

Skammtareikningar, skammtatölvur og hönnun ofurleiðandi segulflæðisskammtabita

Tryggvi Ingason og Snorri Ingvarsson

Raunvísindastofnun Háskólans

Vefútgáfa: 26. apríl 2006

Ágrip – Hér eru kynntir skammtareikningar og skammtatölvur. Fjallað er um hagnýtingu skammtatölva við lausn verkefna sem eru óviðráðanleg með tölvum nútímans. Við gerum einnig grein fyrir helstu eiginleikum segulflæðisskammtabita sem nú eru í þróun hjá IBM. Vonir eru bundnar við að þessi gerð skammtabita opni möguleika á sköpun, þ.e. tengingu fleiri bita í stærri starfhæfar skammtatölvur. Kynnt er endurhönnun skammtabitans sem auðveldar stjórnun hans og dregur úr áhrifum ytra suðs.

1. Inngangur

Undanfarin misseri hefur orðið æ erfiðara að beita “smækkunarlíkaninu” til þess að byggja nýjar og öflugri tölvur. Það gengur út á að búa til sífellt smærri útgáfur rása og rásafhluta til þess að öðlast hraðvirkari reiknitæki og þéttari geymslueiningar. Vandamál sem fylgja aðferðinni eru hækkandi smugstraumar í gegnum æ þynnri einangrandi lög stýrihlíða í smárum [1] og varmaörvun seglaðra geymslueininga (t.d. bita á hörðum diskum) [2]. Því er nú leitað nýrra leiða við hönnun tölva. Sumar hugmyndirnar virðast eiga lítið skylt við þær tölvur sem notaðar eru í dag.

Byggja má örsmáar reglulega raðaðar og tengdar einingar með sjálfröðun víxlverkandi sameinda [3] eða örkristalla [2], þ.e. að leyfa náttúrunni að beita sínum lögmálum við leit að hentugustu uppröðun slíks kerfis. Vísindamönnum hjá Hewlett-Packard tókst að framkvæma rökaðgerðir þar sem virka einingin var einfalt lag sjálfraðandi sameinda [3]. Einnig hefur tekist að byggja rökrásir á víxlverkun milli járnseglandi eyja [4]. Þessar aðferðir bjóða hins vegar ekki upp á lausn reikniverkefna sem tölvur nútímans ráða ekki við, enda byggðar á sömu tvíundatækni. Við munum oft vísa til tölva, bita og gista (e. register) af þessu tagi sem “sígildra” (e. classical).

Samhliða eiginleikar skammtatölva (e. quantum parallelism), sem byggja á skammtabitum, ættu hins vegar að gera mönnum kleift að leysa verkefni sem eru ill- eða óleysanleg með sígildum tölvum. Þessu til

skýringar er best að taka dæmi. Segjum að við ætlum að reikna gildi falls í 2^N punktum með rökhliði sem tekur N bita inntak og reiknar fallgildið fyrir gefið inntak. Með sígildri tölvu þarf að reikna fallgildi 2^N sinnum og skrá þau öll niður. Með skammtatölvu og skammtabitum er hins vegar hægt að stilla bitunum haganlega upp (þeir taka samfelld gildi, en ekki “0” og “1” eins og sígildir bitar) þannig að með einni reikniaðgerð innihalda úttak rökhliðsins upplýsingar um öll 2^N fallgildin sem við erum á höttunum eftir. Ef N er t.d. 100 þyrfti í sígilda tilfellinu að reikna fallgildið rúmlega 10^{30} sinnum en aðeins einu sinni á skammtatölvunni! Hins vegar þarf að *nálgast* allar þessar upplýsingar eftir aðgerðina á skammtabitana. Það er ekki einfalt mál, og ekki hægt að heimfæra aðferðir sígildra reikninga yfir á skammtareikninga. Algrím fyrir skammtatölvur hafa verið reynd fyrir minni verkefni, sem flýta lausn ákveðinna tegunda stærri verkefna nógu mikið til að gera þau leysanleg með skammtatölvum þótt þau hafi verið óleysanleg á sígildum tölvum. (Sjá t.d. [5, 6]).

