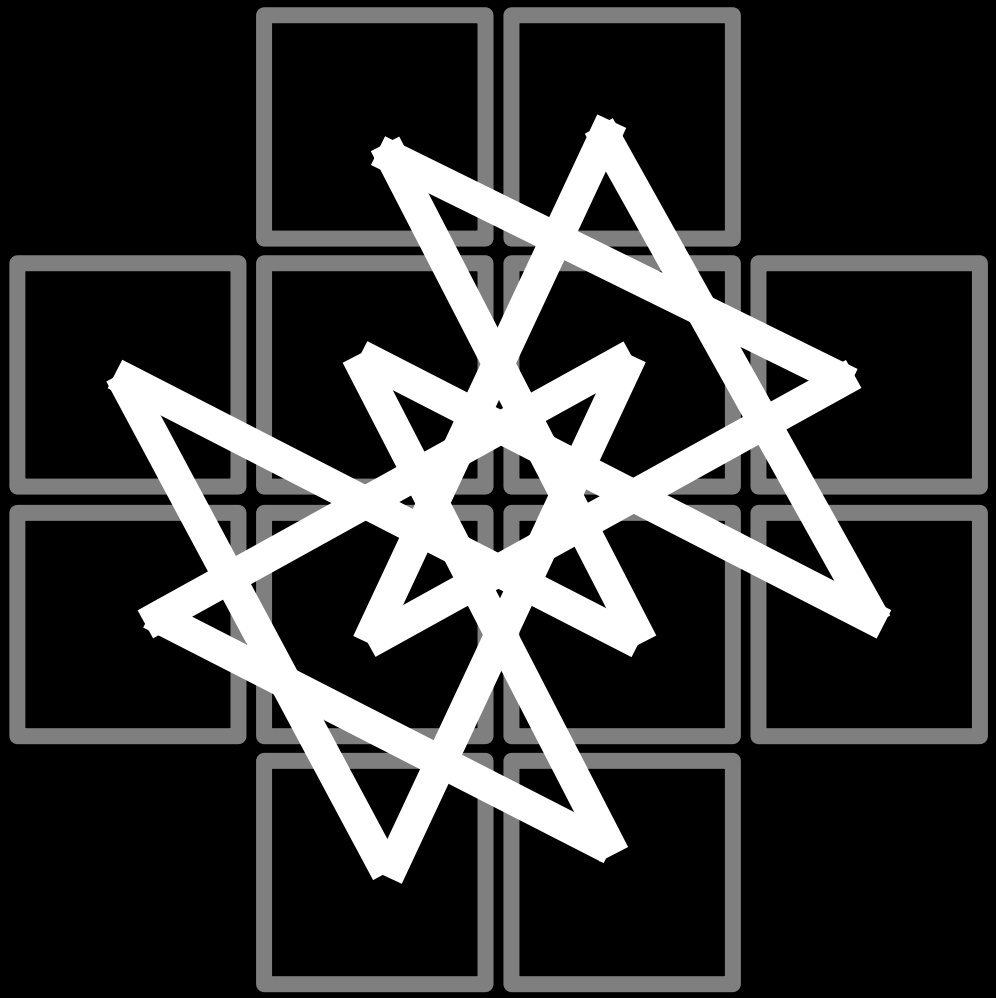


Logika.

Logika & symetria.



Logika & symetria.



Prípad ťažkej úlohy – Hamiltonian cycle.

$673 \times 3 =$

Menej ako 2000?

$$673 \times 3 = 2019$$

Menej ako 2000?

$$2021 = \ldots \times \ldots$$

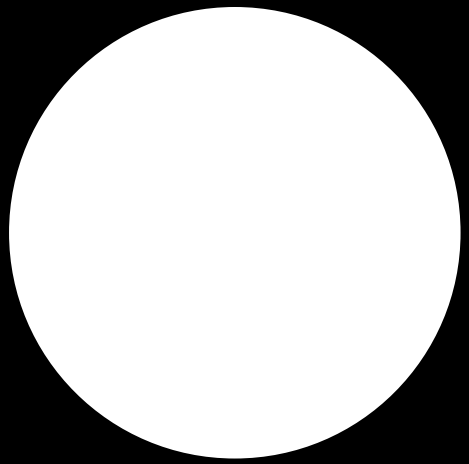
Je to prvočíslo?

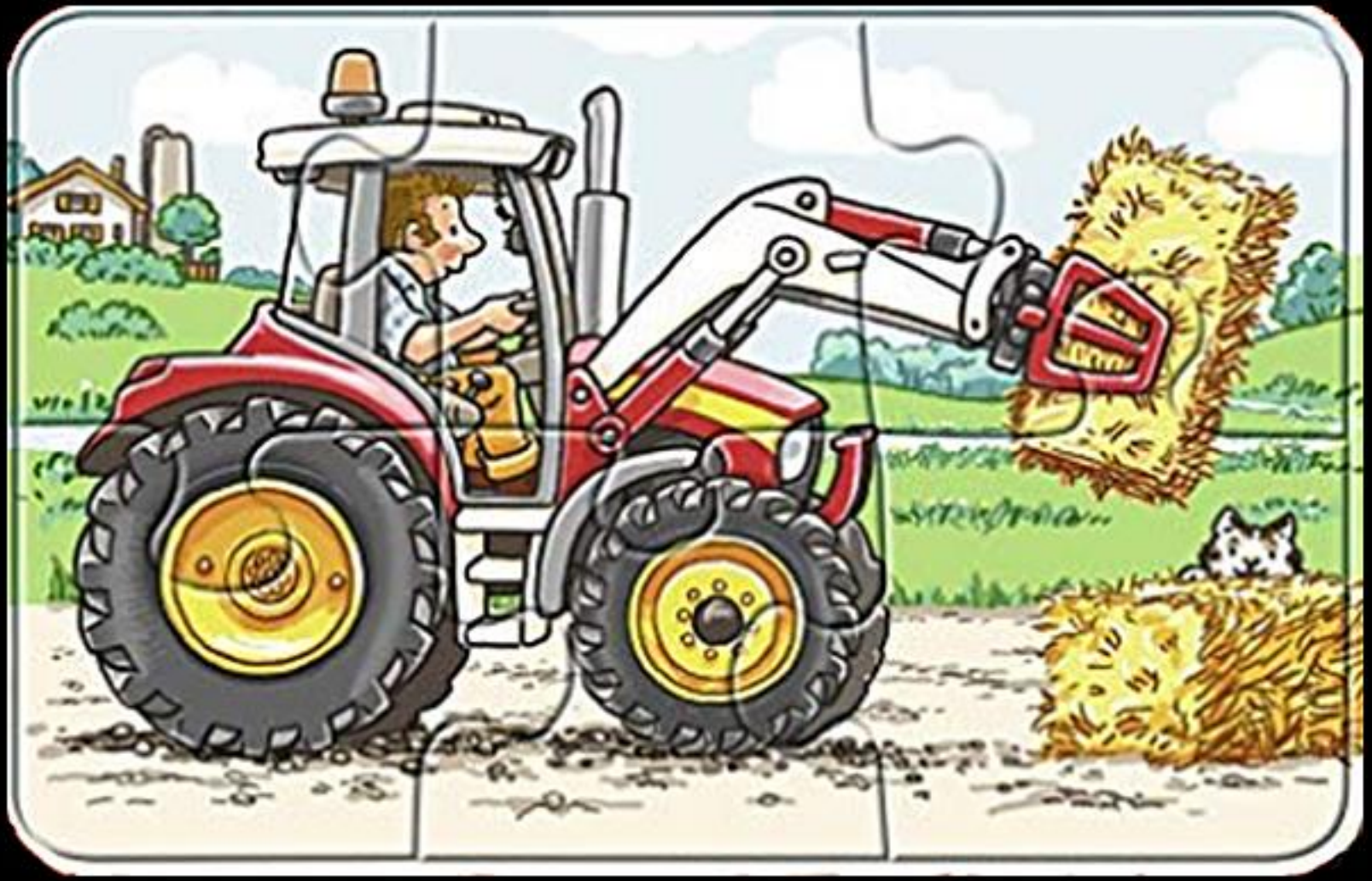
$$2021 = \ldots \times \ldots$$

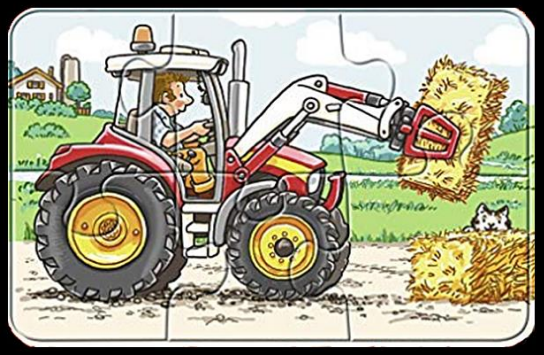
Netriviálny deliteľ < 45?

$$2021 = 43 \times 47$$

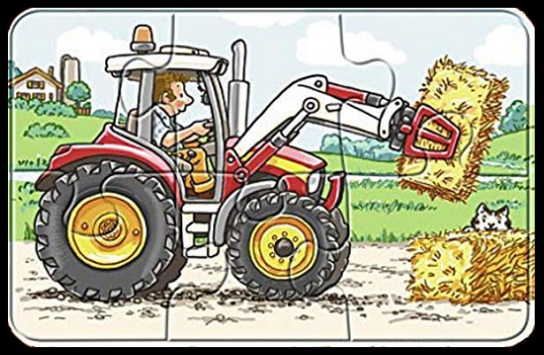
škálovanie



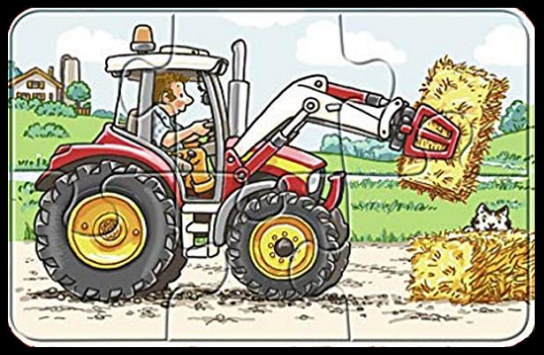




5 + 4 + 3 + 2 + 1

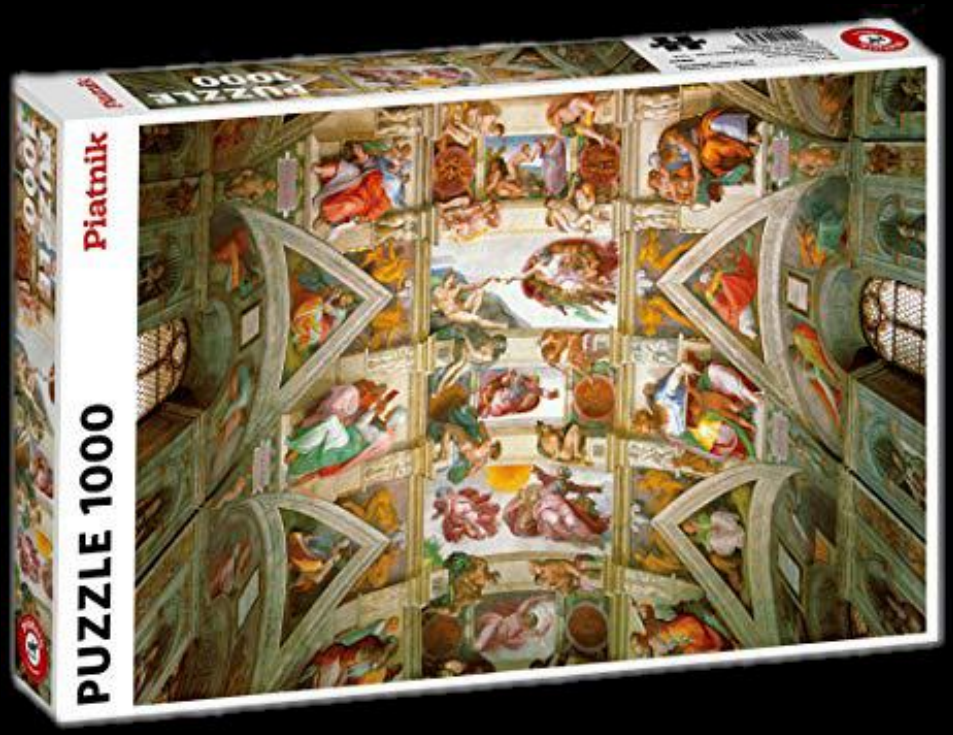


$$4 \times (5 + 4 + 3 + 2 + 1) =$$



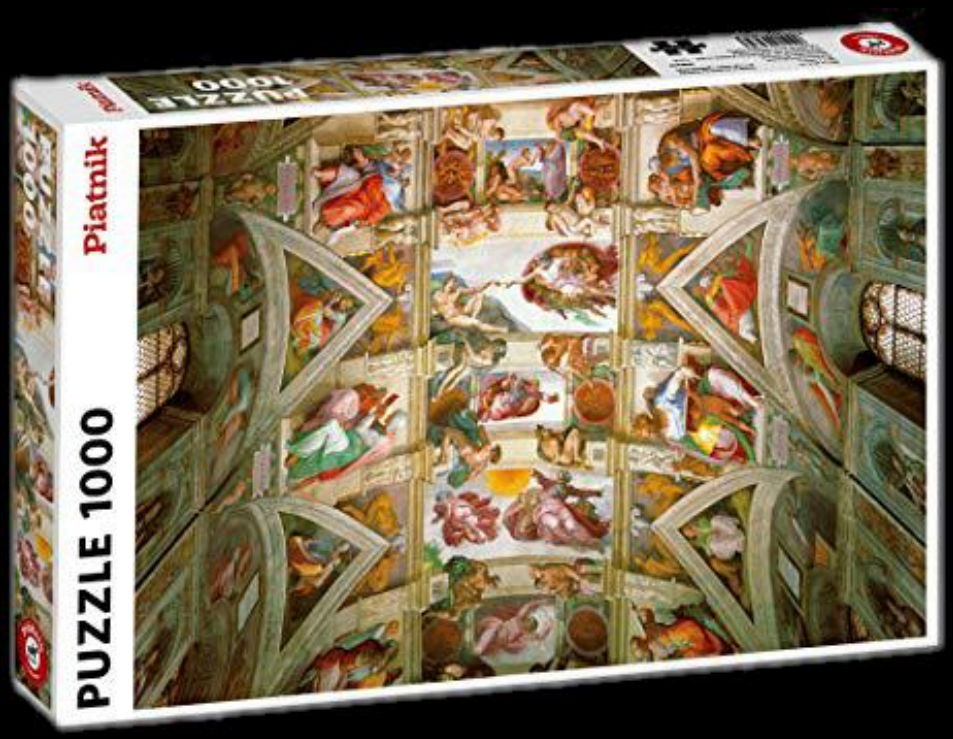
$$4 \times (5 + 4 + 3 + 2 + 1) = \mathbf{60}$$


PUZZLE 1000
Piatnik



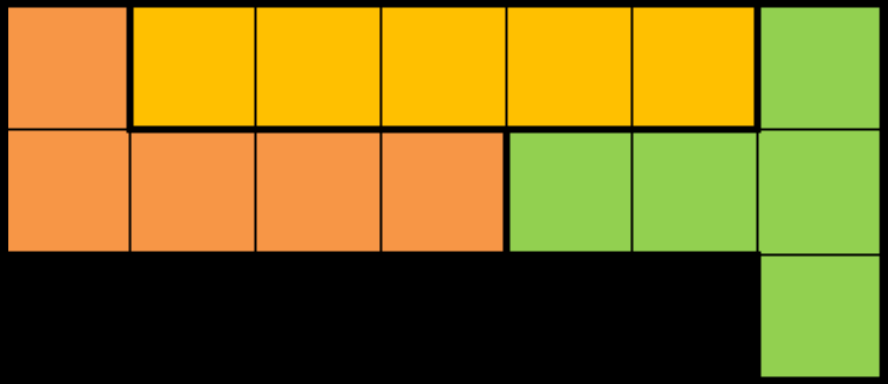
$4 \times (999 + \ldots + 1) = \ldots$

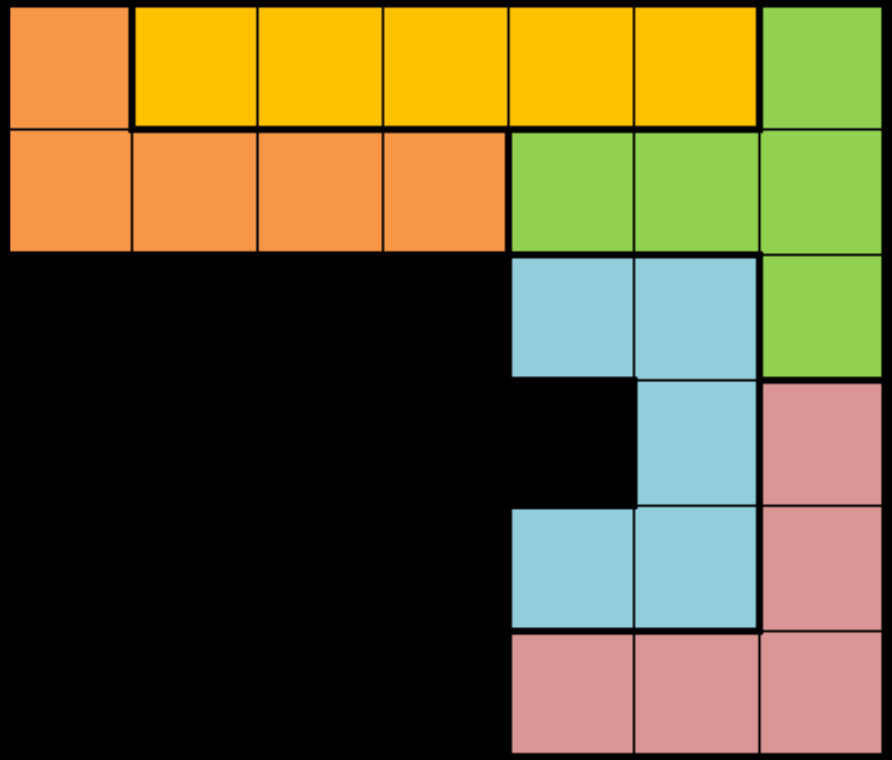
$4 \times (999 + \ldots + 1) \sim \mathbf{2\,000\,000}$

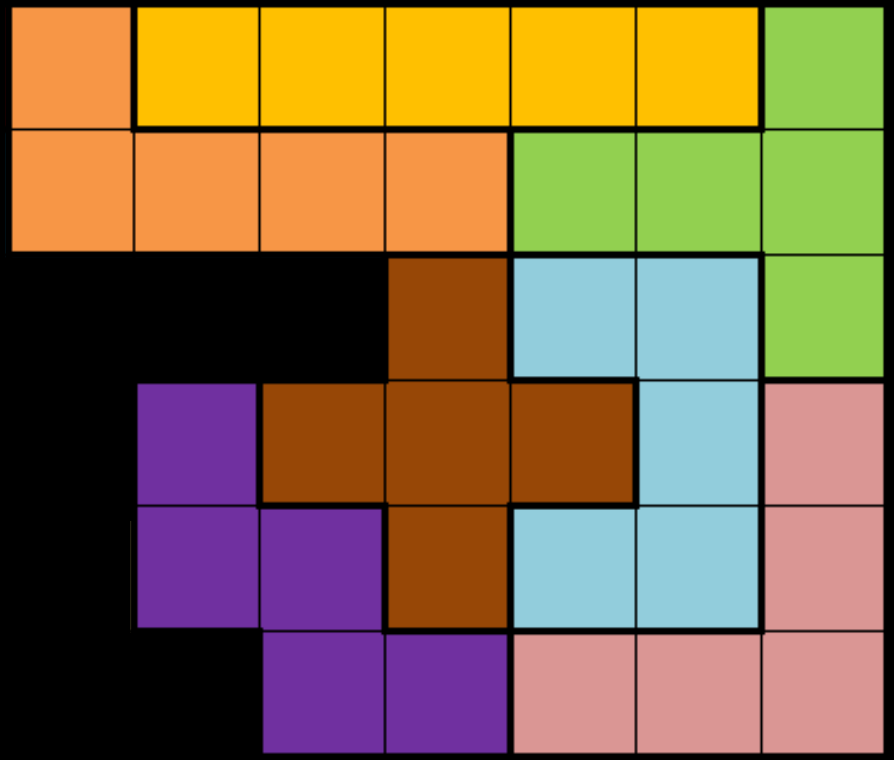


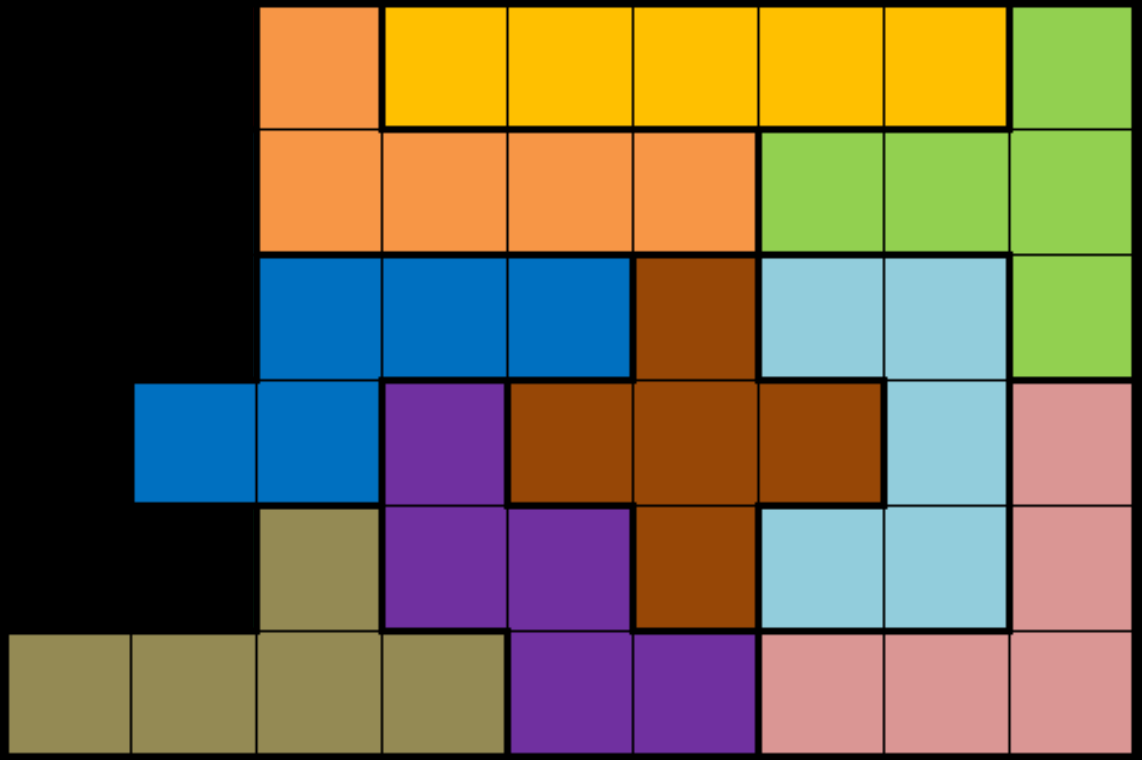
$4 \times (999 + \ldots + 1) \sim 2\,000\,000$

