

Leksikono de kvantika informadiko

Christian Rivière

(la 15-an de marto 2020-a)

Enkonduko

Redakti leksikonon de naskiĝanta fako estas malfacila tasko. Unue, ĉar eĉ la nomo de la fako ne komune ekzistas. Due, ĉar ne eblas listigi la ĉifakajn terminojn en multaj lingvoj. En la postaj paĝoj, tradukoj estas proponataj en nur du lingvoj, nome en la angla kaj en la franca. Estas verŝajne ke ne ĉiuj koncepto-vortigoj estus facile troveblaj en la korpusoj de iuj ajn lingvoj de la mondo, eĉ de la plej grandaj, almenaŭ pro la fakto ke la kelkaj homoj kiuj profesie esploras la kvantikon, plej ofte uzas la anglan (almenaŭ por la fakaj vortoj), i.a. ĉar tia speco de esploro necesigas kolektivan laboron sine de internacia medio.

En 2019, malmultaj homoj jam aŭdis pri la kvantika informadiko. Cetere estas ofta la konfuzo inter du fakoj, laŭ evidenta anakronismo :

- . la kvantuma fiziko (studado kaj formulado de naturaj fenomenoj) ;
- . la kvantika komputiko (inspirita de principoj de la kvantuma fiziko).

Siaflanke, la kvantika komputiko, same kiel la klasika komputiko havas du vizaĝojn : la hardvaran kaj la softvaran.

. la unua rilatas al la konstruado de nova generacio de kvantikaj komputoroj, kiuj grandparte iam funkcios surbaze de kvantumaj fenomenoj. En 2019, ekzistas (de proks. dek du jaroj) nur prototipoj sen evidenta utileco, sed la situacio evoluas pli kaj pli rapide ;

. la dua (ĉi tie nomata « kvantika informadiko ») rilatas al la « programado de algoritmoj », kiuj iam funkcios per komputoroj apriorie kvantikaj. Sed la pritraktataj problemoj mem havas **neniun rilaton** kun la kvantuma mondo. En kelkaj okazoj, la referenco al principoj de la kvantika informadiko estas nur formulada kaj metodologia (tipa ekzemplo : La « teorio de la elektoj »).

La analogeco kun la klasika informadiko estas nur parta. Estas necese precizigi kelkajn punktojn :

. mezuro de kvantika informo (legado de rezulto) modifas la staton de la legata inform-sistemo ĉiuforte kiam tiu ĉi ne estas en ununura stato. Alidirite, mezuro provizas rezulton detruante la staton de la mezurata sistemo (aŭ de la legata informo) ;

. do legado de intera rezulto ne eblas (des malpli ke ene de algoritmo, la datumoj esence troviĝas en supermetitaj statoj), dum sekurigi informojn meze de programo estas kutimo (eĉ neceso) en klasika programado ;

. korelative, la uzataj operatoroj estu inversigeblaj, kio malpermesas la uzon de la plej komunaj logikiloj (« *and* / kaj », « *or* / aŭ », « *nand* / nek », ...) ;

. ĉiuj valoroj (eventualaj rezultoj de problemoj) estas paralele pritraktataj (samtempe konsiderataj), dum en kutima algoritmo svarmas iteracioj laŭ loka variabla por pritrakti la valorojn sinsekve ;

. en la kvantikaj fenomenoj, larĝskale intervenas la hazardo. Tial por kelkaj algoritmoj la rezulto estu aŭ poste kontrolita. Male, la klasikaj algoritmoj estas entute determinismaj.

Konsekvence, la programado de algoritmoj (eĉ tiuj relative familiaraj en klasika informadiko) estas entute refarenda, cetere laŭ maniero pensi kaj labori tute novspeca.

Tamen, tri rimarkoj :

- . la plej granda parto de la informadiko (administrado de reto, prezentado de interfacio, tajpado de teksto, ...) preskaŭ certe restos klasika ;
- . post kelkaj jardekoj, estas verŝajne ke la kvantika informadiko enestos la privatajn klasikajn komputorojn de pli larĝa publiko, sed nur sub formo de help-procesoro sub-dediĉita al specifaj problemoj : optimizado, analizado, serĉo de solvoj, problemoj de kombinatoriko, eble iam lineara (aŭ nelineara) programado, ... ➡ Algoritmoj
- . momente, la kvantikaj algoritmoj povas funkcii per klasika komputoro (simulado), kaj tiel estos plu poste, almenaŭ por testi antaŭ ol disponigi ilin al uzantoj.

Ni ne forgesu ke la unuaranga (almenaŭ kronologie) fako interesata de la kvantikaj principoj estas la kriptografio (tiu ĉi fako meritis apartan terminaron). Efektive, la uzo de kvantikaj datumoj ne malebligas ties spionadon, sed eventuala spionado estos nerefuteble detektita pro la detruo de la informo vidate de la alsendito. Estas do kompreneble kial financado por esplorado en la fako kriptografio ŝprucis spontanee kaj frue.

Koncerne la disponeblan korpuson en Esperanto, la situacio estas krude simpla : neniuj spuro krom eventuale pri la prakuza « kvantuma meĥaniko ».

La uzeblaj korpuso de kvantika informadiko en aliaj lingvoj estas relative limigitaj. Da aĉeteblaj libroj komence de la jaro 2019, por studentoj aŭ interesatoj, estas deko en la angla, kvin en la franca, verŝajne samnombro en nur kelkaj aliaj lingvoj, do malmulte da. Cetere, la unuaj partoj (proks. triono) de tiuj libroj estas neeviteble dediĉitaj al denova prezento de la plej bazaj nocioj de la kvantuma fiziko (same kiel libro pri klasika informadiko prezentis, antaŭ kvindek jaroj, la funkciadon de la transistoroj aŭ eĉ la dopadon de la silicio !!). Krome, pri informadiko striktasence, ekfloras sur interreto pdf-aj dokumentoj redaktitaj de kompetentuloj (kursoj, disertaĵoj, memuaroj,...). Kelkaj filmetoj de prelegoj utile kompletigas la disponeblan korpuson.

Konstateblas relativa unueco pri la fakaj vortoj uzataj (kaj en la franca kaj en la angla). Pluraj disponeblaj libroj aŭ ret-dokumentoj proponas tradukon francan-anglan de tiuj ĉi vortoj kaj preskaŭ ĉiuj entenas utilan indkson.

La nombro de novaj vortoj necesaj por ĉi tiu fako estas relative malgranda. Dek unu novaj terminoj (plus unu pli specife matematika) estas proponataj, kaj kromaj difinoj de dek kvin aliaj jam PIV-aj (plus unu pli specife fizika) estas aldonitaj. Evidente tiu ĉi magra leksikono ne estas sufiĉa por fako kiu bezonas multajn esprimojn por pli ellaboritaj konceptoj (sama konstato en la angla kaj en la franca lingvoj). Tial sekvas listoj de komune uzataj sigloj, de komentoj aŭ precizigoj de vortoj aŭ esprimoj de matematiko kaj de fiziko, de konceptoj specife kvantikaj, de la bazaj operatoroj, de konataj algoritmoj.

Konkrete, la esenco de la utila esprim-materialo troviĝas en la rubriko « Principoj kaj konceptoj ».

Kelkaj vortoj havas en PIV tiel larĝan difinon ke modifo aŭ aldono ne estas bezonataj pro specifaj trajtoj de la kvantika fako. Tiel estas pri : *algoritmo*, *komputiko* kaj precipe pri *informadiko*.

Kiel eniri la leksikonon ?

La ĉi-posta leksikono provas kiel eble resti en la limigita perimetro de la kvantika informadiko. Tiel, la cetero de la kvantika komputiko (konstruado de komputoroj) ne estas enkalkulita. El la kvantuma fiziko estas prezentitaj nur principaj nocioj kun evidentaj konsekvencoj en informadiko.

La eniroj de la leksikono (laŭalfabeta) estas plurspecaj :

- . jam PIVaj terminoj al kiuj specifa kromsenko estas aldonita ;
- . jam PIVaj terminoj kies senco necesigas precizigajn komentojn rilate la kvantikon ;
- . kelkaj novaj terminoj (vinjeto ^{NPIV}) jam kutime uzataj de la profesiuloj.

Sekve utilajn nociojn (por ĉiuj el ili la ena ordo celas koheron laŭ sub-temoj) listigas :

- . sigloj,
- . specifaj matematikaj nocioj,
- . specifaj fizikaj scioj,
- . principoj kaj konceptoj,
- . operatoroj,
- . algoritmoj,
- . ekzemplo de programo,
- . komentoj pri la « informacio »,
- . apendico pri « utila formularo »,
- . apendico pri « bildoj de prototipaj komputoroj ».

Je ĉiu eniro estas (aŭ povas esti) prezentataj :

- . la vorto kaj la difino (respektive esprimo aŭ siglo kun eksplicitaĵo),
- . eventualaj derivaĵoj,
- . lingvaj komentoj (*lingv.*),
- . alternativaj proponoj (*alter.*) aŭ sinonimoj (*sin.*),
- . la vorto en la angla (*angl.*) kaj en la franca (*fr.*) lingvoj,
- . teknikaj aŭ teoriaj klarigoj (*klar.*),
- . notacio (*not.*) formulo (*form.*) ekzemplo (*ekz.*) matrico (*matr.*) demonstro (*dem.*),
- . principo (*princ.*) solvado (*solv.*),
- . kromaj rimarkoj (*rim.*) resendo al figuro (*fig.*).



Kvantika komputoro imagita de artisto.
El « *Pour la science* »

Leksikono

bit/o. **1.** Mezurunujo de informacio (de informo-kvanto) : *~o estas la oka baza mezurunuo de la internacia sistemo de unuoj.* **2.** Duuma memor-ĉelo de fizika sistemo (ekz. de komputoro). **3.** Averaĝa informokvanto provizita per legado de duuma memor-ĉelo. ➡ PIV
lingv. Etimologie *bit* estas la mallongigo de *binary digit* en la angla.
angl. bit / *fr.* bit

bra/o. ^{NPIV} **1.** Stat-vektoro konjugajo de keto. **2.** Notacia simbolo de $\sim$ o (laŭ Dirac).
lingv. bra estas la unua silabo de la angla vorto « bracket ». ➡ *braketo*
angl. bra / *fr.* bra
klar. Transponajo de la konjugajo de keto. ➡ *keto*
not. $\langle \psi |$ ($= |\psi^* \rangle^T$)

braket/o. ^{NPIV} **1.** Skalara produkto de brao kaj keto. **2.** Notacia simbolo de $\sim$ o (laŭ Dirac).
alt. brao-keto, hoko
lingv. La homonimeco kun « brak-et » ne ĝenas en la kunteksto.
angl. bracket (hoko), bra-ket / *fr.* braket
not. $\langle \psi | \phi \rangle$

degener/i. $\sim$ o **3.** Situacio kiam du aŭ pluraj eĝen-vektoroj de hermita operatoro (tipe de observeblo) havas saman eĝenon : *projekciatoro estas ĝenerale ~a.*
angl. quantum degeneracy / *fr.* dégénérescence quantique
ekz. La tripleto estas vektor-triopo kun la sama eĝeno (=1) de la 3D-operatoro-vektoro (spin-operatoro) laŭ la diagonalo de la spaca koordinataro *xyz*. ➡ Apendico pri « *utila formularo* »

init/i. (tr.) ^{NPIV} Meti sistemon aŭ variablon en staton adekvatan por ke programo aŭ algoritmo povu efektiviĝi.
lingv. Kvankam nePIVa tiu vorto jam enradikiĝis en informadiko.
angl. to initialize / *fr.* initialiser
rim. En klasika informadiko, inito efektive konsistas en dono de valoroj al kelkaj variabloj antaŭ ol komenci la funkciadon, sed en kvantika informadiko ĝi evidente havas pli gravan kaj definitivan rolon : preparo de la tuta kunteksto, t.e. de ĉiuj variabloj inkluzive de la pritraktotaj datumoj mem, ĉar neniu posta interveno ĝis la lego de la rezulto estas ebla.

intrik/i. (tr.) ^{NPIV} Fari ke la diversaj partoj de kvantika sistemo estu en reciproka dependeco.
 $\sim$ o. Ago $\sim$ i. **mal~i.** Detrui $\sim$ itan staton de sistemo per mezuro aŭ interago. **~iteco.** Mezurebla kvalito de kvantika sistemo esti $\sim$ ita. ➡ *koeficiento de korelacio*
alt. kuntriki, impliki (kroma senco, sed iom tro aparta)
angl. to entangle (v.) entanglement (subs.) / *fr.* intriquer (v.) intrication (subs.)
klar. Kiam mezuro de la unua kjubito de la intrikita sistemo $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ donas la valoron $|0\rangle$ (respektive $|1\rangle$), la dua kjubito ekde tiam valoras $|1\rangle$ (respektive $|0\rangle$), do ekde tiam (ekde la mezuro) la sistemo-stato estas $|01\rangle$ (respektive $|10\rangle$).

ket/o. ^{NPIV} **1.** Stat-vektoro de kvantika sistemo. **2.** Notacia simbolo de $\sim$ o (laŭ Dirac).

lingv. « ket » estas la dua silabo de la angla vorto « bracket ». ➡ *braketo*

angl. ket / *fr.* ket

klar. Matricoj de keto estas unukolumna. La koordinatoj (unu por ĉiu mezurebla valoro) estas kompleksaj nombroj kies moduloj estas la respektivaj kvadrataj radikoj de la probablecoj mezuri ĉi tiujn valorojn.

not. $|\psi\rangle$

kju/. ^{NPIV} **1.** Prefikso indikanta la kvantikan karakteron de io. Ekz : *kjubito*. **2.** $\sim$ -io = io kvantika :

kju-operatoro, kju-sistemo, kju-stato.

lingv. analoge al la anglalingva prononco, eĉ foje imitita de alilingvanoj.

alter. ku, kvantika. Ekz. *ku-bito, ku-operatoro* resp. *kvantika bito, kvantika operatoro*

angl. qu / *fr.* qu

kjubito/o. ^{NPIV} Elementa informero en kvantiko kun du bazaj valoroj. ➡ *bit/o* **2.**

angl. qubit aŭ qbit / *fr.* qu-bit

not. $|0\rangle$ aŭ $|1\rangle$ aŭ pli ĝenerale $\alpha|0\rangle + \beta|1\rangle$ kun $\alpha\alpha^* + \beta\beta^* = 1$

kjutrit/o. ^{NPIV} Elementa informero en kvantiko kun tri bazaj valoroj.

lingv. analoge al « kjubito »

angl. qutrit / *fr.* qu-trit

klar. Sistemo kun tri bazaj valoroj ne estas apriorie taŭga, nek facile uzebla.

not. $|0\rangle$, $|1\rangle$ ou $|2\rangle$ aŭ pli ĝenerale $\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ kun $\alpha\alpha^* + \beta\beta^* + \gamma\gamma^* = 1$

klon/i. **2.** Obligi kvantikan sistemon tiel ke ĉiuj $\sim$ aĵoj havu la samajn probablecojn de mezur-rezultoj. ➡ *kopi/i*

angl. to clone / *fr.* cloner

form. Por kjubito : $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$ estas la klon-paro de $\alpha|0\rangle + \beta|1\rangle$

rim. Klonado de kvantika sistemo estas neebla krom de eĝena stato. ➡ *teoremo de nekloneblo*

koher/i. mal~o. Stato de kjusistemo kiu perdis sian intrikitecon, kaj kies sub-sistemoj fariĝis sendependaj, sekve de interago kun ekstera sistemo.

angl. quantum decoherence / *fr.* décohérence

klar. Ekstera sistemo okaziganta malkoheron povas esti mezurilo. Ĉi-kaze la malkoherigo rilatas ne nur al la mezurita kju-bito, sed ankaŭ al iu alia kun-intrikita sub-sistemo (aliaj kju-bitoj). ➡ Algoritmoj ➡ Apendico pri la materialo

kolaps/o. **5.** Perdo de ĉiuj siaj kju-statoj krom de unu, pro interago kun ekstera sistemo (i.a. okaze de mezuro).

sin. disfalo, reduktiĝo de la ondo-funkcio

angl. collapse of the wave function / *fr.* effondrement de la fonction d'onde

komutator/o. **2.** Operatoro kiu kvantigas la nekomuteblon de observebloj per sia nenuleco.

angl. switch, commutator / *fr.* commutateur

not. $[A, B] = AB - BA$

rim. Komutatoro estas anti-hermita : $[A, B]^* = -[A, B]$, do $[A, B] = iC$ kun C hermita

kopi/i. **5.** Obligi kvantikan sistemon tiel ke ĉiuj $\sim$ aĵoj donu la samajn rezultojn sekve de mezuro.

