

Informacioni dhe Kompjuteri Kuantik

Ervin Kafexhiu

Universiteti Tiranës, Fakulteti i Shkencave të Natyrës

20 Tetorë 2022

Permbajtja

- 1 Hyrje
- 2 Teoria Informacionit
- 3 Llogaritja (Computation) & Makina Turing
- 4 Informacioni Kuantik
- 5 Kompjuteri Kuantik
- 6 Permbledhje

Hyrje

Çmimi Nobel ne Fizike 2022

“for experiments with entangled photons, establishing the violation of Bell inequalities and **pioneering quantum information science**”



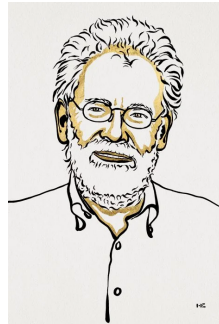
Alain Aspect

Prize share: 1/3



John F. Clauser

Prize share: 1/3



Anton Zeilinger

Prize share: 1/3

Ref: [nobelprize.org](https://www.nobelprize.org)

Motivimi

- Kompjuterat luajnë një rol themelorë sot në gjithë shoqërinë.
- Sa i kuptojmë funksionin e kompjuterave?
- Jemi pranë një *Revolucioni te Dytë Kuantike*. Zhvillim shume i shpejte i teknologjive te reja kuantike.
- Informacioni luan një rol fondamental në Fizikë.
- Shumë pak trajtohen këto tema në programet e Fizikës.

Dy konceptet themelore ne kete prezantim jane:

1) Informacioni 2) Llogaritja (Computing).

Teoria Informacionit

Çfare eshte Informacioni?

Informacioni:

- **Nuk eshte njohuri.** Interpretimi i tij eshte njohuri!
- **Zvogelon paqartesine/pasigurine.** Informacioni plote paqartesia/pasiguria shkojne ne zero.
- Eshte **pa-parashikueshmeri.** Gjerat e papritura jane informacion!
- **Prodhet, Ruhet, Fshihet, Transmetohet dhe Manipulohet/Ndryshet.**
- **Mbartet nga sistemet fizike.** Nuk eshte abstrakt.
- **Shprehet me Simbole/Gjuhe.**

Informacioni nuk eshte Njohuri!



Pavaresisht se ktu shkruhet informacion per jeten e Egjptianeve, ju duhet te interpretoni gjuhen/simbolet.

Informacioni zvogelon paqartesine/pasigurine



Informacioni zvogelon pasigurine/paqartesine (inJORANCEN).
Informacion i plote pasiguria apo inJORANCA shkon ne zero.

Informacioni eshte Aditiv!

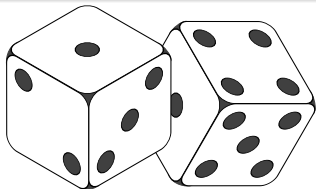
Informacioni duhet te gezoje vetine e mbledhjes. Le te jete I_1 dhe I_2 dy pjese informacioni, atehere:

$$I_3 = I_1 + I_2 \quad \text{ku} \quad I_3 > I_1, I_2$$

Dy emaille kane me shume informacion se nje.

Informacioni eshte pa-parashikueshmeri

- Nese lajmet e djeshme jane njelloj me te sotshmet, nuk kemi lajm/informacion!
- Nese moti eshte njelloj çdo dite. Nuk ka informacion prej parashikimit te motit.
- Rrjedhimisht, ngjarjet e parashikueshme (dmth me probabilitet $p = 0$ ose 1) kane informacion zero.
- Ngjarjet qe kane element rastesore ($0 < p < 1$) jane te pa-parashikueshme dhe permbajne informacion.



Informacioni mund te

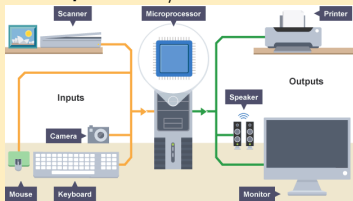
- Ruhet (Memorizohet).



