Tekijöihinjaon kvanttialgoritmi

Vesa Kivistö

Helsinki 14.11.2004

Vaihtoehtoiset laskentaparadigmat -seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Monet laajassa käytössä olevat epäsymmetriset salakirjoitusmenetelmät perustuvat suurten kokonaislukujen tekijöihinjaon laskennalliseen vaikeuteen. Kaikki tunnetut klassiset tekijöihinjaon algoritmit ovatkin suoritusajaltaan ylipolynomisia syötteen kokoon nähden ja kryptologien keskuudessa uskottiin yleisesti että suoritusajaltaan polynomista algoritmia ei voida kehittää.

Vuonna 1994 Peter Shor kuitenkin esitteli tekijöihinjaon kvanttialgoritmin, joka suurella todennäköisyydellä antaa oikean vastauksen ja joka on suoritusajaltaan polynominen syötteen kokoon nähden. Shorin tekijöihinjaon kvanttialgoritmi oli ensimmäinen konkreettinen todiste kvanttialgoritmien tuomasta eksponentiaalisesta suoritusnopeuden lisäyksestä klassisiin algoritmeihin nähden. Tämän seurauksena kiinnostus kvanttilaskennan kehittämiseen nousi aivan uudelle tasolle.

Tämän työn tarkoituksena on esitellä pääpiirteissään Shorin tekijöihinjaon kvanttialgoritmia ja siihen liittyvää formalismia. Lukijalta edellytetään kvanttilaskennan [Mal04] ja numeroteorian perusteiden hallintaa.

Luvussa 2 esitellään Hadamard ja Walsh-Hadamard kvanttiportit. Luvussa 3 esitellään Fourier-muunnoksen kvanttiversio. Luvussa 4 käydään yksityiskohtaisesti läpi Shorin tekijöihinjaon kvanttialgoritmi. Luvussa 5 analysoidaan Shorin tekijöihinjaon kvanttialgoritmin laskennallista vaativuutta. Luku 6 on lyhyt yhteenveto.

2 Hadamard ja Walsh-Hadamard kvanttiportit

Toisin kuin klassiset portit, kvanttiportit operoivat tilojen superpositoilla. Kaikki kvanttiportit voidaankin määritellä unitaarisina lineaaritransformaatioina [Mal04, RiP00].

Eräs tärkeimmistä yhtä kvanttibittiä käsittelevistä kvanttiporteista on Hadamard kvanttiportti.

H:

$$|0> \rightarrow \frac{1}{\sqrt{2}}(|0>+|1>)$$

$$|1> \rightarrow \frac{1}{\sqrt{2}}(|0>-|1>)$$

Hadamard kvanttiportti siis muuntaa puhtaan perustilan kahden perustilan superpositioksi, joilla on mitattaessa kummallakin yhtä suuri esiintymistodennäköisyys. Mikäli mittausta ei suoriteta ja superpositio syötetään uudestaan läpi Hadamard kvanttiportista, tuloksena on konstruktiivisen ja destruktiivisen interferenssin seurauksena alkuperäinen puhdas perustila [Hir02].

H_2:

$$|0> \rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0>+|1>)+\frac{1}{\sqrt{2}}(|0>-|1>)\right) = |0>$$

$$|1> \rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0>+|1>)-\frac{1}{\sqrt{2}}(|0>-|1>)\right) = |1>$$

Jos n kappaletta perustilaista kvanttibittiä muunnetaan yksi kerrallaan Hadamard kvanttiportilla superpositioihinsa, tuloksena on superpositio kaikista mahdollisista yhdistetyistä tiloista. Näitä tiloja on kaikkiaan 2^n kappaletta ja tilojen superpositio voidaan mieltää binääriesitykseksi luvuille 0 .. 2^n-1.

