Quantummechanische Computers

Ronald de Wolf

Centrum voor Wiskunde en Informatica

Amsterdam

Achtergrond

Achtergrond

Hier zijn drie plausibele assumpties:

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar
2. Het is voor “gewone” computers moeilijk om grote getallen te factoriseren

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar

2. Het is voor “gewone” computers moeilijk om grote getallen te factoriseren (basis voor RSA cryptografie)

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar
2. Het is voor “gewone” computers moeilijk om grote getallen te factoriseren (basis voor RSA cryptografie)
3. Alle “redelijke” soorten computers kunnen elkaar efficiënt simuleren

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar
2. Het is voor “gewone” computers moeilijk om grote getallen te factoriseren (basis voor RSA cryptografie)
3. Alle “redelijke” soorten computers kunnen elkaar efficiënt simuleren (uitgebreide Church-Turing these)

Achtergrond

Hier zijn drie plausibele assumpties:

1. De quantummechanica is waar
2. Het is voor “gewone” computers moeilijk om grote getallen te factoriseren (basis voor RSA cryptografie)
3. Alle “redelijke” soorten computers kunnen elkaar efficiënt simuleren (uitgebreide Church-Turing these)

Minstens één van deze drie assumpties is onwaar!

Quantummechanica

Quantummechanica

- Ontwikkeld vanaf 1900

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten: superpositie

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten: superpositie, interferentie

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement, onzekerheid

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement, onzekerheid
  (straks meer hierover. . .)

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement, onzekerheid
  (straks meer hierover. . .)
- Quantummechanica doet hele vreemde voorspellingen. . .

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement, onzekerheid
  (straks meer hierover. . .)
- Quantummechanica doet hele vreemde voorspellingen. . . maar al die voorspellingen komen uit!

Quantummechanica

- Ontwikkeld vanaf 1900 door
  Planck, Einstein, Bohr, Schrödinger, Heisenberg, . . .
- Eén van de twee belangrijkste theorieën van de moderne natuurkunde
- Allerlei vreemde, tegen-intuïtieve effecten:
  superpositie, interferentie, entanglement, onzekerheid
  (straks meer hierover. . .)
- Quantummechanica doet hele vreemde voorspellingen. . . maar al die voorspellingen komen uit!
- Nog nooit door een experiment weerlegd

Factorisatie van gehele getallen

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N
- De beste algoritmes die we hebben lopen in (bijna) exponentiële tijd

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N
- De beste algoritmes die we hebben lopen in (bijna) exponentiële tijd, die hebben miljoenen jaren nodig om een getal van 400 cijfers te factoriseren
- Dit geeft een “one-way function”:

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N
- De beste algoritmes die we hebben lopen in (bijna) exponentiële tijd, die hebben miljoenen jaren nodig om een getal van 400 cijfers te factoriseren
- Dit geeft een “one-way function”:
  - $N = p \times q$ berekenen uit p en q is makkelijk

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N
- De beste algoritmes die we hebben lopen in (bijna) exponentiële tijd, die hebben miljoenen jaren nodig om een getal van 400 cijfers te factoriseren
- Dit geeft een “one-way function”:
  - $N = p \times q$ berekenen uit p en q is makkelijk
  - p en q berekenen uit N is moeilijk

Factorisatie van gehele getallen

- Euclides (300 vC): elk geheel getal heeft een unieke factorisatie in priemgetallen (bv $15 = 3 \times 5$)
- Fundamenteel wiskundig/computationeel probleem: vind de priemfactoren van een gegeven getal N
- De beste algoritmes die we hebben lopen in (bijna) exponentiële tijd, die hebben miljoenen jaren nodig om een getal van 400 cijfers te factoriseren
- Dit geeft een “one-way function”:
  - $N = p \times q$ berekenen uit p en q is makkelijk
  - p en q berekenen uit N is moeilijk
- RSA public-key cryptography is hierop gebaseerd

De (uitgebreide) Church-Turing these

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!
- De Church-Turing these: Alle “redelijke” modellen van computers kunnen elkaar simuleren

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!
- Uitgebreide Church-Turing these: Alle “redelijke” modellen van computers kunnen elkaar efficiënt simuleren

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!
- Uitgebreide Church-Turing these: Alle “redelijke” modellen van computers kunnen elkaar efficiënt simuleren
- Efficiënt = in polynomiale tijd

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!
- Uitgebreide Church-Turing these: Alle “redelijke” modellen van computers kunnen elkaar efficiënt simuleren
- Efficiënt = in polynomiale tijd
- Wat is “redelijk”?