- Transmetohet



- Manipulohet/Transformohet (nga kompjuterat)



Simbolet dhe Gjuha ne Kodimin e Informacionit

- **A mendojme dot pa fjale?**
- **A komunikojme dot pa nje gjuhe, Simbole, dhe Rregulla Sintaksore?**

Gjuha luan nje rol themelore, me konkretisht Gjuhët Formale.

Përkufizim

Një gjuhë formale L mbi një alfabet Σ është nënbashkësia e “fjalëve” nga Σ^* ($L \subset \Sigma^*$) që i bindet një grupi rregullash sintaksore për formimin e “fjalive” në L .

- Σ^* është “Ylli i Kleene” për bashkësinë Σ .
- Σ^* është bashkësia e fjalëve që formohet nga çdo kombinim mundëshëm i simboleve të Σ (për të gjitha gjatësitë e mundëshme të fjalëve).
- Gjuha L formohet nga një nënbashkësi fjalësh nga Σ^* bashkangjitur dhe rregullat e sintaksës (jo çdo rradhitje e fjalëve formon fjali në L).

Çfare eshte Σ^*

- Le te jete $\Sigma = \{|\}$ nje bashkesi unare (vetem me nje simbol) atehere $\Sigma^* = \{-, |, ||, |||, ||||, \dots\}$.
- Le te jete $\Sigma = \{a, b\}$ mje bashkesi binare simbolesh (ose $\Sigma = \{0, 1\}$ etj...) atehere $\Sigma^* = \{-, a, b, ab, aa, ab, ba, bb, aaa, aab, aba, \dots\}$.
- $\Sigma = \{a, b, c, \text{ç}, d, \dots \text{zh}, A, B, C, \text{Ç}, D, \dots, \text{Zh}\}$ eshte alfabeti Shqiptare, $\Sigma^* =$ te gjitha kombinimet e mundeshme te ketyre simboleve. Gjuha shqipe permban nje nenbashkesi te vogel te fjaleve ne Σ^* .

Çfarë është Sintaksa

Supozojmë një gjuhë L me alfabet $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, =\}$ dhe rregulla sintaksore:

- 1 Çdo fjali që ka fjalë që nuk përmbajnë “+” ose “=” dhe nuk përmbajnë “0” në fillim te fjalës, janë pjesë e L .
 - 2 Fjala “0” është në L .
 - 3 Një fjali që përmbanë “=” është në L nëqoftëse “=” ndan dy fjalë të lejuara në L .
 - 4 Një fjali që përmban “+” por jo “=” është në L vetëm nëse “+” ndan dy fjalë të lejuara në L .
 - 5 Nuk ka fjali në L përveç atyre që vendosen nga rregullat e mësipërme.
- Sintaksa vendos që jo çdo kombinim i fjaleve nga L është pjesë e gjuhës.
 - Nga mesiper, fjalia “103+41=777” $\in L$, ndersa “=524=+” $\notin L$.
 - Pavaresisht se fjalia “103+41=777” është sintaktikisht korrekt, nuk ka kuptim nëse simbolet janë numrat natyrore.
 - Jemi në qe i vendosim kuptim fjaleve – Semantika.

Gjuha Binare

Alfabeti ka dy simbole $\Sigma = \{0, 1\} = \{T, F\} = \{\bullet, -\}$.

Çdo gjuhe mund te codohet/perkthehet ne gjuhe binare.

Kodi Morse:

A	● —	N	— ●
B	— ● ● ●	O	— — —
C	— ● — ●	P	● — — ●
D	— ● ●	Q	— — ● —
E	●	R	● — ●
F	● ● — ●	S	● ● ●
G	— — ●	T	—
H	● ● ● ●	U	● ● —
I	● ●	V	● ● ● —
J	● — — —	W	● — —
K	— ● —	X	— ● ● —
L	● — ● ●	Y	— ● — —
M	— —	Z	— — ● ●

Gjuha Grafike

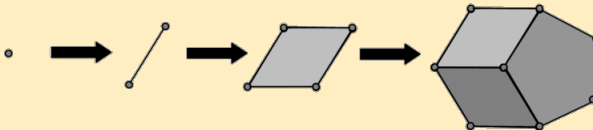
Alfabeti Σ :



*Aa Bb Cc Dd Ee Ff Gg Hh
Ii Jj Kk Ll Mm Nn Oo Pp
Qq Rr Ss Tt Uu Vv Ww
Xx Yy Zz . ? 1 2 3 4 5 6 7 8 9 10*

Gjuha Gjeometrike

Alfabeti gjeometrik do permbante primitivat si pika, vija etj...



