9. losse aantekeningen

9.1 Opbouw van dit document

Moeilijkheidsgraad

- ● Rustig beginnen
- ■ Dat gaat lukken
- ♦ Gaat lekker zo
- ★ Fun park

9.2 spelvormen / practica

- Entangle me (flauw)
- Quantum tic tac toe
- Entanglion
- Spelletjes Annemarije
- quantum eraser
- Young (Quantum Rules)

Figuur 9.1: Makkelijke en moeilijke onderdelen.

9.3 aantekeningen (uit bronnen van) EdX course

idee:

- Moeder Natuur berekent
- Hefboom: gewogen gemiddelde
- serie weertanden: optellen
- parallelle weerstanden: reciprook optellen
- lenzenformule
- twee gewichten op een weegschaal
- water computer (Science museum Bill Phillips)
- analoge computer opamps integrators

Gebruik natuurwetten F=ma Maar er zijn meer regels. Voor quantum systemen kun je beter quantumregels gebruiken. Berekenen van chemische substanties

$$\nabla \cdot \vec{E} = \frac{\rho}{\epsilon_0} \tag{9.1}$$

$$\begin{aligned} \nabla \cdot \vec{B} &= 0 \\ \nabla \times \vec{E} &= -\frac{\partial B}{\partial t} \\ \nabla \times \vec{B} &= \mu_0 \vec{J} + \mu_0 \epsilon_0 \frac{\partial E}{\partial t} \end{aligned} \tag{9.2}$$

bronnen Quantum Zoo [1] Quanttiki [2]

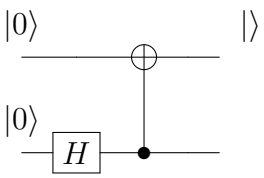
bij de vragen: parser geeft het geinterpreteerde getal weer. Hiervoor is een submit knop nodig Die heb je ook nodig voor een meermerkeuzevraag Understanding chemistry Zuurstof met twee streepjes

De covalente binding Uitleg in Absolutely small

The focus in QM is shifting from

$$\frac{i}{\hbar}\frac{d\Psi}{dt} = H\Psi$$

to



information

Nice: Solving a maze animation

Challenges for society

- spoiling energy
- waising materials

[1] https://math.nist.gov/quantum/zoo/
[2] https://www.quantiki.org/wiki/teleportation-protocol

- climate is changing too fast
- need for medicine
- ..

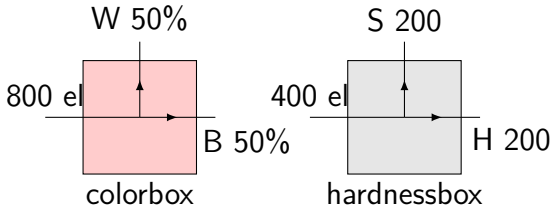
- electrical cables without loss of energy
- Drug development (Quantum Chemistry)
- Predicting material properties for electronics, energy storage
- machine learning
- optimization in robotics
- handling big data for sequencing genomics
- airplane desing
- ..

photosynthesis pathway antenna chlorophyll: extreme fast solving of labyrinth

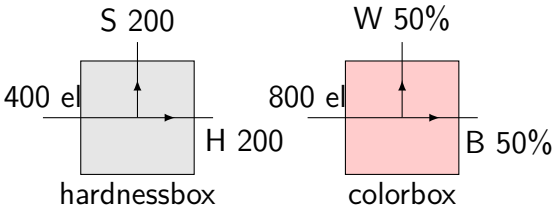
film Lieven van der siepen: Twee mensen lopen in schadusspel en botsen, of lopen langs elkaar . (plato's grot, superpositie)

film how to understand superposition Stel dat electronen twee eigenschappen hebben, kleur en hardheid

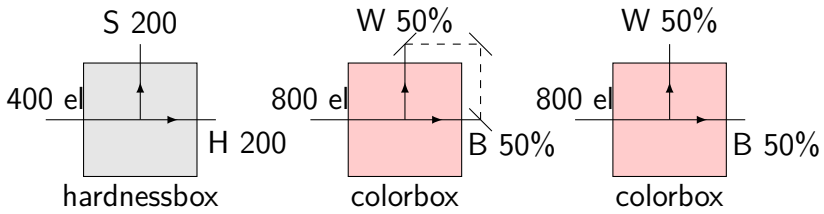
kleur: [B,W] hardheid: [H,S] (hmm zacht en zwart zelfde letter) twee apparaten: een om kleur te sorteren, en een om hardheid te sorteren (eigenlijk spin in twee verschillende richtingen,