De (uitgebreide) Church-Turing these

- Er zijn allerlei wiskundige modellen van “computers”:
  - Turing machines
  - Circuits van logische “poorten”
  - Random Access Machines
  - Cellulaire automaten (“The Game of Life”)
  - Expressies in lambda-calculus
  - . . .
- Al deze modellen kunnen elkaar efficiënt simuleren!
- Uitgebreide Church-Turing these: Alle “redelijke” modellen van computers kunnen elkaar efficiënt simuleren
- Efficiënt = in polynomiale tijd
- Wat is “redelijk”? Te implementeren in de natuur.

Waarom is er minstens één onwaar?

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar, dus quantum computers zijn een redelijk model van computers

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar, dus quantum computers zijn een redelijk model van computers

Dus: er is een redelijk model van computers dat efficiënt kan factoriseren

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar, dus quantum computers zijn een redelijk model van computers

Dus: er is een redelijk model van computers dat efficiënt kan factoriseren

Assumptie 2: “gewone” computers kunnen dat niet

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar, dus quantum computers zijn een redelijk model van computers

Dus: er is een redelijk model van computers dat efficiënt kan factoriseren

Assumptie 2: “gewone” computers kunnen dat niet

Maar dan kunnen “gewone” computers quantum computers niet efficiënt simuleren

Waarom is er minstens één onwaar?

Peter Shor (1994): Een quantummechanische computer can efficiënt getallen factoriseren

Assumptie 1: quantummechanica is waar, dus quantum computers zijn een redelijk model van computers

Dus: er is een redelijk model van computers dat efficiënt kan factoriseren

Assumptie 2: “gewone” computers kunnen dat niet

Maar dan kunnen “gewone” computers quantum computers niet efficiënt simuleren $\Rightarrow$ assumptie 3 is onwaar!

Gewone, klassieke computers

Gewone, klassieke computers

- Werken met bits

Gewone, klassieke computers

- Werken met bits
- Een bit is 0 of 1

Gewone, klassieke computers

- Werken met bits
- Een bit is 0 of 1
- Allerlei verschillende equivalente modellen:

Gewone, klassieke computers

- Werken met bits
- Een bit is 0 of 1
- Allerlei verschillende equivalente modellen:

  Turing machines,

Gewone, klassieke computers

- Werken met bits
- Een bit is 0 of 1
- Allerlei verschillende equivalente modellen:

  Turing machines, logische circuits, ...

Gewone, klassieke computers

- Werken met bits
- Een bit is 0 of 1
- Allerlei verschillende equivalente modellen:

  Turing machines, logische circuits, ...
- Circuits zijn het eenvoudigst te generaliseren naar de quantummechanische wereld

