’n Universele programmeerbare kwantumrekenaar?

A universal programmable quantum computer?

WL Fouché & PH Potgieter
Departement Besluitkunde
Universiteit van Suid-Afrika (Pretoria)
Posbus 392, 0003 Unisa
php@member.ams.org

J Heidema
Departement Wiskundige Wetenskappe
Universiteit van Suid-Afrika (Pretoria)
EG Jones
Departement Fisika
Universiteit van Suid-Afrika (Pretoria)

WL Fouché

J Heidema

EG Jones

PH Potgieter

Willem Fouché (gebore 1953) verwerf in 1976 die graad M.Sc. en in 1982 die graad Ph.D. in Wiskunde, beide aan die Universiteit van Stellenbosch. Hy doseer eers by die Universiteit van die Oranje-Vrystaat, toe by die Universiteit van Pretoria, en is sedert 2000 verbonde aan die Departement Besluitkunde (voorheen Kwantitatiewe Bestuur) by die Universiteit van Suid-Afrika. Sy akademiese hoofbelangstellings is in die grondslae van waarskynlikheidsleer en die rol van selfverwysing in die grondslae van rekenaarwetenskap en wiskunde. Verder bestudeer hy die toepassings van getalleteorie op kriptografie en die voortbring van pseudo-ewekansigheid.

Willem Fouché (born 1953) obtained the degree M.Sc. in 1976 and the degree Ph.D. in Mathematics in 1982, both from the University of Stellenbosch. He started lecturing at the University of the Free State, later at the University of Pretoria and since 2000 has been in the Department of Decision Sciences (formerly Quantitative Management) at the University of South Africa. His main interests are in the foundations of probability theory and the rôle of self-referentiality in the foundations of computer science and mathematics. He also studies applications of number theory in cryptography and the generation of pseudo-randomness.

Petrus Potgieter (gebore 1968) voltooi in 1992 die graad MA(Math) aan die Kent State University in die VSA en keer terug na Suid-Afrika in dieselfde jaar vir doktorale studies by die Universiteit van Pretoria waar die graad PhD (Wiskunde) aan hom toegeken word in 1996. In 1995–1996 is hy werksaam aan die Universiteit van Stellenbosch. Sedert 1997 is hy by die Universiteit van Suid-Afrika in Pretoria, in die Departement Besluitkunde.

Petrus Potgieter (born 1968) completed the degree MA(Math) at Kent State University in the USA and returned to South Africa during the same year for doctoral studies, obtaining the degree PhD (Mathematics), awarded to him in 1996. During 1995–1996 he worked at the University of Stellenbosch. Since 1997 he has been employed at the University of South Africa in Pretoria, in the Department of Decision Sciences.

JOHANNES HEIDEMA (gebore 1941) verwerf in 1963 die M.Sc. in Wiskunde aan die PU vir CHO, in 1964 die doktoraaleksamen in Wiskunde en Logika aan die Universiteit van Amsterdam, en in 1966 die D.Sc. in Wiskunde aan die PU vir CHO. Hy doseer Wiskunde, twee jaar aan die PU vir CHO, drie jaar aan UPE, en daarna vir 22 jaar (1970–1991) as professor aan die RAU. Sedert 1992 is hy professor in Wiskunde aan UNISA, van 2007 af emeritus. Sy akademiese hoofbelangstelling is die grondslae van die wiskunde en die logika, veral die implikasies van 'n semantiese en modelteoretiese benadering vir die teoretiese fisika (kwantumberekening en -logika), vir die rekenaarwetenskap (nie-monotone logika vir kunsmatige intelligensie), en vir die wetenskapfilosofie (epistemologie en realisme).

JOHANNES HEIDEMA (born 1941) obtained the M.Sc. in Mathematics in 1963 at the PU for CHE, the doctoral exam in Mathematics and Logic in 1964 at the University of Amsterdam, and the D.Sc. in Mathematics in 1966 at the PU for CHE. He lectured Mathematics for two years at the PU for CHE, three years at UPE, and then for 22 years (1970-91) as professor at the RAU. He has been a professor in Mathematics at UNISA since 1992, emeritus from 2007. His main academic interests are the foundations of mathematics and logic, and in particular the implications of a model-theoretic approach in theoretical physics (quantum computation and logic), in computer science (nonmonotonic logic for artificial intelligence), and in the philosophy of science (epistemology and realism).

GLYN JONES (gebore 1953) verwerf in 1979 die graad M.Sc. en in 1989 die graad D.Sc. in Fisika beide aan die Universiteit van Pretoria. Hy het as navorser in 1977 by die Laserafdeling van die Nasionale Fisikanavorsingslaboratorium by die WNNR aangesluit waar hy vir 11 jaar op verskillende gasontladingopgewektelasersisteme gewerk het. Hy is toe vir vier jaar in die industrie as konsultant bedrywig en het in 1993 die pos van Senior Lektor in die pas gestigte Departement Fisika by Vista Universiteit aanvaar. Hy is sedert 2002 'n dosent in die Departement Fisika by UNISA. Sy huidige hoofbelanstellings behels aspekte van die grondslae van kwantumstelsels, veral op die gebied van kwantuminligting.

GLYN JONES (born 1953) obtained his M.Sc. (1979) and D.Sc. (1989) degrees in Physics at the University of Pretoria. He joined the Laser Section of the National Physical Research Laboratory at the CSIR in 1977 as a Researcher and his research encompassed several gas-discharge laser excitation systems. From 1989 to 1992 he served as consultant to industry and in 1993 accepted the post of Senior Lecturer in the newly formed Physics Department of Vista University. He has been lecturing in the Physics Department of UNISA since 2002 and his current interests include aspects of the foundations of quantum theory, particularly in the area of quantum information.

ABSTRACT

Research into quantum computation over the past 20 years has been very successful in stimulating the development of quantum cryptography (already in industrial application), the study of quantum information and the discovery of novel algorithms for traditionally hard and interesting problems such as prime factorisation. This paper attempts to explain why certain (strong and interesting) results in quantum computation still fall short of establishing universality (and programmability) for quantum computing. The notion of a universal computing device in a specific class is crucial for the development of a complexity theory and – more basically – establishes the notion of programmability. We review the well-established notions of universality in classical deterministic and probabilistic computing before moving on to examine the concept of a "universal QTM" introduced by Deutsch.

We first discuss universality in a general context. Suppose Φ_n to be the partial function computed by machine n in a class and fix a computable (in the same model) bijective function $h : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow$

$\mathbb{N}_0$. *Since halting is a probabilistic notion for a QTM, the notion of universality for quantum devices should be akin to that for probabilistic machines. For deterministic and probabilistic machines we define universality as follows.*

Definition *If there exists a number N such that*

$$\Phi_N\left(h(n,m)\right) = \Phi_n(m)$$

which means that the functions are either equal and both defined or both undefined (if deterministic) and if not deterministic then the values have the same distribution, for all n and m, then the machine described by N is called a universal machine.

For probabilistic Turing machines (with computable transition probabilities) a universal machine of this kind does exist, and likewise for the subclass of deterministic Turing machines. The paper discusses whether universality – in this sense – has been demonstrated for quantum Turing machines (QTMs).

Deutsch introduced a "universal quantum computer" (uQC, where u has not been capitalised in order to emphasise the difference between this universality concept and the preceding). Deutsch showed[5] that for any given L, $\varepsilon > 0$ and quantum device U operating on L qubits, there exists a program p_L (a classical finite string of bits) for the uQC that (with input $|p_L\rangle$ followed by any finite superposition of L-qubit basic states) approximates the operation of U on the finite superposition of L-qubit basic states with accuracy at least ε (in the inner-product norm). This is not the same kind of universality that we have for probabilistic and for deterministic Turing machines!

Bernstein and Vazirani have given another partial solution.[3] They showed that there exists a quantum Turing machine $\mathcal{U}$ (they actually wrote $\mathcal{M}$) such that

> *"for any well-formed* QTM M, any $\varepsilon > 0$, and any T, $\mathcal{U}$ can simulate M with accuracy ε for T steps with slowdown polynomial in T and $\frac{1}{\varepsilon}$."*

The slowdown and the program for $\mathcal{U}$ both depend here on the length of the input*. The full Bernstein-Vazirani result could be summarised by the statement that*

> *there exists a QTM $\mathcal{U}$ such that for each QTM M with finite description $\bar{M}$, n, ε and T there is a program $\mathcal{P}(\bar{M}, n, \varepsilon, T)$ and a function $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ (both recursive in their inputs) such that running $\mathcal{U}$ on input $|\mathcal{P}(\bar{M}, n, \varepsilon, T)\rangle \otimes |x\rangle$ where $|x| = n$ for $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ steps results – within accuracy ε – in the same distribution over observable states as running M on input $|x\rangle$ for T steps.*

The simulation is clearly only approximate*. What Bernstein and Vazirani mean "with accuracy ε" is that if P is the probability distribution over all observable states of $\mathcal{U}$ after $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ steps with the given input and Q is the corresponding probability distribution of M after T steps then*

$$\frac{1}{2}\sum_x |P(x) - Q(x)| \;\leq\; \varepsilon$$

where the summation is over all possible observable states x. Again, approximate simulation is quite different from the universality concept for ordinary and for probabilistic Turing machines (with computable probabilities).

