# Deutschin algoritmi

Petri Savola

T-79.4001 - Seminaari vappuaattona

30.4.2008

# Seminaarin sisältö

- Motivointia: Miksi Deutschin algoritmi on merkittävä?
- Kertausta: Kvanttiportit ja -piirit
- Deutschin algoritmi
- Pohdintaa
- Yhteenveto

# Motivointia

- Deutschin algoritmi on esimerkki siitä, miten kvanttitietokone voi päihittää perinteisen tietokoneen.
- Algoritmi on varsin yksinkertainen, joten ideaa on melko helppo havainnollistaa.
- Saman kaltainen idea on käytössä Shorin algoritmissa, jota voidaan käyttää luvun jakamisessa tekijöihin.
- Alkuperäinen idea on yleistettävissä monimutkaisempiin ja mielenkiintoisempiin ongelmiin.

# Merkintöjä ja määritelmiä

- Käytetään lyhennysmerkintää $|a\rangle|b\rangle = |a\rangle \otimes |b\rangle = |ab\rangle$.
- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Portti $X$ matriisimuodossa: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- Portti $H$ matriisimuodossa: $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

# Deutschin algoritmi

- Olkoon $f : \mathbb{Z}_2 \to \mathbb{Z}_2$.
- Tällaisia funktioita on olemassa 4 kappaletta.
- Algoritmin ideana on selvittää palauttaako annettu funktio vakion vai ei.
- Jos $f(0) \oplus f(1) = 0$, niin $f$ on vakiofunktio.
- Perinteisellä tietokoneella tämän tiedon selvittäminen vaatii kaksi funktiokutsua, mutta Deutschin algoritmi osoittaa, että kvanttitietokone selviää tehtävästä ainoastaan yhdellä kutsulla.

# Funktion arvon määrittäminen

- Määritellään $U_{f_k}$ seuraavasti:
- $U_{f_k}|x, y\rangle = |x, y \oplus f(x)\rangle$
- Tässä $x$ ja $y$ voivat olla vektoreita, mutta kuvauksen $f$ tapauksessa ne ovat qubittejä.
- $f(x)$ voidaan selvittää laskemalla $U_{f_k}|x, 0\rangle$ ja mittaamalla toinen qubitti.

# Deutschin algoritmi

- 1. Alustus:
  $|\Psi_1\rangle = |00\rangle = |0\rangle|0\rangle$
- 2. Käytetään porttia $X$ toiseen qubittiin:
  $|\Psi_2\rangle = X_2|\Psi_1\rangle = |0\rangle|1\rangle$
- 3. Käytetään porttia $H$ molempiin qubitteihin:
  $|\Psi_3\rangle = H_1H_2|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$
- 4. Käytetään annettua kvantti-implementaatiota $U_{f_k}$:
  $|\Psi_4\rangle = U_{f_k}|\Psi_3\rangle = \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) = \frac{1}{2}(|0\rangle(-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle(-1)^{f(1)}(|0\rangle - |1\rangle)) = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

# Deutschin algoritmi

- 5. Käytetään porttia $H$ ensimmäiseen qubittiin:
  $|\Psi_5\rangle = H_1|\Psi_4\rangle =$
  $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
  $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)}|1\rangle))\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- 6. Mitataan ensimmäinen qubitti kannassa $(|0\rangle, |1\rangle)$:
  $\pm|0\rangle$, jos $f(0) \oplus f(1) = 0$.
  $\pm|1\rangle$, jos $f(0) \oplus f(1) = 1$.

# Pohdintaa

- Deutschin algoritmi selvisi tehtävästä ainoastaan yhdellä funktiokutsulla, koska funktiolle annettiin parametrina qubittien superpositio.
- Saatiin selvitettyä $f(0) \oplus f(1)$, mutta ei selvitetty kumpkaakaan arvoista $f(0)$ tai $f(1)$ erikseen.
- Idea voidaan yleistää, jolloin kvanttitietokoneella saavutettava hyöty kasvaa merkittävästi. Jos funktio olisi esimerkiksi $f : \mathbb{Z}_2^N \to \mathbb{Z}_2$, niin perinteinen tietokone tarvitsee $\mathcal{O}(2^N)$ funktiokutsua selvittääkseen onko funktio vakio vai ei, kun taas kvanttitietokone selviää yhdellä funktiokutsulla.
- Vertailu perinteisen ja kvanttitietokoneen välillä ei ole täysin reilu, koska kvanttitietokone käyttää hyväkseen annettua unitaarista implementaatiota $U_{f_k}$.

# Tiivistelmä

- Deutschin algoritmin idea on osoittaa, että kvanttitietokoneella voidaan ratkaista erilaisia ongelmia tehokkaammin kuin perinteisellä tietokoneella.
- Deutschin algoritmi ratkaisee yhden funktiokutsun avulla onko funktio $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ vakio vai ei.
- Menetelmä perustuu siihen, että kvanttitietokone ei ratkaise funktion arvoja yksittäisillä parametreilla, vaan laskee kaikki vaihtoehdot kerralla.
- Deutschin algoritmissa käytetty idea on yleistettävissä erilaisille funktioille.