Kvantumszámítógép

Nagy Dávid

Informatikai eszközök fizikai alapjai szeminárium

2013

Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?

Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?

Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?

Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?

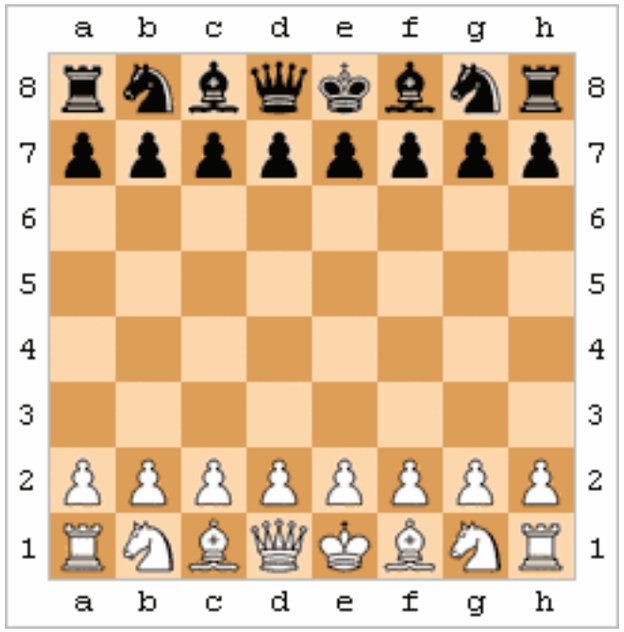
Mitől lesz valami számítógép?

Mitől lesz valami számítógép?

Mitől lesz valami számítógép?

formális rendszer

a sakk formális rendszer



a sakk formális rendszer

{♖, ♔, ♕, ♗, ♘, ♙, ♜, ♚, ♛, ♝, ♞, ♟, □}

a sakk formális rendszer

{♖, ♔, ♕, ♗, ♘, ♙, ♜, ♚, ♛, ♝, ♞, ♟, □}

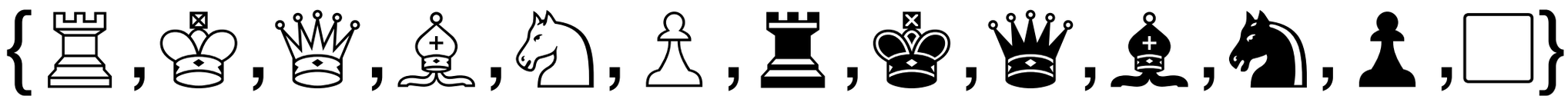
♖ ♘ ♗ [...] □ □ □ □ □ □ □ [...] ♝ ♞ ♜

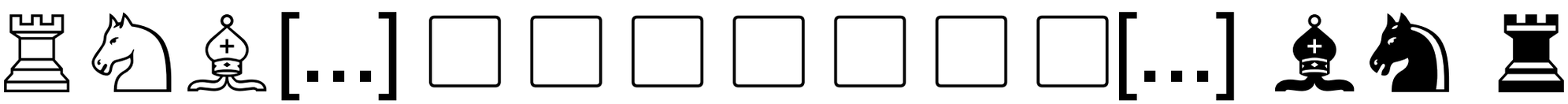
a sakk formális rendszer

{♖, ♔, ♕, ♗, ♘, ♙, ♜, ♚, ♛, ♝, ♞, ♟, □}

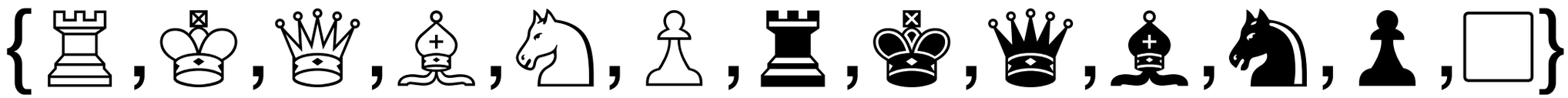
♖ ♘ ♗ [...] □ □ □ □ □ □ □ [...] ♝ ♞ ♜

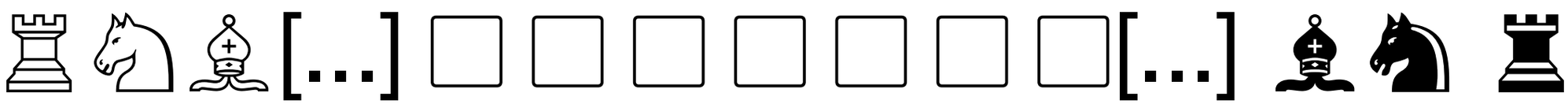
... ♖ □ □ □ ... → ... □ □ □ ♖ ...



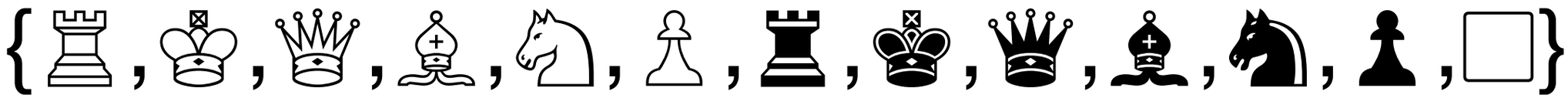


szimbólumok

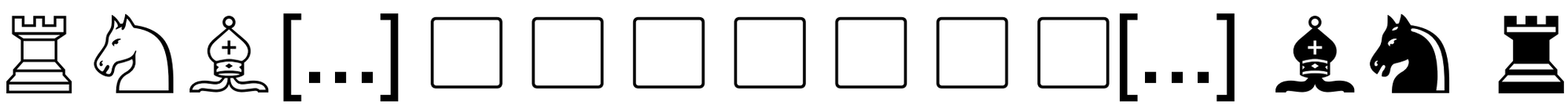




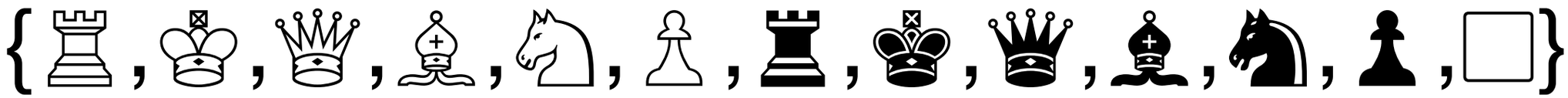
szimbólumok



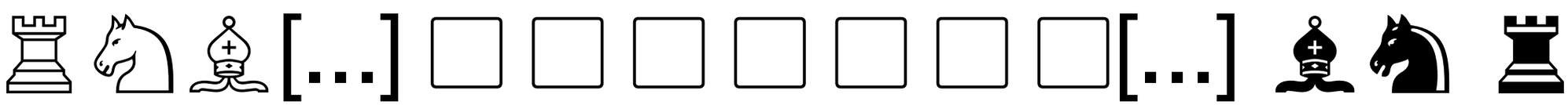
axiómák



szimbólumok



axiómák



következtetési szabályok

szimbólumok

axiómák

következtetési szabályok

formális rendszer

szimbólumok

axiómák

következtetési szabályok

matematika = formális rendszer

$$L = \begin{cases} \{a, b\} & (symbols) \\ a & (axiom) \\ X \vdash Xb & (rule\,1) \\ X \vdash aXa & (rule\,2) \end{cases}$$

<formal_system.py>

csoportelmélet:

Alphabet

variables	$x, y, z, \ldots$	
individual constants	e	(identity)
function symbols	i, p	(inverse, product)
predicate symbol	$=$	
others	$(,),,$	
logical symbols	$\forall, \neg \rightarrow$	

Derivation rules

(MP)	$\phi, (\phi \rightarrow \psi) \Rightarrow \psi$	(modus ponens)
(G)	$\phi \Rightarrow \forall x \phi$	(generalization)

Axioms I. (logical)

(PC1)	$(\phi \rightarrow (\psi \rightarrow \phi))$
(PC2)	$((\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow (\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \chi))$
(PC3)	$((\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi))$
(PC4)	$(\forall x(\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \forall x \psi))$ (given that x is not free in ϕ)
(PC5)	$(\forall x \phi \rightarrow \phi)$ (given that x is not free in ϕ)
(PC6)	$(\forall x \phi(x) \rightarrow \phi(y))$ (given that whenever a free occurrence of x is replaced by y, y is free in $\phi(y)$)
(E1)	$x = x$
(E2)	$t = s \rightarrow f^n(u_1, u_2, \ldots, t, \ldots u_n) = f^n(u_1, u_2, \ldots, s, \ldots u_n)$
(E3)	$t = s \rightarrow (\phi(u_1, u_2, \ldots, t, \ldots u_n) \rightarrow \phi(u_1, u_2, \ldots, s, \ldots u_n))$

Axioms II. (of group theory)

(G1)	$p(p(x,y),z) = p(x, p(y,z))$	(associative law)
(G2)	$p(e,x) = x$	(left identity)
(G3)	$p(i(x),x) = e$	(left inverse)