*Meaning that the time evolution operator is unitary.

The paper concludes that these (strong and interesting) results in quantum computation still fall short of establishing universality (and programmability) for quantum computing. At the very least, researchers in the field should attempt to explain how the results of Deutsch, Bernstein and Vazirani, and others can be used or expanded to construct a fully programmable universal quantum device. In the worst case, one needs to prove that such a fully universal quantum computer does not exist.

KEY CONCEPTS: Universal quantum computers, programmable quantum computers, universal quantum Turing machine, quantum computation.

TREFWOORDE: Universele kwantumrekenaars, programmeerbare kwantumrekenaars, universele kwantummeganiese Turing-masjien, kwantumberekening.

OPSOMMING

In hierdie bydrae word die vernaamste resultate oor sogenaamde *universele* kwantumberekening toegelig. Daar word 'n oorsig gegee oor die model wat gebaseer is op die kwantummeganiese Turing-masjien (KTM) van Deutsch. Ons lig die konsep van berekeningsuniversaliteit toe vir probabilistiese rekentoestelle en vergelyk dít met die vereistes wat aan 'n veronderstelde universele KTM gestel sou word. Die vermoede word geopper dat die semi-universele hibriede toestel (SUHT) wat deur die resultaat van Bernstein en Vazirani gesuggereer word, essensieel nie kwantummeganies is nie.

1. INLEIDING

'n Mens kan onderskei tussen eendoelige, meerdoelige en aldoelige rekenmasjiene. In 2001 het by IBM 'n eendoelige kwantumrekenmasjien met 'n register van sewe kwantumbisse die priemfaktorisering $15 = 3 \times 5$ met Shor se Algoritme fisies verwerklik.[15,17] 'n Sakrekenmasjien ("pocket calculator") is meerdoelig. Ons tafel- en skootrekenaars is – ten minste as mens hul geheues as onbeperk uitbreibaar sien – aldoelig of "universeel".

Die argetipiese formele model van enigiets wat ons 'n berekeningsprosedure sou noem, is die *Turing-masjien*,[15] wat dan ook eendoelig, meerdoelig, of universeel kan wees. In sy klassieke inleiding[10] tot die teorie van rekursiewe funksies en berekenbaarheid bewys Hans Hermes in sy laaste hoofstuk dat daar 'n universele Turing-masjien (TM) bestaan, wat die invoer-afvoer-gedrag van enige TM kan naboots wanneer dit 'n gepaste program as deel van sy invoer ontvang. Hier het ons 'n duidelike voorbeeld van *universaliteit in 'n klas* van masjiene.

Maar daar is ook 'n tweede begrip van "universaliteit", naamlik dié van 'n *universele voortbringende versameling* van "komponente" vir 'n klas van masjiene. Hermes wy Hoofstuk 2 van sy boek aan die "ingenieurswese" van Turing-masjiene. Hy voer 'n eindige versameling van "elementêre" TMe in ("komponente" of "subroetines", as u wil) en beskryf dan hoe om hulle te kombineer om meer komplekse masjiene te bou. Dan bewys hy dat die elementêre masjiene 'n universele voortbringende versameling is vir die klas van alle TMe: *enige* TM is ekwivalent (wat sy invoer-afvoer-gedrag betref) aan 'n TM wat gekonstrueer is deur elementêre masjiene te kombineer.

Vir begripsmatige helderheid is dit dan belangrik om die twee konsepte te onderskei, maar ook hul logiese samehang te verstaan: aan die een kant 'n *universele masjien* (in 'n klas) en aan die ander kant 'n *universele voortbringende versameling* (vir 'n klas). As U 'n universele masjien in 'n klas

is, dan is $\{U\}$ sekerlik 'n universele voortbringende versameling vir daardie klas (al sal U waarskynlik nie besonder "elementêr" wees nie!). Aan die ander kant is dit ook denkbaar dat daar wel 'n universele voortbringende versameling vir 'n klas bekend is, sonder dat 'n universele masjien vir daardie klas nog gebou is, of selfs kan bestaan. Dit is duidelik dat "programmeerbaarheid" slegs van toepassing is op 'n universele (of dan ten minste meerdoelige) masjien. 'n Program sal gewoonlik instruksies gebruik wat ooreenkom met elemente van 'n universele voortbringende versameling.

Uitgaande van die bestaande literatuur oor kwantumberekening, wil hierdie artikel lig werp op die omstrede vrae rondom die bestaan, al dan nie, van 'n klas van kwantummeganiese Turing-masjiene en van 'n universele masjien in só 'n klas. In Afdeling 2 word, as agtergrond vir die oorgang na die kwantumregime, geskets wat 'n klassieke Turing-masjien en 'n probabilistiese Turing-masjien is. Afdeling 3 verduidelik 'n klas van kwantummeganiese Turing-masjiene as direk analoog aan klassieke en probabilistiese TMe. Afdeling 4 bespreek aspekte soos die bestaan van 'n universele masjien in 'n klas en sy programmeerbaarheid, asook eksakte teenoor benaderde simulasie deur so 'n universele masjien – eers vir klassieke en probabilistiese masjiene en dan vir die klas van kwantum-TMe van Afdeling 3, met taamlik negatiewe gevolgtrekkings vir laasgenoemde klas. Afdeling 5 gee 'n kort slotsom. 'n Konferensievoordrag[9] was die voorloper van hierdie artikel. In vroeëre artikels[15,8] word baie van die begrippe wat hierin 'n rol speel in meer besonderhede verduidelik.

2. KLASSIEKE EN PROBABILISTIESE TURING-MASJIENE

Aangesien kwantum-TMe (KTMe) gebaseer is op gewone klassieke TMe, begin ons met 'n kort hersiening van die klassieke model.[15] Aan die begin van die twintigste eeu het wiskundiges baie belang gestel in die opstel van 'n formele model vir berekening. In 1936 het Alan Turing 'n abstrakte toestel beskryf, wat ons nou 'n *Turing-masjien* noem, wat 'n eenvoudige, eindige stel reëls op 'n voorspelbare wyse volg om 'n eindige string simbole (die *invoer*) te transformeer na 'n eindige string (die *afvoer*, indien gedefinieer). Die Turing-masjien (TM) is in ons voorstelling 'n klein apparaat met 'n "kop" wat oor 'n lineêre band van diskrete selle, potensieel oneindig lank na links en regs, kan beweeg. Elke sel bevat slegs die simbool **0** of **1**, of is blanko. Die TM het 'n eindige versameling moontlike interne toestande. Die kop kan die inhoud lees van die sel waaroor dit staan en ook, in elke stap, 'n simbool in daardie sel skryf. Daar is twee interne toestande met 'n spesiale status: die *begintoestand* q_0 en die *halttoestand* q_H.

'n TM het 'n eindige lys opdragte, die *oorgangsreëls* of *program*, wat sy werking beskryf. Vir elke kombinasie van selinhoud (onder die kop) en interne toestand is daar hoogstens een oorgangsreël. As die interne toestand q_i is en die kop staan oor 'n sel met die simbool S_j, dan kyk die masjien vir die oorgangsreël wat ooreenkom met (q_i, S_j). As daar so 'n reël in die program is, dan vertel dit die masjien watter simbool om in die sel onder die kop te skryf, of die kop een sel na links of na regs moet beweeg of glad nie, en na watter interne toestand dit moet oorgaan. As daar geen reël vir (q_i, S_j) in die program is nie, gaan die masjien onmiddellik in die halttoestand q_H oor, waarmee daar geen oorgangsreël ooreenkom nie, of hoogstens (vir omkeerbare TMe) reëls wat opdrag gee om die kop in elke stap een sel in 'n spesifieke rigting te skuif sonder om ooit weer 'n simbool op die band te verander.

'n *Berekening* begin met die TM se kop oor die eerste nie-blanko sel van links af (sê in posisie 0 op die band, waarop slegs die eindige *invoer* verskyn) en die masjien in interne begintoestand q_0. Nou word die oorgangsreëls eenvoudig toegepas tot die masjien die halttoestand q_H binnegaan, waarna die inhoud van die band die *afvoer* van die berekening is. Indien, vir 'n invoer, die masjien nooit halt nie, dan is die ooreenkomstige afvoer ongedefinieer. Dit is nou duidelik hoe elke TM 'n

(moontlik parsiële) funksie $f : \mathbb{N}_0 \to \mathbb{N}_0$ van die versameling telgetalle (binêr gekodeer) na sigself definieer.

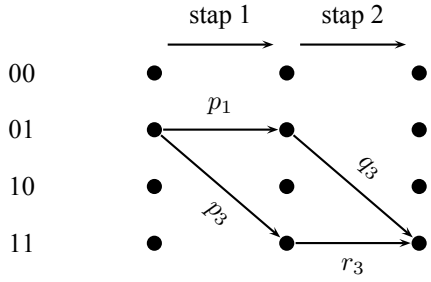
Turing-masjiene is die kanoniese modelle vir rekenapparate. Geen deterministiese toestel wat met eindige (maar moontlik onbegrensde) middele werk, is ooit bevind as in staat om funksies te bereken wat nie Turing-berekenbaar is nie. Trouens, mens kan jou tafelrekenaar maar sien as 'n TM met 'n *eindige* band.

