Inleiding op Quantum Computing en Algoritmen

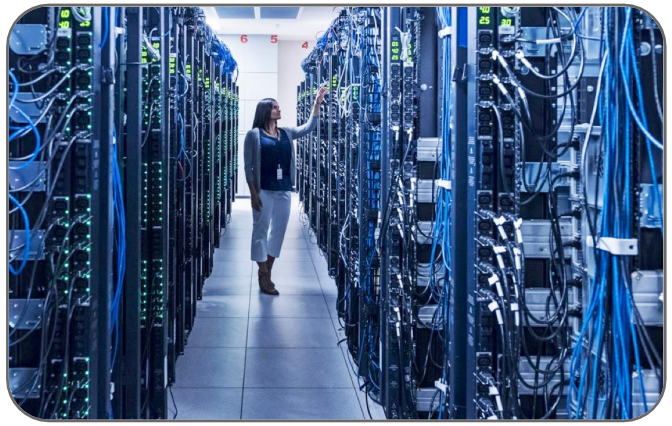
Dr. Ir. Adil Acun

November 2022

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ING Quantum

do your thing



Hedendaagse digitale computers

Wiskunde op Fysieke Apparaten

Informatiedragers: bits

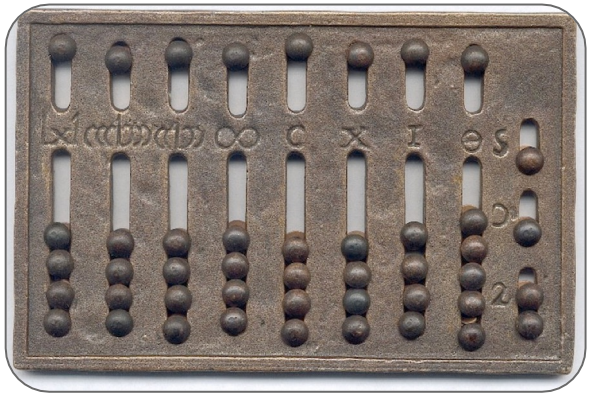
Wiskunde: boolean algebra

Apparaat: Laptop met een siliciumchip

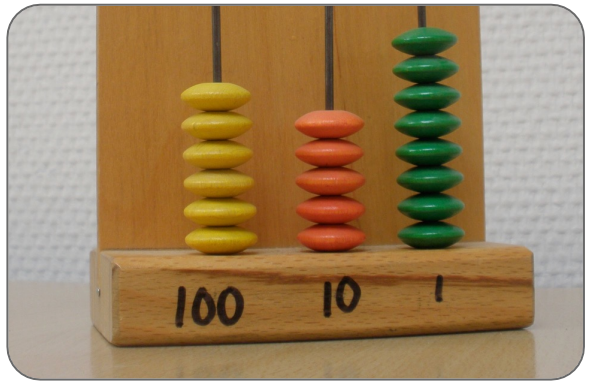
Transistor: binaire hoog/laag spanningswaarden

Ordinateur schikt beter als term voor hedendaagse computers; het brengt orde aan data

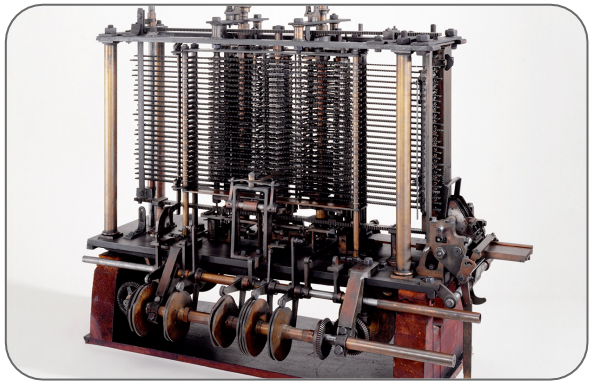
“Computation”: een uitvoering van een berekening



Telraam
Romeins



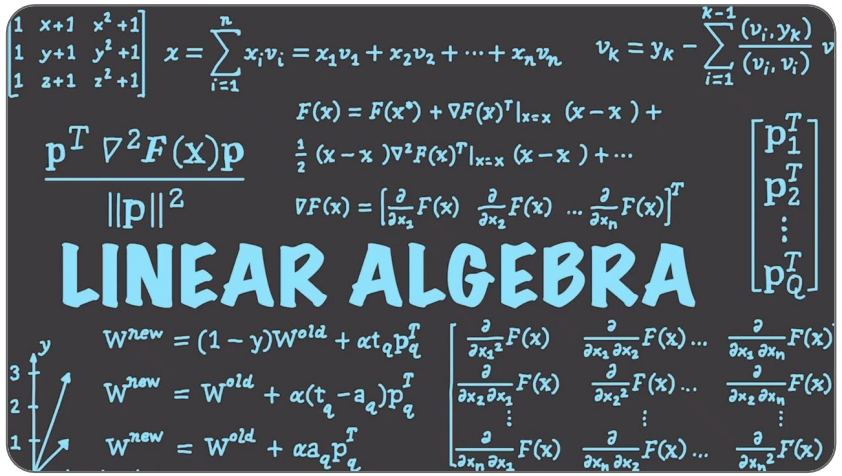
Telraam
Decimaal



Analytical Engine
Decimaal

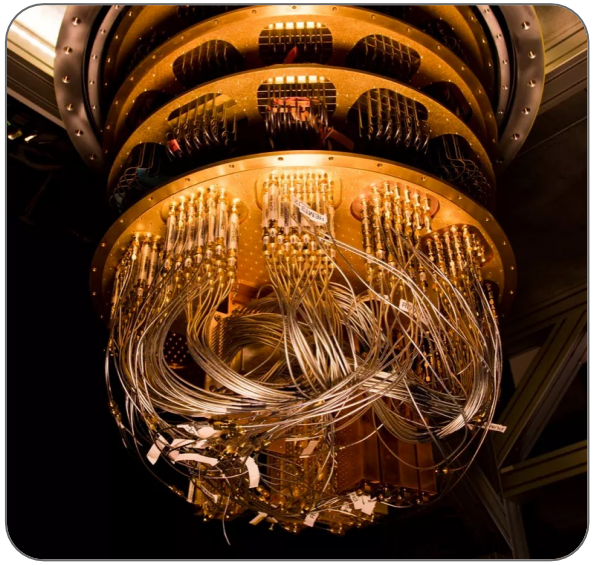
Hoofdrekenaars
Beroep

Wiskunde op Fysieke Apparaten



Informatiedragers: qubits

Wiskunde: lineaire algebra en kansberekeningen



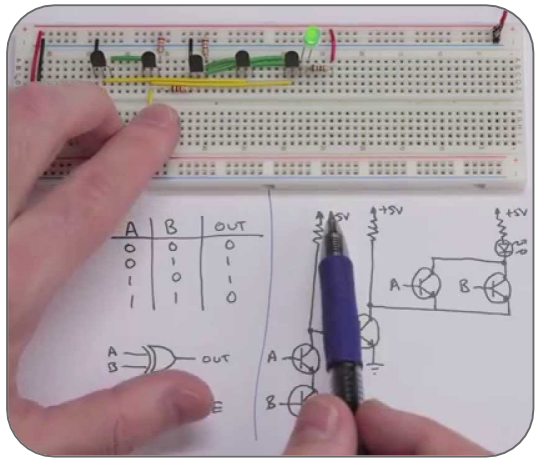
Apparaat: Quantum Computer

Fysica: quantummechanica

Lineaire algebra vindt zijn toepassingen in zeer verscheidene (wiskundige) vakgebieden

Concept van Quantum Computing

Vergelijking



Logische circuits

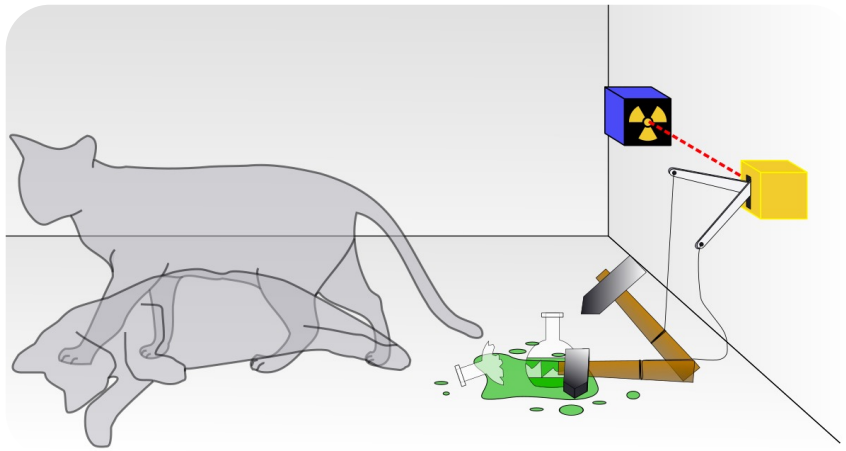
Bits
Gates (Poorten)

Wiskunde:
Boolean algebra

Quantum circuits

Qubits
Quantum-gates

Wiskunde:
Lineaire algebra

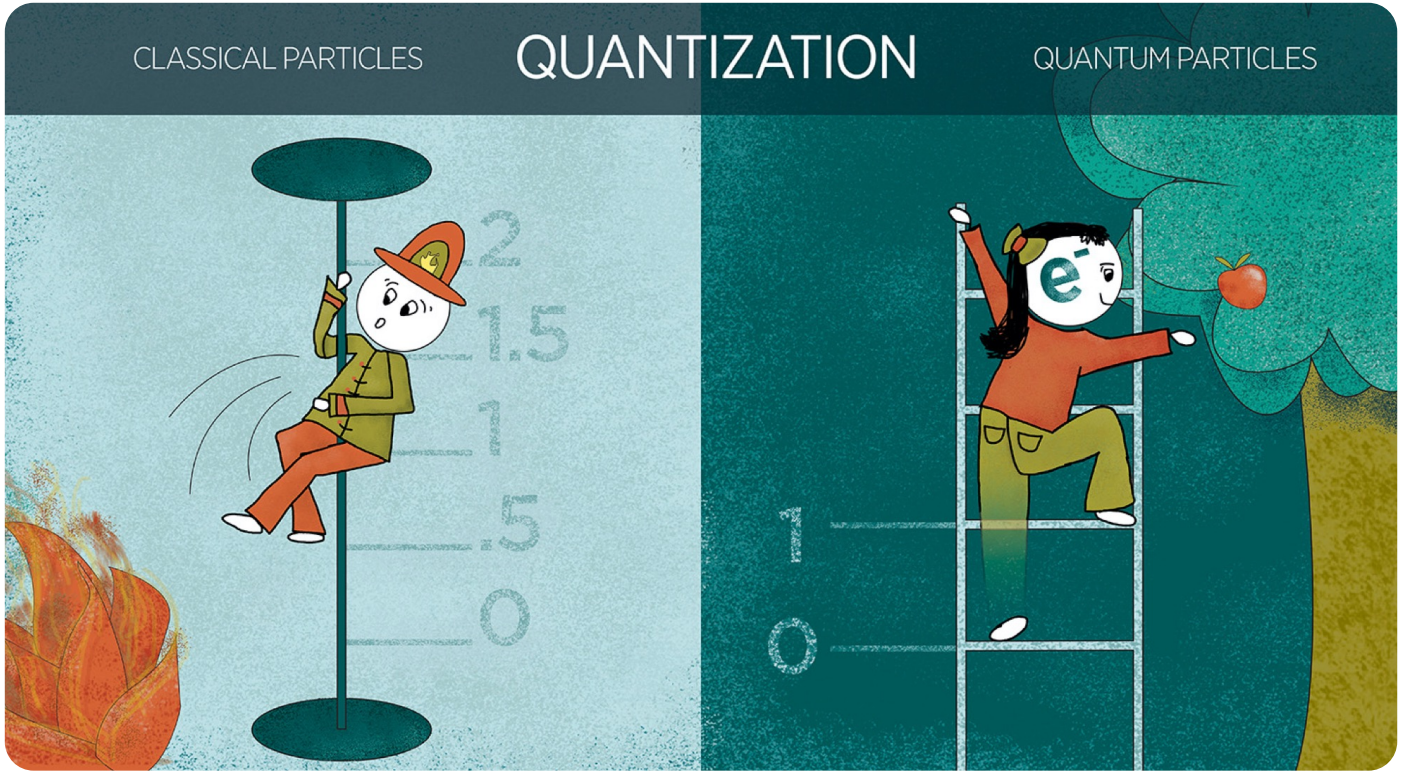


Onderliggende quantumfenomenen

Superposition / Superpositie
Entanglement / Verstrengeling
Interference / Interference
Measurement / Meting

Continue en Discrete Toestanden

Toestand: staat waarin iemand of iets zich bevindt



Discrete basistoestanden

$$|girl\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

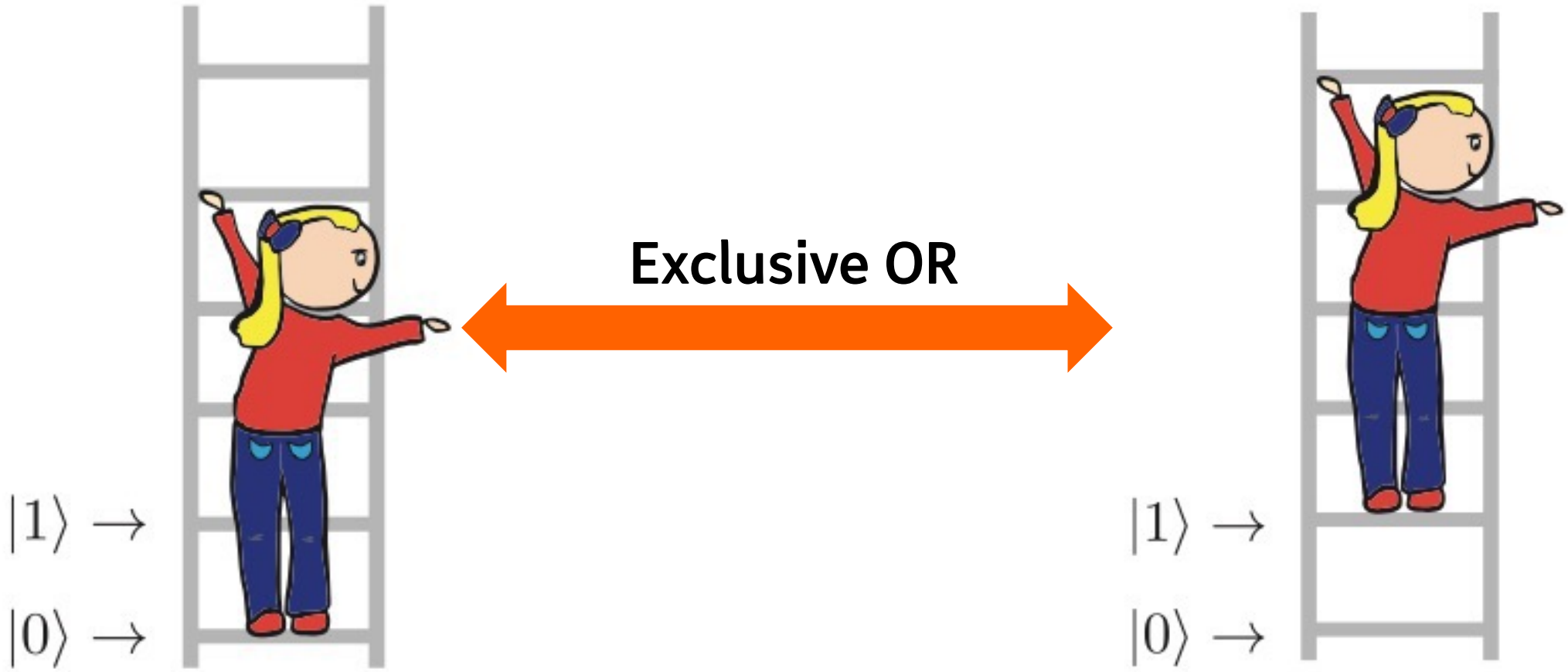
Toestand van object

Coefficienten (Verdeling)

