Divu q-bitu sistēma

Iespējamo alternatīvo (bāzes) stāvokļu skaits ir $2^2 = 4$. Tie ir

$$\begin{aligned} |0\rangle_1|0\rangle_2 &\equiv |00\rangle \\ |0\rangle_1|1\rangle_2 &\equiv |01\rangle \\ |1\rangle_1|0\rangle_2 &\equiv |10\rangle \\ |1\rangle_1|1\rangle_2 &\equiv |11\rangle \end{aligned}$$

Divu q-bitu operācija "**kontrolētais NOT**" $\hat{U}_C$ invertē otro bitu tad un tikai tad, ja pirmais ir $= 1$.

$$\boxed{\hat{U}_C|0\rangle_1|0\rangle_2 = |0\rangle_1|0\rangle_2,}$$
$$\hat{U}_C|0\rangle_1|1\rangle_2 = |0\rangle_1|1\rangle_2,$$
$$\boxed{\hat{U}_C|1\rangle_1|0\rangle_2 = |1\rangle_1|1\rangle_2,}$$
$$\hat{U}_C|1\rangle_1|1\rangle_2 = |1\rangle_1|0\rangle_2.$$

Šķiet, ka $\hat{U}_C$ der q-bitu kopēšanai

$\hat{U}_C|x\rangle_1|0\rangle_2 = |x\rangle_1|x\rangle_2$, $x = 0$ vai 1, bet . . .

. . . *superpozīciju nevar nokopēt* :

$$\hat{U}_C\big(c_0|0\rangle_1 + c_1|1\rangle_1\big)|0\rangle_2 = \\ = c_0|0\rangle_1|0\rangle_2 + c_1|1\rangle_1|1\rangle_2.$$

Iegūtais stāvoklis ir **sapīts** (*entangled*) $\Leftrightarrow$ varam runāt tikai par visas sistēmas stāvokli, bet ne katras tās daļas atsevišķi.

Izmantojot sapītos stāvokļus, tomēr ir iespējams identiski nokopēt kvantu stāvokli. Šo procesu sauc par **teleportāciju**.

Kvantu **nelokalitātes** piemērs:

$$\begin{aligned} \hat{U}_C|1\rangle_1\big(|0\rangle_2 - |1\rangle_2\big) &= |1\rangle_1\big(\boxed{|1\rangle_2 - |0\rangle_2}\big) \\ &= \boxed{-|1\rangle_1}\big(|0\rangle_2 - |1\rangle_2\big) \end{aligned}$$

Uz kuru tad no q-bitiem mēs īsti esam iedarbojušies?

Sistēmā ar n q-bitiem – kvantu reģistrs.
Bāzes stāvokļi :

$$|00\ldots0\rangle$$
$$|00\ldots1\rangle$$
$$\ldots$$
$$|11\ldots1\rangle$$

Sistēmu raksturo nevis $2n$, bet 2^n koeficienti:

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle,$$
$$\sum_{x=0}^{2^n-1} |c_x|^2 = 1.$$

A. Barenco (1995): Ar secīgām viena un divu q-bitu transformācijām var veikt patvaļīgu n q-bitu operāciju.

"Minimālais" komplekts: 1 q-bita fāzes nobīde un rotācija + 2 q-bitu kontrolētais NOT.

Kriptogrāfiskās sistēmas RSA pamats:

Lielu skaitli ir grūti sadalīt reizinātājos (faktorizēt)

Grūti ⇔ laiks aug līdz ar ciparu skaitu n ***eksponenciāli,***
Daudz vieglāk ⇔ laiks pieaug līdz ar n ***polinomiāli.***

Labākais klasiskais algoritms (*Number Field Sieve*):

