

Veijo Hänninen

Tavoitteena kvanttietokone

Millalle

Tavoitteena kvanttietokone

Veijo Hänninen

© 2018 Veijo Hänninen

Kustantaja: BoD™ – Books on Demand, Helsinki, Suomi

Valmistaja: Books on Demand GmbH, Norderstedt, Saksa

ISBN: 978-951-568-005-1

SISÄLLYSLUETTELO

KVANTTITIETOKONE	5
SOVELLUKSIA JA OHJELMOINTIA.....	13
KUBITIT JA KUDITIT	17
KÄYTÄNNÖN KUBITTEJA	21
SUPRAJOHTAVIA KUBITTEJA	27
KOHTI PIITEKNIKKAA.....	31
TOPOLOGISET KUBITIT.....	39
TIMANTTISET VAKANSSIT JA KUBITIT	44
FOTONIT ja MUISTIT	46
VIRHEENKORJAUS.....	51
D-WAVE	56
KEHITTÄJIÄ JA HYBRIDEITÄ	60
SIMULOINTI.....	67
SALAUUS JA SEN PURKU.....	71
KILPAILEVIA VAIHTOEHTOJA	77
KVANTTITULEVAISUUDEN NÄKYMIÄ.....	79
UUSIA ULOTTUVUUKSIA	81

KVANTTITIETOKONE

Mullistus vai ei

Kvanttitietokone on herättänyt vahvaa kiinnostusta, varsinkin sen suhteen, että se kykenisi purkamaan nykyisin laajasti käytetyt tietoturvamenettelyt eli Internetin salaustekniikan.

Luonnollisesti sekin, että mennään yhä syvemmälle kvanttimaailmaan kiinnostaa erityisesti tutkijoita ja tieteilijöitä.

Aihe esiintyy ajoittain myös tietotekniikan käyttäjien keskuudessa mutta miten aihe tällä hetkellä edistyy ja on tämän kirjan teema.

Tutkijapiireissä kvanttitietokoneen tuloon uskotaan aika vahvasti. Osittain voidaan sanoa että se on jo todellisuutta mutta tuleeko se olemaan sitä tasolla jolle sitä eniten hehkutettiin.

Kvanttirajoista kvanttiavaruuteen

Elektroniikka ja tietotekniikka sukeltavat nykyään yhä syvemmälle kvanttimaailmaan.

Aikoinaan ajateltiin, että kvanttimekaniikka on itse asiassa eräänlainen raja tietotekniikan kehitykselle koska komponenttien jatkuvasti pienetessä ne saavuttavat kvanttimaailman hauraat ilmiöt.

Vuonna 1985 teoreettinen fyysikko David Deutsch Oxfordin yliopistosta käänsi asetelman kuitenkin päälaelleen. Hän osoitti, että kvanttimekaniikka ei suinkaan rajoita laskentaa vaan laajentaa sitä häikäisevällä tavalla.

Kun tavallisen tietotekniikan piiritekniiikan etu on komponenttitiheys, kvanttikoneen etu ei ole niinkään kubittien tiheys vaan mahdollisuus operoida kvanttitilojen superpositioilla. Toki kvanttikoneenkin toiminnan perustaa voi tavoitella vaikkapa vain yhden atomin tasolla.

Laskenta-avaruus

Kvanttifysiikkaan kuuluu käsite Hilbertin avaruus, joka on eräänlainen ”tilojen” avaruus. Vaikka klassinen tila-avaruus on avaruudellisesti rajaton, siinä kuitenkin aika virtaa vain yhteen suuntaan. Fyysikko Robert Penrosen ilmaisemana ”Hilbertin avaruus on sama kuin maailmankaikkeus, jossa aika ja kaikki muut mahdolliset vektorit virtaavat kaikkiin mahdollisiin suuntiin”. Tällaisesta lisävapausasteista saadaan huikea bonus ja sen ansiosta kvanttietokone laskee joitakin asioita erittäin nopeasti. Se nimittäin pääsee äärettömän paljon suurempaan avaruuteen – Hilbertin avaruuteen – kuin klassinen kone, jonka avaruus on yksiulotteinen jono.