➡ *klon/i*

form. Por kjubito : $\alpha|00\rangle + \beta|11\rangle$ estas la kopi-rezulto de $\alpha|0\rangle + \beta|1\rangle$

angl. to copy, to duplicate / *fr.* recopier, dupliquer

- kvantik/o.** ^{NPIV} 1. Informo-teorio konstruita el kvantumaj fenomenoj (kvantuma mekaniko).
 2. Scienco por ellaborado de novaj komputiko, informadiko kaj kriptografio surbaze de ~aj principoj. ~a. rilata al ~o : ~a *algoritmo*
angl. quantum / *fr.* quantique
- mezur/o.** 12. Operacio sur keto, kies rezulto estas eĝeno de observeblo. ➡ *redukt/iĝo* 4.
 13. Valoro rezultanta de la ~o, t.e. la eĝeno de tiu nova stato.
angl. measure / *fr.* mesure
rim. 1. Paradokse, kvantika mezuro preskaŭ neniam (krom kaze de eĝena stato) informas pri la stato de la sistemo antaŭ la mezuro. Eĉ plie, mezuro neinversigeble detruas la staton mezuratan. 2. Du sinsekvaj mezuroj estas komuteblaj nur se ili havas komunajn eĝen-vektorojn. ➡ *komutator/o* 2.
- observ/i.** ~**ebl/o.** Abstrakta kju-operatoro kies eĝenoj estas la mezureblaj valoroj de fizika grando.
alt. mezureblo.
angl. observable / *fr.* observable
klar. Observeblo estas hermita do ĝiaj eĝenoj estas reelaj.
- orakol/o.** 3. Kvantika skatolo entenanta sinsekvon de pordoj agantaj sur intrikita sistemo ĝis disponigo de la rezulto.
angl. oracle / *fr.* oracle
klar. Laŭ tre ĝenerala skemo, orakolo funkcias per du variabloj. La unua (x) reprezentas samtempe ĉiujn eblajn binarajn rezultojn (inite produkto-stato : $H|0\rangle^{\otimes n} = \frac{1}{\sqrt{n}}(|0\rangle + |1\rangle)^{\otimes n}$), kaj disponigas la finan rezulton. La dua (inite produkto-stato : $y = H|1\rangle^{\otimes n} = \frac{1}{\sqrt{n}}(|0\rangle - |1\rangle)^{\otimes n}$) estas kombinita kun la kunteksta informacio $f(x)$ (funkcio de x). Tiel ambaŭ sub-sistemoj estas implice kun-intrikitaj. ➡ Algoritmoj
form. $U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$
- plet/.** ^{NPIV} Sufikso montranta la degeneron de eĝeno kaj uzata por derivi el numeralo substantivon signifantan « la aro da eĝenaj vektoroj kun la sama eĝeno ». Ekz : *unuplet*o, *triplet*o.
 ➡ *triplet*o, *singuleto*
lingv. La homonimeco kun « plet » ^{PIV} ne ĝenas en la kunteksto.
- pord/o.** 4. Kvantika unumodula operatoro kiu modifas la staton de sistemo en la spaco de Hilbert : *pordo Hadamard*.
angl. gate / *fr.* porte
klar. Pordo ne modifas la modulon de la stat-vektoro, sed ne ĉiam estas hermita. ➡ *logika kjuoperatoro*
- projekciatoro.** 2. Hermita operatoro kies rezulto estas la komponanto de vektoro sur specifa bazelemento.
angl. projection operator / *fr.* projecteur
rim. Alprojekciebla baz-vektoro estas eĝena vektoro de la projekciatoro kun eĝeno 1, dum la aliaj baz-vektoroj estas eĝenaj vektoroj kun eĝeno 0.
- pur/a.** 6. Tia, ke kono de ĝia stato necesigas nenian konon de alia sistemo. **ne~a.** Tia, ke ĝia stato ne estas aparte konebla kaj difinebla.
angl. pure / *fr.* pur
klar. Sistemo nepura estas pli-malpli intrikita kun alia sistemo, aŭ konebla nur stokaste. ➡ *pura stato*

singulet/o. 2. Keto de la duelementa stato maksimume intrikita, kaj estanta la ejgena vektoro (ejgeno = -3) de la 3D-operatoro-vektoro (spin-operatoro) laŭ la diagonalo de la spaca koordinataro *xyz*. ➡ *tripleto*

alt. unupleto.

angl. singlet state / *fr.* singulet

klar. Singuleto estas unu el la kvar statoj de Bell.

form. $|Sing\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

redukt/i. ~iĝo 4. Modifiĝo de kvantika stato sekve de mezuro. ➡ *mezur/o 12.*

alter. disfalo, kolapso

angl. (wave function) collapse / *fr.* réduction / effondrement (de la fonction d'onde)

triplet/o. ^{NPIV} Unu el la tri ketoj de la duelementaj statoj maksimume intrikitaj, kaj estantaj la ejgenaj vektoroj (ejgeno = 1) de la 3D-operatoro-vektoro (spin-operatoro) laŭ la diagonalo de la spaca koordinataro *xyz*. ➡ *plet, singuleto 2.*

angl. triplet state / *fr.* triplet

klar. Tripletoj estas tri el la kvar statoj de Bell.

form. $|T_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ $|T_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ $|T_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

Sigloj

PKP : Probableca Komplekseco en Polinoma tempo

angl. BPP bounded-error probabilistic polynomial time / *fr.* complexité probabiliste en temps polynomial

klar. Kategorio de probablecaj problemoj solveblaj en polinoma tempo kun maksimuma probableco de eraro je 25%.

KKP : Kvantika Komplekseco en Polinoma tempo

angl. BQP bounded-error quantum polynomial time / *fr.* complexité quantique en temps polynomial

klar. Kategorio de problemoj kvantike solveblaj en polinoma tempo kun maksimuma probableco de eraro je 25%.

KAOK : Kompleta Aro da Observebloj Komuteblaj

angl. CSCO (Complete Set of Commuting Observables) / *fr.* ECOC (Ensemble Complet d'Observables Commutantes)

klar. $\forall (A, B) \in KAOK \quad [A, B] = \hat{0}$. La bazo de komunaj ejgen-vektoroj kaj la mezuroj ne perturbas sin reciproke. Tiujn ĉi eblas efektivigi sammomente laŭ maniero infinite preciza, kaj la observeblojn (mezurojn) oni asertas kongruaj. ➡ *kongruaj observebloj*

MNB / MUB : Maksimume Nekongruaj Bazoj

angl. MUB (Mutually Unbiased Bases) / *fr.* Bases mutuellement non biaisées, maximalement incompatibles, maximalement décorrélées ➡ *maksimume nekongruaj bazoj*

POVM : Operatoro kun Pozitivaj Mezuritaj Valoroj (Pozitiva Operatoro)

angl. Positive Operator Valued Measure / *fr.* Opérateur à Valeurs Mesurées Positives (Opérateur Positif)

klar. La ejgenoj de Pozitiva Operatoro estas pozitivaj.

ekz. Operatoro de denseco, malforta mezuro

EPR : Einstein, Podolsky, Rosen. ➡ *paradokso EPR*

GRW : G.C. Ghirardi, A.Rimini, T.Weber ➡ *paradokso EPR*

TUM : Teorio pri Universo-Multopo ➡ *paradokso EPR*

angl. Multiple observer theory, Many-minds theory / *fr.* Interprétation des mondes multiples (IMM), des Multivers, Théorie des états relatifs, Théorie des observateurs multiples

Specifaj matematikaj nocioj

ejgeno : ➡ PIV

angl. eigenvalue / *fr.* valeur propre

rim. En kvantiko, ejgeno povas escept-okaze esti kompleksa nombro kiam la operatoro ne estas hermita. ➡ *pordo cPHASE*

ejgena vektoro : Vektoro rilatanta al ejgeno.

alt. ejgen-vektoro

angl. eigenvector / *fr.* vecteur propre

ejgena spaco : Aro da ejgen-vektoroj, plus la nulo-vektoro.

angl. eigenspace / *fr.* espace propre

hermita operatoro : Kies matrico egalas la transponaĵon de sia konjugajo.

angl. Hermitian operator / *fr.* opérateur hermitien / hermitique

klar. La ejgenoj (do ankaŭ la spuro) de hermita operatoro estas reelaj.

rim. En kvantiko, la hermitaj operatoroj (type observebloj) estas aplikataj al la stat-vektoroj de fizikaj grandoj.

unumodula operatoro : Kiu ne modifas la modulon de vektoro.

sin. unita operatoro

angl. unitary operator / *fr.* opérateur unitaire

rim. **1.** Produkto de unumodula operatoro per la transponaĵo de ĝia konjugajo estas egala al la idento-operatoro ($U^{*T}U = I$). **2.** La determinanto de U egalas al $e^{i\alpha}$ kun $\alpha \in R$ **3.** En kvantiko, la unumodulaj operatoroj (type pordo / logika operatoro) estas uzataj por ŝanĝo de stato.

projekcia operatoro : Projekciatoro. ➡ *projekciatoro 2.*

angl. projection operator / *fr.* opérateur de projection, projecteur

rim. **1.** En kvantiko, la alprojekciatan bazon konsistigas la ejgenaj vektoroj ($P_i = |e_i\rangle\langle e_i|$).

2. $P = |\psi\rangle\langle\psi|$ estas la projekciatoro sur $|\psi\rangle$.

tensora produkto : ➡ PIV produkto / **tensora ~o**

angl. tensor product / *fr.* produit tensoriel

klar. La dimensio de la produkto de du vektoraj spacoj (je respektivaj dimensioj n kaj m) egalas al nm .

not. $\otimes$ Se A kaj B estas operatoroj, a kaj b vektoroj : $(A \otimes B)(a \otimes b) = (Aa \otimes Bb)$. Praktike, oni uzas unu el la pli simplaj formoj : $(A \otimes B)|ab\rangle = |AaBb\rangle = (A|a\rangle)(B|b\rangle)$

interna produkto : ➡ PIV produkto / **interna ~o**

angl. inner product / *fr.* produit intérieur

sin. skalara produkto

klar. Produkto de linia matrico per kolumna matrico estas kompleksa nombro.

not. $\langle\psi|\phi\rangle$ kaj $\langle\psi|\psi\rangle = \langle\psi|$

rim. **1.** $\langle\psi|\psi\rangle = \|\psi\|^2$ **2.** $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

ekstera produkto : Produto de keto per brao.

angl. outer product / *fr.* produit extérieur

klar. Produto de kolumna matrico per linia matrico estas kvadrata matrico (kun kompleksaj nombroj).

not. $|\psi\rangle\langle\phi|$

spuro : ➡ PIV ~o 3. Sumo de la ejgenoj de operatoro.

angl. trace / *fr.* trace

rim. La spuro de matrico ne dependas de la vektorbazo.

parta spuro de A : Operatoro kies matrico-membroj estas la redukto laŭ B de la tensor-produkta matrico AB . ➡ *matrico de denseco*

sin. parta operatoro

angl. partial trace / *fr.* trace partielle

form. $\rho_A = Tr_B(\rho_{AB}) = \sum_B \langle i_B | \rho_{AB} | i_B \rangle = \langle 0_B | \rho_{AB} | 0_B \rangle + \langle 1_B | \rho_{AB} | 1_B \rangle$ (kaze de kju bitoj A kaj B)

rim. Parta spuro ne estas nombro sed operatoro. Tamen, la vorto « spuro » estas pravigebla

jene : $Tr(\rho_{AB}) = Tr_A(Tr_B(\rho_{AB})) = Tr_B(Tr_A(\rho_{AB}))$

$$\text{ekz. } |\psi\rangle = \sqrt{0,6}|ud\rangle - \sqrt{0,4}|du\rangle \quad \rho_{AB} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0,6 & -\sqrt{0,24} & 0 \\ 0 & -\sqrt{0,24} & 0,4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rho_A = Tr_B(\rho_{AB}) = \begin{pmatrix} 0,6 & 0 \\ 0 & 0,4 \end{pmatrix} \quad \rho_B = Tr_A(\rho_{AB}) = \begin{pmatrix} 0,4 & 0 \\ 0 & 0,6 \end{pmatrix} \quad Tr(\rho_{AB}) = Tr(\rho_A) = Tr(\rho_B) = 1$$

➡ aliaj ekzemploj apendice

kvaterniono : kvardimensia hiperkompleksa nombro kies formo estas $a+bi+cj+dk$ kun $i^2=j^2=k^2=ijk=-1$.

angl. quaternion / *fr.* quaternion

rim. **1.** La multiplikado de kvaternionoj ne estas komutativa (interalie : $(ijk)^2 = 1 \neq i^2 j^2 k^2 = -1$). **2.** Pli ĝenerale, la spaco de la kvaternionoj estas tre simila al tiu de la matricoj de Pauli plus la matrico identeco (pri kiuj : $(\sigma_x \sigma_y \sigma_z)^2 = -I \neq \sigma_x^2 \sigma_y^2 \sigma_z^2 = I$)

➡ *matricoj de Pauli*

Specifaj fizikaj nocioj

spino : ➡ PIV

angl. spin / *fr.* spin

rim. La spino (en rilato kun momanto de elektrono) estas unu el la plej konataj rimedoj por fari kju-bitojn. ➡ *sfero de Bloch, operatoro-vektoro-3D, matricoj de Pauli*

polarizo : ➡ PIV

angl. polarization / *fr.* polarisation

rim. La polarizo (de fotono) estas rimedo por fari kju-bitojn (*horizontala, vertikala*).

not. $|\leftrightarrow\rangle$ kun la ejgeno -1, $|\updownarrow\rangle$ kun la ejgeno 1

koloro : ➡ PIV ~ 7.

angl. color / *fr.* couleur

rim. La koloro (de kvarko aŭ de gluono) estus rimedo por fari kju-tritojn (*ruĝa, blua, verda*).

saporo : 2. Kvantika karakterizo de kvarkoj kaj de leptonoj kun kvar eigenaj statoj (nomataj *strango, ĉarmo, belo, vero*)

angl. flavor / *fr.* saveur

ondo-funkcio : Esprimo de kvantika stato kiam la nombro da mezureblaj valoroj (ejgenoj) estas nefinia, do same la dimensio de la spaco de Hilbert estas nefinia.

angl. wave function / *fr.* fonction d'onde

$$\text{form. } \psi(x) = \int_{-\infty}^{+\infty} \psi(y) \delta(x-y) dy = \langle x | \psi \rangle = \int_{-\infty}^{+\infty} \langle y | \psi \rangle \langle x | y \rangle dy = \langle x | \left(\int_{-\infty}^{+\infty} |y\rangle \langle y| dy \right) | \psi \rangle$$

$$\text{kun : } \langle \psi | \psi \rangle = \int_{-\infty}^{+\infty} \psi^*(x) \psi(x) dx = 1$$

$$|\psi\rangle = \int_{-\infty}^{+\infty} \langle x | \psi \rangle |x\rangle dx \quad x \text{ reprezentas la ejgenojn, } |x\rangle \text{ la ejgenajn vektorojn}$$

hamiltoniano : Operatoro kiu esprimas la evoluon de kvantika stato laŭ la tempo (ekvacio de Schrödinger laŭ la tempo). ➡ *ekvacio de Schrödinger dependa de la tempo*

angl. Hamiltonian / *fr.* hamiltonien

$$\text{form. } H|\psi\rangle = i\hbar \frac{d\psi}{dt} = i\hbar \frac{d}{dt}|\psi\rangle$$

ekvacio de Schrödinger dependa de la tempo : Ekvacio de Schrödinger por simpla partiklo libera, sen konsidero de la relativecaj efikoj.