Logische circuits

Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten

Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn

Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is

Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit

Logische circuits

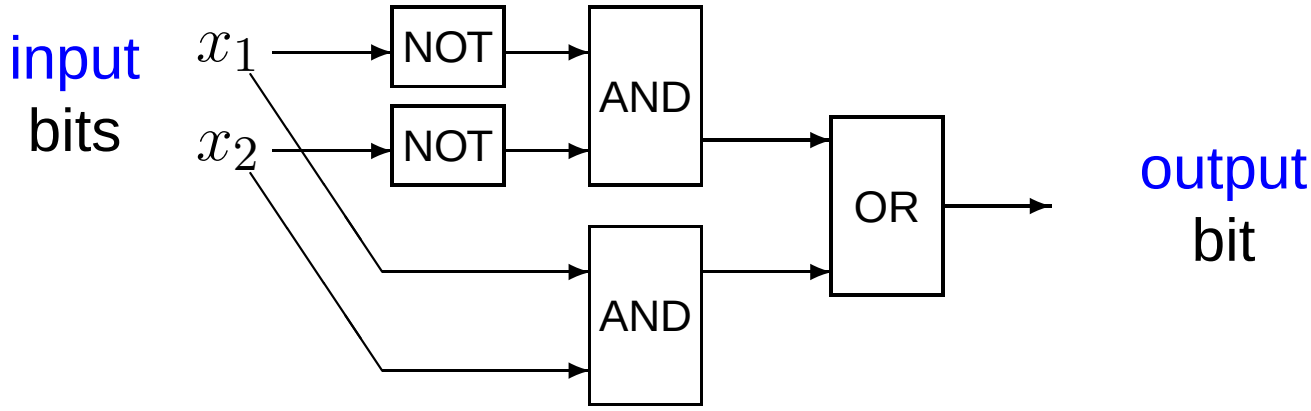
- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit
- Bereken een functie van n input bits naar m output bits door successievelijk alle poorten te evalueren

Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit
- Bereken een functie van n input bits naar m output bits door successievelijk alle poorten te evalueren
- Voorbeeld: circuit dat checkt of $x_1 = x_2$ (“ja”=output 1)

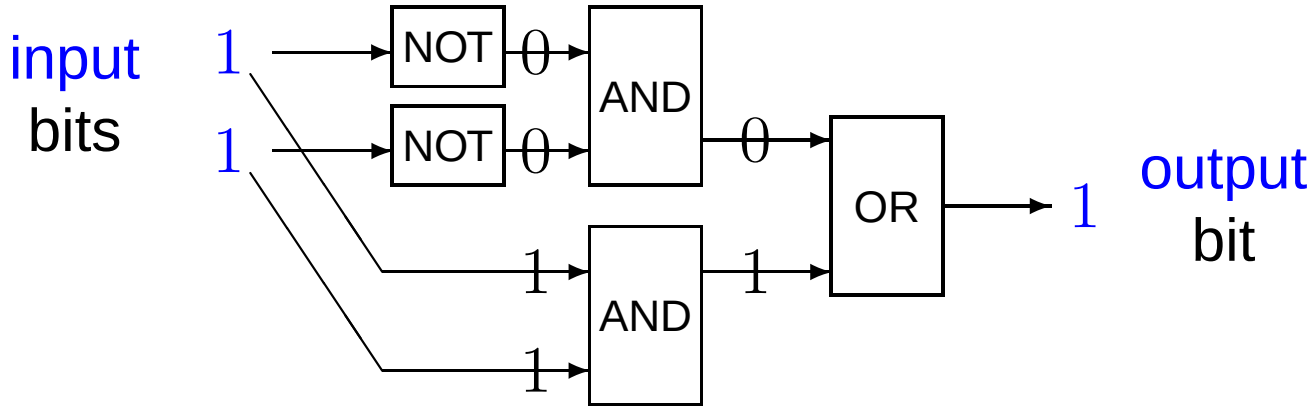
Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit
- Bereken een functie van n input bits naar m output bits door successievelijk alle poorten te evalueren
- Voorbeeld: circuit dat checkt of $x_1 = x_2$ (“ja”=output 1)