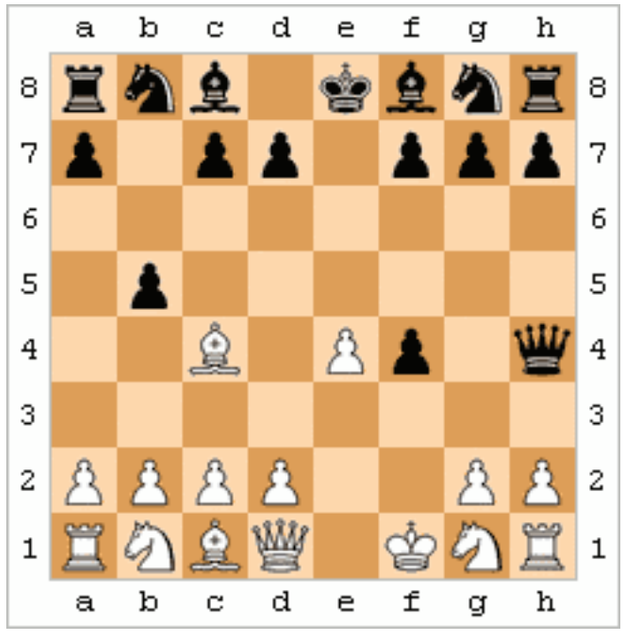
számítás:

számítás:

formális rendszer működtetése

számítás:

formális rendszer működtetése



a számítást végző absztrakt gép modellje

Turing-gép

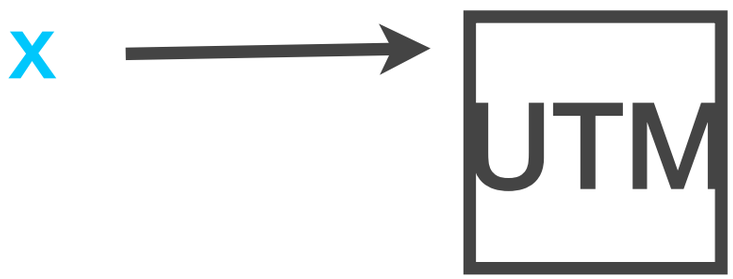
TM1

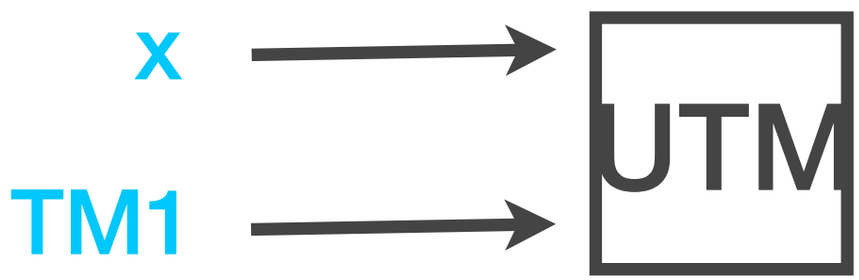
x
TM1
f(x)

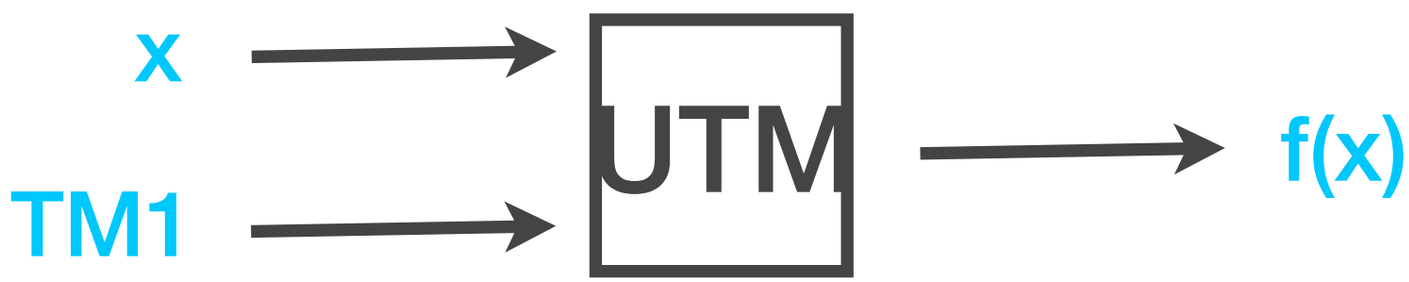
x
f
f(x)

UTM

Universal Turing Machine


x
UTM


x
TM1
UTM


x
TM1
UTM
f(x)

x
TM2
UTM
g(x)

x
F
∀F
F(x)

$\forall F \in \{\mu\text{-recursive functions}\}$

CHURCH-TURING TÉZIS

∀F∈{μ-recursive functions}

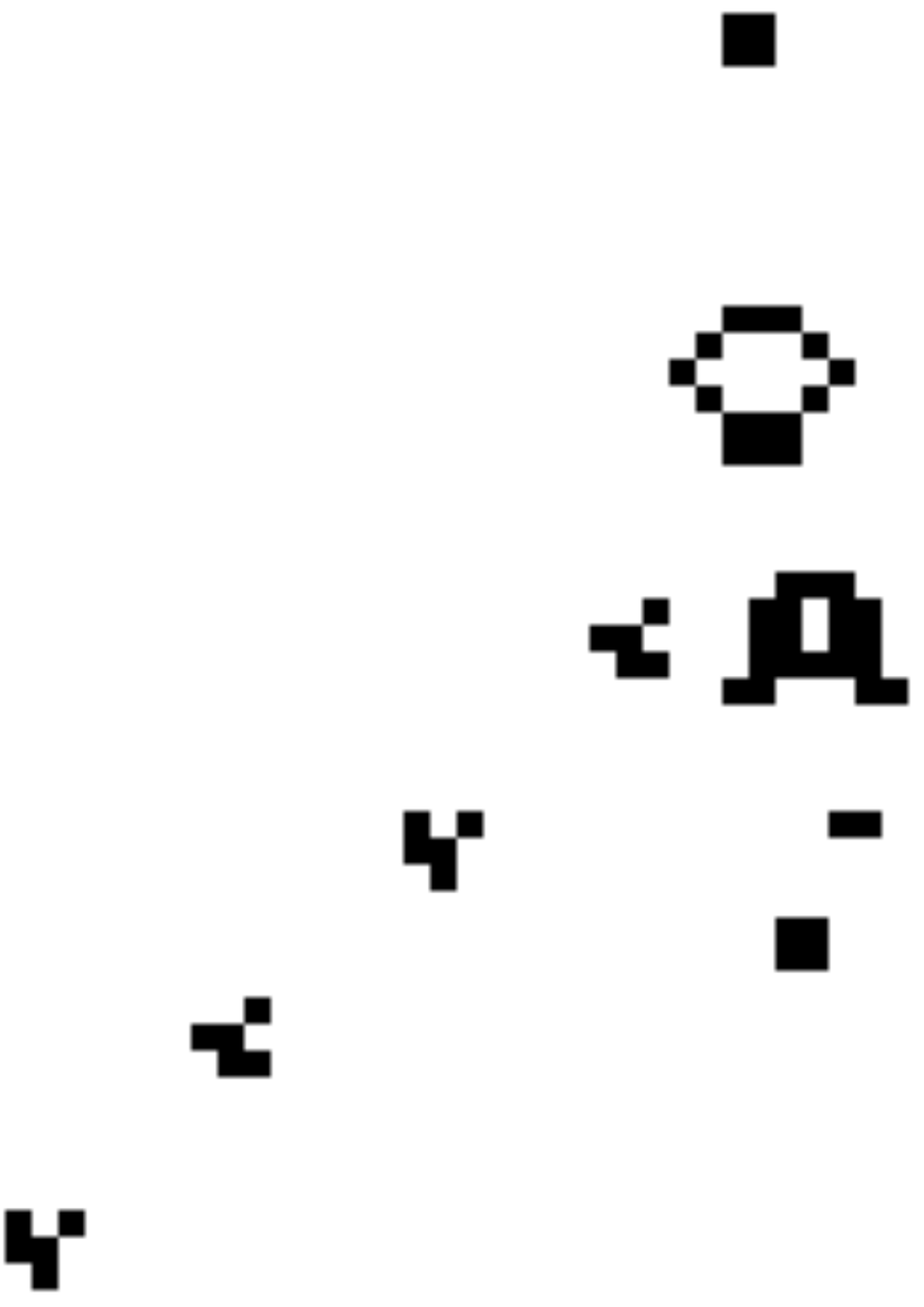
$\forall F \in \{\mu\text{-recursive functions}\}$

