11 Kvanttilaskenta

Jan Lindström

Kvanttilaskennassa pyritään kehittämään uusia järjestelmiä ja tekniikoita tiedon käsittelyyn ja tietoliikenteeseen käyttäen kvanttiteoriaa. Käyttämällä kvanttimekaniikkaa tietoa voidaan koodata sekä kvanttimaterian tiloihin tai valoon että käsitellä ennennäkemättömällä nopeudella ja tehokkuudella.

MÄÄRITELMÄ 11.1 *Qubit on kvanttitila $|\gamma\rangle$ muotoa:*

$$|\gamma\rangle = \alpha|0\rangle + \beta|1\rangle,$$
$$\textit{missä } \alpha, \beta \in \mathbf{C} \textit{ ja } \parallel \alpha \parallel^2 + \parallel \beta \parallel^2 = 1.$$

Yllä oleva määritelmä jättää qubitin tosiasiallisen median kokonaan määrittelemättä. Tosiasiassa määritelmän kannalta ei ole tärkeää onko qubit koodattu protonien polarisaatioon, atomin spin:iin, atomin energiatiloihin tai muuhun menetelmään. Tässä esityksessä oletamme, että jotain menetelmää on käytetty.

Suurin ero qubitin ja klassisen bitin välillä on se, että klassinen bitti voi olla asetettuna vain joko 1:ksi tai 0:ksi, kun taas qubit voi olla missä tahansa (äärettömän monessa) kvanttiylitilassa (quantum superposition). Siis ääretön määrä informaatiota voidaan teoriassa koodata yhteen qubittiin sopivasti valitsemalla värähtelytaajuudet (amplitudes) α ja β. Valitettavasti kaikkea mitä voidaan tallettaa ei voida lukea. Kvanttimekaniikka sisältää tarkat säännöt kuinka kvanttitilasta voidaan lukea. Jätän tämän osuuden lukian mielenkiinnon varaan, koska se vaatisi Hilbertin avaruuksiksi kutsutun matemaattisen mallin tietämystä. Kvanttilaskenta normaalisti käyttää useampaan kuin yhtä qubittia.

MÄÄRITELMÄ 11.2 *Kvanttirekisteri on järjestetty joukko äärellisen monta qubittia.*

ESIMERKKI 11.3 *Kvanttirekisteri, joka koostuu kolmesta qubitista voi tallettaa tiettynä hetkenä kaikki kahdenksan numeroa* $000, 001, ...111$ *kvanttiylitilassa. Yleisesti kvanttirekisteri, jossa on L qubittia voi tallettaa 2^L numeroa samanaikaisesti.*

Teoriassa tiedetään kuinka kvanttitietokone rakennetaan. Aloitetaan yksinkertaisista loogisista kvanttipiireistä ja yhdistetään ne kvanttiverkoksi. Looginen kvanttipiiri vastaa klassista loogista piiriä. Looginen piiri on yksinkertainen laskentalaite, joka suorittaa yhden alkeisoperaation yleensä kahdella qubitilla. Itse asiassa yhden qubitin piirit yhdessä erittäin yksinkertaisen kahden qubitin piirin (kvanttikontrolloitu NOT) kanssa riittävät toteuttamaan kvanttiverkon mihin tahansa laskentaan.

Kvanttilaskennassa on myös omat ongelmansa. Mitä enemmän qubitteja on sitä vaikeammaksi tulee muodostaa oikea yhteistyö qubittien välillä tarvittavan laskennan suorittamiseen ja tulosten selvittämiseen. Paljon pahempi ongelma on kuitenkin estää kvanttikoneen ympäristön vaikutus kvanttilaskentaa. Mitä enemmän komponentteja on sitä todennäköisemmin kvantti-informaatio leviää kvanttikoneen ulkopuolella ja häviää ympäristöön pilaten laskennan. Tätä ilmiötä kutsutaan decoherenceski.

Yksi ratkaisu on käyttää kvanttivirheenkorjausta. Teoriassa siis laskenta voidaan suorittaa oikein, joten en puutu ongelmiin tai virheenkorjaukseen.

