Deutschin algoritmi

The project is co-funded by the Erasmus+ Programme of the European Union. Grant Agreement n° 2016-1-IT02-KA201-024373.

It's your time to imagine the futures

Kvanttialgoritmit

- Kvanttialgoritmeja voidaan rakentaa yhdistelemällä kvanttiportteja.
- Kvanttialgoritmeilla voidaan vielä ratkaista vain hyvin rajallinen määrä ongelmia. Tällaisia ovat esimerkiksi tekijöihin jakaminen, etsintä ja jotkin simulaatiot.
- Yksinkertaisin mahdollinen kvanttialgoritmi: Deutschin algoritmi

Deutschin ongelma

Deutschin algoritmi kehitettiin ratkaisemaan seuraava ongelma:

Meillä on funktio $f: \{0,1\} \rightarrow \{0,1\}$.
Funktio on joko

1. $f(0) = f(1)$ ”vakiofunktio” tai
2. $f(0) \neq f(1)$ ”tasapainotettu funktio”.

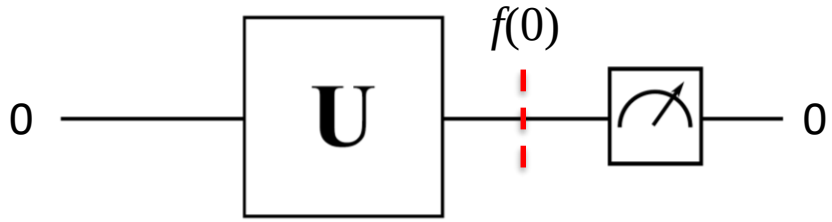
Kumpi funktio on kyseessä?

Klassinen ratkaisu

Klassisesti ongelma voidaan ratkaista testaamalla funktio kahdesti. U-portti sisältää tiedon tuntemattoman funktion toiminnasta.

Esimerkiksi

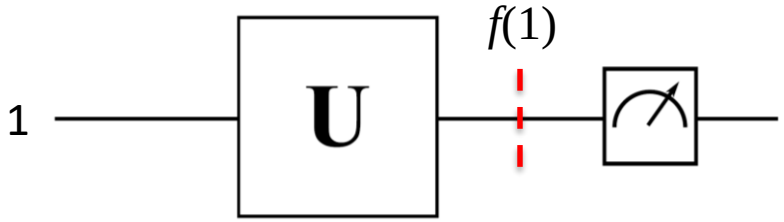
Ensimmäinen testi



Syötetään arvo 0 U-porttiin.

Tuloste: 0.

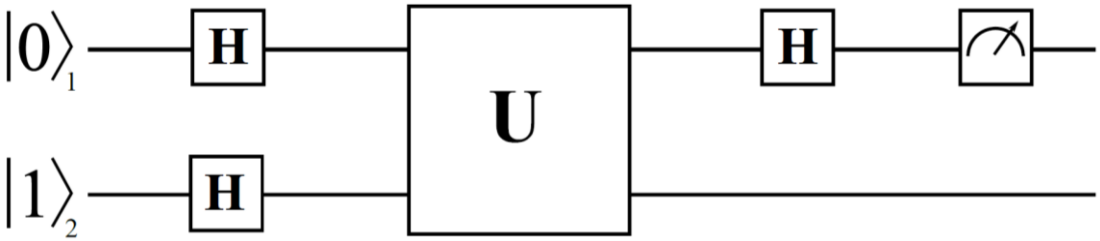
Toinen testi



Syötetään arvo 1 U-porttiin.

1. Tuloste: 0 → vakiofunktio
2. Tuloste: 1 → tasapainotettu funktio

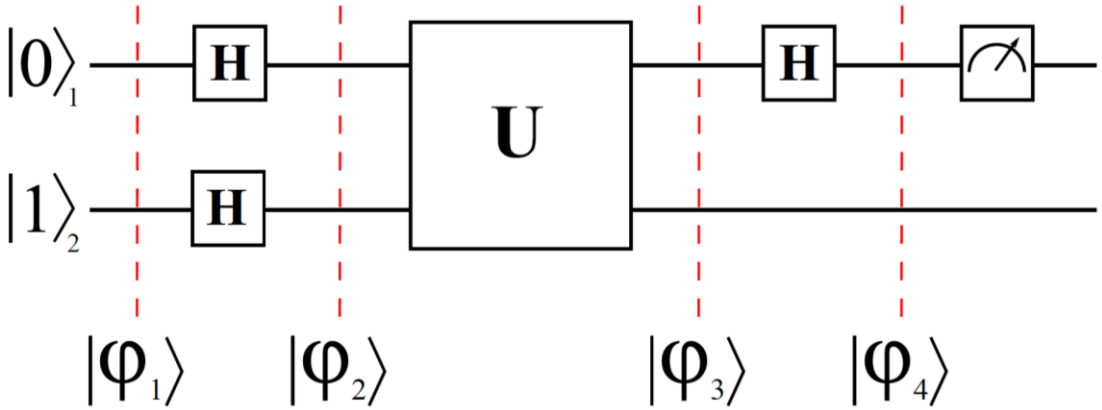
Deutschin algoritmi



Kaksi kubittia (merkitty alaindekseillä).