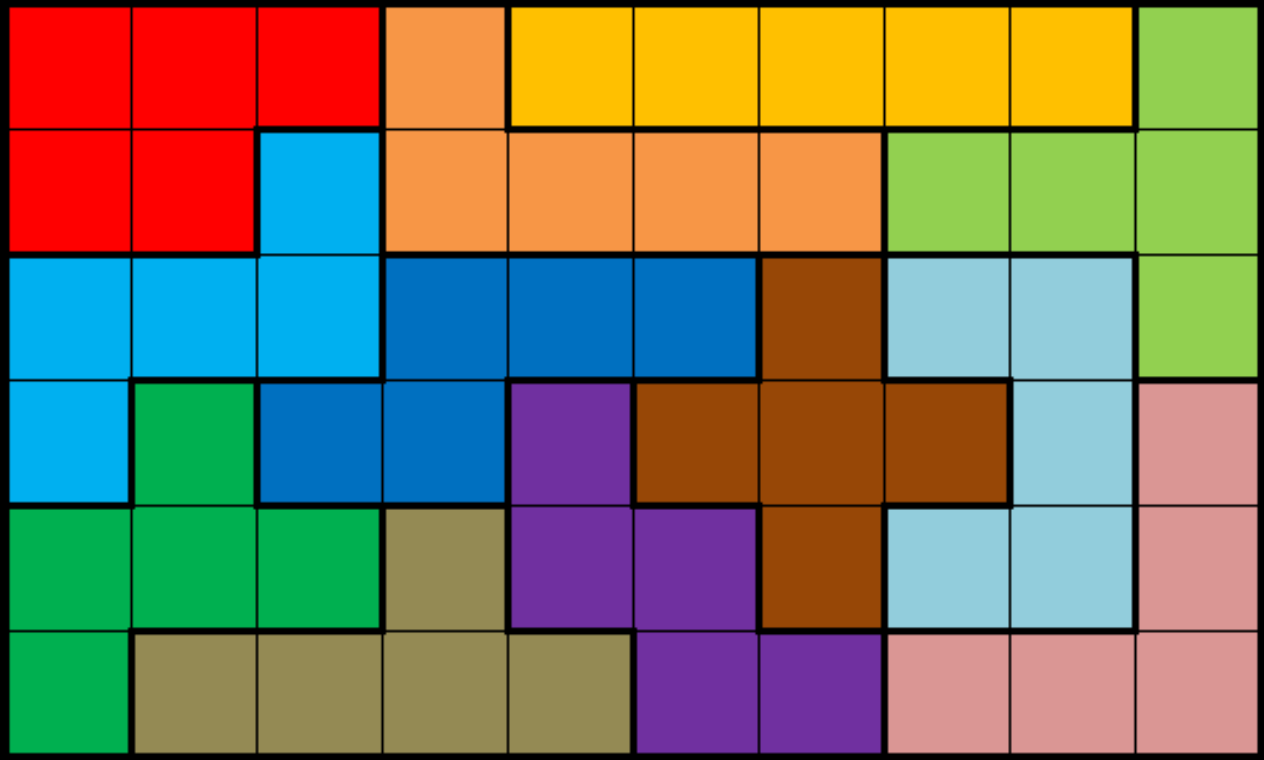
kvadratické škálovanie $O(n^2)$

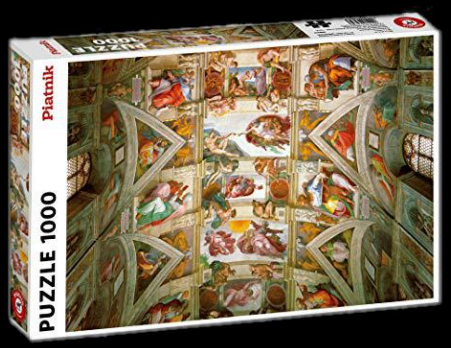






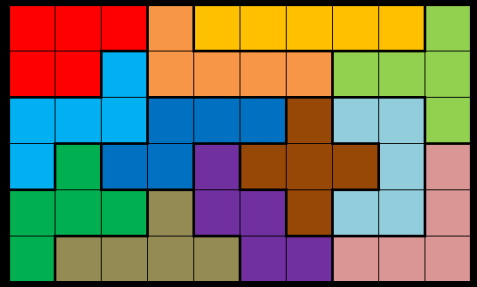






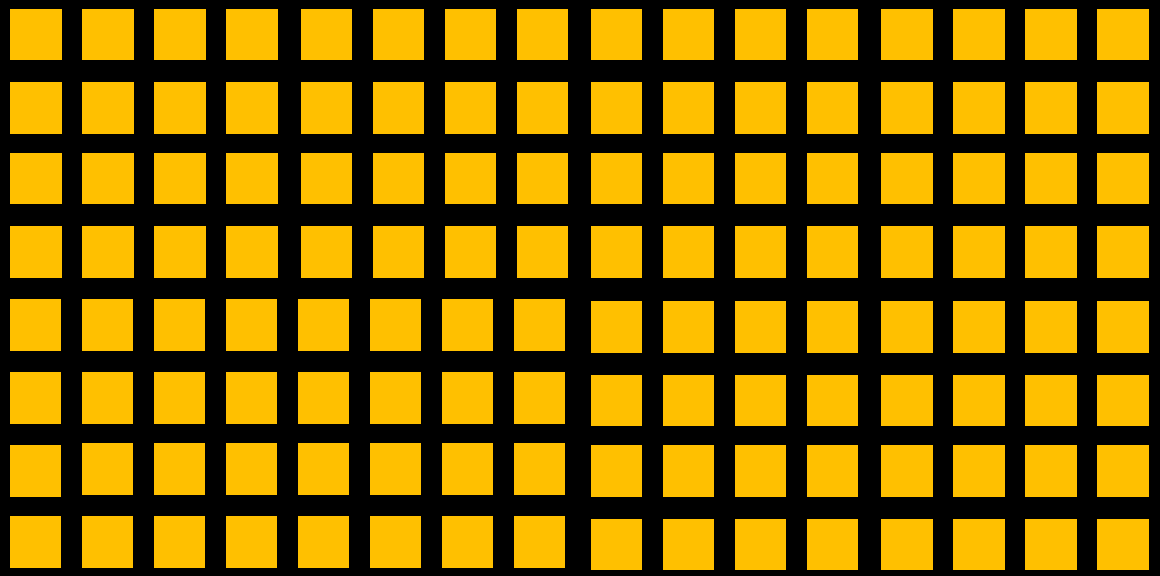
$$999 + \ldots + 1$$

$\times 4$

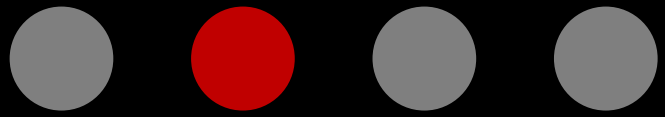


$$12 \times 11 \times 10 \times \ldots$$

$\times 8$ $\times 8$ $\times 8$



ľahké/**ťažké**

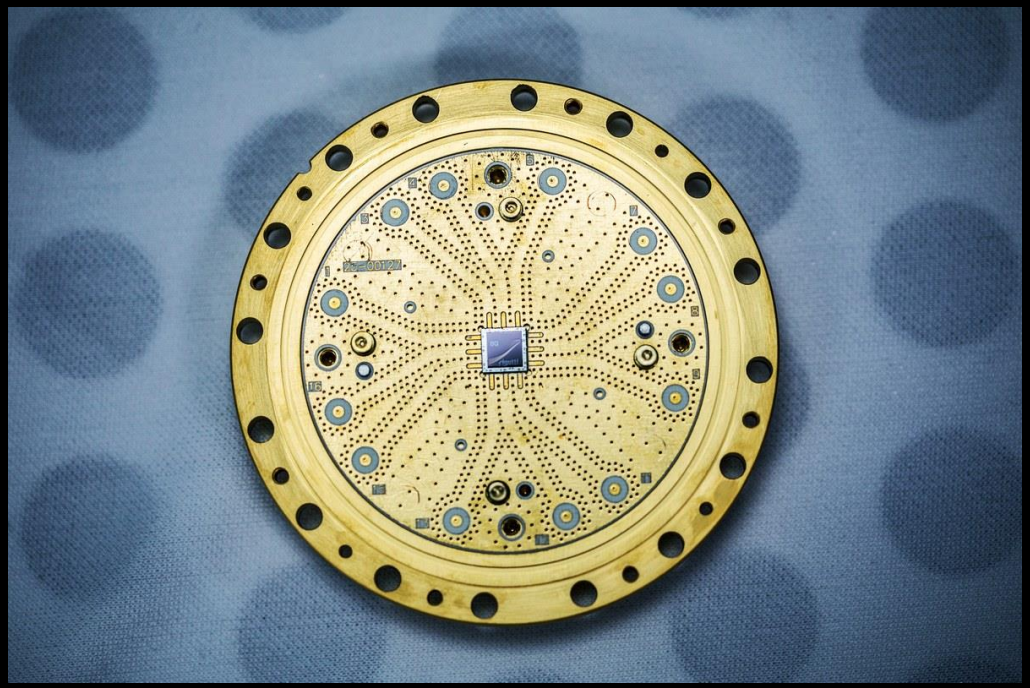


kvantová hra

nové nápady

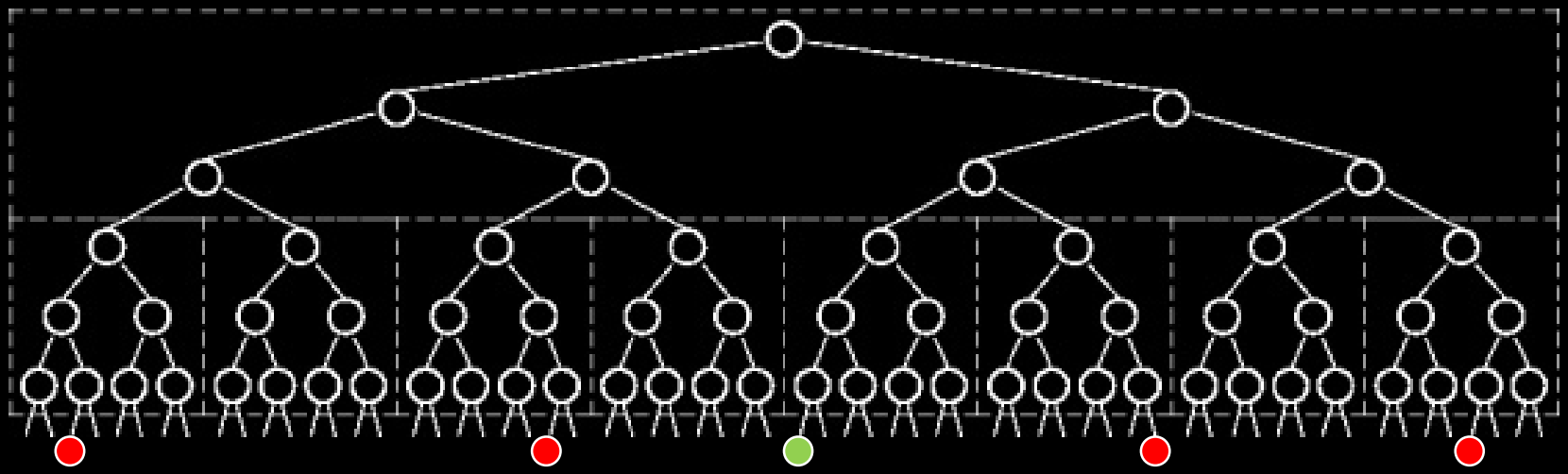
mnoho ciest naraz (superpozícia)
šikovne prepojených (interferencia)

superpozícia
previazanie
unitárne operácie



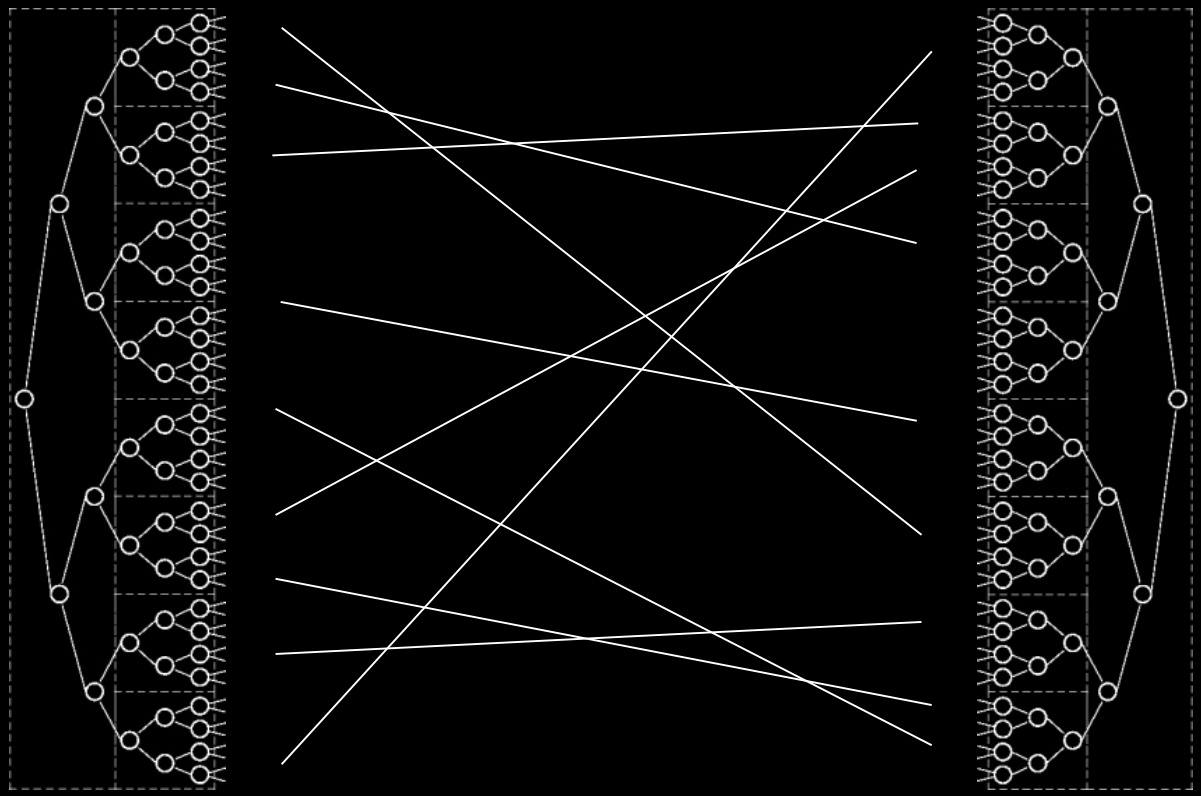
Rigetti Computing 2017

superpozícia



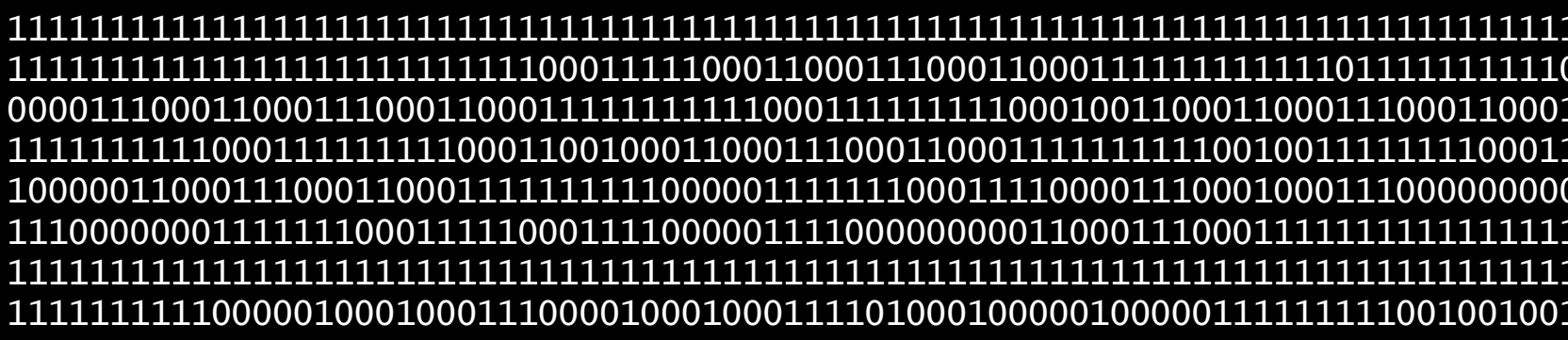
všetky cesty naraz... no čo z toho?

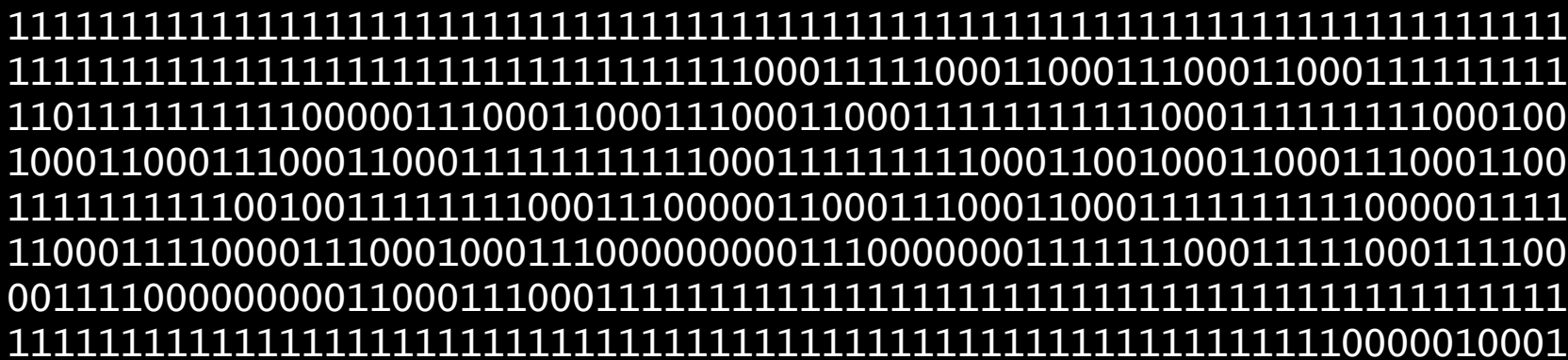
superpozícia

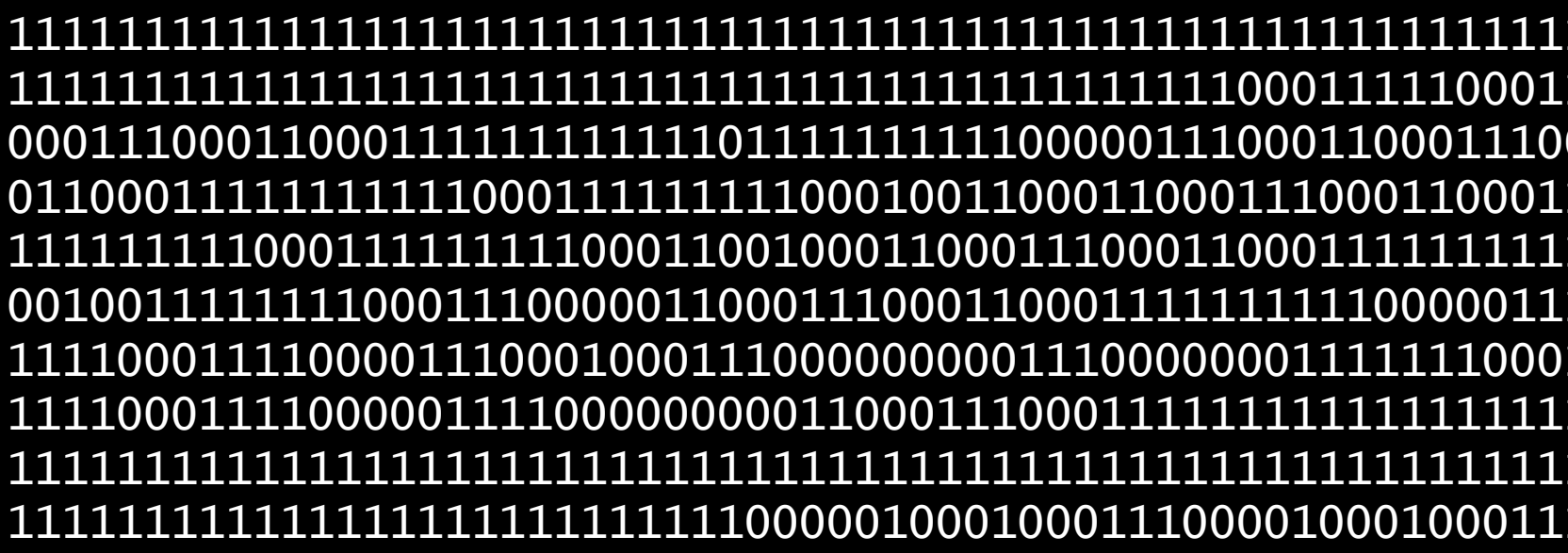


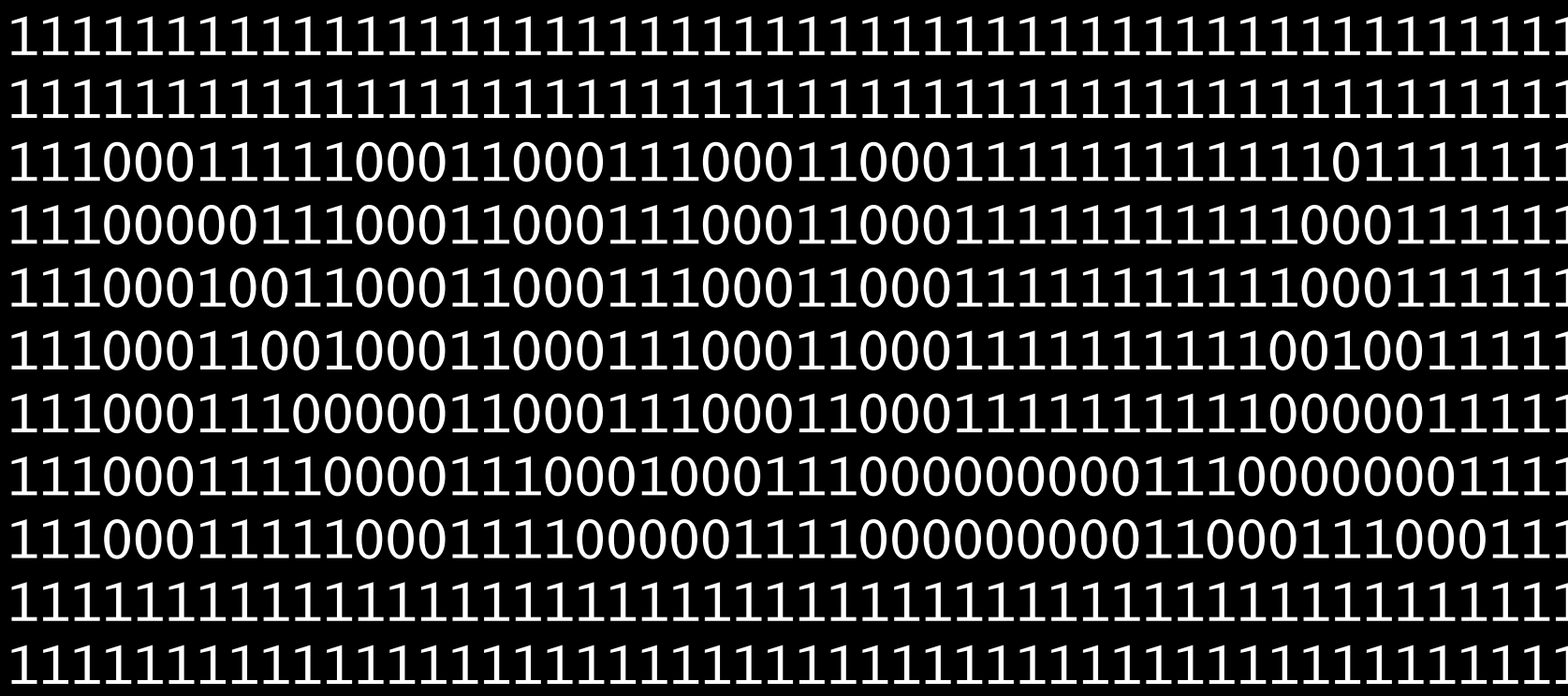
umne využi štruktúru

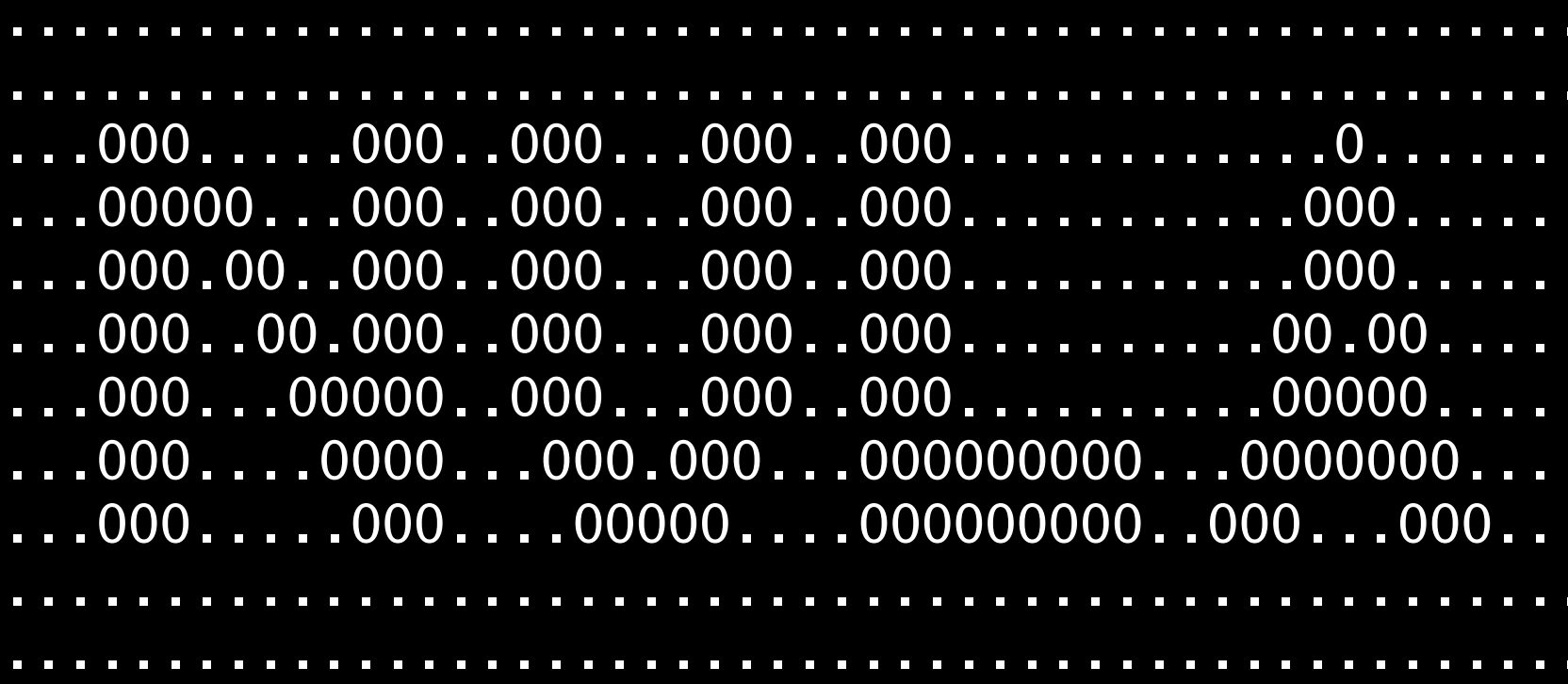
skrytá štruktúra

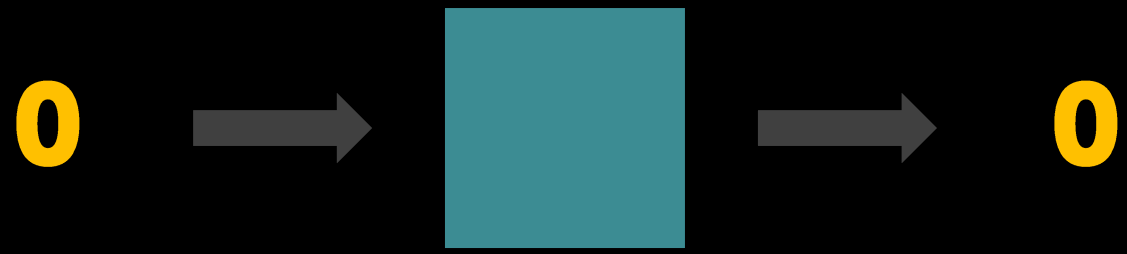


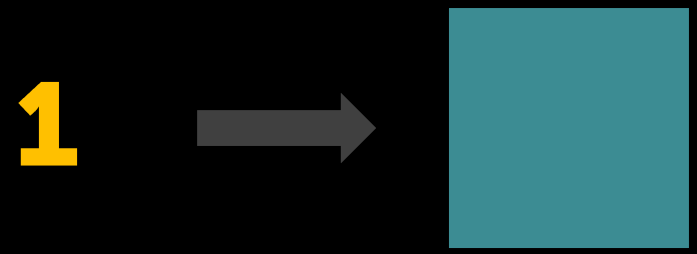

11111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111110001111000110001110001100011111111
11011111111110000011100011000111000110001111111111100011111111100010010
10001100011100011000111111111100011111111100011001000110001110001100
11111111100100111111110001110000011000111000110001111111100000111111
11000111100001110001000111000000000111000000011111110001111100011110000
00111100000000011000111000111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111100000100010