Laskentatapa

Perinteiset tietokoneet laskevat askel askeleelta, tavalla jota sanotaan sarjalaskennaksi. Ne voivat myös jakaa laskentatyön laskemalla erikseen vaikkapa ykköset, kymmenet, sadat ja tuhannet ja laskea sitten tulokset lopussa yhteen. Tällaiseen rinnakkaislaskentaan kuluva aika jaetaan osallistuvien osuuksien kesken.

Mutta kvanttietokoneet toimivat massiivisen rinnakkaislaskennan menetelmällä. Nopea rinnakkainen logiikkaoperaatioiden toteutus saavutetaan superposition tiloilla.

Tavallisissa tietokoneissa hyödynnetään transistoriperustaisia logiikkaportteja, jotka ovat pitkin piirilevyllä olevia piirejä. Kvanttilogiikan portit toimivat kubittitilojen superpositioilla. Eli eräänlaisilla avaruudellisilla tiloilla.

Kun Deutch kehitti massiivisen rinnakkaislaskennan, hän tajusi se olevan periaatteessa loistava ja vahva ratkaisu, joka hakee sopivia ongelmia.

Niiden etsimisessä onkin sitten oma työnsä sopivan algoritmin luomiseksi.

Dekoherenssi

Vaikka kvanttilaskenta on tehokasta se on myös teknisesti ristiriitaista. Kvanttilaskennan ne ominaisuudet jotka tekevät siitä erittäin tehokkaan, tekevät siitä myös poikkeuksellisen haavoittuvan.

Kvanttilaskennan ydintä on lomittuminen. Sen ansiosta kubitteja ja niiden yhdistelmiä voidaan käsitellä yhtenä yksikkönä, koska ne liittyvät erottamattomasti toisiinsa.

Mutta sellainen on myös erittäin herkkä ulkoisen ympäristön ei-toivotuille häiriöille. Häiriöt voivat romahduttaa koko lomittuneiden kubittien ketjun jonoksi perinteisiä satunnaisia bittejä jolloin alkuperäinen laskentatavoite on menetetty.

Kehitys uhkasi jopa kaatua tähän ongelmaan. Mutta kehittäjät hyväksyivät esimerkiksi kohinasta johtuvien virheiden välttämättömyyden ja keksivät virheiden korjaamisen erilaisia keinoja.

Koska laskentavoima on niin vahva, virheenkorjaukseen voidaan uhrata paljonkin resursseja eli kubitteja.

Monimutkainen laitteisto

Kvanttitietokoneiden nykyiset kokeelliset toteutukset perustuvat monenlaisiin ratkaisuihin. Periaatteessa riittää kaksitilainen fyysinen järjestelmä kubittien muodostamiseksi. Teknisesti vaikein osuus on pitää kubitit ja niistä luodut erilaiset tilat eristettynä ulkoisista häiriöistä sillä muuten kubittien kvanttimekaaniset ominaisuudet menetetään. Eräs tässä auttava perusratkaisu on pitää kubittien lämpötila hyvin lähellä absoluuttista nollaa.

Kubittien tilojen muokkaamiseen voidaan käyttää esimerkiksi lasereita sekä tarkkoja mikroaaltoja ja/tai muita sähkömagneettisia aaltoja mutta uusimmissa ratkaisuissa ohjaukset tapahtuvat jännitteillä.

Näin monimutkaisten toimintojen ohjailuun tarvitaan tietenkin perinteistä ohjaustekniikkaa kuten myös kvanttilaskennan syötteiden antoon ja tulosten lukemiseen.

Miten kvanttilaskenta toimii?

Kvanttikoneen toiminnan perusyksikkö on kubitti. Se voi olla mikä tahansa kaksitilainen kvanttisysteemi. Sellaisia ilmenee muun muassa atomeissa, elektroneissa, fotoneissa tai suprajohtavissa liitoksissa. Idea on, että niiden kaksi tilaa voidaan saada superpositiotilaan.

Digitaalinen bitti on **1 tai 0**. Analoginen bitti voi saada minkä tahansa arvo välillä 0 ja 1. Esimerkiksi jokin arvo säätösuureessa 0 – 1 voltia, jollain resoluutiolla.

Kubitit on arvojen 0 ja 1 superpositio ja se voidaan ilmaista vektorilla sähkömiehille tutun imaginääriluvun tapaan mutta kaksitasoisesta koordinaatiosta poiketen pallomaisessa avaruudessa.