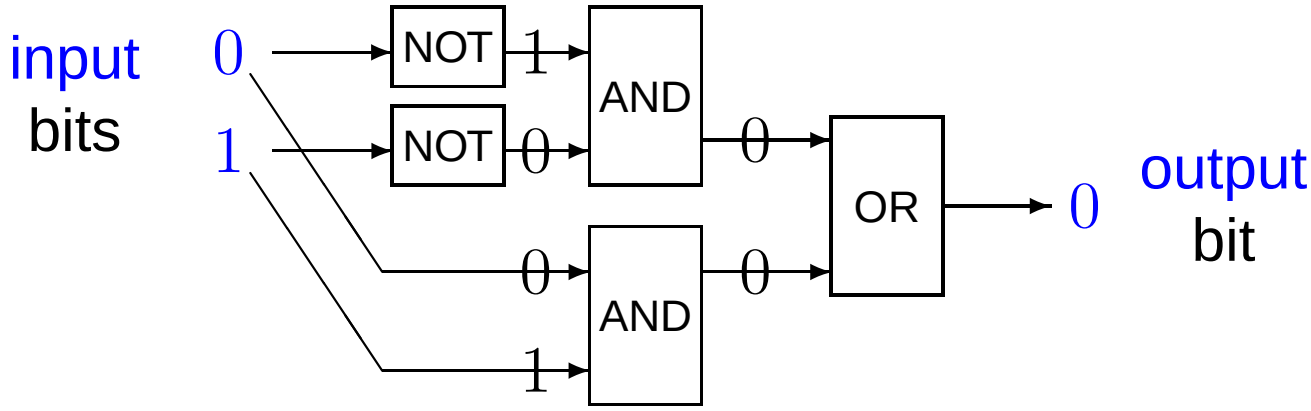
Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit
- Bereken een functie van n input bits naar m output bits door successievelijk alle poorten te evalueren
- Voorbeeld: circuit dat checkt of $x_1 = x_2$ ("ja"=output 1)



Logische circuits

- Gerichte acyclische graaf met AND, OR, NOT poorten
- AND=1 als beide inkomende bits 1 zijn
  OR=1 als minstens één van de inkomende bits 1 is
  NOT flipt zijn inkomende bit
- Bereken een functie van n input bits naar m output bits door successievelijk alle poorten te evalueren
- Voorbeeld: circuit dat checkt of $x_1 = x_2$ (“ja”=output 1)



Van klassiek naar quantum

Van klassiek naar quantum

- bits $\longrightarrow$ qubits

Van klassiek naar quantum

- bits $\longrightarrow$ qubits
- AND/OR/NOT poorten $\longrightarrow$ unitaire quantum poorten

Van klassiek naar quantum

- bits $\longrightarrow$ qubits
- AND/OR/NOT poorten $\longrightarrow$ unitaire quantum poorten
- klassiek circuit $\longrightarrow$ quantum circuit

Van klassiek naar quantum

- bits $\longrightarrow$ qubits
- AND/OR/NOT poorten $\longrightarrow$ unitaire quantum poorten
- klassiek circuit $\longrightarrow$ quantum circuit
- lezen van de output bits $\longrightarrow$ meting van eindtoestand

Quantum bits

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$”

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!

- Identificeer met vectoren:

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Qubit: superpositie $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Qubit: superpositie $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Qubit: superpositie $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$
- Dus: quantum bits leven in een lineaire ruimte

Quantum bits

- Fysisch systeem met 2 identificeerbare toestanden, bv:
  - polarisatie van licht is “horizontaal” of “verticaal”
  - een electron kan “spin up” of “spin down” hebben
  - een kat kan “dood” of “levend” zijn. . .
- Noem deze toestanden “$|0\rangle$” en “$|1\rangle$” — dit is een bit!
- Identificeer met vectoren: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Qubit: superpositie $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$
- Dus: quantum bits leven in een lineaire ruimte, met de twee klassieke toestanden $|0\rangle$ en $|1\rangle$ als basisvectoren

Toestand = vector, operatie = matrix

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis

- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden “tegelijk”

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte
- Twee soorten quantum operaties op $|\phi\rangle$:

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte
- Twee soorten quantum operaties op $|\phi\rangle$:

  1. Meting geeft klassieke uitkomst $|x\rangle$ met kans $|\alpha_x|^2$.

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte
- Twee soorten quantum operaties op $|\phi\rangle$:
  1. Meting geeft klassieke uitkomst $|x\rangle$ met kans $|\alpha_x|^2$.
     $\sum_x |\alpha_x|^2 = 1$, dus $|\phi\rangle$ is altijd vector van lengte 1

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte
- Twee soorten quantum operaties op $|\phi\rangle$:
  1. Meting geeft klassieke uitkomst $|x\rangle$ met kans $|\alpha_x|^2$. $\sum_x |\alpha_x|^2 = 1$, dus $|\phi\rangle$ is altijd vector van lengte 1
  2. Verander de amplitude-vector met een unitaire matrix