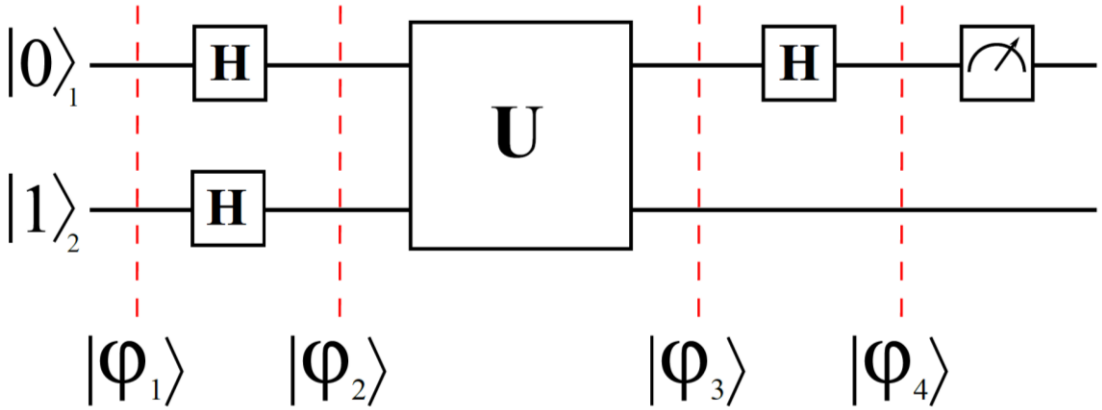
H-portit ovat Hadamartin portteja ja U-portti sisältää jälleen tiedon tuntemattoman funktion f operaatiosta.

Deutschin algoritmi



Jaetaan ongelma paloihin.

Deutschin algoritmi



Hadamartin portti operoi tiloihin seuraavasti:

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

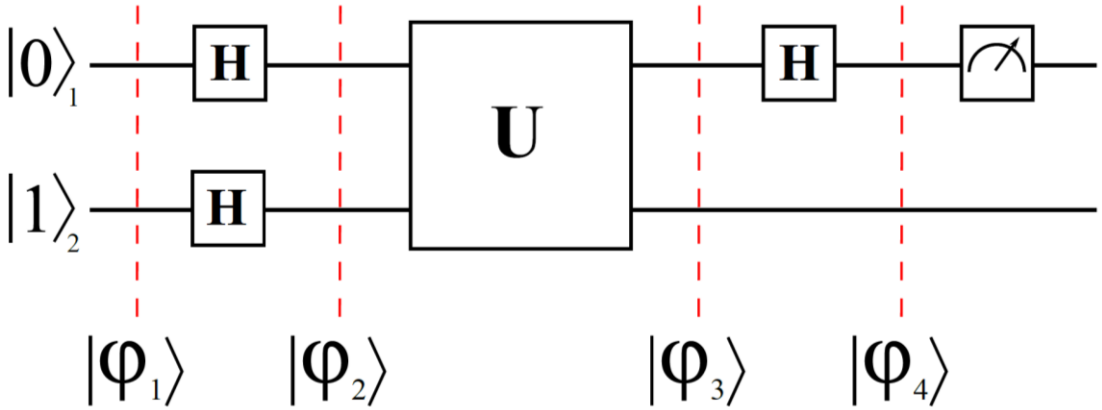
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\varphi_1\rangle = |0\rangle_1|1\rangle_2$$

$$|\varphi_2\rangle = \frac{1}{2}(|0\rangle_1 + |1\rangle_1)(|0\rangle_2 - |1\rangle_2)$$

Kahden kubitin yhdistetty tila esitetään niiden tulona.