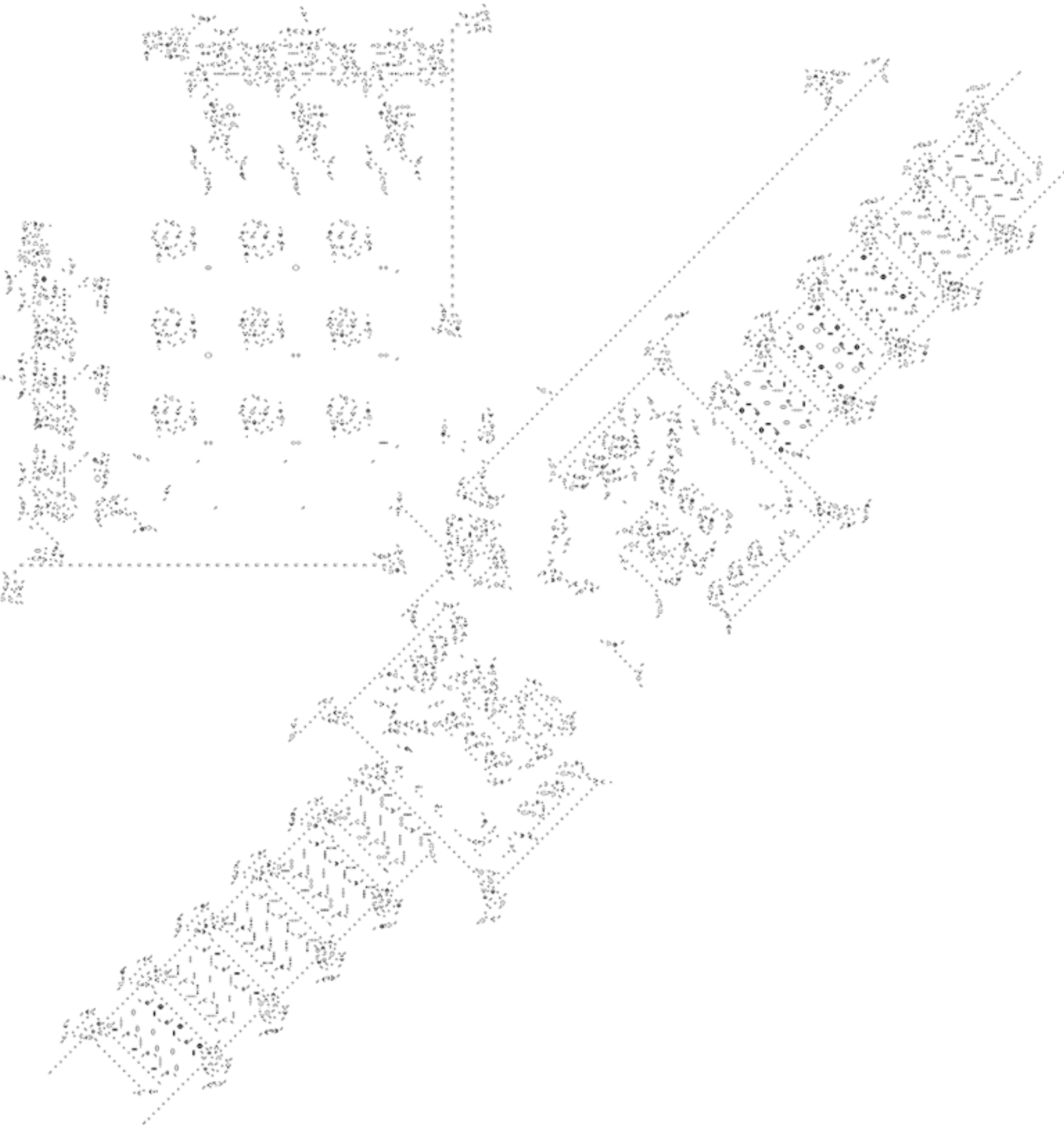
N({μ-recursive functions})= megszámlálhatóan sok

N({functions})= kontinuum sok

legfeljebb polinomiális lassulással

legfeljebb polinomiális lassulással





minden formális rendszerhez létezik izomorf TM

minden formális rendszerhez létezik izomorf TM

+

létezik UTM ami minden más TM-t képes szimulálni

minden formális rendszerhez létezik izomorf TM

+

létezik UTM ami minden más TM-t képes szimulálni

↓

ha tudunk készíteni UTM-et, akkor lesz egy gépünk ami bármilyen kiszámítható függvényt képes kiszámítani

fizikai rendszer $\approx$ UTM

hogyan?

Example: state table for the 3-state 2-symbol busy beaver reduced to 5-tuples

Current state	Scanned symbol	Print symbol	Move tape	Final (i.e. next) state	5-tuples
A	0	1	R	**B**	(**A**, 0, 1, R, **B**)
A	1	1	L	**C**	(**A**, 1, 1, L, **C**)
B	0	1	L	**A**	(**B**, 0, 1, L, **A**)
B	1	1	R	**B**	(**B**, 1, 1, R, **B**)
C	0	1	L	**B**	(**C**, 0, 1, L, **B**)
C	1	1	N	**H**	(**C**, 1, 1, N, **H**)

Example: state table for the 3-state 2-symbol busy beaver reduced to 5-tuples

Current state	Scanned symbol	Print symbol	Move tape	Final (i.e. next) state	5-tuples
A	0	1	R	**B**	(**A**, 0, 1, R, **B**)
A	1	1	L	**C**	(**A**, 1, 1, L, **C**)
B	0	1	L	**A**	(**B**, 0, 1, L, **A**)
B	1	1	R	**B**	(**B**, 1, 1, R, **B**)
C	0	1	L	**B**	(**C**, 0, 1, L, **B**)
C	1	1	N	**H**	(**C**, 1, 1, N, **H**)

A	2
B	3
C	4
R	5
L →	6
H	7
N	8
0	0
1	1

5-tuples
(**A**, 0, 1, R, **B**)
(**A**, 1, 1, L, **C**)
(**B**, 0, 1, L, **A**)
(**B**, 1, 1, R, **B**)
(**C**, 0, 1, L, **B**)
(**C**, 1, 1, N, **H**)

TM1=(2,0,1,5,3,..
.,1,1,8,7)

gödel numbering

$$enc(x_1, x_2, x_3, \ldots, x_n) = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \cdots p_n^{x_n}$$

enc(TM1)=2138935[...]39638

enc(TM1)=2138935[...]39638

↓

binary(2138935[...]39638)=
1010001011101...111011101

kétállapotú fizikai rendszereket könnyen találhatunk
(pl spin)

kétállapotú fizikai rendszereket könnyen találhatunk
(pl spin)

ezzel az UTM állapotait és ‘programját’ modellezhetjük

↑↓↑↓↓↓↑↓↑↑↑↓↑...↑↑↑↓↑↑↑↓↑

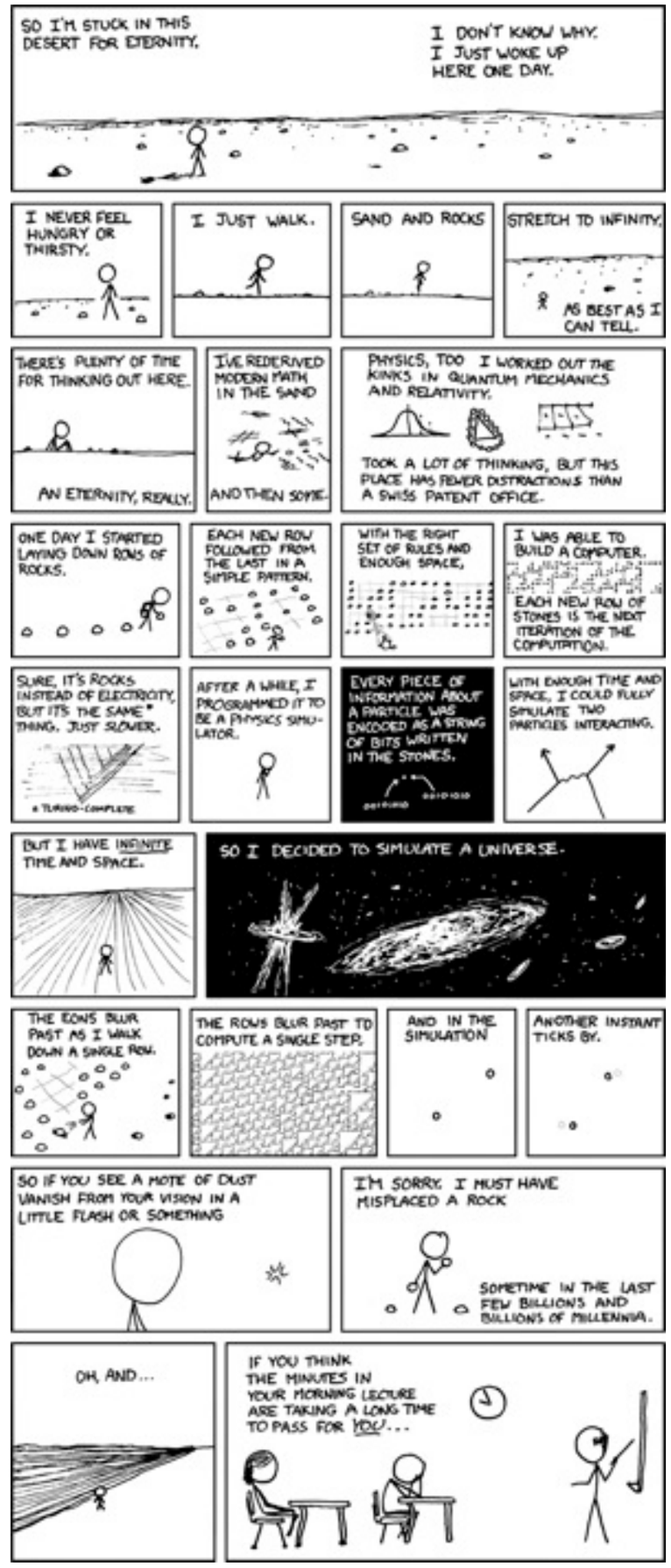
1010001011101...111011101

a trükk hogy lehet találni egyszerű
rendszereket amik izomorfak az
egyszerű UTM alkatrészekkel

miért?

miért?