Toestand = vector, operatie = matrix

- Algemeen: quantum toestanden zijn vectoren in een lineaire ruimte, met klassieke toestanden als basis
- n-qubit toestand: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix}$
- *Informeel*: we zijn in alle 2^n basis toestanden "tegelijk"
  Formeel: $|\phi\rangle$ is een vector in 2^n-dimensionale ruimte
- Twee soorten quantum operaties op $|\phi\rangle$:
  1. Meting geeft klassieke uitkomst $|x\rangle$ met kans $|\alpha_x|^2$. $\sum_x |\alpha_x|^2 = 1$, dus $|\phi\rangle$ is altijd vector van lengte 1
  2. Verander de amplitude-vector met een unitaire matrix (= een lengte-bewarende matrix)

Quantum poorten

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

  $H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

  $H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) =$

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

$$H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

$$H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $$H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

  Interferentie van positieve en negatieve amplitudes!

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $$H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

  Interferentie van positieve en negatieve amplitudes!
- 2-qubit controlled-NOT:

Quantum poorten

- Unitaire transformaties op 1 of 2 qubits tegelijk
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  Voorbeelden:

  $$H|1\rangle = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

  Interferentie van positieve en negatieve amplitudes!
- 2-qubit controlled-NOT:
  flip het 2e bit als het 1e bit waarde $|1\rangle$ heeft

Quantum circuits

Quantum circuits

- Circuit van unitaire quantum poorten is zelf ook unitair

Quantum circuits

- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)

Quantum circuits

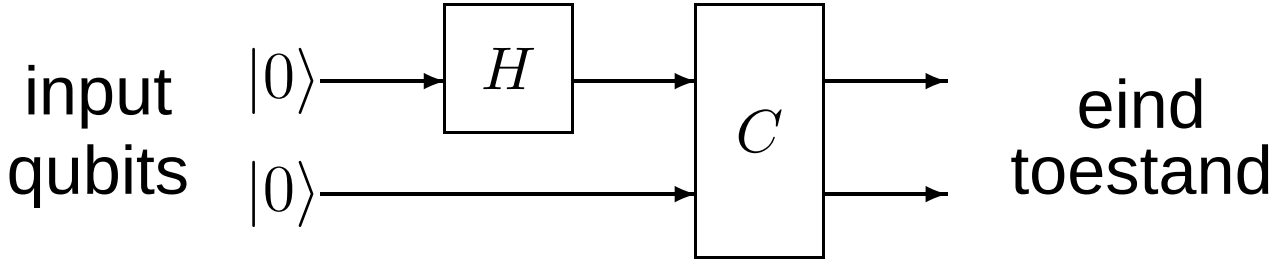
- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand

Quantum circuits

- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand
- Meet de eindtoestand om de klassieke output van het algoritme te krijgen (probabilistisch!)

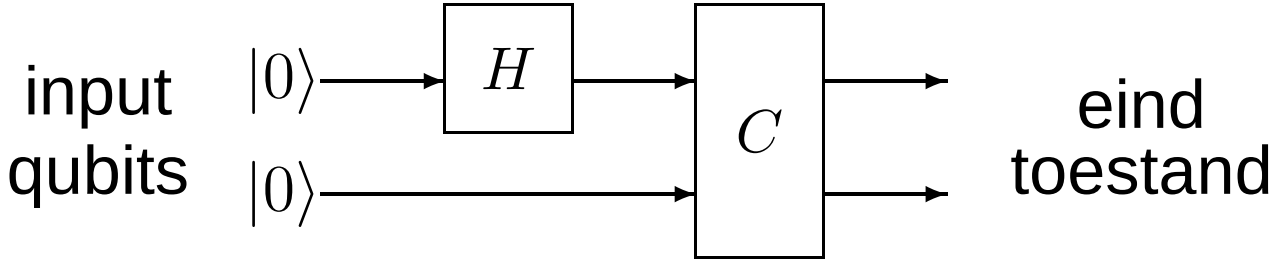
Quantum circuits

- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand
- Meet de eindtoestand om de klassieke output van het algoritme te krijgen (probabilistisch!)