Figuur 9.2: experiment 1



Figuur 9.3: experiment 2



Figuur 9.4: experiment 2

module 2

trage video: superposition interference entanglement cloning is not possible error correction not simple but can be done

Divicencio

- QC must be scalable
- Qbits must be initiable
- good qbits are needed, long coherence
- have a universal set of quantum gates
- you can measere them

video high-level languare to compiler error correction converted into quantum instructions converted into physical signals (pulsees) to control and operate physical qubits time constraint synchonicity is a challenge

video what is q internet?

technologies not available in classic internet

- secure communication
- secure identification
- position verification
- secure dedicated computing
- ...

end node are qcompters small ones, less than 10 qb, mosly 1 qb is enough power of entanglement incontrast on a qc we always need more qubits than can besimulated on a classical computer in order to do something new and interesting ??

switches repeaters traffic control

why powerful? secure - not qubits cannot copied

entangelment maximum coordination (=maximum correlation??) only two qubits can be maximally entangled

module 3

classic factoring goes with 2^n quantum factroing N^3 -hard to build -need large nr of qubits to factor: a number of 2000 bitswill take 10000 qubits minimum Redundancy needed for erroro correction vcan be factor of 1000-10000 So for now we are safe, but in 10-20 yrs other encryption systems are rerquitred

video encryption

classic: shared key One Time Pad The message and key have the same length Message and key are bitwise multiplied modulo 2 msg 0110 key 1010 enc 1100 if key==message send 0 else send 1 Bob can reverses the operation

msg .... key 1010 enc 1100

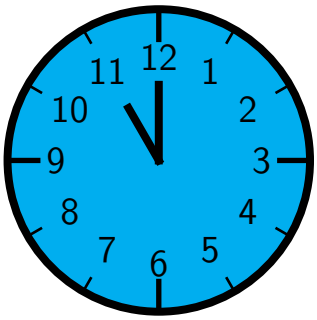
Eve cannot decrypt the message if she has no info on the key

Shannon proved that to be totally secure, you need a key just as long as the message A BW image 64x64=4096 bits info would require a 4096 bit key

in practice keys are much shorter

The number of key is limited. Easy proof (??)

A little variation of an example taken from the PGF documentation (Section 83 Repeating Things: The Foreach Statement, page 912 for version 3.0):



regels klok liegt niet (6 of 12) en (3 of 9).

Korte filmpjes -collapse in superposition (ps duidelijk na spel met klok)

bit flip uitleg bitflip / sign flip is me onduidelijk

iig computational basis (6,12), Hadamard basis (3,9) scenarios's met Alice, Bob, Eve niet moeilijk.

module3, Learn more

learn more encryptie methoden **RSA** http://doctrina.org/How-RSA-Works-With html lastiger. meer voorbeelden bij multiplicatieve inverse nodig.

eulersś totient

shor's algorithm (wikipedia pagina) veel te lastig

caesar's cipher te simpel

enigma machine interessant maar off topic?

braket wikipaedia artikel overstijgt vwo niveau

BB84 Bennett and Brassard 1984 https://www.youtube.com/watch?v=UVzRbU6y7Ks&feature=youtu.be zie ook teoelichting bij video.

volgt logischerwijs op spel met de klok

uit https://www.youtube.com/watch?v=7SMcf1MdOaQ:

//table op zijn plek houden

Alice's bit value	1	0	0	1	0	1	1	1
Alice's sending mode	+	+	+	X	X	+	+	+
Bob's receiving mode	+	+	X	+	+	+	+	X
Bob's result	1	0	0	0	0	1	1	0
Same mode?	Y	N	Y	N	N	Y	Y	N
Shared secret key	1		0			1	1	