Shkruajmë të njëjtin informacion në dy gjuhë L_1 dhe L_2 :

Gjuha L_1 : Ligji II i Newton-it

$$\dot{\vec{p}} = \vec{F}$$

Gjuha L_2 : Ligji II i Newton-it

Derivati kohor i impulsit të një pike masore është i barabartë me forcën rezultante që vepron mbi të.

Eshte e qarte qe pavaresisht se fjalite e mesiperme ne gjuhen L_1 dhe L_2 kane te njejtin kuptim (Semantike) dhe shprehin ekzaktesisht te njejtin informacion, gjuha L_2 eshte me pak eficiente (“redundant” –teprice simbolesh).

⇒ **Sasia e informacionit nuk varet nga numri i simboleve qe duhet per te shprehur nje kuptim.**

Teprica ne nje gjuhe (“Redundancy”)

A mund ta lexoni fjaline e meposhteme?

J_m d_ke prez_ntu_r pun_n tim_.

Jo te gjitha shkronjat nevojiten per te kuptuar informacinin e fjalise.

Pra disa shkronja jane te “tepërta”.

Pse ekziston tepërsia “redundancy” në gjuhën tonë?

- Arsya eshte zhurma. Biseda në zhurmë rrit përsëritshmërinë e fjalëve.
- **Pse kur bisedojmë në largësi tentojmë ti zgjasim fjalët që themi?**

Sasia informacionit

- Kuantifikimi i informacionit ka nje histori te gjate dhe shume diskutim filozofik (Shiko: [Stanford Encyclopedia of Philosophy](#))
- Per te matur **kapacitetin (dhe shpejtesine) e transmetimit te informacionit** ne nje kanal ne prani ose jo te zhurmes, [Harry Nyquist](#) dhe [Ralph Hartley](#) ne vitet 1920 dhe [Claude Shannon](#) ne vitet 1940, themeluan Teorine e Informacionit.

Teoria Informacionit

- Studion: [Kuantifikimin, ruajtjen dhe komunikimin e informacionit digjital.](#)
- Koncepti **themelore** eshte **Entropia** qe [kuantifikon sasin e papercaktueshmerise](#) qe lidhet me nje variabel rastesore ose rezultati nga matja e nje procesi rastesore.

Sasia informacionit = Entropi

Entropia e Shannon

[Shannon(1948), Shannon & Weaver(1949)]

$$H = - \sum_i p_i \log_2(p_i) \quad [\text{ne bit}]$$

nese baza logaritmit eshte *e*, *H* matet me *nat* dhe nese 10 matet me *hartley* ose *dit*

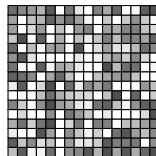
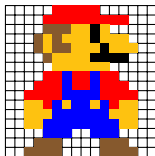
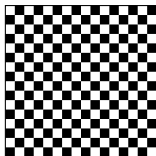
Sasia informacioni eshte $I = -\log_2(p)$ dhe $H = E[I]$ eshte mesatarja informacionit.

Shembulli Monedhes

Monedha ka dy ane $\{K, P\}$. Per probabilitete te barabarta $p_K = p_P = 1/2$ papercaktueshmeri eshte maksimale. Ne rast se $p_K \neq p_P$ njera ane do bie me shpesh, pra “ka me shume nje rregullsi” (papercaktueshmeri me te vogel).

$$H = -p_K \log_2(p_K) - p_P \log_2(p_P) = -p_K \log_2(p_K) - (1 - p_K) \log_2(1 - p_K)$$
$$p_K = \frac{1}{2} \Rightarrow H = 1 \text{ bit.}$$