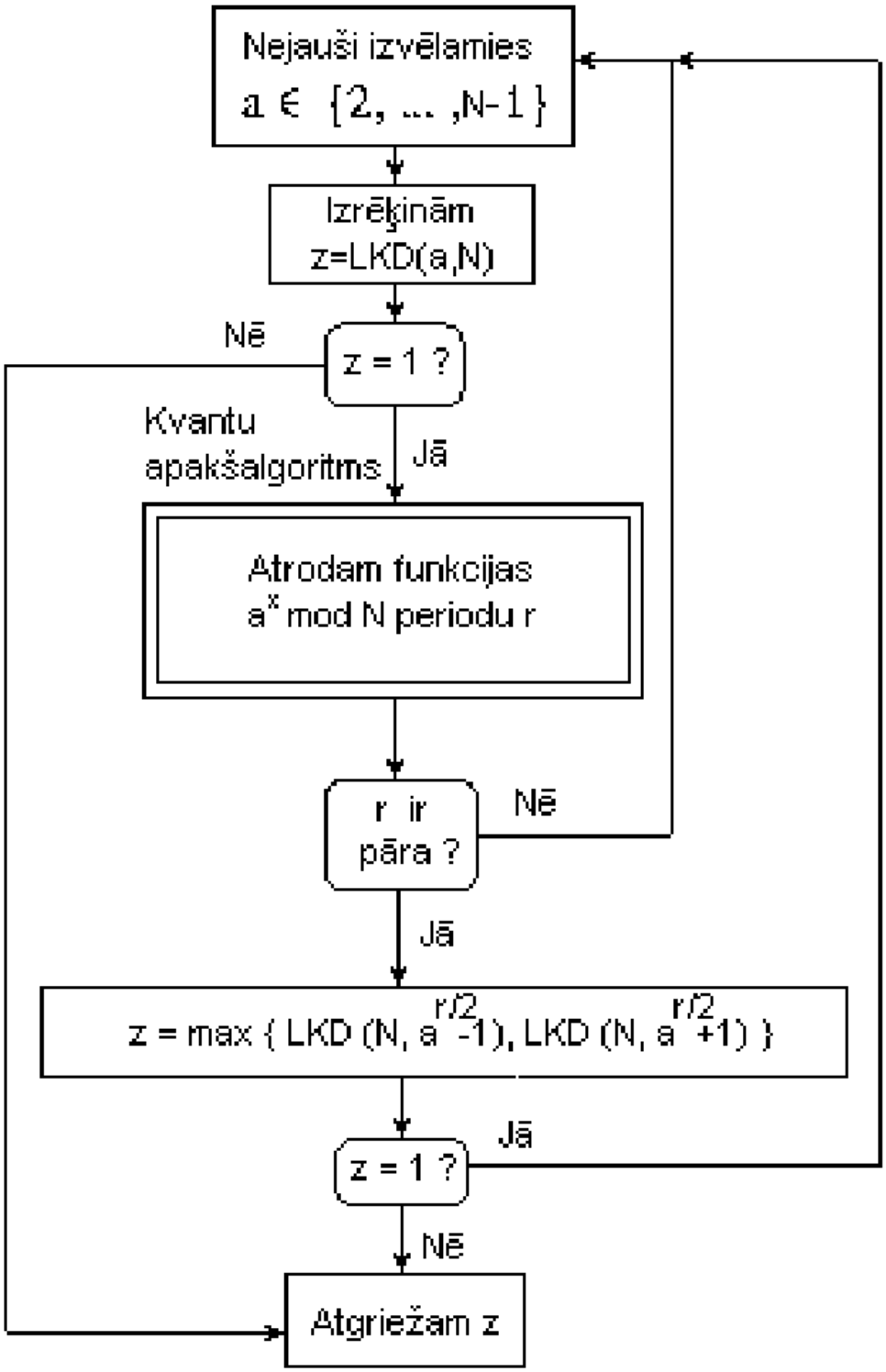
$$O(e^{1.9\ (\ln n)^{\frac{1}{3}}(\ln(\ln n))^{\frac{2}{3}}}) >$$ polinoms(n)

Pītera Šora kvantu algoritms:

$$O((\ln n)^3) \sim$$ polinoms(n)

Faktorizācijas redukcija uz perioda noteikšanu

Meklējam skaitļa N dalītāju z.



Kvantu perioda noteikšana

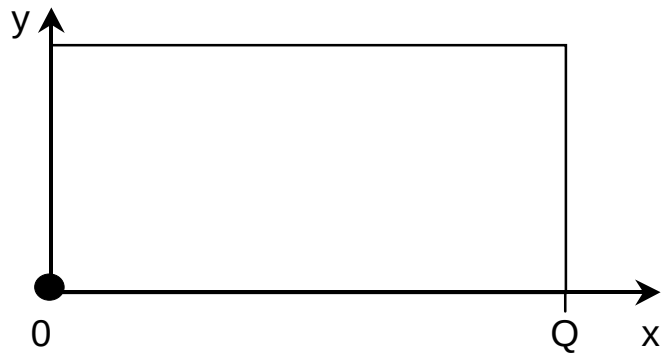
Uzdevums: Noteikt funkcijas $f(x) = f(x + r)$, $\forall x \in \mathbb{Z}$, periodu r.