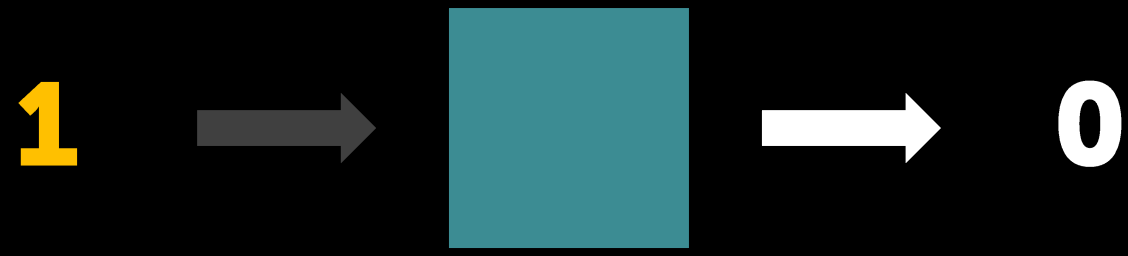



1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1110001111100011000111000110001111111111101111111
1110000011100011000111000110001111111111000111111
1110001001100011000111000110001111111111000111111
1110001100100011000111000110001111111111001011111
1110001110000011000111000110001111111111000011111
1110001111000011100010001110000000001110000000111
1110001111100011110000011110000000001100011100011
1111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111

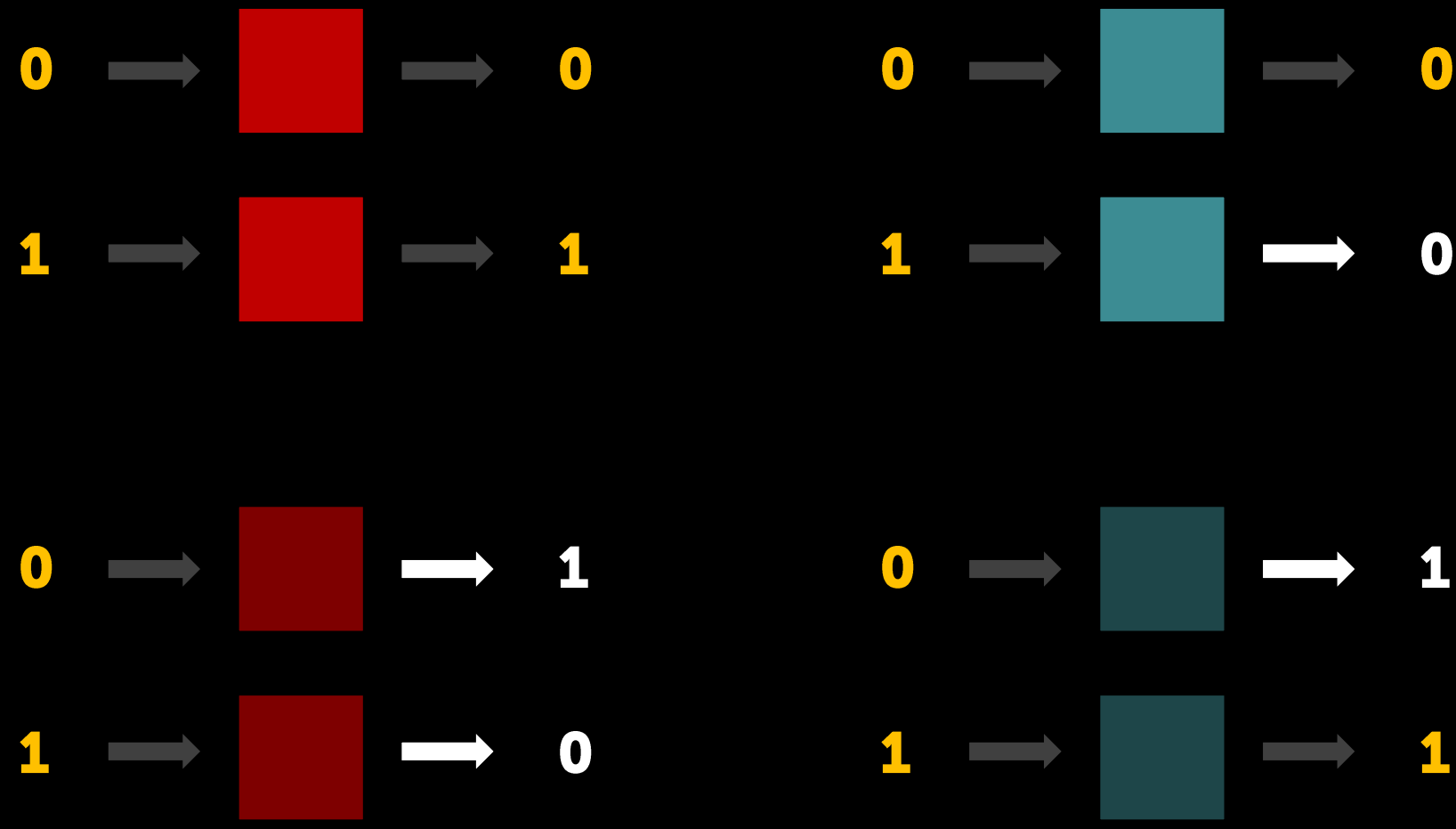



0
0

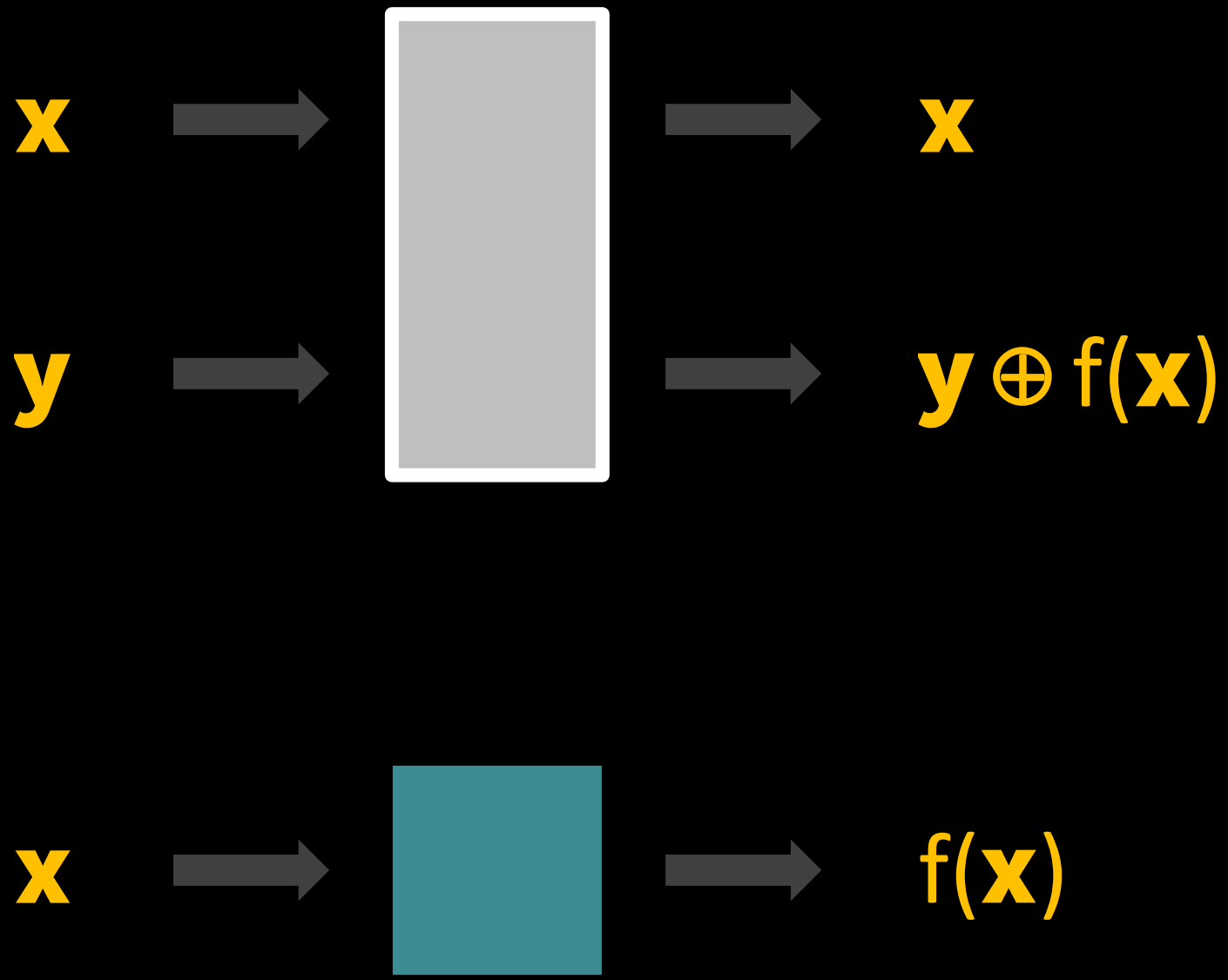

1

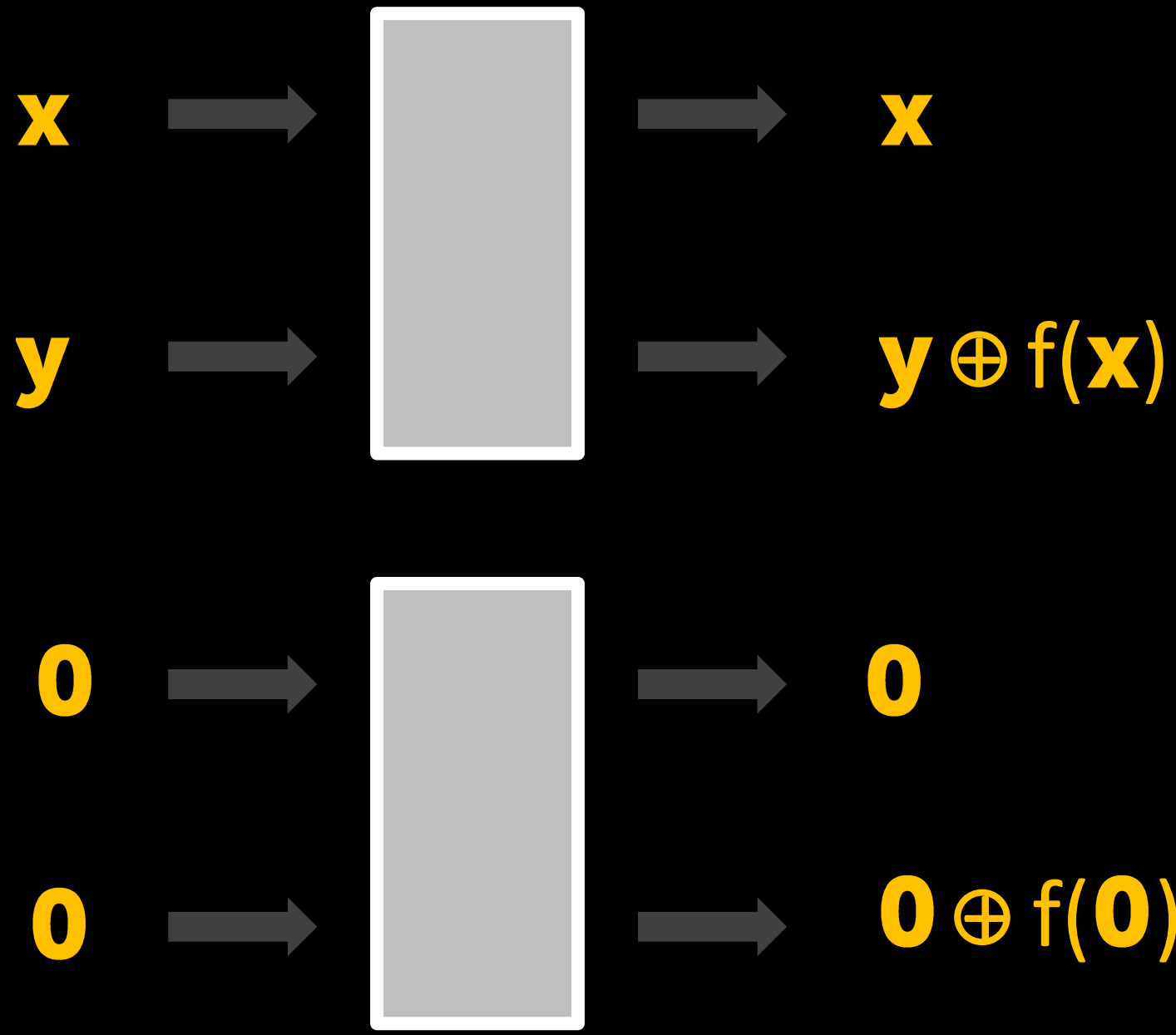

1
0

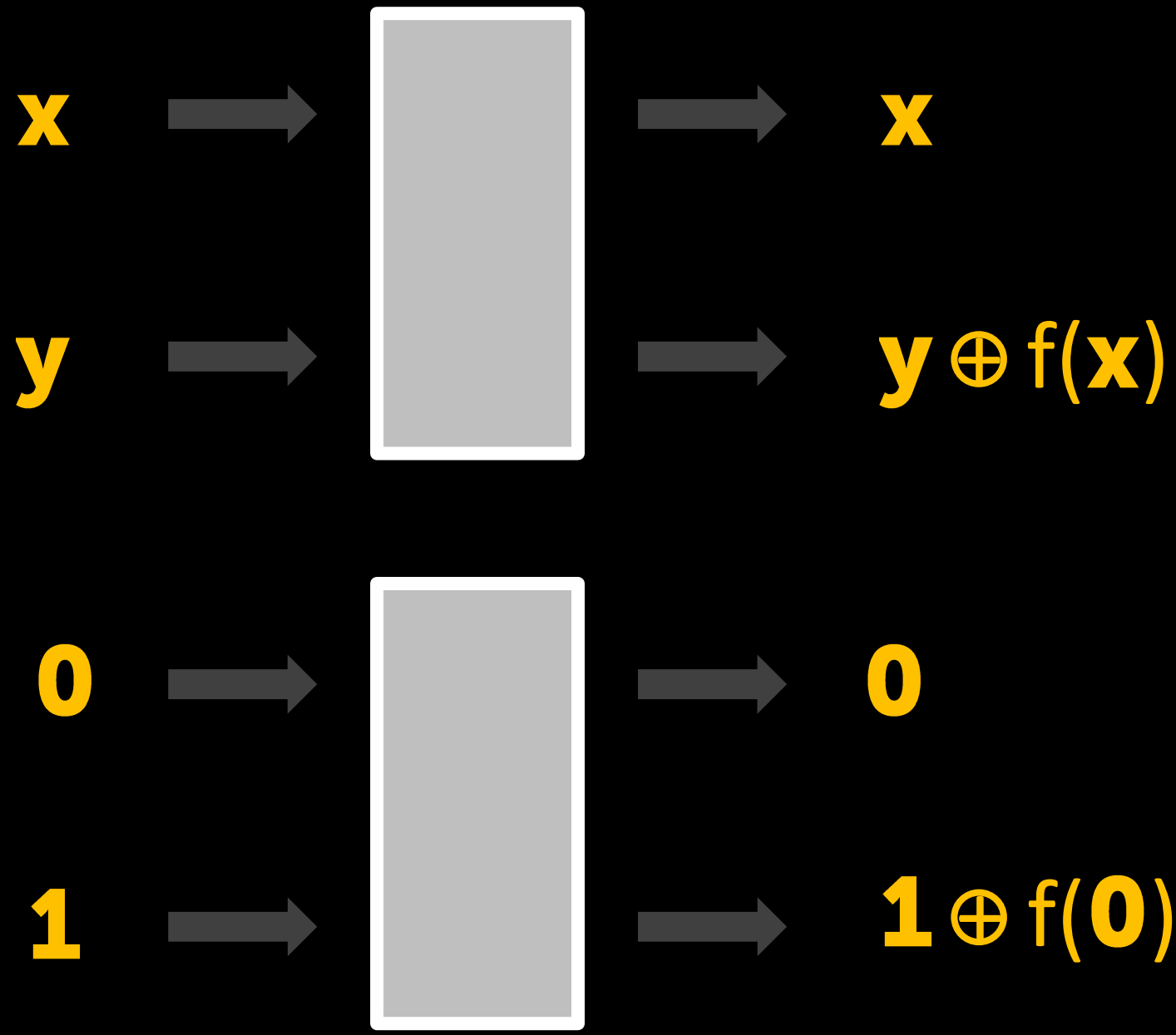
Deutsch-Jozsa

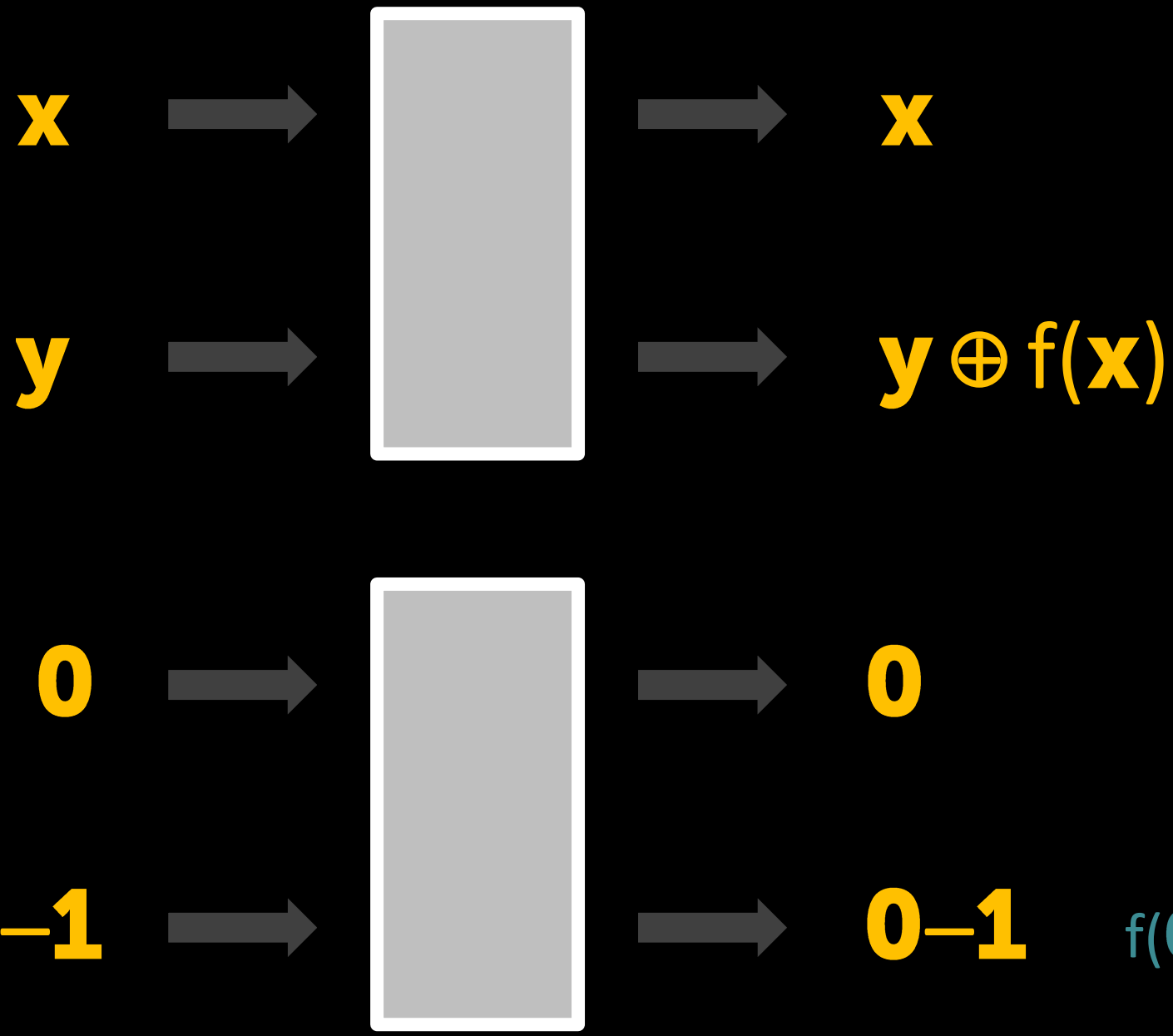


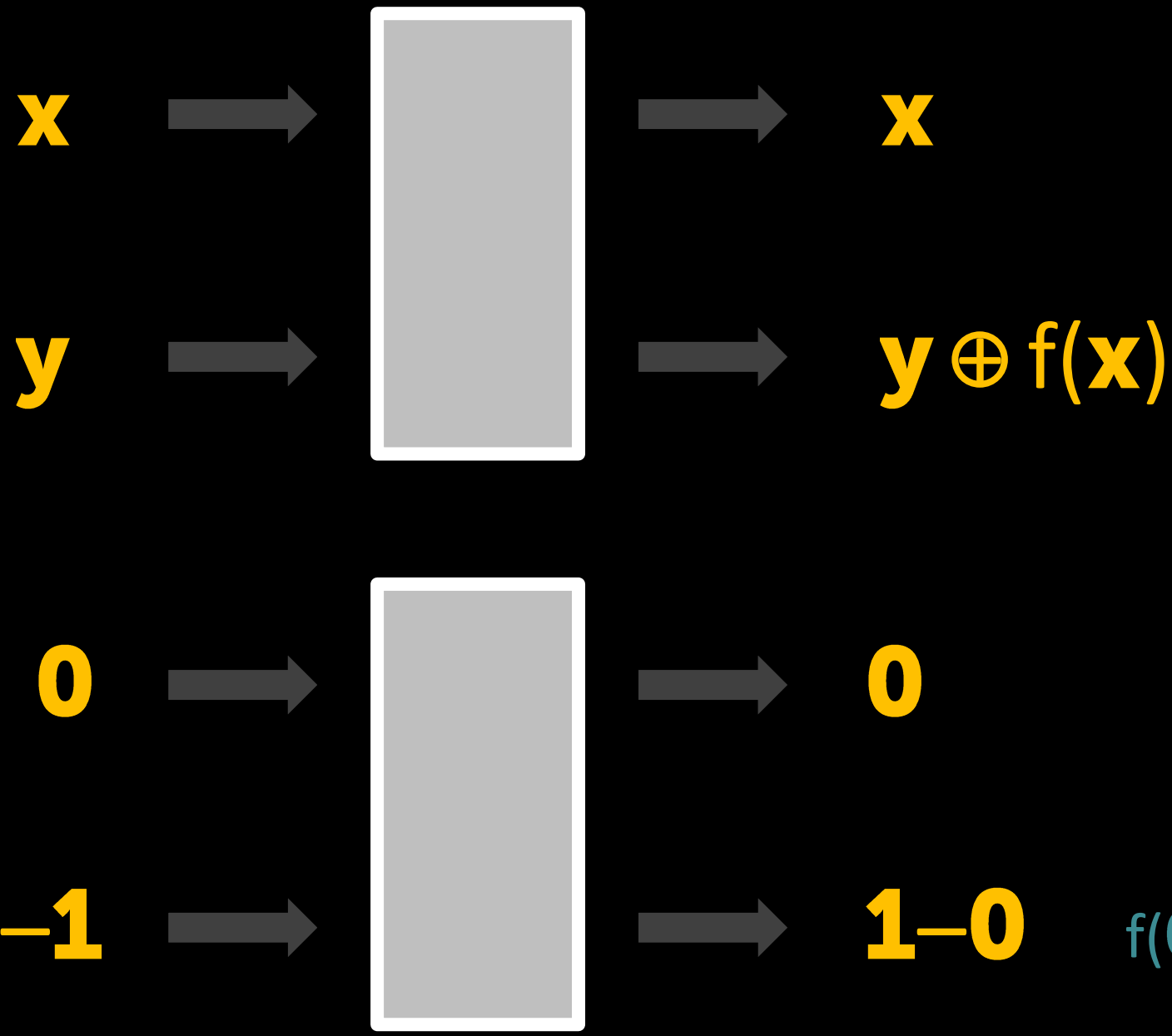

x
f(x)

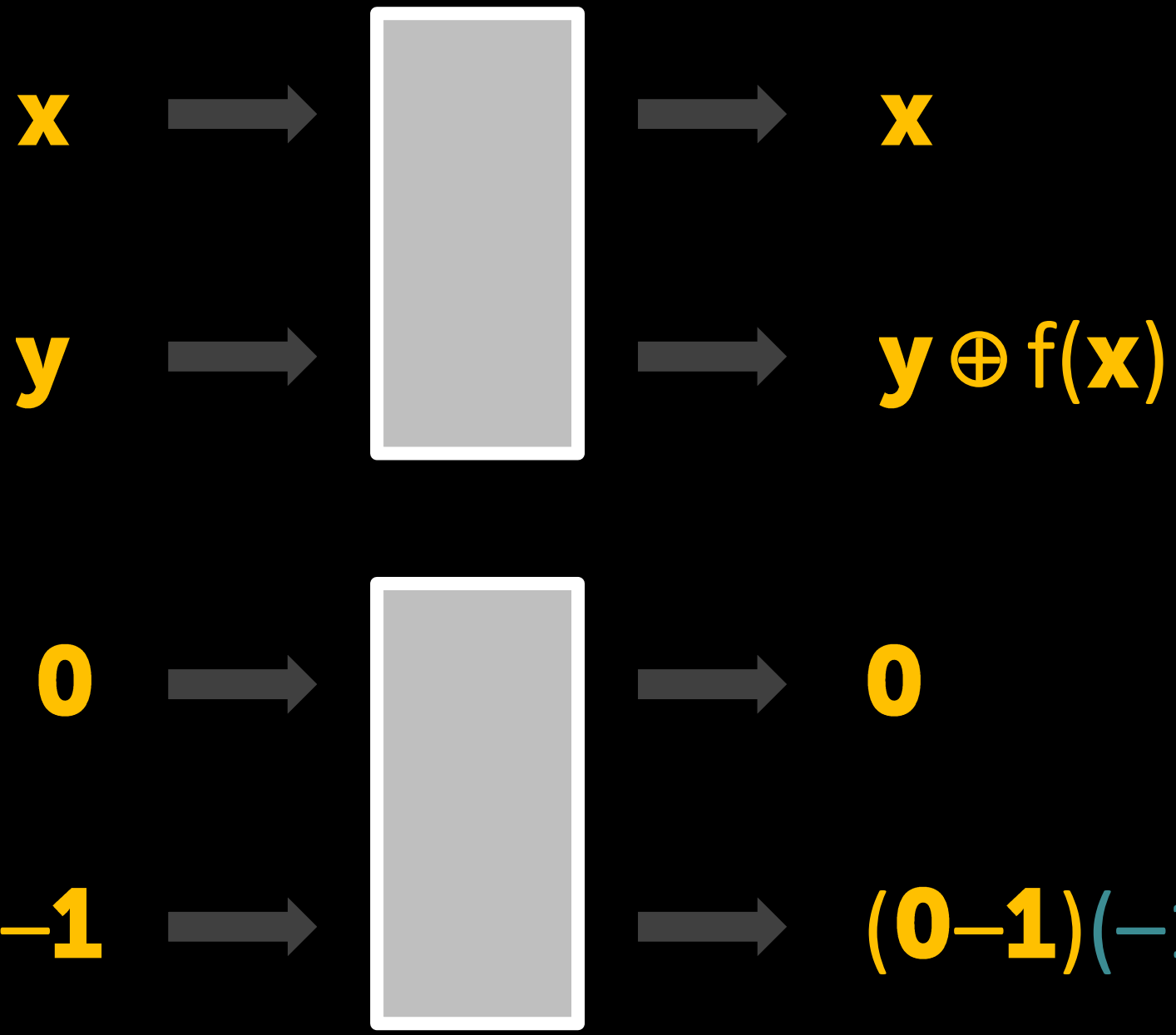

x
y
x
y ⊕ f(x)
x
f(x)