Hugmyndin um skammtatölvur er ekki ný af nálinni en áhugi á henni hefur vaxið gífurlega undanfarin ár. Árið 1981 hélt Richard Feynman fyrirlestur á ráðstefnunni “First Conference on the Physics of Computation” [7], þar sem hann benti á að reikniþörf algríma, sem líkja eiga eftir skammtakerfum, þ.e. að reikna út ástönd þeirra og þróun í tíma, vex sem veldisfall með stærð kerfisins. Hann varpaði fram þeirri hugmynd að sennilega þyrfti skammtakerfi til þess

að herma eftir öðru skammtakerfi. Jafnframt væri aðgerðin að herma eftir öðru skammtakerfi í einhverjum skilningi jafngild því að framkvæma hermireikning, þ.e. því að leysa verkefni sem fyrir sígilda tölvu vex sem veldisfall af stærð kerfisins! Lykilatriði er auðvitað hvernig lesa skal upplýsingar um lokaástandi kerfisins. Nokkrum árum síðar var sýnt hvernig reikna mætti með skammtatölvu, en fram að því var engan veginn ljóst hvort eða hvernig nýta mætti skammtakerfi til reikninga. Einnig var sýnt að skammtatölva getur alltaf hermt eftir sígildri tölvu án þess að verkefnið vaxi sem veldisfall. Með útsjónarsemi má einnig leysa önnur verkefni, sem vaxa sem veldisfall á sígildum tölvum, með skammtatölvum án þess að verkefnið vaxi með þeim hætti.

2. Skammtabitar og skammtahlið

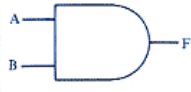



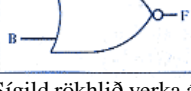
Tölvur nútímans byggja á tvíundatækni. Upplýsingar eru færðar milli eininga og vistaðar sem safn sígildra bita. Bitarnir geta hver um sig tekið annað tveggja gilda sem við munum hér kalla 0 og 1. Meðhöndlun gagnanna fer fram með smárum sem opna eða loka fyrir straumrás með spennu sem er lögð á stýrihlið smárans (e. gate). Samtengdir smárir mynda rökhlið sem síðan eru tengd saman til að mynda rökrásir.

Grunneining skammtatölvu er skammtabiti (e. quantum bit, eða qubit). Skammtabiti er skammtakerfi með tvö aðgreinanleg eiginástönd. Sem dæmi má nefna spunastöðu rafeindar í skammtapunkti, rafeindaástönd tveggja orkulægstu spunasvigrúma frumeindar eða segulflæðiþéttleiki gegnum ofurleiðandi lykkju. Ennfremur gerum við ráð fyrir að við getum einangrað umrædd ástönd nægilega vel frá öðrum ástöndum og ytra umhverfi til að líta megi á þau sem einangrað tveggja þrepa kerfi. Ef við táknum ástöndin með vigrunum $|0\rangle$ og $|1\rangle$ getum við lýst stöðu kerfisins sem línulegri samantekt

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle . \quad (1)$$

Stuðlarnir α og β geta tekið tvíinntölugildi og kallast líkindavísar. Talað er um að ástand sé normað ef um það gildir $|\alpha|^2 + |\beta|^2 = 1$ og þá segjum við að $|\alpha|^2$ gefi líkindin á að mæling sýni kerfið í ástandi $|0\rangle$ og $|\beta|^2$ líkurnar á að kerfið mælist í ástandi $|1\rangle$.

Þar sem stuðlarnir geta tekið samfelld gildi getur skammtabiti tekið óendanlega margar stöður í tvívíðu Hilbertrúmi sem vigrarnir tveir spanna. Þetta er gjörólíkt sígildum bitum, sem hver um sig taka einungis annað tveggja gilda. Því virðist sem skammtabiti