Joten kubitit voi olla kahden tilan superpositiossa, ja kun se mitataan, se palauttaa toisen kahdesta tilasta perustuen kunkin tilan todennäköisyyteen ja se saa arvon 0 tai 1.

Yhdellä kubitilla ei vielä tehdä mitään laskentaa vaan sitä varten tarvitaan keskenään vuorovaikutuksessa olevia kubitteja. Tällöin niiden sanotaan olevan lomittuneita ja vasta niiden kautta varsinainen rinnakkainen laskenta tapahtuu.

Kun kaksi kubitia tulevat lomittuneiksi ja jos mittaamme ensin yhden ja saamme ylös-spinin silloin toinen antaa alas-spinin ja päinvastoin. Siksi kunnes mittaamme ne, näitä kahta kubitia voidaan pitää vain yhtenä järjestelmänä jolla on todennäköiset arvot eli amplitudit.

Jos käsittelemme kahta kubitia perustilat voivat olla 00, 01, 10, 11 mutta kubitit voivat olla myös samanaikaisesti näiden kaikkien superpositiossa. Jotta voidaan esittää kahta kubitia, tarvitsemme neljä todennäköisyyttä/amplitudia, jos esitetään kolme kubitia tarvitaan kahdeksan todennäköisyyttä/amplitudia.

Amplitudia kasvatetaan tai vaimennetaan konstruktiivisella tai destruktiivisella interferenssillä. Jonkin amplitudin saavuttaessa 1 tai 0 laskenta päättyy.

Superpositiolla on keskeinen merkitys kvanttilaskennassa sillä ne käyttäytyvät hieman samalla tavalla kuin toisensa peittävät aallot.

Jos meillä on n -määrä kubitteja, tarvitsemme 2^n määrän edustamaan kyseisen kvanttijärjestelmän yleistä tilaa. Joten kubitien määrän

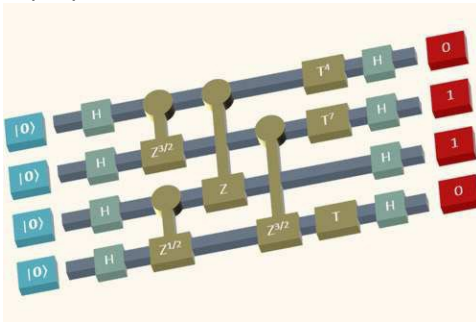
lisäyksellä voimme tuottaa järjestelmiä, jotka voivat edustaa valtavia määriä tiloja.

Kvanttilogiikan portit

Kvanttikoneessakin tarvitaan logiikkaa, joka käsittelee useampaa kuin yhtä kubitia.

Kvanttipiirien rakennemuodut (kvanttilaskennan malli) ovat kvanttilogiikkaportit. Ne ovat kuten klassisen tietojenkäsittelymallin logiikkaportteja, mutta toisin kuin monet klassiset logiikkaportit, kvantti-logiikkaportit ovat palautuvia.

Esimerkiksi klassinen AND-portti ei sovellu kvanttimaailmaan mutta NOT-portti toimii. Hadamard-portti toimii myös yhtenä kubitina ja luo superposition.



University of Bristol

Erilaiset ohjatut portit toimivat kahdella tai useammalla kubitilla, jossa yksi tai useampi kubit toimivat ohjauksena jollekin toiminnalle. Esimerkiksi hallittu NOT-portti (CNOT) toimii kahdella kubitilla ja suorittaa NOT-operaation toisella kubitilla vain kun ensimmäinen kubit on $|1\rangle$ ja muuten jättää sen muuttumattomaksi.

Kvanttitietokone on herättänyt vahvaa kiinnostusta, varsinkin sen suhteen, että se kykenisi purkamaan nykyisin laajasti käytetyt tietoturvamenettelyt eli Internetin salaustekniikan.

Tutkijapiireissä kvanttitietokoneen tuloon uskotaan aika vahvasti. Osittain voidaan sanoa että se on jo todellisuutta mutta onko sen tulevaisuus sillä tasolla jolle sitä eniten hehkutettiin.

Kirjoittaja on toiminut elektroniikka-alan toimittajana ja yllpitää nykyään tulevaisuuden elektroniikkaan keskittyvää nanobittaj.fi -sivustoa