Digital Universe hipotézis


SO I'M STUCK IN THIS DESERT FOR ETERNITY.
I DON'T KNOW WHY. I JUST WOKE UP HERE ONE DAY.
I NEVER FEEL HUNGRY OR THIRSTY.
I JUST WALK.
SAND AND ROCKS
STRETCH TO INFINITY.
AS BEST AS I CAN TELL.
THERE'S PLENTY OF TIME FOR THINKING OUT HERE.
AN ETERNITY, REALLY.
I'VE REDERIVED MODERN MATH IN THE SAND
AND THEN SOME.
PHYSICS, TOO. I WORKED OUT THE KINKS IN QUANTUM MECHANICS AND RELATIVITY.
TOOK A LOT OF THINKING, BUT THIS PLACE HAS FEWER DISTRACTIONS THAN A SWISS PATENT OFFICE.
ONE DAY I STARTED LAYING DOWN ROWS OF ROCKS.
EACH NEW ROW FOLLOWED FROM THE LAST IN A SIMPLE PATTERN.
WITH THE RIGHT SET OF RULES AND ENOUGH SPACE,
I WAS ABLE TO BUILD A COMPUTER.
EACH NEW ROW OF STONES IS THE NEXT ITERATION OF THE COMPUTATION.
SURE, IT'S ROCKS INSTEAD OF ELECTRICITY, BUT ITS THE SAME* THING, JUST SLOWER.
* TURING-COMPLETE
AFTER A WHILE, I PROGRAMMED IT TO BE A PHYSICS SIMULATOR.
EVERY PIECE OF INFORMATION ABOUT A PARTICLE WAS ENCODED AS A STRING OF BITS WRITTEN IN THE STONES.
WITH ENOUGH TIME AND SPACE, I COULD FULLY SIMULATE TWO PARTICLES INTERACTING.
BUT I HAVE INFINITE TIME AND SPACE.
SO I DECIDED TO SIMULATE A UNIVERSE.
THE EONS BLUR PAST AS I WALK DOWN A SINGLE ROW.
THE ROWS BLUR PAST TO COMPUTE A SINGLE STEP.
AND IN THE SIMULATION
ANOTHER INSTANT TICKS BY.
SO IF YOU SEE A MOTE OF DUST VANISH FROM YOUR VISION IN A LITTLE FLASH OR SOMETHING
I'M SORRY. I MUST HAVE MISPLACED A ROCK
SOMETIME IN THE LAST FEW BILLIONS AND BILLIONS OF MILLENNIA.
OH, AND...
IF YOU THINK THE MINUTES IN YOUR MORNING LECTURE ARE TAKING A LONG TIME TO PASS FOR YOU...

Mitől lesz valami számítógép?

Mitől lesz valami számítógép?

A számítógépek UTM-el izomorf fizikai rendszerek

kitérő

Komplexitási osztályok

$$\mathit{asymptotic}(\ T(\ n\ )\ )$$

futási idő

↓

asymptotic(T(n))

futási idő

$$\mathit{asymptotic}(\,T(\,n\,)\,)$$

bemenet hossza

$$T(n) \propto 1$$

$$T(n) \propto n$$

$$T(n) \propto n^k$$

$$T(n) \propto e^n$$

$T(n) \propto 1$

$T(n) \propto n$

$T(n) \propto n^k$

$T(n) \propto e^n$

$T(n) \propto 1$

$T(n) \propto n \longrightarrow L$

$T(n) \propto n^k \longrightarrow P$

$T(n) \propto e^n \longrightarrow EXP$

$T(n) \propto 1$

$T(n) \propto n \longrightarrow L \searrow$

$T(n) \propto n^k \longrightarrow P \longrightarrow$ tractable

$T(n) \propto e^n \longrightarrow EXP \longrightarrow$ intractable

$T(n) \propto 1$

$T(n) \propto n \longrightarrow L \searrow$

$T(n) \propto n^k \longrightarrow P \longrightarrow$ tractable

$T(n) \propto e^n \longrightarrow EXP \longrightarrow$ intractable

$\forall F \notin \mu \longrightarrow$ uncomputable

a komplexitási osztály a
probléma sajátja, de az
algoritmusra számoljuk

$$\text{time}(n)=T(n)$$

time(n)=T(n)

méret (n)

time(n)=T(n)

méret (n)

energia (n)

time(n)=T(n)

méret (n)

energia (n)

.

.

.

time(n)=T(n) → PTIME

méret (n) → PSPACE

energia (n)

.

.

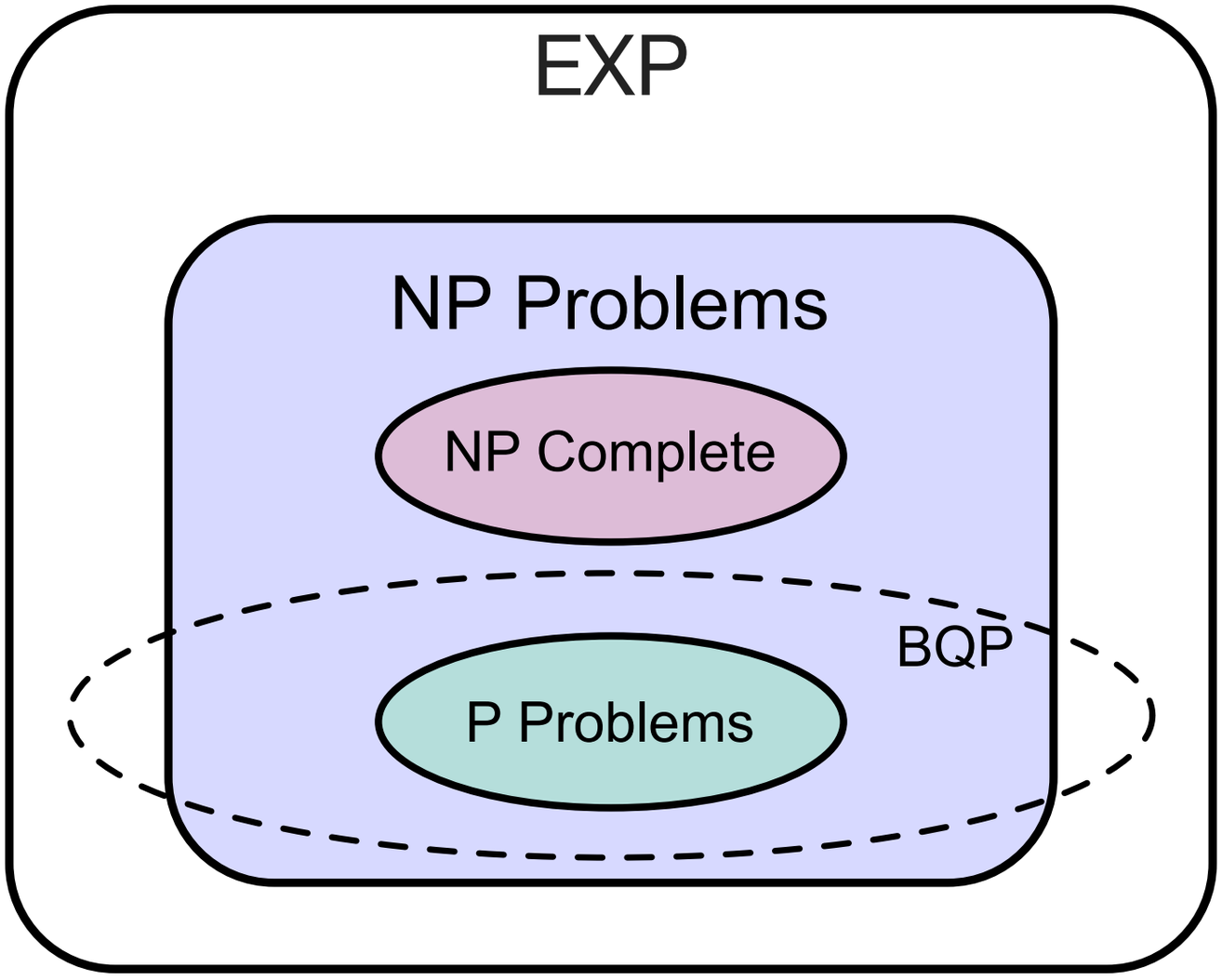
.