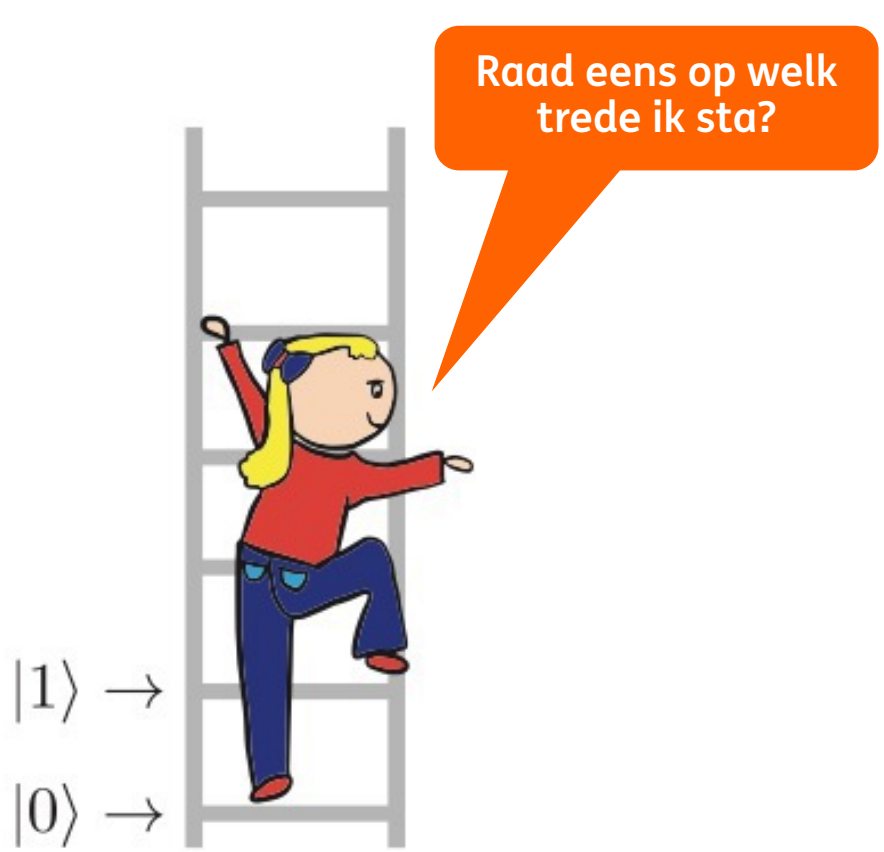
Image Author: N. Hanacek/NIST

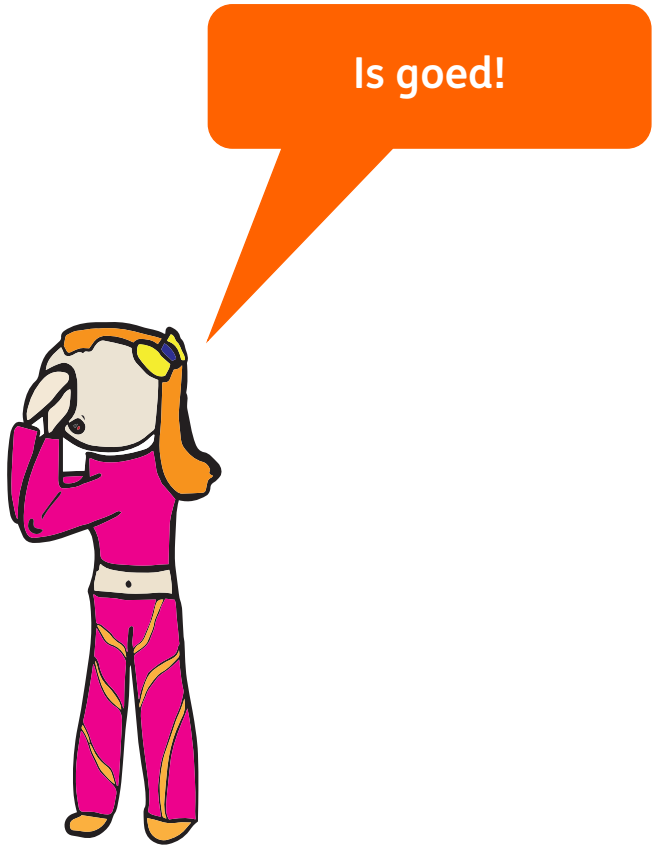
Deterministiche Toestanden

Uitsluitend één toestand op elk moment

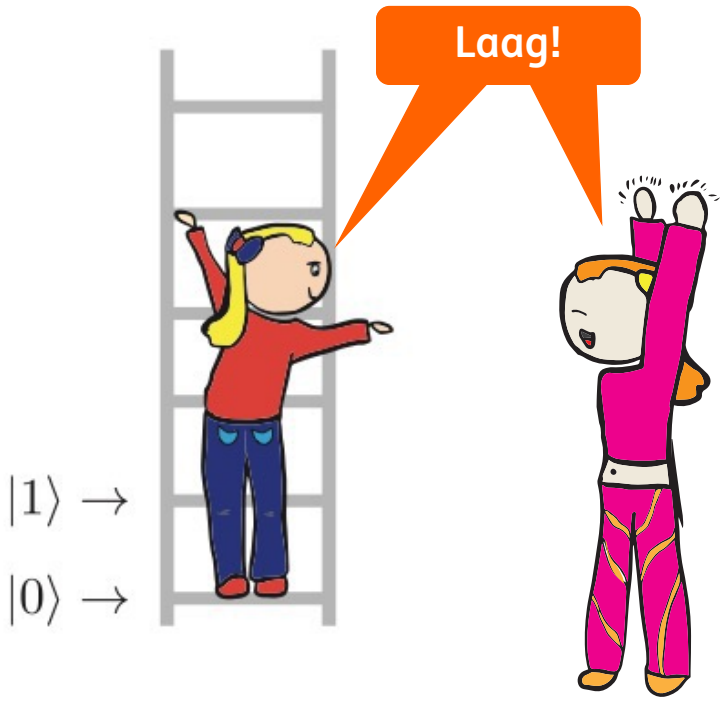


Stochastische Toestanden





Stochastische en Deterministische Toestanden



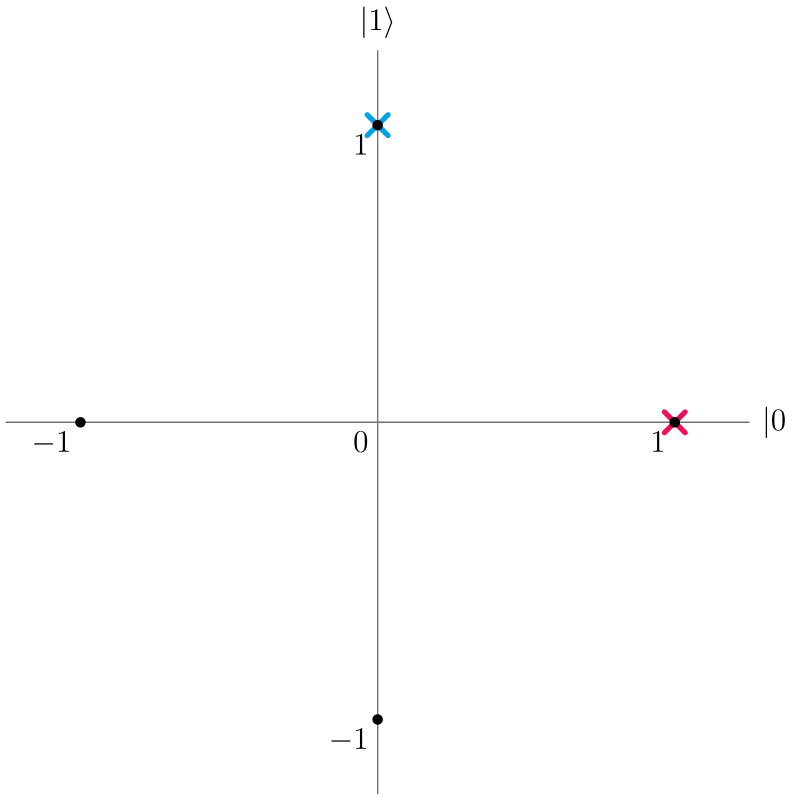
$$\vec{p} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} \xrightarrow{\text{Neem monster}} b = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

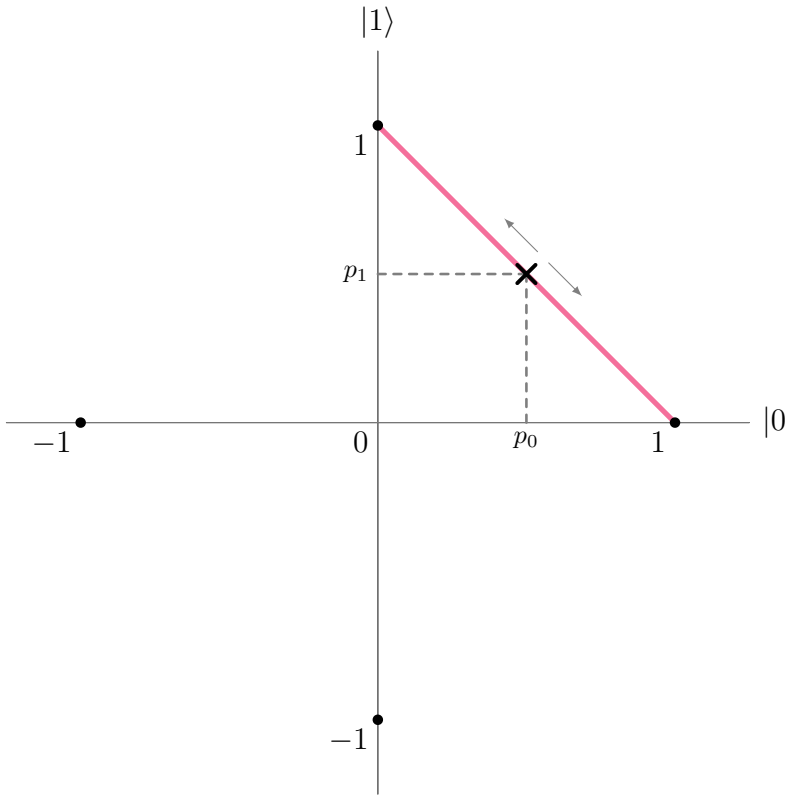
Stochastisch
Exact, verborgen

Deterministisch
Exact, waargenomen

Stochastische en Deterministische Toestanden

Grafische representatie





Quantum Toestanden

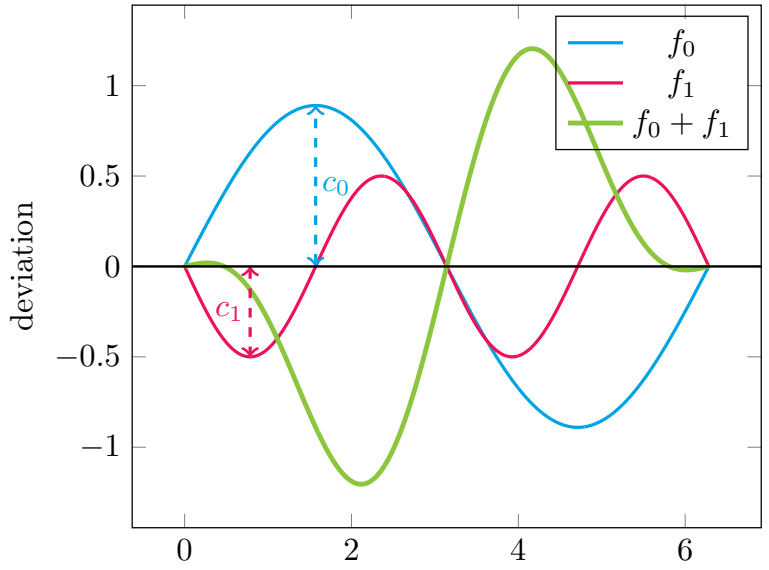
Samenspel van golven en kansen; Fase

Kansberekening

$$|coin\rangle = p_h\,|heads\rangle + p_t\,|tails\rangle$$

Waarschijnlijkheden tussen 0 en 1

Golven



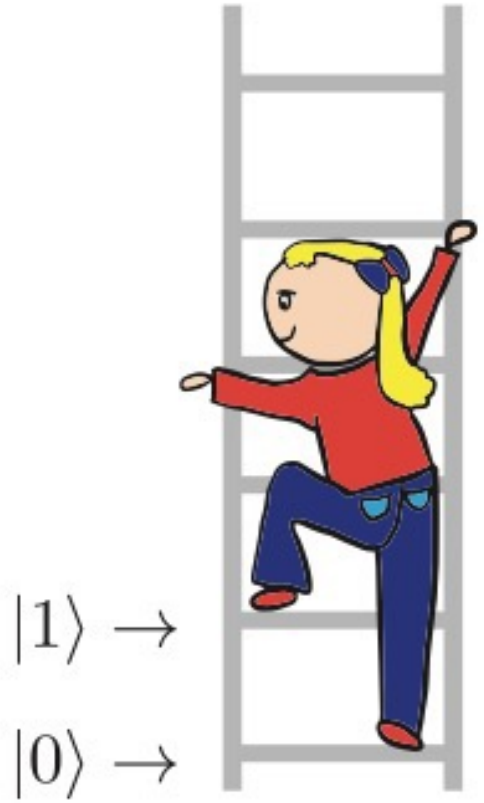
$$|u\rangle = c_0\,|0\rangle + c_1\,|1\rangle$$

Amplitudes kunnen elk getal aannemen

$$f_0(x) = \underbrace{\frac{\sqrt{3}}{2}}_{c_0}\underbrace{\sin(x)}_{|0\rangle} \qquad f_1(x) = \underbrace{-\frac{1}{2}}_{c_1}\underbrace{\sin(2x)}_{|1\rangle}$$

Quantum en Kansberekening

Verband tussen amplitudes en waarschijnlijkheden



$$p_0 + p_1 = 1 \iff c_0^2 + c_1^2 = 1$$

Quantum toestand: $|girl\rangle = \frac{-1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

$$p_0 = \frac{1}{4} \qquad p_1 = \frac{3}{4}$$

*Voor complexe getallen $p_i = |c_i|^2, \quad |c_0|^2 + |c_1|^2 = 1$

Randvoorwaarde aan Amplitudes

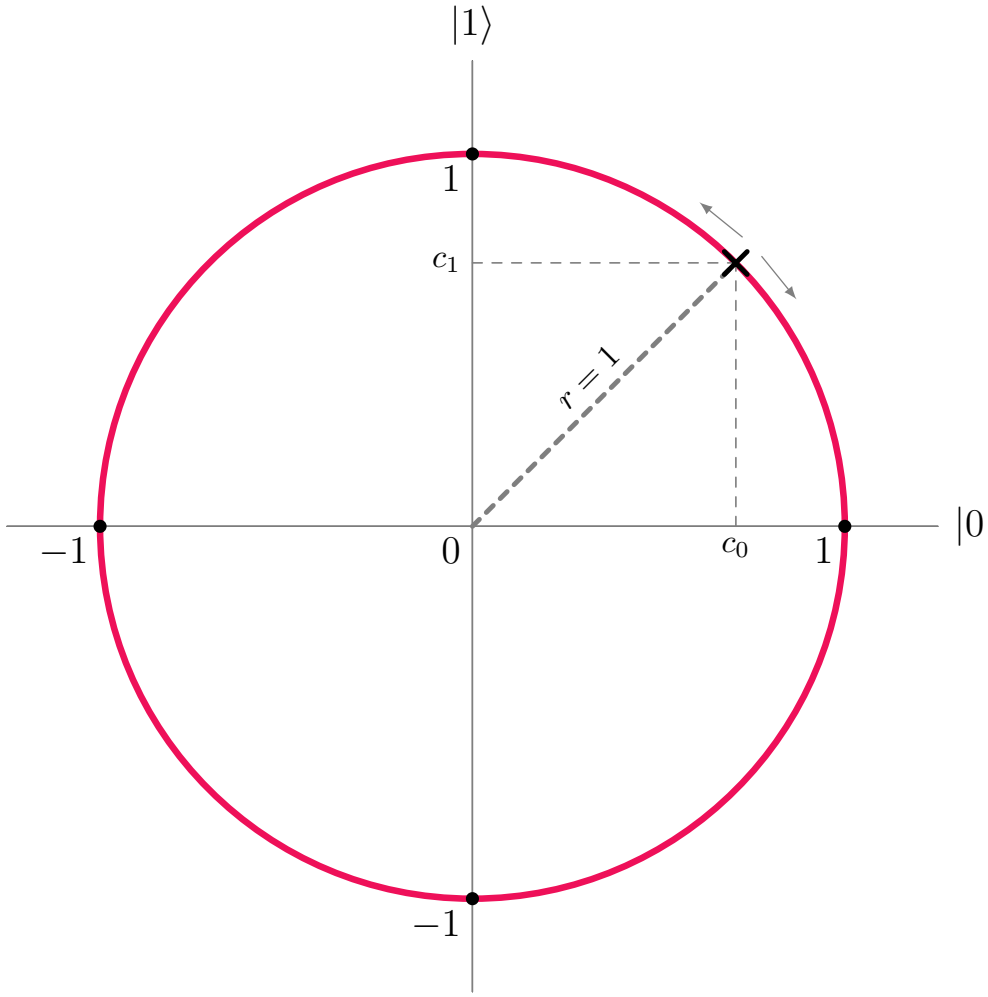
Totstandkoming van de Bloch cirkel

$$|girl\rangle = c_0 |0\rangle + c_1 |1\rangle$$

$$c_0^2 + c_1^2 = 1$$

Net als met Pythagoras!