Kompresimi Informacionit



$$H_1 < H_2 < H_3 < H_4$$

- Entropia na lejon te masim sasine e vertete te informacionit dhe te gjejme kur ka “redundancy” dhe te ndertojme nje kod optimal per transmetimin e informacionit.
- Informacioni i permbajtur ne çdo figure rritet me parregullsine. Fot 1 ka entropine minimale ndersa foto 4 ka maksimumin.
- Foto 1 me entropi minimale mund te kompresohet ne vetem ngjyre pikseli dhe numri total pikselash. Ndersa foto 4 me maksimum entropie nuk mund te kompresohet.
- Natyra dhe bota e gjalle nuk jane plotesisht te rregullta si H_1 dhe H_2 dhe as totalisht te çrregullta dhe rastesore si H_4 . Ato jane ne midis tyre dhe ngjajne si H_3 qe kane ndonje pattern dhe mund te kompresohen.

Gjithe ligjet e Fizikes jane kompresim i fenomeneve natyrore.

Informacionit ne Termodinamike

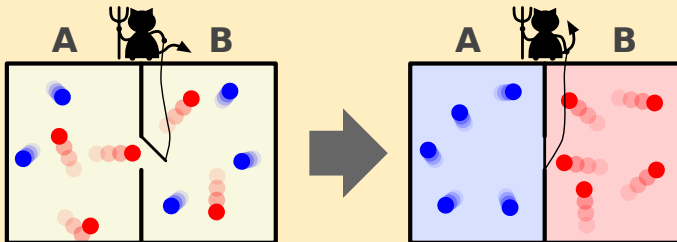
- Informacioni nuk eshte thjeshte komunikimi mes pajisjeve apo njerezve.
- Ne **Fizike Informacioni luan nje rol themelore** (nga makinat me avull, tek vrimat e zeza dhe vete perberja e hapesire-kohe.)
- **Koncepti i Entropise ne Teorine e Informacionit e ka origjinen ne Termodinamike.**
- **Entropia e Boltzmann-it:** $S = k_B \log(W)$. k_B konstantia e Boltzmann, W numri mikrogjendjeve qe konfigurojne makrogjendjen e sistemit.
- **Entropia e Gibbs-it:** $S = -k_B \sum_i p_i \log(p_i)$. p_i eshte probabiliteti i çdo mikrogjendje i te makrogjendjes se sistemit.

Ligji II i Termodinamikes

- Formulimi 1: Entropia e nje sistemi termodinamik te izoluar nuk zvogelohet me kohen ($\dot{S} \geq 0$).
- Formulimi 2: Nxehtesia kalon gjithmone nga trupi me i nxehte drejt atij me te ftohte.
- Formulimi ...

Ky ligji ka nje natyre empirike dhe verehet ne çdo sistem termodinamik. Per te kuptuar implikimet e ketij ligji, Maxwell propozoj nje eksperiment te menduar.

Demonët e Maxwell-it



Dy dhoma A dhe B me gaz janë të ndara nga një mur. **Ne qender të murit është një dërë të vogël dhe që komandohet nga një Demon i cili ka njohuri/vezhëgim të plotë mbi çdo molekulë.** Sa herë që një molekulë e shpejtë nga dhoma A i afrohet derës, demoni e hap dhe lejon të kalojë në B . Gjithashtu sa herë që një molekulë e ngadalte nga dhoma B i afrohet derës, demoni e hap derën të kalojë në A . Mbas një fare kohe, në dhomen A janë mbledhur vetëm molekula të ngadalta ndërsa në B vetëm të shpejta.

- Informacioni i demonit lejon te krijojme rregull nga çrregullsia dhe zvogelimin e Entropise me kohen $\dot{S} < 0$, ne kundërshtim me ligjin e dyte te Termodinamikes!
- Nisur nga kjo, **Szilard propozoj nje makine termodinamike** qe mund te prodhoje energji nga informacioni [Szilard (1929)].
- Landauer llogariti sasine minimale te energjise qe duhet me fshi nje bit, i njohur si **Principi i Landauer** [Landauer (1961)]:

Minimumi i energjise se mundeshme qe nje pajisje kompjuterike do shpenzoje per te kryer nje veprim/proces te pa-kthyeshme sic eshte fshirja e 1 bit eshte
 $E = k_B T \ln 2$ [psh. Berut et al. (2012)].