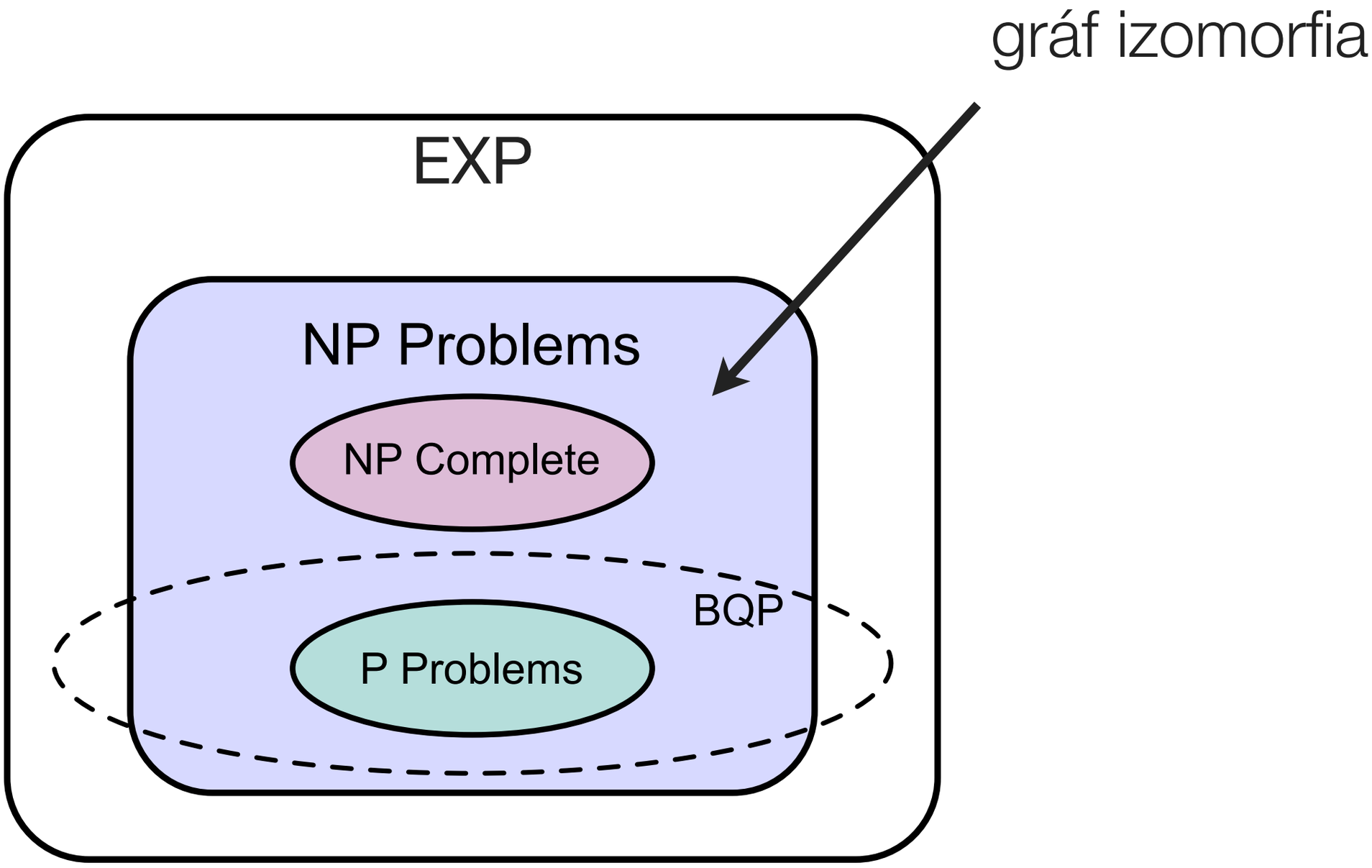
párhuzamosítás = TIME szükséglet

SPACE szükséglet

NP

nem-
determinisztikus
algoritmussal
polinom idő


EXP
NP Problems
NP Complete
BQP
P Problems


gráf izomorfia
EXP
NP Problems
NP Complete
BQP
P Problems

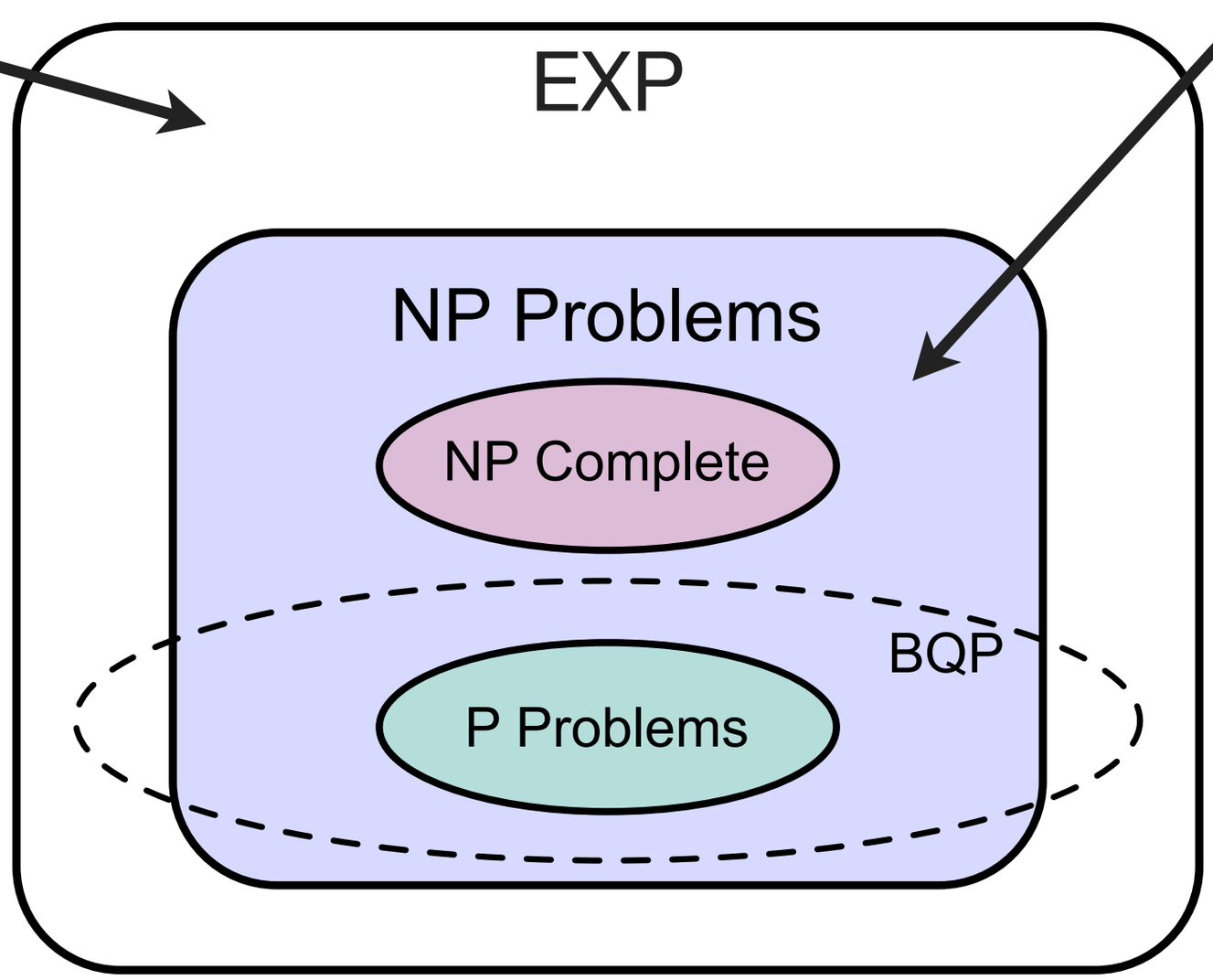
dobozrendezés

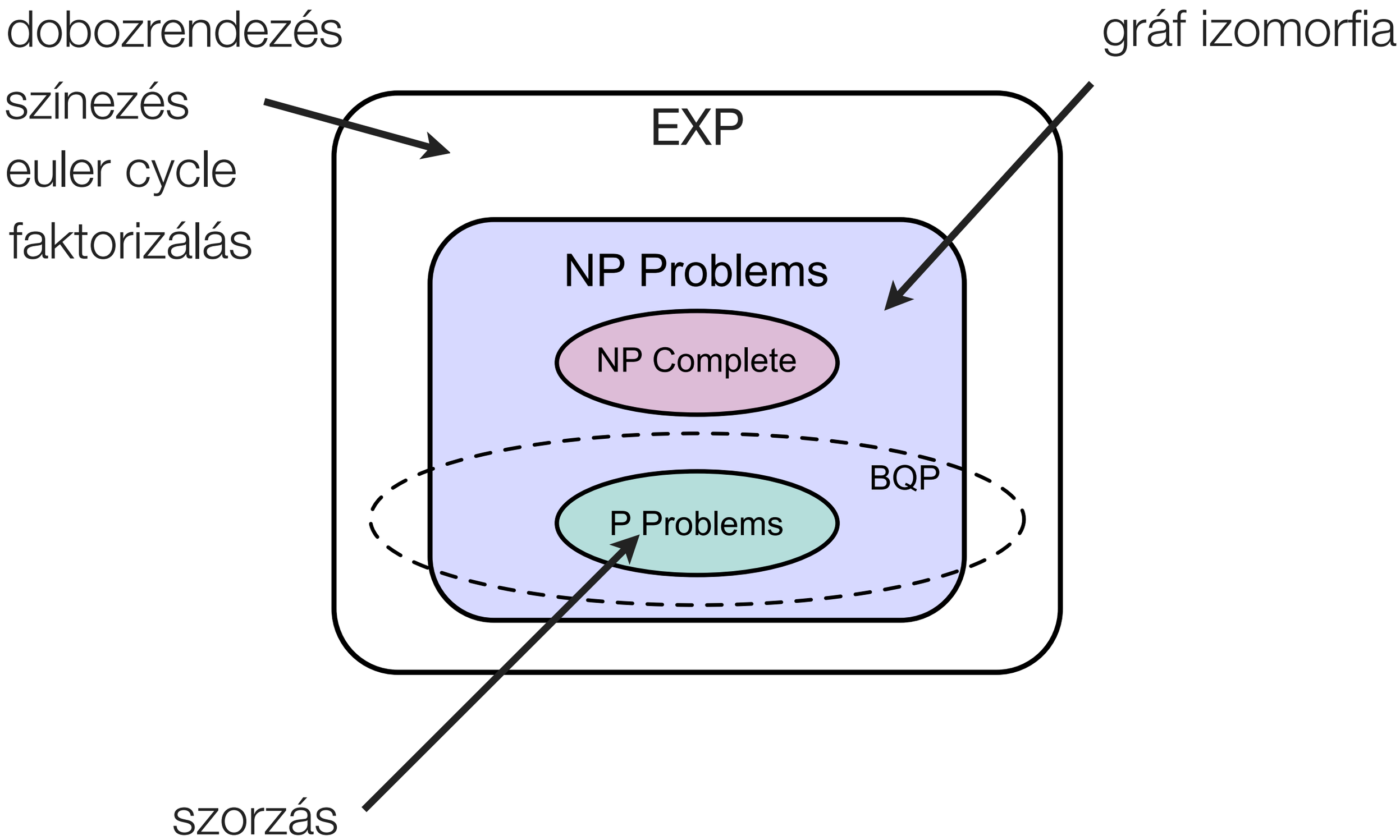
gráf izomorfia

színezés

euler cycle

faktorizálás




dobozrendezés
gráf izomorfia
színezés
euler cycle
faktorizálás
EXP
NP Problems
NP Complete
BQP
P Problems
szorzás