$$a^2 + b^2 = c^2$$



*Voor complexe getallen gebruikt men een Bloch bol

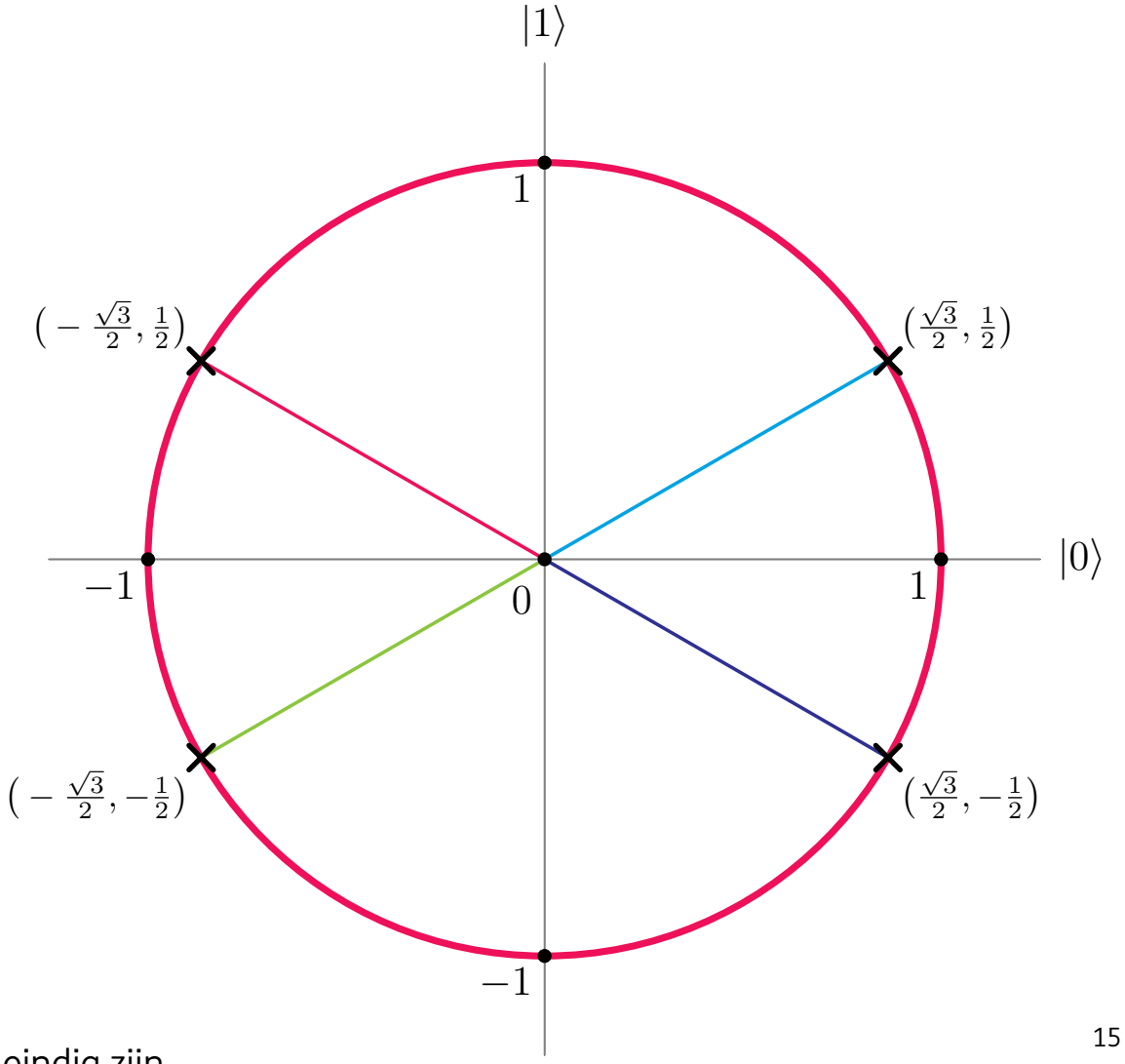
van Waarschijnlijkheden naar Amplitudes

Dubbelzinnigheid leidt tot onomkeerbaarheid

$$p_0 = \frac{3}{4} \qquad p_1 = \frac{1}{4}$$

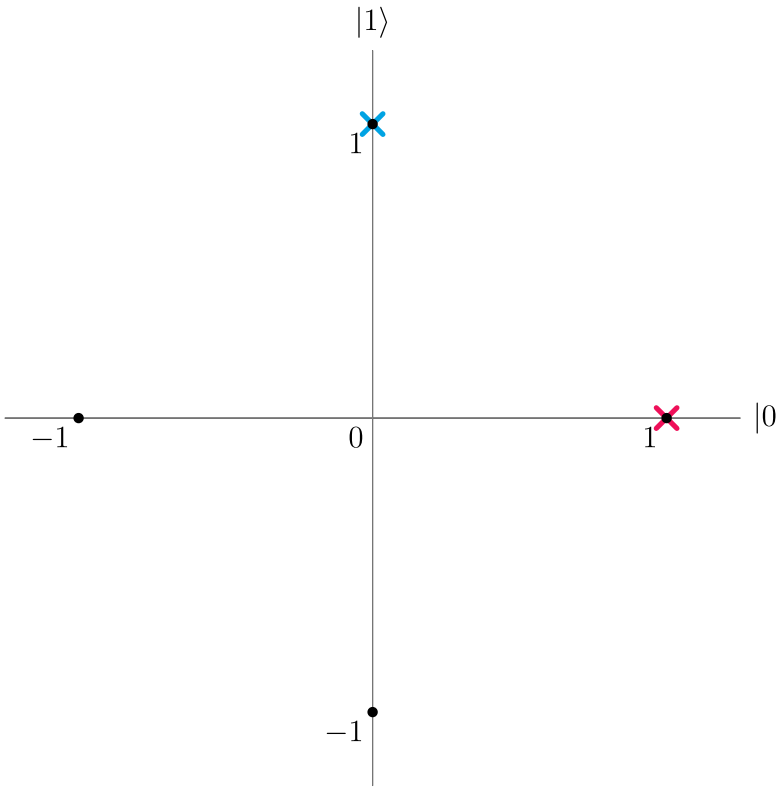
$$c_i = \sqrt{p_i}$$

$$c_0 = \pm\frac{\sqrt{3}}{2} \qquad c_1 = \pm\frac{1}{2}$$



*Voor complexe getallen kunnen de mogelijke coefficiëntencombinaties oneindig zijn

Deterministisch, Stochastisch en Quantum

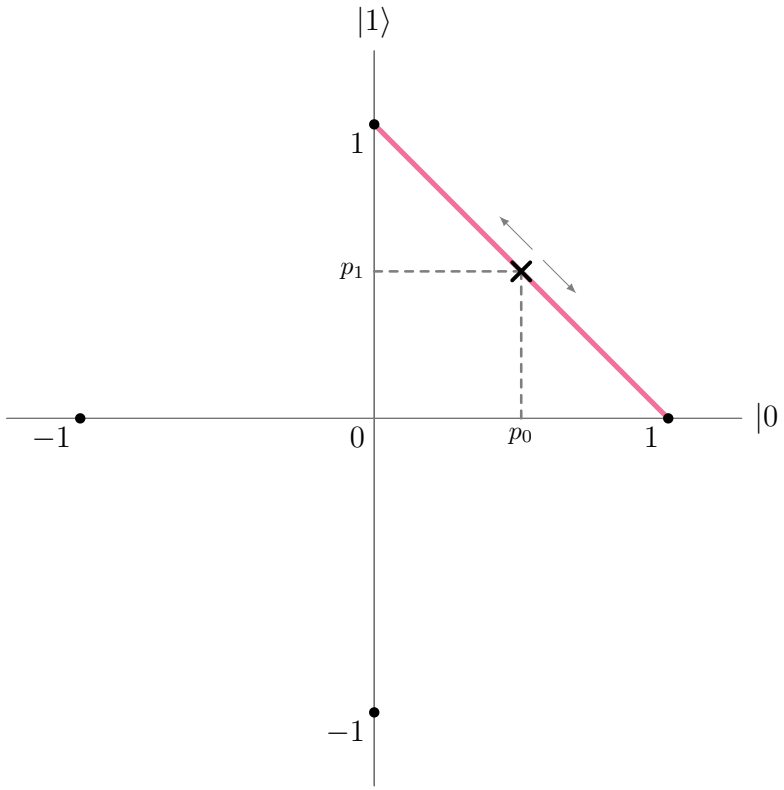


Klassieke Computer

Bits

0 of 1

Stay or switch operatoren

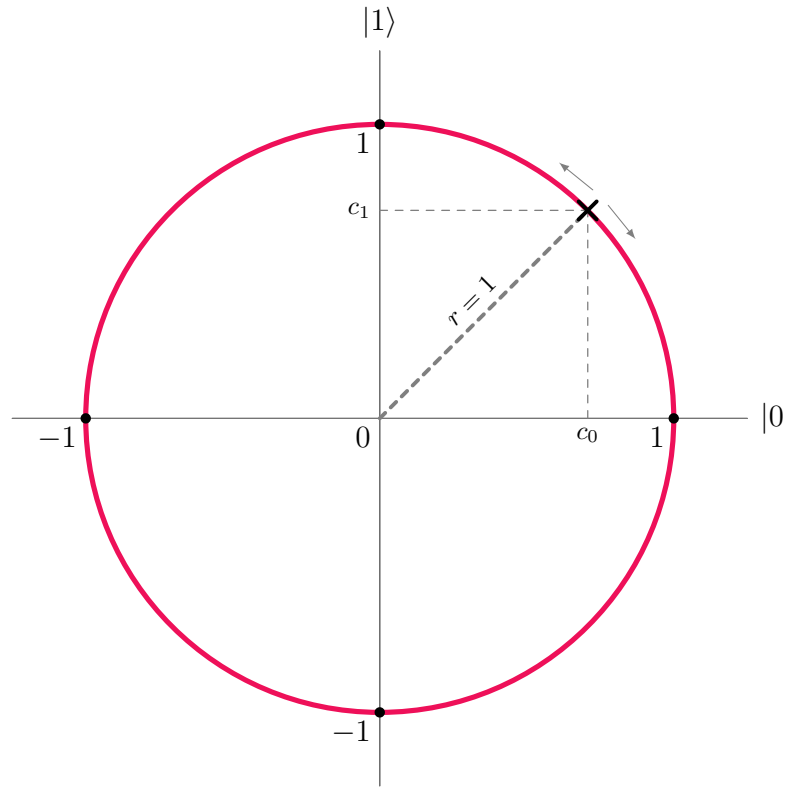


Probabilistic computing

P-bits

Fluctuaties tussen 0 en 1

Operatoren: verandering van waarschijnlijkheidsverdeling



Quantum computing

Qubits

Elk coördinaat op de cirkel

Operatoren: verandering van waarschijnlijkheidsverdeling en fase

Bloch Bol

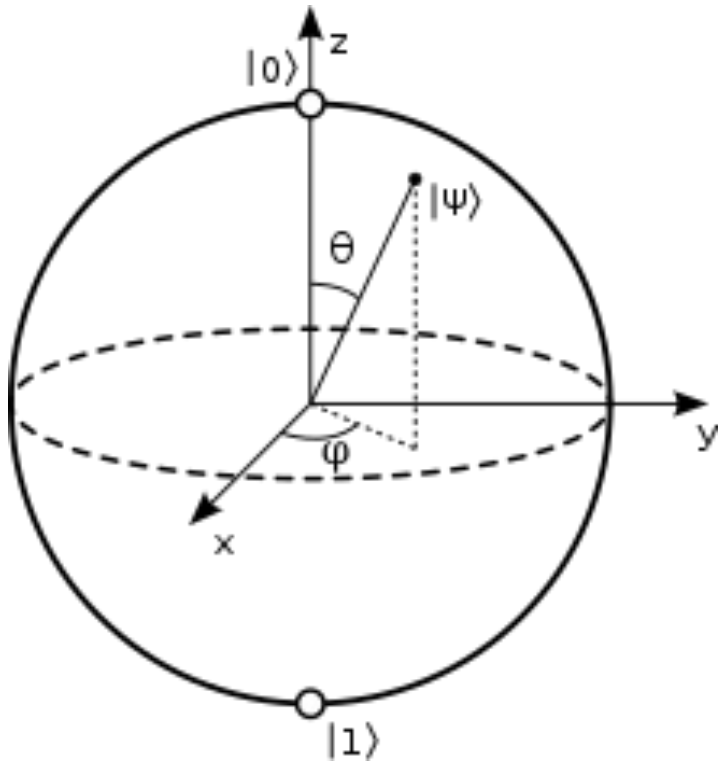
Representatie van een Qubit

Alle mogelijke qubittoestanden liggen op het **oppervlak**

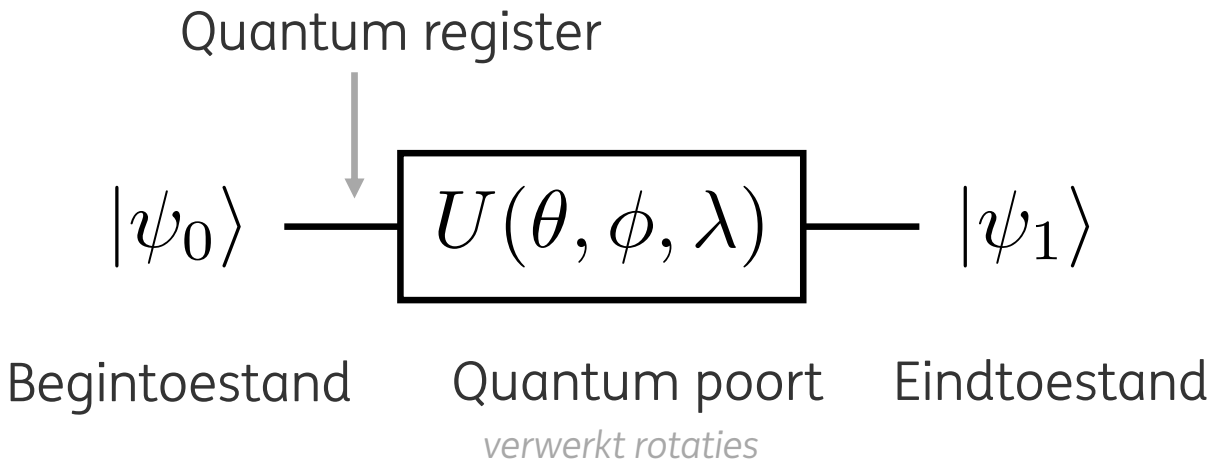
Informatieverwerking o.b.v. bewegen over het oppervlak,
leidt tot verandering in **amplitudes**,