'n *Probabilistiese Turing-masjien* (PTM) is soortgelyk aan 'n gewone TM, behalwe vir die feit dat daar vir elke masjienkonfigurasie (q_i, S_j) 'n eindige versameling oorgangsrëels – elk met 'n geassosieerde waarskynlikheid – bestaan, en dat keuses (met die ooreenkomstige waarskynlikheidsverdeling) bepaal watter reël in 'n spesifieke stap toegepas word. Ons stel 'n sekere drumpelwaarskynlikheid vas (groter as 50%, sê 75%) en sê dan dat 'n spesifieke PTM $f(x)$ op invoer x bereken as en slegs as dit halt met afvoer $f(x)$ met 'n waarskynlikheid groter as 75%.

3. KWANTUMMEGANIESE TURING-MASJIENE (KTME)

'n Natuurlike model vir kwantumberekening word gebaseer op die klassieke Turing-masjien. Die *kwantummeganiese Turing-masjien* (KTM) is vir die eerste keer duidelik deur David Deutsch beskryf.[5] (Paul Benioff het wel 'n soortgelyke gedagte ietwat vroeër geopper,[2] maar dit was hoofsaaklik in die konteks van die vind van 'n moontlike fisiese basis vir omkeerbare berekening.) Die onderliggende idee is eenvoudig: 'n KTM is rofweg 'n probabilistiese Turing-masjien (PTM) met in plaas van reële waarskynlikhede vir die verskillende alternatiewe in 'n oorgangsreël (gekoppel aan 'n spesifieke (q_i, S_j)), nou komplekse oorgangsamplitudes – waarvan die gekwadreerde moduli optel na een vir die betrokke reël.

Om ons begrip van die ooreenkomste en verskille tussen klassieke waarskynlikhede en kwantumamplitudes te verhelder, loon dit die moeite om met 'n voorbeeld die funksionering van 'n PTM en 'n analoë KTM te vergelyk. Beskou 'n PTM met sy waarskynlikhede vir oorgange van een konfigurasie (interne toestand + posisie van die kop + string op die band) na 'n ander. Ons dui, kortweg en onvolledig, 'n konfigurasie sommer aan met die ooreenstemmende string, bv. 00, 01, 10, 11. Veronderstel die PTM is in 'n konfigurasie 01 en kan in een stap net na konfigurasies 01 of 11 gaan met nie-nul waarskynlikhede onderskeidelik p_1 en p_3; $p_1 + p_3 = 1$.



Nou wil ons in 'n tweede stap na 'n konfigurasie 11 gaan, wat uit die huidige 01 moontlik is met waarskynlikheid q_3 en uit die huidige 11 met waarskynlikheid r_3. Daar is dus net twee paaie van die oorspronklike 01 na die finale 11:

$01 \xrightarrow{p_1} 01 \xrightarrow{q_3} 11$ met waarskynlikheid $p_1 q_3$; en

$01 \xrightarrow{p_3} 11 \xrightarrow{r_3} 11$ met waarskynlikheid $p_3 r_3$.

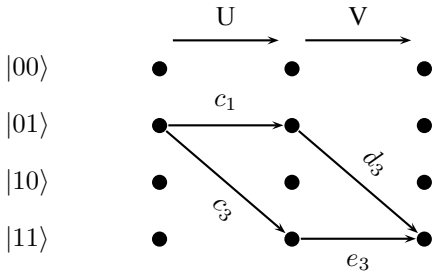
Die waarskynlikheid om in twee stappe van 01 na 11 oor te gaan is dan $p_1q_3 + p_3r_3$.

Ter vergelyking beskou ons nou 'n KTM met 'n register van twee kwabisse en Hilbert-toestandruimte met die standaardbasis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Die masjien begin in basistoestand $|01\rangle$, wat eerstens onderwerp word aan 'n unitêre transformasie U van die toestandruimte, met

$$\begin{aligned} U|01\rangle &= c_1|01\rangle + c_3|11\rangle \\ &= 0|00\rangle + c_1|01\rangle + 0|10\rangle + c_3|11\rangle \quad \text{, byvoorbeeld} \end{aligned}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & c_1 & 0 & -c_3^* \\ 0 & 0 & 1 & 0 \\ 0 & c_3 & 0 & c_1^* \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ c_1 \\ 0 \\ c_3 \end{bmatrix},$$

waar $|c_1|^2 + |c_3|^2 = 1$.



Nou word 'n tweede unitêre transformasie, V, op die toestandruimte toegepas, waarby

$$\begin{aligned} V|00\rangle &= \ldots \\ V|01\rangle &= d_0|00\rangle + d_1|01\rangle + d_2|10\rangle + d_3|11\rangle \\ V|10\rangle &= \ldots \\ V|11\rangle &= e_0|00\rangle + e_1|01\rangle + e_2|10\rangle + e_3|11\rangle. \end{aligned}$$

Gevolglik is

$$\begin{aligned} VU|01\rangle &= V\left(c_1|01\rangle + c_3|11\rangle\right) \\ &= c_1V|01\rangle + c_3V|11\rangle \\ &= c_1\left(d_0|00\rangle + d_1|01\rangle + d_2|10\rangle + d_3|11\rangle\right) + c_3\left(e_0|00\rangle + e_1|01\rangle + e_2|10\rangle + e_3|11\rangle\right) \\ &= \ldots + (c_1d_3 + c_3e_3)|11\rangle, \end{aligned}$$

wat aandui dat, ná toepassing van die saamgestelde unitêre transformasie VU op $|01\rangle$ en meting ten opsigte van die standaardbasis, die waarskynlikheid om die uitkomstoestand $|11\rangle$ te vind, $|c_1d_3 + c_3e_3|^2$ is (en *nie* $|c_1|^2|d_3|^2 + |c_3|^2|e_3|^2$ nie!).

Die ooreenkomste tussen klassieke waarskynlikhede vir 'n PTM en waarskynlikheidsamplitudes vir 'n KTM is dus dat die betrokke (respektiewelik reële en komplekse) getalle *vermenigvuldig* vir seriële samestelling van berekeningstappe en *optel* vir alternatiewe parallelle paaie met dieselfde begin- en eindpunte (dink aan Feynman se som-oor-paaie-benadering tot kwantumfisika!). Die verskil is dat 'n amplitude c meer inligting bevat as net 'n oorgangswaarskynlikheid $|c|^2$; dit het ook 'n

fase, en die rytjie koëffisiënte (amplitudes) wanneer ons 'n toestandvektor skryf as 'n lineêre kombinasie van basisvektore, verteenwoordig ook die faserelasies tussen al die terme, relasies wat behoue bly onder unitêre transformasies vanweë die lineariteit van laasgenoemde. Somme van klassieke waarskynlikhede lewer altyd 'n groter waarskynlikheid as die sommande, maar kwantumpaaie kan destruktief of konstruktief interfereer, wat dit moontlik maak om 'n kwantumrekenmasjien na groter waarskynlikheid vir die regte antwoord en kleiner waarskynlikhede vir verkeerde antwoorde te dryf.

Ons herinner kortliks aan die wiskundige raamwerk waarbinne kwantumberekening, en in die besonder dan 'n KTM, geplaas word.[15] Sonder verlies aan algemeenheid neem ons aan dat alles binêr gekodeer word, sodat elke gevulde posisie of die band van 'n KTM ooreenkom met 'n enkele kwabis (kwantumbis). As die eenheid van kwantuminligting is die kwabis 'n kwantumstelsel met twee toestandvlakke, sodat sy kwantumtoestand 'n lineêre superposisie is van twee basistoestande, gewoonlik aangedui met $|0\rangle$ en $|1\rangle$. Die werklike (kwantum-) toestandruimte van die KTM is 'n direkte som van *n*-kwabis-ruimtes (waar n aandui hoeveel bandselle gebruik is, terwyl elke n-kwabis-ruimte die n-voudige tensor is van die enkel-kwabis-ruimte). Daardie direkte som is egter nie 'n *volledige* inproduk-ruimte nie, dit wil sê 'n Hilbert-ruimte nie en dus – volgens kwantumteorie se postulate – nie 'n geldige toestandruimte nie. Gelukkig kan ons die vervolledigding van die direkte som as die onderliggende Hilbert-ruimte neem. Elke unitêre operator U oor die direkte som kan uitgebrei word[3] tot 'n unitêre operator $\widehat{U}$ op die Hilbert-ruimte. Hierdie vervolledigde ruimte en operatore kom dan ooreen met die fisiese stelsel wat ooreenkom met die KTM onder beskouing, waarmee, ten minste in die ortodokse kwantumdenke, die *fisikaliteit* van die KTM verseker is.

3.1 Werking van 'n KTM

In wat nou volg, is die *klassieke masjien* een met 'n band, oneindig in beide rigtings, wat begin in toestand q_0 oor posisie 0 op die band, wat ons soos 'n templaat gebruik vir die KTM. Die ooreenstemmende KTM mag soos volg werk (gebaseer op Deutsch se beskrywing,[5] Ozawa,[14] Bernstein en Vazirani).[3]

I. Die kwantumruimte van die KTM se toestande word onderspan deur 'n basis (wat ons die *berekeningsbasis* noem) bestaande uit toestande

$$|h\rangle|q_C\rangle|T_C\rangle|x_C\rangle$$

waar $|h\rangle$ die haltkwabis is, $h \in \{0,1\}$ en (q_C, T_C, x_C) 'n konfigurasie van die ooreenstemmende klassieke masjien, met x_C 'n aanduiding van die kop se posisie op die band, q_C die interne toestand en T_C die nie-blanko inhoud van die band.