Informacioni eshte binar

Sinjali digjital

- Ne praktike informacioni qe perdorim eshte me dy simbole psh. $\Sigma = \{0, 1\}$.
- Secili simbol permban 1 bit informacion.
- Sinjali binar dallohet lehte ne prani te zhurmes dhe pajisjet elektronike ndertohen lehte.

Informacioni ne Sinjalet Analoge

- **sinjalet analoge – niveli i zhurmes dhe rezolucioni i matjes kufizon numrin e gjendjeve qe mund te perdorem per te koduar informacion.**
- Sinjali analog mund te kodohet vetem ne nje numer te fundem/diskret gjendjesh [Shannon (1948)]

Llogaritja (Computation) & Makina Turing

Llogaritja (Computation)

Makina qe Manipulon Simbole

- Maxwell, Szilard, Landauer, Brillouin dhe te tjere, po mendonin si te ndertojne makina termodinamike qe manipulojne informacionin per te prodhuar energji. (shiko psh [Szilard (1929), Toyabe et al. (2010)])
- Te pakte ishin ata qe mund te enderronin per nje makine universale qe do mund te manipulonte informacionin vete, siç eshte psh. truri i njeriut.
- Kjo makine quhet sot **Kompjuter** dhe origjine e ka nga avancimet ne **Matematiken Fundamentale**, fusha e **Logjikes**.

Llogaritja Digjitale

- Nocioni me i rendesishem i llogaritjes eshte ai i *“Llogaritjes Digjitale”*.
- Ky nocion u zhvilluar dhe u formalizua ne vitet 1930 nga Turing, Gödel, Church, Post dhe Kleene.
- Ato po investigonin themelet e matematikes nisur nga problemi i 10 i Hilbert: **“Entscheidungsproblem”**.
- “Entscheidungsproblem” lidhet me problemin i vendimarrjes ne logjiken matematike te rendit te pare (first-order logic) dhe kerkon nese ekzston nje Algoritem qe te percaktoje nese nje shprehje logjike eshte teoreme ose jo.

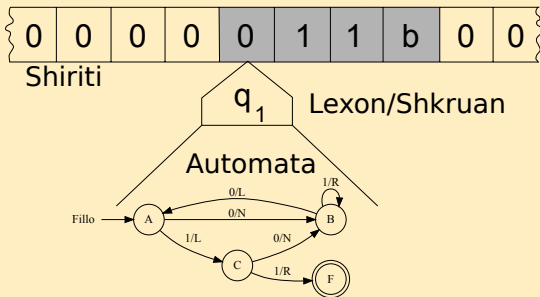
Llogaritja (Computation)

Llogaritja Digjitale

- Pergjigja e ketij problemi eshte jo! (shiko [Turing (1936,1937), Church (1936)])
- Per te provuar kete, Turing dhe Church ofruan nocionin e **“funksioneve qe llogariten ne menyre efektive”**.
- Turing e beri kete nepermjet asaj qe quhet **Makina Turing**: Nje pajisje qe manipulon/ndryshon simbole diskrete te shkruara mbi nje shirit ne perputhje me nje numer te fundem instruksionesh.
- Ekzistojne modele te tjera llogaritese, por eshte provuar matematikisht qe ato jane ekuivalente me nje Makine Turing.

Perkufizimi i Makinës Turing

Makina Turing është një model matematikorë që operon mbi një shirit infinit të gjatë të ndare me qeliza që makina i lexon dhe shkruan një nga një në menyre sekuenciale. Koka e makinës e cila lexon dhe shkruan, operohet nga një bashkësi e fundme instruksionesh elementare.