X **reģistrs** satur n q-bitus.
Kopējais bāzes stāvokļu skaits $Q \equiv 2^n > r^2$.

Y **reģistra** ietilpību nosaka iespējamo $f(x)$ vērtību intervāls.

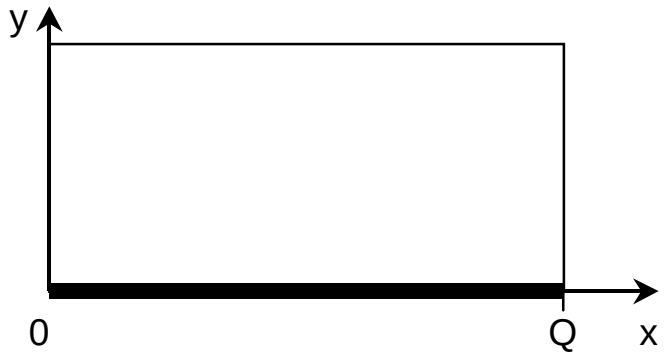
1. solis. Datoru sagatavo stāvoklī $x = 0$, $y = 0$:

$$|\underbrace{00\ldots0}_{n}\rangle_X|00\ldots0\rangle_Y \equiv |0\rangle_X|0\rangle_Y.$$



2. solis. X reģistru pārvērš homogēnā superpozīcijā:

$$\frac{1}{\sqrt{Q}} \sum_{x_1,\ldots,x_n=0,1} |x_1 x_2 \ldots x_n\rangle_X |0\rangle_Y \equiv \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle_X |0\rangle_Y .$$

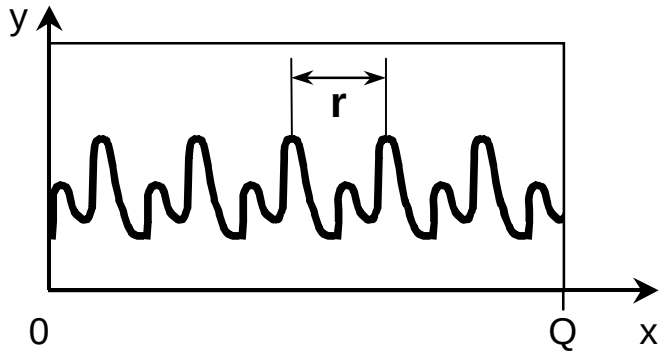


3. solis. Izpilda $f(x)$ aprēķinu : $|x\rangle_X |0\rangle_Y \longrightarrow |x\rangle_X |f(x)\rangle_Y$.

Vienu reizi aprēķinot $f(x)$, kvantu dators izpilda to *visu* Q stāvokļu superpozīcijai !

Reģistru stāvoklis pēc 3. soļa būs:

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle_X |f(x)\rangle_Y$$



Kvantu Furjē transformācija (QFT)

QFT: Katru $|x\rangle$ aizstāj ar superpozīciju:

$$|x\rangle \stackrel{QFT}{\longrightarrow} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} e^{2\pi ikx/Q} |k\rangle.$$

4. solis. Reģistram X pielietojot QFT, stāvoklis

$$\frac{1}{\sqrt{Q}} \sum_x |x\rangle_X |f(x)\rangle_Y$$

pārtop par

$$|\Phi\rangle = \frac{1}{Q} \sum_x \sum_k e^{2\pi ikx/Q} |k\rangle_X |f(x)\rangle_Y.$$

$$|\Phi\rangle = \frac{1}{Q}\sum_k |k\rangle_X \sum_{x=0}^{Q-1} e^{2\pi i k x/Q} |f(x)\rangle_Y$$

Visi $|K\rangle_X$ ir dažādi un ortogonāli ($k = 0, \ldots, Q-1$).