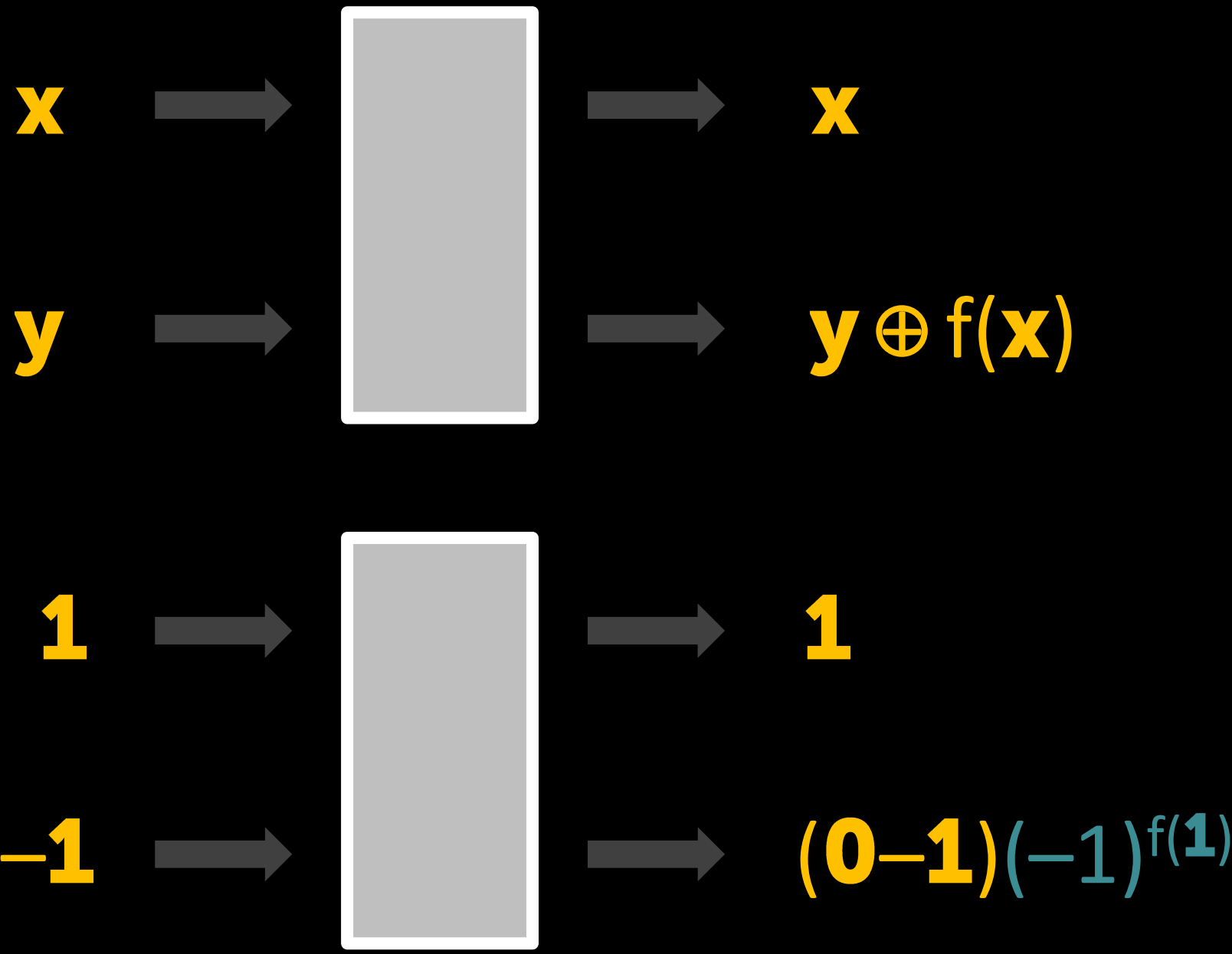

x
y
x
y ⊕ f(x)
0
0
0
0 ⊕ f(0)

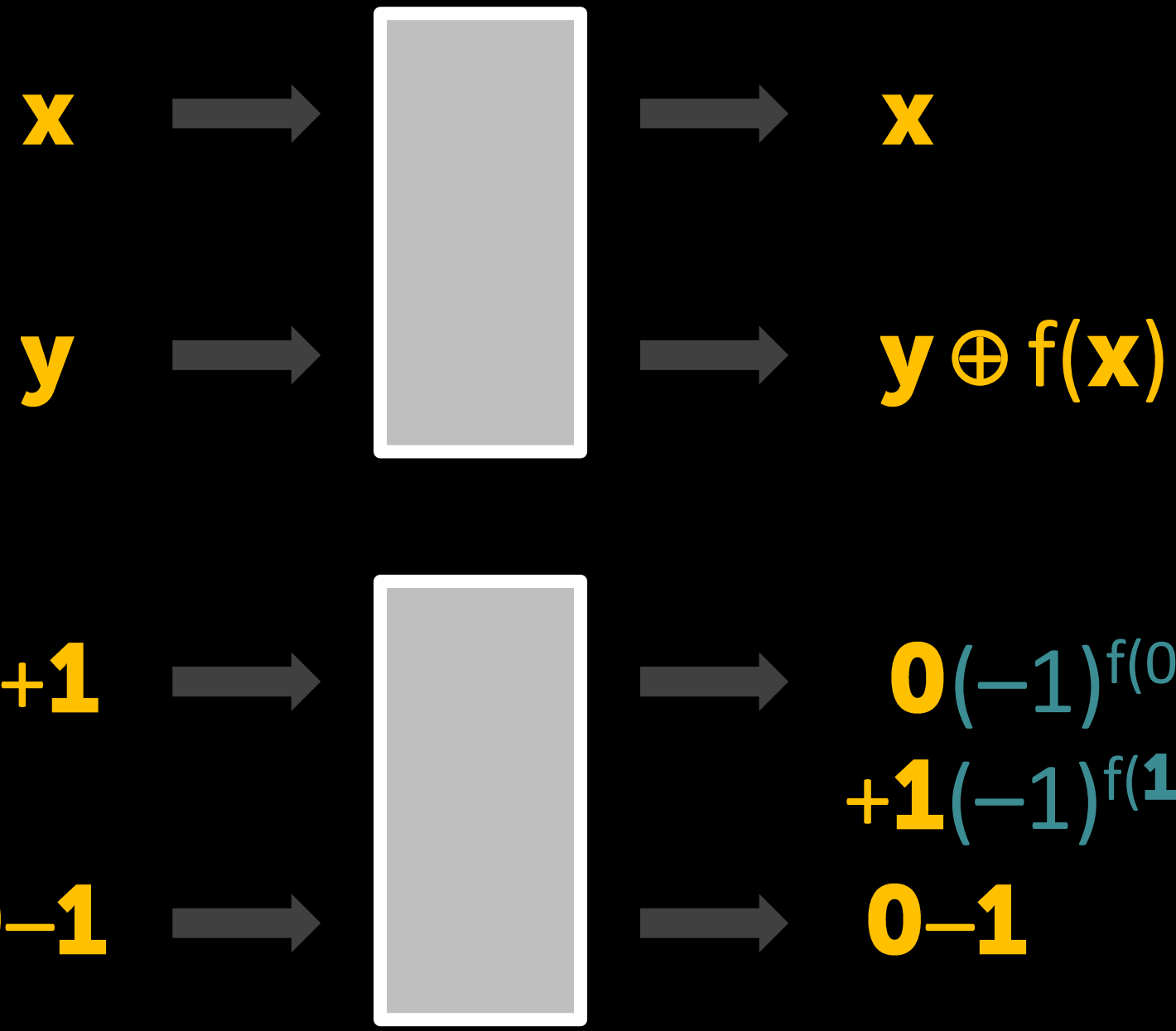

x
y
x
y ⊕ f(x)
0
1
0
1 ⊕ f(0)

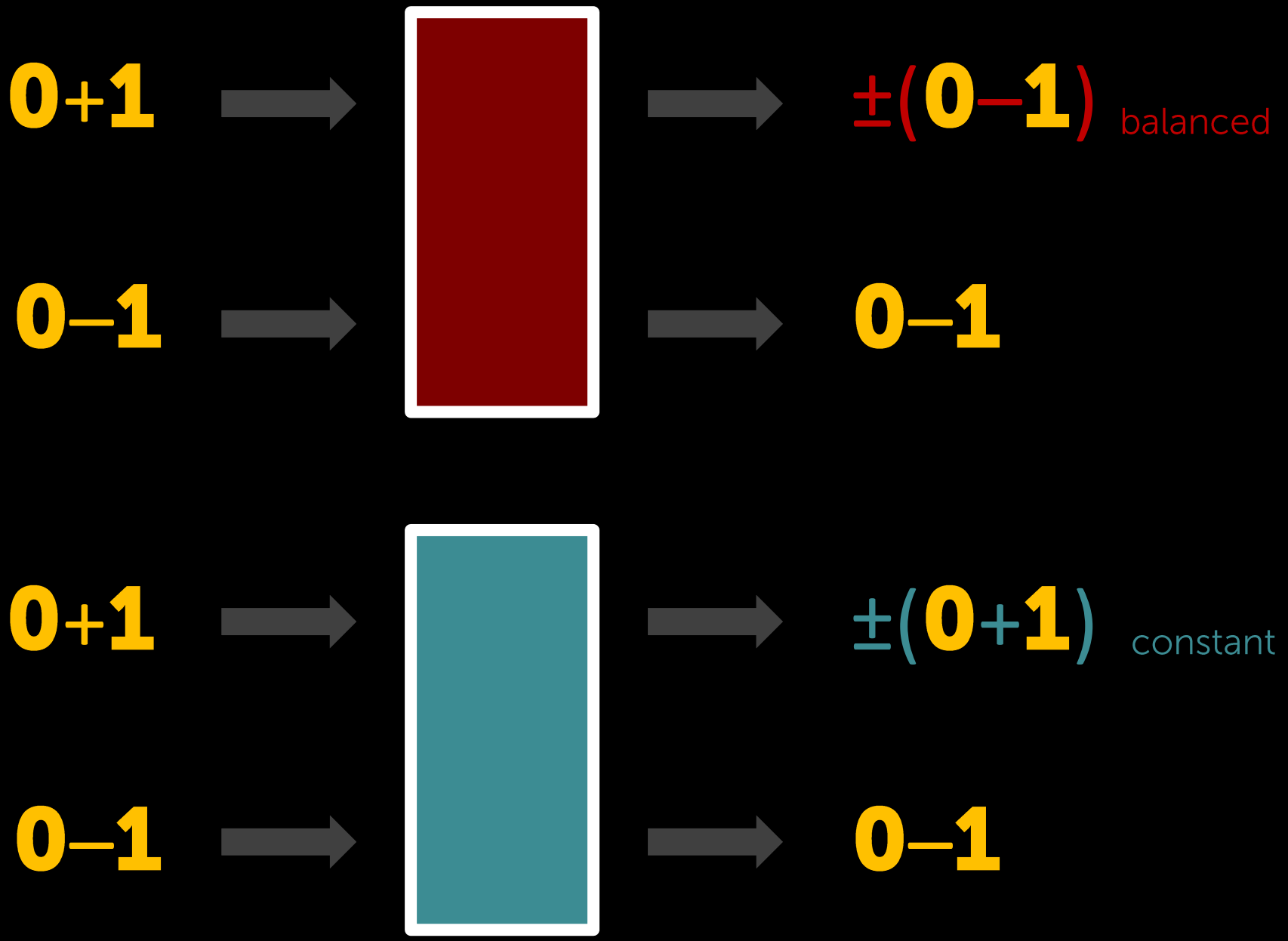

x
x
y
y ⊕ f(x)
0
0
0–1
0–1
f(0) = 0


x
x
y
y ⊕ f(x)
0
0
0–1
1–0
f(0) = 1

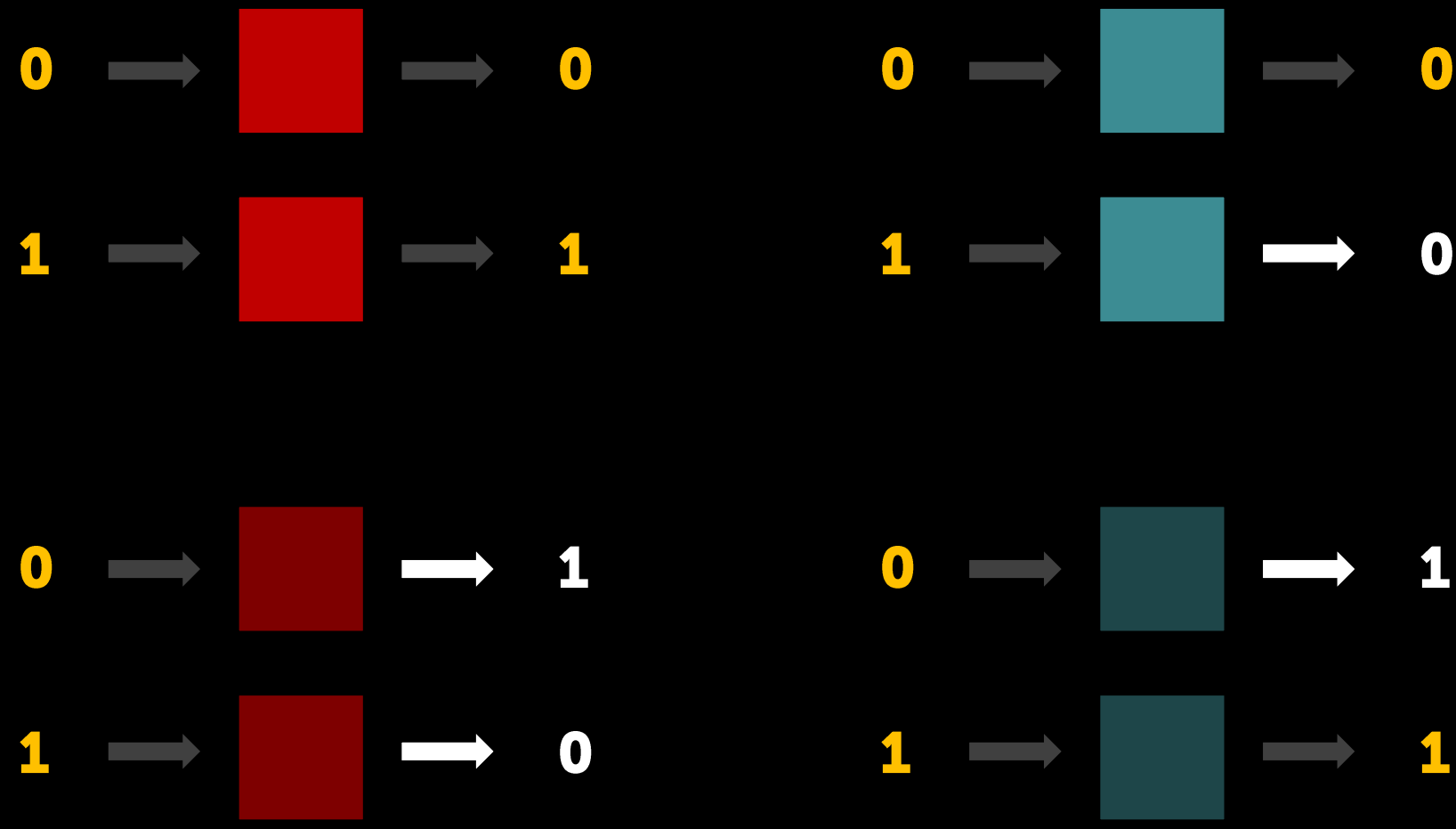

x
y
x
y ⊕ f(x)
0
0–1
0
(0–1)(−1)^f(0)


x
y
x
y ⊕ f(x)
1
0–1
1
(0–1)(−1)^f(1)

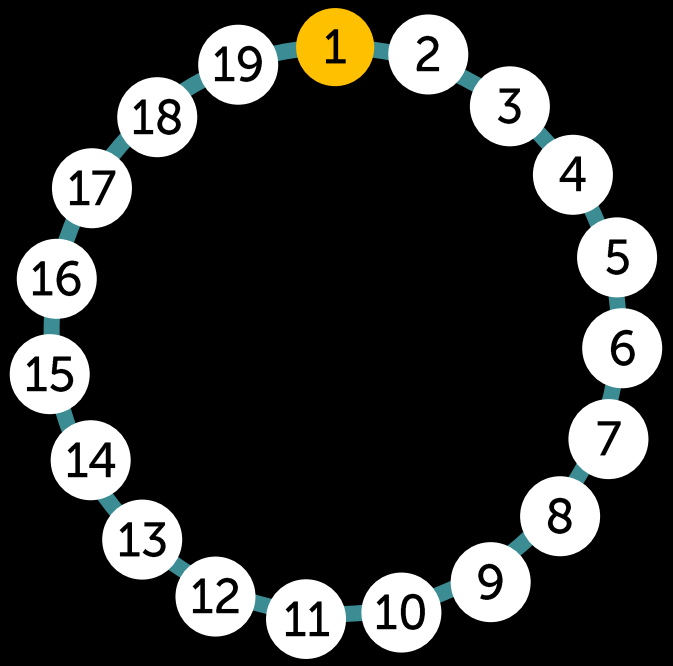

x
y
x
y ⊕ f(x)
0+1
0–1
0(–1)^f(0)
+1(–1)^f(1)
0–1


0+1
0–1
±(0–1)
balanced
0–1
0+1
0–1
±(0+1)
constant
0–1

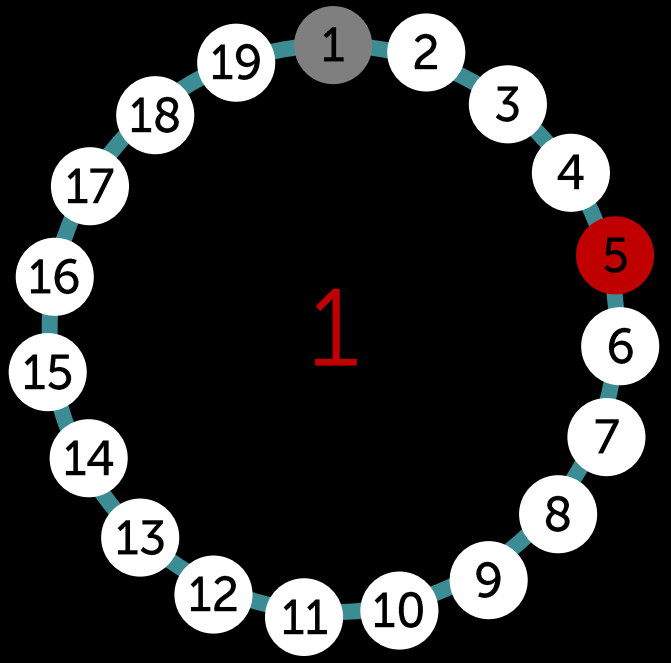
Deutsch-Jozsa, Simon, Shor...



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

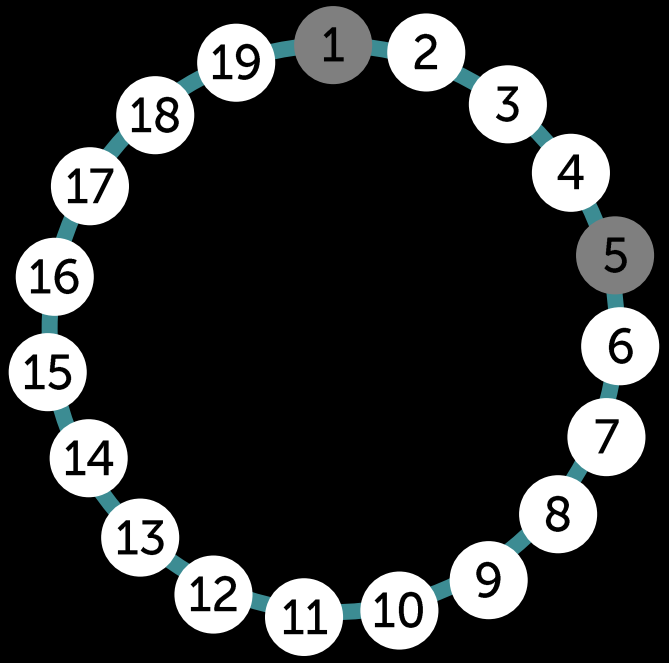


Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



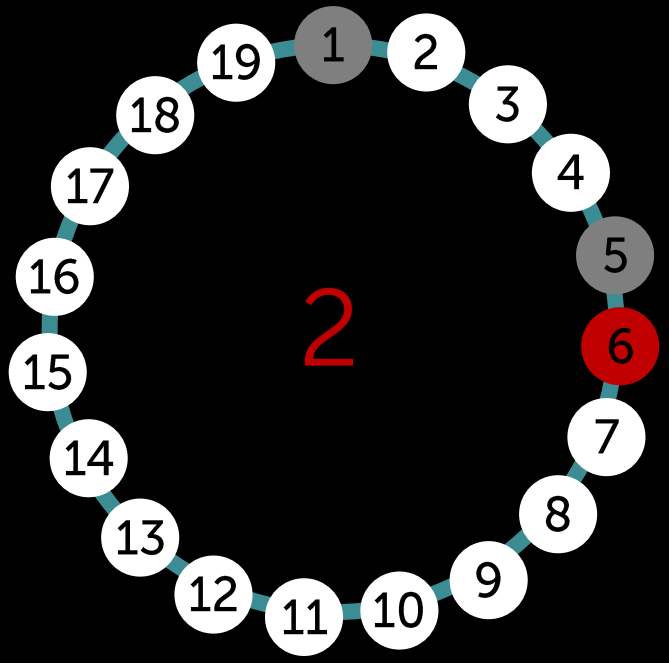
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

$5 \times 5 = 25$



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

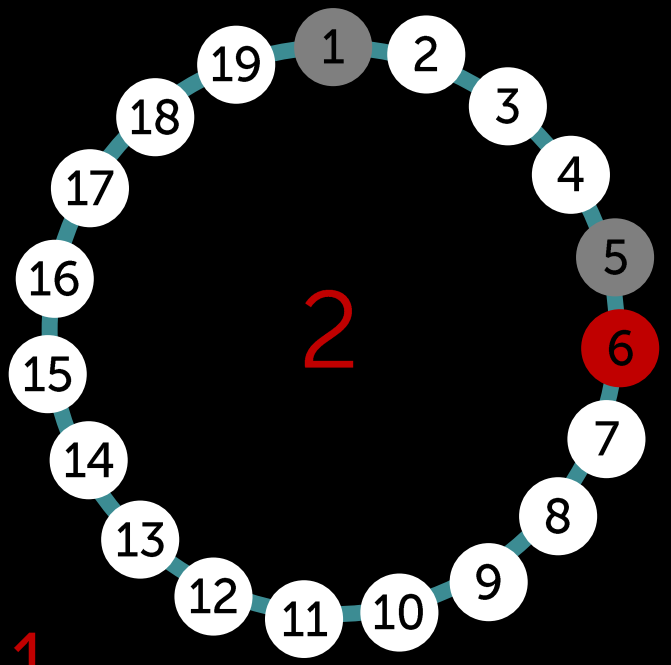
$5 \times 5 = 19 + 6$



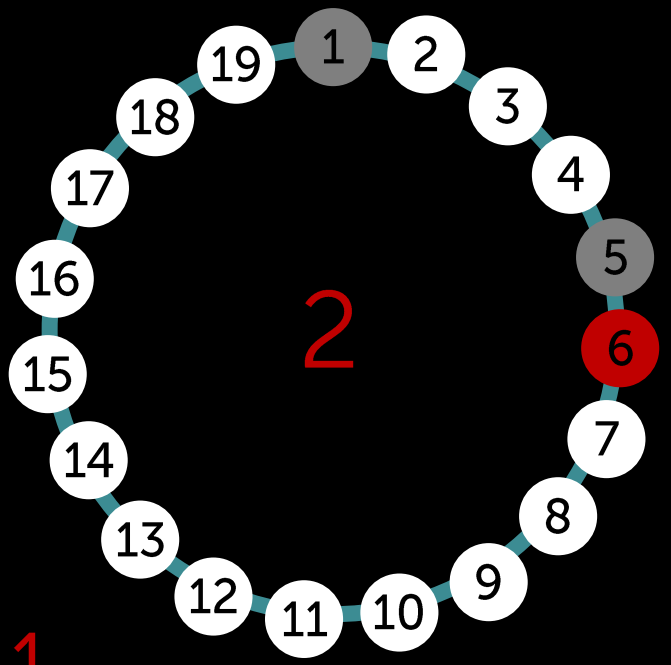
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