angl. time-dependent Schrödinger equation / *fr.* équation de Schrödinger dépendante du temps

$$\text{form. } H|\psi\rangle = i\hbar \frac{\partial \psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m} \cdot \frac{\partial^2 \psi(x,t)}{\partial x^2}$$

ekvacio de Schrödinger sendependa de la tempo : Ekvacio de la eĝenoj kaj eĝenaj vektoroj de la hamiltoniano.

angl. Schrödinger equation independent of time / *fr.* équation de Schrödinger indépendante du temps

$$\text{form. } H|\psi\rangle = E|\psi\rangle = -\frac{\hbar^2}{2m} \cdot \frac{\partial^2 \psi(x, t=0)}{\partial x^2} \quad E \text{ (energio) estas eĝeno de } H$$

$$E\psi(x) = -\frac{\hbar^2}{2m} \cdot \frac{\partial^2 \psi(x)}{\partial x^2}$$

evoluo de observeblo laŭ la tempo : Ekvacio kiu rilatigas la derivaĵon laŭ la tempo de la mezvaloro de la mezuroj de observeblo L , kun la mezvaloro de la komutatoro $[H, L]$.

$$\text{form. } \frac{d}{dt}\langle L \rangle = \frac{i}{\hbar} \langle [H, L] \rangle$$

dem.

$$\begin{aligned} \frac{d}{dt}\langle \psi(t) | L | \psi(t) \rangle &= \left\langle \frac{d}{dt} \psi(t) \right| L | \psi(t) \rangle + \langle \psi(t) | L \left| \frac{d}{dt} \psi(t) \right\rangle = \frac{i}{\hbar} \langle \psi(t) | HL | \psi(t) \rangle - \frac{i}{\hbar} \langle \psi(t) | LH | \psi(t) \rangle \\ \langle \psi(t) | \frac{d}{dt} L | \psi(t) \rangle &= \frac{i}{\hbar} \langle \psi(t) | [HL - LH] | \psi(t) \rangle = \frac{i}{\hbar} \langle \psi(t) | [H, L] | \psi(t) \rangle \end{aligned}$$

klar. Laŭ la prezento de Heisenberg, la stat-vektoro ne dependas de la tempo, sed la observeblo evoluas laŭ la tempo. Male, Schrödinger opiniis ke la stat-vektoro evoluas laŭ la tempo. Ili kompreneble ambaŭ pravis.

principo de necerteco de Heisenberg : La produkto de la mezaj devioj de la spaco-situo kaj de la movo-kvanto de partiklo estas supera ol la duono de la konstanto de Planck ($\hbar$). ➡ *meza devio, komutatoro*

angl. Heisenberg's uncertainty principle / *fr.* principe d'incertitude de Heisenberg

sin. Rilato de nedetermineblo de Heisenberg (*angl.* Heisenberg uncertainty relation / *fr.* relation d'indétermination de Heisenberg)

klar. Pli ĝenerale :

$$\begin{aligned} \text{Neegalajo de Cauchy-Schwarz : } \quad & 2|X||Y| \geq |\langle X | Y \rangle + \langle Y | X \rangle| \\ & 2|A|\psi\rangle||B|\psi\rangle| \geq |\langle \psi | AB | \psi \rangle - \langle \psi | BA | \psi \rangle| \\ & 2\sqrt{\langle A^2 \rangle \langle B^2 \rangle} \geq |\langle \psi | [A, B] | \psi \rangle| \\ \text{Neegalajo de Heisenberg : } \quad & \Delta A \Delta B \geq \frac{1}{2} |\langle \psi | [A, B] | \psi \rangle| = \frac{1}{2} |\langle \psi | iC | \psi \rangle| = \frac{\langle C \rangle}{2} \\ \text{Pri la loko kaj la movo-kvanto : } \quad & \Delta x \Delta p \geq \frac{\hbar}{2} \end{aligned}$$

nelokeco : Kiam du sistemoj estas intrikitaj, mezuro de unu el ili fiksas la staton de ambaŭ ĝuste en la sama momento, sendepende de la distanco inter ili (eventuale tiel granda, ke eĉ la lumo ne estus sufiĉe rapida por pravigi tian fakton). ➡ *paradokso EPR*

angl. nonlocality / *fr.* non-localité

rim. La nelokeco estas pli utila en kvantika kriptografio ol en kvantika informadiko. Ĝi ebligas sendon de informo al malproksima korespondanto sen risko de spionado (eventuala spionado detruus la informon, do estus sammomente sciata ĉu de la sendinto ĉu de la alsendito).

paradokso EPR : Einstein, Podolsky kaj Rosen malakceptis la nelokecon de la intrikiteco, asertante ke sistemo povas interagi nur kun sia proksima medio, krom enkonduki « kaŝitan variablon » kiun kunportus kun si ambaŭ sistemoj momente de la intrikado. Laŭ tiu vidpunkto, la rezulto de eventuala parta mezuro estus konata antaŭ la malproksimiĝo.

angl. EPR paradox / *fr.* paradoxe EPR

klar. La neekziston de kaŝita variablo eksperimente demonstris Alain Aspect en 1981, kaj definitive Marissa Giustina kaj Lynden K. Shalm en 2015.

rim. Aliaj proponis alternativajn klarigojn. Ĉiu el tiuj ĉi siaflanke alportas « sufiĉan » pravigon de la nelokeco, neniigante la paradokson EPR : **1.** GRW : anstataŭigante la ekvacion de Schrödinger per ekvacio nelineara. **2.** TUM / IMM : asertante pri kunekzistantaj mondoj, inter kiuj nur unu riviĝus al nia percepto okaze de mezuro (teorio de Hugh Everett). **3.** BOHM : konjektante ke la spacaj koordinatoj mem estas la kaŝitaj variabloj.

Principioj kaj konceptoj

kvantika informadiko : Scienco pri traktado de informo (informacio) laŭ principoj de la kvantuma fiziko.

angl. quantum computing / *fr.* informatique quantique

rim. Kvantika informadiko iam funkcios per komputoroj apriorie kvantikaj, sed tio ne estas absolute necesa. La klasikaj komputoroj ja povas simuli la tipe kvantikajn algoritmojn.

notacio de Dirac : Tuto de la simboloj uzataj por identigi la kvantikajn stat-vektorojn (kun kompleksaj koordinatoj) kaj por esprimi iliajn produktojn.

not. $|\psi\rangle$ $\langle\psi|$ $\langle\psi|\phi\rangle$ $\langle\psi|$ $|\psi\rangle\langle\psi|$ $\langle\psi|A|\psi\rangle$

kvantika stato : Stato de sistemo kies mezuro povas doni plurajn rezultojn kun specifaj probablecoj. La diversaj probablecoj difinas la staton.

angl. quantum state / *fr.* état quantique

rim. $|\psi\rangle$, $-2|\psi\rangle$, kaj $e^{-3i}|\psi\rangle$ rilatas al la sama kvantika stato.

dustata sistemo : Sistemo kies mezuro povas doni du rezultojn (du eĝenojn).

angl. two-level system / *fr.* système à deux états

ekz. $|0\rangle$, $|1\rangle$ $|+\rangle$, $|-\rangle$ $|bilde\rangle$, $|reverse\rangle$ $|vera\rangle$, $|malvera\rangle$

supermeto de statoj : Kvantika stato kies mezuro povas rezultigi plurajn valorojn.

sin. plurstateco

angl. quantum superposition / *fr.* superposition d'états

ekz. $\alpha|0\rangle + \beta|1\rangle$ $\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$

$\alpha_1|trefo\rangle + \alpha_2|karoo\rangle + \alpha_3|kero\rangle + \alpha_4|piko\rangle$

rim. **1.** Principe, en la ĉi-antaŭaj ekzemploj $\alpha^2 + \beta^2$ kaj resp. $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = 1$ **2.** Cetere, α^2 kaj β^2 estas la probablecoj mezuri resp. $|0\rangle$ kaj $|1\rangle$ (same pri $\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2$).

kato de Schrödinger : Alegoria figuro pri dustateco de kvantika sistemo, laŭ kiu kato povas esti kaj vivanta kaj mortinta.

angl. Schrödinger's cat / *fr.* chat de Schrödinger

klar. Dustateco de sistemo povas ekzisti je la skalo de la partikloj, eventuale de la atomoj, sed ne je la skalo de la hejma feliso.

form. $|\psi_{kato}\rangle = \alpha_1|vivanta\rangle + \alpha_2|senviva\rangle$

teoremo pri nekloneblo : Vortigo : « Ne ekzistas operatoro kapabla kloni iun ajn kju-biton ».

angl. nocloning theorem / *fr.* théorème de non-clonage

klar. Praktike, nur eĝenan vektoron eblas kloni.

dem. Se ekzistus tia operatoro U , klono de $|\psi\rangle$ implicas $U(|\psi\rangle \otimes |b\rangle) = |\psi\rangle |\psi\rangle$, kaj klono de $|\phi\rangle$ implicas $U(|\phi\rangle \otimes |b\rangle) = |\phi\rangle |\phi\rangle$.

La skalara produkto de ambaŭ ketoj donas : $\langle\phi|\langle b|U^+U|\psi\rangle|b\rangle = \langle\phi|\langle\phi||\psi\rangle|b\rangle$

do $\langle\phi|\langle b|U^+U|\psi\rangle|b\rangle = \langle\phi|\langle b||\psi\rangle|b\rangle = \langle\phi|\psi\rangle\langle b|b\rangle = \langle\phi|\psi\rangle = \langle\phi|\langle\phi||\psi\rangle|b\rangle = \langle\phi\phi||\psi\psi\rangle = (\langle\phi|\psi\rangle)^2$

do $\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$, do $\langle\phi|\psi\rangle = 0$ aŭ $\langle\phi|\psi\rangle = 1$, do $|\phi\rangle$ kaj $|\psi\rangle$ estas ĉu egalaj ĉu ortaj.

Ĉar estas facile prui ke eĝenaj vektoroj estas kloneblaj, ili do ambaŭ ($|\phi\rangle$ kaj $|\psi\rangle$) estas eĝenaj.

rim. **1.** La teoremo de nekloneblo tute ne signifas ke kju-bito ne estas kopiebla. Ĝi signifas ke ne el ĉiuj vektoroj $\alpha|0\rangle + \beta|1\rangle$ eblas fari $(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$. Sed ĉiam eblas la faro de $\alpha|00\rangle + \beta|11\rangle$ (du logikaj kjubitoj el la sama fizika kju-bito. ➡ *logikaj kjubitoj*). La unua estas produto-stato (eventuale eĝena) de kjubito per si mem, la dua estas intrikita stato (krom se la deirpunkta kjubito estas eĝena), do ĉikaze la du kjubitoj plu restas dependaj. **2.** Okaze de mezuro, la valoro de logikaj kjubitoj estas nepre identaj, sed la mezuro de klon-paro (se klonado estus ebla) donus rezultojn sendependajn (do ne ĉiam identajn krom okaze de eĝena stato). ➡ Algoritmoj (korektado de transsendo-eraroj).

vektoro de Bloch : Vektoro en la spaco de Hilbert, kiu identigas la kvantikan staton de kju-bito, do kiu estas prezentebla sur la sfero de Bloch.

angl. Bloch-vector / *fr.* vecteur de Bloch

klar. La du bazaj vektoroj $|0\rangle$ aŭ $|1\rangle$ kun kompleksaj koordinatoj disponigas apriorie kvar dimensiojn. Sed praktike, la modulo de vektoro valoras unu, kaj la fazo (δ) estas neefika (ĉiuj ĝiaj valoroj respondas al la sama kvantika stato). Do kjubito estas dudimensia : 2×2 .

$$\text{form. } |\psi\rangle = e^{i\delta} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad \text{do} \quad |\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad \forall \delta$$

rim. Tradicie, $\delta=0$ do $e^{i\delta}=1$, do la koordinato de $|\psi\rangle$ laŭ $|0\rangle$ estas reela.

stat-vektoro : Vektoro de la tensora spaco de Hilbert, kiu identigas la kvantikan staton de sistemo.

angl. quantum state vector / *fr.* vecteur-état

klar. Kiam sistemo konsistas en n kjubitoj, la disponebla dimensio estas $4^n - 2$, dum la simpla tensora produto supozigus nur 2^n (inkluzive de priskribo de intrikitaj statoj). La diferenco estas uzata por priskribi diversmaniere la saman kvantikan staton de kju-bito (ekz. spino en la tridimensia spaco), tiel konservante « eksteran informon » kiu koncernas alian 3D-operatoron-vektoron. Ekzemple : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ kaj $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ donas statistike samajn rezultojn de mezuro laŭ z , sed ne laŭ la aliaj direktoj x kaj y . ➡ *sfero de Bloch*

meza valoro : Meznombro de rezultoj okaze de mezuroj de keto $|\psi\rangle$ laŭ observeblo A .

sin. mezvaloro, ekspekto

angl. expectation value / *fr.* valeur moyenne, espérance

klar. La pluralo « mezuroj » en la difino estas kompreneble fiktivaĵo (krom disponi samplon da ketoj, ĉiuj en la sama pura stato), ĉar la unua mezuro detruus la kju-staton neinvertigeble.

$$\text{form. } \langle A \rangle_{|\psi\rangle} = \sum_{n=1}^N a_n p_{|\psi\rangle}(a_n) = \langle \psi | A | \psi \rangle$$

meza devio : Meznombro de devio disde la mezvaloro okaze de mezuroj de keto $|\psi\rangle$ laŭ observeblo A .

sin. kvadrata radiko de la varianco

angl. standard deviation / *fr.* écart quadratique moyen, écart type

$$\text{form. } \Delta A = \langle A - \langle A \rangle_{|\psi\rangle} \rangle_{|\psi\rangle}$$

$$\text{rim. } \Delta A = \sqrt{\langle A^2 \rangle_{|\psi\rangle} - \langle A \rangle_{|\psi\rangle}^2}$$

pura stato : Kvantika stato perfekte difinita pro la konateco de siaj koordinatoj en la eĝena bazo.

angl. pure state / *fr.* état pur

klar. **1.** Pura stato (male al stokasta mikso) estas entute determinisma, kvankam ĉiu perfekte konata koordinato estas la (kvadrata radiko de) probableco de la koncernata eĝena valoro okaze de mezuro. Pura stato estas preciza stato (eĉ se ne eĝena). Stokasta mikso de statoj estas aleatora. **2.** Sistemo el du subsistemoj intrikitaj estas en pura stato, sed la statoj de la subsistemoj ne estas puraj ĉar ne individue difinitaj. **3.** Pli ĝenerale, pura stato estas sistemo kies entuta difino kaj kono ne dependas de ekstera sistemo kun kiu ĝi estus pli-malpli intrikita. ➡ *matrico de denseco*

form. $|\psi\rangle = \sum_{i=1}^n \alpha_i |e_i\rangle$ $|e_i\rangle$ estas la eĝenaj vektoroj (praktike ankaŭ la uzataj bazvektoroj).

stokasta mikso : Kvantika stato ne difinita pro la aleatoreco de siaj koordinatoj en la eĝena bazo.

sin. nekohera supermeto de statoj

angl. statistical mixture / *fr.* mélange statistique

klar. Stokasta mikso (male al pura stato) estas aleatora. Ne ĉiuj koordinatoj estas precize konataj.

form. La sistemo estas en la pura stato $|\psi_i\rangle$ kun la probableco p_i

pureco de stato : Nombro inter $1/n$ kaj 1 (kun n eĝenaj vektoroj), kiu taksas la purecon de kvantika sistemo.

angl. purity of state / *fr.* pureté d'un état quantique

form. Pureco : $P = \text{Tr}(\rho^2)$ $P=1$, se la sistemo estas pura, $P=1/n$, se la sistemo estas nepura (stokasta mikso aŭ elemento intrikita kun alia).

eĝena stato : Stato kies mezuro donas ununuran rezulton (eĝenon) kun probableco unu.

angl. eigenstate / *fr.* état propre

klar. Krom precizigo de alia direkto, por binara elemento, konvencie temas pri mezuro laŭ la direkto z .