II. Spesiale begin- en halttoestande $|q_0\rangle$ en $|q_H\rangle$ van die KTM kom ooreen met die begin- en halttoestande q_0 en q_H van die klassieke masjien.

III. Die enkele samevattende oorgangsreël is nou 'n unitêre operator U wat herhaaldelik in opeenvolgende stappe toegepas word, en wat in elke stap elke basisvektor $|h\rangle|q\rangle|T\rangle|x\rangle$ afbeeld op 'n superposisie van slegs eindig veel $|h'\rangle|q'\rangle|T'\rangle|x'\rangle$, waarby

   (a) die beeld onder reël U identies is vir $|h\rangle|q\rangle|T_1\rangle|x\rangle$ en $|h\rangle|q\rangle|T_2\rangle|y\rangle$ indien T_1 in posisie x en T_2 in posisie y dieselfde inhoud het – dit wil sê die reël hang slegs af van die band se inhoud onder die kop en die interne toestand q en nié van die kop se posisie of die inhoud van die res van die band nie;

   (b) T' verskil hoogstens in posisie x van T;

(c) $|x' - x| \leq 1$ (afhangende van of die ooreenkomstige klassieke masjien een sel na links, of na regs, of glad nie beweeg nie);

(d) $h' = 1$ as en slegs as $q' = q_H$; en

(e) $T' = T$, $q' = q$ en $h' = h$ wanneer $h = 1$.

Eindig veel subreëls

$$|h\rangle|q\rangle|T\rangle|x\rangle \quad \longmapsto \quad \sum_{i=1}^{n} c_i|h_i\rangle|q_i\rangle|T_i\rangle|x_i\rangle \tag{1}$$

bepaal reeds U, want daar is, volgens bostaande voorskrifte, slegs eindig veel sulke subreëls moontlik – gegee dat die alfabet van simbole (hier binêr) en die aantal interne toestande beide eindig is. Let op dat die oorgangsreël ("program") 'n eindige spesifikasie het slegs indien die oorgangsamplitudes, die c_i in die subreëls hier bo, almal *berekenbare* komplekse getalle is, wat ons natuurlik deurgaans sal veronderstel. Die oorgangsreëls kan natuurlik lineêr uitgebrei word na eindige superposisies van die $|h\rangle|q\rangle|T\rangle|x\rangle$.

IV. Die KTM word aan die gang gesit met 'n eindige superposisie van invoere

$$|0\rangle|q_0\rangle|T\rangle|x\rangle.$$

Gesien die vorm wat die oorgangsreël mag aanneem en die feit dat daar slegs eindig veel interne masjientoestande is, sal die masjien by enige stap in sy berekeningslopie in die superposisie van slegs *eindig veel* toestande $|h\rangle|q\rangle|T\rangle|x\rangle$ uit die berekeningsbasis wees. Die begrip "berekening" vir 'n KTM is minder helder as vir 'n klassieke TM, want die KTM stop die voortgang van sy stappe slegs wanneer ons die haltkwabis waargeneem het en dan ook die inhoud van die band. 'n Mens mag dus aan die oorgangsreël U dink as stap-vir-stap *ad infinitum* toegepas, tensy die bediener van die masjien dit fisies, klassiek, van buite af stop.

Die beskrywing van die KTM wat ons hier gee, verskil van 'n klassieke omkeerbare TM in twee voor die hand liggende opsigte:

(a) Oorgangsreëls mag die masjien se kwantumtoestand afbeeld op die superposisie van verskillende toestande. Die wesenlike verskil met klassieke PTMe is dat, waar die KTM na 'n kwantumsuperposisie van toestande oorgaan, die klassieke PTM gesien kan word as oorgaande na òf 'n klassieke waarskynlikheidsverdeling oor klassieke toestande, òf na 'n spesifieke klassieke toestand met 'n sekere klassieke waarskynlikheid. Natuurlik gebruik kwantumberekening op 'n wesenlike wyse superposisie – soos in Shor en Grover se algoritmes.[15] Hoe en waarom dit werk, word toeganklik uiteengesit deur Fortnow.[7]

(b) Die invoer mag 'n superposisie van 'n eindige aantal "klassieke" invoere wees.

Dit volg nie onmiddellik dat 'n eindige versameling spesifikasies van die vorm (1) noodwendig 'n unitêre oorgangsreël U sal definieer nie, net soos wat 'n eindige versameling reëls

$$|h\rangle|q\rangle|T\rangle|x\rangle \quad \longmapsto \quad |h'\rangle|q'\rangle|T'\rangle|x'\rangle$$

vir 'n "klassieke" masjien nie noodwendig 'n omkeerbare TM sal bepaal nie. Natuurlik is unitariteit 'n voorwaarde vir 'n lewensvatbare kwantumtoestel.

Ons toon aan dat die spesifikasie van KTMe ten minste bevredigbaar is, dat sulke skepsels wiskundig bestaan. Veronderstel dat die onderliggende klassieke templaat 'n omkeerbare TM is, wat, nadat dit sy halttoestand bereik het, sy kop stapsgewys in een rigting aanhou verplaas sonder om ooit weer enigiets op sy band te verander. (Let op dat III(e) nie voorskryf dat $x' = x$ wanneer $h = 1$ nie; om omkeerbaar te wees, moet *iets* by elke stap verander.) Die ooreenkomstige KTM word nou gekonstrueer deur sy U lineêr voort te bring volgens die ooreenkomstige oorgangsreëls met die eenvoudige vorm hier bo – sonder superposisies. Hierdie U word dus bepaal deur 'n permutasie van die KTM se berekeningsbasis en is dus unitêr. Sou die reëls superposisies betrek (soos wat in alle interessante gevalle gebeur), dan word 'n bewys van unitariteit vir die geïnduseerde U vereis.

Om te toon dat só 'n bewys nie 'n onbenulligheid hoef te wees nie, beskou ons 'n vermeende KTM met interne begintoestand q_0 en halttoestand q_H gedefinieer deur die volgende subreëls:

$$\begin{aligned}
|0\rangle|q_0\rangle|\ldots 0\ldots\rangle|x\rangle \quad &\longmapsto \quad \frac{1}{\sqrt{2}}|1\rangle|q_H\rangle\left(|\ldots 0\ldots\rangle + |\ldots 1\ldots\rangle\right)|x+1\rangle \\
|0\rangle|q_0\rangle|\ldots 1\ldots\rangle|x\rangle \quad &\longmapsto \quad |1\rangle|q_H\rangle|\ldots 1\ldots\rangle|x+1\rangle \\
|1\rangle|q_H\rangle|T\rangle|x\rangle \quad &\longmapsto \quad |1\rangle|q_H\rangle|T\rangle|x+1\rangle
\end{aligned}$$

Dié subreëls skryf voor dat die masjien begin deur 'n $|0\rangle$ onder die kop te vervang met 'n superposisie van $|0\rangle$ en $|1\rangle$, 'n aanvanklike $|1\rangle$ onder die kop onveranderd te laat, en dan te halt, dit wil sê die finale toestand in te gaan waarin slegs die kop nog mag beweeg. Met 'n gegewe "klassieke" invoer sou ons kon sê dat die masjien omkeerbaar werk, want die invoer kan eenduidig uit die afvoer herwin word. Maar die vermeende KTM is nie *goedgevorm* nie en dus glad nie 'n egte KTM nie, aangesien

$$|0\rangle|q_0\rangle|\ldots 0\ldots\rangle|x\rangle \quad \text{ortogonaal op} \quad |0\rangle|q_0\rangle|\ldots 1\ldots\rangle|x\rangle \quad \text{is,}$$

maar

$$\frac{1}{\sqrt{2}}|1\rangle|q_H\rangle\left(|\ldots 0\ldots\rangle + |\ldots 1\ldots\rangle\right)|x+1\rangle$$

is beslis glad nie ortogonaal op $|1\rangle|q_H\rangle|\ldots 1\ldots\rangle|x+1\rangle$ nie. 'n Moontlike korrekte weergawe van so 'n masjien kan dalk gegee word deur

$$\begin{aligned}
|0\rangle|q_0\rangle|\ldots 0\ldots\rangle|x\rangle \quad &\longmapsto \quad \frac{1}{\sqrt{2}}|1\rangle|q_H\rangle\left(|\ldots 0\ldots\rangle + |\ldots 1\ldots\rangle\right)|x+1\rangle \\
|0\rangle|q_0\rangle|\ldots 1\ldots\rangle|x\rangle \quad &\longmapsto \quad \frac{1}{\sqrt{2}}|1\rangle|q_H\rangle\left(|\ldots 0\ldots\rangle - |\ldots 1\ldots\rangle\right)|x+1\rangle \\
|1\rangle|q_H\rangle|T\rangle|x\rangle \quad &\longmapsto \quad |1\rangle|q_H\rangle|T\rangle|x+1\rangle,
\end{aligned}$$

aangesien die vorige beswaar dan uitgeskakel is. Die eis van unitariteit verbied klaarblyklik sekere kombinasies van voortbringende subreëls van die vorm (1) en verg groot sorg om die goedgevormdheid te verseker van enige masjien wat mens mag konstrueer.