Tabel 9.1: BB-84

gesprek Vedran jan 2020

Kunnen we spellen op grond van gesimuleerde quantum logica bouwen

Welke toepassingen die met quantum (internet/computing) gerealiseerd kunnen worden kunnen we simuleren in een game. W

zoekwoorden: // non-local quantum games// https://pdfs.semanticscholar.org/487a/3da75724273c94a9007cebcc6cc2df02b1f6.pdf

-IBM spel//

-teleportatie

-Kun je het voordeel van de Bell ongelijkheid (85

bring in a bit of reality with limited coherence time

CHSH

model: spelleider genereert random coefficienten van een qubit. Dat is het te teleporterren bit

Alice en Bob moeten het qubit transporteren. Bob stuurt het qubit ter controle naar de spelleider. Beste tijd, misnte foute potgingen.

Dating game probabilistic graphica model

Scott Aaronson (Quantum Computing Since Democritus) https://www.scottaaronson.com/qclec/combined.pdf

ihb lecture 14 non local games

9.4 platforms voor quizzies

aantekening 20200715

kahoot: kan geen latex aan, mathmode niet voldoende workaround vraag als plaatje inladen

socrates: math alleen by paid version, kan wel als plaatje

classmaker: zeer uitgebried, maar math support alleen via omweg

codecogs kan image links leveren met late code werkt bij google forms(paste by url), en classmaker

werkt ook bij kahoot, maar dan als gifje

bij kahoot ziet het er niet uit

bij google ziet het er goed uit, maar het plaatje kan daar niet in-line staan maar onder aan de tekst. formule kan ook in de alternatieven staan.

google forms lijkt de beste keus nu.

google forms

settings>quizzies>make this a quiz

release later (email gathering)

balen, kan alleen maar een figuur ter illustrait, niet inline

Al te zeer terzijde wiskunde in de docentenhandleiding. Bijvoorbeeld vectoren en basisverandering

Geogebra kan helpen, verwijzen met een QR code

enkele voorbeelden

https://www.geogebra.org/classic/vNjMv6FQ

kijk eens naar het inwendig product

inwendig product

9.5 quantum inspire knowlegdebase

Op de site van quantum inspire korte uitleg van begrippen

fault correction

site

bases

z-basis: $|0\rangle$ en $|1\rangle$

x-basis: $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ en $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

y-basis: $|R\rangle = \frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle$ en $|L\rangle = \frac{1}{\sqrt{2}}|0\rangle - i\frac{1}{\sqrt{2}}|1\rangle$

foto's van systemen, wat is de schaal, geen idee wat ik zie.

interessant artikeltje over meting ,probability (vankampen) [**vankampen2008scandal**]

Q-superposition is fundamentally different form classical superposistion. leading to 2^n states. classically, a combination of n musical notes can be at most a superposition of n frequencies

verstrengeling lot verbonden meting van een legt de ander vast 1.kan niet gedeeld worden. Handig voor cryptografie monogaam

2. maximal coordination Als twee verstrengelde qubits in dezelfde basis gemeten worden, levern zij dezelfde uitkomst. Hoe ver ze ook uit van elkaar verwijderd zijn. De uitkomst is vollegid random, niet van te voren maar pas op het moment van meten bepaald.

vb: twee deeltjes worden geprearеerd zodat hun totale spin nul is. Als een deeltje met spin up gemeten wordt zal de ander in dezelfde basis spin down geven. ook al zijn ze kilometers van elkaar. NB er vindt geen informatieuitwissling plaats .

q-allgoritme

Een algoritme is een stapgewijs protocol om een probleem op te lossen. Als je gebruik maakt van superpositie of verstrengeling is het een quntum algoritme.

Een verschil met klassiek is dat QA *altijd* reversibel zijn. ALs je een circuit uitvoert en daarna nerovetsrethcaachterstevoren dan ben je weer waar je begon.

Problemen die theoretisch onbeslisbaar zijn kan een QC ook niet oplossen. Een QC kan problemen wel enorm versneld oplossen. Vbb: Shor Grover.

Shor's algoritme kan integers ontbienden in proemfactoren.Exponentieel sneller dan klassieke algoritmes dat kunnen. Grover kan kwadratishc sneller zoeken in een ongesorteerde lijst.

Hello quantum world

link broken cASM