<i>not.</i>	$ 0\rangle, 1\rangle$	aŭ $ u\rangle, d\rangle$	laŭ z	(up / down en la angla)
	$ +\rangle, -\rangle$	aŭ $ r\rangle, l\rangle$	laŭ x	(right / left en la angla)
	$ +i\rangle, -i\rangle$	aŭ $ i\rangle, o\rangle$	laŭ y	(in / out en la angla)

plurelementa stato : Kvantika stato de sistemo kun minimume du subsistemoj.

angl. composite state / *fr.* état composite, état combiné

klar. La stato de la sistemo estas la tensora produto de la statoj de la subsistemoj.

produto-stato : Plurelementa stato de subsistemoj sendependaj.

angl. product state / *fr.* état-produit

klar. **1.** La stato povas esti formulata per tensora produto de la keto de la unua subsistemo kaj de la keto de la dua. Mezuro de unu subsistemo ne ŝanĝas la staton de la alia. **2.** La stato de la sistemo estas konata nur ĉar la statoj de la subsistemoj estas aparte konataj.

form. $\alpha_1\beta_1|00\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle + \alpha_2\beta_2|11\rangle = (\alpha_1|0\rangle + \alpha_2|1\rangle) \otimes (\beta_1|0\rangle + \beta_2|1\rangle)$

ekz. $|01\rangle = |0\rangle \otimes |1\rangle$ $\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$

$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

intrikita stato : Plurelementa stato de subsistemoj pli-malpli dependaj.

angl. entangled state / *fr.* état intriqué

klar. **1.** La stato ne povas esti formulata per tensora produto de la keto de la unua subsistemo kaj de la keto de la dua. Mezuro de unu subsistemo ŝanĝas la staton de la alia. **2.** La stato de la sistemo estas konata sed ne la statoj de la subsistemoj.

ekz. stato maksimume intrikita : $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ $\frac{1}{\sqrt{2}}(|01\rangle + i|10\rangle)$

stato parte intrikita : $\frac{1}{2}|01\rangle + \frac{\sqrt{3}}{2}|10\rangle$ $\frac{\sqrt{2}}{2}|00\rangle + i\frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle$ $\frac{1}{4}|01\rangle + i\frac{\sqrt{15}}{4}|10\rangle$

stato ne intrikita : $\frac{\sqrt{3}}{2}|10\rangle + \frac{1}{2}|11\rangle$ $\frac{1}{4}|00\rangle + i\frac{\sqrt{15}}{4}|10\rangle$ $\leftarrow$ *produto-stato*

statoj de Bell : La singuleto kaj la tripleto (do kvar statoj entute).

angl. Bell's states / *fr.* états de Bell

spaco de Hilbert : **1.** Abstrakta vektor-spaco kun kompleksaj koordinatoj, kies bazvektoroj identigas la diversajn mezureblajn valorojn de kvantika sistemo. **2.** Tensora produto de la spacoj de Hilbert de la pli-malpli intrikitaj sub-sistemoj.

angl. Hilbert space / *fr.* espace de Hilbert

ekz. de bazoj :

difino 1 : $|0\rangle, |1\rangle$ spino mezurata laŭ z , $|+\rangle, |-\rangle$ spino mezurata laŭ x

difino 1 : $|r\rangle, |b\rangle, |v\rangle$ kju-trito

difino 2 : $(|0\rangle, |1\rangle) \otimes (|+\rangle, |-\rangle) = |0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle$

difino 2 : $(|0\rangle, |1\rangle) \otimes (|r\rangle, |b\rangle, |v\rangle) = |0r\rangle, |0b\rangle, |0v\rangle, |1r\rangle, |1b\rangle, |1v\rangle$

koeficiento de korelacio : Mezvaloro de du-kjubita sistemo minus la produto de la individuaj mezvaloroj de la kju-bitoj.

angl. correlation coefficient / *fr.* coefficient de corrélation

klar. La koeficiento karakterizas la nivelon de intrikiteco (inter -1 kaj 1). Ĝi estas nula kiam la du kju-bitoj estas sendependaj. Ĝi valoras 1 aŭ -1 je maksimuma intrikiteco.

form. $kor(A, B) = \langle \sigma_A \sigma_B \rangle - \langle \sigma_A \rangle \langle \sigma_B \rangle$

rim. Tiuj ĉi pentraĵoj de V.Kandinsky estas ofte konsiderataj kiel alegorioj de la kvantuma mondo :



Vassily Kandinsky (1940) Ĉiela bluo
Sendependeco de sistemoj
(produto-stato)



Vassily Kandinsky (1939) Komponaĵo X
Intrikiteco de sistemoj
(intrikita stato)

sfero de Bloch : Matematika prezento de la kvantika stato de kubitito en la reala tridimensia spaco.

angl. Bloch sphere / *fr.* sphère de Bloch

$$\text{form. } |\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

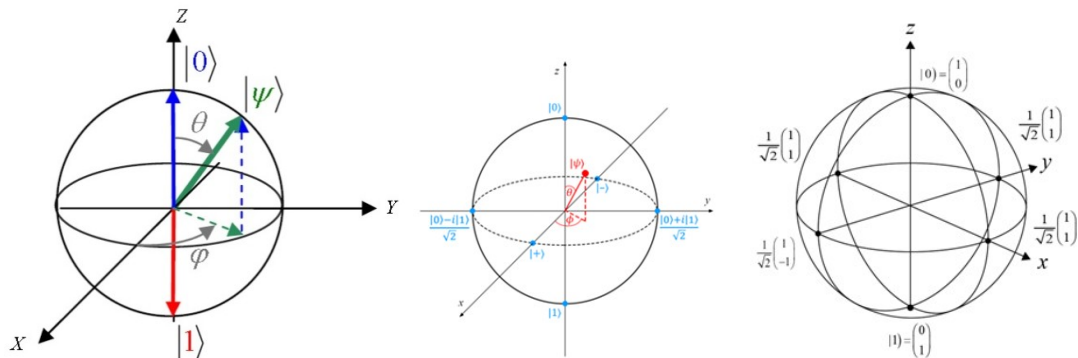


fig. Diversaj prezentoj de la sfero de Bloch

rim. **1.** La ketoj kun sama direkto sed kun kontraŭaj sencoj (ekz. $|0\rangle$ kaj $|1\rangle$) estas ortaj en la spaco de Hilbert. **2.** La eĝeno de $|0\rangle$ estas 1 kaj la eĝeno de $|1\rangle$ estas -1.

kjuoperatoro : Operatoro difinebla per kvadrata matrico kun kompleksaj membroj.

alt. kvantika operatoro

angl. quantum operator / *fr.* opérateur quantique

klar. ➡ operatoroj / pordoj

logika kjuoperatoro : Operatoro kiu modifas la staton de kvantika sistemo, sen modifi la modulon de ĝia stat-vektoro.

alt. kjuopordo, pordo

klar. Logika kjuoperatoro ne ĉiam estas hermita. Male al la klasikaj (klasika informadiko) logikaj operatoroj, la logikaj kjuoperatoroj estu preferinde inversigeblaj por perdi nenium informon, ĉar legado (por sekurigo de intera rezulto) ne eblas dum kvantika procezo.

3D-operatoro-vektoro : Observeblo de spino laŭ specifa direkto.

angl. Pauli vector / *fr.* opérateur-vecteur-3D

klar. 3D estas mallongigo de « tridimensia » ➡ *matricoj de Pauli*

matricoj de Pauli : Vektora bazo de la 3D-operatoro-vektoroj (spin-operatoroj) laŭ la direktoj x , y kaj z .

angl. Pauli matrices / *fr.* matrices de Pauli

klar. Ĉiu 3D-operatoro-vektoro (laŭ ajna direkto) estas lineare esprimebla per la matricoj de Pauli.

rim. **1.** La multiplikado de tiuj matricoj ne estas komutebla. Ekzemple $\sigma_x \cdot \sigma_z \neq \sigma_z \cdot \sigma_x$. Konsekvence, la rezulto (stat-vektoro) de sinsekvaj mezuroj de spino laŭ x kaj z , dependas de la ordo de tiuj mezuroj. ➡ *komutatoro* **2.** Korelative al la antaŭa rimarko, la eĝenoj de ĉiu el tiuj matricoj estas identaj (1 kaj -1), sed la eĝenaj vektoroj malsamas laŭ la direkto. ➡ *komutatoro* **3.** La matricoj de Pauli plus la matrico identeco formas la bazon de kvardimensia spaco tre simila al la spaco de la kvaternionoj (hiperkompleksaj nombroj). Cetere ili estas kvar « kvadrataj radikoj » de la matrico identeco.

$$\text{matr.} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

kongrua(j) observeblo(j) : Observebloj kun komunaj eigen-vektoroj, tiel ke la mezuroj ne estas en konflikto.

angl. observable(s) compatible / *fr.* observable(s) compatible(s)

klar. La mezuroj povas esti farataj infinite precize sammomente. Male, nekongruaj observebloj estus nekomuteblaj, do la rezulto dependus de la mezur-ordo. ➡ *komutatoro*

form. $[A, B] = 0$

ekz. nekongruaj observebloj : $[\sigma_x, \sigma_y] = 2i\sigma_z \neq 0$ $[\sigma_y, \sigma_z] = 2i\sigma_x \neq 0$ $[\sigma_z, \sigma_x] = 2i\sigma_y \neq 0$

maksimume nekongruaj bazoj : kiam mezuro farita en unu bazo donas rezulton maksimume aleatoran, kaj tute antaŭvideblan rezulton en la alia

angl. mutually unbiased bases / *fr.* bases mutuellement non biaisées, maximalement incompatibles, maximalement décorrélées, bases complémentaires

form. A kaj B du bazoj (kun dimensio d) $\forall a \in A, \forall b \in B, |\langle a | b \rangle| = \frac{1}{\sqrt{d}}$

projekcia mezuro : Operatoro de mezuro difinita elde observeblo. ➡ *projekciatoro 2.*

angl. projection measurement / *fr.* mesure projective

rim. projekcia operatoro estas hermita

form. $M = \sum_m m P_m$ kaj $M|\psi\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}}$

poa mezurado : Kiam estas bezonataj tiom da mezuroj kiom da sub-sistemoj por entute koni la sistemon.

angl. multiple measurement / *fr.* mesures multiples

klar. La mezuroj povas esti efektivigitaj sammomente. Alidirite, la observebloj estas komuteblaj.

form. $[O_i, O_j] = 0, \forall (i, j) \in [1, n]^2$ (n estas la nombro de subsistemoj).

ekz. **1.** koordinatoj en la tridimensia spaco : $|xyz\rangle$ **2.** du sendependaj (ne intrikitaj) kjubitoj : $|\psi\phi\rangle$

operatoro de denseco : ➡ *matrico de denseco*

not. $|\psi\rangle\langle\psi|$

matrico de denseco : Ekstera produkto de keto per ĝia brao.

sin. operatoro de denseco

angl. density matrice / *fr.* matrice de densité, opérateur de densité

klar. La eigenoj de la matrico de denseco estas la probablecoj de la mezureblaj valoroj. La spuro de la matrico de denseco (kaze de pura stato) valoras 1. Cetere en la ejgena bazo, la matrico de denseco ebligas manipulado de nur pozitivaj reeloj (la situo de la keto en la spaco de Hilbert ne estas esprimita).

not. $|\psi\rangle\langle\psi|$

ekz. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ do en la ejgena bazo : $\rho_\psi = \begin{pmatrix} \alpha\alpha^* & 0 \\ 0 & \beta\beta^* \end{pmatrix} = \begin{pmatrix} p_{|0\rangle} & 0 \\ 0 & p_{|1\rangle} \end{pmatrix}$

rim. **1.** La operatoro de denseco estas hermita kun pozitivaj eigenoj. **2.** La matrico de denseco estas esprimebla jene : $\rho = |\psi\rangle\langle\psi| = \frac{1}{2}(I + \vec{n} \cdot \vec{\sigma})$ $\vec{n}$ estas la vektoro sur la sfero de Bloch kaj

$\vec{\sigma}$ la 3D-operatoro-vektoro (spin-operatoro).

nombro de Schmidt : Nombro de ne nulaj eĝenoj ĉe operatoro de denseco.

angl. Schmidt number / *fr.* nombre de Schmidt

klar. Praktike, la nombro de Schmidt ĉe operatoro de denseco estas la nombro de eblaj mezur-rezultoj (kun probableco ne nula).

ekz. La nombro de Schmidt de $\frac{\sqrt{2}}{2}|00\rangle + i\frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle$ estas 3.

parta spuro de matrico de denseco : Matrico de denseco de A post redukto laŭ B de la tensor-produta matrico de denseco AB . ➡ *parta spuro*

not. ρ_A kaj ρ_B

klar. $Tr(\rho_{AB}) = Tr(\rho_A^2) = Tr(\rho_A) = Tr(\rho_B) = 1$

se la sistemo AB estas intrikita, $Tr(\rho_A^2) = Tr(\rho_B^2) = \frac{1}{2} \quad |kor(A, B)| = 1$

se la sistemo AB estas parte intrikita, $Tr(\rho_A^2) = Tr(\rho_B^2) < 1 \quad 0 < |kor(A, B)| < 1$

se la sistemo AB ne estas intrikita (produkt-stato), $Tr(\rho_A^2) = Tr(\rho_B^2) = 1 \quad |kor(A, B)| = 0$

ekz. ➡ ekzemploj apendice

malforta mezuro : Pozitivaj operatoroj (kun pozitivaj eĝenoj) E_1 kun eĝenoj $\frac{1+\varepsilon}{2}$ kaj $\frac{1-\varepsilon}{2}$ (nu

$\varepsilon \ll 1$ do preskaŭ egalprobablaj), kaj E_2 kun eĝenoj $\frac{1-\varepsilon}{2}$ kaj $\frac{1+\varepsilon}{2}$.

angl. weak measurement / *fr.* mesure faible

klar. Estas apriorie paradokse ke egalprobableco havas utilecon (ĝuste por efika distingo), des pli ke, konsekvence, estos necese refari la mezuron multfoje por evidentigi statistikan diferencon. Tamen, la « malforteco » de la mezuro faras ke la sistemo estas apenaŭ modifita de la mezuro, do facile ebligas ripeton de la operacio.

kvantika operacio : Operacio kiu modifas matricon de denseco, sekve de interago kun mezurilo aŭ kun la ekstera medio.

angl. quantum operation / *fr.* opération quantique

lingv. la operatoro estas foje nomata per la greka litero ε , foje per E : *angl.* environment *fr.* environnement, do « ekstero » en *Esperanto*.

form. $\rho' = \varepsilon(\rho) \quad \rho' = E(\rho)$

ekz. hamiltoniano (evoluo en la tempo), mezuro, ... estas kvantikaj operacioj.

mezuro POVM : Aro da pozitivaj operatoroj E_n tiaj kiaj $\langle \psi | E_n | \psi \rangle \geq 0, \forall \psi$ kaj $\sum_{j=1}^N E_j = \hat{1}$

angl. POVM measurement *fr.* mesure POVM

klar. **1.** N : dimensio de la mezurata sistemo plus la dimensio de la mezurilo. **2.** Se la mezurilo ne estas enkalkulata, la mezuro POVM estas simpla projekciatoro.

ekz. malforta mezuro, operatoro de denseco.

operatoro de Kraus : Operatoroj kiuj, okaze de kvantika operacio, konsistigas la priskribon de la interago kun la ekstero. ➡ *kvantika operacio*

angl. Kraus operator / *fr.* opérateur de Kraus

form. $\varepsilon(\rho) = \sum_i E_i \rho E_i^{*t}$ operatoroj de Kraus E_i kun $\sum_i E_i^{*t} E_i = I$

klar. **1.** Por ĉiu kvantika operacio, ekzistas pluraj operatoroj de Kraus, eĉ pluraj manieroj malkombini ε -on. **2.** Principe $\varepsilon(\rho) = p.I/2 + (1-p)\rho$, kio signifas ke la kĵubito retroviĝas en stokasta mikso, kaj ke $(1-p)$ estas la probableco ke la kvantika stato ne estos modifita.