LAUSE 11.4 *(Lecerf,1963-Bennet,1973): Jokaiselle Turingin koneelle M, joka laskee funktion f ajassa O(t) on olemassa käännettävissä oleva Turingin kone T, joka laskee parin* $< x, f(x) >$ *syötteellä x ajassa* $c * O(t)$, *c vakio. Laskenta käytää tilaa polinomiaalisesti suhteessa* $|x|$, *mutta kaikki laskennan* $< x, f(x) >$ *käyttämät työnauhan nauhapaikat ovat tyhjentyneet (käännettävyys) [6, 2]* □.

Käännettävä Turingin koneessä millä laskennan hetkellä tahansa kaksi operaatiota ovat mahdollista: jatketaan laskentaan eteenpäin yhden askeleen tai perutaan edellinen askel. Täsmällisempi määritelmä löytyy lähteestä [5]. Benioff [1] ja Deutsch [3] ovat osoittaneet, että kvanttikone voi suoraan simuloida käännettävää Turingin konetta. Koska kvanttikoneet ovat käännettäviä, saamme seuraavan korollaarin:

KOROLLAARI 11.5 *Turing laskettava funktio f on aina laskettavissa kvanttipiireillä (häviävän pienellä aikasakolla).*

MÄÄRITELMÄ 11.6 *Kvantti-Turing kone on kolmikko*

$$(Q, \sigma, \rho),$$

missä

$Q = q_0, q_1, ..., q_h$ *on äärellinen joukko tiloja,*

σ *on äärellinen aakkosto, ja*

ρ *on siirtymäfunktio.*

Siirtymäfunktio $\rho(p, \sigma, \tau, q, d)$ *antaa kompleksisen värähtelytaajuuden,*

jossa kone tilassa p lukee merkin τ*, kirjoittaa merkin* σ

, siirtyy tilaan q ja kulkee suuntaan d*.*

Laskenta alkaa alkutilanteesta q_0 ja työnauhat ovat tyhjiä. Laskenta eteneen seuraten siirtymäfunktion sääntöjä. Erikoista on se, että kone ei siirrykkään vain yhteen suoraan seuraavaan tilaan vaan kvantti-Turing kone siirtyy yhdessä laskenta-askeleessa kaikkiin suoraan seuraaviin konfiguraatioihin.

Näyttäisi siltä, että klassinen Turingin kone ja kvantti-Turing kone tunnistavat samat kieliluokat. Klassinen Turingin kone voi simuloida kvantti-Turing konetta ja päinvastoin. Kuitenkin, kuten edellä havaittiin, kvantti-Turing kone voi ratkaista ongelmia nopeammin kuin klassinen Turingin kone.

MÄÄRITELMÄ 11.7 *EQP = kielet, jotka voidaan ratkaista kvanttikoneella täsmälleen polynomisessa ajassa.*

LAUSE 11.8 $P \subseteq EQP$ *(* $P \subsetneq EQP$ *?)*
. Siis $P \subseteq EQP \subseteq PSPACE$*. Lisäksi voidaan osoittaa, että* $\exists X \subseteq \Sigma^* s.e. P^X \subsetneq EQP^X$*. Vastaavasti pätee:* $\exists Y \subseteq \Sigma^* s.e. EQP^Y \not\subseteq NP^Y$*.*

MÄÄRITELMÄ 11.9 *BPP = kielet, joille on olemassa* $\epsilon \in]0, 1/2[$ *ja joille on olemassa probabilistinen Turingin kone M s.e.* $\forall x Prob[M(X)$ *oikein* $] > 1/2 + \epsilon$*.*

MÄÄRITELMÄ 11.10 *BQP = kielet, joille on olemassa* $\epsilon \in]0, 1/2[$ *ja joille on olemassa Kvantti-Turingin kone M s.e.* $\forall x Prob[M(X)$ *oikein* $] > 1/2 + \epsilon$*.*

LAUSE 11.11 *(Simon,1995): On olemassa oraakkeli, jonka suhteen ongelma on ratkaistavissa polynomisessa ajassa kvanttikoneella, mutta probabilistinen Turingin kone rajoitetulla vir-*

hetodennäköisyydellä, joka väittää ratkaisevan saman ongelman käyttäen oraakkelia tarvitsee exponentiaalisen ajan äärettömän moneen syötteeseen [10].