3.2 Tydevolusie en die haltskema van die KTM

As U die unitêre operator is wat een toepassing van die oorgangsreël (dit wil sê een stap in 'n berekening) van die KTM beskryf, dan word die onwaargenome evolusie van die masjien (waarby

nie eens die haltkwabis gemeet word nie) oor n stappe eenvoudig deur $V = U^n$ beskryf. As die eerste meting, beskryf deur die selftoegevoegde operator J_1 (in die berekeningsbasis van eievektore van J_1) na n_1 stappe plaasvind, dan word die evolusie van die masjien vir die eerste $n_1 + j$ stappe beskryf deur

$$U^j J_1 U^{n_1}.$$

Laasgenoemde is in die algemeen nie meer unitêr nie, omdat J_1 dit nie is nie. Masjiene ontwikkel dus unitêr slegs as geen meting plaasvind nie. Daarom moet die KTM dus nie as 'n suiwer kwantumtoestel gesien word nie, maar eerder as 'n soort hibriede apparaat. In feite, soos ons hier onder sal sien, is die afvoer van die masjien na n stappe sonder meting van die haltkwabis ekwivalent aan wat verkry word deur die haltkwabis na elk van die stappe waar te neem. Nogtans het die KTM geen eksplisiete bogrens op die aantal stappe wat dit mag loop nie, sodat die werking van die masjien nie gesien kan word as die ekwivalent van enige enkele kwantumeksperiment nie.

Die afvoer op die band van 'n KTM is natuurlik 'n superposisie van basisvektore wat afgelees (gemeet) moet word nadat meting van die haltkwabis dit in toestand 1 gevind het. Die bediener van die masjien mag enige tyd, selfs tussen elke twee toepassings van U op die masjien se kwantumtoestand, die haltkwabis meet om te besluit of die bandinhoud gemeet moet word (wat die masjien laat verval in een van sy basistoestande). Die gemete haltbis (0 of 1) dui vir die bediener aan wanneer (vir $h = 1$) die afvoer van die berekening van die band afgelees kan word sonder om die berekening onbehoorlik te versteur – iets wat ons hier onder in meer besonderhede verduidelik.

Deutsch se oorspronklike idee was skynbaar dat daar geen verstrengeling tussen die haltkwabis (as komponentjie van die KTM) en die res van die masjien moet wees nie, maar, soos deur Myers[13] beskryf, kan dít nie gewaarborg word nie. Die *afvoer* van 'n KTM vir 'n spesifieke invoer x (moontlik 'n superposisie van "klassieke" invoere) – ná die waarneming $h = 1$, maar vóór waarneming van die res van die band se inhoud – kan gesien word as 'n waarskynlikheidsverdeling P_x oor alle moontlike bandinhoude. Die bydrae van Miyadera en Ohya[12] beklemtoon ook hierdie punt.

3.3 Geldigheid van die haltskema

Die evolusie van 'n KTM gaan voort selfs nadat die haltkwabis waargeneem is – en wel sonder dat die waarskynlikheidsverdeling oor bandinhoude wat ons hier bo die *afvoer* genoem het versteur word. Dit is so omdat die waarneming die evolusie in 'n sekere sin maar net in een van twee takke ($h = 0$ of $h = 1$) van die berekening projekteer.[14] Laat ons dié resultaat in bietjie meer besonderhede uitpluis.

Veronderstel U beskryf 'n KTM met 'n behoorlike haltskema soos hier bo beskryf, dit wil sê U is unitêr en wanneer, vir een of ander geldige invoer, die haltkonfigurasie

$$|1\rangle|q_H\rangle|T\rangle \sum_i c_i|x_i\rangle$$

in 'n evolusiestap voorkom (moontlik in 'n superposisie), dan geld

$$U|1\rangle|q_H\rangle|T\rangle \sum_i c_i|x_i\rangle = |1\rangle|q_H\rangle|T\rangle \sum_j d_j|y_j\rangle$$

vir een of ander y. Dit beteken eenvoudig dat U voorwaarde III(e) in Afdeling 3.1 gehoorsaam. Veronderstel dat die KTM na $n > 0$ toepassings van U in die toestand

$$c_1|1\rangle|\phi_1\rangle + c_2|0\rangle|\phi_2\rangle$$

is, en dat (Geval 1) die haltkwabis nie nou gelees word nie. Ons aanvaar dat $|\phi_1\rangle$ and $|\phi_2\rangle$ genormaliseer is en aangesien $|1\rangle|\phi_1\rangle$ en $|0\rangle|\phi_2\rangle$ ortogonaal is, het ons dat

$$|c_1|^2 + |c_2|^2 = 1.$$

(Let op dat die waarskynlikheid om nou (Geval 2) by meting van die haltkwabis dit geaktiveerd, $h = 1$, te vind, $|c_1|^2$ is.)

As U nog een keer toegepas word, kry ons die toestand

$$c_1 U|1\rangle|\phi_1\rangle + c_2 U|0\rangle|\phi_2\rangle.$$

Aangesien U unitêr is en III(e) geld, moet

$$U|1\rangle|\phi_1\rangle = |1\rangle|\psi_1\rangle$$

en ook

$$U|0\rangle|\phi_2\rangle = d_1|1\rangle|\psi_2\rangle + d_2|0\rangle|\psi_3\rangle$$

vir genormaliseerde ψ_i en d_i met

$$|d_1|^2 + |d_2|^2 = 1.$$

Die KTM se toestand is nou

$$c_1|1\rangle|\psi_1\rangle + c_2 d_1|1\rangle|\psi_2\rangle + c_2 d_2|0\rangle|\psi_3\rangle.$$

Uit die unitariteit van U en die ortogonaliteit van $|1\rangle|\phi_1\rangle$ en $|0\rangle|\phi_2\rangle$ volg dat $U|1\rangle|\phi_1\rangle$ ortogonaal op $U|0\rangle|\phi_2\rangle$ is, dit wil sê

$$|1\rangle|\psi_1\rangle \quad \text{is ortogonaal op} \quad d_1|1\rangle|\psi_2\rangle + d_2|0\rangle|\psi_3\rangle.$$

Maar $|1\rangle|\psi_1\rangle$ is ortogonaal op $|0\rangle|\psi_3\rangle$ en gevolglik is die drie genormaliseerde toestande

$$|1\rangle|\psi_1\rangle, \quad |1\rangle|\psi_2\rangle, \quad |0\rangle|\psi_3\rangle$$

paarsgewys ortogonaal. Die waarskynlikheid om nou 'n geaktiveerde haltkwabis, $h = 1$, te meet is

$$|c_1|^2 + |c_2 d_1|^2,$$

wat groter is as die $|c_1|^2$ wat by 'n vorige stap die waarskynlikheid sou wees – soos te verwagte. Sou ons by 'n vorige stap (Geval 2) reeds die haltkwabis gemeet het, sou ons met waarskynlikheid $|c_1|^2$ 'n geaktiveerde en met waarskynlikheid $|c_2|^2$ 'n ongeaktiveerde haltbis gevind het. In laasgenoemde geval, $h = 0$, sou die toestand van die masjien na $|0\rangle|\phi_2\rangle$ verval het, waarna nog 'n toepassing van U die toestand sou bring tot

$$d_1|1\rangle|\psi_2\rangle + d_2|0\rangle|\psi_3\rangle.$$

Waarneming van die haltkwabis in hierdie toestand sou met waarskynlikheid $|d_1|^2$ resultaat $h = 1$ lewer. Siende dat die twee meetgebeurtenisse in Geval 2 onafhanklik is, lewer klassieke waarskynlikheidsleer met Bayes se stelling vir die meting $h = 1$ na die laaste stap in Geval 2 nou die waarskynlikheid

$$|c_1|^2 + |c_2|^2 \cdot |d_1|^2,$$

wat dan dieselfde waarskynlikheid is as om $h = 1$ te meet na die laaste stap in Geval 1. Die waarskynlikheid om nou $h = 1$ te meet op enige stadium in die berekeningsproses, bly dus presies

dieselfde wanneer $h = 0$ in feite gemeet word en die berekening daarna een U-stap verder gevoer word.

Die voorafgaande elementêre uiteensetting illustreer die gedagte wat Ozawa[14] ontwikkel het. Daardie artikel bespreek die waarskynlikheid om die bandinhoud T, met die masjien in 'n spesifieke toestand en die haltkwabis (iewers in die toestand) geaktiveer, waar te neem in twee gevalle:

(i) deur die haltkwabis na n_1 U-stappe waar te neem (en, indien $h = 1$, dalk T te lees) en dan na 'n verdere n_2 U-stappe dit weer te doen;
of

(ii) deur die masjien sonder enige waarneming deur $n_1 + n_2$ U-stappe te laat loop en dan die haltkwabis (en dalk T) waar te neem.

Ozawa bewys dat die waarskynlikheid om 'n spesifieke inhoud T van die band waar te neem in die twee gevalle presies identies is. Miskien behoort dit genoem te word dat in Ozawa se beskrywing die posisie van die kop op die band deel van die bandinhoud is, terwyl ons dit 'n afsonderlike deel van die basisvektor hou. Maar dit verander niks wesenliks aan Ozawa se resultaat nie.