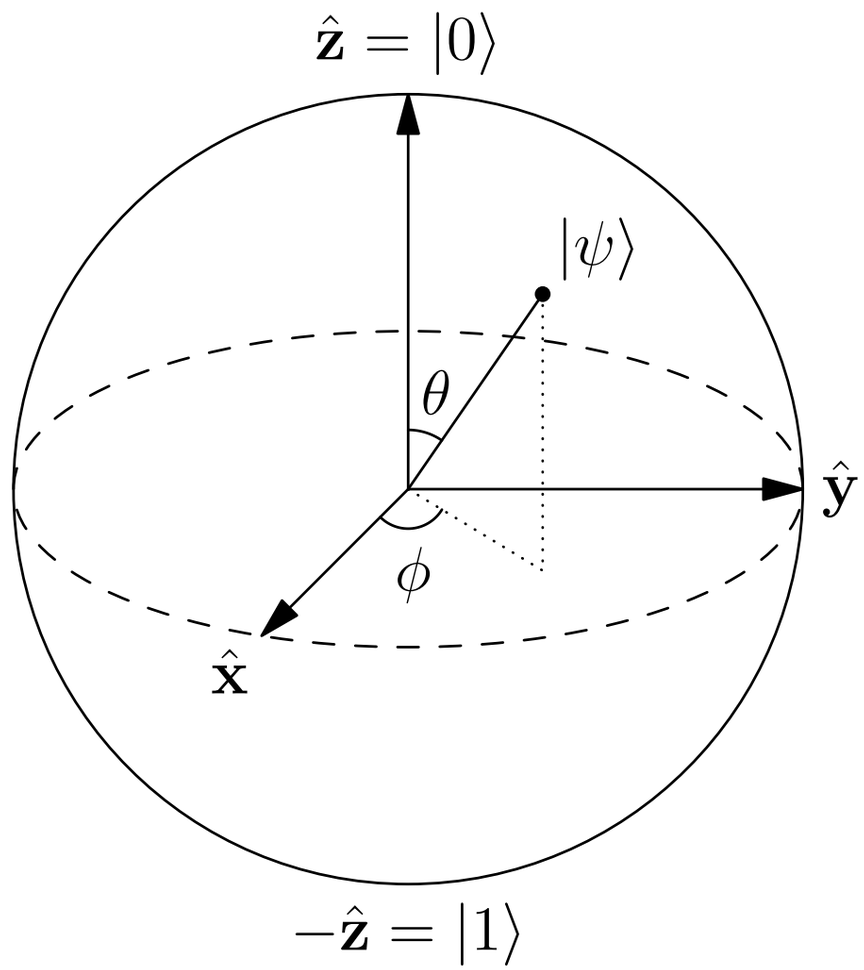
Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?

0

qubit


$\hat{\mathbf{z}} = |0\rangle$
$|\psi\rangle$
θ
$\hat{\mathbf{y}}$
ϕ
$\hat{\mathbf{x}}$
$-\hat{\mathbf{z}} = |1\rangle$

1

qubit

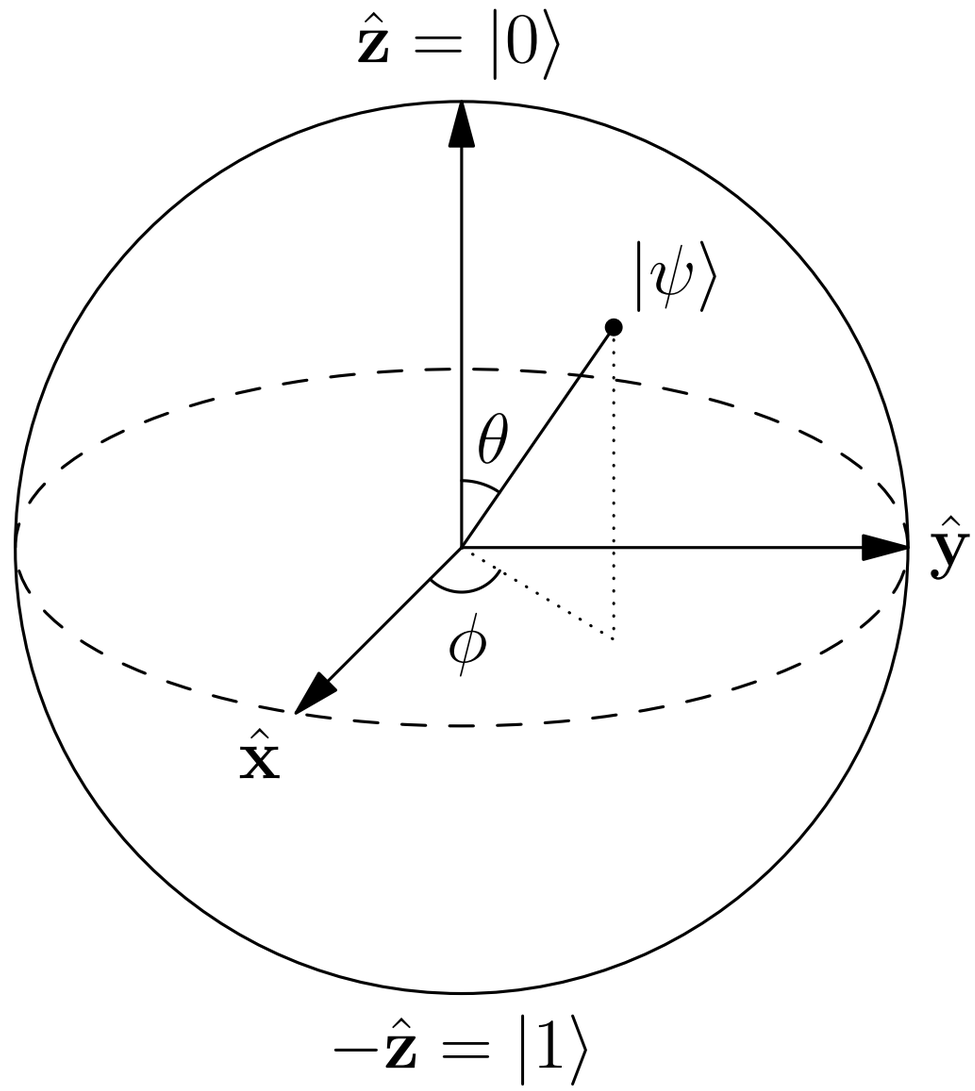
$$\psi = \alpha \, 0 + \beta \, 1$$

qubit

$$\psi = \alpha \, |0\rangle + \beta \, |1\rangle$$

ahol α és β eleme C
és absz négyz=1

ha nem lenne komplex akkor csak kör lenne



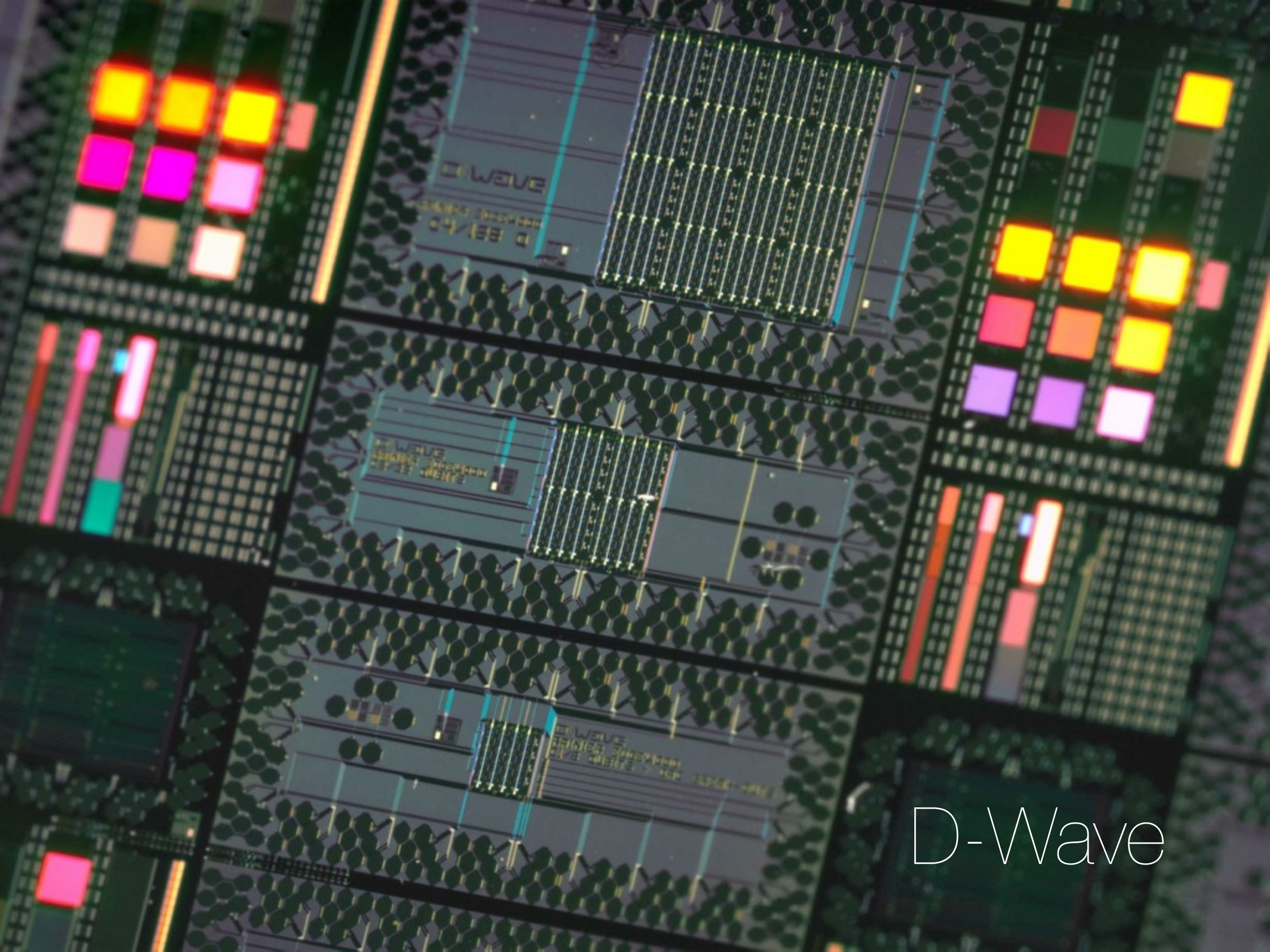
$(\theta,\phi) \longleftrightarrow (\alpha,\beta)$