Quantum circuits

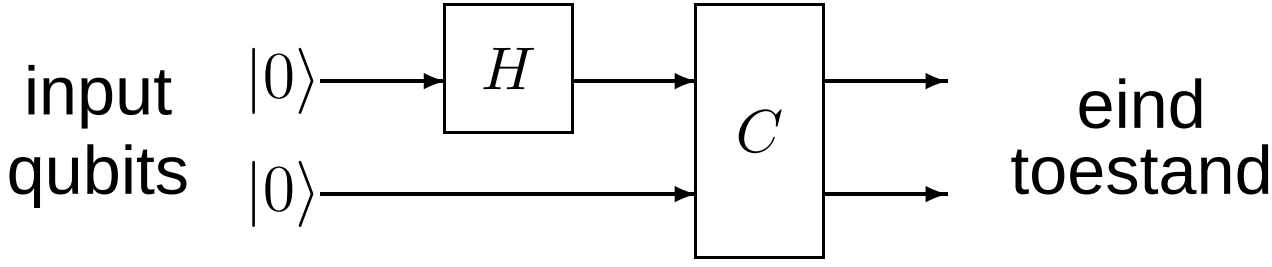
- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand
- Meet de eindtoestand om de klassieke output van het algoritme te krijgen (probabilistisch!)



- Eindtoestand: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Quantum circuits

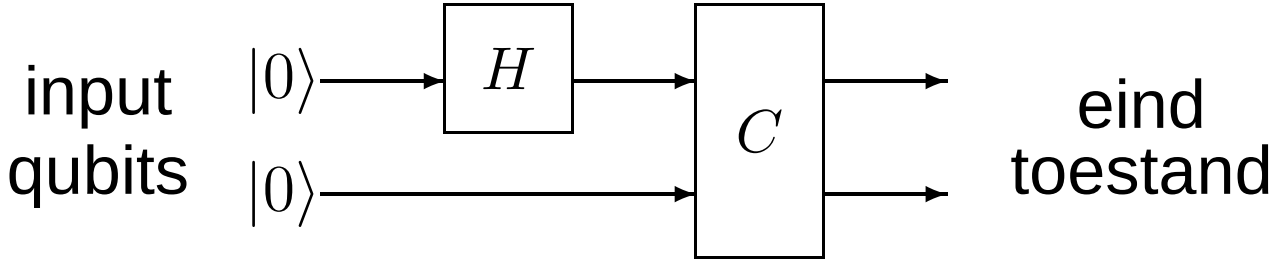
- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand
- Meet de eindtoestand om de klassieke output van het algoritme te krijgen (probabilistisch!)



- Eindtoestand: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (EPR-state, entangled)

Quantum circuits

- Circuit van unitaire quantum poorten is zelf ook unitair (formeel: combineer gates via tensor product)
- Transformeert begintoestand naar eindtoestand
- Meet de eindtoestand om de klassieke output van het algoritme te krijgen (probabilistisch!)



- Eindtoestand: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (EPR-state, entangled)
- Efficiënt quantum circuit: aantal poorten is “klein”

Quantum parallelisme

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- Door hier één keer unitaire U op los te laten, bereken je $U|x\rangle$ voor alle x tegelijk (in superpositie):

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- Door hier één keer unitaire U op los te laten, bereken je $U|x\rangle$ voor alle x tegelijk (in superpositie):

$$U \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U|x\rangle$$

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- Door hier één keer unitaire U op los te laten, bereken je $U|x\rangle$ voor alle x tegelijk (in superpositie):

$$U \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U|x\rangle$$

- Probleem: hoe krijg je hieruit de informatie die je wilt?