3.4 Besware teen die haltskema

Soos reeds in Afdeling 3.2 genoem, het Myers[13] aangetoon dat dit moontlik moet wees om 'n KTM te vind in 'n superposisie van basistoestande met die haltkwabis geaktiveer en basistoestande met die haltkwabis (nog) nie geaktiveer nie. Onder andere is dit so in die volgende geval: x is 'n invoer waarvoor die masjien na N_x stappe die haltkwabis aktiveer en y 'n invoer waarvoor dit N_y ($\neq N_x$) stappe neem. Dan sal die masjien met invoer 'n superposisie van x en y – tussen stappe nommers N_x en N_y – sigself in só 'n superposisie bevind. Daarmee word die inherent probabilistiese aard van KTMe beklemtoon, soos ook duidelik aangedui deur Miyadera en Ohya.[12] Dat dit nie *per se* 'n beswaar is nie, het ons aan die hand van Ozawa[14] in Afdeling 3.3 betoog.

Kieu en Danos[11] gee voor om die onmoontlikheid van die gewenste haltskema vir enige unitêre operator U aan te toon. Hulle redeneer soos volg. Veronderstel daar bestaan 'n toestand $|\psi\rangle$ van die masjien sodanig dat

$$(\langle 0| \otimes I)\ |\psi\rangle = 1,$$

waar I die identiteitsoperator is, en daar bestaan'n $N > 0$ waarvoor geld dat

$$(\langle 1| \otimes I)\ U^N|\psi\rangle > 0. \tag{2}$$

Laat verder N die kleinste getal wees waarvoor relasie (2) geld. Só 'n $|\psi\rangle$ sou die begintoestand kon wees van 'n KTM wat voorberei is met 'n geldige invoer wat mettertyd die haltkwabis – ten minste 'n bietjie – aktiveer, terwyl n die aantal U-stappe verteenwoordig wat nodig is vir 'n positiewe kans om hoegenaamd $h = 1$ waar te neem. As daar geen sodanige U bestaan nie, dan is daar vir die masjien wat deur U beskryf word geen geldige invoer wat tot 'n positiewe waarskynlikheid vir 'n afvoer kan lei nie – en die masjien is dus nutteloos. Kieu en Danos gaan voort deur korrek op te merk dat (in ons notasie)

$$U^{N-1}|\psi\rangle \quad \text{loodreg op alle} \quad |1\rangle|q_H\rangle|T\rangle|x\rangle$$

is as gevolg van N se minimaliteit en dat gevolglik, siende dat U unitêr is,

$$U^N|\psi\rangle \quad \text{loodreg is op alle} \quad U|1\rangle|q_H\rangle|T\rangle|x\rangle.$$

Dit is dan veronderstel om in stryd met (2) te wees. Ja, dit sou waar wees indien, soos beweer in Kieu en Danos se artikel, die deelruimte V onderspan deur al die $|1\rangle|q_H\rangle|T\rangle|x\rangle$ identies sou wees aan die deelruimte $\tilde{V}$ onderspan deur al die $U|1\rangle|q_H\rangle|T\rangle|x\rangle$. Dit lyk of Kieu en Danos eenvoudig veronderstel dat die beperking $U|_V$ van U tot V unitêr is, waaruit inderdaad sou volg dat $V = \tilde{V}$, maar vir hierdie veronderstelling ontbreek 'n bewys. Hoewel $U|_V$ die inproduk behou, is dit nie noodwendig unitêr nie, want sy waardegebied onderspan nie noodwendig die hele V nie. Trouens, unitariteit van $U|_V$ (dit wil sê $V = \tilde{V}$) sou *direk* impliseer dat daar geen $|\psi\rangle$ soos hier bo bestaan nie.

Bedenkinge oor die haltskema is ook deur Shi[16] geopper, hoewel in Deutsch[5] se oorspronklike konteks, waar superposisies

$$c_1|1\rangle|\phi_1\rangle + c_2|0\rangle|\phi_2\rangle$$

met $|c_1 c_2| > 0$ verbode is, met ander woorde waar superposisies met nie-nul waarskynlikhede vir beide haltbisse nie voorkom nie. In feite het Shi die bestaan ondersoek van universele kwantumrekenaars, 'n vraagstuk waarvoor die haltskema groot relevansie het en waarheen ons die fokus nou verskuif.

4. UNIVERSALITEIT EN PROGRAMMEERBAARHEID IN DIE MASJIENMODEL

Die begrip van 'n *universele* rekentoestel in 'n spesifieke klas is van kritieke belang vir programmeerbaarheid. Sonder universaliteit kan daar geen programmeringsbegrip wees nie, want elke probleem sal 'n pasgemaakte rekenmasjien vereis. Die bestaan van 'n universele masjien in 'n klas (byvoorbeeld 'n universele Turing-masjien), en die ekwivalensie van alle universele masjiene in 'n klas, maak dit ook moontlik om 'n teorie van berekeningskompleksiteit te ontwikkel. Vanselfsprekend, spring ons weg met 'n oorsig oor die gevestigde universaliteitsbegrippe in klassieke deterministiese en in probabilistiese berekening, voordat ons die begrip van 'n "universele KTM" – wat deur Deutsch ingevoer is – ondersoek.

4.1 Klassieke universaliteit en berekenbaarheid

Beskou 'n algemene aftelbare klas masjiene wat parsiële funksies bereken, dit wil sê funksies wat nie noodwendig vir alle invoere gedefinieer is nie (aangesien, in die geval van 'n Turing-masjien, die masjien dalk nie halt nie). Noem dié klas *Manchester-masjiene* (MMe). Aangesien daar net aftelbaar veel masjienbeskrywings is, sal ons aanneem iedere Manchester*-masjien word beskryf deur 'n natuurlike getal. Dit hoort moontlik te wees om die volledige beskrywing van die masjien op 'n baie intuïtiewe manier te herwin van die natuurlik getal en dit kan derhalwe nie 'n eenvoudige enumerasie van die aftelbare versameling wees nie. Gestel Φ_n is die parsiële funksie wat deur die masjien n bereken word en kies 'n vaste MM-berekenbare bijeksie† $h : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, gegewe dat 'n dergelike funksie wel bestaan.‡

*Alan Turing het ná die Tweede Wêreldoorlog in die stad Manchester gewerk aan die bou en programmeer van een van die eerste elektroniese rekenaars.

†Die oplettende leser sal dit byval dat h die eerste (en laaste) tweeveranderlike funksie is wat hier voorkom, maar dat ons eksplisiet Manchester-masjiene met slegs een invoer beskryf het. Dít is nie heeltemal logies nie, maar die probleem kan opgelos word op 'n gevestigde wyse. Dit voldoen om te sê dat 'n mens h MM-berekenbaar moet kan beskou op 'n natuurlike en logiese manier. 'n Mens het maar één so 'n funksie h nodig en ons brei nie hier verder daaroor uit nie.

‡Indien nie, dan sou die klas van Manchester-masjiene regtig arm wees. Dit sou regtig nie saak maak indien ons $h : (x, y) \mapsto 2^x 3^y$ sou kies nie, maar die verdere aanname dat h surjektief is, is skadeloos en gerieflik.

Definisie 1 *Indien daar 'n getal N bestaan, só dat*

$$\Phi_N\left(h(n,m)\right) = \Phi_n(m)$$

wat beteken dat die funksies òf gelyk aan mekaar is en beide gedefinieer òf beide ongedefinieer, vir alle n en m, dan word die masjien wat deur N beskryf word 'n universele Manchester-masjien *(UMM) genoem.*

Programmeerbaarheid is onlosmaakbaar gekoppel aan die universaliteitsbegrip en is, natuurlik, 'n voorvereiste vir universaliteit. Is dit 'n voldoende voorvereiste? 'n Spesifieke Turing-masjien word normaalweg toegewy aan 'n spesifieke taak, gedefinieer deur 'n versameling vyftalle wat die bewerkings beskryf wat sekwensieel uitgevoer moet word. Elke Turing-masjien het dus 'n eindige beskrywing (van interne toestande, bandinskrywings en oorgangsreëls – wat onbegrens is, maar altyd eindig veel) wat gebruik sou kon word as die invoer vir 'n ander Turing-masjien. 'n Universele Turing-masjien (waarvan daar natuurlik oneindig veel bestaan) kan alle ander Turing-masjiene naboots en is dus programmeerbaar vir die hele klas van Turing-masjiene. Indien 'n masjien programmeerbaar is vir enige toestel in sy klas, dan is dit universeel. Nie alle programmeerbare rekentoestelle is universeel nie. Om die waarheid te sê, 'n mens kan die term *programmeerbaar* gebruik om enige toestel te beskryf wat invoere aanvaar van die vorm $\langle p, x\rangle$ waar p die "program" en x die "data" is en die inwerking van die masjien op x afhang van p. Sulke masjiene is universeel (vir hulle klas) indien hulle – deur 'n geskikte keuse van p – die werking van enige ander masjien in die klas kan naboots.