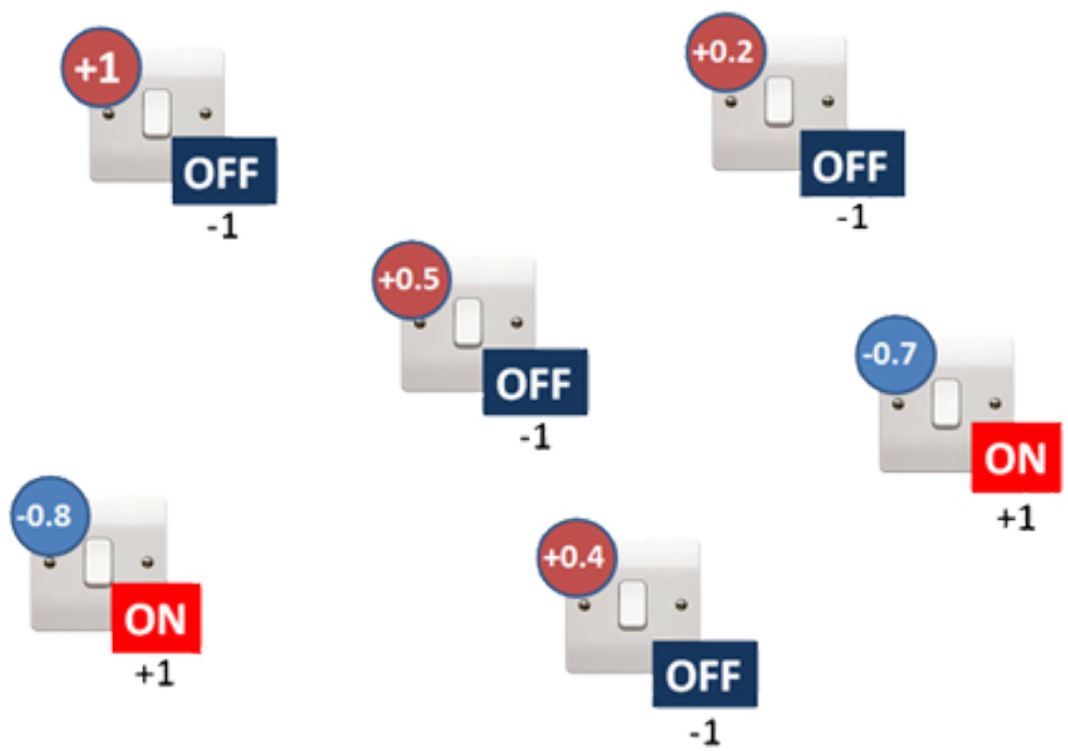
sokszor le kell futtatni mert csak 0 v 1 lehet az eredmény

Mitől lesz valami számítógép?

Mitől lesz valami kvantumszámítógép?

Létezhetnek kvantumszámítógépek?


D-Wave

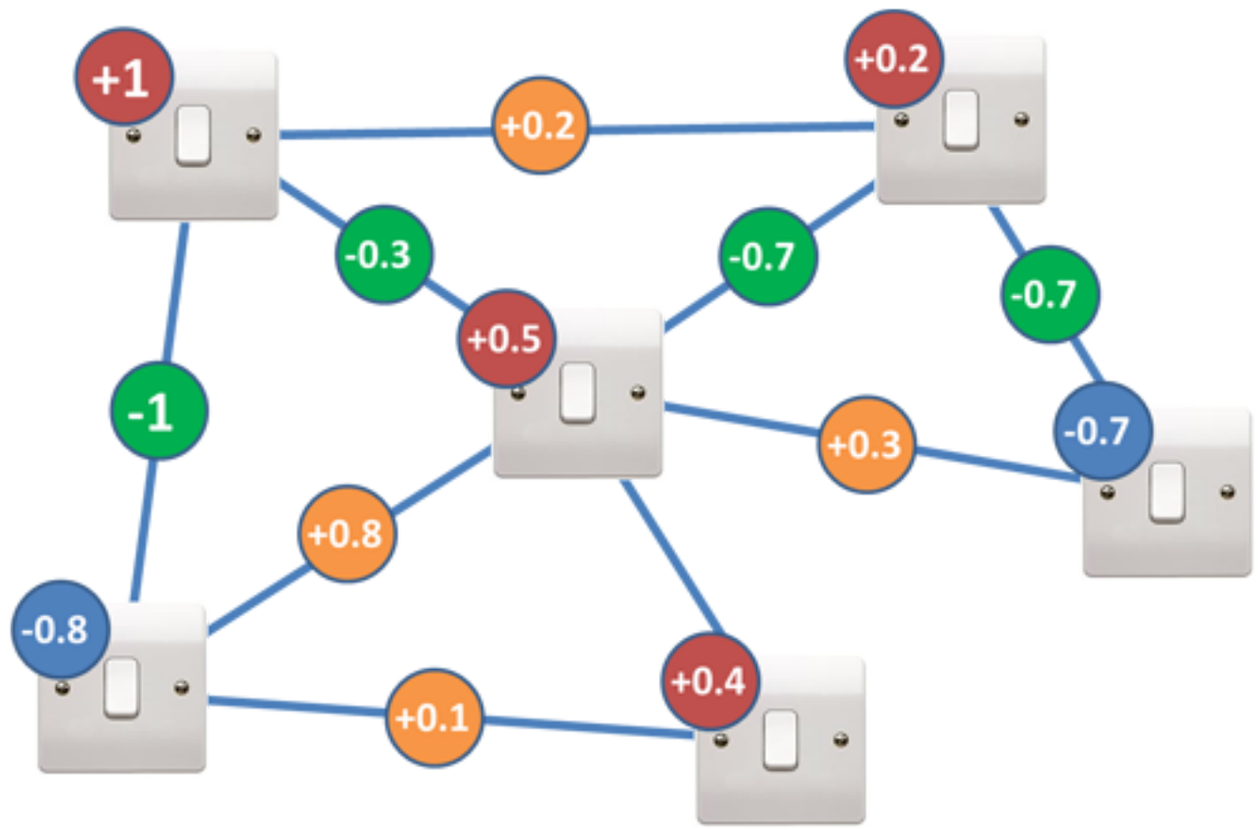


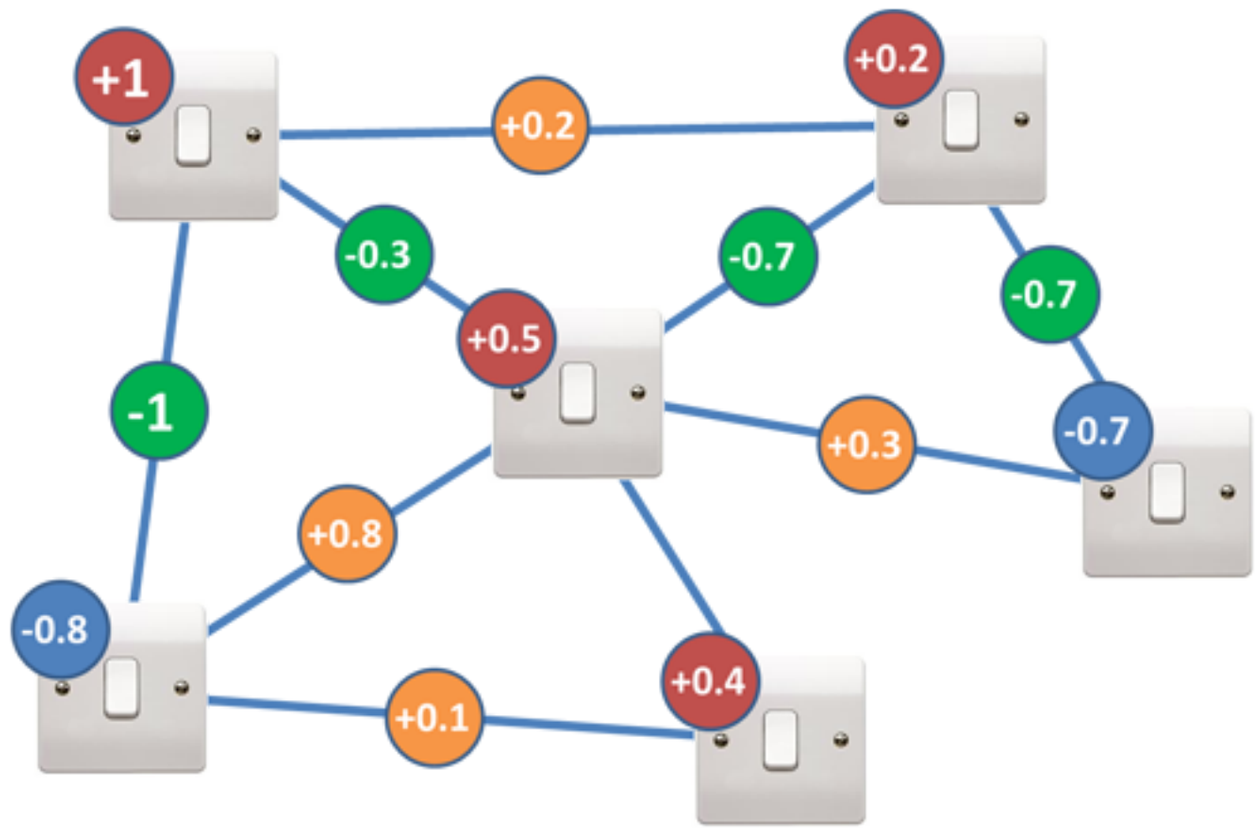
+1	x	-1	=	-1
+0.2	x	-1	=	-0.2
+0.5	x	-1	=	-0.5
-0.8	x	+1	=	-0.8
+0.4	x	-1	=	-0.4
-0.7	x	+1	=	-0.7