Starp $|f(x)\rangle_Y$ ir daudz (vismaz $Q/r > r$) identiski vienādo:

$|f(0)\rangle_Y \equiv |f(0+r)\rangle_Y \equiv |f(0+2r)\rangle_Y \equiv \ldots,$
$|f(1)\rangle_Y \equiv |f(1+r)\rangle_Y \equiv |f(1+2r)\rangle_Y \equiv \ldots$ utt.

Savilksim tos kopā un pārgrupēsim (pieņem $Q/r \in \mathbb{Z}$):

$$|\Phi\rangle = \frac{1}{Q}\sum_k |k\rangle_X \sum_{l=0}^{Q/r-1} \sum_{x=0}^{r-1} e^{2\pi i k(lr+x)/Q} |f(x)\rangle_Y =$$

$$= \frac{1}{Q}\sum_k |k\rangle_X \sum_{x=0}^{r-1} e^{2\pi i k x/Q} |f(x)\rangle_Y \boxed{\sum_{l=0}^{Q/r-1} e^{2\pi i k l r/Q}}.$$

Kad apvilktā summa būs maksimāla ?

$$\sum_{l=0}^{Q/r-1} e^{2\pi i k l r/Q} = 1 + q + q^2 + \ldots + q^{Q/r-1},\ q = e^{2\pi i\, kr/Q}$$

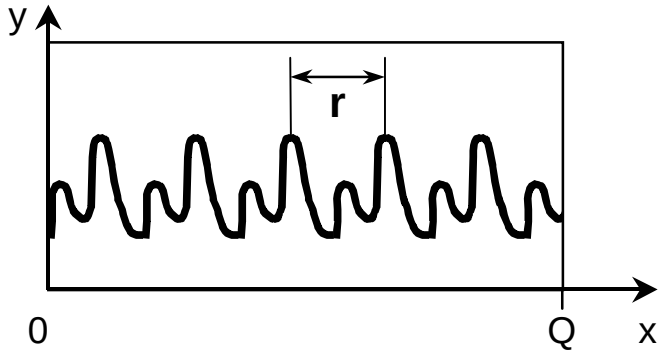
$$\sum_{l=0}^{Q/r-1} q^l = \begin{cases} 1+1+1+\ldots = Q/r, & \text{ja } q = 1, \\ \dfrac{q^{Q/r}-1}{q-1} = \dfrac{e^{2\pi i k}-1}{q-1} = 0, & \text{ja } q \neq 1. \end{cases}$$

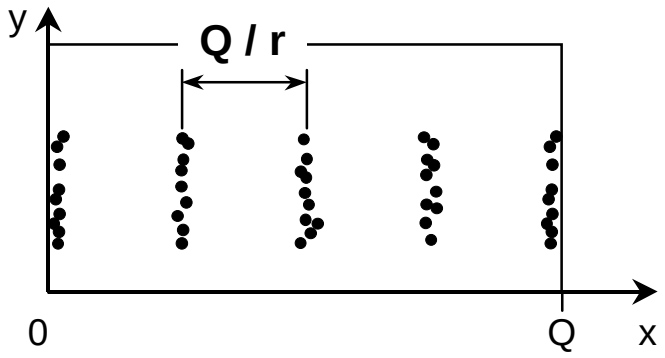
Secinājums.
Pēc QFT reģistru stāvoklī

$$|\Phi\rangle = \frac{1}{Q}\sum_x \sum_k e^{2\pi i k x/Q}|k\rangle_X |f(x)\rangle_Y$$