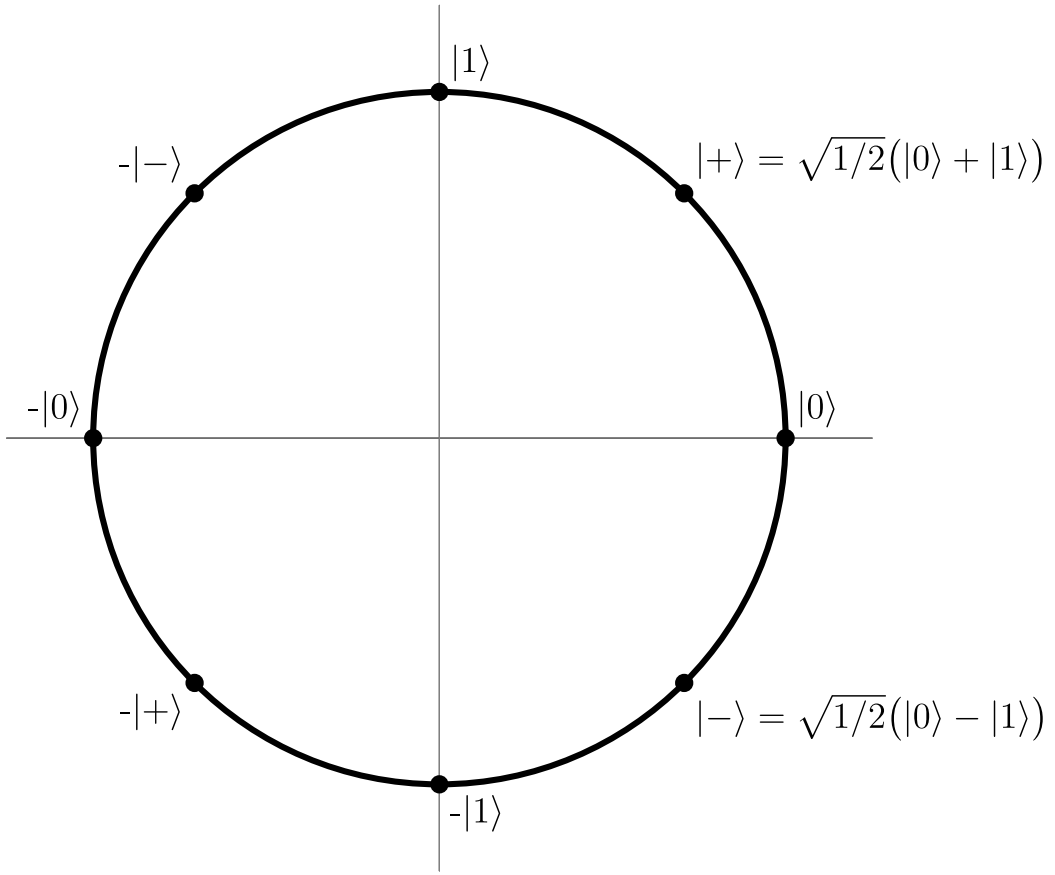
Toestand veranderingen door verticale bewegingen
(effect op de waarschijnlijkheidsverdeling)

Faseveranderingen door horizontale beweging
(geen effect op de waarschijnlijkheidsverdeling)



Quantum Circuit Model





De drie parameters maken elke rotatie mogelijk

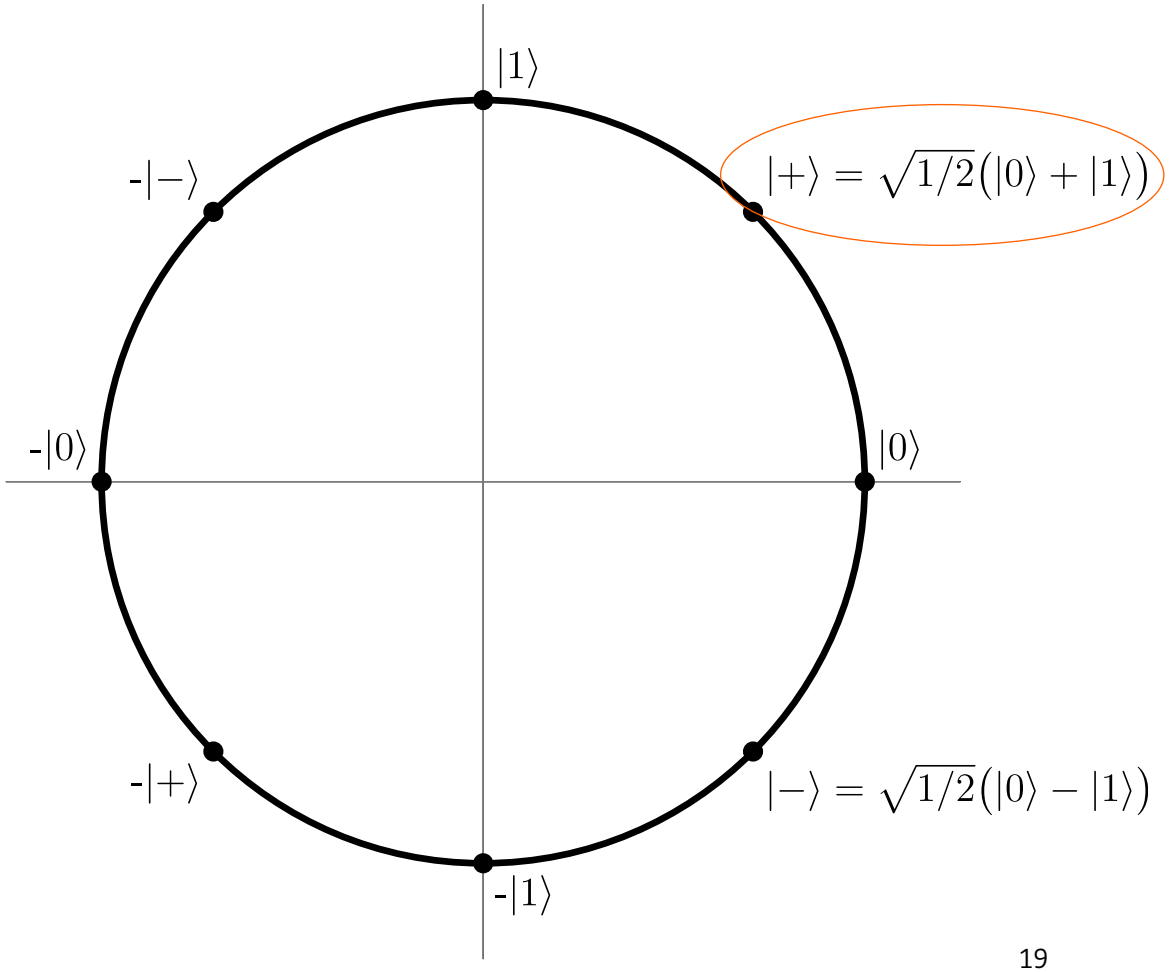
Quantum Effect 1: Superpositie

Superpositie:

Gelijktijdig voorkomen van meerdere toestanden.

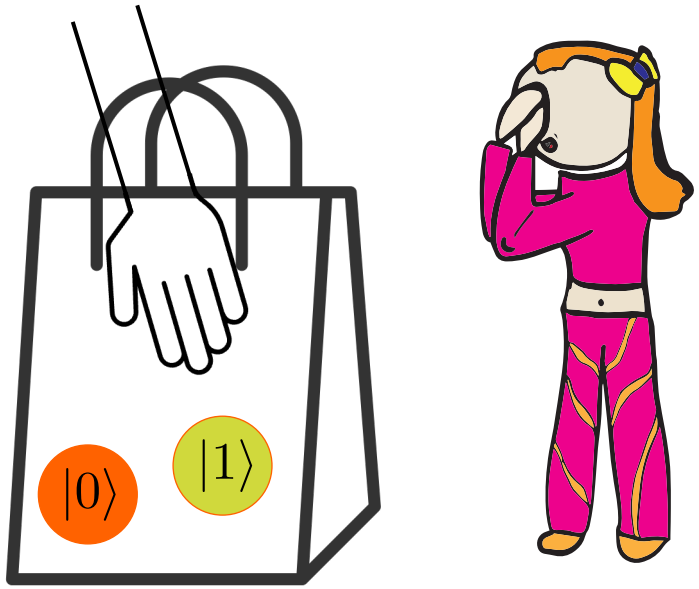
Leidt tot enorme parallelisme

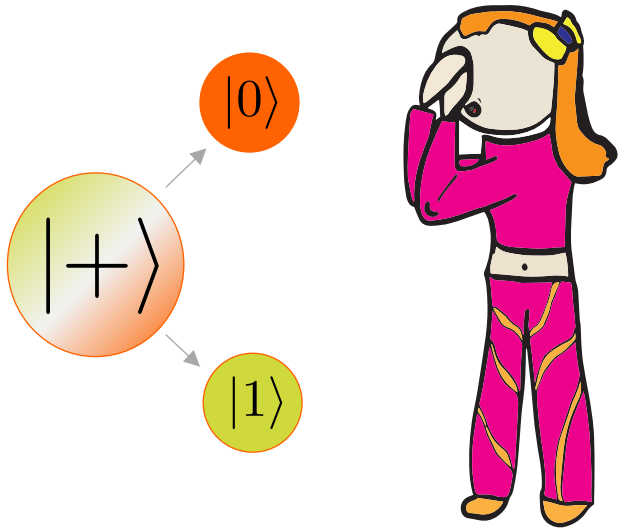
Enkel een superpositie zou geen speedup geven



Superpositie of Ensembles

Wezenlijk verschil, ondanks de gelijkwaardige verdelingen





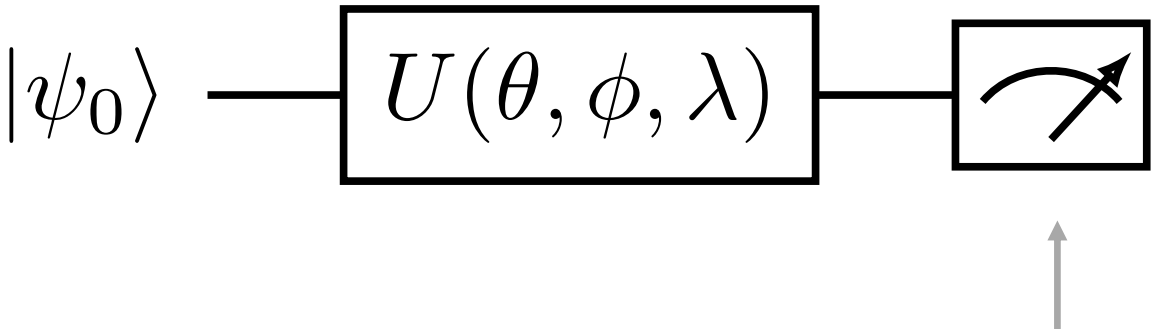
De zak is een **gemengde toestand**
Ensemble van een 0 en een 1
Beschreven door dichtheidsmatrices

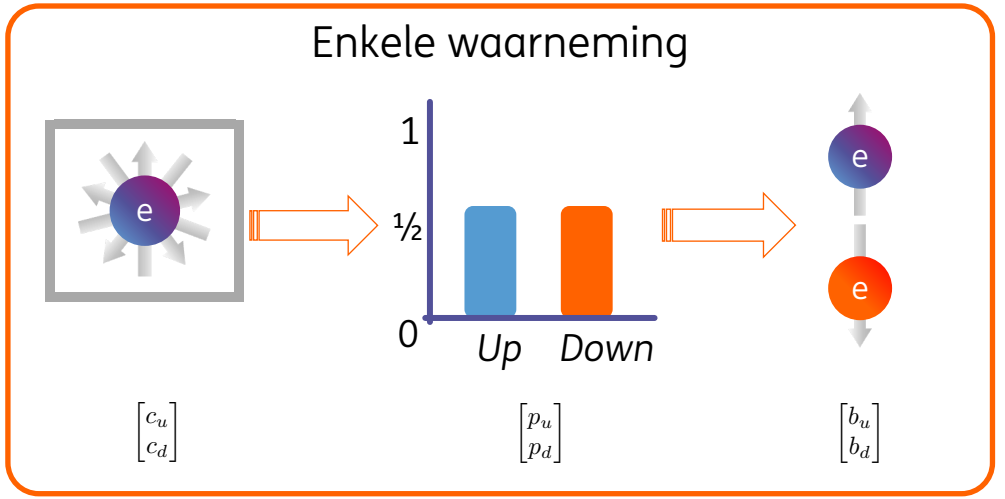
Een qubit is een **pure toestand**
Superpositie van 0 en 1
Beschreven door vectoren (of dichtheidsmatrices)

De zak mag ook meerdere pure quantumtoestanden bevatten

Quantum Effect 2: Meting

Instorting van de quantum toestand tot een deterministische toestand





Meting

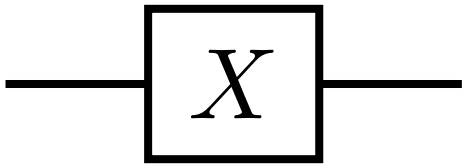
Keert een deterministische toestand terug
o.b.v. een waarschijnlijkheidsverdelingen
o.b.v. de amplitudes