Deutschin algoritmi

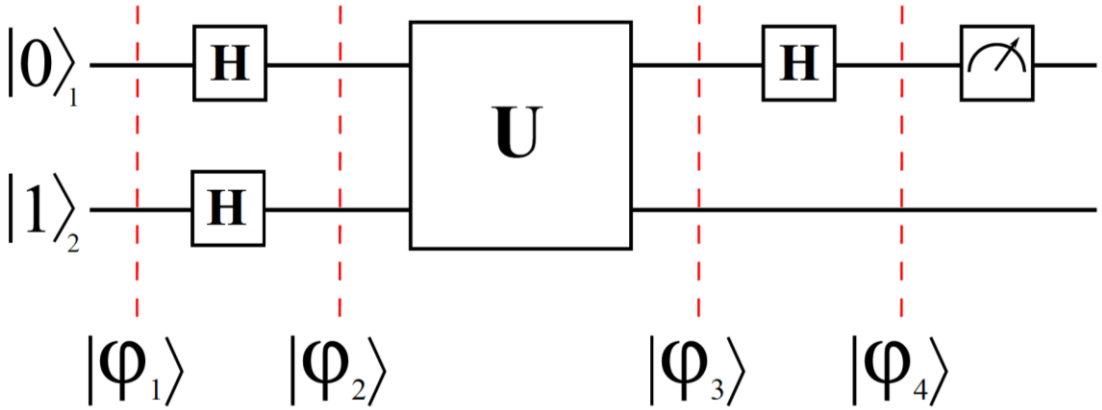


Avataan sulut.

$$|\varphi_2\rangle = \frac{1}{2}(|0\rangle_1 + |1\rangle_1)(|0\rangle_2 - |1\rangle_2)$$

$$= \frac{1}{2}(|0\rangle_1|0\rangle_2 - |0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2)$$

Deutschin algoritmi



U-portti operoi tilaan seuraavasti:

$$|x\rangle_1|y\rangle_2 \rightarrow |x\rangle_1|y + f(x)\rangle_2$$

$$|\varphi_3\rangle = \frac{1}{2}(|0\rangle_1|0 + f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|0 + f(1)\rangle_2 - |1\rangle_1|1 + f(1)\rangle_2)$$

$$= \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|f(1)\rangle_2 - |1\rangle_1|1 + f(1)\rangle_2)$$

Deutschin algoritmi

$$|\varphi_3\rangle = \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|f(1)\rangle_2 - |1\rangle_1|1 + f(1)\rangle_2)$$

1. $f(0) = f(1)$ ”vakiofunktio” tai
2. $f(0) \neq f(1)$ ”tasapainotettu funktio”.

$$|\varphi_3\rangle = \begin{cases} \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|f(0)\rangle_2 - |1\rangle_1|1 + f(0)\rangle_2) & \text{jos } f(0) = f(1) \\ \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|1 + f(0)\rangle_2 - |1\rangle_1|f(0)\rangle_2) & \text{jos } f(0) \neq f(1) \end{cases}$$

Deutschin algoritmi

$$|\varphi_3\rangle = \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1 + f(0)\rangle_2 + |1\rangle_1|f(1)\rangle_2 - |1\rangle_1|1 + f(1)\rangle_2)$$

1. $f(0) = f(1)$ ”vakiofunktio”

$$|f(1)\rangle_2 = |f(0)\rangle_2$$

$$|1 + f(1)\rangle_2 = |1 + f(0)\rangle_2$$

2. $f(0) \neq f(1)$ ”tasapainotettu funktio”.