➡ ekzemploj apendice

logika kju-bito : kopio de fizika kju-bito. Ĉiu kopio estas same pritraktata de algoritmo, do apriorie donas la saman rezulton, krom pro akcidenta problemo ĉe la materialo. La logikaj kju-bitoj (pluraj estas necesaj) estas poste analizataj de algoritmo de detekto (por scii kiu logika kju-bito estas erara) kaj de korekto. ➡ Algoritmoj (korektado de eraroj)
angl. qu-bit logic / *fr.* qu-bit logique

kvantika datumingo : Aro da kju-bitoj.

sin. kvantika registro, kvantika dateningo

angl. quantum register / *fr.* registre quantique

klar. Dum klasika datumingo el n bitoj havas ununuran valoron inter 0 kaj 2^{n-1} , kvantika datumingo havas samtempe inter unu ĝis ĉiuj el tiuj valoroj.

rim. Same kiel ĉe klasika informadiko, datumingo estas uzebla ĉu kiel logika bitaro (ekz.

➡ *Logikaj kju-bitoj*), ĉu kiel binara nombringo.

fideleco de datumingo : Nombro inter 0 kaj 1, kiu taksas la kju-statan similecon de kvantikaj sistemoj (de kju-bitoj de datumingo, de datumingo).

angl. fidelity of register / *fr.* fidélité d'un registre

form. Fideleco de $|\psi\rangle$ rilate al $|\phi\rangle$: $F(\psi, \phi) = \langle \psi | \phi \rangle \langle \phi | \psi \rangle = \langle \psi | \phi | \psi \rangle = \text{Tr}(\sqrt{\sqrt{\rho_\phi} \rho_\psi \sqrt{\rho_\phi}})$ do $F=1$ se la sistemo estas fidela, sed $F=0$ se la du sistemoj estas entute ortaj en la spaco de Hilbert.

rim. $F(\psi, \phi) = F(\phi, \psi)$

ideala mezuro : Mezuro de stato konforma (rezultoj kaj probablecoj) al la teorio, kvazaŭ mezuro de izolita sistemo, t.e. enkalkulanta nek la mezurilon nek la medion.

angl. ideal measurement / *fr.* mesure idéale

klar. **1.** Praktike, por kompleta priskribo, oni enkalkulu kaj la mezuratan sistemon kaj la mezurilon en pli granda spaco de Hilbert. Krome, ankaŭ la ekstero povas malkoherige interagi (detruo de supermeto de statoj aŭ de intrikiteco). **2.** Male, la kvantika informadiko manipulas idealajn kju-bitojn, arbitre asertante ke la komputoro teknike funkcias « ideale ».

Operatoroj

Por unu kju-bito

konvencie kun :

$$\begin{aligned} |\phi\rangle &= \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \\ |j\rangle &= |0\rangle \text{ aŭ } |j\rangle = |1\rangle \end{aligned}$$

Operatoro $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $X|j\rangle = |j \oplus 1\rangle$ $X|\phi\rangle = e^{i\varphi} \sin \frac{\theta}{2} |0\rangle + \cos \frac{\theta}{2} |1\rangle$
 $X|0\rangle = |1\rangle$ kaj $X|1\rangle = |0\rangle$

Operatoro $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $Y|j\rangle = i(-1)^j |1-j\rangle$ $Y|\phi\rangle = -e^{i\varphi} \sin \frac{\theta}{2} |0\rangle + i \cos \frac{\theta}{2} |1\rangle$
 $Y|0\rangle = i|1\rangle$ kaj $Y|1\rangle = -i|0\rangle$

Operatoro $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $Z|j\rangle = (-1)^j |j\rangle$ $Z|\phi\rangle = \cos \frac{\theta}{2} |0\rangle - e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$
 $Z|0\rangle = |0\rangle$ kaj $Z|1\rangle = -|1\rangle$ $Z|+\rangle = |-\rangle$ kaj $Z|-\rangle = |+\rangle$

Operatoro de rotacio : $R = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$

Operatoro de defaziĝo : $P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix}$ $P|\phi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i(\varphi+\gamma)} \sin \frac{\theta}{2} |1\rangle$ (ne hermita)

Pordo Hadamard : $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = R(\pi/4).P(\pi)$ $H|j\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^j |1\rangle)$

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle \quad \text{kaj} \quad H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle$$

Noto : $H = \frac{1}{\sqrt{2}}(X + Z)$ cetere $HZH = X$

Pordo NOT : $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = R(\pi/2).P(\pi) = X$ eigenoj : $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$ et $|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
 $NOT|0\rangle = |1\rangle$ kaj $NOT|1\rangle = |0\rangle$

Operatoro mezuro $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$

Por du kju-bitoj

$$\text{Pordo } X_A \otimes X_B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$(X_A \otimes X_B)|00\rangle = |11\rangle \quad (X_A \otimes X_B)|01\rangle = |10\rangle$$

$$(X_A \otimes X_B)|10\rangle = |01\rangle \quad (X_A \otimes X_B)|11\rangle = |00\rangle$$

$$\text{Pordo } Y_A \otimes Y_B = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

$$(Y_A \otimes Y_B)|00\rangle = -|11\rangle \quad (Y_A \otimes Y_B)|01\rangle = |10\rangle$$

$$(Y_A \otimes Y_B)|10\rangle = |01\rangle \quad (Y_A \otimes Y_B)|11\rangle = -|00\rangle$$

$$\text{Pordo } Z_A \otimes Z_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(Z_A \otimes Z_B)|00\rangle = |00\rangle \quad (Z_A \otimes Z_B)|01\rangle = -|01\rangle$$

$$(Z_A \otimes Z_B)|10\rangle = -|10\rangle \quad (Z_A \otimes Z_B)|11\rangle = |11\rangle$$

$$\text{Pordo } cPHASE = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \quad (\text{ne hermita})$$

$$cPHASE|00\rangle = |00\rangle \quad cPHASE|01\rangle = |01\rangle$$

$$cPHASE|10\rangle = |10\rangle \quad cPHASE|11\rangle = e^{i\phi}|11\rangle$$

$$\text{Pordo } cNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad cNOT|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$$

$$cNOT|00\rangle = |00\rangle \quad cNOT|01\rangle = |01\rangle$$

$$cNOT|10\rangle = |11\rangle \quad cNOT|11\rangle = |10\rangle$$

Noto : en la pordoj *cPHASE* kaj *cNOT*, la rolo de la unua kju-bito estas kontrolo ($|c\rangle$: « control » en la angla, « contrôle » en la franca), tio signifas ke la dua kju-bito estas pritraktata nur se $|c\rangle = |1\rangle$, dum tiu ĉi lasta ne estas modifita.

$$\text{Pordo } SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{aligned} SWAP |x\rangle|y\rangle &= |y\rangle|x\rangle \\ SWAP |00\rangle &= |00\rangle \\ SWAP |01\rangle &= |10\rangle \\ SWAP |10\rangle &= |01\rangle \\ SWAP |11\rangle &= |11\rangle \end{aligned}$$

$$\text{Pordo Hadamard : } H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\begin{aligned} H|00\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ H|01\rangle &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ H|10\rangle &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \\ H|11\rangle &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \end{aligned}$$

$$\text{Transformado de Fourier} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad (\text{ne hermita})$$

$$\begin{aligned} F|00\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ F|01\rangle &= \frac{1}{2}(|00\rangle + e^{i\frac{\pi}{2}}|01\rangle + e^{i\frac{2\pi}{2}}|10\rangle + e^{i\frac{3\pi}{2}}|11\rangle) \\ F|10\rangle &= \frac{1}{2}(|00\rangle + e^{i\frac{2\pi}{2}}|01\rangle + e^{i\frac{4\pi}{2}}|10\rangle + e^{i\frac{6\pi}{2}}|11\rangle) \\ F|11\rangle &= \frac{1}{2}(|00\rangle + e^{i\frac{3\pi}{2}}|01\rangle + e^{i\frac{6\pi}{2}}|10\rangle + e^{i\frac{9\pi}{2}}|11\rangle) \end{aligned}$$

Por tri kju-bitoj

$$\text{Pordo de } FREDKIN = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{Se } |c\rangle = |0\rangle, FREDKIN |cAB\rangle = |cAB\rangle$$

$$\text{Se } |c\rangle = |1\rangle, FREDKIN |cAB\rangle = |c\rangle \otimes SWAP |AB\rangle$$

$$\text{Pordo de } TOFFOLI = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{alia notacio : } TOFFOLI |c_1 c_2 A\rangle = C^2 NOT |A\rangle$$

$$\text{Se } |c_1 c_2\rangle \neq |11\rangle, TOFFOLI |c_1 c_2 A\rangle = |c_1 c_2 A\rangle$$

$$\text{Se } |c_1 c_2\rangle = |11\rangle, TOFFOLI |c_1 c_2 A\rangle = |c_1 c_2\rangle \otimes NOT |A\rangle$$

$$\text{Noto : } TOFFOLI |x\rangle |y\rangle |0\rangle = |x\rangle |y\rangle |x KAJ y\rangle$$

$$\text{Transformado de } Fourier = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{i\pi/4} & i & ie^{i\pi/4} & -1 & -e^{i\pi/4} & -i & -ie^{i\pi/4} \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & ie^{i\pi/4} & -i & e^{i\pi/4} & -1 & -ie^{i\pi/4} & i & -e^{i\pi/4} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -e^{i\pi/4} & i & -ie^{i\pi/4} & -1 & e^{i\pi/4} & -i & ie^{i\pi/4} \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -ie^{i\pi/4} & -i & -e^{i\pi/4} & -1 & ie^{i\pi/4} & i & e^{i\pi/4} \end{pmatrix} \quad (\text{ne hermita})$$

Por n kju-bitoj

Pordoj *Hadamard* : $H^{\otimes n} |x\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle$ $x \cdot y$ sumo de la laŭbitaj produktoj

Noto : $H^{\otimes n} (H^{\otimes n} |x\rangle^{\otimes n}) = |x\rangle^{\otimes n}$

Transformado de *Fourier* : $F |x\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{iz \frac{\pi}{2^n}} |z\rangle$

Operatoroj (ĝenerala prezento)

nomo	difino / eĝenoj	komento
observeblo	eblaj mezuroj	hermita ne unumodula $\langle A \rangle_{ \psi\rangle} = \langle \psi \hat{A} \psi \rangle$
3D-operatoro-vektoro (lego de spino)	$\sigma = x\sigma_x + y\sigma_y + z\sigma_z$ eĝenoj : 1, -1	hermita unumodula
komutatoro	$[A, B] = AB - BA$	anti-hermita
logikaj operatoroj	defaziĝo, rotacio, <i>NOT</i> , <i>Hadamard</i>	unumodulaj ne ĉiuj hermitaj
pordoj	<i>cPHASE</i> , <i>cNOT</i> , <i>SWAP</i> , <i>X</i> , <i>Y</i> , <i>Z</i> , <i>Hadamard</i> , ...	unumodulaj
pozitiva operatoro	$\langle \psi E_n \psi \rangle \geq 0$ (pozitivaj eĝenoj)	
denseco	probableco de la mezuroj, do $\rho = \phi\rangle\langle\phi $	spuro : 1 hermita, difinita kaj pozitiva
projekciatoro (projekcia mezuro)	1 por la g_n eĝenoj de la eĝena vektoro n , 0 por la aliaj $P_n = \sum_{i=1}^{g_n} u_{n,g_i}\rangle\langle u_{g_i,n} $	unumodula krom okaze de degenera sistemo spuro : g_n
malforta mezuro (pozitiva operatoro)	eĝenoj (pozitivaj) : $\frac{1+\varepsilon}{2}, \frac{1-\varepsilon}{2}$	spuro : 1
kvantika operacio	E (modifo de la operatoro de denseco) $\rho' = E(\rho)$	unumodula
operatoro de Kraus (interagoj kun la medio)	$E(\rho) = E_0 + E_1 + E_2 + E_3$ $E(\rho) = \sqrt{1-p}I + \sqrt{p/3}X + \sqrt{p/3}Y + \sqrt{p/3}Z$ malŝparo, malkoherigo, malpolarizo, ...	unumodula spuro : < 1 modifo de la sfero de Bloch
hamiltoniano	$i\hbar \frac{d \psi\rangle}{dt} = H \psi\rangle$	unumodula

Operatoroj de Kraus (Interago kun la medio)

malpolarizo $\varepsilon(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$ maldikiĝo de la sfero de Bloch

$$E_0 = \sqrt{1-p} I \quad E_1 = \sqrt{\frac{p}{3}} X \quad E_2 = \sqrt{\frac{p}{3}} Y \quad E_3 = \sqrt{\frac{p}{3}} Z$$

inversigo de kju-bito $\varepsilon(\rho) = (1-p)\rho + pX\rho X$ malgrandiĝo de la sfero de Bloch laŭ z (platiĝo)

$$E_0 = \sqrt{1-p} I \quad E_1 = \sqrt{p} X$$

inversigo de fazo $\varepsilon(\rho) = (1-p)\rho + pZ\rho Z$ malgrandiĝo de la sfero de Bloch laŭ x kaj y (longiĝo)

$$E_0 = \sqrt{1-p} I \quad E_1 = \sqrt{p} Z$$

malpliigo de la modulo $\varepsilon(\rho) = (1-p)\rho + p I$ premiĝo de la sfero de Bloch al la poluso (al $|0\rangle$)

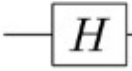
$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \quad E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}$$

salto de fazo (malkoherigo) $\varepsilon \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix}$

$$E_0 = \sqrt{1-p} I \quad E_1 = \sqrt{p} |0\rangle\langle 0| \quad E_2 = \sqrt{p} |1\rangle\langle 1|$$

Skemoj de bazaj logik-cirkvitoj

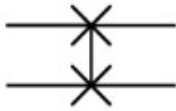
La skema elemento kiu simbolas operatoron estas « skatolo » (*fr.* boîte), *ekz.* la skatolo H ĉi-sube. La linioj kiuj simbolas la eniroj kaj eliroj nomiĝas « fadeno » (*fr.* boîte) por unu kju-bito, kaj « stango » (*fr.* barre) por pli ol du kju-bitoj.

Hadamard  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

NOT / Pauli X  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

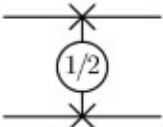
Mezuro 

SWAP



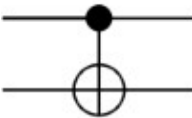
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Radiko de SWAP



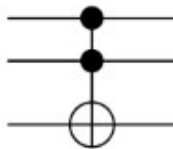
$$\sqrt{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

cNOT



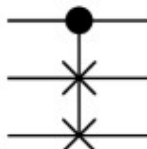
$$cNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Toffoli



$$TOFFOLI = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Fredkin



$$FREDKIN = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Algoritmoj

Kvantika algoritmo funkcias laŭ variantoj de tre ĝenerala skemo (la orakolo). Ĝi uzas du seriojn da kjuĉitoj, kiujn oni nomas x kaj y :

- . x , ĉiita je $H|0^{\otimes n}\rangle$, ĉtenas ĉiujn eblajn valorojn, kiuj estos paralele pritraktataj ;
- . y , ĉiita je $H|1^{\otimes m}\rangle$ kaj kombinita kun funkcio $f(x)$, ĉtenas la kuntekston (tion jam konatan, do la funkcion f kiun oni volas studi aŭ uzi), kaj ĉmplice efektivas intrikitecon kun x , transigante al x la negativajn signojn de siaj komponantoj $|1^{\otimes m}\rangle$ laŭ la valoroj de $f(x)$;
- . fine, laŭ la signoj de la komponantoj $|1^{\otimes m}\rangle$ de x , $H|x\rangle$ donas la rezulton (la kjuĉitoj de $|y\rangle$ estas ĉmplice malkoherigitaj).

Ne estas la rolo de leksikono detale priskribi algoritmojn. La ĉi-postaj specimenoj plej ofte estas prototipaj, kaj utilas precipe por montri la fareblon de kvantikaj algoritmoj, ĉu kiel studobjekto, ĉu kiel testilo de materialo, ĉu por provizi studentojn per interesaj ekzemploj.