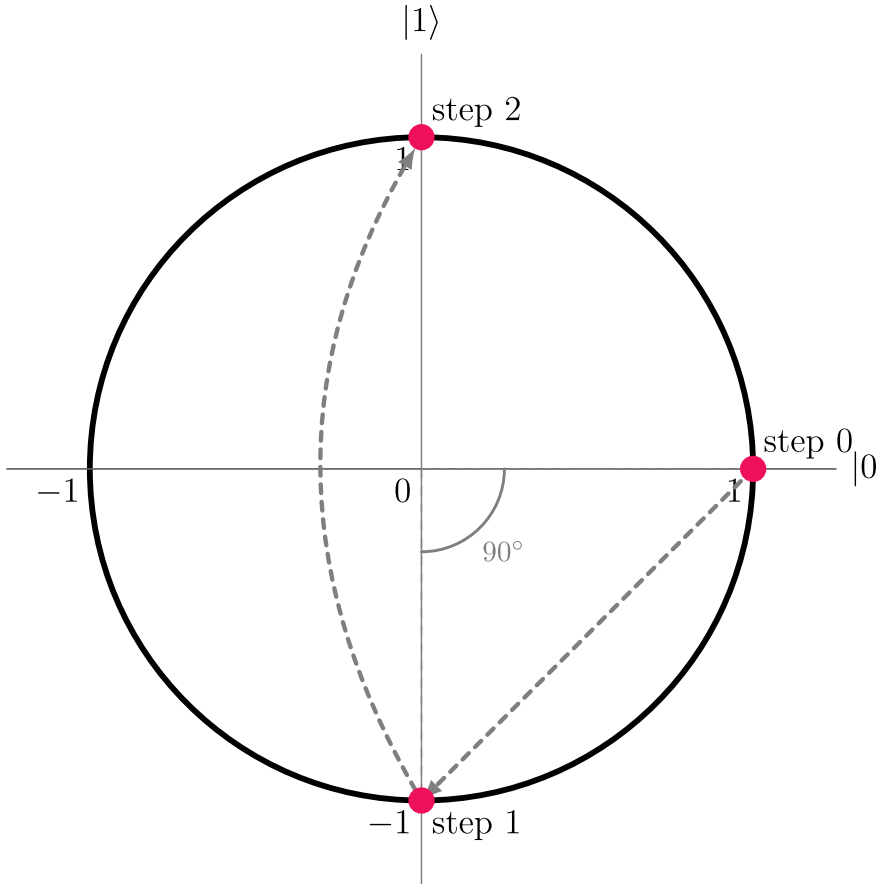
Enkel-qubit poorten

X-gate

1: **90° met de klok mee**

2: Spiegelen langs X-as





$$X = U(\pi, 0, \pi) \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

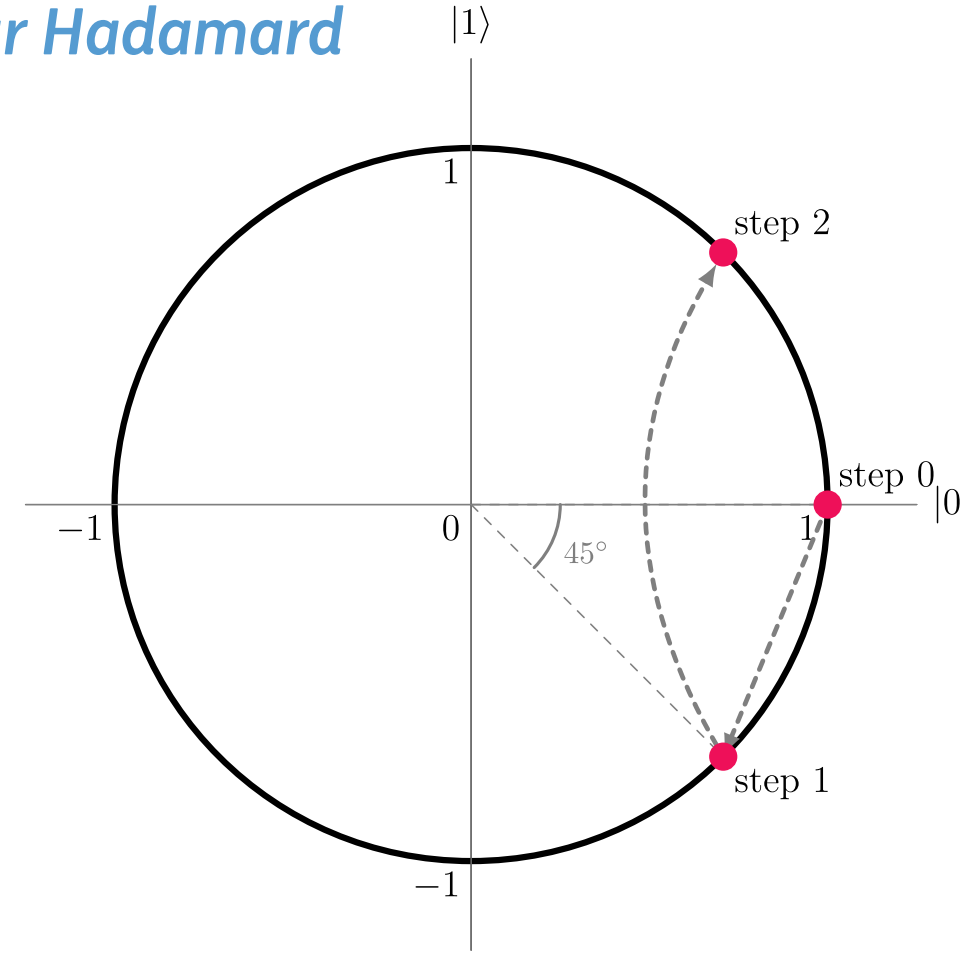
$$X\,|0\rangle = |1\rangle$$

Enkel-Qubit oorten

H-poort: vernoemd naar Hadamard

1: **45° met de klok mee**

2: Spiegelen langs X-as

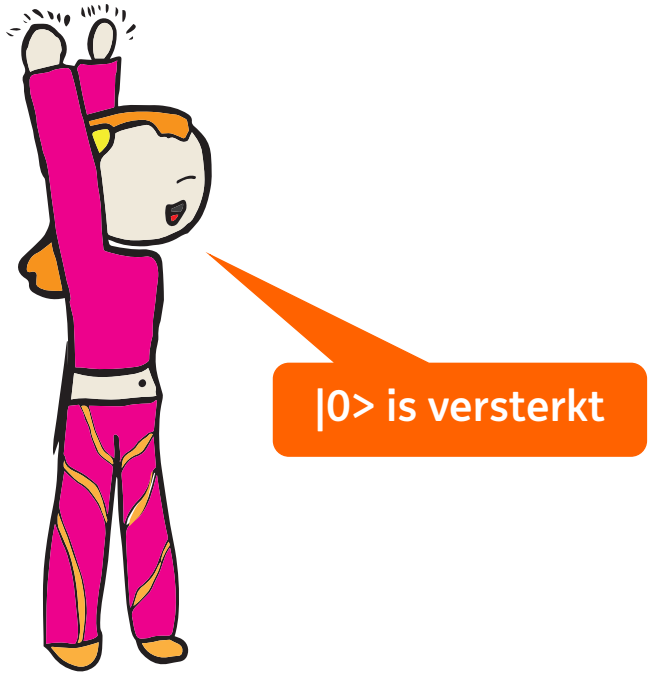


$$H\,|0\rangle = |+\rangle$$

$X = U(\pi/2, 0, \pi)$ $\frac{1}{2}\sqrt{2}\cdot\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{1}{2}\sqrt{2}\cdot\begin{bmatrix}\alpha+\beta\\ \alpha-\beta\end{bmatrix}$

Quantum Effect 3: Interferentie

Constructieve en Destructieve; bewerkstelligt zinvolle algoritmen

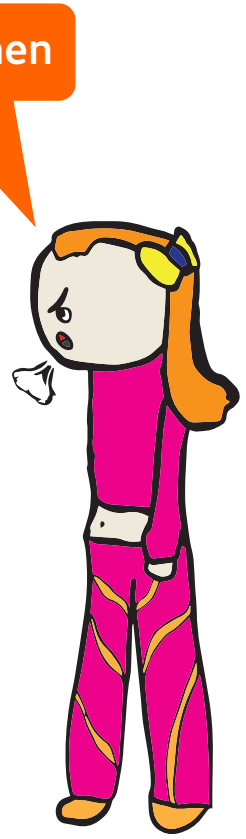


$$H|+\rangle = H|0\rangle + H|1\rangle$$

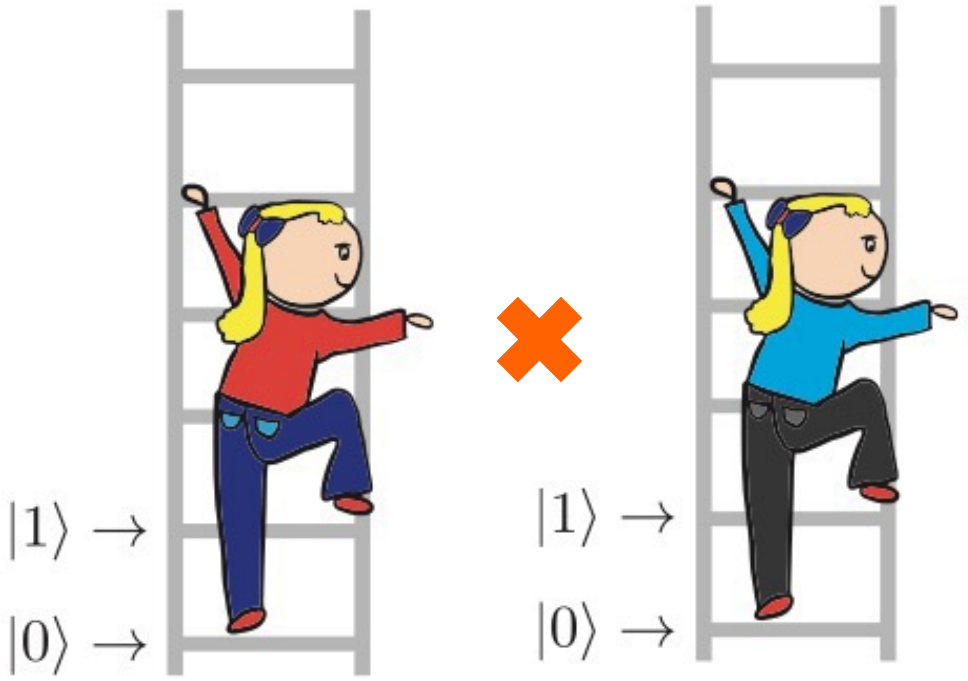
$$= |+\rangle + |-\rangle$$

$$= |0\rangle + |1\rangle + |0\rangle - |1\rangle$$

$$= |0\rangle$$



Multi-qubit toestanden



$$|girls\rangle = |red\rangle\,|blue\rangle$$

Basistoestanden

$$|girls\rangle = |0\rangle\,|0\rangle$$
$$|girls\rangle = |0\rangle\,|1\rangle$$
$$|girls\rangle = |1\rangle\,|0\rangle$$
$$|girls\rangle = |1\rangle\,|1\rangle$$

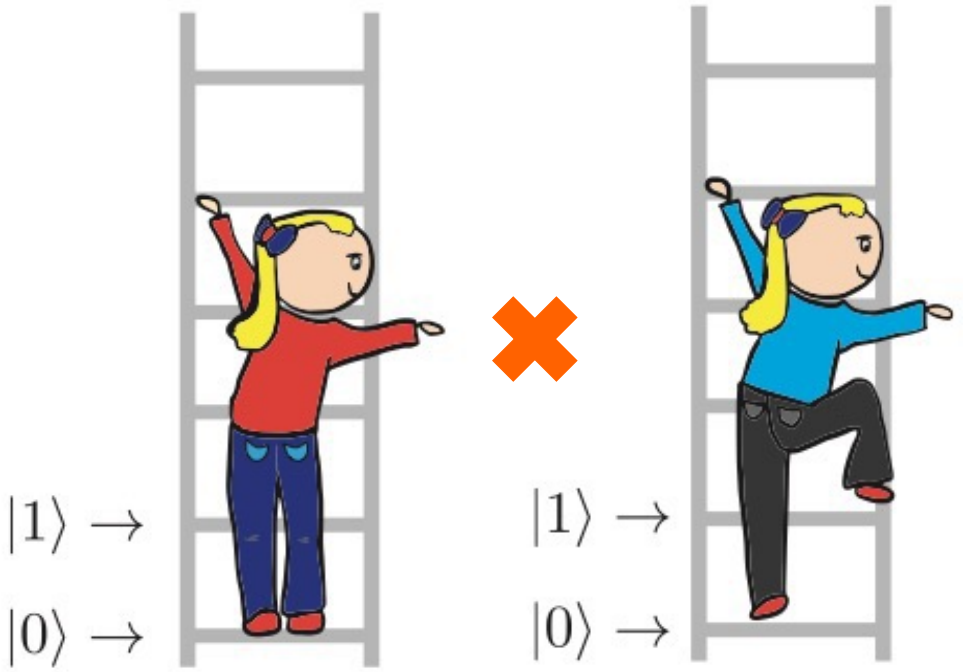
Quantum toestanden

$$|girls\rangle = c_{00}\,|0\rangle\,|0\rangle + c_{01}\,|0\rangle\,|1\rangle$$
$$+c_{10}\,|1\rangle\,|0\rangle + c_{11}\,|1\rangle\,|1\rangle$$

$$c_{ij} = c_i \cdot c_j$$

Multi-qubit toestanden

Voorbeeld

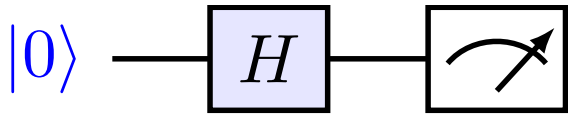


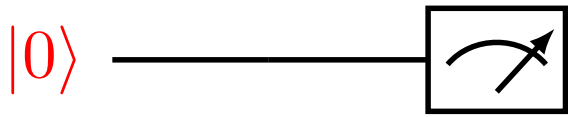
$$|girls\rangle = (\,|0\rangle\,)(\sqrt{1/2}\,|0\rangle + \sqrt{1/2}\,|1\rangle\,)$$

Verwerk alle combinaties $c_{ij} = c_i \cdot c_j$

$$c_0 = 1 \qquad c_0 = \frac{\sqrt{2}}{2}$$
$$c_1 = 0 \qquad c_1 = \frac{\sqrt{2}}{2}$$

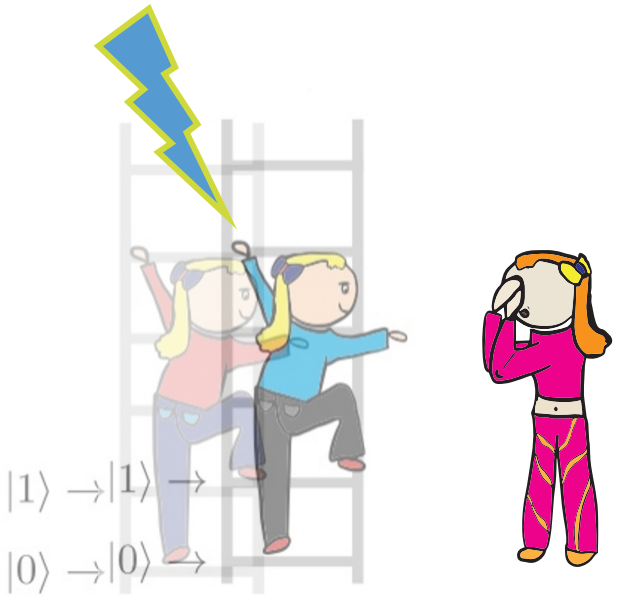
$$|girls\rangle = \frac{\sqrt{2}}{2}\,|0\rangle\,|0\rangle + \frac{\sqrt{2}}{2}\,|0\rangle\,|1\rangle$$





Quantum Effect 4: Verstrengeling

Sterk gecorreleerde toestanden



Herinnert u zich dit? $c_{ij} = c_i \cdot c_j$

Find the two amplitudes of the quantum state below

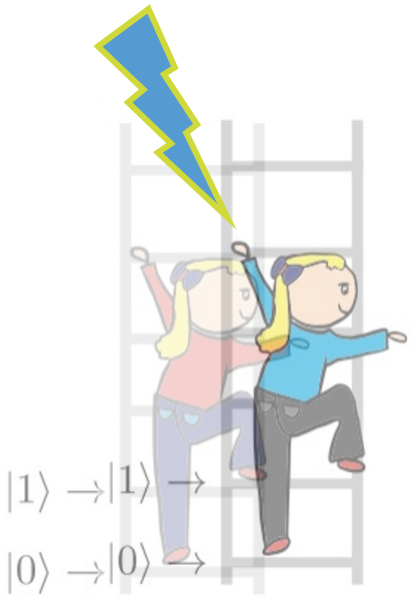
$$|girls\rangle = \frac{\sqrt{2}}{2}|0\rangle|0\rangle + \frac{\sqrt{2}}{2}|1\rangle|1\rangle$$

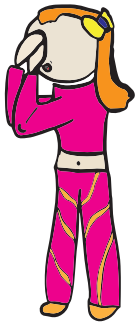
Impossible! The two states are not separable

Using conditional multi-qubit gates entanglement can be achieved on quantum computers

Quantum Effect 4: Verstrengeling

Sterk gecorreleerde toestanden





$$|girls\rangle = \frac{\sqrt{2}}{2}|0\rangle|0\rangle + \frac{\sqrt{2}}{2}|1\rangle|1\rangle$$

Schrijf als twee toestanden

$$(c_0|0\rangle + c_1|1\rangle) \otimes (c_0|0\rangle + c_1|1\rangle)$$

Vind de juiste amplitudes

$$c_0 \cdot c_0 = \frac{1}{\sqrt{2}} \qquad c_0 \cdot c_1 = 0 \qquad c_1 \cdot c_0 = 0 \qquad c_1 \cdot c_1 = \frac{1}{\sqrt{2}}$$

Onmogelijk! De twee toestanden kunnen niet onderscheiden worden

Meten van multi-qubit toestanden

Onafhankelijke toestanden en Verstrengelde toestanden

$$|girls\rangle = \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle + \frac{1}{2}|1\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle$$

meet rood meisje, resultaat: 0

$$|girls\rangle = \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle$$

meet blauw meisje, resultaat: 1

$$|girls\rangle = \frac{1}{2}|0\rangle|1\rangle$$

$$|girls\rangle = \frac{\sqrt{2}}{2}|0\rangle|0\rangle + \frac{\sqrt{2}}{2}|1\rangle|1\rangle$$

meet rood meisje, resultaat: 0

$$|girls\rangle = \frac{\sqrt{2}}{2}|0\rangle|0\rangle$$

Samenvatting van Quantum Effecten

Absoluut afwezig in klassieke computers

Superpositie:
Meerdere toestanden leven gelijktijdig en leveren parallelisme. Enkel superpositie geeft geen speedup.