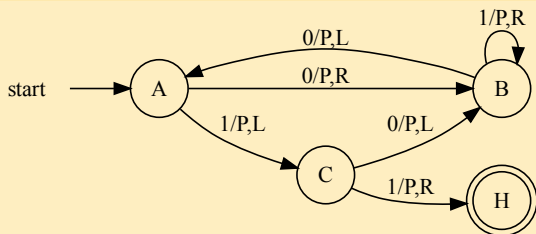


Perkufizimi Formal i Makinës Turing

Makina Turing është shtateshja $M = \{\Gamma, b, \Sigma, Q, q_0, F, \delta\}$ ku:

- Γ është alfabeti i simboleve të shiritit (zakonisht $\Gamma = \{0, 1\}$).
- b është simboli bosh (blank) (lejohet të ndodhi pafundesisht herë në shirit në çdo hap të llogaritjes).
- $\Sigma \subseteq \Gamma / \{b\}$ bashkësia e simboleve të lejuara të shfaqen në përmbajtjen fillestare të shiritit.
- Q është bashkësia e fundeme të gjendjeve të makines.
- $q_0 \in Q$ është gjendja fillestare e makines.
- $F \subseteq Q$ është bashkësia e gjendjeve përfundimtare ose gjendjet e pranueshme. Thuhet që përmbajtja M fillestare e shiritit pranohet nëse makina përfundon llogaritjen në një nga gjendjet F .
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R, N\}$ qu funksioni kalimeve (next-state function). δ merr një input nga Γ dhe gjendjen q_i që ndodhet makina dhe bën kalimin në gjendjen e re q , shkruan ose jo një simbol mbi shirit dhe lëviz koken e makines majtas L , djathtas R ose nuk lëviz N .

Shembull i nje Makine Turing

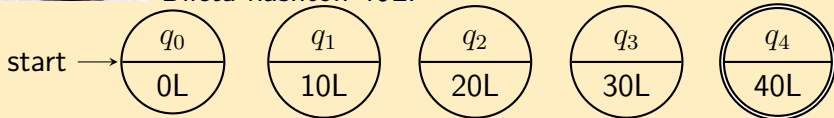


- $\Gamma = \{0, 1\}$ (alfabeti shiritit);
- $b = 0$ (simboli bosh/blank);
- $\Sigma = \{1\}$ (symbolet fillestare);
- $Q = \{A, B, C, \text{HALT}\}$ (gjendjet);
- $q_0 = A$ (gjendja fillestare);
- $F = \{\text{HALT}\}$ (gjendja perfundimtare);
- δ jipet nga grafi ne figure.

Shembull i nje Automate FSM



Bileta kushton 40L.



Implementimi Fizik i Makines Turing

- Te ndertosh nje sistem llogarites duhet qe te implementosh nje Makine Turing mbi nje sistem fizik.
- Duhet nje sistem me nje numer te fundem gjendjesh Q dhe funksion kalimi mes gjendjeve δ (dinamika e sistemit).
- A mund qe çdo sistem fizik te llogarisi? Nga ndryshon nje gur, nje makine llogaritese dhe nje kompjuter?
- Ajo qe i dallon eshte se sa kompleks jane keto sisteme fizike per te implementuar/suportuar nje model llogarites.
- Sa e lehte eshte per ti kontrolluar gjendjet fizike dhe dinamiken e ketyre sistemeve.
- **Nje sistem llogarites eshte nje izomorfizem e nje modeli matematik llogarites sic eshte Makina Turing.**

Limitimet

- **Makinat Turing llogarisin funksione te tipit $f : \mathcal{N} \rightarrow \mathcal{N}$** dhe mund te modelojne çdo (mbi numrat natyrore). Numrat reale \mathcal{R} nuk jane pjese e bashkesise (dhe problemet me numrat reale qe ka interes ne simulimet fizie, vetem mund te perafrohen).
- **Klomplesiteti i Algoritmeve:** Jo çdo algoritem mund te ekzekutohet ne menyre eficiente nga nje Makine Turing. Sa kohe dhe memorie i duhet nje Makine Turing per te llogaritur nje Algoritem. Klasat e algoritmeve eficiente.
- Çdo kompjuter i ndertuar deri me sot eshte ekuivalent me nje Makine Turing.
- **Pavaresisht perpjekjeve te medha, deri me sot nuk ka patur sukses te ndertohet nje makine universale qe nuk eshte Makine Turing.**

Informacioni Kuantik

Themelet e Mekanikes Kuantike

Mekanika Kuantike ndryshon totalisht menyren e pershkrimtit te nje sistemi kuantik.