La plej promesplena (i.a. por malĉifrado de kriptokodoj), sed ankaŭ la plej ellaborita kaj kompleksa el ili (la algoritmo de Shor), funkciis unuafoje la 19^{an} de decembro 2001^a per kvantika komputoro (firmao IBM) kun sep kjuĉitoj. Ĝi faktorigis la nombron 15 laŭ primoj.

Jen ili prezentataj nur skize kaj principe.

testo de Bell : Konsistas en multfoja ĝenero de unu el la du statoj de Bell kun du egalaj kjuĉitoj, nome $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ kaj $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. La sinsekvaj mezuroj de la du kjuĉitoj devas doni identan rezulton, duonprobable $|0\rangle$ duonprobable $|1\rangle$.

solv. Per du kjuĉitoj :

$$\forall x, |x\rangle|1\rangle \xrightarrow{H_x} \left(\frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)|1\rangle\right) \xrightarrow{cNOT} \frac{1}{\sqrt{2}}(|00\rangle + (-1)^x|11\rangle) \xrightarrow{\text{Mezuro}}$$

klar. La testo de Bell estas utila por testi materialon.

konstruo de la statoj de Bell : La statoj de Bell β_{xy} estas ĝenerataj el la paro $|xy\rangle$.

solv. Per du kjuĉitoj :

$$|x\rangle|y\rangle \xrightarrow{H_x} \left(\frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)|y\rangle\right) \xrightarrow{cNOT} \frac{1}{\sqrt{2}}cNOT(|0\rangle + (-1)^x|1\rangle)|y\rangle = \beta_{xy}$$

problemo de Deutsch : Laŭ la hipotezo ke $|x\rangle$ estas unu-kjubita variablo, ke la rezulto (observo pri funkcio $f(x)$) estas unu-kjubita, la problemo estas : specifi operatoron (inversigeblan) nomatan U_f , sendepende kaj de la enir-variablo $|x\rangle$ kaj de la funkcio f , por scii ĉu f estas konstanta.

solv. Per du kjujbitoj :

$$|0\rangle|1\rangle \xrightarrow{H} H|0\rangle H|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |xy\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{H_x} |x\rangle \xrightarrow{\text{Mezuro}}$$

klar. **1.** La efiko de H (pordo Hadamard) sur la unua kjujbitoj estas ke $|x\rangle$ konsistos kaj el $|0\rangle$ kaj el $|1\rangle$ kiujn estos eble pritrakti samtempe. **2.** H agas sur la dua kjujbitoj tiel ke $|y\rangle$ efikos kontrole, ebligante la enkalkulon de $f(x)$ kun signo malsama (inversa) laŭ la valoro de x . **3.** La efiko de la intriko videblas en la fakto, ke x aperas en ambaŭ kjujbitoj. **4.** La rezulto de la mezuro : se $|0\rangle$ tio signifas ke $f(0) = f(1)$, se $|1\rangle$ tio signifas ke $f(0) \neq f(1)$.

problemo de Deutsch-Jozsa : Laŭ la hipotezo ke $|x\rangle^{\otimes n}$ estas n -kjubita variablo (n estas para), ke la rezulto (observo pri funkcio $f(x)$) estas unu-kjubita, la problemo estas : specifi operatoron (inversigeblan) nomatan U_f , sendepende kaj de la enir-variablo $|x\rangle^{\otimes n}$ kaj de la funkcio f (aŭ konstanta aŭ ekvilibra), por scii ĉu f estas konstanta aŭ ekvilibra.

solv. Per $n+1$ kjujbitoj :

$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H} H^{\otimes n}|0\rangle H|1\rangle = \frac{1}{\sqrt{2^{n+1}}}(|0\rangle + |1\rangle)^{\otimes n}(|0\rangle - |1\rangle) = |xy\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{H_x} |x\rangle \xrightarrow{\text{Mezuro}}$$

klar. **1.** Temas evidente pri ĝeneraligo de la problemo de Deutsch. **2.** La rezulto de la mezuro : se $|00\rangle$ tio signifas ke f estas konstanta, male tio signifas ke f estas ekvilibra.

problemo de Bernstein-Vazirani : Laŭ la hipotezo ke $|x\rangle^{\otimes n}$ estas n -kjubita variablo, ke la rezulto (observo pri funkcio $f(x) = ax$) estas m -kjubita, la problemo estas : specifi operatoron (inversigeblan) nomatan U_f , sendepende kaj de la enir-variablo $|x\rangle^{\otimes n}$ kaj de la funkcio f , por koni la valoron de a .

solv. La solvo relative similas tiun de la antaŭa problemo (Deutsch-Jozsa), kaj ĉifoje la mezuro de $|x\rangle^{\otimes n}$ donas rekte la binaran valoron de a .

problemo de Simon : Laŭ la hipotezo ke $|x\rangle^{\otimes n}$ estas n -kjubita variablo, ke la rezulto (observo pri perioda funkcio $f(x)$) ankaŭ estas n -kjubita, la problemo estas : specifi operatoron (inversigeblan) nomatan U_f , sendepende kaj de la enir-variablo $|x\rangle^{\otimes n}$ kaj de la funkcio f , por koni la periodon de f .

solv. La solvo relative similas tiujn de la antaŭaj problemoj. Estas notinde ke la programo ne estas entute kvantika : la orakolon oni pridemandu plurfoje sinsekve, notante la rezultojn, kaj starigante ekvacion per ĉiu rezulto trovita. La lasta ŝtupo de la solvado konsistas en solvado de la ekvaciaro kadre de klasika (nekvantika) programo.

algoritmo de Grover (1996) : ebligas trovon de elemento en ne antaŭ-strukturita datumaro (el n elementoj).

klar. La algoritmo de Grover estas iteracia, sed la nombro de iteracioj, por plej proksimiĝi al la solvo, estu antaŭ-kalkulita ($\approx \sqrt{n}$) kaj zorge observata. Transe, oni neinvertigeble malproksimiĝus de la solvo. Tiam algoritmon oni metafore nomas *pufkuka*.

princ. La dimensio de la spaco de Hilbert estas n (nombro de elementoj). Deirante de la hiper-diagonalo ($H|0^{\otimes n}\rangle$), oni, je ĉiu iteracio, aplikas du operatorojn kiuj modifas ĉiujn koordinatojn (laŭ simetrio) tiel ke la solva koordinato grandiĝas, la aliaj egale malgrandiĝas. Tiel oni angule proksimiĝas al unu el la eigenaj vektoroj (la solvo).

solv. : Je ĉiu iteracio (kun $f(x) = 1$ se $x = q$, $f(x) = 0$ se $x \neq q$) :

$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H} H^{\otimes n}|0\rangle H|1\rangle = \frac{1}{\sqrt{n+1}}(|0\rangle + |1\rangle)^{\otimes n}(|0\rangle - |1\rangle) = |xy\rangle \left[\xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{U_\phi} U_\phi U_f |x\rangle \right]^{\sqrt{n}} \xrightarrow{\text{Mezuro}} |x\rangle$$

$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle = (-1)^{f(x)}|x\rangle|y\rangle$ (orakolo : ŝanĝo de la signo de la « solva » koordinato)

$U_\phi(|x\rangle) = (2|\phi\rangle\langle\phi| - I)|x\rangle$ simetria operatoro trans $|\phi\rangle = H^{\otimes n}|0\rangle$ (hiper-diagonalo)

rim. **1.** La trovo de la solvo fariĝas tre probabla, sed ne tute certa (la keto proksimiĝas al la ejgena vektoro, sed nur escepte ĉeigās ekzakte). Kaze de maltrafo, oni rekomencu, kio ne estas grava ĉar unuiteracia kvantika procezo estas multoble malpli daŭra ol sekvenca klasika algoritmo. **2.** La funkciado-daŭro evoluas proporcie al $\sqrt{n}$, dum ĝi evoluas proporcie al n ĉe klasika programo. Cetere, la kvantika algoritmo estas facile ĝeneraligebla al samtempa serĉado de pluraj elementoj, kaj ĉikaze la komparo fariĝas des pli favora (serĉo de m elementoj el n evoluas proporcie al $\approx \sqrt{n/m}$ anstataŭ nm).

kvantika transformado de Fourier : Analoge al la klasika transformado de Fourier, ĝi transformas binaran nombron x (n kubitaj valoroj inter 0 kaj 2^n-1) en linearan sumon (kompleksaj koeficientoj je modulo unu) da ketoj inter $|0\rangle^{\otimes n}$ kaj $|1\rangle^{\otimes n}$. La kompleksaj koeficientoj estas la potencoj de $\omega = e^{2i\pi \cdot (x/2^n)}$ do koincidas kun la harmonoj de $x/2^n$.

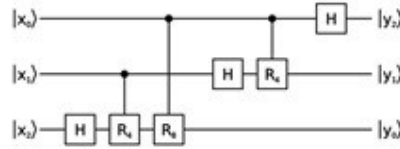
◀ Operatoroj / « transformado de Fourier »

$$\text{form. } U_F|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2i\pi y \cdot (x/2^n)} |y\rangle \quad xy \text{ ordinara produkto}$$

klar. Se $|x\rangle$ estas supermeto de statoj $\sum_j |x_j\rangle = \sum_j \alpha_j |e_j\rangle$, tiam $U_F|x\rangle = \sum_{j=0}^{2^n-1} \alpha_j U_F|e_j\rangle$, kaj ĉiu j havas sian propran frekvencon $j/2^n$.

rim. $U_F U_F |x\rangle = |x\rangle$

Transformado de Fourier



algoritmo de Shor (1994) : Ebligas la erigon de nombro N laŭ primoj.

klar. la algoritmo de Shor funkcias surbaze de la malgranda teoremo de Fermat kaj uzas la kvantikan transformadon de Fourier.

rim. **1.** Intervenias la hazardo en la inito (elektio de la parametro a), do ne ĉiufoje funkcias la algoritmo, kio ĉikaze necesigas rekomencon per eltiraĵo de nova inito-valor. **2.** Same kiel la problemo de Simon, la lasta ŝtupo de la algoritmo de Shor estas klasika.

princ. $|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) |0\rangle$ Hadamard

Oni elektu $a < N$ ĝis $\text{pgcd}(a, N) = 1$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |a^x \bmod N\rangle \quad U_f \text{ de la funkcio } a^x \bmod N$$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} e^{2i\pi xy} |y\rangle |a^x \bmod N\rangle \quad \text{Transformado de Fourier}$$

Oni faru projekcion de la registro de la datumoj sur la bazon : y

Oni malvolvu $y / 2^n$ en kontinuajn frakciojn per **klasika komputoro** ĝis trovo de :

$$a^{Q_t} \equiv 1 \bmod N \text{ tiam : } T = Q_t$$

Se T estas nepara, oni reiru al la komenco, male :

$$a^T - 1 = (a^{T/2} - 1)(a^{T/2} + 1) \equiv 0 \bmod N$$

Se $a^{T/2} + 1 \equiv 0 \bmod N$, oni reiru al la komenco, male :

Oni kalkulu : $\text{pgcd}(a^{T/2} - 1, N)$ kaj $\text{pgcd}(a^{T/2} + 1, N)$, kaj oni kontrolu ke unu el ili estas netriviala faktoro, do rezulto.

La algoritmo de Shor interesas la kriptografion ĉar la malĉifrado de la plej rezistaj sekur-kodoj fariĝas ebla dank' al la rapideco de kvantikaj algoritmoj kaj komputoroj. La ĉi-suba tabelo taksas la daŭrojn de funkciado tre krude, sed, kio estas pli interesa, ĝi komparas la evoluon de la rapideco laŭ la longeco (nombro de ciferoj) de la pritraktita nombro, de la klasika kun la kvantika rimedoj.

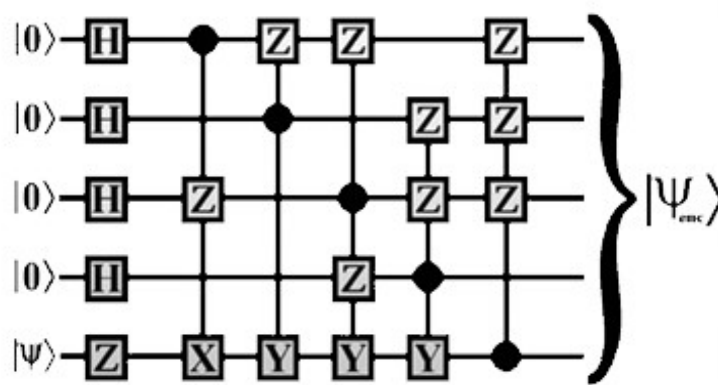
nombro de ciferoj	daŭro por klasika komputoro	daŭro por kvantika komputoro
50	1 sekundon	1 horon
300	2,5 tagojn	2,5 tagojn
1000	19 000 jarojn	42 tagojn
2000	14 000 000 000 jarojn	6 monatojn

fonto : J.Stolze kaj D.Suter

detekto kaj korekto de eraroj : Rezulto de algoritmo povas esti erara pro pluraj materialaj kialoj (do pro interago kun la medio). Praktike, ekzistas du specoj de eraroj : inversigo de la rezulta kju-bito (operatoro X) kaj inversigo de ĝia fazo (operatoro Z). ➡ Operatoroj de Kraus (interago kun la medio). Post obligo (kopio) de ĉiu rezulta fizika kju-bito en plurajn logikajn kju-bitojn, eventuala fuŝa rezulto ĉe unu el ili estas detektita kaj korektita (kondiĉe ke estu ne pli ol unu eraro).

rim. **1.** La algoritmo de korektado estu sufiĉe ellaborita por detekti kaj eventualan inversigon de bito kaj inversigon de fazo. **2.** Korelative, la tuto (detekto kaj korekto de ambaŭ eraro-specoj) estu farata nepre antaŭ la fina mezuro de la algoritmo.

princ. **1.** Por korekti inversigon de kju-bito estas uzataj tri logikaj kju-bitoj (do du kju-bitoj da redundanco), same por korekti inversigon de fazo. **2.** Peter Shor proponis korekto-algoritmon kun naŭ (trioble tri) kju-bitoj (ok kju-bitoj da redundanco). Koncerne la inversigon de fazo, pordoj de Hadamard unue transformas la kju-bitojn al $|+\rangle$ aŭ al $|-\rangle$, kiuj estas pritraktataj poste kvazaŭ por inversigo de kju-bito. **3.** Poste A.R.Calderman, P.Shor kaj siaflanke M.Steane proponis korekto-algoritmon kun sep kju-bitoj. **4.** Fine, R.Laflamme, C.Miguel, J-P. Paz kaj W.H.Zurek proponis korekto-algoritmon kun kvin kju-bitoj, kio estas la teoria minimumo (ĉi-posta skemo-figuro).



Kvantika programo en klasika formo

Eblas funkciigi kvantikan algoritmon per klasika komputoro, almenaŭ por testi ĝin. En la ĉi-suba ekzemplo (banale en C++) :

- . la variabloj (kvantikaj aŭ ne) estas **verdaj** ;
- . ĉio kvantika estas *kursive* skribita ;
- . la kvantikaj operatoroj estas **ruĝaj** ;
- . la dekstra parto estas komentoj kaj klarigoj.

```
BellTest (kiomfoje : int, Initial: rezulto) : (int,int,int)
{
  int kiomUnu = 0;
  int bone = 0;
  using (kjubitoj = Qubit[2]) // deklaro de sistemo kun du kju-bitoj

  for (test in 1..kiomfoje) // la testo estas farata « kiomfoje »
  {
    Set (Initial, kjubitoj [0]); // |x>
    Set (Zero, kjubitoj [1]); // |0> do la stato de la sistemo estas : |S>=|x0>
    H(qubits[0]); // Hadamard → |S>= (|00>+|10>) se |x>=|0>
    // aŭ |S>= (|00>-|10>) se |x>=|1>
    CNOT (kjubitoj [0], kjubitoj [1]); // → |S>= (|00>+|11>) aŭ |S>= (|00>-|11>)
    let rezulto = M(qubits[0]); // mezuro

    if (M (kjubitoj [1]) == rezulto) // kontrolo pri la egaleco de ambaŭ kju-bitoj
      set bone = bone + 1; // normala funkciado

    if (rezulto == One) // nombras la mezuritajn |1>
      set kiomUnu++; // unu plia
  }
  Set (Zero, kjubitoj [0]); // reinito
  Set (Zero, kjubitoj [1]);

  return (kiomfoje - kiomUnu, kiomUnu, bone); // resendas la nombron de |0> kaj la nombron de |1>
  // (se bone funkcias la testo,
  // tiuj du nombroj estas pli-malpli egalaj)
}
```

Komentoj pri la informacio

N kju-bitoj povas enteni plurajn (ĝis 2^N) valorojn **samtempe**, dum N bitoj de klasika komputoro entenas nur unu valoron en preciza momento. Kvantika komputiko estas multe pli efika ĉar ĝi povas pritrakti plurajn valorojn samtempe. Foje legeblas ke, konsekvence, kju-bito entenus multe pli da informacio (informo-kvanto). Tiu lasta aserto estas entute erara. Ĉi-rilate, unu kju-bito entenas nek pli nek malpli da informacio ol klasika bito.