Walsh-Hadamard kvanttiportti suorittaa Hadamard transformaation n kappaleelle kvanttibittejä. Tämä voidaan määrittää rekursiivisena tensorifunktiona

$$W_1 = H$$
$$W_{i+1} = H \otimes W_i$$

3 Kvanttimekaaninen Fourier-muunnos

Fourier-teoreeman mukaan mielivaltaisen muotoinen funktio voidaan esittää eritaajuisten siniaaltofunktioiden summana [Bro00, Hir02]. Näiden sinimuotoisten perusfunktioiden tekijät voidaan mieltää omaksi funktiokseen, alkuperäisen funktion Fourier-muunnokseksi. Fourier-muunnoksen ideana on saada selville alkuperäisen funktion sisältämien sinimuotoisten perusfunktioiden taajuudet. Fourier-muunnoksessa jakson r omaava funktio muuntuu siten että funktiolla on nollasta poikkeava arvo vain taajuuden $\frac{2\pi}{r}$ moninkertojen kohdalla.

Diskreetissä Fourier-muunnoksessa tarkasteluväli on jaettu N kappaleeseen yhtä suuria näytealueita. Tällöin perusjakson r omaava alkuperäinen funktio muuntuu siten että funktiolla on nollasta poikkeava arvo vain N/r moninkertojen kohdalla, jos jako menee tasan. Jakojäännöstapauksessa nollasta poikkeava arvo esiintyy lähimpien kokonanaislukujen kohdalla.

Nopea Fourier-muunnos on diskreetti Fourier-muunnos, jossa N on numeron kaksi jokin potenssi.

Kvanttimekaaninen Fourier-muunnos on sovellus nopeasta Fourier-muunnoksesta, joka operoi kvanttitilojen amplitudeilla

$$\sum_x g(x)|x> \ \rightarrow \ \sum_c G(c)|c>$$

jossa G(c) on g(x):n diskreetti Fourier-muunnos. Muuttujien x ja c arvot ovat binäärilukuesityksiä ja liikkuvat välillä 0..N-1. Jos tila mitataan Fourier-muunnoksen jälkeen, todennäköisyys mittaustulokselle $|c>$ on $|G(c)|^2$.

Koska kvanttimekaaninen Fourier-muunnos on sovellus nopeasta Fourier-muunnoksesta, antaa se vain aproksimoituja tuloksia jos jakso ei ole numeron kaksi jokin potenssi. Suuremmilla numeron kaksi pontenssiarvoilla aproksimaation tarkkuus luonnollisesti paranee.

Kvanttimekaaninen Fourier-muunnos U_{QFT} jossa $N=2^m$ voidaan määrittää seuraavasti [Hir01, Hir02, RiP00]

$$U_{QFT}: \quad |x> \ \rightarrow \ \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} \mathrm{e}^{\frac{2\pi icx}{2^m}} |c>$$

4 Tekijöihinjaon kvanttialgoritmi

Tekijöihinjaon algoritmilla pyritään selvittämään kokonaisluvun M alkulukutekijät p ja q

$$M = pq$$

Kaikki tunnetut klassiset tekijöihinjaon algoritmit ovat suoritusajaltaan ylipolynomisia syötteen kokoon nähden. Shorin vuonna 1994 kehittämä tekijöihinjaon kvanttialgoritmi antaa suurella todennäköisyydellä oikean vastauksen ja on polynominen syötteen kokoon nähden.

Shorin tekijöihinjaon kvanttialgoritmi perustuu siihen että suoran tekijöihinjaon sijasta tutkitaan potenssisarjojen jaksollisuutta. Tässä voidaan hyödyntää kvanttimekaanista rinnakkaisuutta ja saavuttaa eksponentiaalinen nopeutus klassisiin algoritmeihin nähden.

Luvuissa 4.1 – 4.7 [RiP00, Hir02] esitellään tekijöihinjaon kvanttialgoritmi pääpiirteissään.

4.1 Muuttujien alustus

Valitaan kokonaisluku a satunnaisesti väliltä $0..M$ ja tarkistetaan Euklideen algoritmilla [Sta98] mikä on a:n ja M:n suurin yhteinen tekijä. Jos suurin yhteinen tekijä on suurempi kuin yksi, niin M:n tekijä on löydetty ja algoritmin suoritus voidaan lopettaa. Muussa tapauksessa jatketaan eteenpäin.