ar ievērojami $\neq 0$ amplitūdu ieiet tikai tiek $|k\rangle_X$, kuriem

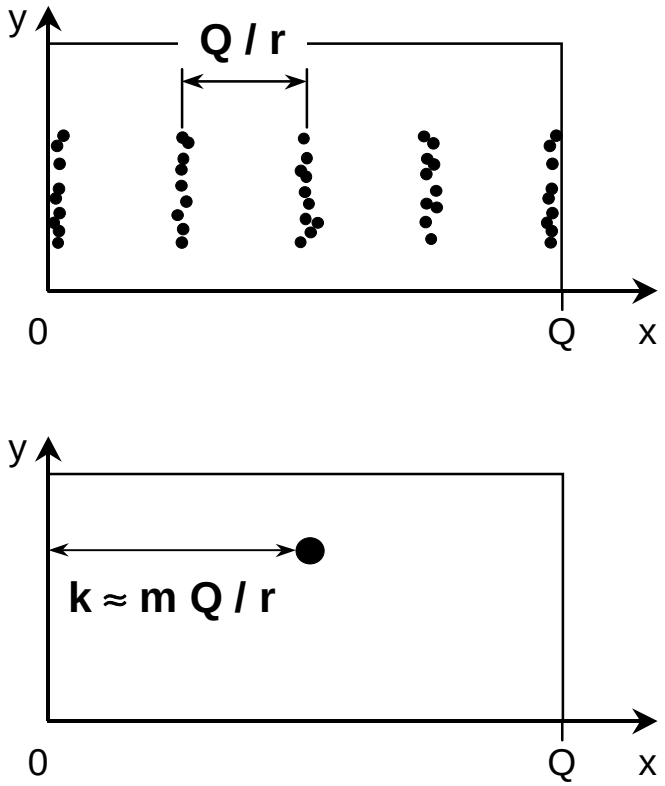
$$e^{2\pi i\, kr/Q} = 1 \Rightarrow \boxed{k = m\frac{Q}{r}, m \in \mathbb{Z}.}$$





5. solis. X reģistru izmērot, iegūst $k = m\frac{Q}{r}$ ar nezināmu, bet veselu m.

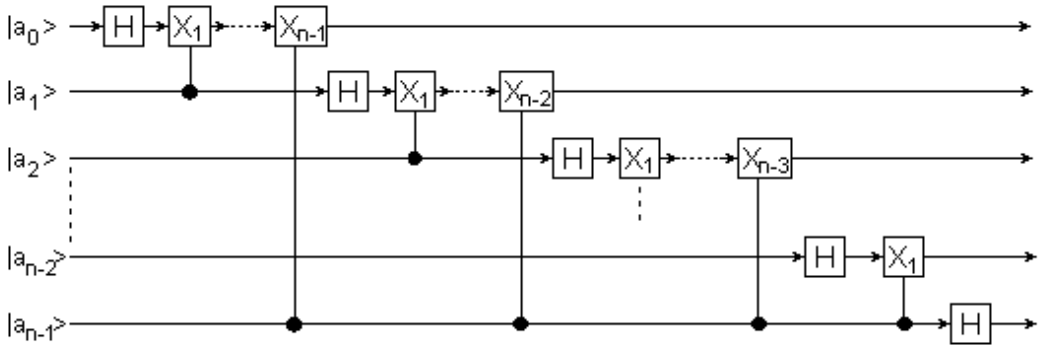
Periodu atrod, uzrakstot k/Q kā racionālu daļu ar saucēju $r < \sqrt{Q}$.



Kvantu Furjē transormācija ir bāzes maiņa

$$|x\rangle \xrightarrow{QFT} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} e^{2\pi i k x/Q} |k\rangle.$$

To var izpildīt ar $O((\log Q)^2)$ loģiskajiem vārtiem.



zīmējums © BS D.Bogdanovs

Klasiskajai FT operāciju skaits $O(Q^2)$,
ātrajai FT — $O(Q \log Q)$.

Kvantu datorikas principi

- ***superpozīcija***
  eksponenciāli daudzu vērtību paralēlā apstrāde

- ***interference***
  vajadzīgā rezultāta pastiprināšana

- ***``sapinums"*** (*entaglment*)
  informācijas nesadalāmība un acumirklīgā lokalizācija

- ***mērījums***
  informācijas neatgriezeniskā zaudēšana,
  izpildot novērojumu

Kvantu datorikas pētniecības virzieni

- Skaitļošanas algoritmu konstruēšana
  - Izskaitļojamības un algoritmu sarežģītības pētījumi
  - Šora faktorizācija
  - Grovera meklēšana

- Informācijas pārraide un kodēšana
  - teleportācija
  - super-blīvā kodēšana (*super dense coding*)
  - kriptogrāfija
  - kļūdu korekcijas kodi

- Kvantu datoru praktiskā realizācija
  - dekoherences un mērījuma dziļāka izpēte
  - *fault tolerant computation*
  - vairāku q-bitu realizācija

Prasības reālajam kvantu datoram

- Glabāšana
  q-bitiem jāsaglabā savs stāvoklis pietiekoši ilgi, lai veiktu mums vajadzīgo skaitļošānu

- Izolācija
  mijiedarbība ar apkārtni ir jāminimizē, izvairoties no dekoherences efektiem

- Nolasīšana
  q-bitiem ir jābūt precīzi izmērāmiem

- Loģika
  mums jāprot kontrolēti iedarboties uz atsevišķiem q-bitiem, lai realizētu kvantu loģiskos vārtus

Strādājošie kvantu datori

- Jonu slazdi (*ion traps*)

  Brīvo jonu ķēde tiek izolēta vakuumā pie ultrazemas T ar elektromagnētisko lauku palīdzību.