Verstrengeld:
Sterke correlatie tussen meerdere toestanden. Een superpositie van deze correlaties kan leiden tot enorme speedups.

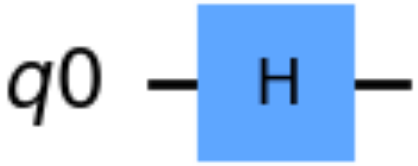
Interferentie:
Toestanden die versterkt of gedimd kunnen worden. Dit kan leiden tot zinvolle algoritmiek.

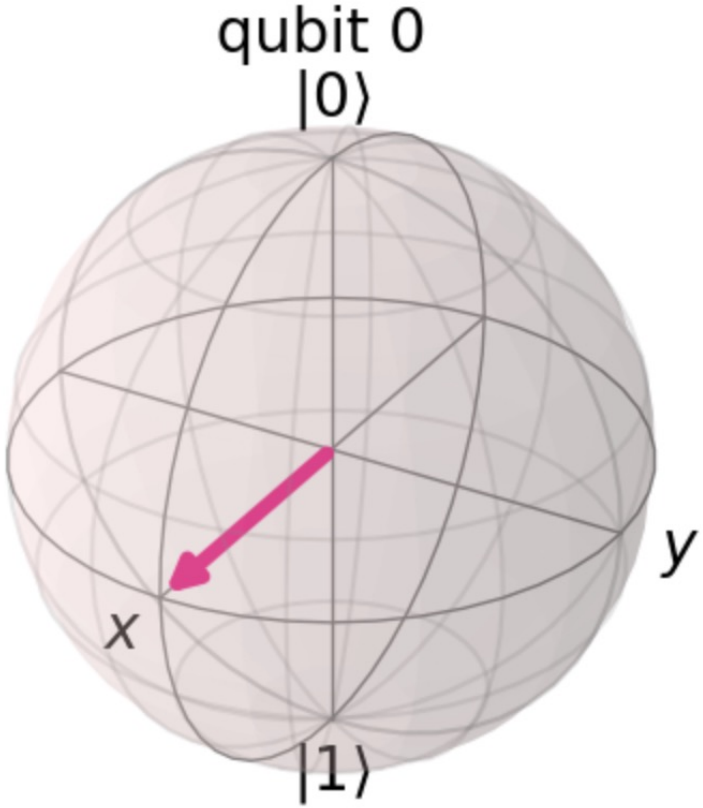
Meting:
Quantum toestanden storten ineen en worden deterministische discrete toestanden. Veelvuldig herhalen van experimenten leidt tot een waarschijnlijkheidsverdeling. Belangrijk om een circuit te leiden tot gewenste / nuttige klassieke toestanden waaruit een oplossing te herleiden valt.

Quantum Computing met Python

Statevector Simulatie

```
q = QuantumRegister(1) # qubit
circ = QuantumCircuit(q) # circuit

# H-gate on quantum register
circ.h(q[0])

# choose a backend, simulators or real q. computers
backend = BasicAer.get_backend('statevector_simulator')

# execute experiment on backend
job = execute(backend=backend, experiments=circ)

# get results
results = job.result()

# get statevector
statevector = results.get_statevector(circ)

# plot results
plot_bloch_multivector(statevector)
```

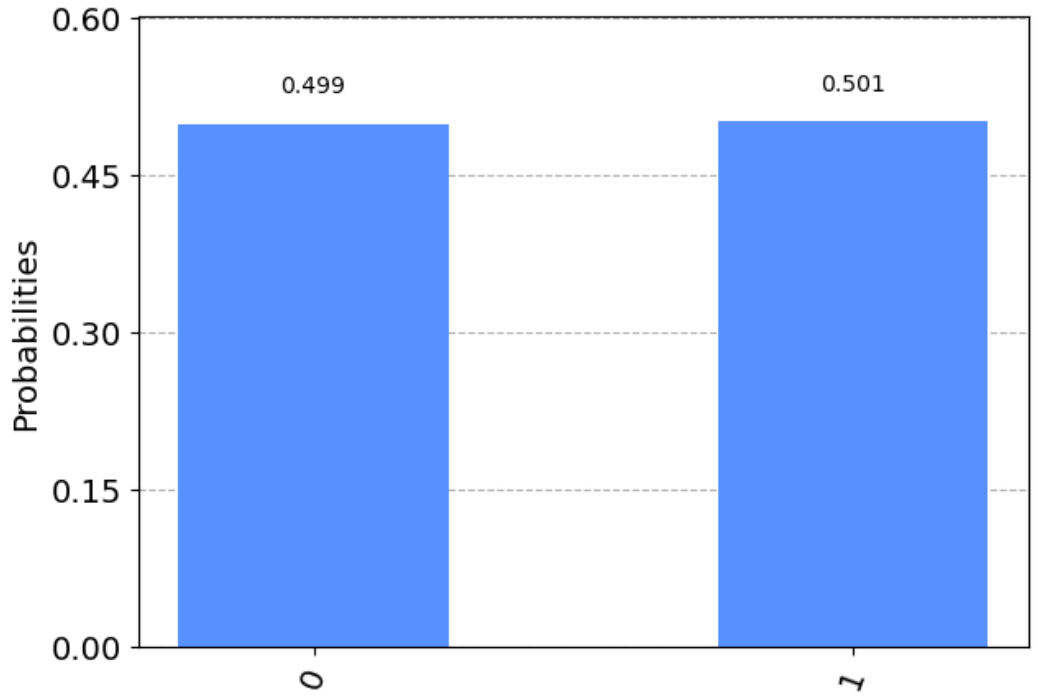




Quantum Computing met Python

Ruisvrije simulaties met metingen

```
q = QuantumRegister(1) # qubit
c = ClassicalRegister(1) # deterministic state
circ = QuantumCircuit(q, c) # circuit

# H-gate on quantum register
circ.h(q[0])

circ.measure(q, c) # measure circuit

circ.draw() # draw the circuit

# choose a backend, simulators or real q. computers
backend = BasicAer.get_backend('qasm_simulator')

# execute experiment on backend
job = execute(backend=backend, shots=10000, experiments=circ)

# get results
results = job.result()

# get count distribution
counts = results.get_counts(circ)

# plot results
plot_histogram(counts)
```



Quantum Computing with Python

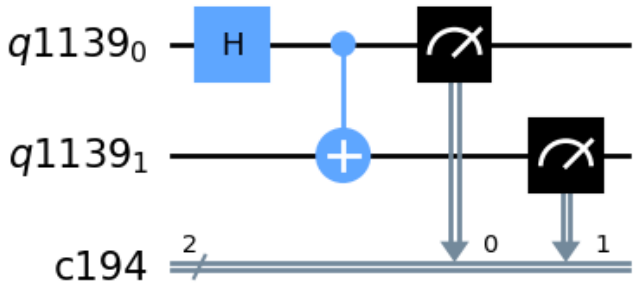
Op echte IBMQ hardware

```
from qiskit import IBMQ
from qiskit.compiler import transpile, assemble

IBMQ.save_account(token) # get from IBMQ account (it's a string)
IBMQ.load_account()

provider = IBMQ.get_provider()
provider.backends(simulator=False, operational=True)
```

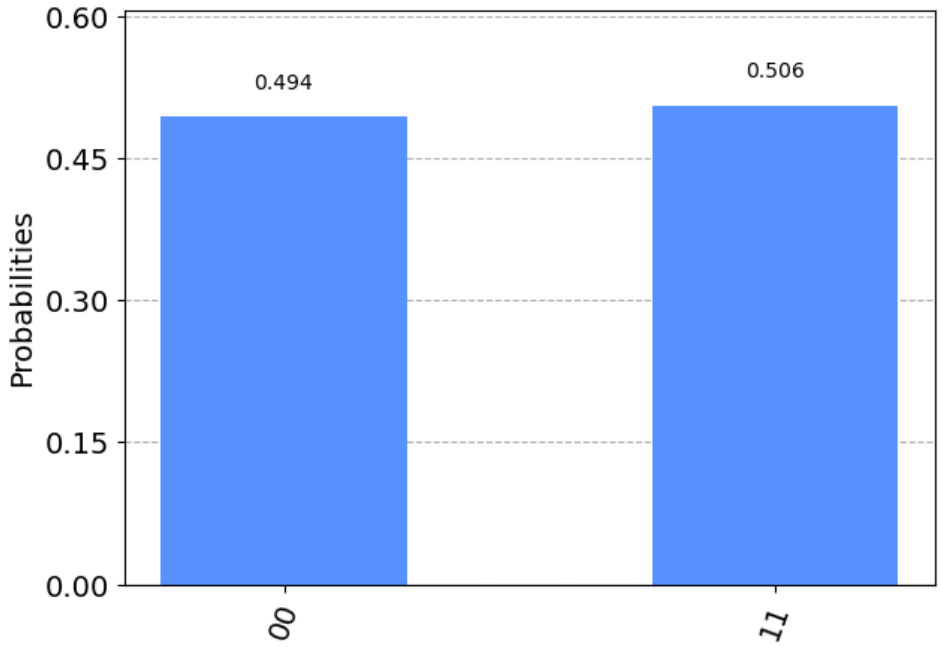
```
[<IBMQBackend('ibmq_lima') from IBMQ(hub='ibm-q', group='open', project='main')>,
 <IBMQBackend('ibmq_belem') from IBMQ(hub='ibm-q', group='open', project='main')>,
 <IBMQBackend('ibmq_quito') from IBMQ(hub='ibm-q', group='open', project='main')>,
 <IBMQBackend('ibmq_manila') from IBMQ(hub='ibm-q', group='open', project='main')>,
 <IBMQBackend('ibm_nairobi') from IBMQ(hub='ibm-q', group='open', project='main')>,
 <IBMQBackend('ibm_oslo') from IBMQ(hub='ibm-q', group='open', project='main')>]
```

Quantum Computing met Python

Op echte hardware: een verstrengelingsexperiment

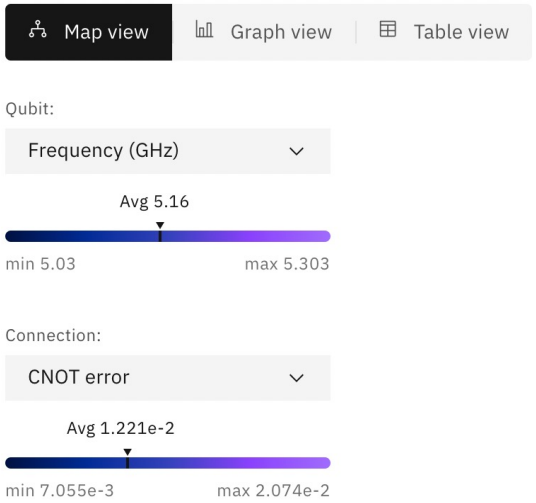


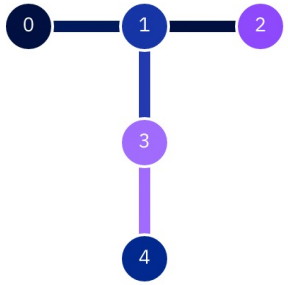

```
real_backend = provider.get_backend('ibmq_lima')
mapped_circuit = transpile(circ, backend=real_backend)
qobj = assemble(mapped_circuit, backend=backend, shots=10000)
job = backend.run(qobj)

result = job.result()
counts = result.get_counts(circ)
plot_histogram(counts)
```

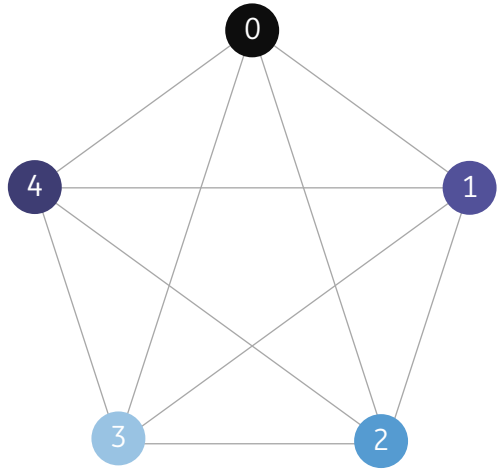


Quantum Computing met Python

De Lima Backend; connectiviteit van qubits







De Lima backend

Verstrengeling tussen 0 en 4: opoffering van 1 en 3

Kan 0 and 3 niet gelijktijdig verstrengelen met 2 en 4

Door ruis moeten berekeningen in ondiepe circuits plaatsvinden

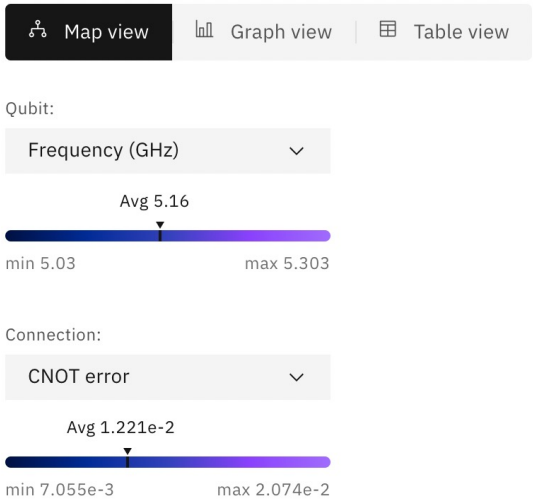
Ideaal 5 qubit systeem

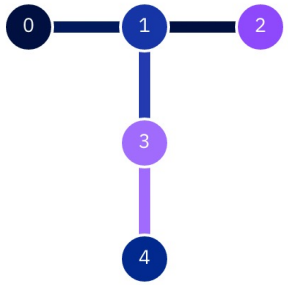
Geen opofferingen nodig

Zo goed als ruisloos: zeer diepe circuits

Quantum Computing met Python

NISQ-Tijdperk





De Lima backend

Verminderde connectiviteit ->
verminderde toepasselijkheid

Qubits zijn niet homogeen

Foutenpercentage van poorten: ondiepe circuits

Pas allerlei technieken toe:
Errorcorrecties
Optimaal mappen van qubits

Richting Toepassingen

M.b.v. quantumfenomenen

Verstrengel een input met een output middels een (wiskundige) functie

Start met een superpositie van alle inputs

$$|\psi\rangle = c_0 \, |x_0, f(x_0)\rangle + c_1 \, |x_1, f(x_1)\rangle + \ldots + c_n \, |x_n, f(x_n)\rangle$$