Valitaan kokonaisluku m siten että $M^2 < 2^m < 2M^2$

4.2 Rekisterien alustus

Varataan rekisterille R1 tilaa m kvanttibittiä. Rekisteriin alustetaan Walsh-Hadamard kvanttiportilla superpositio kaikista mahdollisista tiloista. Rekisterin sisältö voidaan nyt mieltää superpositioksi kaikista numeroista välillä $0..2^m-1$.

Varataan rekisterille R2 tilaa $ceil(\log_2 M)$ kvanttibittiä. Rekisterin kaikki kvanttibitit alustetaan tilaan $|0>$.

4.3 Potenssisarjan laskeminen

Annetaan rekisterin R1 sisältö syötteenä polynomisessa ajassa toimivalle kvanttipiirille F, joka laskee arvon $f(x)=a^x \bmod M$ ja tallettaa sen rekisterin R2 sisällöksi. Muuttuja x on rekisterin R1 sisältämän luvun arvo.

Koska x on superpositio kaikista mahdollisista arvoista, rekisterissä R2 on superpositio kaikista mahdollista f(x):n arvoista. Transformaation F seurauksena rekisterien R1 ja R2 superpositiot ovat nyt sitoutuneita.

4.4 Rekisterin R2 mittaaminen

Koska rekisterit R1 ja R2 ovat sitoutuneita, vaikuttaa toisen rekisterin mittaaminen myös toiseen rekisteriin.

Mitataan rekisterin R2 sisältö, jolloin rekisterissä oleva superpositio romahtaa satunnaisesti arvoon u. Arvo u ei itsessään ole oleellinen ja se voidaan unohtaa samantien. Rekisterin R2 mittauksen seurauksena rekisterin R1 sisältö muuttuu siten että rekisteriin jää superpositio x:n arvoista joista F on voinut laskea arvon u. Rekisterin R2 mittaaminen on siis projisoinut rekisterin R1 superposition vastaamaan mitattua arvoa u.

$$C\sum_x g(x)|x,u>$$

jossa C on jokin skaalauskerroin ja

$$g(x)=1 \quad jos\ f(x)=u$$
$$g(x)=0 \quad jos\ f(x)\neq u$$

4.5 Kvanttimekaaninen Fourier-muunnos ja potenssisarjan jakson laskeminen

Erillinen polynomisessa ajassa toimiva kvanttipiiri toteuttaa kvanttimekaanisen Fourier-muunnoksen rekisterin R1 sisällölle.

$$\sum_x g(x)|x> \ \rightarrow \ \sum_c G(c)|c>$$

Mitataan rekisterin R1 sisältö, jolloin rekisterissä oleva superpositio romahtaa arvoon v. Jos jakso on numero kahden jokin potenssi, niin

$$v = j\frac{2^m}{r}$$

jossa j on jokin sopiva kerroin. Jos jakso ei ole numero kahden jokin potenssi, niin jaksoa voidaan yrittää arvata käyttämällä jatkuvan tekijöinnin laajennusmenetelmää [RiP00].

4.6 Tekijän laskeminen

Jos jakso r on parillinen, asetetaan $p_1 = a^{(r/2)}+1$ ja $p_2 = a^{(r/2)}+1$. Selvitetään Euklideen algoritmilla onko joko $p_1 : llä$ tai $p_2 : lla$ ykköstä suurempi yhteinen tekijä M:n kanssa. Tulos on suurella todennäköisyydellä kyllä, koska on epätodennäköistä että tutkittavien lukujen jokin moninkerta olisi tasan M. Jos suurin yhteinen tekijä löytyy, on se luonnollisesti tekijä luvulle M.