- Gjendjet e sistemit pershkruhen nga “funksionet valore” $|\psi\rangle \in \mathcal{H}$ nga nje hapsire Hilbert mbi numra kompleks.
- Madhesite fizike jane operatore Hermitian ne \mathcal{H} dhe veprojne mbi funksionet valore.

Jane tre fenomene kuantike qe e bejne informacionin kuantik te ndryshem nga ai klasik:

- **Superpozimi kuantik.**
- **Entanglement (korrelacioni kuantik).**
- **Matja (dekoherenca).**

Informacioni Kuantik

Informacioni klasik digjital perbehet nga dy gjendje $\{0, 1\}$.

Superpozimi kuantik

Supozojme qe sistemi kuantik me dy gjendje, simbolikisht $|0\rangle$ dhe $|1\rangle$ atehere çdo kombinim linear i tyre eshte serisht nje gjendje e sistemit

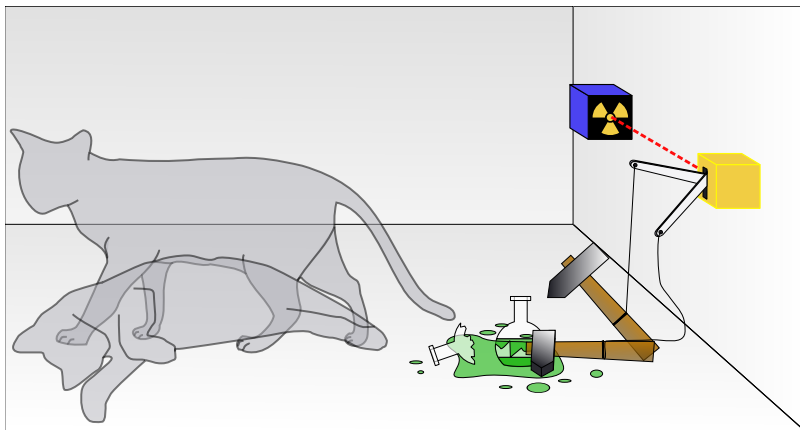
$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \text{per } \alpha, \beta \in \mathbb{C} \quad \text{dhe} \quad |\alpha|^2 + |\beta|^2 = 1.$$

- $|\alpha|^2$ dhe $|\beta|^2$ japin probabilitete e matjes ne gjendjet $|0\rangle$ dhe $|1\rangle$, respektivisht.
- Ekziston nje numer i pafundem gjendjesh $|\psi\rangle$.
- $|0\rangle$ dhe $|1\rangle$ quhen bite kuantike (qubit).
- Informacioni qe mund te kodohet nga nje sistem binare kuantik eshte me i madh se ne rasting klasik.

Entanglement (korrelacioni kuantik)

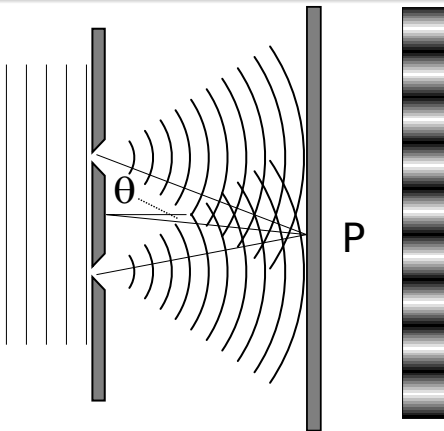
- Dy grimca qe afrohen afer dhe lejohen te bashkeveprojne, funksionet valore te tyre “superpozohen” dhe formojne nje funksion te perbashket.
- Nese te dy grimcat largohen me pas shume larg njera tjetres dhe matet gjendja e njerës, atehere edhe grimca tjetër ne cast i dihet gjendja.
- Hapsira e Hilbert-it per dy qubit paraqitet nga gjendejet e Bell-it
$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle)$$
ku psh $|00\rangle = |0\rangle_1 \otimes |0\rangle_2$.
- Çmimi nobel u mor per kuptimin me te thelle te ketij fenomeni.
- Entanglement shton informacion per sistemin me dy bite, lejon teleportimin dhe shkembimin e informacionit kuantik.