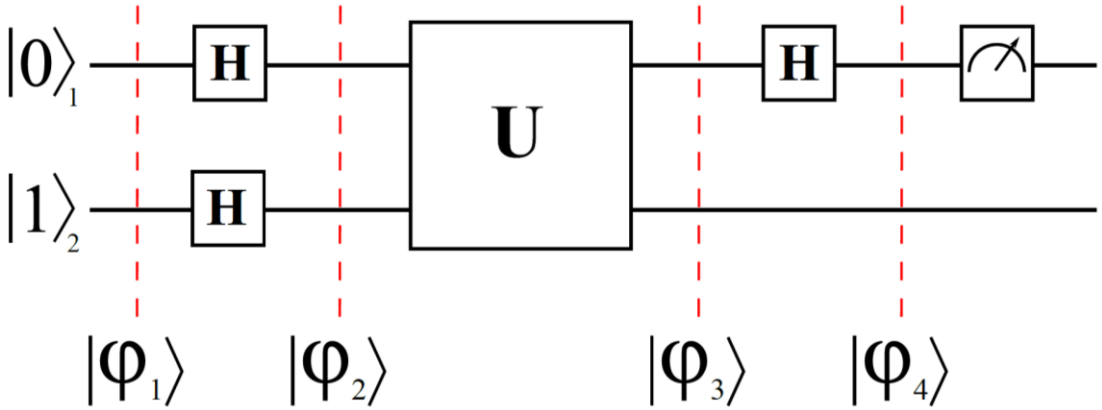
$$|f(1)\rangle_2 = |1 + f(0)\rangle_2$$

$$|1 + f(1)\rangle_2 = |f(0)\rangle_2$$

Muista binäärilukujen yhteenlasku!
Nyt 1 + 1 = 0

I SEE
It's your time to imagine the futures

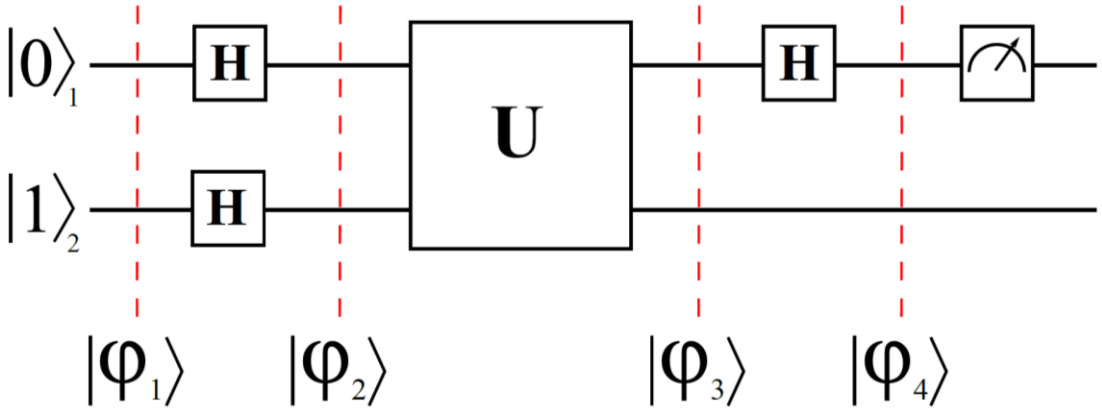
Deutschin algoritmi



Ratkaisu voidaan jakaa kahteen osaan funktion f toiminnan mukaan.

$$|\varphi_3\rangle = \begin{cases} \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1+f(0)\rangle_2 + |1\rangle_1|f(0)\rangle_2 - |1\rangle_1|1+f(0)\rangle_2) & \text{jos } f(0) = f(1) \\ \frac{1}{2}(|0\rangle_1|f(0)\rangle_2 - |0\rangle_1|1+f(0)\rangle_2 + |1\rangle_1|1+f(0)\rangle_2 - |1\rangle_1|f(0)\rangle_2) & \text{jos } f(0) \neq f(1) \end{cases}$$

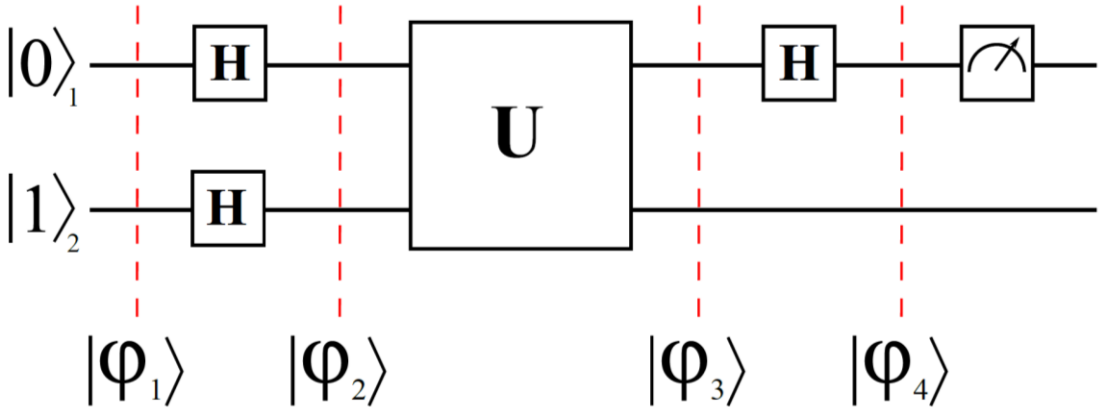
Deutschin algoritmi



Järjestetään termit uudelleen.

$$|\varphi_3\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1)\frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1 + f(0)\rangle_2) & \text{jos } f(0) = f(1) \\ \frac{1}{\sqrt{2}}(|0\rangle_1 - |1\rangle_1)\frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1 + f(0)\rangle_2) & \text{jos } f(0) \neq f(1) \end{cases}$$