Por simple klarigi, ni elektu la tripleton : $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

Antaŭ la mezuro, la keto $|\psi\rangle$ entenas **unu biton** da informacio : egalprobable supermetitaj estas **du** eĝenaj valoroj ($|01\rangle$ kaj $|10\rangle$) el kvar. Alidirite, ĝi entenas regulon kiu eldiras, ke estas **du** alternativoj : aŭ la unua kju-bito (okaze de mezuro) valoros $|0\rangle$ kaj la dua valoros $|1\rangle$, aŭ inverse. Tiu bito da informacio estas la deirpunkta scio, nomata « kunteksta informacio ».

Post la mezuro, la keto $|\psi\rangle$ entenas **du bitojn** da informacio ($|\psi\rangle$ valoras ĉu $|01\rangle$ ĉu $|10\rangle$). La mezuro kompletigis la kuntekstan informacion per **unu** kroma bito da informacio : definitiva elekto inter la du ebloj.

Evidente, la informacio (entropio) entenata en la du kju-bitoj neniumomente superas du bitojn, kio tute identas al du fizikaj bitoj (memorĉeloj) de klasika situacio. Ni ĝeneraligu al N bitoj :

Hipotezo : N kju-bitoj $|x\rangle_i$ (eĝenaj vektoroj de ĉiu kju-bito : $|0\rangle$ kaj $|1\rangle$)

$$|\psi\rangle = \sum_{i=1}^N \alpha_i |x_i\rangle = \sum_{i=1}^N \sqrt{p_i} |x_i\rangle \quad \text{oni simplige supozas ke la koordinatoj } \alpha_i \text{ estas reelaj}$$

Informacio (inform-kvanto) ricevita okaze de unuopa mezuro aŭ legado :
 $0 \leq -\log_2 p_i < \infty$.

Signifo : ju pli probabla (do ju pli ofta) des malpli informiva estas la mezuro de la eĝeno i .

Averaĝa informacio ricevebla (entropio) : $0 \leq -\sum_{i=1}^N p_i \cdot \log_2 p_i \leq N$

Signifo : se $p_i \approx 0$, rezulto de mezuro de la eĝeno i estus tre informiva sed malofta do neefika ; se $p_i \approx 1$ ĝi estus ofta sed apenaŭ informiva do neefika. La optimuma efikeco okazas kiam ĉiuj valoroj estas egalprobablaj ($p_i = 1/N$) (teoremo de Zipf).

Kunteksta redundanco (entropio) : $0 \leq \sum_{i=1}^N (p_i \cdot \log_2 p_i + 1) \leq N$

Signifo : informacio efektive entenata de la sistemo antaŭ ajna mezuro (inita informo).

Noto : mezuro de bito (memorĉelo) povas alporti informon superan al unu bito da informacio, sed ĉar tio okazas malprobable (do malofte), la averaĝa informacio plu estas malsupera al unu bito. Ĉiukaze, tiu konstato estas sendependa ĉu temas pri klasika komputiko, ĉu temas pri kvantika. La diferenco kuŝas en la fakto ke, la kunteksto (eblaj solvoj) estas priskribita en la kjobitoj mem (dank' al la eblo fari supermeton, kio neblas en klasika informadiko), kaj tio estas la rolo de la orakolo. La diversaj sekvaj pritraktoj celas selekti la solvon, t.e. proksimigi la keton al unu el la eĝenaj vektoroj.

Ĉi-sube kelkaj ekzemploj :

Unu kjobito :

$ \psi\rangle$ (inito)	Kunteksto (bito)	Informacio ricevita (bito)		Averaĝa informacio ricevebla (bito)
		se $ 0\rangle$	se $ 1\rangle$	
$ 0\rangle$	1	0		0
$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	0	1	1	1
$\frac{1}{2} 0\rangle + \frac{\sqrt{3}}{2} 1\rangle$	0,189	2	0,415	0,811

Du kjobitoj :

$ \psi\rangle$ (inito)	Kunteksto (bito)	Informacio ricevita (bito)				Averaĝa informacio ricevebla (bito)
		se $ 00\rangle$	se $ 01\rangle$	se $ 10\rangle$	se $ 11\rangle$	
$ 01\rangle$	2		0			0
$\frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$	1		1	1		1
$\frac{1}{2}(00\rangle + 01\rangle + 10\rangle + 11\rangle)$	0	2	2	2	2	2
$\frac{1}{2} 01\rangle + \frac{\sqrt{3}}{2} 10\rangle$	1,19		2	0,415		0,81
$\frac{1}{2} 01\rangle + \frac{\sqrt{3}}{2} 11\rangle$	1,19		2		0,415	0,81
$\frac{1}{2} 00\rangle + \frac{1}{\sqrt{2}} 01\rangle + \frac{1}{\sqrt{2}} 11\rangle$	0,5	2	1		1	1,5
$\frac{1}{4} 00\rangle + \frac{1}{4} 01\rangle + \frac{\sqrt{7}}{4} 10\rangle + \frac{\sqrt{7}}{4} 11\rangle$	0,46	4	4	1,19	1,19	1,54

Sur ĉiu linio de ambaŭ tabeloj, la sumoj de la du gras-karaktraj kvantoj de informo samvaloras kiel la nombro de kju-bitoj (resp. 1 kaj 2), nek pli nek malpli, kaj tio estas la fina informacio. Do la sola diferenco en kvantiko, estas ke la deirpunkta informacio-valoro ne estas nula, kaj rilatas al la kunteksta informo.

Noto : En praktika situacio, la ne nulaj valoroj (probablecoj) de α_i (do de p_i) estas ĝenerale egalaj (konata escepto : algoritmo de Grover). Konsekvence, la ricevita informacio neniam estos supera al N .

Komparo de la informaciaj konsideroj inter la klasika informadiko, la kvantika informadiko kaj homa lingvo :

	klasika informadiko	kvantika informadiko	homa lingvo
dimensio	nombro de bitoj : N fareblaj valoroj : 2^N	nombro de kĵubitoj : N dimensio de la spaco de Hilbert : $2^{N+1} - 2$ nombro de eĵgenoj : 2^N	Finia sed $\approx \infty$ (semantika spaco) kaj literaro kaj vortaro (do du spacoj de Hilbert) aliaj niveloj ekzistas, i.a. la frazo
alfabeto	0 kaj 1 ĝenerale egalprobablaj interligo inter la leksika, semantika kaj sintaksa niveloj (tipo de variabloj)	$ 0\rangle$ kaj $ 1\rangle$ ĝenerale egalprobablaj apriore, neniuj interligoj inter la leksika kaj la semantika niveloj	kaj literaro kaj vortaro nek la literoj nek la vortoj estas egalprobablaj tre forta interligo inter la leksiko kaj la semantiko
kunteksto	tio jam konata : inito de variabloj sintakso troviĝas en la programo (eĉ estas ĝia rolo)	tio jam konata : $f(x)$ kombinita de orakolo troviĝas en la kĵubitoj mem (laŭ la nivelo de supermetiteco)	tio jam konata : kulturo, medio, spaco-tempo, pri la kunparolanto, lingvo (leksiko, gramatiko, ...) troviĝas ie en la homa cerbo
informo ricevita de mezuro	el lego de variabloj ne detruas la kontekston	el fina mezuro de kĵubitoj detruas la kontekston (kvantika redukto)	el legado aŭ aŭskultado riĉigas la kontekston (spertiĝo)
pritrakto de eraroj	teknike apenaŭ eblas eraroj okazas nur pro fuŝa programado	teknike oftas pro interago kun la medio (malgrandigo de la sfero de Bloch) ☛ <i>operatoroj de Kraus</i> la algoritmoj nur plej « proksimiĝas » al la solvo, do eraro ne entute malprobablas (nesolvado)	senĉesa mensa vagado : kompromisoj, supozoj, hezitoj, subtaksoj, ... alta nivelo de memkorektado la konteksto estas nestabila, senĉese modifita

Konkludoj

Pro la rapida disvolviĝo de la kvantika informadiko, same rapida influo estas antaŭvidebla en diversaj fakoj kaj sub-fakoj. Supozeble, tiu influo ne estos samspeca por ĉiuj el ili. La konsekvencoj povos esti ĉu konkretaj, ĉu teoriaj kaj intelektaj. La evoluo de la kvantika informadiko generos novajn nesolvitajn problemojn, grandigos la scipovon de la teknikistoj kaj akrigos la scivolon de esploremluloj, sed ankaŭ naskos novan manieron pensi kaj koncepti nian mondon.

En fiziko kaj filozofio, la fenomenoj kiaj la plurstateco, la nelokeco kaj la nekontinuo (interago kun la medio, mezuro, nekomuteblo) ne ankoraŭ ricevis unuanimajn klarigojn kaj pravigojn.

En informadiko mem kaj en kriptografio, la paŝoj faritaj estas malmulto. Ekzemple, amaso da algoritmoj estos necese elpensi. Tre signifoplena estas la ekzemplo de la lineara programado per entjeraj nombroj (algoritmo *Simplexe* kaj esploro de decido-arboj), ofte citita kiel fertila tereno por kvantikaj algoritmoj.

En komputiko, multegaj problemoj restas plu solvendaj por realigi komputorojn ne tro multekostajn, enhavantajn sufiĉe da kjubitoj sen risko de malkohero, kaj funkciajn je « media » temperaturo (en la faka literaturo, « media » foje signifas « je almenaŭ kelkaj kelvinoj »!). Momente, neniuj povas aserti kio estos kvantika komputoro post dek jaroj. Eĉ la elekto de la partiklo kaj de la fizikaj fenomenoj uzotaj ne estas definitiva.

Matematiko, kaj eventuale statistiko, devos aktive kontribui kaj solvi novajn problemojn. Ĥaoso-teorio (studo de la nestabilaj sistemoj) jam estas formulata per la notacio de Dirac kaj sekvas la spurojn de la kvantiko en sia formulado. Elektro-teorio povos modelizi situaciojn apriorie neraciajn (uzo de partaj operatoroj okaze de sinsekvaj decidoj ➡ Kontribuo de Hervé Zwirn en « *Philosophie de la mécanique quantique* » eldono Vuibert 2009).

Kvantiko pozitive kontribuos en aliaj fakoj, alportante al tiuj teoriajn, pedagogiajn, kaj metodologiajn instruojn. Inter tiuj verŝajne troviĝas la informo-teorio kaj la lingviko.

Apendico pri utila formularo

I

Ejgenaj vektoroj de 3D-operatoro-vektoroj (spin-operatoroj)

Ejgenaj vektoroj de σ_z : $|u\rangle$ kaj $|d\rangle$ (« *up* » kaj « *down* » en la angla) alinomataj $|0\rangle$ kaj $|1\rangle$

Ejgenaj vektoroj de σ_x : $|r\rangle$ kaj $|l\rangle$ (« *right* » kaj « *left* » en la angla) alinomataj $|+\rangle$ kaj $|-\rangle$

Ejgenaj vektoroj de σ_y : $|i\rangle$ kaj $|o\rangle$ (« *in* » kaj « *out* » en la angla)

$$\begin{aligned}
|r\rangle &= \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle) & |l\rangle &= \frac{1}{\sqrt{2}}(|u\rangle - |d\rangle) \\
|i\rangle &= \frac{1}{\sqrt{2}}(|u\rangle + i|d\rangle) & |o\rangle &= \frac{1}{\sqrt{2}}(|u\rangle - i|d\rangle)
\end{aligned}$$

II

Rezulto de 3D-operatoro-vektoroj (spin-operatoroj) sur la ejgenaj vektoroj

sur $ u\rangle$: $\sigma_z(u\rangle) = u\rangle$	$\sigma_x(u\rangle) = d\rangle$	$\sigma_y(u\rangle) = i d\rangle$
sur $ d\rangle$: $\sigma_z(d\rangle) = - d\rangle$	$\sigma_x(d\rangle) = u\rangle$	$\sigma_y(d\rangle) = -i u\rangle$
sur $ r\rangle$: $\sigma_z(r\rangle) = l\rangle$	$\sigma_x(r\rangle) = r\rangle$	$\sigma_y(r\rangle) = -i l\rangle$
sur $ l\rangle$: $\sigma_z(l\rangle) = r\rangle$	$\sigma_x(l\rangle) = - l\rangle$	$\sigma_y(l\rangle) = i r\rangle$
sur $ i\rangle$: $\sigma_z(i\rangle) = o\rangle$	$\sigma_x(i\rangle) = i o\rangle$	$\sigma_y(i\rangle) = i\rangle$
sur $ o\rangle$: $\sigma_z(o\rangle) = i\rangle$	$\sigma_x(o\rangle) = i i\rangle$	$\sigma_y(o\rangle) = - o\rangle$

III

Statoj de maksimuma intrikiteco (statoj de Bell)

$$|Sing\rangle = \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle) = |\psi_-\rangle = |\beta_{11}\rangle \text{ singuleto}$$

$$|T_1\rangle = \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) = |\psi_+\rangle = |\beta_{01}\rangle \text{ tripleto}$$

$$|T_2\rangle = \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) = |\phi_+\rangle = |\beta_{00}\rangle \text{ tripleto}$$

$$|T_3\rangle = \frac{1}{\sqrt{2}}(|uu\rangle - |dd\rangle) = |\phi_-\rangle = |\beta_{10}\rangle \text{ tripleto}$$

$$\text{Konstruo de la statoj de Bell : } B|xy\rangle = |Hx, Hx \oplus y\rangle = |\beta_{xy}\rangle$$

IV

Tensora produto de observebloj (3D-operatoro-vektoro de kjubito-duopo)

Noto : $\tau_x \sigma_x = \tau_x \otimes \sigma_x$, τ por la unua kjubito, σ por la dua (temas pri tensora produto) :

$$\tau_x \sigma_x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}; \tau_y \sigma_y = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}; \tau_z \sigma_z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\tau_x \sigma_x |Sing\rangle = \tau_y \sigma_y |Sing\rangle = \tau_z \sigma_z |Sing\rangle = -|Sing\rangle$$

$$\tau_x \sigma_x |T_1\rangle = \tau_y \sigma_y |T_1\rangle = -\tau_z \sigma_z |T_1\rangle = |T_1\rangle$$

$$\tau_x \sigma_x |T_2\rangle = -\tau_y \sigma_y |T_2\rangle = \tau_z \sigma_z |T_2\rangle = |T_2\rangle$$

$$-\tau_x \sigma_x |T_3\rangle = \tau_y \sigma_y |T_3\rangle = \tau_z \sigma_z |T_3\rangle = |T_3\rangle$$

Se $\tau\sigma = \tau_x \sigma_x + \tau_y \sigma_y + \tau_z \sigma_z$

$$\tau\sigma |Sing\rangle = -3|Sing\rangle \quad \text{ejgeno : -3}$$

$$\tau\sigma |T_1\rangle = |T_1\rangle \quad \text{ejgeno : 1}$$

$$\tau\sigma |T_2\rangle = |T_2\rangle \quad \text{ejgeno : 1}$$

$$\tau\sigma |T_3\rangle = |T_3\rangle \quad \text{ejgeno : 1}$$

Do la observeblo $\tau\sigma$ estas degenera. Ĝia nombro de Schmidt valoras 2 (du ejgenoj : -3 kaj 1).