Macja e Schröndinger



Matja dhe Dekoherenca

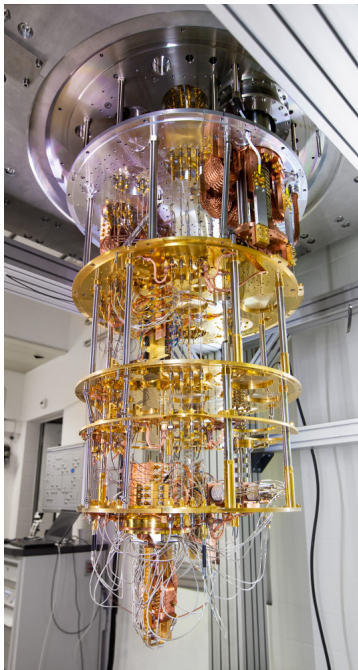
Roli i matjes: Matja kuantike e “shkatarron” ne menyre te pa kthyeshme superpozimin dhe shemb funksionin valor ne nje nga gjendjet vetjake/pastra. Matjet kan thelbesisht natyre probabilitare.



Ndryshimet mes informacionit kuantik dhe atij klasik

- Informacioni Klasik: **0 OSE 1**
- Informacioni Kuantik: **0 DHE 1**, superpozimi gjendjeve, entanglement.
- Informacioni Kuantik ka natyre probabiliste.
- Gjendjet Kuantike shkaterrohen lehte nga dekoherenca dhe kerkojn temperatura krijogjenike.

Kompjuteri Kuantik



Kompjuteri Kuantik shfrytezon

- Superpozimin kuantik per te enkoduar me shume informacion
- Entanglement per te komunikuar mes qubit apo ruajtur info.
- Quantum Gates per te manipuluar qubits (jo Logical Gates si kompjuteri klasik)

Kompjuteri Kuantik funksionon ne temperatura te uleta ($T \sim 1$ K) per te mbrojtur sa me gjate sistemin nga dekoherenca ambjentit.

Cfare mund te bej nje kompjuter kuantik?

Kompjuterat kuantik pritet te shkelqejne ne:

- Kriptografi (nga teorema e pa klonueshmerise)
- Kerkim database (algoritmat kuantike premtone shpejtesi kerkimi te pa arriteshme nga kompjuteri klasik)
- Simulime kuantike te proceseve fizike dhe kimike qe jan te pamundura nga kompjuteri klasik.
- Inteligjence artificiale
- Parashikime te motit
- Modelimi financiar etj...

Permbledhje

Permbledhje

- Informacioni luan nje rol themelore ne fizik (nga termodinamika, te vrimat e zeza e te vete hapesire–koha)
- Informacioni kuantik eshte nje pergjithesim i atij klasik.
- Kompjuterat jane sisteme fizike dhe llogarisin duke ju bindur ligjeve te fizikes.
- Llogaritja eshte manipulim/ndryshim i objekteve diskrete (sistemi dhe informacioni fizik) ne menyre lokale dhe sekuenciale sipas disa rregullave qe mund te jene deterministe ose jo.
- Kompjuteri Kuantik eshte nje Makine Turing, dhe ne princip eshte ekuivalent me ate klasik. Algoritmet kuantike shkelqejne ne disa klasa problemesh qe kompjuer klasik i duhet kohe jo polinomiale (psh kriptografi, kerkim databazash, machine learning, simulime sistemesh fizike etj...).

Permbledhje

- Jemi ne revolucionin e dyte kuantik, dhe kemi nje mori teknologjise te reja qe rrjedhin nga manipulimi i informacionit kuantik (gjeneratori i numrave te rastit, teleportimi, quantum key distribution, kompjuteri kuantik, sensoret....)
- Mundesite qe ju te merrni pjese ne kete revolucion dhe te kontribuoni jane realisht shume te medha...