Total: -3.6

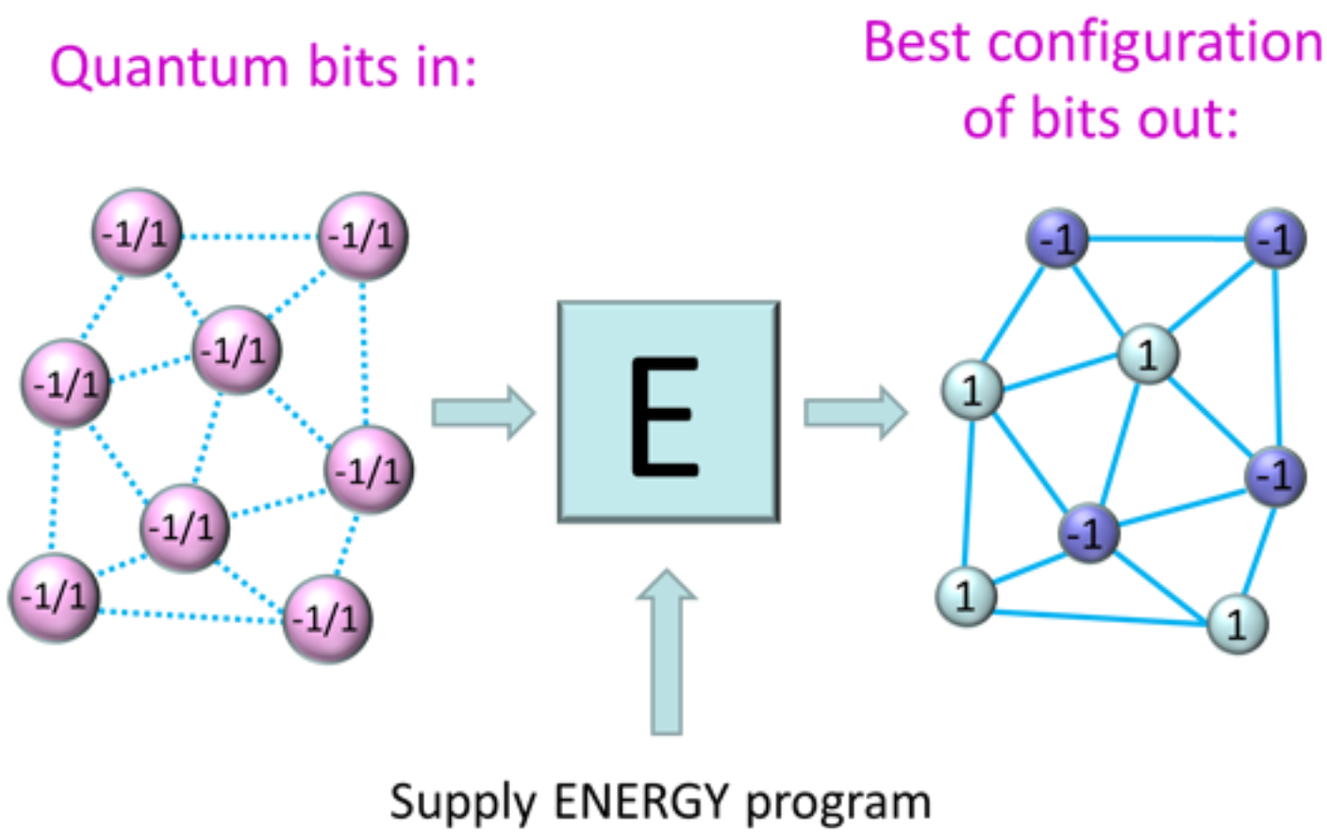
$$E(\mathbf{s}) = \sum_i h_i s_i + \boxed{\sum_{i,j} J_{i,j} s_i s_j}$$

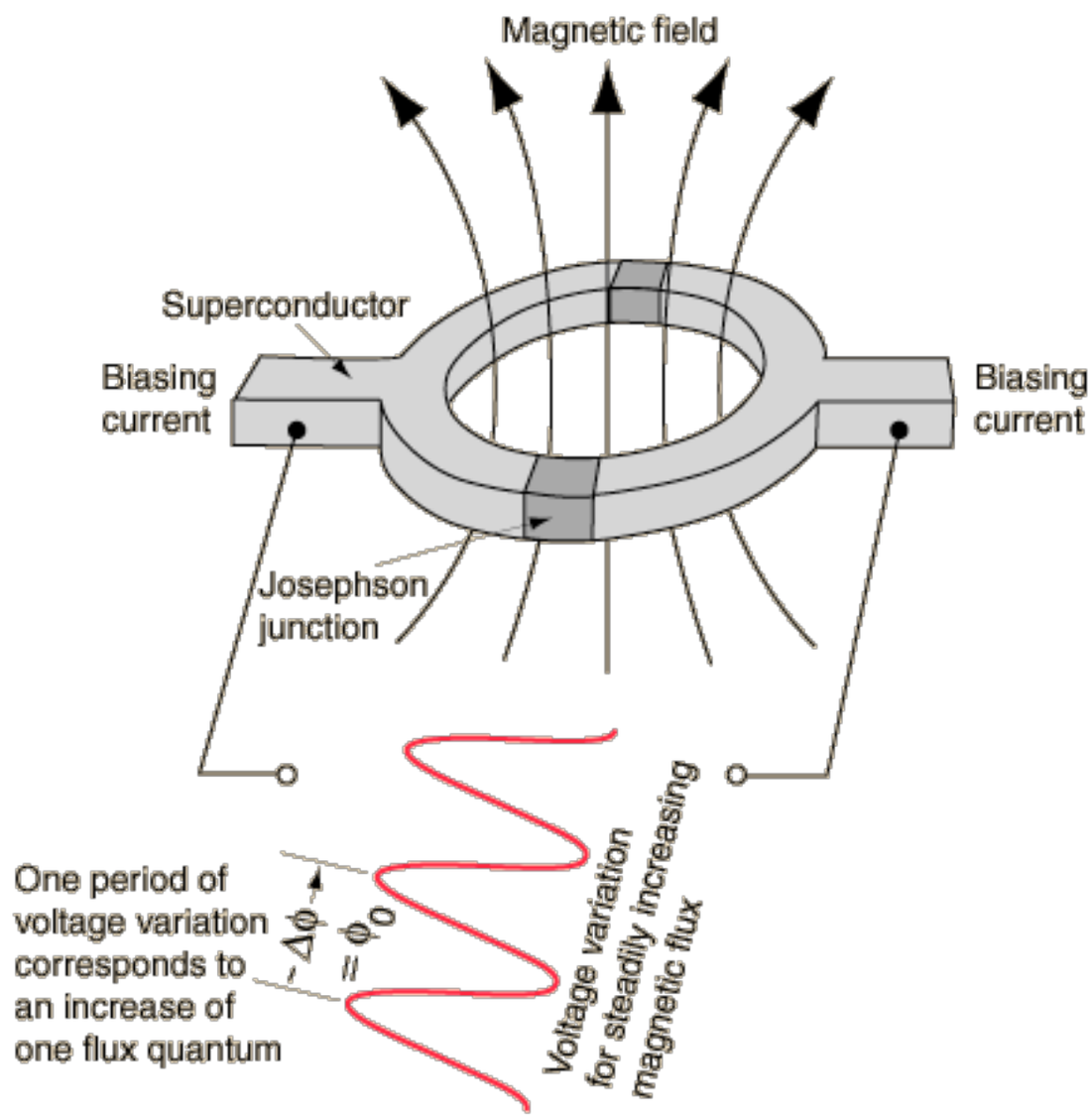
Adding another weight, J, which multiplies the product of the two switch settings.


+1
+0.2
+0.2
-0.3
-0.7
-0.7
+0.5
-1
+0.3
-0.7
+0.8
-0.8
+0.4
+0.1



NP teljes probléma


Quantum bits in:
Best configuration of bits out:
-1/1
-1/1
-1/1
-1/1
-1/1
-1/1
-1/1
-1/1
E
-1
-1
1
1
-1
-1
1
1
Supply ENERGY program


Magnetic field
Superconductor
Biasing current
Biasing current
Josephson junction
One period of voltage variation corresponds to an increase of one flux quantum
$\Delta\phi = \phi_0$
Voltage variation for steadily increasing magnetic flux

mitől kvantumos a kvantumszámítógép?

kísérleti metafizika

léteznek komplexitási osztályok?