4.2 Universaliteit vir probabilistiese Turing-masjiene

Aangesien halt 'n probabilistiese begrip is vir die KTM, moet die universaliteitsbegrip vir kwantumtoestelle ná wees aan dié vir probabilistiese masjiene. Definisie 1 is egter nie direk van toepassing op probabilistiese masjiene nie en dit moet soos volg veralgemeen word.

Definisie 2 *Indien daar 'n getal N bestaan, só dat*

$$\Phi_N\left(h(n,m)\right) = \Phi_n(m),$$

wat beteken dat die funksies òf gelyk aan mekaar is en beide gedefinieer òf beide ongedefinieer (indien deterministies) en indien nie deterministies nie dat die waardes dieselfde waarskynlikheidsverdeling het*, vir alle n en m, dan word die masjien wat deur N beskryf word 'n* universele Manchester-masjien *(UMM) genoem.*

In die geval, byvoorbeeld, van deterministiese Turing-masjiene ('n egte deelversameling van die probabilistiese masjiene) stem die twee begrippe natuurlik presies ooreen. Die hoofdoelwit van hierdie afdeling is om hierdie (tweede) universaliteitsbegrip vir kwantummeganiese Turing-masjiene (KTMe) te bespreek.

'n Mens kan, terloops, maklik aantoon dat elke funksie f wat bereken kan word in hierdie sin deur 'n PTM ook berekenbaar is deur 'n gewone TM in die gebruiklike sin. Desnieteenstaande het PTMe nog altyd belangstelling gewek omdat probabilistiese algoritmes wat heel vinnig is in vergelyking met die beste bekende klassieke algoritmes, dikwels gevind kan word. Die klas van PTMe word dikwels gedefinieer deur die waarskynlikhede tot $\frac{1}{2}$ en 1 alleen te beperk. In dié geval kan die klas ook verkry word deur die gewone TMe te neem en 'n spesiale skryfinstruksie toe te voeg wat 'n toevalsbis op die band skryf. PTMe word dikwels, in dié model, beskryf as "TMe met

toegang tot die werp van 'n foutvrye muntstuk". Dit is maklik om te sien hoe 'n universele masjien in dié klas daar sou uitsien: dit sou eenvoudig 'n gewone UTM wees, toegerus met die bykomende instruksie vir die skryf van 'n toevalsbis op die band. So 'n *universele PTM* (UPTM) sou enige ander "muntstukwerp"-masjien perfek kan naboots, waarmee bedoel word dat die afvoer van die PTM presies dieselfde verdeling sou hê as die afvoer van die PTM wat dit besig is om na te boots.

Watter algemene PTMe sou ons UPTM dan eksak kan naboots? Wel, aangesien elke PTM 'n eindige beskrywing het, sou die UPTM slegs nodig hê om 'n aftelbare versameling PTMe na te boots. Kom ons beperk onsself tot die PTMe met *berekenbare* oorgangswaarskynlikhede. Elke masjien van dié aard word volledig beskryf deur 'n stel oorgangsreëls en programme vir die berekening van die gepaardgaande waarskynlikhede. Dié beskrywing is eindig – danksy die beperking van die waarskynlikhede tot berekenbare getalle. Aangesien daar geen redelike manier is om 'n eindige beskrywing te gee van PTMe met nie-berekenbare oorgangswaarskynlikhede nie, behalwe vir die gewone teenstrydige definisies van die tipe "één meer as die grootste getal wat met dertien woorde beskryf kan word", sluit hierdie die bespreking vir PTMe af. Om willekeurige reële oorgangswaarskynlikhede te beskou sou, terloops, ook heeltemal geen sin maak nie, want die (PTM-)berekenbaarheid van enige deelversameling van die natuurlike getalle sou onmiddellik hieruit volg.

4.3 'n Universele KTM?

Deutsch het die begrip "universele kwantumrekenaar" (uKR, waar *u* met opset met 'n kleinletter geskryf word om die verskil te beklemtoon tussen dié universaliteitsbegrip en die voorafgaande) ingevoer.[5] Die uKR van Deutsch is in wese 'n KTM soos hier bo, in Afdeling 3, beskryf – gebaseer op 'n klassieke UTM met addisionele bewerkings wat die benadering tot willekeurige noukeurigheid van enige unitêre transformasie op 'n enkele kwabis moontlik maak. Deutsch het in dié artikel aangetoon dat vir enige gegewe L, $\varepsilon > 0$ en kwantumtoestel U wat inwerk op L kwabisse, daar 'n program p_L vir die uKR bestaan ('n klassieke eindige string bisse) wat (met invoer $|p_L\rangle$ gevolg deur 'n eindige superposisie van basiese L-kwabistoestande) die inwerking van U op die eindige superposisie van basiese L-kwabistoestande benader met akkuraatheid van minstens ε (in die inproduknorm). Dít is nie dieselfde tipe van universaliteit wat ons vir probabilistiese en vir deterministiese Turing-masjiene gesien het nie en selfs die konkatenasie-skema wat deur Deutsch voorgestel is, is bevraagteken – byvoorbeeld, deur Shi.[16]

Indien ons nou die vorige (tweede) definisie van universaliteit beskou, dan kan daar geen universele masjien wees nie, vir die eenvoudige rede dat in Deutsch se model daar ooraftelbaar veel (oorgangsreëls vir) KTMe is. Vir breedweg dieselfde redes as wat hier bo uiteengesit is vir PTMe, beperk ons onsself voortaan tot KTMe met berekenbare oorgangswaarskynlikhede, dit wil sê oorgangsamplitudes waarvoor beide die reële en die imaginêre dele berekenbare getalle is. Ons kies nou 'n vaste metodiek vir die enkodering van die KTMe en assosieer met enige masjien M die kleinste* natuurlike getal wat M voorstel. Let op dat ons sê dat 'n KTM afvoer y het met waarskynlikheid p indien die waarskynlikheid dat 'n mens *ooit* die masjien in die halttoestand waarneem, met die band in toestand $|y\rangle$, wel p is. Bestaan daar 'n universele masjien, in die sin van Definisie 2 vir dié (beperkte) klas KTMe?

Deutsch het die ietwat onvolledige resultaat hier bo vermeld bewys. 'n Ander gedeeltelike oplossing is deur Bernstein en Vazirani[3] gegee. Hulle het aangetoon dat daar 'n kwantummeganiese Turing-masjien $\mathcal{U}$ bestaan ($\mathcal{M}$ in hulle notasie), sodat (in die outeurs se vertaling)

> "vir enige welgevormde† KTM M, enige $\varepsilon > 0$, en enige T, kan $\mathcal{U}$ vir M naboots met

*Twee verskillende natuurlike getalle mag, natuurlik, fisies identiese masjiene voorstel.

†Bedoelende dat die operator vir tydevolusie unitêr is, trouens aan al die voorskrifte in Afdeling 3.1 voldoen.

akkuraatheid ε vir T stappe met tydsvertraging 'n polinoomfunksie van T en $\frac{1}{\varepsilon}$."

Die tydsvertraging en die program vir $\mathcal{U}$ hang beide af van die lengte van die invoer. Die volledige Bernstein-Vazirani-resultaat sou saamgevat kon word met die stelling dat

> daar bestaan 'n KTM $\mathcal{U}$ só dat vir elke KTM M met eindige beskrywing $\bar{M}$, n, ε en T, 'n program $\mathcal{P}(\bar{M}, n, \varepsilon, T)$ en 'n funksie $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ (beide berekenbaar, in die klassieke sin) bestaan sodat wanneer $\mathcal{U}$ met die invoer $|\mathcal{P}(\bar{M}, n, \varepsilon, T)\rangle \otimes |x\rangle$ bedryf word, waar $|x| = n$, vir $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ stappe, dan het – met akkuraatheid binne ε – die afvoer dieselfde verdeling oor die waarneembare toestande as wanneer 'n mens M op die invoer $|x\rangle$ laat inwerk vir T stappe.

Die nabootsing is duidelik slegs *benaderd*. Dít wat Bernstein en Vazirani bedoel met "akkuraatheid binne ε" is dat indien P die waarskynlikheidsverdeling is vir die waarneembare toestande van $\mathcal{U}$ na $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ stappe met die gegegewe invoer en Q die ooreenstemmende waarskynlikheidsverdeling van M na T stappe, dan is

$$\frac{1}{2}\sum_{x} |P(x) - Q(x)| \;\leq\; \varepsilon,$$

waar die sommasie gaan oor alle moontlike waarneembare toestande x. Weereens is benaderde simulasie iets heel anders as die universaliteitsbegrip vir gewone en probabilistiese Turing-masjiene (met berekenbare waarskynlikhede), aangesien die universele masjien se nabootsing, in laasgenoemde geval, *eksak* is. Om $\mathcal{U}$ vir presies $f_{\bar{M}}(T, n, \frac{1}{\varepsilon})$ stappe op enige invoer $|\mathcal{P}(\bar{M}, n, \varepsilon, T)\rangle \otimes |x\rangle$ te laat inwerk, sal die inwerking van M op $|x\rangle$ vir T stappe (benaderd) naboots. Ons mag nie $\mathcal{U}$ enige verdere aantal stappe laat inwerk nie aangesien die toestand van die masjien dan kan begin wegdryf van die nagebootste toestand van M na T stappe. Hierdie gedrag is heel anders as dié van die UTM of UPTM – waar dit nie nodig is om die aantal stappe wat uitgevoer word te beperk nie.