V

Matrico de denseco / partaj spuroj / nivelo de intrikiteco ➡ *parta spuro de la matrico de denseco*

Kalkulado de la partaj spuroj :

$$\rho_{Auu} = \psi^*(u,u)\psi(u,u) + \psi^*(u,d)\psi(u,d)$$

$$\rho_{Aud} = \psi^*(u,u)\psi(d,u) + \psi^*(u,d)\psi(d,d)$$

$$\rho_{Adu} = \psi^*(d,u)\psi(u,u) + \psi^*(d,d)\psi(u,d)$$

$$\rho_{Add} = \psi^*(d,u)\psi(d,u) + \psi^*(d,d)\psi(d,d)$$

$$\rho_{Buu} = \psi^*(u,u)\psi(u,u) + \psi^*(d,u)\psi(d,u)$$

$$\rho_{Bud} = \psi^*(u,u)\psi(u,d) + \psi^*(d,u)\psi(d,d)$$

$$\rho_{Bdu} = \psi^*(u,d)\psi(u,u) + \psi^*(d,d)\psi(d,u)$$

$$\rho_{Bdd} = \psi^*(u,d)\psi(u,d) + \psi^*(d,d)\psi(d,d)$$

Ekzemploj :

$$|\psi\rangle = |Sing\rangle = \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle)$$

$$\rho_{AB} = |Sing\rangle\langle Sing| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}_{B=|00\rangle|01\rangle|10\rangle|11\rangle} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}_{B=|Sing\rangle|T_1\rangle|T_2\rangle|T_3\rangle}$$

$$\rho_{AB}^2 = \rho_{AB} \text{ kaj } Tr(\rho_{AB}^2) = 1$$

$$\rho_A = Tr_B(\rho_{AB}) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}_{B=|0\rangle|1\rangle} \text{ kun } \rho_A^2 = \rho_B^2 \neq \rho_A = \rho_B \text{ kaj } Tr(\rho_A) = Tr(\rho_B) = 1 \neq Tr(\rho_A^2) = Tr(\rho_B^2) = \frac{1}{2}$$

Kvin aliaj ekzemploj (en la bazo $B = |00\rangle|01\rangle|10\rangle|11\rangle$) :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) \quad \rho = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \rho^2 \quad \rho_A = \rho_B = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \neq \rho_A^2 = \rho_B^2 = \begin{pmatrix} \frac{1}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \quad \rho = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix} = \rho^2 \quad \rho_A = \rho_B = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \neq \rho_A^2 = \rho_B^2 = \begin{pmatrix} \frac{1}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}$$

$$|\psi\rangle = \frac{1}{2}(|uu\rangle + |ud\rangle + |du\rangle + |dd\rangle) \quad \rho = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix} = \rho^2 \quad \rho_A = \rho_B = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \rho_A^2 = \rho_B^2$$

$$|\psi\rangle = \frac{1}{5}(3|uu\rangle + 4|ud\rangle) \quad \rho = \begin{pmatrix} \frac{9}{25} & \frac{12}{25} & 0 & 0 \\ \frac{12}{25} & \frac{16}{25} & 0 & 0 \\ \frac{0}{25} & \frac{0}{25} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \rho^2 \quad \rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \rho_A^2 \quad \rho_B = \begin{pmatrix} \frac{9}{25} & \frac{12}{25} \\ \frac{12}{25} & \frac{16}{25} \end{pmatrix} = \rho_B^2$$

$$|\psi\rangle = \sqrt{0,6}|ud\rangle - \sqrt{0,4}|du\rangle \quad \rho = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0,6 & -\sqrt{0,24} & 0 \\ 0 & -\sqrt{0,24} & 0,4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \rho^2$$

$$\rho_A = \begin{pmatrix} 0,6 & 0 \\ 0 & 0,4 \end{pmatrix} \neq \rho_A^2 = \begin{pmatrix} 0,36 & 0 \\ 0 & 0,16 \end{pmatrix} \quad \rho_B = \begin{pmatrix} 0,4 & 0 \\ 0 & 0,6 \end{pmatrix} \neq \rho_B^2 = \begin{pmatrix} 0,16 & 0 \\ 0 & 0,36 \end{pmatrix}$$

Apendico pri la materialo

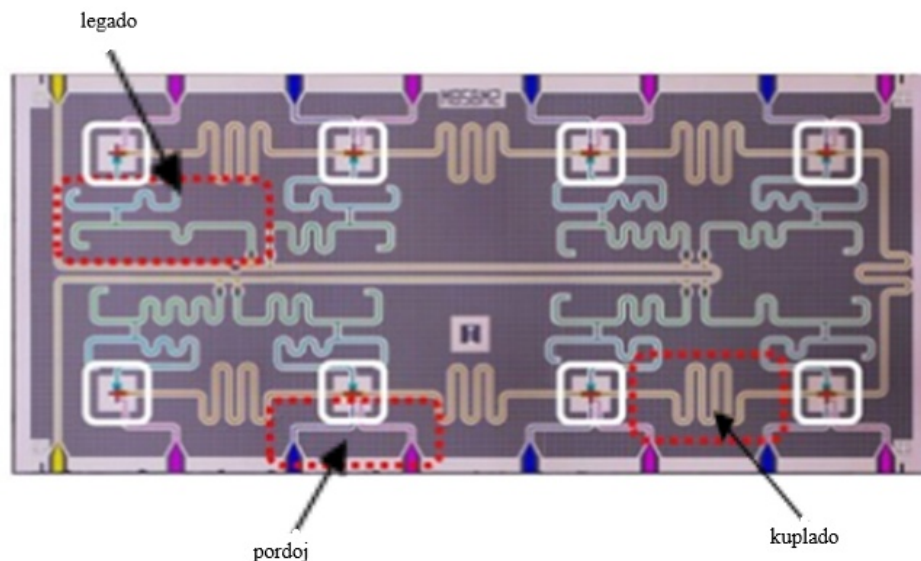
La stokado kaj la pritrakto de la kvantika informacio necesigas fizikajn sistemojn, kiuj respektu la jenajn kondiĉojn :

1. fizika kju-bito stabila kaj bone difinita
2. sistemoj longigeblaj al kju-bitaro sufiĉe granda
3. kju-bito initebla en iu ajn konata stato
4. fizikaj kjuĉeloj kun sufiĉe granda vivdaŭro por certigi la koherecon de la kvantikaj statoj dum la funkciado de algoritmo
5. ekzisto de aro da universalaj kvantikaj pordoj : rotacio de individuaj kju-bitoj kaj pordo cNOT
6. efika mezur-proceduro de la kju-bitoj fine de la algoritmo

Tiuj kondiĉoj estas malfacile realigeblaj samtempe, kaj konstruo de kvantika komputoro plu restas je la nivelo de la unuaj balbutoj. El tiuj kondiĉoj, la ĉefa malamiko de la kvantika komputoro estas la interago kun la ekstera medio, kaŭzo de la malkoheriga fenomeno, kies konsekvenco estas la perdo de la fazo en lineara supermeto de la kju-bitoj. La algoritmoj estu do efektivigitaj en malpli granda daŭro ol tiu de la kohereco (inter $10^{-10}s$ kaj $10^{-8}s$). Foje, tiu daŭro ŝajnas terure malgranda, sed oni konsideru ke elementa operacio (logika pordo) pri kju-bito daŭras inter $10^{-14}s$ kaj $10^{-13}s$.

El ĉiuj ĝis nun imagitaj procedoj, neniuj estas apriorie promesplena por la estonteco de la kvantika komputoro.

Ekzemplo de cirkvito kun ok kju-bitoj « ETH », Zurich (kvantika komputoro surbaze de suprakonduktoroj) :



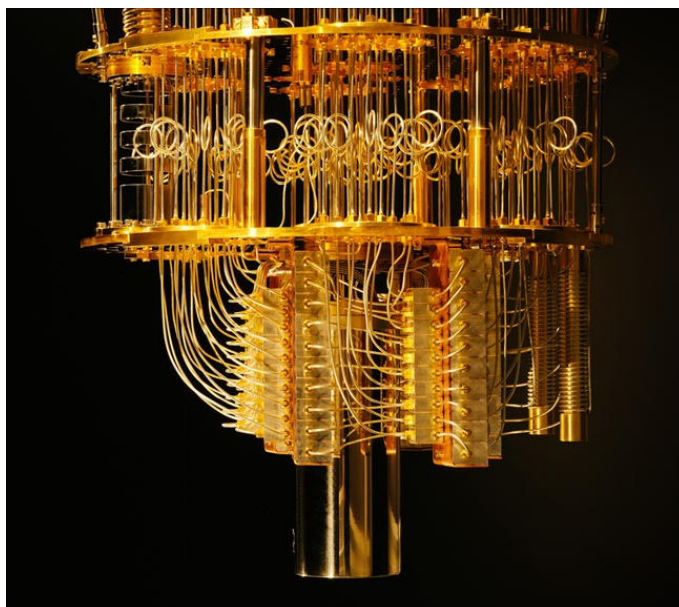
La (ok) **kju-bitoj** situas en la blankaj ortanguloj.

Ili estas interligitaj per **cirkvitoj de kuplado**, utilaj por kontroli ilian intrikitecon.

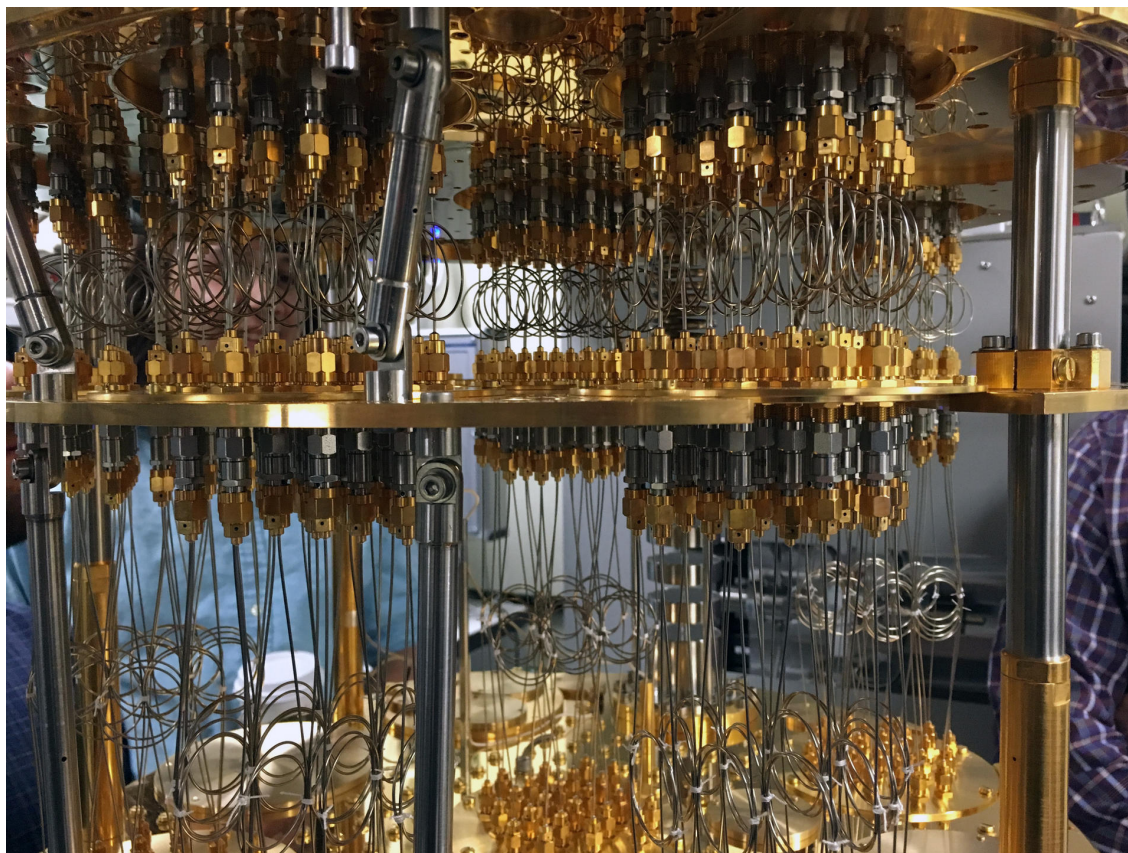
La (bluaj kaj violkoloraj) pordoj ebligas agon sur la kju-bitoj. Tiuj ĉi du universalaj pordoj, se kombinitaj, rekonstituas la aliajn kvantikajn pordojn necesajn en la funkciado de la algoritmoj.

La **mezur**o (**legado**) efektiviĝas per aliaj cirkvitoj, parte en la cirkvito mem.

Ekzemplo de kvantika komputoro :



Kvantika komputoro (el « CNRS Le Journal »)



Kvantika komputoro (el « CNRS Le Journal »)

Propraj nomoj

Alain Aspect [*alan aspe*]
John Bell [*ĝon bel*] (1928-1990)
Ethan Bernstein [*etan berŝten*]
Félix Bloch [*feliks blok*] (1905-1983)
David Bohm [*david bom*] (1917-1992)
Paul Dirac [*pol dirak*] (1902-1984) (*Nobelpremio 1933*)
David Deutsch [*david deĉ*]
Hugh Everett [*ug everet*] (1930-1982)
Marissa Giustina [*marisa ĵjustina*]
Lov Grover [*lov grover*]
Jacques Hadamard [*ĵak adamar*] (1865-1963)
Werner Karl Heisenberg [*verner karl ajzenberg*] (1901-1976) (*Nobelpremio 1932*)
David Hilbert [*david ilber*] (1862-1943)
Richard Jozsa [*riŝar ĵoza*]
Karl Kraus [*karl kros*] (1938-1988)
Wolfgang Pauli [*ŭolfgang poli*] (1900-1958) (*Nobelpremio 1945*)
Otto Schmidt [*oto ŝmit*] (1891-1956)
Lynden K. Shalm [*linden k ŝalm*]
Peter Shor [*piter ŝor*]
Dan Simon [*dan simon*]
Erwin Schrödinger [*erŭin ŝrodinger*] (1887-1961) (*Nobelpremio 1933*)
Umesh Vazirani [*umeŝ vazirani*]

Enhavo

ENKONDUKO	2
KIEL ENIRI LA LEKSIKONON.....	4
LEKSIKONO	5
SIGLOJ.....	9
SPECIFAJ MATEMATIKAJ NOCIOJ	10
SPECIFAJ FIZIKAJ NOCIOJ	12
PRINCIPOJ KAJ KONCEPTOJ	15
OPERATOROJ	23
POR UNU KJUBITO	23
POR DU KJUBITOJ	24
POR TRI KJUBITOJ	26
POR N KJUBITOJ	27
OPERATOROJ (ĜENERALA PREZENTO)	27
OPERATOROJ DE KRAUS (INTERAGO KUN LA MEDIO)	28
SKEMOJ DE BAZAJ LOGIK-CIRKVITOJ	28
ALGORITMOJ	30
KVANTIKA PROGRAMO EN KLASIKA FORMO (EKZEMPLO).....	35
KOMENTOJ PRI INFORMACIO	36
KONKLUDOJ	39
APENDICO PRI UTILA FORMULARO	40
EJGENAJ VEKTOROJ DE 3D-OPERATORO-VEKTOROJ (SPIN-OPERATOROJ)	40
REZULTO DE 3D-OPERATORO-VEKTOROJ (SPIN-OPERATOROJ) SUR EJGENAJ VEKTOROJ	40
STATOJ DE MAKSIMUMA INTRIKITECO (STATOJ DE BELL)	40
TENSORA PRODUTO DE OBSERVEBLOJ (3 D-OPERATORO-VEKTORO DE KJUBITO-DUOPO)	41
MATRICO DE DENSECO / PARTAJ SPUROJ / NIVelo DE INTRIKITECO.....	41
APENDICO PRI LA MATERIALO	43
PROPRAJ NOMOJ DE FAMULOJ	45

Mi sincere dankas je
Jesper Jacobsen (profesoro pri Teoria Fiziko / ENS)
pro liaj utilaj rimarkoj, konsiloj kaj korektoj.