  - **q-bits** – jona stacionārā un metastabila ierosinātā stāvokļa superpozīcija
  - **atsevišķas operācijas** – kontrolētas frekvences, lokalizācijas un ilguma lāzeru impulsi
  - **q-bitu mijiedarbība** – jonu ķēdes kolektīvie svārstību stāvokļi (fononi)

- Kodolu magnētiskā rezonanse

  Šķidrā vai kristāliskā viela makroskopiskos daudzumos magnētiskajā laukā pie istabas temperatūras.

  - **q-bits** – kodola spina dažādas orientācijas ārējā magnētiskajā laukā
  - **atsevišķas operācijas** – magnētiskā lauka modulācija, mikroviļņu starojums
  - **q-bitu mijiedarbība** – spinu dipola-dipola un citas elektromagnētiskās mijiedarbība

- Augsta labuma mikroviļņu rezonatori (*high finess microwave cavities, cavity QED*)

  Elektromagnētiskais lauks (fotoni) starp supravadošajiem rezonatora spoguļiem

  - **q-bits** – fotonu polarizācijas stāvokļi, fotonu skaits
  - **q-bitu mijiedarbība** – neitrālo atomu, fotonu iziešana caur rezonatoru.

Cilvēki

Prof., Dr.h.fiz. Mārcis Auziņš,
<mauzins@lanet.lv>, LU FMF Zeļļu ielā 8

Doc., Dr.h.fiz. Boriss Zapols,
<bzapols@lanet.lv>, LU ĶFI Kronvalda ielā 4

Prof., Dr.h.mat. Rūsiņš Freivalds,
LU MII Raiņa bulv. 29

Literatūra

Physics World, March 1998

Kvantu datoriem veltīts žurnāla numurs,
daudzveidīga informācija lasītajam ar kvantu mehānikas pamatzināšanām.

Scientific American, April 2000

Plašai auditorijai veltīts raksts par kvantu teleportāciju

Interneta resursi

http://xxx.lanl.gov/form/quant-ph

Los Alamosa Nacionālās Laboratorijas elektroniskais arhīvs

Jaunākās publikācijas un pārskati, aktīvo pētījumu rezultāti.
vispilnīgākā informācija, bet iesācējam grūti orientēties

http://theory.caltech.edu/people/preskill/ph229/

Kalifornijas Tehnoloģiskā Institūta lekciju kurss kvantu datoros.

Viegli uztverami, plaši (321 lpp.) lekciju konspekti,
saites uz citiem avotiem, uzdevumi ar atrisinājumiem.

Home page of Prof. Anton Zeilinger

Plaša informācija par eksperimentiem ar sapītiem stāvokļiem:
teleportācija, kriptogrāfija uc.
Saities uz citu eksperimentālo grupu lapām.

Uzdevums ieskaitei kvantu datorikā.

a) Pierakstīt matricas formā pāreju no standartbāzes $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ uz Bela bāzi $\{|\Psi^+\rangle, |\Psi^-\rangle, |\Phi^+\rangle, |\Phi^-\rangle\}$ kā operāciju ar divu q-bitu reģistru.
b) Pierādīt, ka punktā a) iegūtā matrica ir unitāra.
c) Izteikt apskatāmo transformāciju ar kontrolētā NOT un viena q-bita operāciju palīdzību.

Bela stāvokļu bāze

$$
\begin{aligned}
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)
\end{aligned}
$$

Visi Bela stāvokļi ir pilnīgi sapīti, informācija ir abu q-bitu *kopējās īpašībās*.

———————

Risinājumus var sūtīt pa e-pastu

Vjačeslavam Kaščejevam <slava@latnet.lv>

vai nodot personīgi CFI 306. telpā.