4.7 Algoritmin toistaminen vikatilanteessa

Algoritmin suoritusaikana voidaan joutua erilaisiin virhetiloihin, jonka seurauksena M:n tekijän laskeminen epäonnistuu:

1) Arvo v ei ollut tarpeeksi lähellä arvoa $j\frac{2^m}{r}$
2) Jaksolla r ja kertoimella j voi olla yhteinen tekijä, jonka seurauksena r olikin jakson tekijä eikä itse jakso.
3) Luvun tekijäksi voi tekijän laskemisvaiheessa tulla luku M.
4) Jakso r on pariton

Koska jokin voi mennä vikaan algoritmin suorituksen aikana, antaa algoritmi oikean tekijän vain tietyllä todennäköisyydellä. Tekijän löytymisen todennäköisyyttä voidaan rajattomasti parantaa toistamalla algoritmia uudestaan.

5 Tekijöihinjaon kvanttialgoritmin laskennallinen vaativuus

Muuttujien alustusvaiheessa ja tekijän laskemisessa suoritettava Euklideen algoritmi on laskennalliselta vaativuudeltaan luokkaa

$$O(l(N)^3)$$

Rekisterin R1 alustuksessa käytettävä Walsh-Hadamard transformaatio on luokkaa

$$O(l(N))$$

Potenssisarjan laskemisessa käytettävä algoritmi on luokkaa

$$O(l(N)^3)$$

Kvanttimekaaninen Fourier-muunnos on luokkaa

$$O(l(m)^3)$$

Jakson laskemisessa käytettävä algoritmi on luokkaa

$$O(l(N)^3)$$

Koko algoritmin laskennallinen vaativuus on siis luokkaa

$$O(l(N)^3)$$

Tällöin onnistumistodennäköisyys on vähintään luokkaa

$$\Omega(\frac{1}{\log\log N}) = \Omega(\frac{1}{\log(l(N))})$$

Suuri onnistumistodennäköisyys saavutetaan jos algoritmi suoritetaan $\log(l(N))$ kertaa.

Tällöin melko varmasti onnistuvan algoritmin vaativuus on on luokkaa

$$O(l(N)^3 \log(l(N)))$$

6 Yhteenveto

Shorin tekijöihinjakoalgoritmi järkytti kryptologeja, koska se näyttää ainakin teoriassa mahdollistavan suurten kokonaislukujen tekijöihinjaon polynomisessa ajassa. Koska suuri osa nykyisin käytettävistä epäsymmetrisistä salakirjoitukseen ja digitaalisiin allekirjoituksiin käytettävistä algoritmeista perustuu tekijöihinjaon oletettuun vaikeuteen, on asialla melko paljon taloudellista, sotilaallista ja poliittista merkitystä.

Shorin suuri oivallus kvanttialgoritminsa suunnittelussa oli suoran tekijöiden etsinnän sijasta hyödyntää potenssisarjojen jakson etsimistä, joka on läheisesti sidoksissa tekijöiden etsintään. Tällöin kvanttialgoritmi tarjoaa eksponentiaalisen nopeuden lisäyksen klassisiin algoritmeihin verrattuna, koska superpositiossa olevan potenssisarjan kvanttitilan romahtaminen yhteen arvoon jättää syöteavaruuteen vain romahtanutta tilaa vastaavat alkuarvot.

Aidosti isoja kokonaislukuja tekijöihinsä jakava kvanttitietokone on todennäköisesti vielä kaukana tulevaisuudessa ja ei ole ylipäänsä selvää osataanko sellaista koskaan rakentaa.

Lähteet

Bro00 Brown, J., The Quest for the Quantum Computer. Simon & Schuster, Yhdysvallat 2000.

Hir01 Hirvensalo, M., Quantum Computing, Springer-Verlak, Saksa 2001, 42-62.

Hir02 Hirvensalo, M., Quantum computing – Facts and folklore. Natural Computing, Kluwer Academic Publishers, Alankomaat 2002, 135-155.

Mal04 Malinen, J., Kvanttilaskennan perusteet. Helsingin yliopistossa syksyllä 2004 pidetyn vaihtoehtoiset laskentaparadigmat seminaarikurssin oppilastyö, 2004.

RiP00 Rieffel, E., Polak, W., An Introduction for Quantum Computing for Non-Physicists. ACM Computing Surveys, 32(3) 2000, 300-335.

Sta98 Stallings, W., Cryptography and Network Security. Prentice Hall, Yhdysvallat 1998, 208-233.