Wat van die invoer vir die masjien? Oor die algemeen is die invoer van 'n KTM 'n eindige superposisie van basistoestande van die band maar die Bernstein-Vazirani-stelling wat hier bo aangehaal word, is slegs van toepassing op 'n enkele toestand. Dit is nie 'n probleem nie: dit is voor die hand liggend om te sien dat dit ook van toepassing is op 'n superposisie van m basistoestande – vervang net ε deur $\frac{1}{m}\varepsilon$.

Die Bernstein-Vazirani-masjien $\mathcal{U}$ suggereer onmiddellik die volgende semi-universele hibriede toestel (SUHT). Dié toestel neem die beskrywing $\bar{M}$ van 'n KTM M asook x en ε as invoere. Die masjien werk dan soos volg.

```
T := 1;
n := |x|;
doen
     bereken P := P(M̄, n, ε/T, T);
     bereken S := f_M̄(T, n, 1/ε);
     laat U op |P⟩⊗|x⟩ inwerk vir S stappe;
     gee 'n sein dat die kwantumdeel van die toestel waargeneem mag word;
     wag 'n bietjie;
     stel die kwantumdeel van die toestel terug;
     T := T+1;
onderwyl waar;
```

Let op dat, deur ε met $\frac{\varepsilon}{T}$ te vervang, ons verseker het dat deur eenvoudig die SUHT te laat werk, ons nie net die nagebootste gedrag van M vir al hoe langer tydperke sal kan waarneem nie, maar ook met steeds groeiende akkuraatheid. Die SUHT is egter nog nie 'n universele masjien van die klas

van KTMe in die sin van Definisie 1 of Definisie 2 nie. Dít is nie net waar omdat die nabootsings slegs *benaderd* is nie – maar ook vir die fundamentele rede dat ons nie weet of die SUHT self 'n KTM is al dan nie!

Die SUGT lyk na 'n ware hibriede toestel wat bestaan uit 'n klassieke masjien van die Turing-tipe en 'n kwantumdeel. Die SUHT is – in 'n sekere sin – 'n robot wat 'n kwantumtoestel kan bedryf (wat deel van sigself uitmaak) en daar is geen rede om te dink dat so 'n robot nie gebou kan word nie. Die probleem lê egter daarin dat die robot net 'n spesiale sein gee wanneer *ons* die kwantumdeel van die toestel kan waarneem. Dit kan nie weet of ons die kwantumtoestel waargeneem het of nie – andersins sou die waarnemer deel van die toestel word...

Voorts is die werking van enige kwantumtoestel omkeerbaar. In die geval van die SUHT is die stap "stel die kwantumdeel van die toestel terug" in dié opsig problematies. Indien die kwantumdeel nie waargeneem is gedurende die stap "wag 'n bietjie" nie, dan kan die inverse van die evolusie-operator van $\mathcal{U}$ gebruik word om so 'n terugstelling te doen. Maar, gestel die waarnemer(s) het wel 'n waarneming gemaak gedurende "wag 'n bietjie". Nou sal die inverse van die evolusieoperator van $\mathcal{U}$ nie meer die toestel terugstel nie. Dit is 'n ernstige probleem. In 'n gewone KTM gaan die tydevolusie van die masjien voort, selfs al is die haltbis waargeneem. Vir die SUHT sal die waarneming van die haltbis (wat moontlik in 'n gesuperponeerde toestand is, hoewel nie noodwendig verstrengel met die res van die masjien nie) die bewerking van die masjien onomkeerbaar maak. Dit is eenvoudig omdat die evolusie van die gewone KTM kan voortgaan sonder om die waarskynlikheidsverdeling wat as die KTM se afvoer gedefinieer is te versteur (volgens Ozawa,[14] Afdeling 3.3 hier bo), aangesien die waarneming 'n mens, in 'n sekere sin, projekteer op 'n spesifieke vertakking ($h = 0$ of $h = 1$) van die berekening. Vir die hibriede toestel is dit nie so eenvoudig nie, want die terugstel-stap vereis 'n onversteurde kwantumdeel. Indien die kwantumdeel egter op tydstip $T = k$ versteur is, sal die bewerking wat hier bo uiteengesit is nie die kwantumdeel op 'n juiste manier kan terugstel nie en sal dit nie die lus vir $T = k + 1$ getrou kan uitvoer nie.

Dit is natuurlik altyd moontlik vir die operateur om die instruksie te ontvang om die hele hibriede toestel terug te stel na enige waarneming, maar dan sou ons te doen hê met 'n nuwe biohibriede toestel – nog verder van 'n universele masjien in die klas van KTMe. In die klassieke berekening sou dít gelykstaande daaraan wees om te vereis dat die gebruiker streng die rekenaar moet terugstel (*reboot*) elke keer nadat die skerm waargeneem is. Daar sou geen bedryfsoutonomie wees nie. Suiwer kwantumtoestelle word, terloops, deur die Kloonverbodstelling[15] verhoed om aanvangskonfigurasies van deelstelsels te kopieer en dít maak 'n hibriede stelsel gebaseer op aanhoudende kopiëring van die toestel onmoontlik.

Vermoede 1 *Die SUHT wat uit Bernstein en Vazirani se $\mathcal{U}$ afgelei is kan nie omkeerbaar werk nie en is derhalwe nie 'n KTM nie.*

Die onmiddellike gevolg van hierdie vermoede is dat (tot nou) die bestaan van 'n universele toestel binne kwantumberekening nie aangetoon is nie en dat universele programmeerbaarheid in die KTM-model nog ontbreek.

5. SLOTSOM

Die navorsing aangaande kwantumberekening oor die afgelope 20 jaar was baie suksesvol in

- die stimuleer van die ontwikkeling van kwantumkriptografie, wat reeds in bedryfstoepassing is;

- die bestudeer van kwantuminligting; en
- die ontdekking van innoverende nuwe algoritmes vir tradisioneel moeilike en interessante probleme soos priemfaktorisering.

Hierdie bydrae het probeer verduidelik waarom sekere (sterk en interessante) resultate in kwantumberekening steeds nie die mas opkom om universaliteit (en programmeerbaarheid) vir kwantumberekening te bevestig nie. Op die heel minste, hoort navorsers in dié veld te verduidelik hoe die resultate van Deutsch, Bernstein en Vazirani, en ander, gebruik kan word om 'n ten volle programmeerbare universele kwantumtoestel te bou. In die ergste geval, moet daar bewys word dat geen so 'n toestel bestaan nie. Ons vermoed dat, soos by KTMe, ander benaderings tot kwantumberekening (byvoorbeeld netwerkgebaseerde,[6] metinggebaseerde[4] of adiabatiese[1] kwantumberekening) wat aanspraak maak op "universele hulpbronne" soortgelyke konseptuele probleme sal teëkom in die soeke na 'n universele, programmeerbare masjien.

VERWYSINGS

1. Aharonov, D., van Dam, W., Kempe, J., Landau, Z., Lloyd, S., and Regev, O. (2007). Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM Journal on Computing*, 37:166–194.

2. Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22:563–591.

3. Bernstein, E. and Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal on Computing*, 26:1411–1473.

4. den Nest, M. V., Miyake, A., Dur, W., and Briegel, H. J. (2006). Universal resources for measurement-based quantum computation. *Physical Review Letters*, 97:150504–4.

5. Deutsch, D. (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400:97–117.

6. Deutsch, D. (1989). Quantum Computational Networks. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 425:73–90.

7. Fortnow, L. (2000). One complexity theorist's view of quantum computing. *Electronic Notes in Theoretical Computer Science*, 31.

8. Fouché, W., Heidema, J., Jones, G., and Potgieter, P. H. (2008). Universality and programmability of quantum computers. *Theoretical Computer Science*, 403:121–129.

9. Fouché, W. L., Heidema, J., Jones, G., and Potgieter, P. H. (2007). Halting in quantum Turing computation. In Adamatzky, A., Bull, L., Costello, B. D. L., Stepney, S., and Teuscher, C. (eds), *Unconventional Computing 2007*. Frome (UK). Luniver Press.

10. Hermes, H. (1969). *Enumerability, decidability, computability. An introduction to the theory of recursive functions*. Translated from the German by G. T. Hermann and O. Plassmann. Second revised edition. *Die Grundlehren der mathematischen Wissenschaften*, Band 127. Springer-Verlag New York, Inc., New York.

11. Kieu, T. D. and Danos, M. (2001). A No-Go Theorem for Halting a Universal Quantum Computer. *Acta Physica Hungarica A) Heavy Ion Physics*, 14(1):217–225.

12. Miyadera and Ohya (2005). On Halting Process of Quantum Turing Machine. *Open Systems & Information Dynamics*, 12:261–264.

13. Myers, J. M. (1997). Can a Universal Quantum Computer Be Fully Quantum? *Physical Review Letters*, 78(9):1823–1824.

14. Ozawa, M. (1998). Quantum Nondemolition Monitoring of Universal Quantum Computers. *Physical Review Letters*, 80:631–634.

15. Potgieter, P. H., Heidema, J., and Fouché, W. L. (2005). Kwantumberekening. *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie*, 24:60–83.

16. Shi, Y. (2002). Remarks on universal quantum computer. *Physics Letters A*, 293(5–6):277–282.

17. Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883–887.