$5 \times 5 = 19 + 6$

$25 \times 5 = 19 \times \ldots + 11$



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

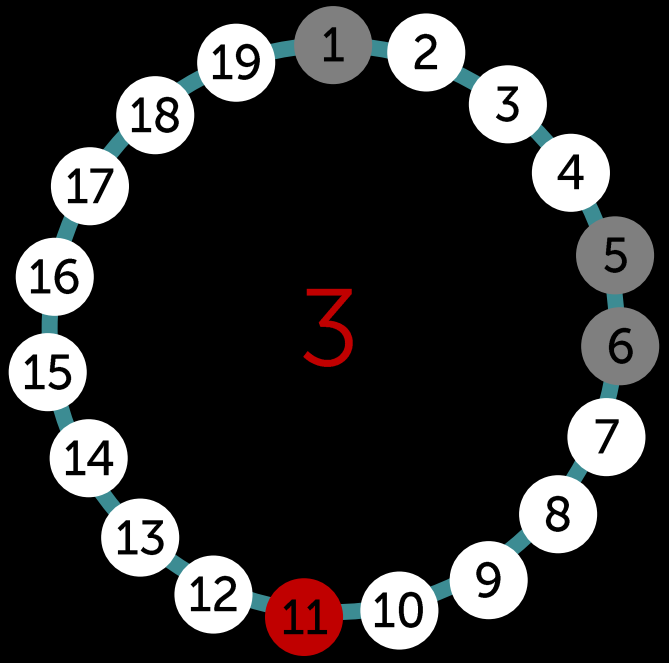


$5 \times 5 = 19 + 6$

$25 \times 5 = 19 \times \ldots + 11$

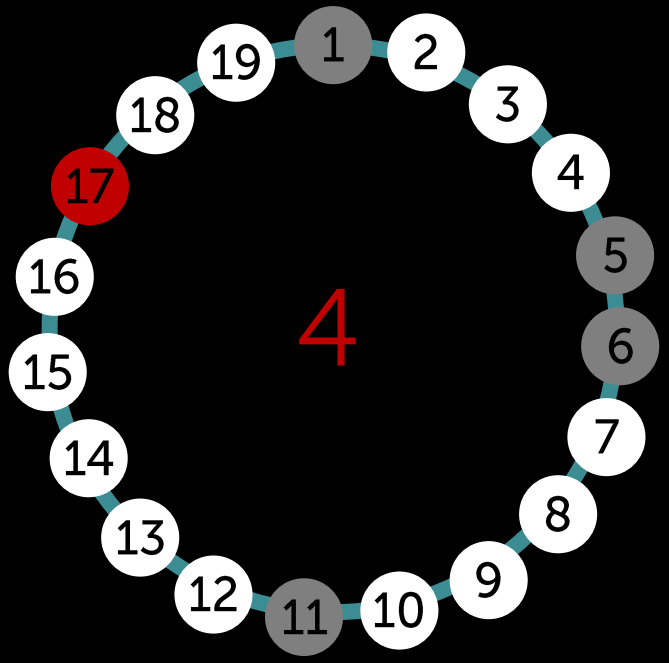
$6 \times 5 = 19 \times \ldots + 11$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



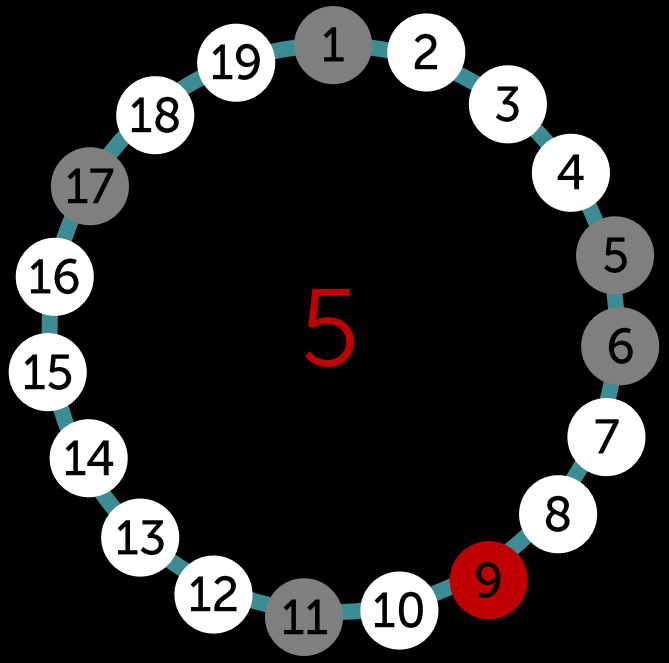
$5^3 = 19 \times \ldots + 11$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



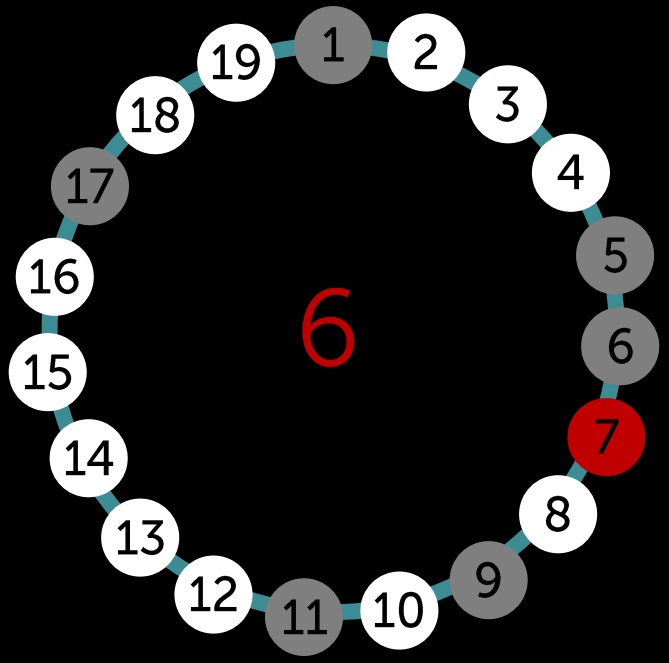
$5^4 = 19 \times \ldots + 17$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



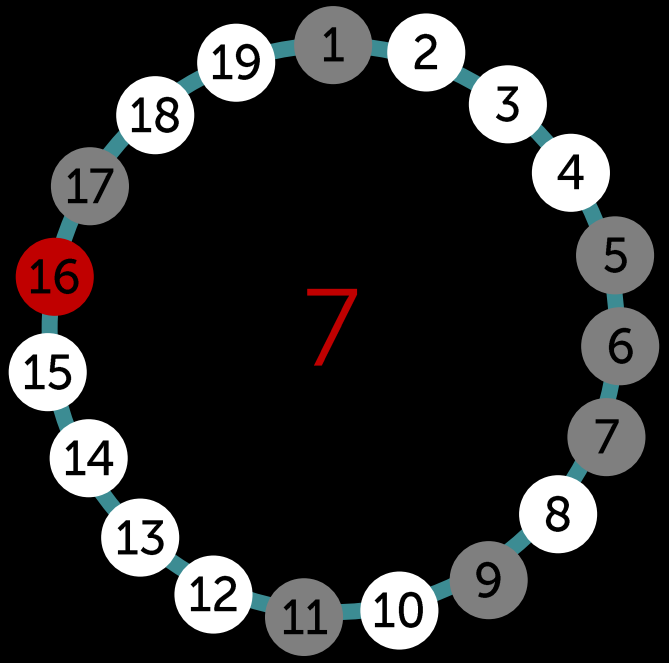
$5^5 = 19 \times \ldots + 9$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



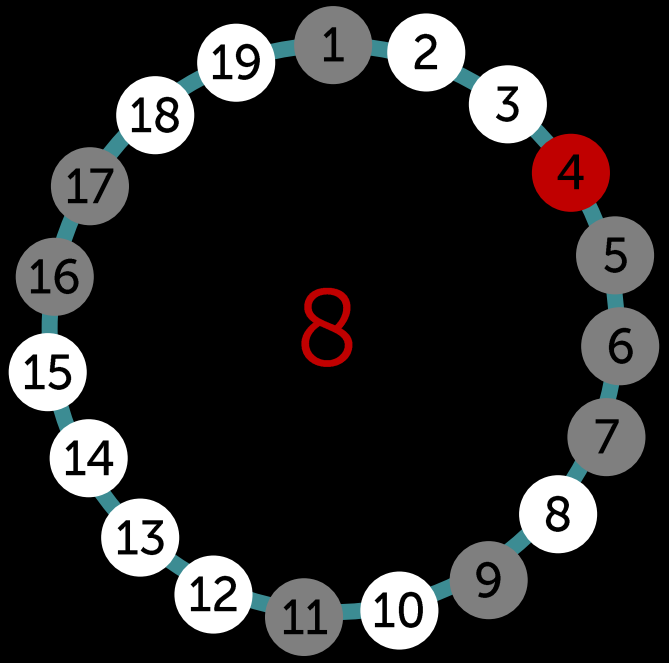
$5^6 = 19 \times \ldots + 7$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



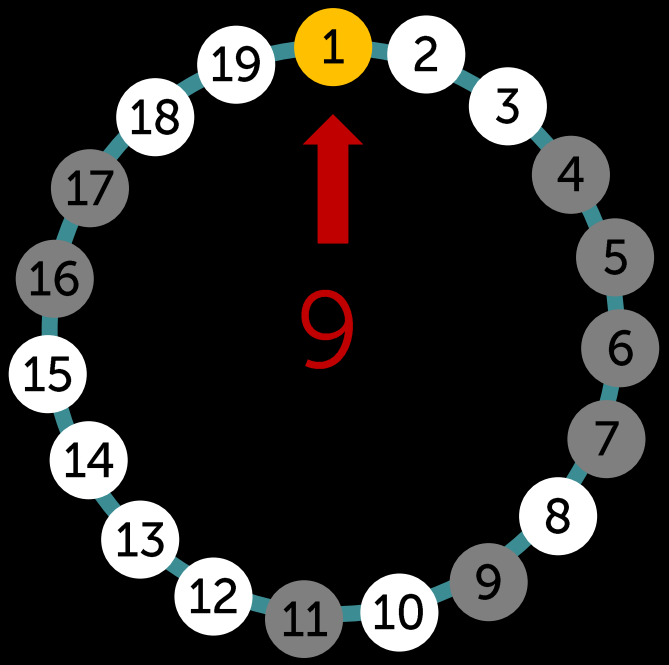
$5^7 = 19 \times \ldots + 16$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



$5^8 = 19 \times \ldots + 4$

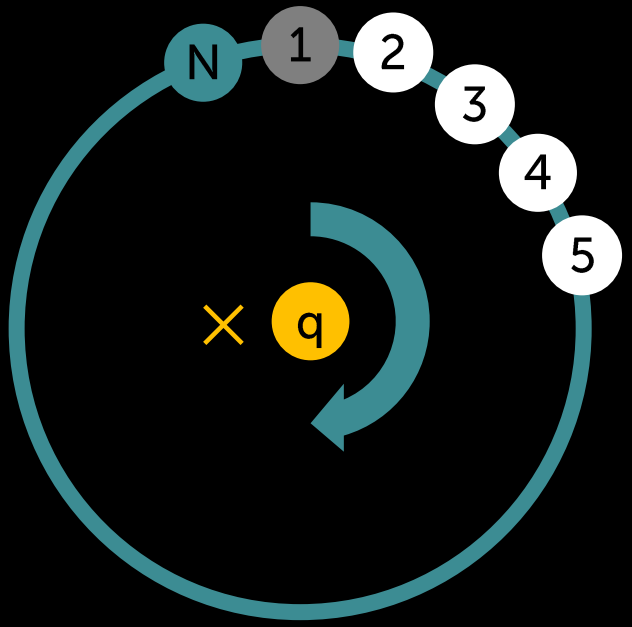
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



$5^9 = 19 \times \ldots + 1$

$$q^r = 1 \bmod N$$

$$r = ?$$



faktorizácia

teória čísel

superpozície a Fourier

super kvantový algoritmus

Peter Shor

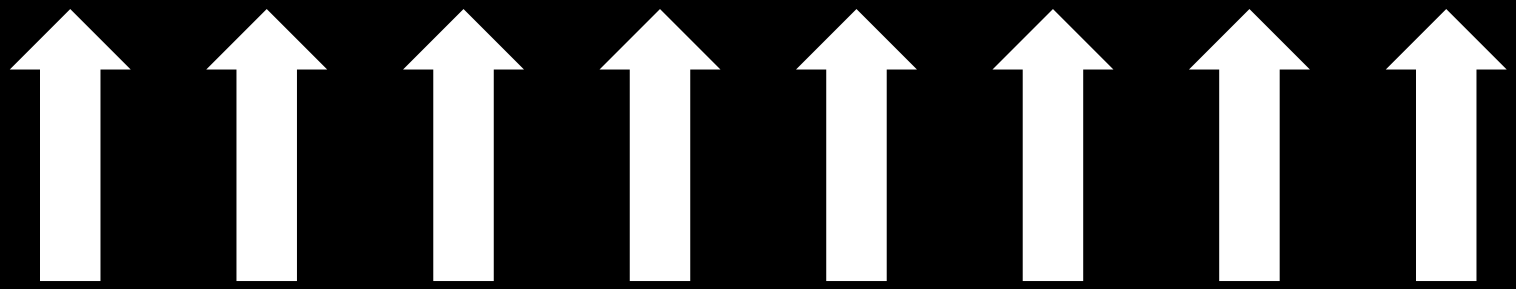
RSA ☹

$21 = 3 \times 7$

ihla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s ena ihla v kope sena ihla v kope sena i hla v kope sena ihla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s

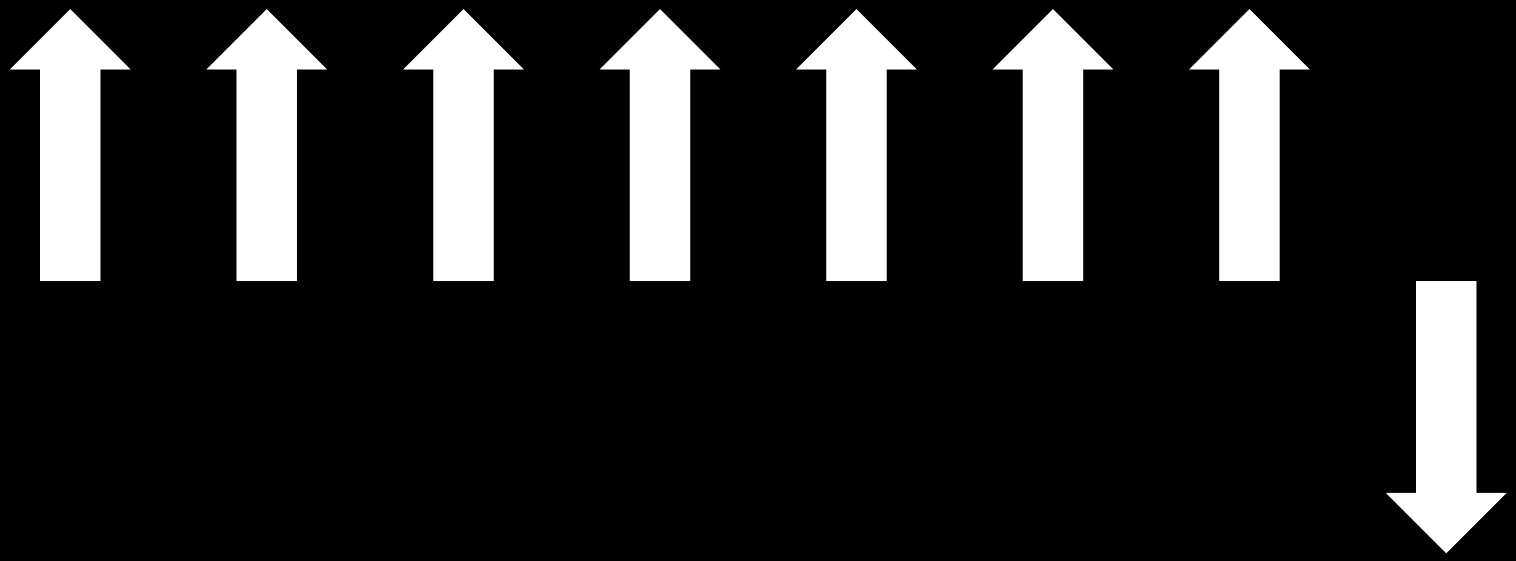
ihla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s ena ihla v kope sena ihla v kope sena i hla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s