Doe wat met de amplitudes tot het algoritme zijn doel bereikt

Veelal door interferentie

Ongesorteerd zoekopdracht

Bevindt de vogel zich in het lijstje

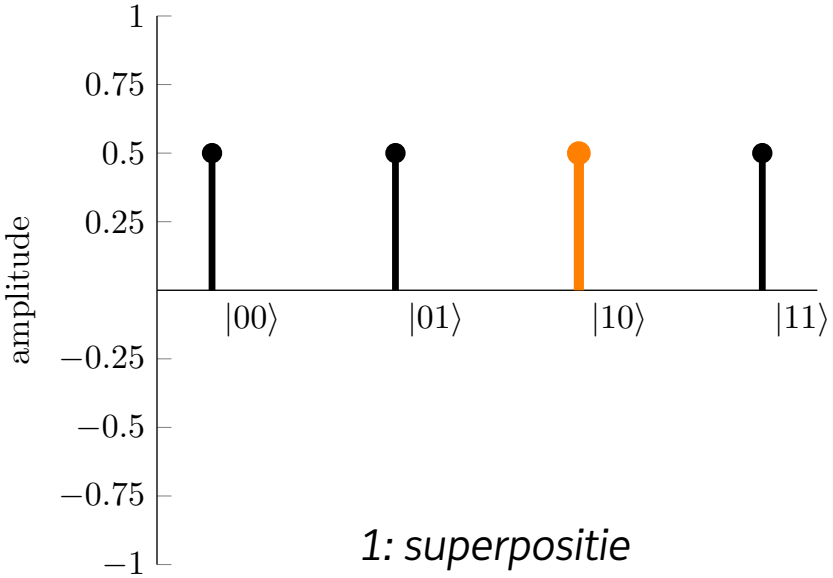
Name	Binary Label
Cat	00
Hamster	01
Bird	10
Dog	11

$$\mathcal{O}(N)$$

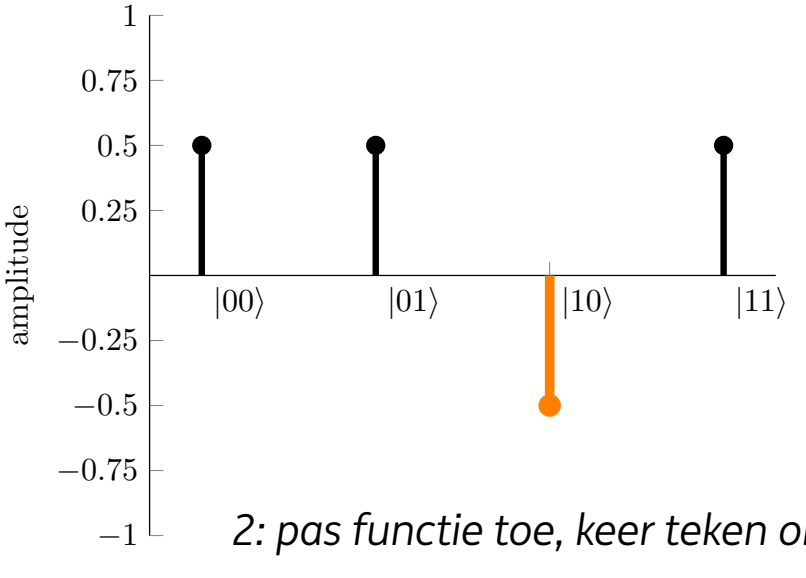
Klassiek, max. 4 stappen

Functie voor het quantumalgoritme $$f(x) = \begin{cases} -1 & \text{if } x = target \\ 1 & \text{otherwise} \end{cases}$$

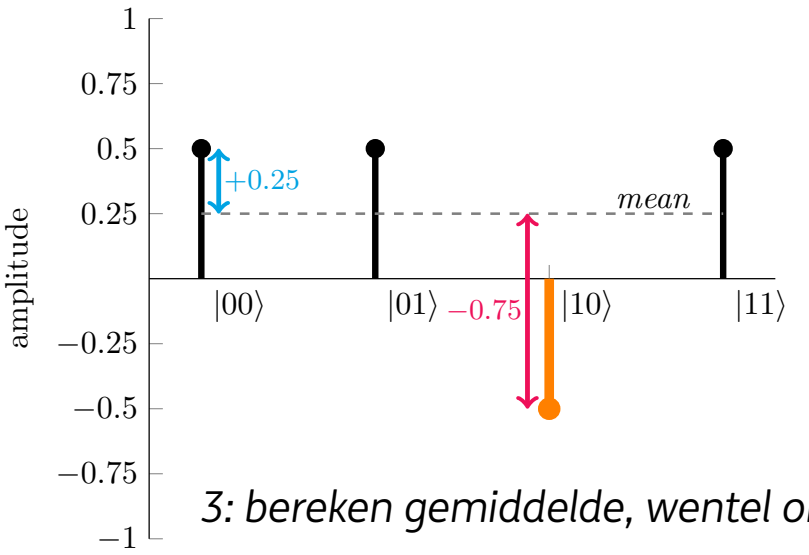
Grover's Algoritme



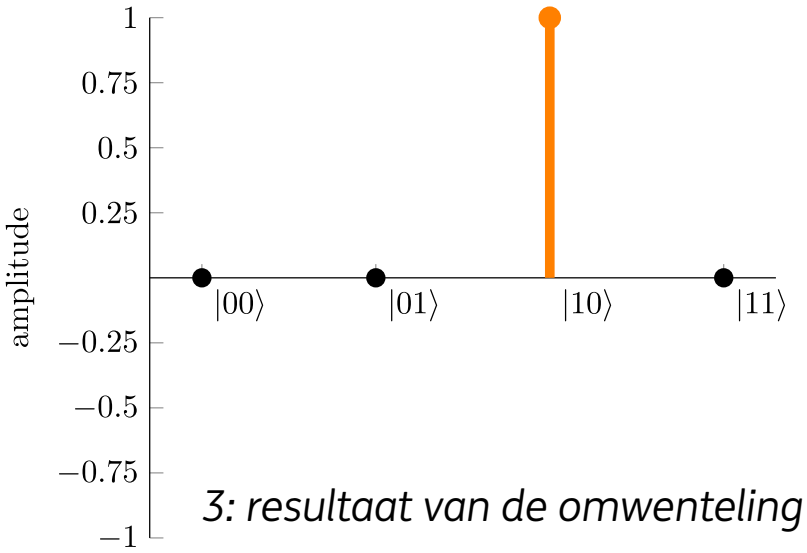
1: superpositie



2: pas functie toe, keer teken om

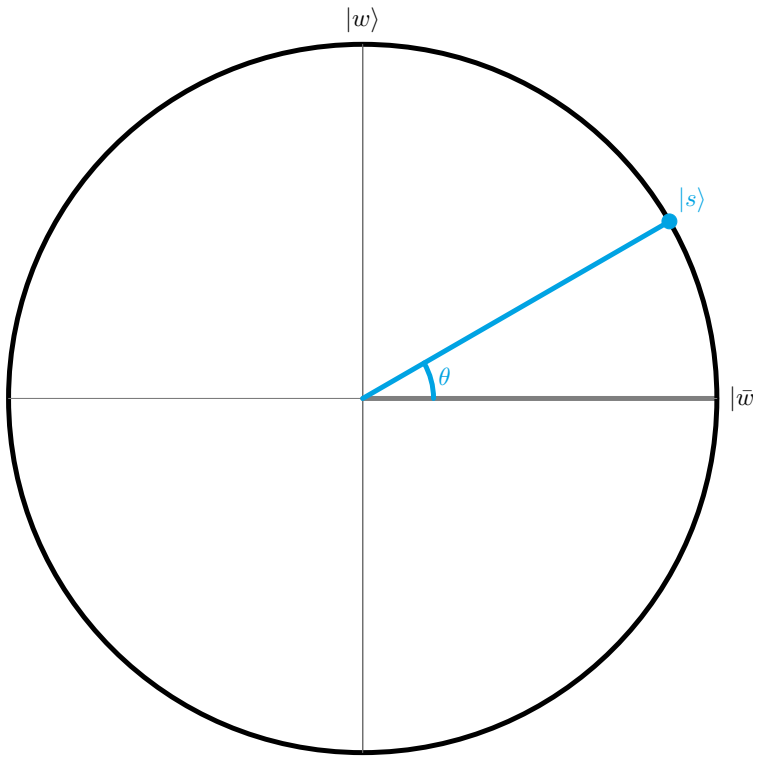


3: bereken gemiddelde, wentel om de gemiddelde

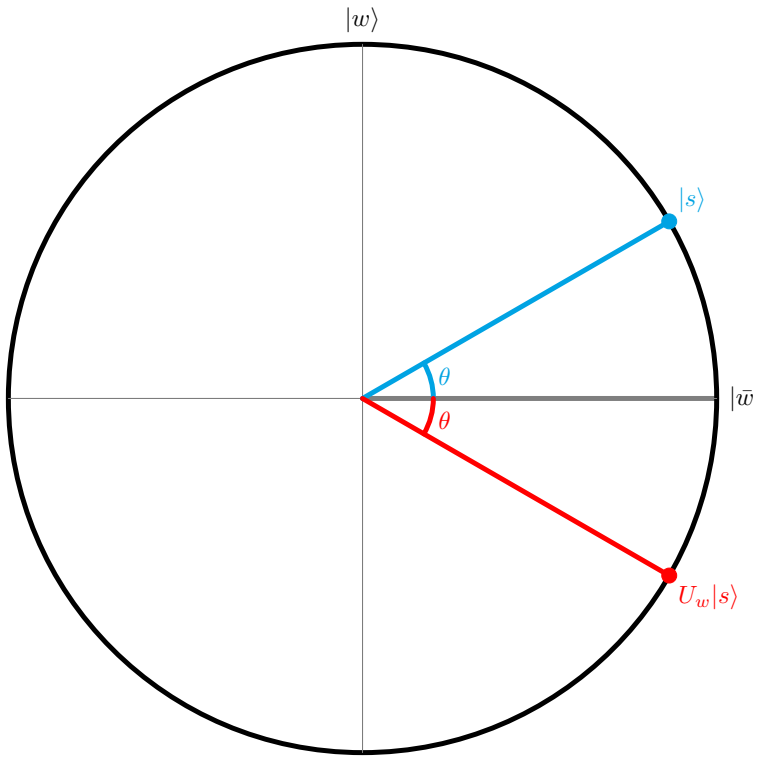


3: resultaat van de omwenteling

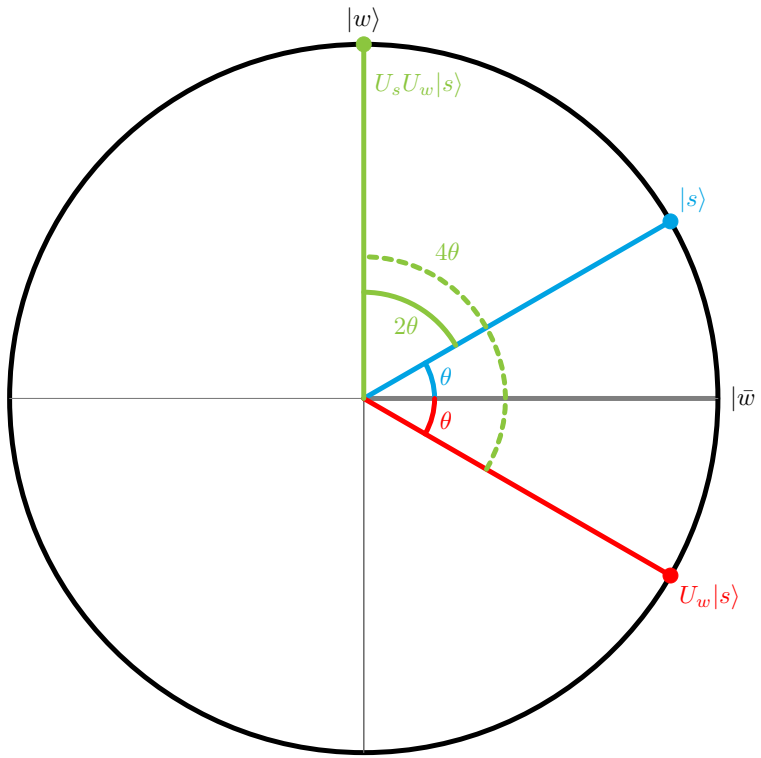
Geometrische Representatie van Grover



Superpositie

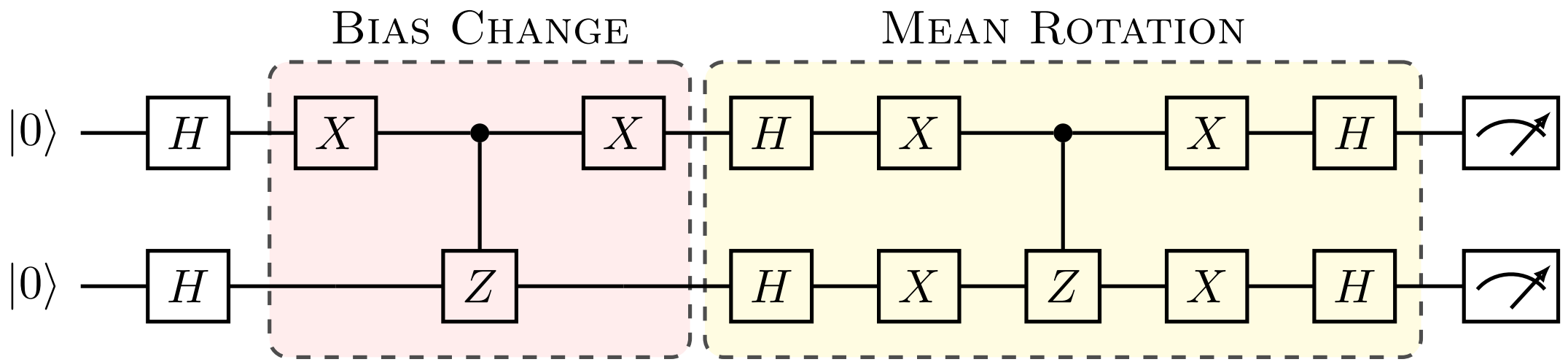


Keer teken om



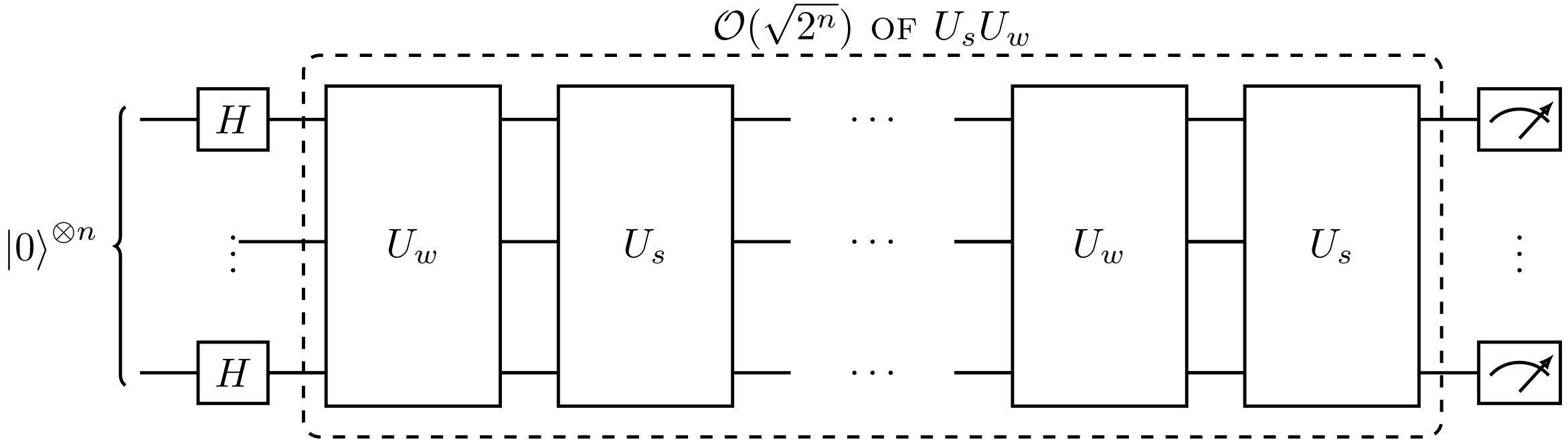
Wenteling om de gemiddelde

Een circuit voor Grover's algoritme



Grover in het algemeen

Kwadratische versnelling t.o.v. snelst (bekende) klassieke algoritme



$$N \sim 2^n$$

Opmerkingen

Reflection around mean done quadratically faster

Voltooi een Grover iteratie $m \leq \frac{\pi}{4}\sqrt{N}$ maal

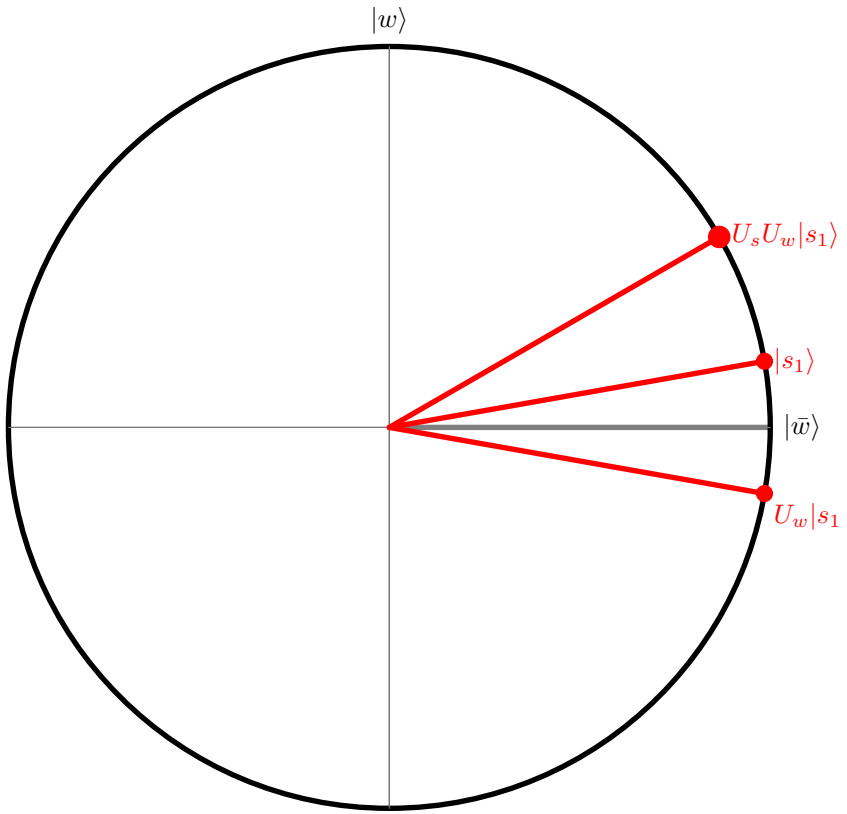
Anders zwenkt hij ver over zijn doel uit