Deutschin algoritmi



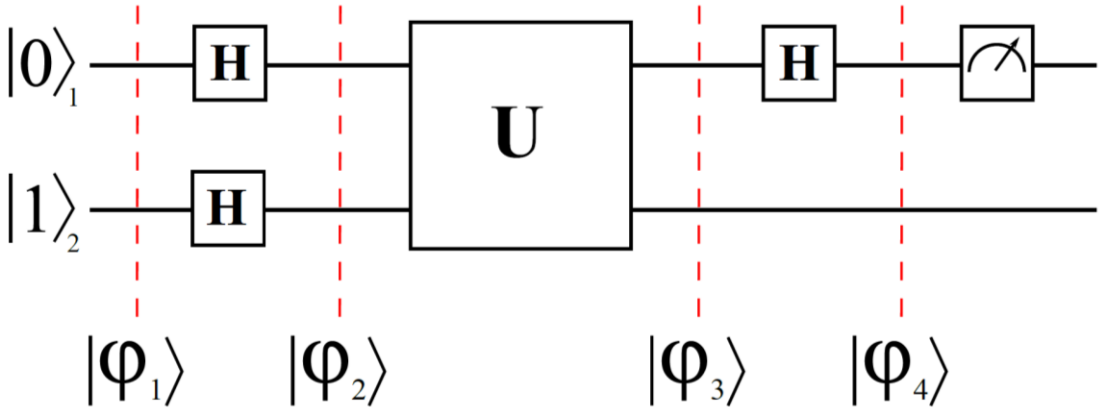
$$|\varphi_3\rangle = \begin{cases} |0\rangle_1 \frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1 + f(0)\rangle_2) & \text{jos } f(0) = f(1) \\ |1\rangle_1 \frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1 + f(0)\rangle_2) & \text{jos } f(0) \neq f(1) \end{cases}$$

Kun operoidaan Hadamartin portilla kahdesti, päädytään alkuperäiseen tilaan:

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

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

Deutschin algoritmi



Jos nyt mitataan ylimmän kubitin arvo, saadaan tietää, onko funktio vakio vai tasapainotettu.

$$|\varphi_3\rangle = \begin{cases} |0\rangle_1 \frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1+f(0)\rangle_2) & \text{jos } f(0) = f(1) \\ |1\rangle_1 \frac{1}{\sqrt{2}}(|f(0)\rangle_2 - |1+f(0)\rangle_2) & \text{jos } f(0) \neq f(1) \end{cases}$$

Muita kvanttialgoritmeja

Deutschin algoritmi on kaikkein yksinkertaisin kvanttialgoritmi.

Kuuluisimmat (ja monimutkaisemmat) algoritmit:

- Shorin algoritmi, joka jakaa kokonaislukuja tekijöihin, eli etsii luvun N alkulukutekijät.
- Groverin algoritmi, joka ratkaisee käänteisfunktion, eli etsii parametrin x, kun funktion arvo ko. x:n arvolla $y = f(x)$ tiedetään.
- Molempia em. algoritmeja voidaan käyttää esimerkiksi salasanojen murtamiseen.

Lähde: https://en.wikipedia.org/wiki/Quantum_algorithm

Mitä opimme?

- Voimme rakentaa kvanttialgoritmeja melkein samaan tapaan kuin klassisia algoritmeja.
- Kvanttialgoritmit ovat melko monimutkaisia, mutta eivät mahdottomia ymmärtää.*
- Koska kvanttialgoritmien keksiminen on niin monimutkaista, vielä ei ole olemassa kvanttialgoritmeja läheskään jokaisen ongelman ratkaisemiseen.
- Ehkä joku teistä kehittää seuraavan kvanttialgoritmin.

*Jos Deutschin algoritmi tuntui monimutkaiselta, älä huolestu. Se *on* melko monimutkainen. Yritä käydä algoritmi läpi hitaasti ja ajatuksella.

Yhteistyökumppanit

FONDAZIONE GOLINELLI

LANDVERND
ICELANDIC ENVIRONMENT ASSOCIATION

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIVERSITY OF HELSINKI

Liceo
Scientifico
Einstein

MENNTASKÓLINN VIÐ HAMRAHLÍÐ
STOFNAÐUR 1966

The Association for Science Education
Promoting Excellence in Science Teaching and Learning

IDEAS SEE
It's your time to imagine the futures

It's your time to imagine the futures

www.**iseeproject.eu**

iseeproject.eu@gmail.com

The project is co-funded by the Erasmus+ Programme of the European Union.
Grant Agreement n° 2016-1-IT02-KA201-024373.