neštruktúrované hľadanie

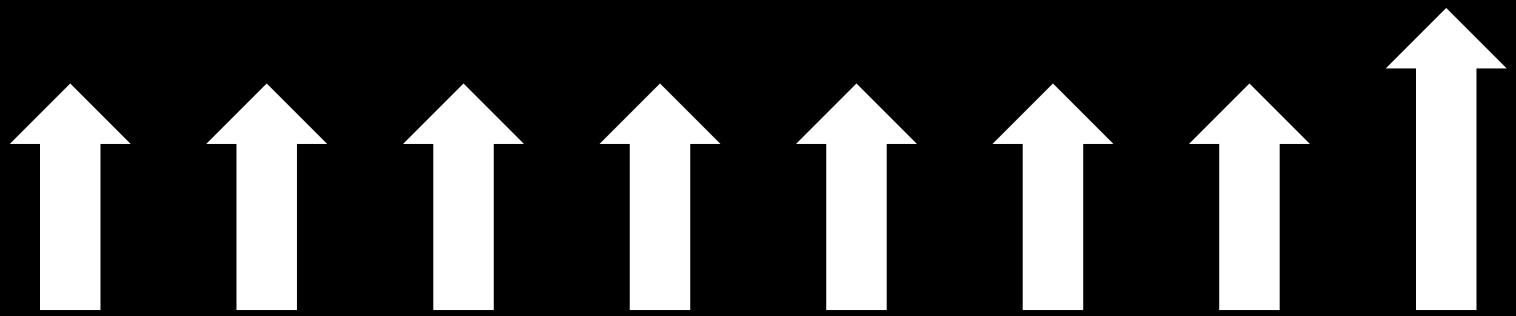


1. zmeň znamienko riešenia
2. prevráť okolo superpozície

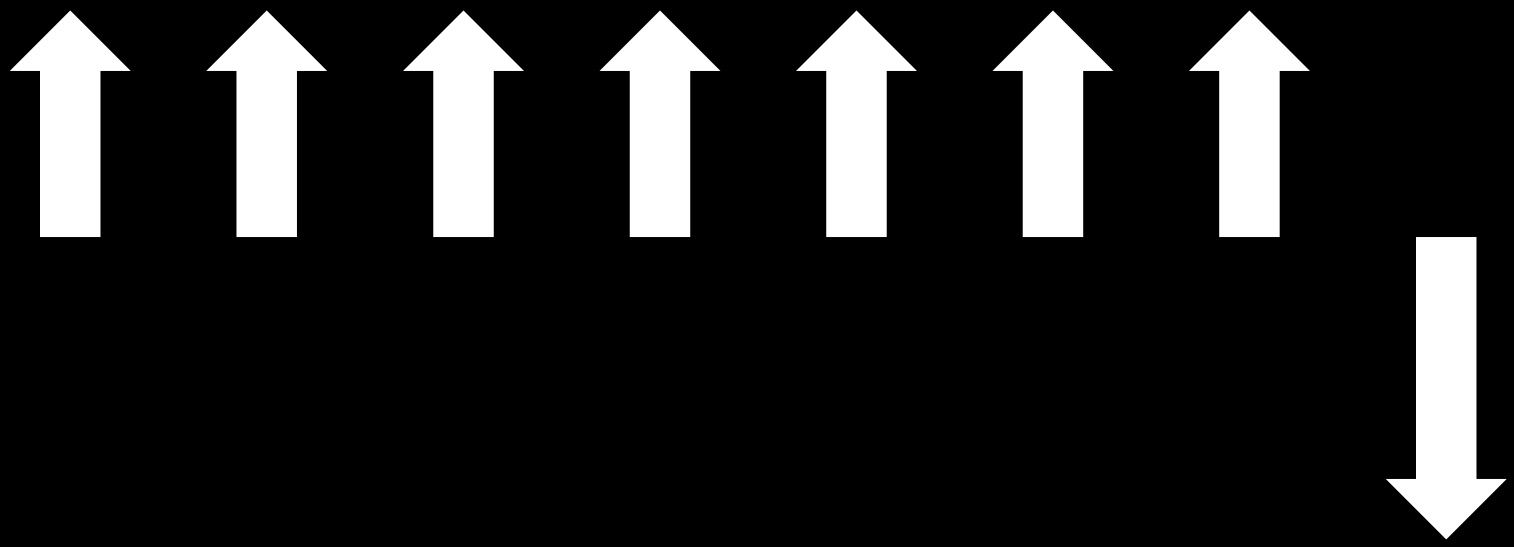
neštruktúrované hľadanie



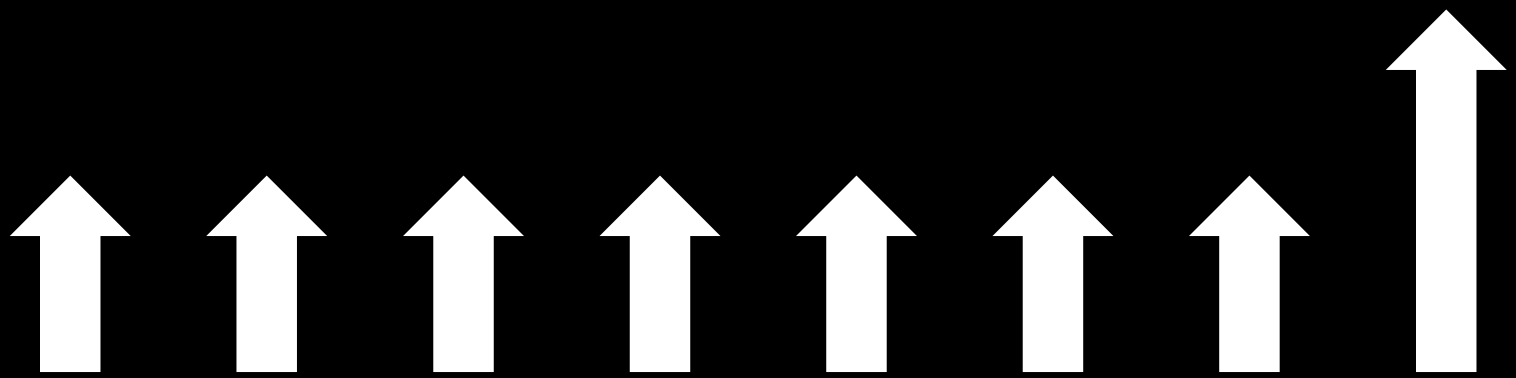
neštruktúrované hľadanie



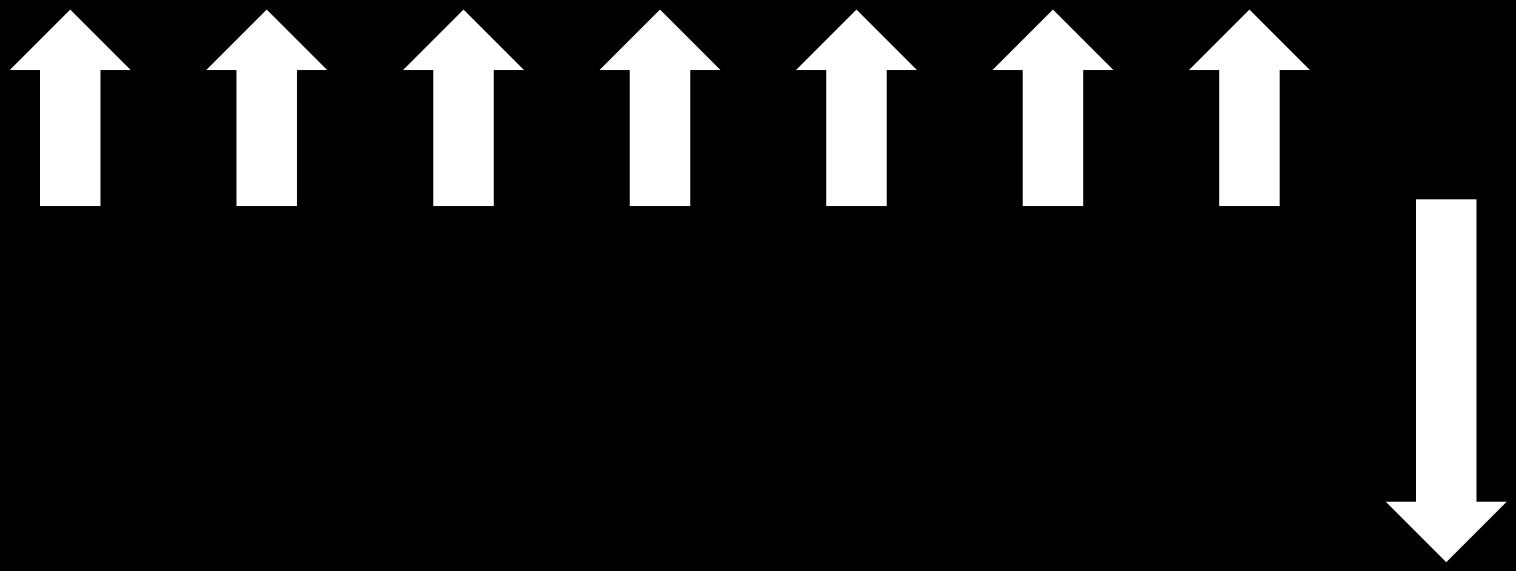
neštruktúrované hľadanie



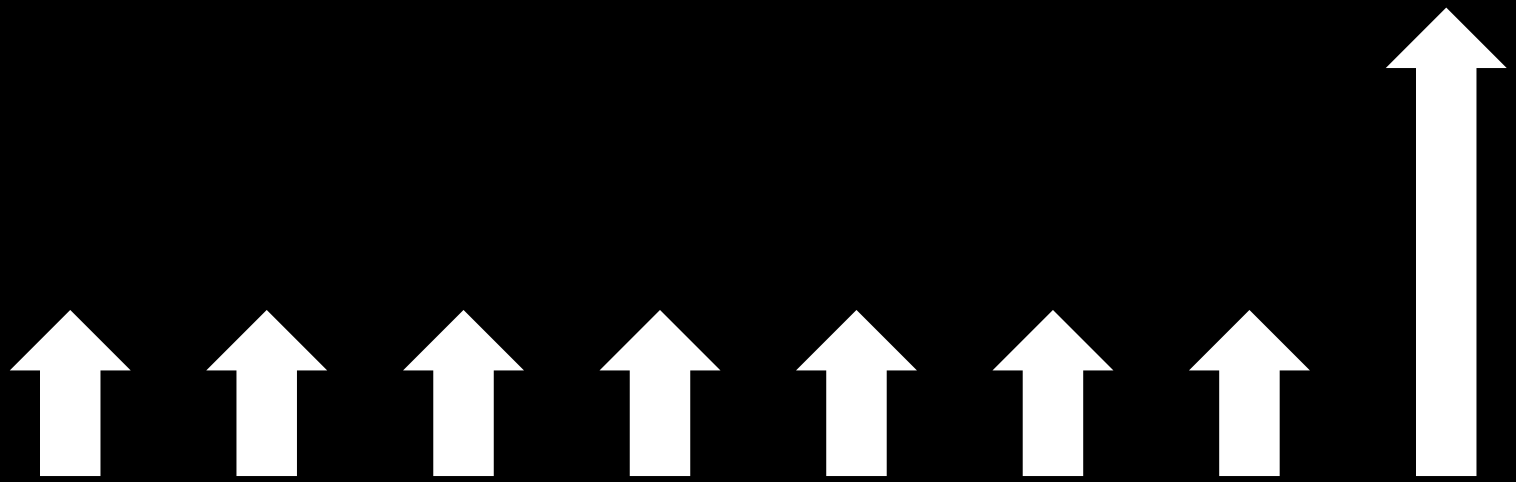
neštruktúrované hľadanie



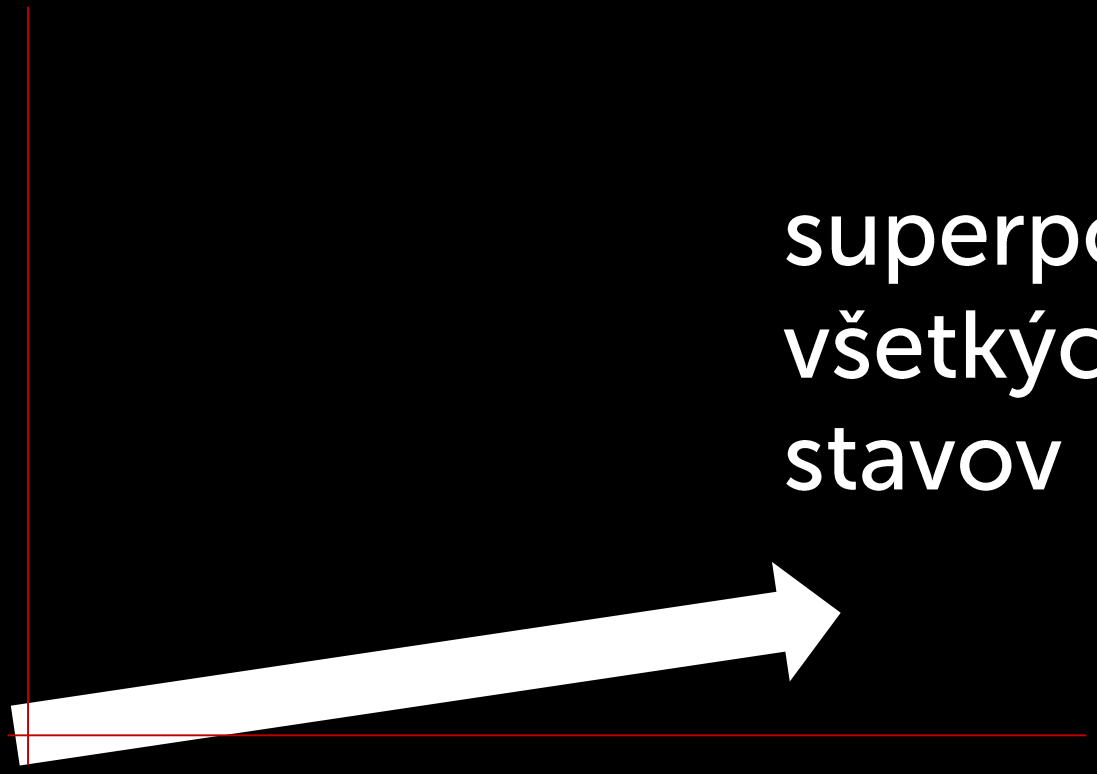
neštruktúrované hľadanie



neštruktúrované hľadanie



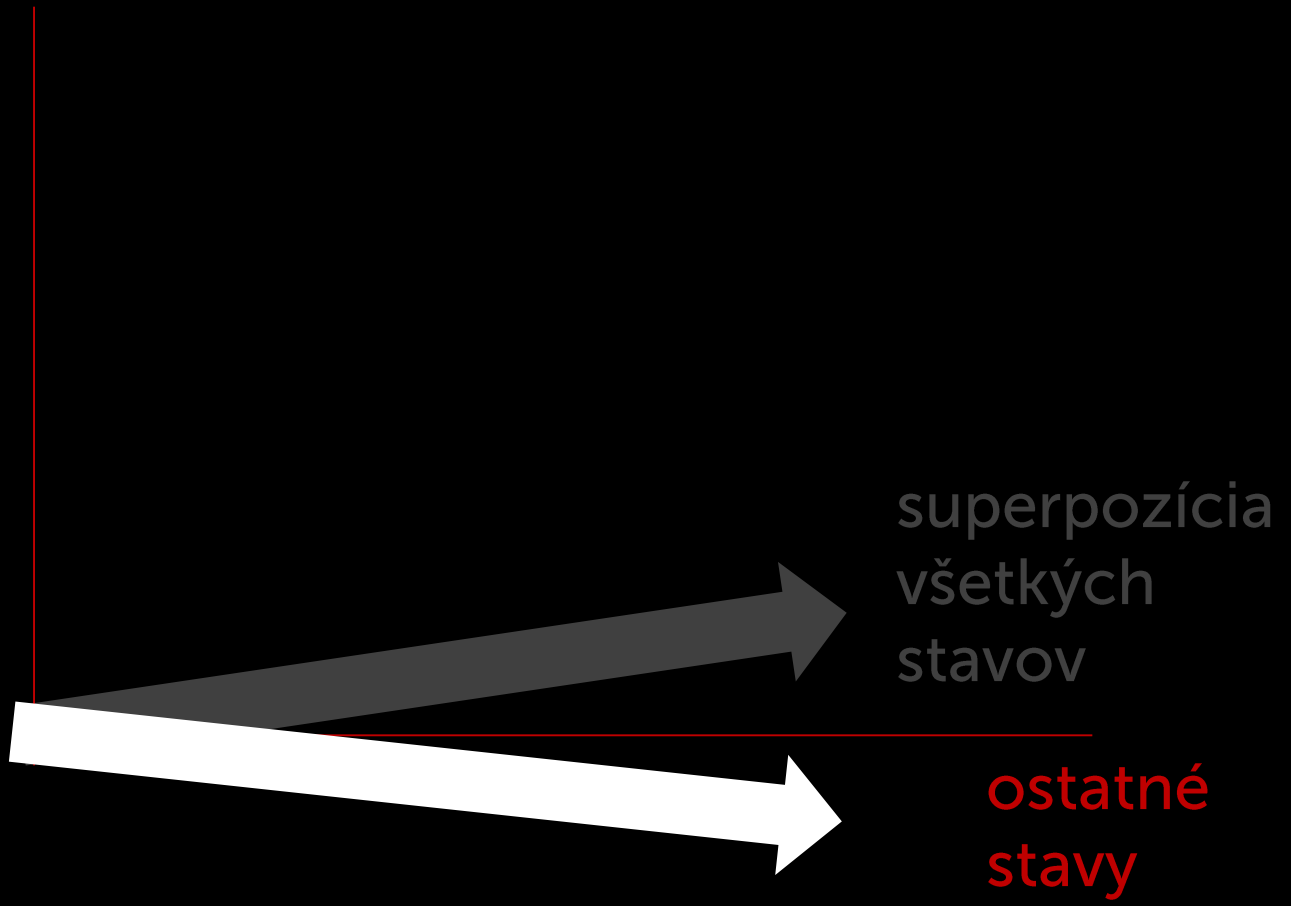
riešenie



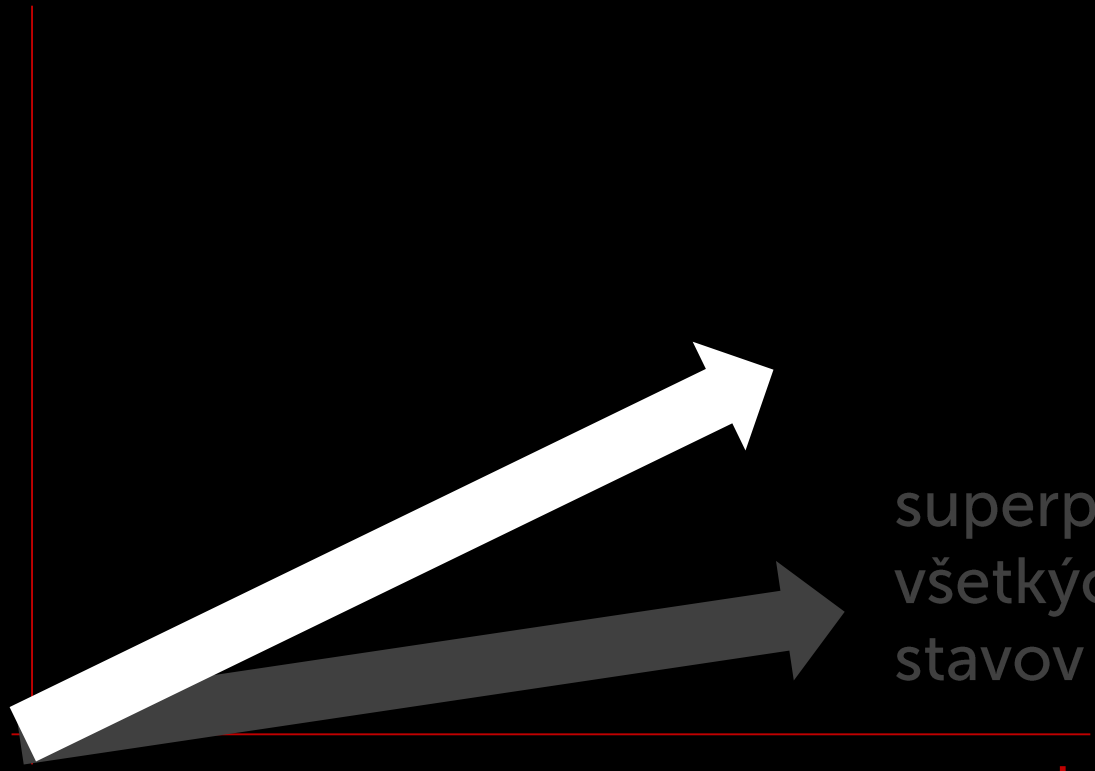
superpozícia
všetkých
stavov

ostatné
stavy

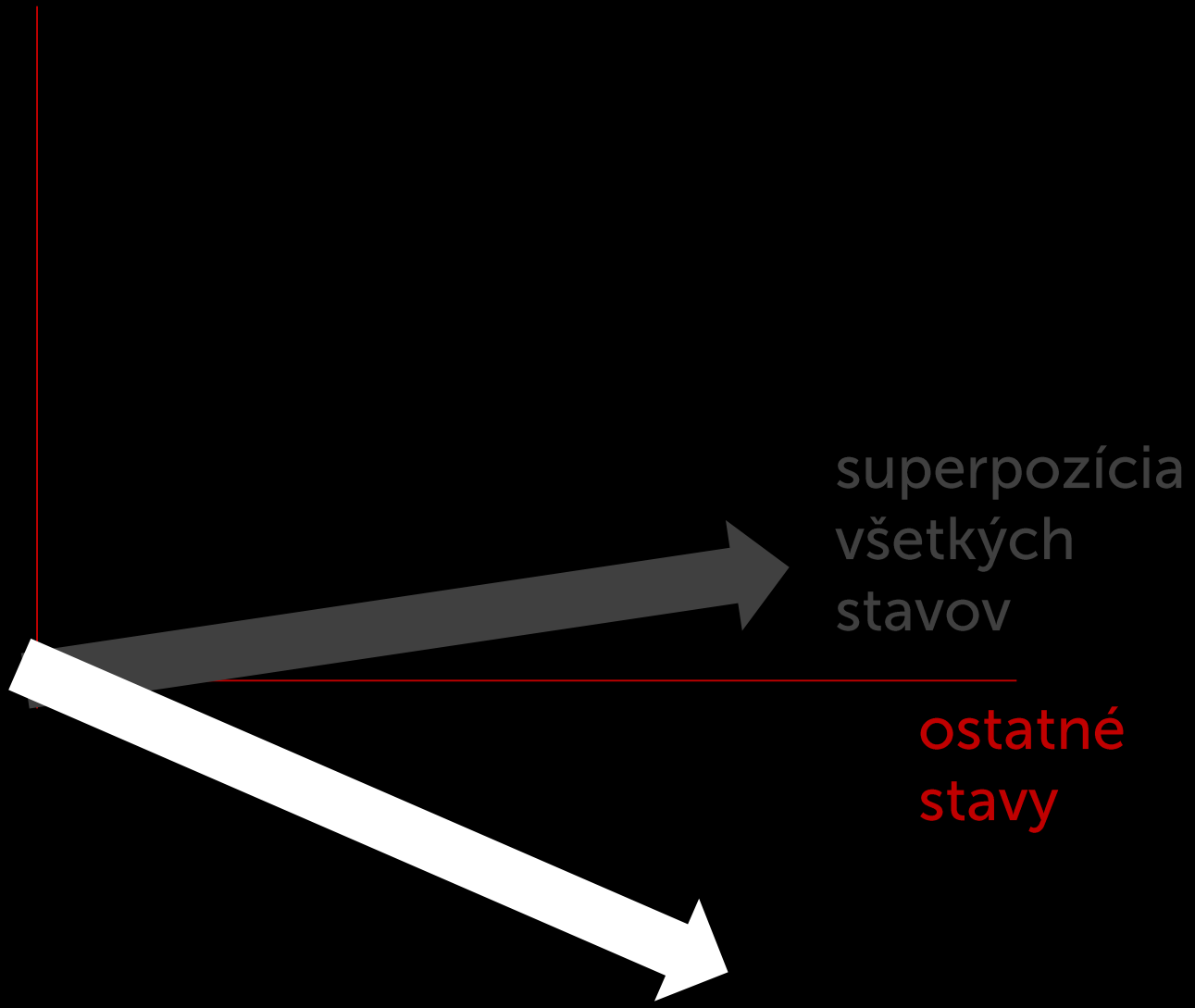
riešenie



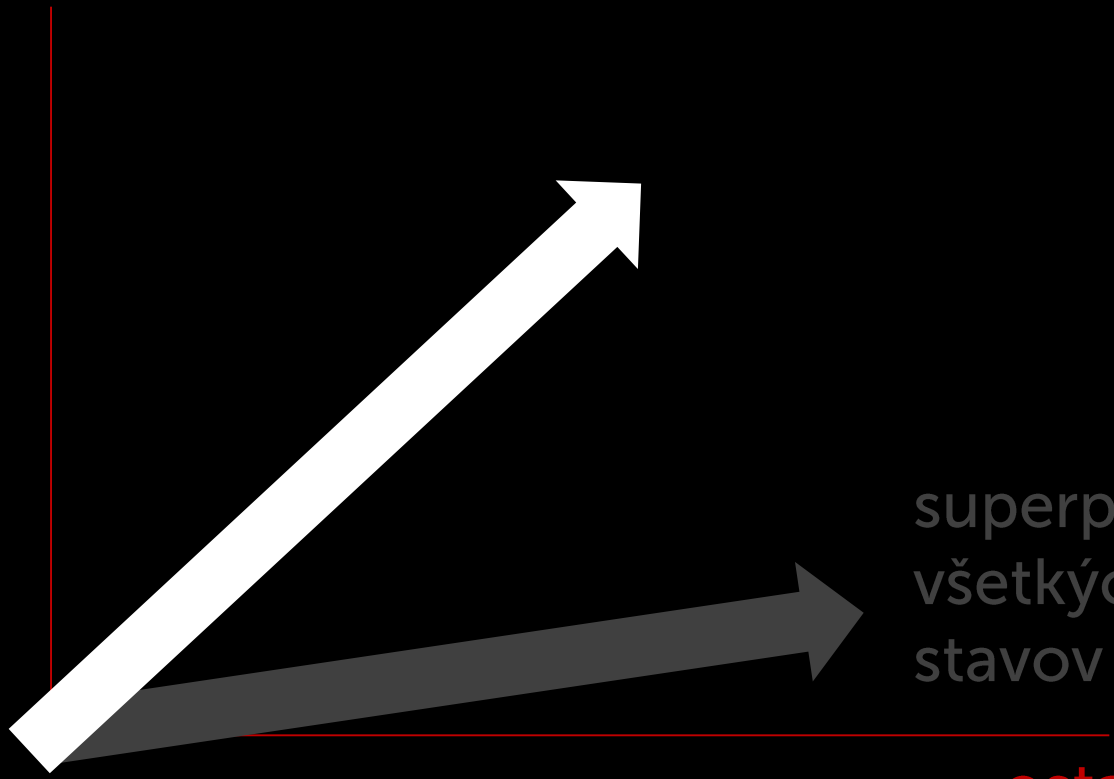
riešenie



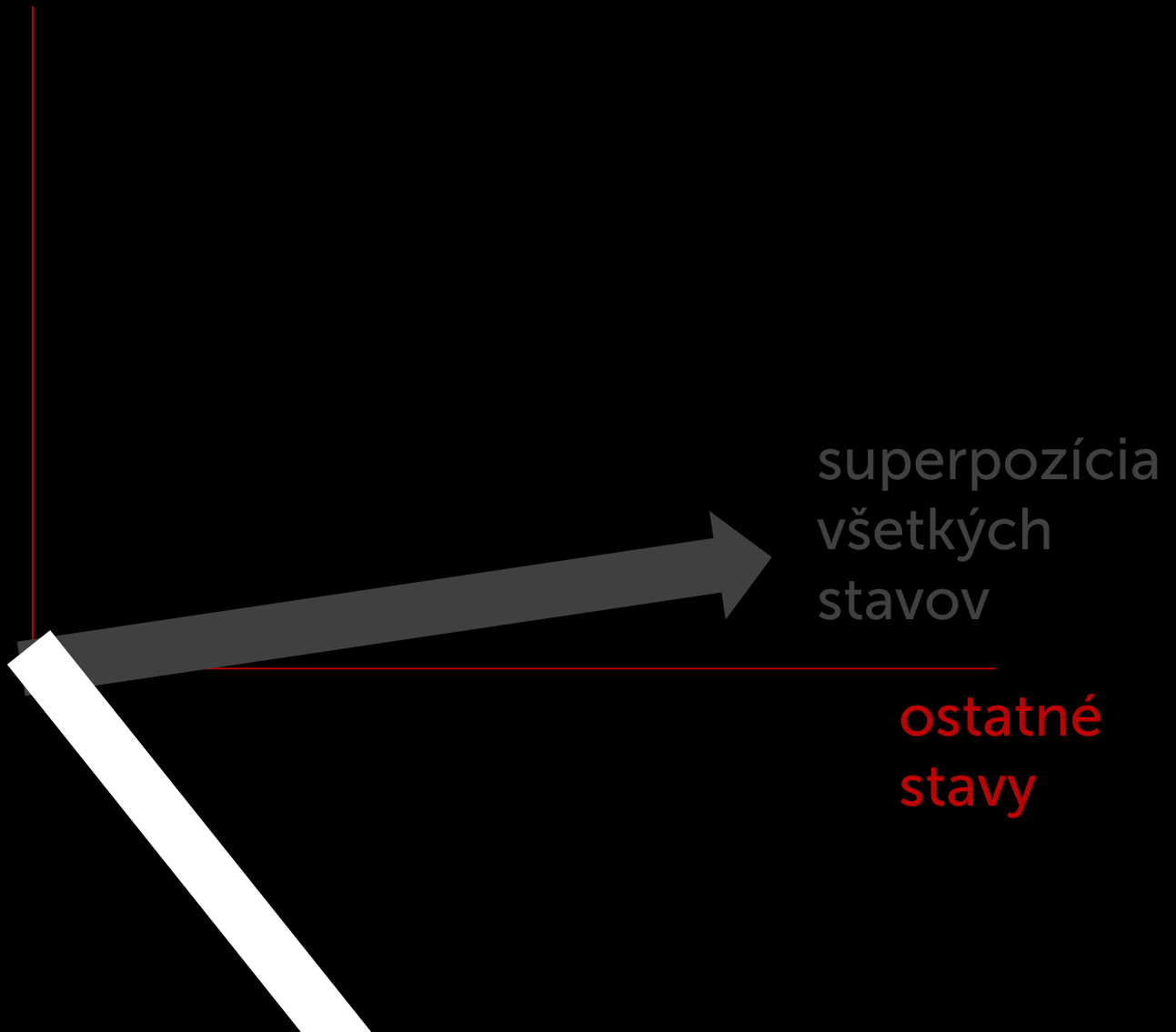
riešenie

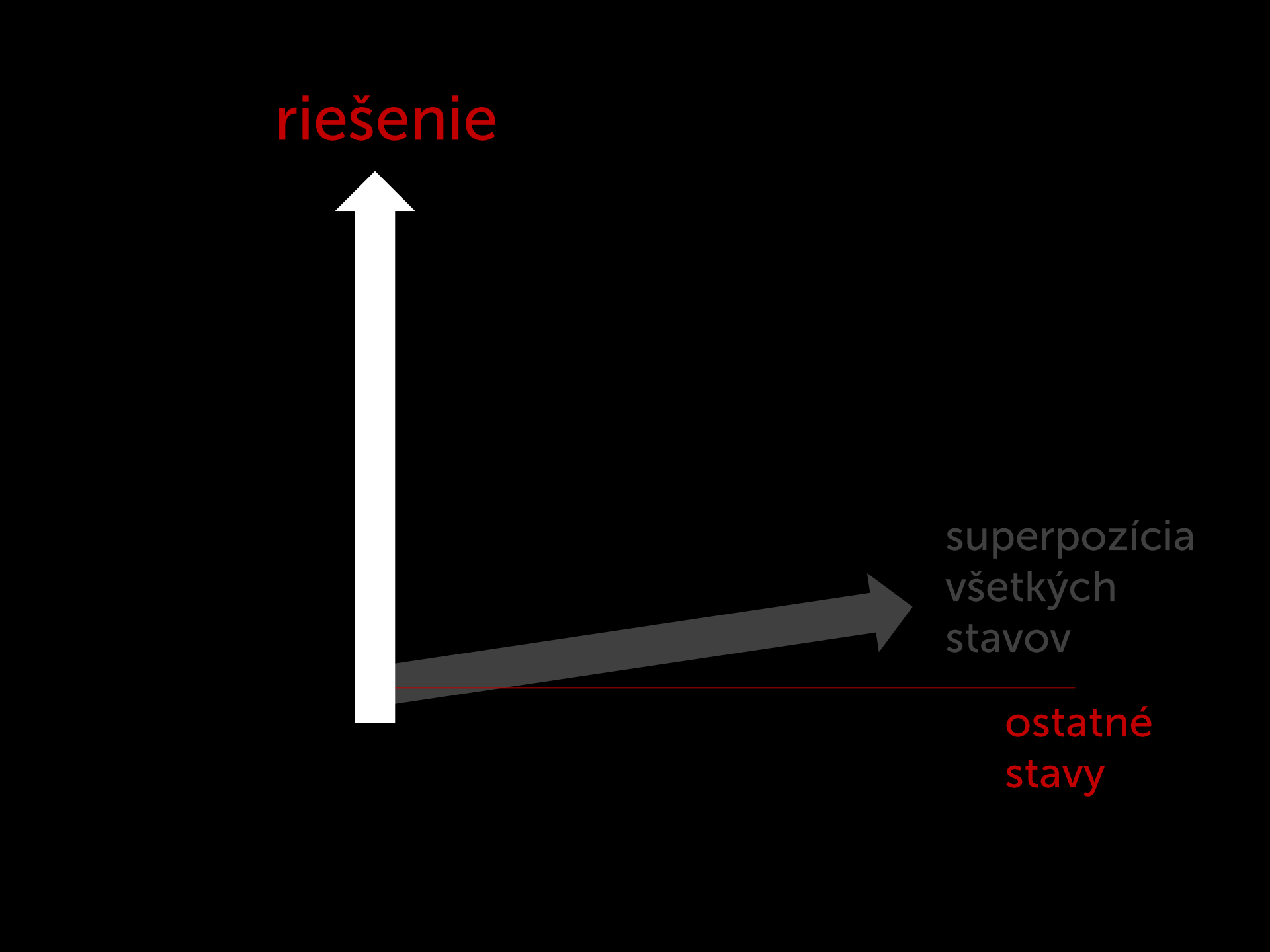


riešenie



riešenie




riešenie
superpozícia
všetkých
stavov
ostatné
stavy

neštruktúrované hľadanie

využitie superpozície

2D geometria

kvadratické zrýchlenie (optimálne)