Behalve basistoestanden ook
zoeken naar operaties op basistoestanden

Dit leidt tot belangrijke toepassingen,
meest opmerkelijk, Amplitude Estimation

Kraken van symmetrische encryptie

Hash collisions



Over kwadratische versnellingen

Aanname: beide computers verwerken 1 miljard stappen per seconde

		Classical		Quantum	
List Size	**Number of steps**	**Computation Time**	**Number of steps**	**Computation Time**
8	8	0	3	0
1.000	1.000	0	32	0
1.000.000	1.000.000	1 millisecond	1.000	0
1.000.000.000	1.000.000.000	0.5 seconds	32.000	0
1.000.000.000.000	1.000.000.000.000	8.3 minutes	1.000.000	1 millisecond
43.252.003.274.489.856.000	43.252.003.274.489.856.000	686 years	6.600.000.000	3.3 seconds

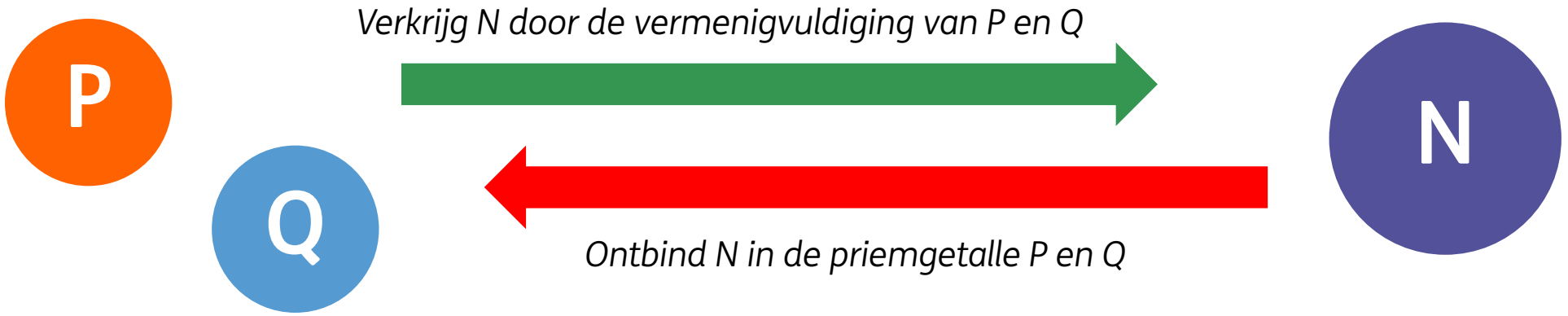
* Huidige quantum computers verwerken een stap 100 maal trager dan klassieke computers

** Sommige kwantumalgoritmen bieden zelfs een exponentiële versnelling

Ontbinden in priemgetallen

One-way functie

Priemgetallen **Vermenigvuldigingen**



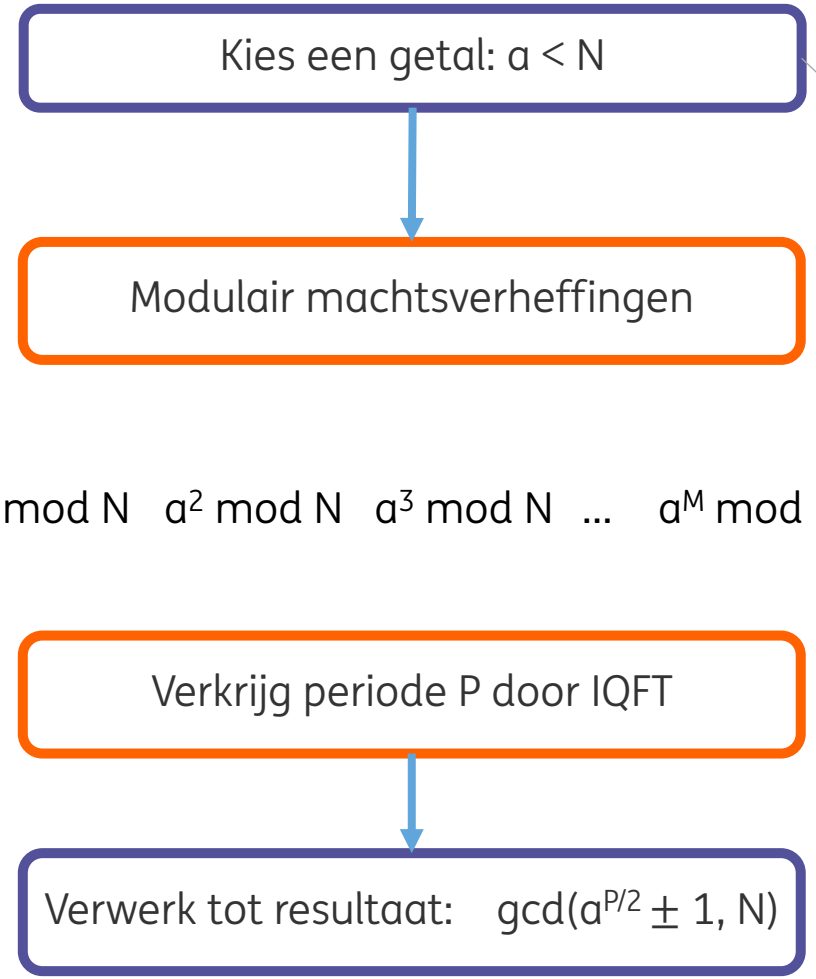
Groen: makkelijk

Rood: moeilijk

Hierdoor interessant voor cryptografie

Shor's Algoritme

Overzicht



$a \bmod N \quad a^2 \bmod N \quad a^3 \bmod N \quad \ldots \quad a^M \bmod N$

Voor de volgende slides, neemt men

$N = 15$

$a = 7$

P moet even zijn; a en N mogen geen gemene deler hebben

Modulair Machtsverheffen

Gebruikmakende van 12 tellerqubits; superpositie van de functie

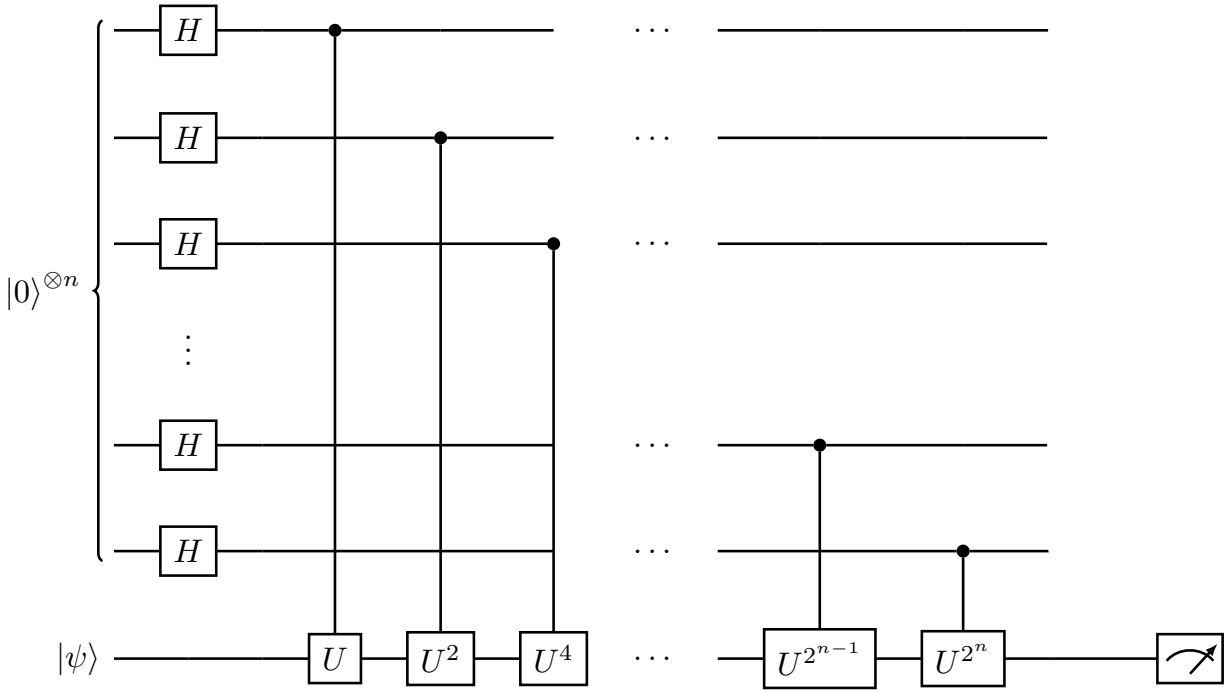
$$7^0 \mod 15 = 1$$
$$7^1 \mod 15 = 7$$
$$7^2 \mod 15 = 4$$
$$7^3 \mod 15 = 13$$
$$7^4 \mod 15 = 1$$
$$7^5 \mod 15 = 7$$
$$7^6 \mod 15 = 4$$
$$7^7 \mod 15 = 13$$
$$7^8 \mod 15 = 1$$
$$7^9 \mod 15 = 7$$
$$\dots$$
$$\dots$$

Een superpositie van verstrengelde input-outputverbanden

$$|\Psi\rangle = \frac{1}{\sqrt{12}}\Big(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + |7\rangle|13\rangle + |8\rangle|1\rangle + |9\rangle|7\rangle + |10\rangle|4\rangle + |11\rangle|13\rangle \Big)$$

Circuit voor modulair machtsverheffen

Inclusief een vervolgstap van een meting



$$|\Psi\rangle = \frac{1}{\sqrt{12}}\Big(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + |7\rangle|13\rangle + |8\rangle|1\rangle + |9\rangle|7\rangle + |10\rangle|4\rangle + |11\rangle|13\rangle \Big)$$

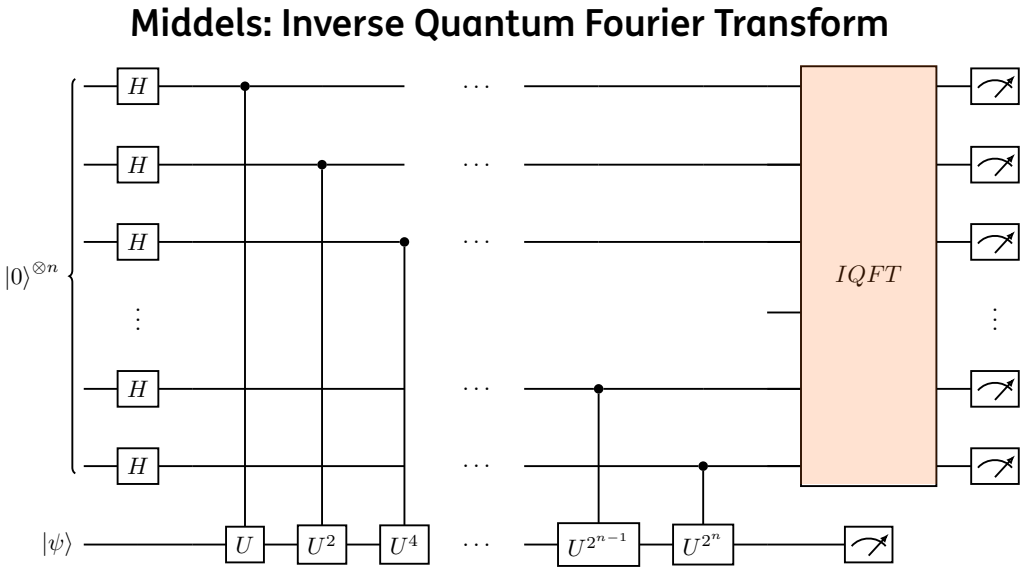
Meet rechter-qubit, bijv. 7

$$|\Psi\rangle = \frac{\sqrt{4}}{\sqrt{12}}\Big(|1\rangle|7\rangle + |5\rangle|7\rangle + |9\rangle|7\rangle \Big)$$

Herleid periode vanuit de amplitude

Periode en Eindresultaat

$$P = 4$$



Exponentiële versnelling

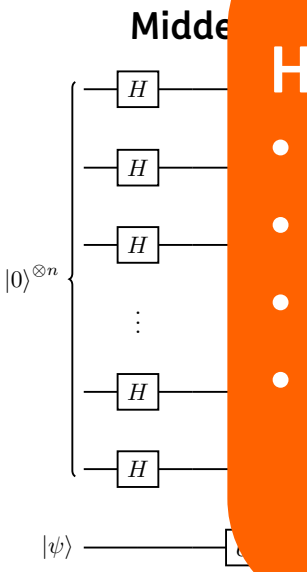
$$\gcd(a^{P/2} \pm 1, N)$$

$$\gcd\left(7^{4/2} - 1, 15\right) = \gcd\left(48, 15\right) = 3$$

$$\gcd\left(7^{4/2} + 1, 15\right) = \gcd\left(50, 15\right) = 5$$

$$3 \cdot 5 = 15$$

Periode en Eindresultaat



Het kraken van RSA-2048 met Shor

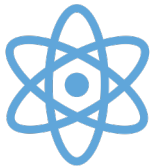
• 300 triljoen jaar	klassieke computer
• 8 uur	20M fysieke qubits met ruis
• 10 seconden	4099 logische qubits
• Grootste getal	21

Exponentiële versnelling

Mogelijkheden binnen de Financiële Sector

quantum mechanics

- superposition
- entanglement
- interference
- measurement
- time evolution
- tunneling



enabling tech

- gated quantum computers
- special-purpose QPU (e.g. annealing)
- quantum-inspired solutions
- classical simulation
- hybrid classical quantum

math affected

- linear algebra
- statistics and stochastics
- differential equations
- unsorted array searches
- pattern recognition
- optimization
- ...

domains

- artificial intelligence
- monte-carlo simulations
- cryptography
- quantitative finance
- analytics
- ...

applications

- predictive modelling
- risk evaluation models
- product recommendation systems
- derivatives pricing
- text processing
- (reverse) stress testing
- fraud detection
- ...

excluding quantum technologies besides computation techniques

Hartelijk Dank!

ING Quantum

Shor's Algorithm

Final remarks

Shor and quantum computing

Breaking RSA-2048 by Shor on Gated Quantum Computers:

- 300 trillion years classical computer
- 8 hours 20M noisy qubits
- 10 seconds 4099 logical qubits
- Largest number 21

Optimization on gated quantum computers

Breaking RSA-768 by Variational Quantum Computing:

- 1.099.551.473.898 was factored on only 3 qubits in 2021

Optimization on special purpose device

Breaking RSA-768 by Quantum Annealing:

- 2 years on classical computer
- ~150k qubits (current state 5k) to crack RSA-768
- Factored N = 1005973 on 98 qubits in 2019