Simonin lause on vahvin argumentti kvanttikoneiden vahvuuden puolesta Turingin koneita kohtaan.

ESIMERKKI 11.12 *(Shor,1996): Jokainen kokonaisluku voidaan muodostaa kahden alkuluvun tulona. Operaatiota kutsutaan kokonaisluvun tekijöihin jaoksi. Tekijöihin jako on tärkeä ongelma tietojenkäsittelytieteessä. Tehokkain tiedetty tekijöihinjakoalgoritmi on number field sieve [7, 8], joka vie asymptoottisesti aikaa $exp(c(logn)^{1/3}(loglogn)^{2/3})$, jollain vakiolla c, mikä on eksponentiaalinen. Shorin [9] kehittämä kvanttitekijöihin jakoalgoritmi vie asympttottisesti $O((logn)^2(loglogn)(logloglogn))$ askelta kvanttikoneella ja $O(logn)$ askelta klassisella koneella. Ongelma voidaan ratkaista probabilistisella Turingin koneella ja oraakkelilla seuraavalla algoritmillä:*

```
PROGRAM One-Factor( syöte: n pariton kokonaisluku)
x := random {0,...,n}
r := käytä oraakkelia löytämään order of x ( mod n)
Tulos: jos r on pariton tai x_{r/2} ≡ −1 ( mod n), hylkää syöte
muuten palauta gcd(x_{r/2} − 1, n).
```

Satunnaisluvun x valinta väliltä $(0, ..., n)$, modulaarinen potenssiinkorotus ja suurimman yhteisen tekijän etsiminen voidaan kaikki tehdä polinomisessa ajassa. Toistamalla algoritmia polynomisen monta kertaa saadaan täydellinen n:n tekijöihin jako. Shor esitti tehokkaan kvanttialgoritmin, joka etsii order of elementin. Eli oraakkelikutsu on korvattu kvanttialgoritmikutsulla.

ESIMERKKI 11.13 *(Glover, 1996): Tietyn avainarvon hakeminen lajittelemattomasta tietokannasta, jossa on N alkiota vie keskimäärin $N/2$ askelta. Glover [4] on löytänyt kvanttialgoritmin, joka ratkaisee ongelman $O(\sqrt{N})$ askeleella.*

Viitteet

[1] P. A. Benioff. Quantum mechanical hamiltonian models of turing machines. *Journal of statistical Physics*, 29(3):515–546, 1982.

[2] C. H. Bennett. Logical reversibility of computations. *IBM Journal of Res. Develop.*, (17):525–532, 1973.

[3] D. Deutsch. Quantum theory, the Curch-Turing principle and the universal quantum computer. *Proc. of the Royal Society, London*, (A400):97–117, 1985.

[4] L. Glover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28nd Annual ACM Symposium on the Theory of Computation*, pages 212–219, 1996.

[5] R. Landauer. Irreversability and heat generation in the computing process. *IBM Journal of Res. Develop.*, (5):183, 1961.

[6] A. Lecef. Machines de turing reversibles. *Comptes rendus de l'academie francaise des sciences*, 257:2597–2600, 1963.

[7] A. K. Lenstra and H. W. Lenstra Jr. The devellopment of the number field sieve. (1554), 1993.

[8] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse, and J. M. Pollard. The number field sieve. In *Proc. of the 22nd Annual ACM Symposium on the Theory of Computation*, pages 564–572, 1990.

[9] P. W. Shor. Algorithms for quantum computation: Discrete log and factoring. In *Proc. of the 35th IEEE Symposium on Foundations of Computer Science*, pages 20–22, 1994.

[10] D. Simon. On the power of quantum computation. In *Proc. of the 35th IEEE Symposium on Foundations of Computer Science*, pages 116–123, 1994.