Lov Grover

štruktúra

superpozície

kam ideme

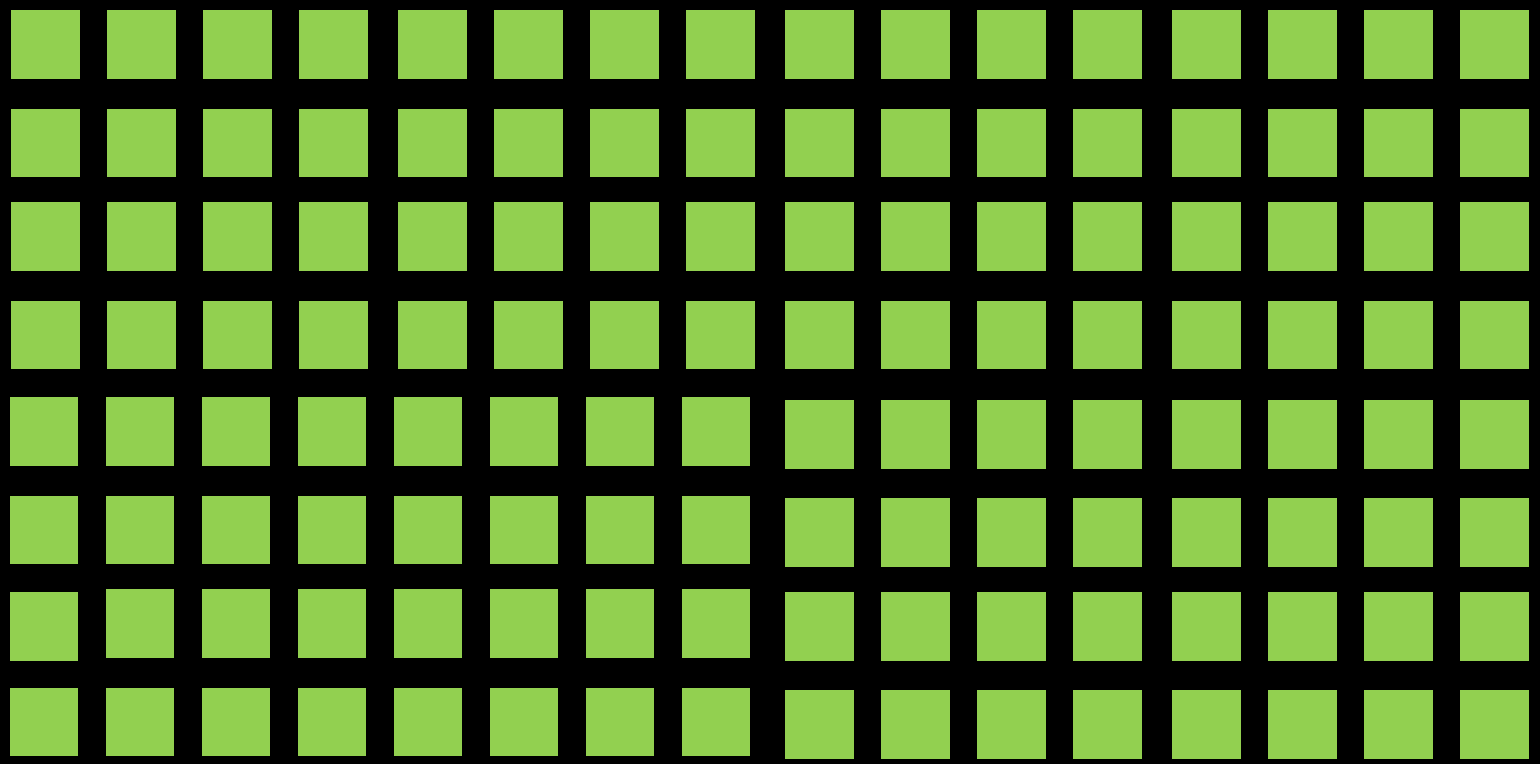
aplikácie QC

načo to je vlastne dobré
a kde sa nám „darí“

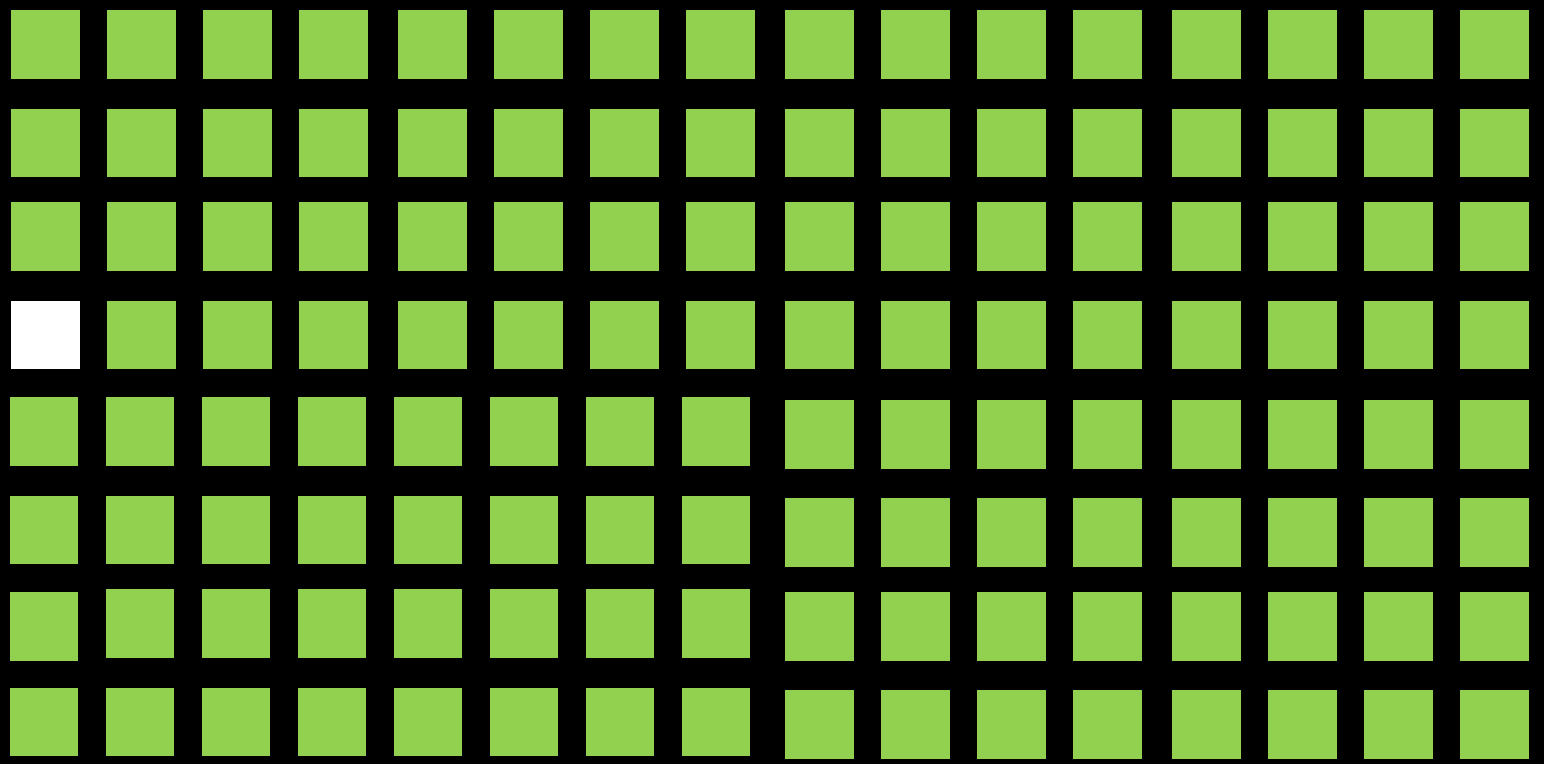
"nature isn't classical"

dammit, and if you want to
make a simulation of nature,
you'd better make it
quantum mechanical,
and by golly it's
a wonderful problem,
because it doesn't
look so easy.

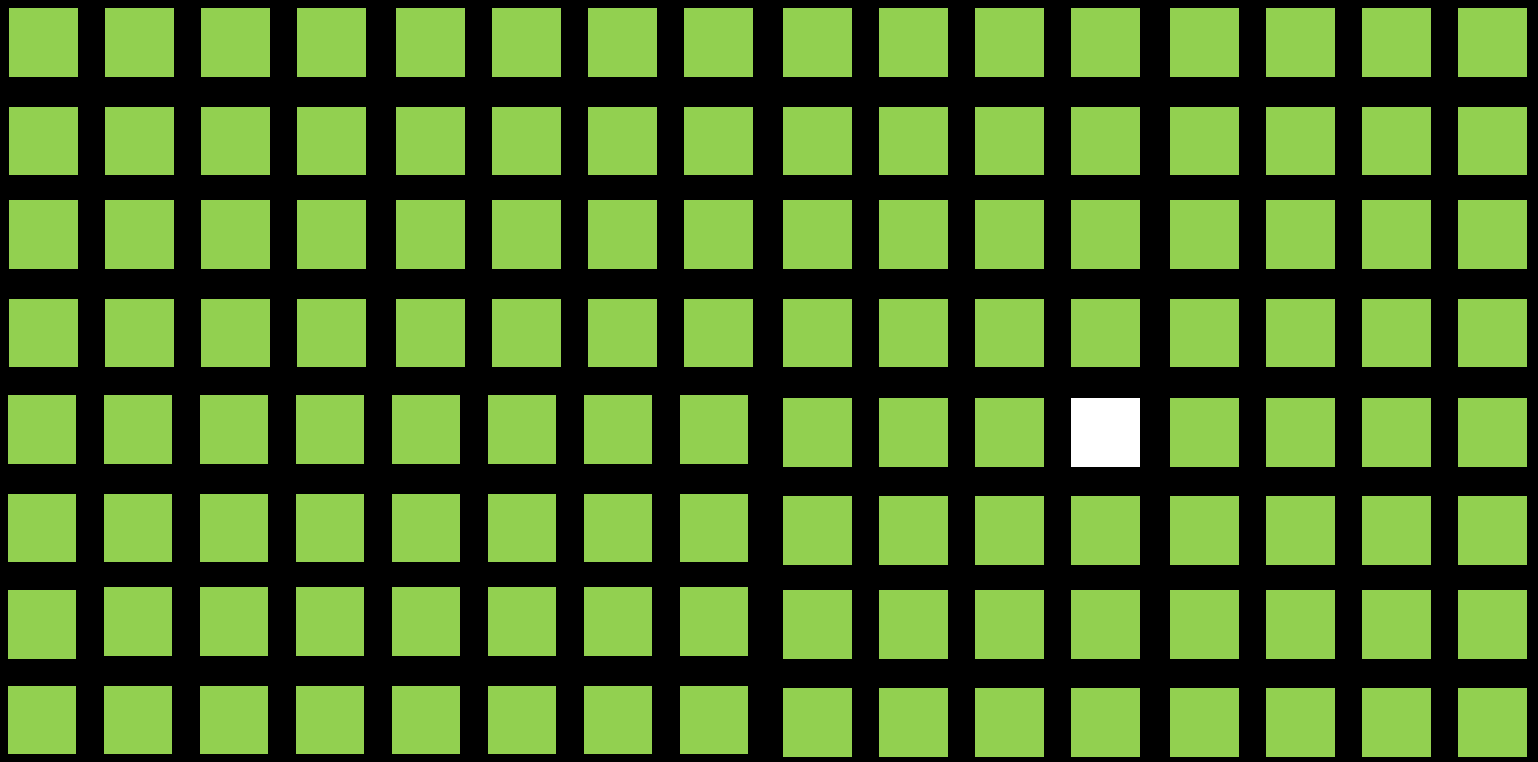
Richard Feynman

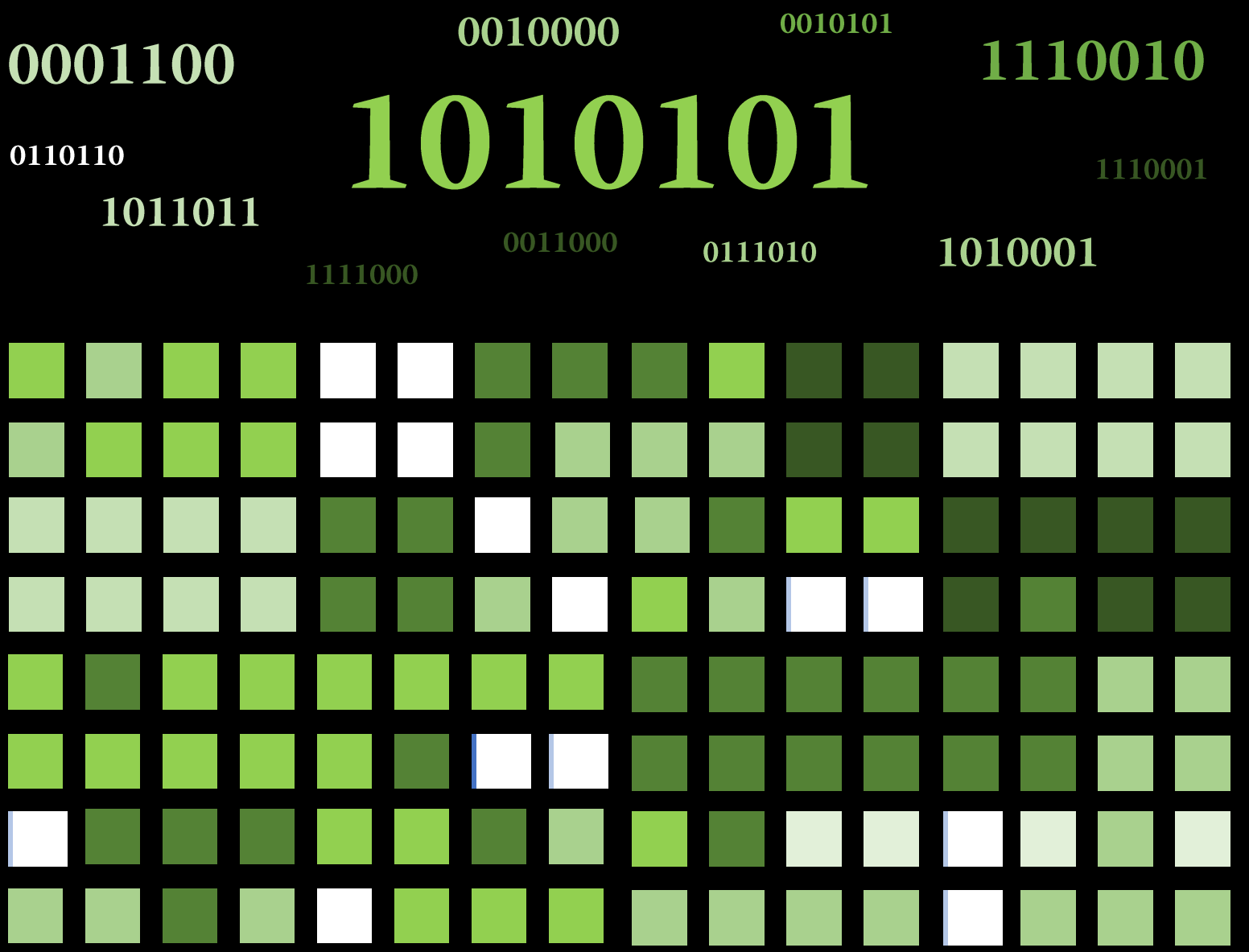


0000011

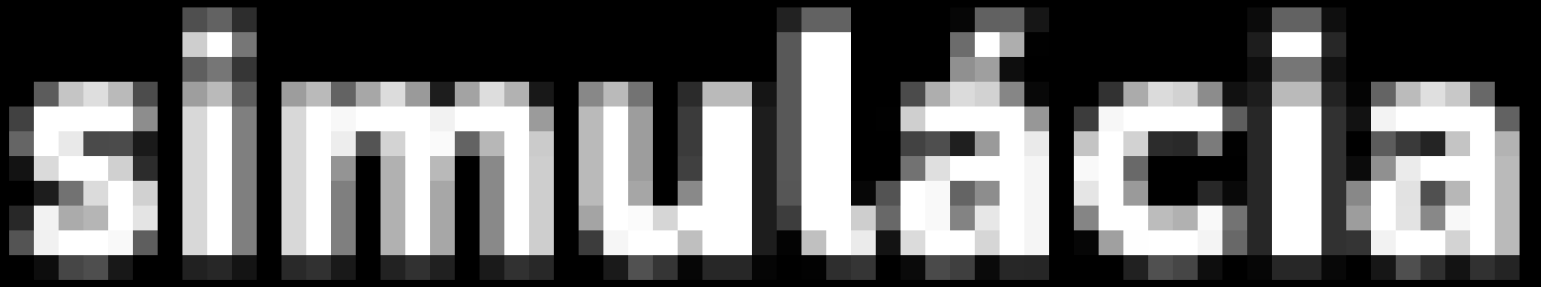


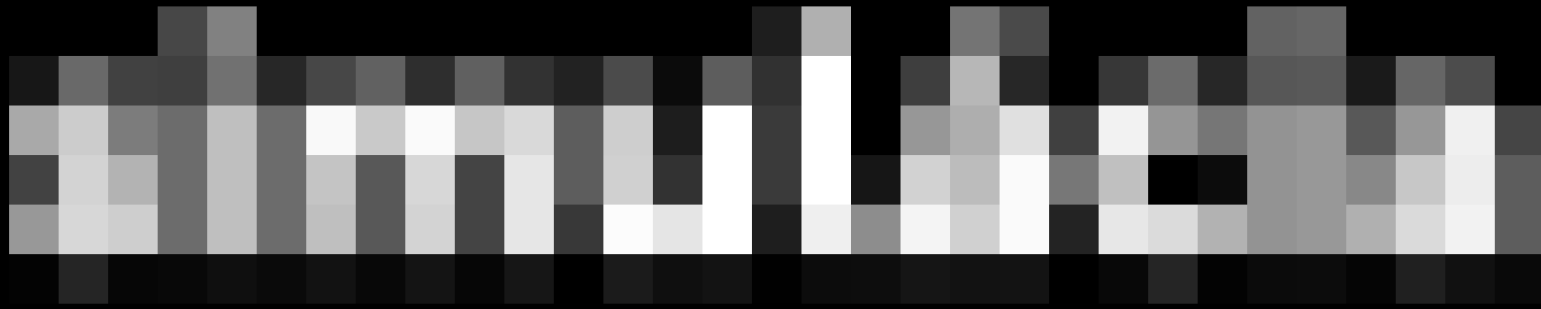
1010101

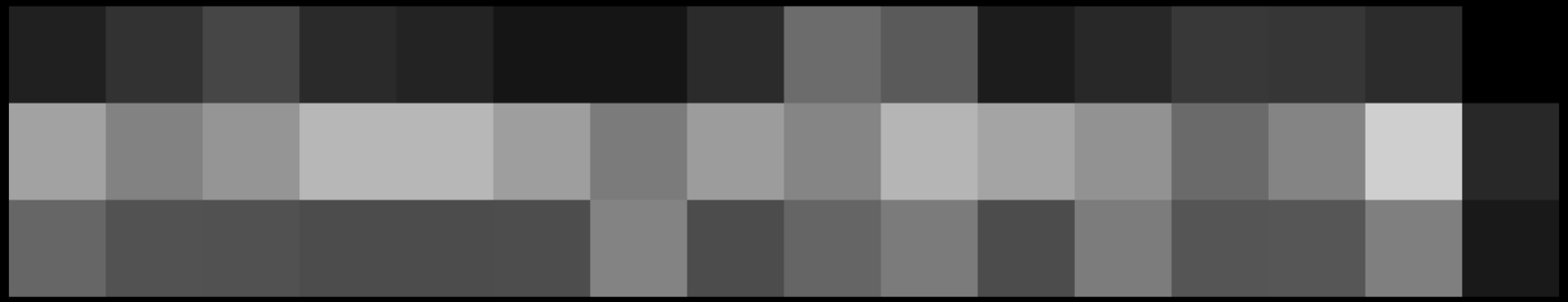



0001100
0010000
0010101
1110010
1010101
0110110
1011011
1110001
0011000
0111010
1010001
1111000

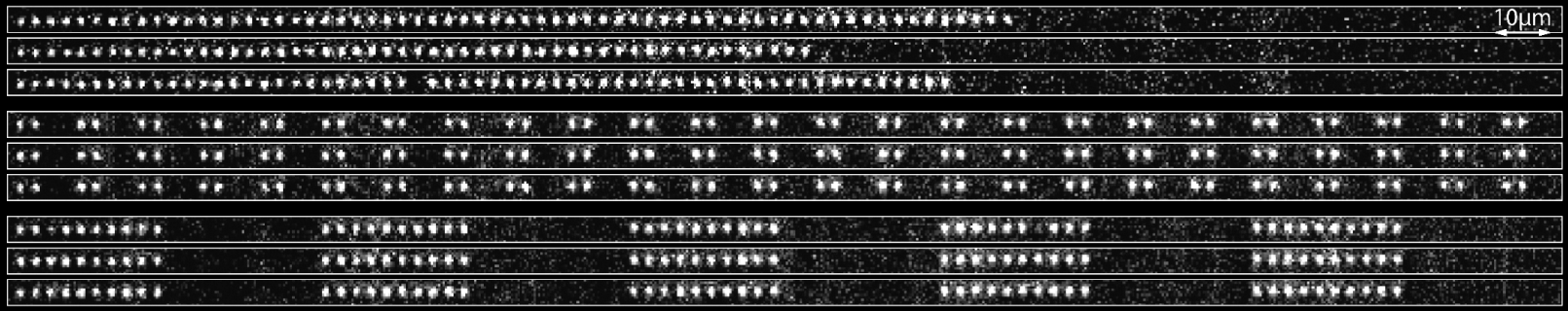
simulácia


simulácia



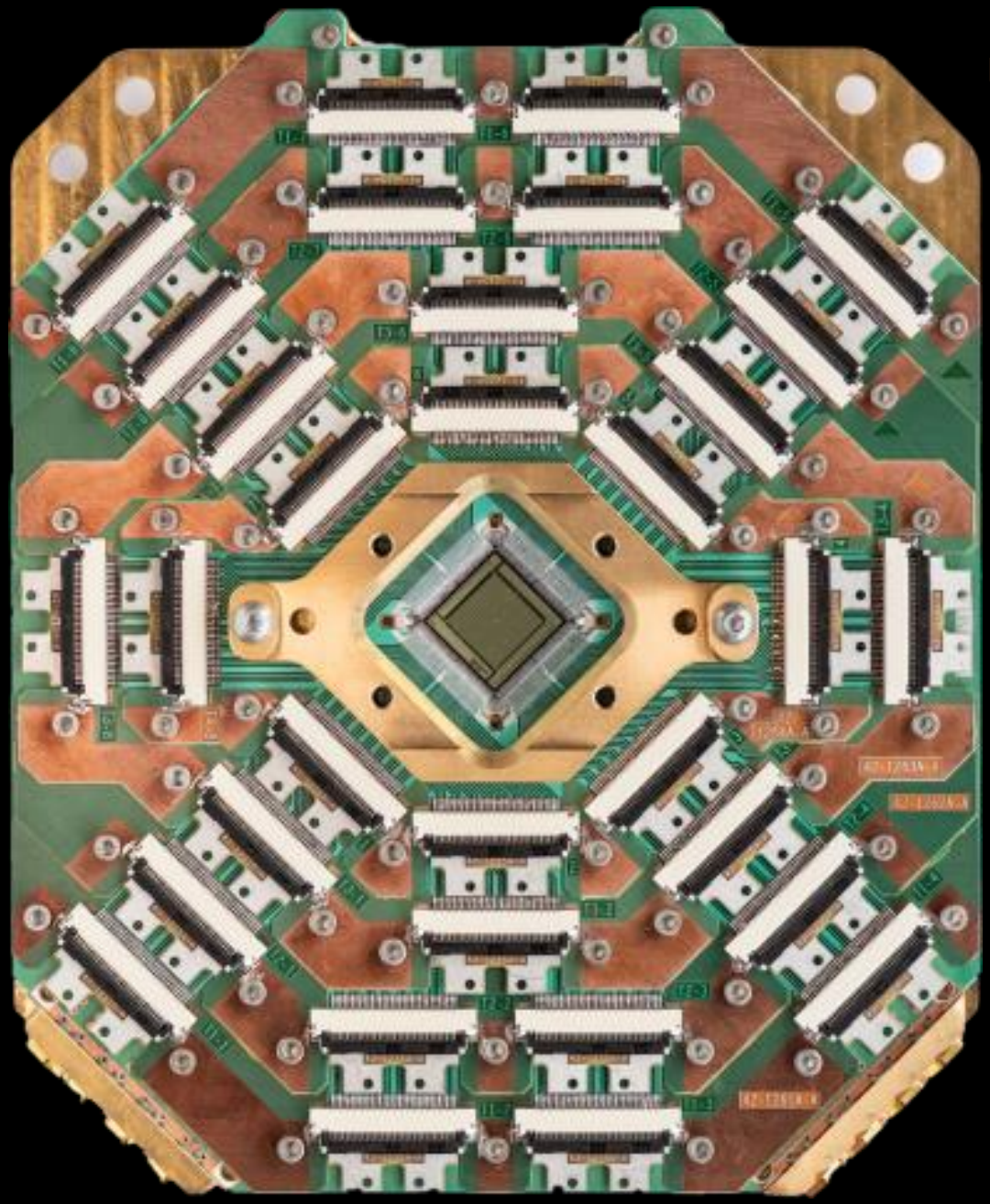


^{87}Rb



[Endres et al., Science 354, 2016]

optimalizácia



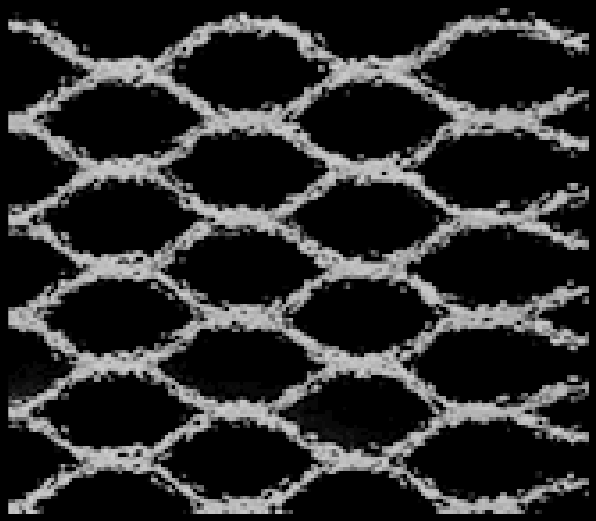
Dwave Advantage
5000 qubits
(2020)

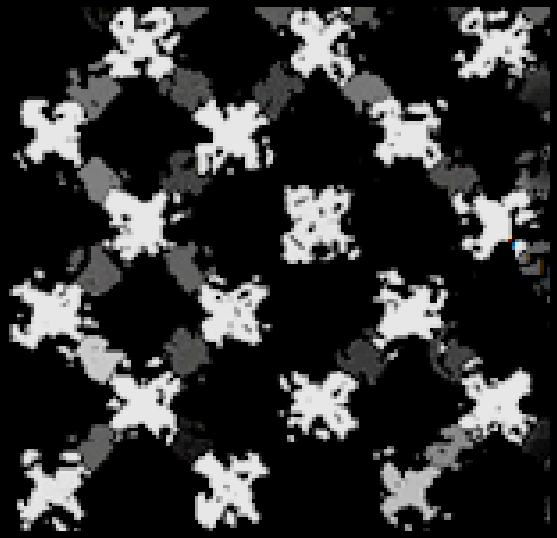
tomografia

+ učenie

Predicting many properties of a q.system from very few measurements
Hsin-Yuan Huang et al., Nature Physics 16, 1050--1057 (2020)

Quantum advantage in learning from experiments
Hsin-Yuan Huang et al., arXiv:2112.00778