Quantum parallelisme

- Met Hadamard gates kun je efficiënt een uniforme superpositie over 2^n basistoestanden maken:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- Door hier één keer unitaire U op los te laten, bereken je $U|x\rangle$ voor alle x tegelijk (in superpositie):

$$U \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U|x\rangle$$

- Probleem: hoe krijg je hieruit de informatie die je wilt?
- Dat kan soms door interferentie

Schets van het quantum algoritme van Shor

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:

  1. Maak uniforme superpositie: $\sum_x |x\rangle|0\rangle$

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:
  1. Maak uniforme superpositie: $\sum_x |x\rangle|0\rangle$
  2. Bereken f in superpositie: $\sum_x |x\rangle|f(x)\rangle$

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:
  1. Maak uniforme superpositie: $\sum_x |x\rangle|0\rangle$
  2. Bereken f in superpositie: $\sum_x |x\rangle|f(x)\rangle$
  3. Meet 2e deel: “collapse” naar $\sum_{x:f(x)=f(a)} |x\rangle|f(a)\rangle$

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:
  1. Maak uniforme superpositie: $\sum_x |x\rangle|0\rangle$
  2. Bereken f in superpositie: $\sum_x |x\rangle|f(x)\rangle$
  3. Meet 2e deel: "collapse" naar $\sum_{x:f(x)=f(a)} |x\rangle|f(a)\rangle$
  4. f heeft periode r, dus 1e deel is nu superpositie

$$|a\rangle + |a+r\rangle + |a+2r\rangle + |a+3r\rangle + \cdots$$

Schets van het quantum algoritme van Shor

- Eeuwenoude reductie:
  om te factoriseren is het genoeg als je de periode r
  kunt vinden van een gegeven periodieke functie f.
- Dat doe je als volgt:
  1. Maak uniforme superpositie: $\sum_x |x\rangle|0\rangle$
  2. Bereken f in superpositie: $\sum_x |x\rangle|f(x)\rangle$
  3. Meet 2e deel: "collapse" naar $\sum_{x:f(x)=f(a)} |x\rangle|f(a)\rangle$
  4. f heeft periode r, dus 1e deel is nu superpositie

$$|a\rangle + |a+r\rangle + |a+2r\rangle + |a+3r\rangle + \cdots$$

  5. Quantum Fourier transformatie verandert dit
     (dmv interferentie) in iets waaruit je r kunt bepalen

Wat kan een quantum computer nog meer?

Wat kan een quantum computer nog meer?

- Onbreekbare quantum cryptografie

Wat kan een quantum computer nog meer?

- Onbreekbare quantum cryptografie

Wat kan een quantum computer nog meer?

- Onbreekbare quantum cryptografie

Spion die een boodschap probeert te lezen, verstoort die ook

Wat kan een quantum computer nog meer?

- Onbreekbare quantum cryptografie

Spion die een boodschap probeert te lezen, verstoort die ook (onzekerheidsprincipe van Heisenberg)

Wat kan een quantum computer nog meer?

- Onbreekbare quantum cryptografie

Spion die een boodschap probeert te lezen, verstoort die ook (onzekerheidsprincipe van Heisenberg)

- Grover's algoritme:
  doorzoeken van database in $\sqrt{n}$ stappen

Samenvatting

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers
- We zijn nu bezig fundamentele kennis op te bouwen

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers
- We zijn nu bezig fundamentele kennis op te bouwen
- Kleine quantum computers op ≈ 10 qubits zijn al geïmplementeerd

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers
- We zijn nu bezig fundamentele kennis op te bouwen
- Kleine quantum computers op ≈ 10 qubits zijn al geïmplementeerd (NMR, ion traps, solid state,. . .)

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers
- We zijn nu bezig fundamentele kennis op te bouwen
- Kleine quantum computers op ≈ 10 qubits zijn al geïmplementeerd (NMR, ion traps, solid state,. . .)
- Praktische applicaties liggen in de (verre) toekomst

Samenvatting

- Quantummechanische computers zijn de krachtigste computers die de natuur ons toestaat
- Voor sommige dingen zijn ze veel krachtiger dan gewone, klassieke computers
- We zijn nu bezig fundamentele kennis op te bouwen
- Kleine quantum computers op ≈ 10 qubits zijn al geïmplementeerd (NMR, ion traps, solid state,. . .)
- Praktische applicaties liggen in de (verre) toekomst
- Maar: dit is een potentiële revolutie