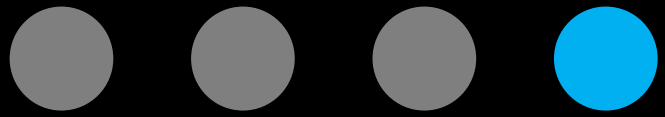
kvantová výhoda

random circuit sampling

nielen

prirodzene

kvantové úlohy

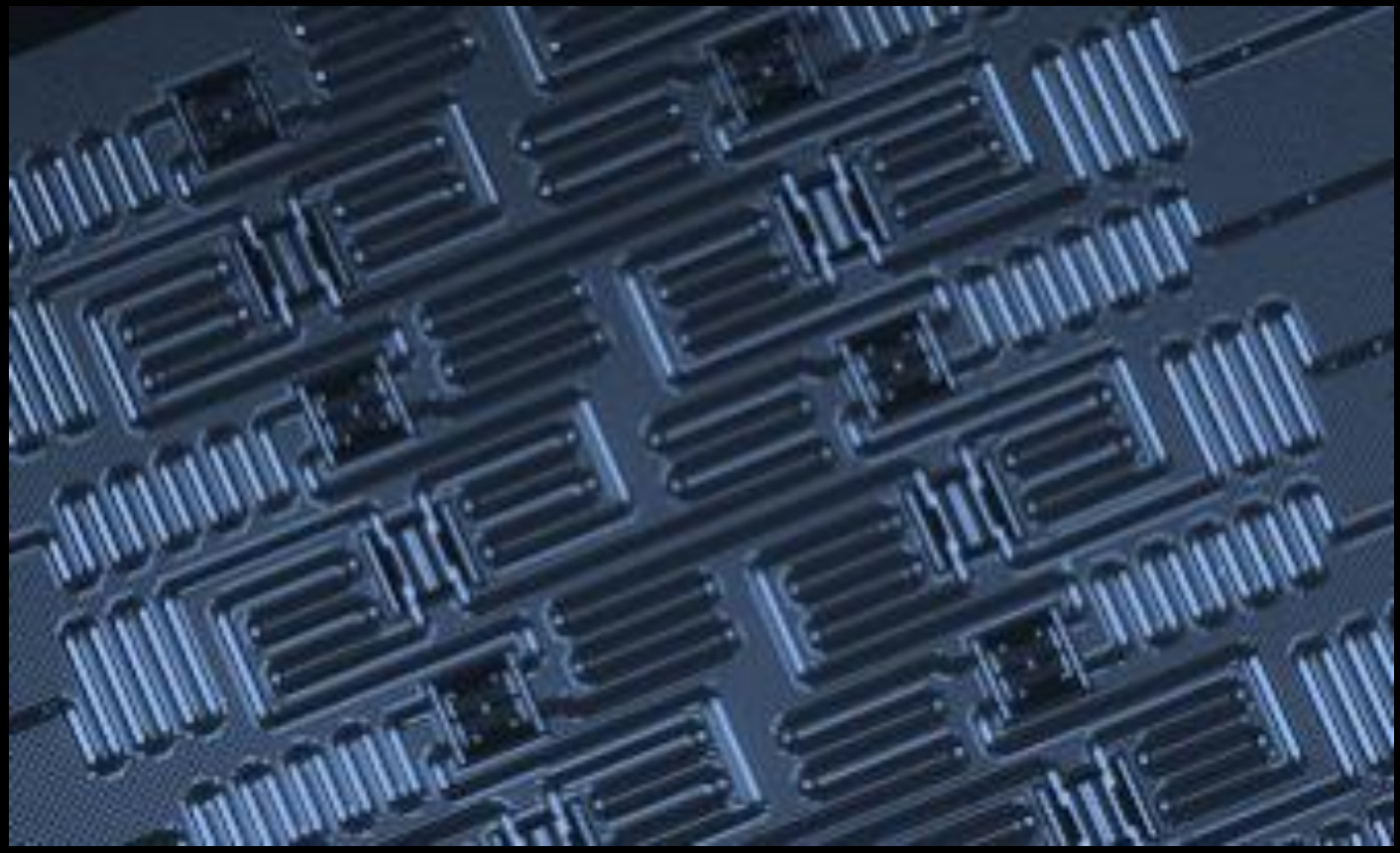


obmedzenia

a limity QC

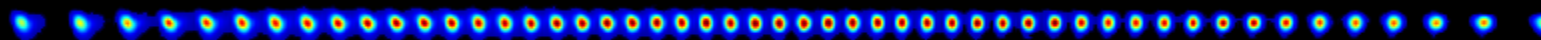
škálovanie a oprava chýb
nie je to všeliek

supravodivé obvody



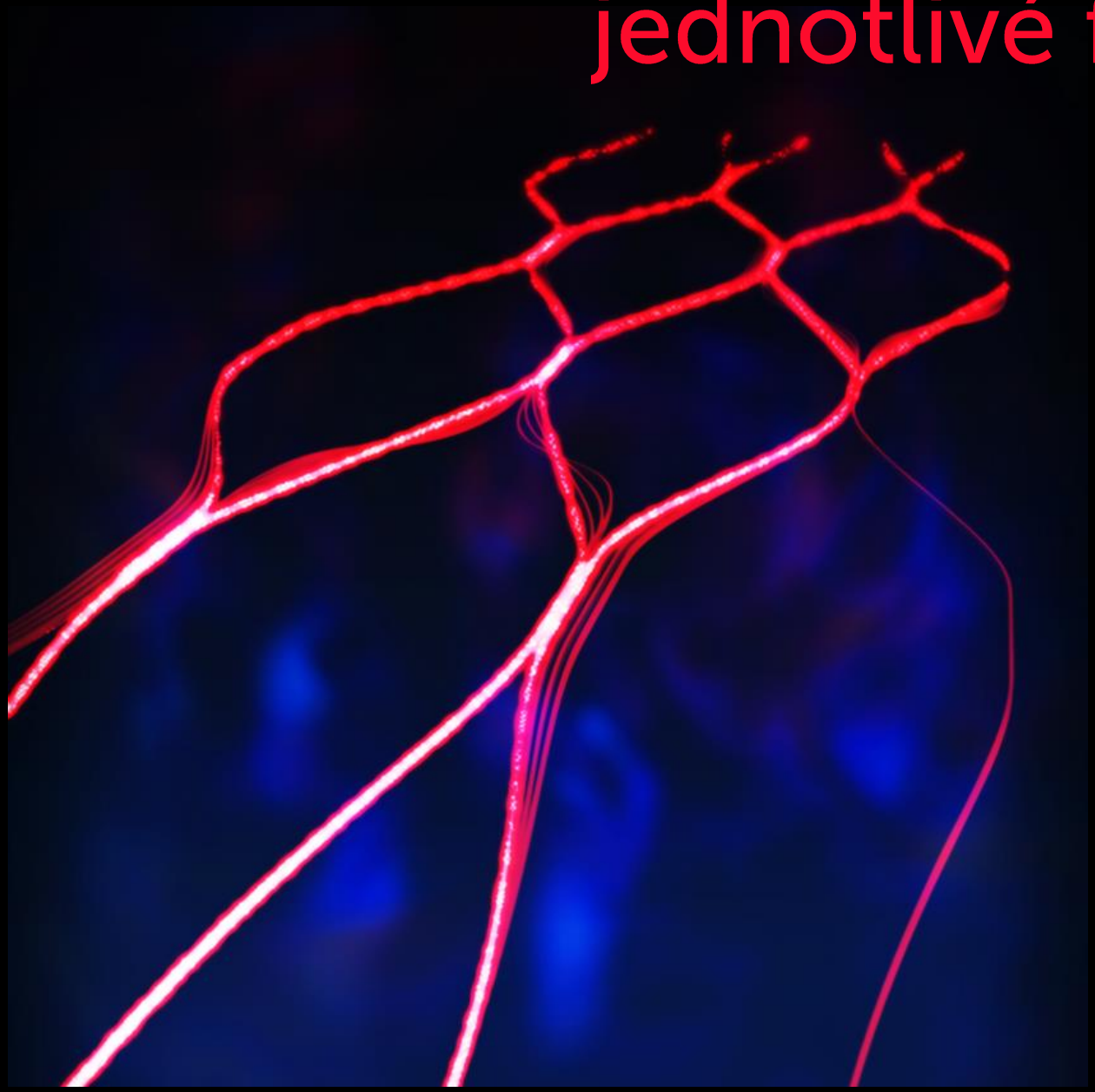
IBM, 2017

lapené ióny

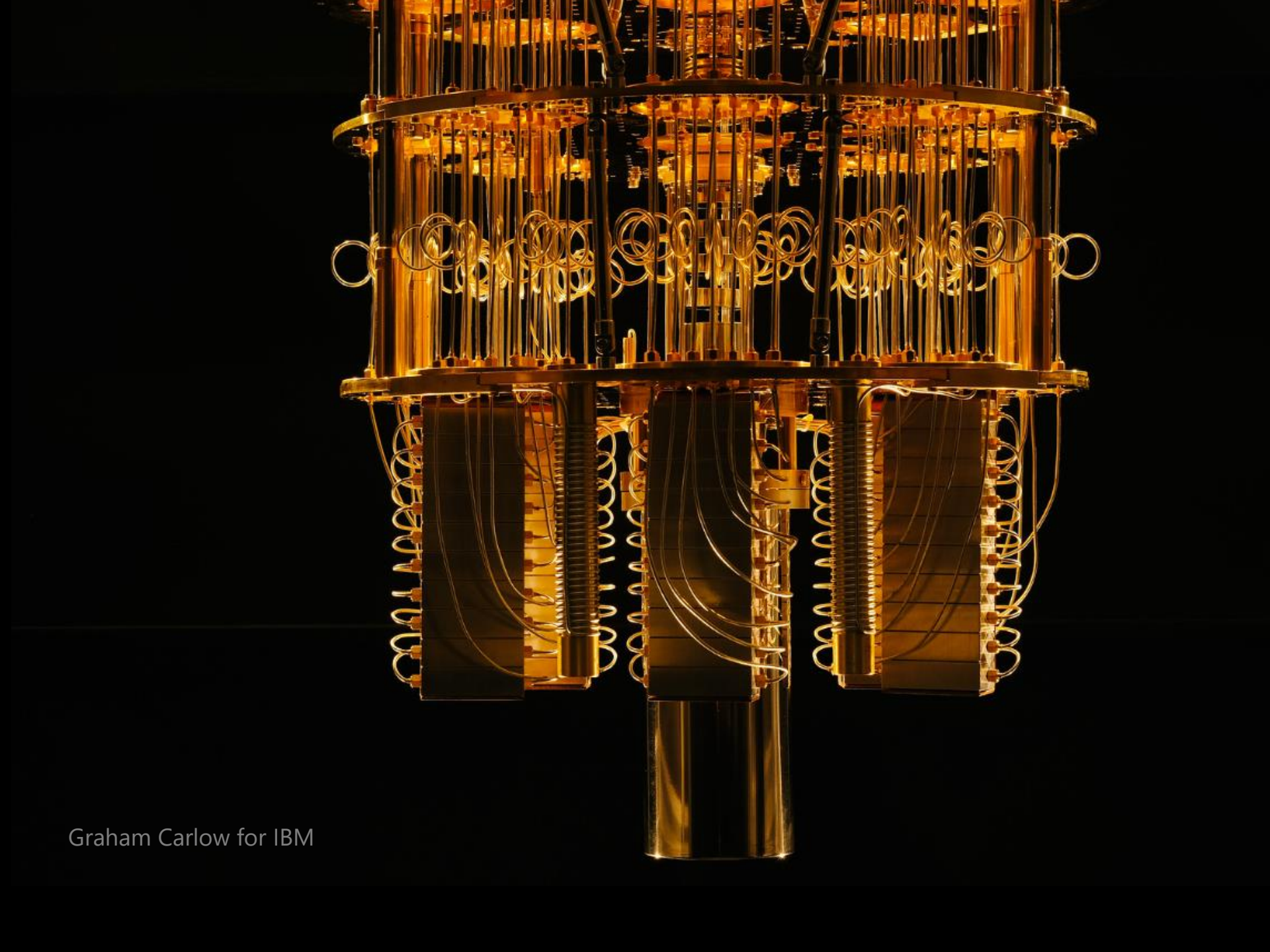


Uni Innsbruck, R. Blatt

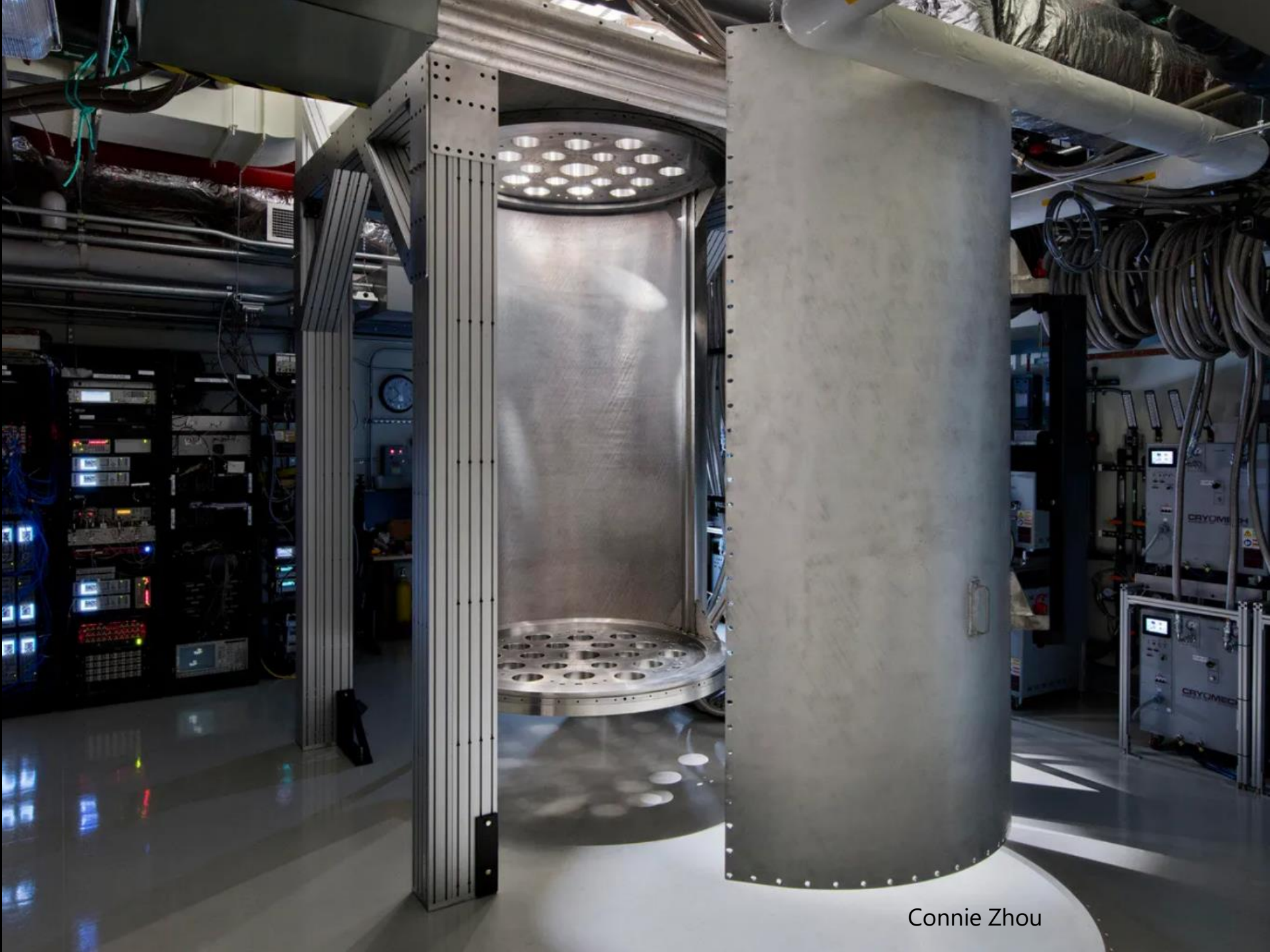
jednotlivé fotóny



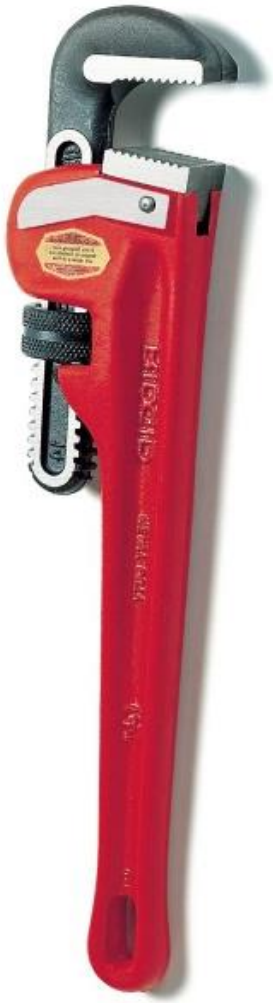
Uni Wien
P. Walther



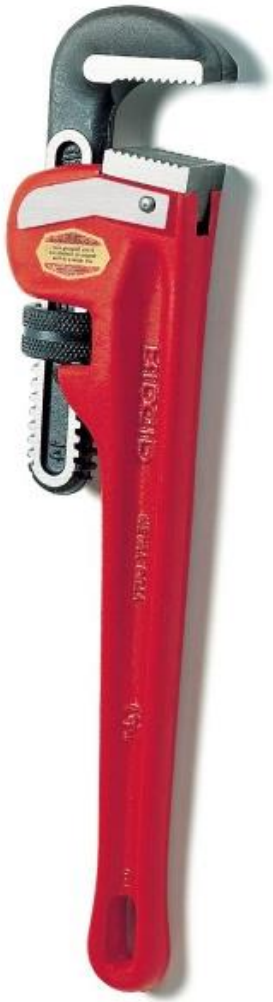
Graham Carlow for IBM



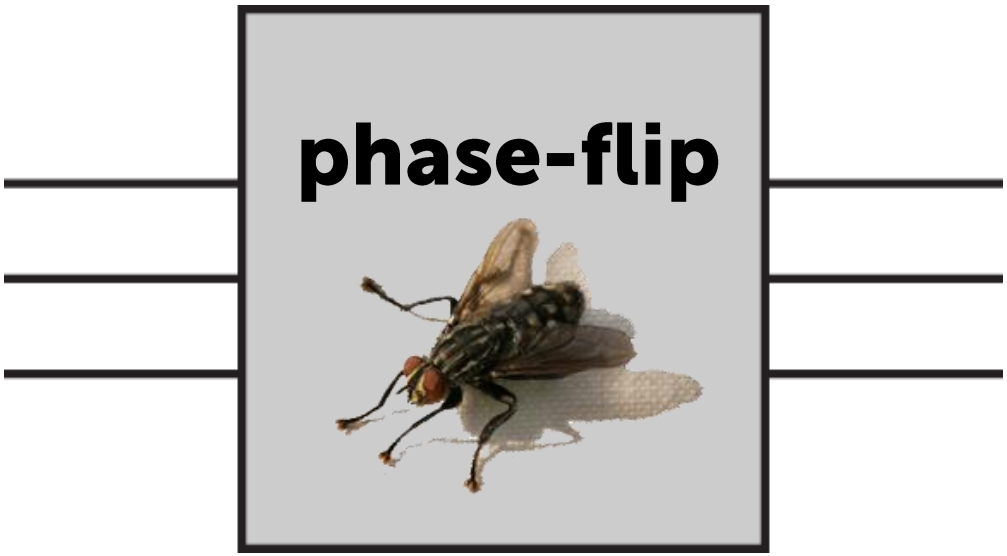
Connie Zhou



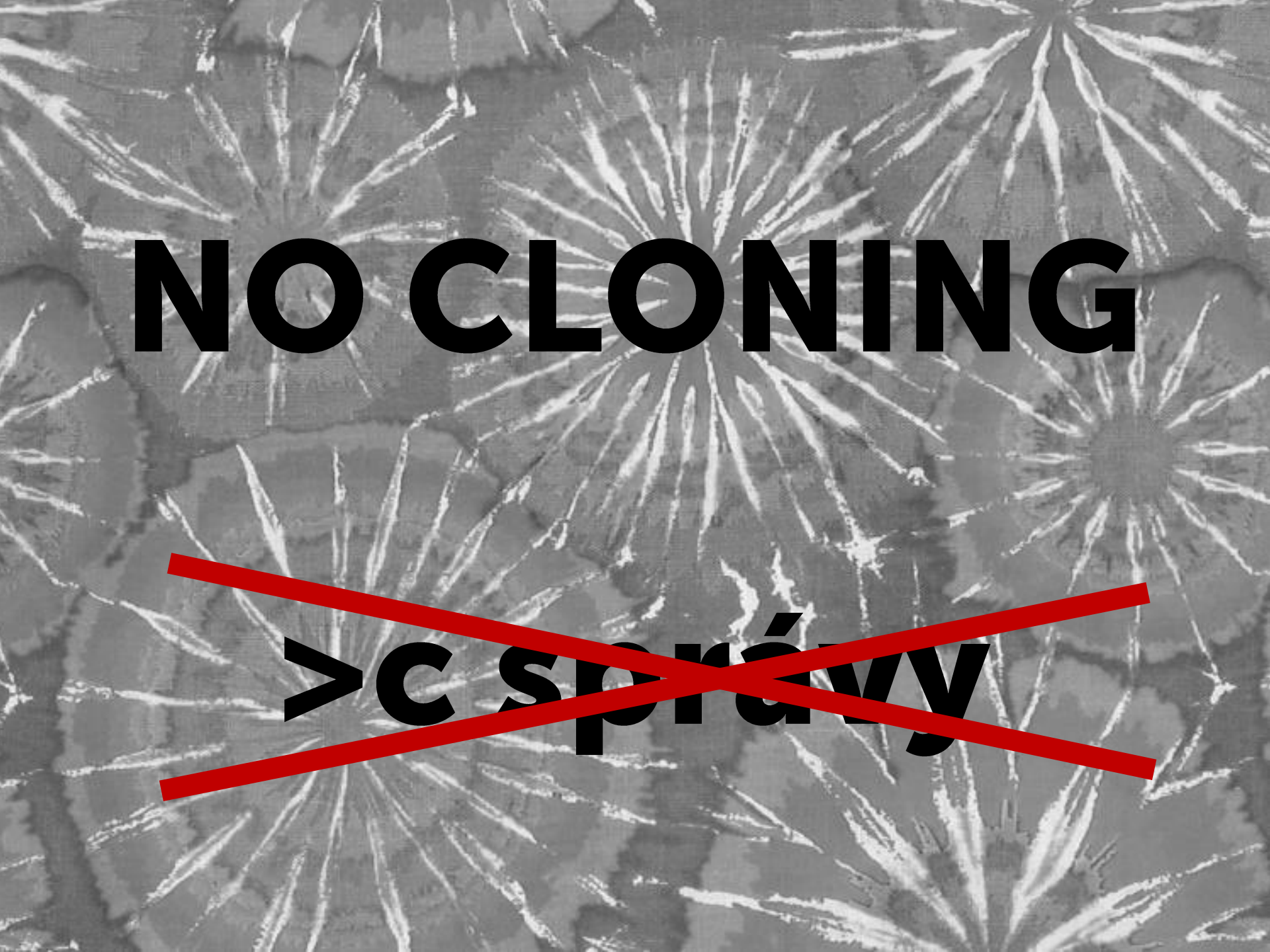
oprava chýb



oprava chýb

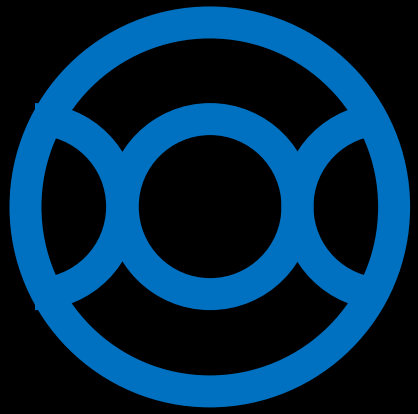


fundamental
fysiks group,
[City magazine, 1975+]


NO CLONING
>c správy

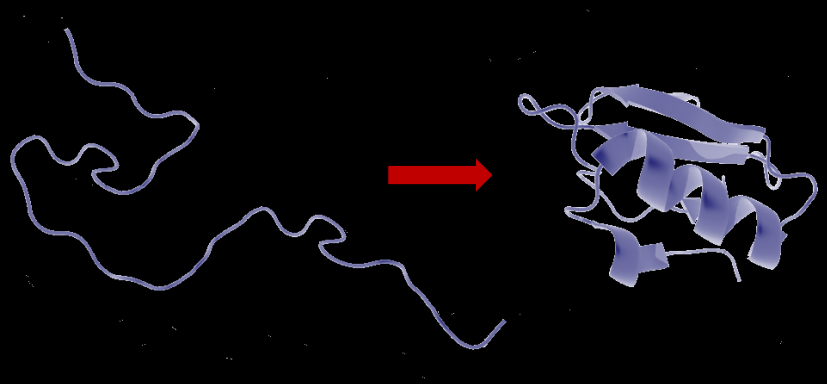
ťažko dokázať, že

niečo sa nedá



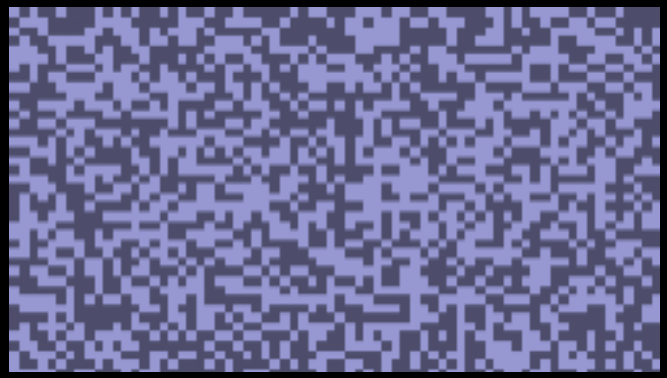

základný stav

skladanie proteínov



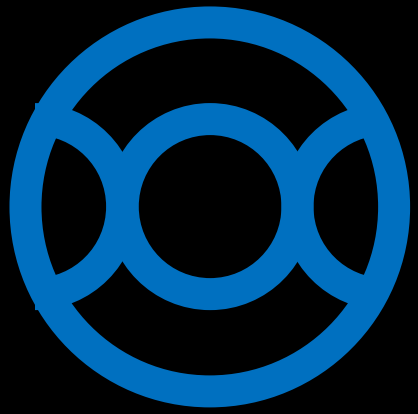
[wikipedia]

spinové sklá



[uni-koeln.de]

úlohy ťažké aj pre
kvantové počítače



ak by to šlo,
diali by sa „divné“ veci

kvantové počítanie

- pestrá zložitosť
- nové nástroje
- špecializované využitie
- mnohé obmedzenia