Name	Graphic Symbol	Algebraic Function	Truth Table															
AND		$F = A \cdot B$ or $F = AB$	<table border="1"><thead><tr><th>A</th><th>B</th><th>F</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></tbody></table>	A	B	F	0	0	0	0	1	0	1	0	0	1	1	1
A	B	F																
0	0	0																
0	1	0																
1	0	0																
1	1	1																
OR		$F = A + B$	<table border="1"><thead><tr><th>A</th><th>B</th><th>F</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></tbody></table>	A	B	F	0	0	0	0	1	1	1	0	1	1	1	1
A	B	F																
0	0	0																
0	1	1																
1	0	1																
1	1	1																
NOT		$F = \bar{A}$ or $F = A'$	<table border="1"><thead><tr><th>A</th><th>F</th></tr></thead><tbody><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></tbody></table>	A	F	0	1	1	0									
A	F																	
0	1																	
1	0																	
NAND		$F = (\overline{AB})$	<table border="1"><thead><tr><th>A</th><th>B</th><th>F</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></tbody></table>	A	B	F	0	0	1	0	1	1	1	0	1	1	1	0
A	B	F																
0	0	1																
0	1	1																
1	0	1																
1	1	0																
NOR		$F = \overline{(A+B)}$	<table border="1"><thead><tr><th>A</th><th>B</th><th>F</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></tbody></table>	A	B	F	0	0	1	0	1	0	1	0	0	1	1	0
A	B	F																
0	0	1																
0	1	0																
1	0	0																
1	1	0																

Mynd 1. Sígild rökhlið verka á sígilda bita í nútíma tölvum. Þau taka við inntökunum A og B og skila út niðurstöðunni F. Með NAND hliðinu einu má byggja allar rökrásir og er NAND því kallað almennt hlið (e. universal gate) [8].

geti geymt óendanlegt magn upplýsinga. En hafa þarf í huga að um leið og mæling á sér stað fellur hann í eiginástand mæliaðgerðarinnar. Það er því ekki hægt að nota skammtabita sem óendanlega stórt minni, en samt má nýta þessa eiginleika skammtabitanna til að taka samfelld gildi til að framkvæma samhliða reikninga sem falla síðan í eina niðurstöðu að þeim loknum.

Sígild tölva er safn rökhliða, sem verka á bita sem fluttir eru til og frá með tengivírum. Mynd 1 sýnir nokkur dæmi um sígild hlið og verkun þeirra á bita. Málum er svipað háttáð í skammtatölvum, en þar verka skammtahlið á skammtabita. Til þess að sjá muninn á skammtahliðum og sígildum hliðum er gott að líta á dæmi. Hugsum okkur sígilt hlið sem hefur eitt inntak og eitt úttak. Hliðið þekkir tvær stöður sem við táknum með 0 og 1. Hliðið varpar inntakinu a yfir í úttakið b og hver og ein vörpun inntaksstöðu í úttaksstöðu hefur ákveðin líkindi p_{ab} sem uppfylla $\sum_b p_{ab} = 1$. Dæmi um slíkt sígilt hlið væri NOT hliðið (e. NOT gate) sem breytir 0 í 1 og 1 í 0, þetta má þá tákna með $p_{00} = p_{11} = 0$ og $p_{01} = p_{10} = 1$ eða sem fylki

$$\text{NOT} = \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2)$$

sem verkar á dálkvigur sem tákna inntakið,

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ eða } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (3)$$

sem tákna ástöndin 0 og 1.

Tvö raðtengd NOT hlið víxla inntakinu með fyrri hliðinu og víxla síðan tilbaka í upphafsstöðuna með seinna hliðinu. Þetta má tákna sem eitt hlið sem hefur vörpunina $p_{00} = p_{11} = 1$ og $p_{01} = p_{10} = 0$, sem hefur sama úttak og inntak. Í fylkjaformi þýðir þetta margföldun

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \quad (4)$$

Sígilda NOT hliðið á sér hliðstæðu meðal skammtahliða sem nefnist skammta NOT hlið. Það breytir $|0\rangle$ inntaki í $|1\rangle$ úttak, og $|1\rangle$ inntaki í $|0\rangle$ úttak. Ef við táknum ástöndin tvö með dálkvigurum líkt og í jöfnu (3) getum við notað sama fylki til tákna vörpunina (jafna (2)). Athugið að nú gilda ekki sömu skilyrði um fylkjastökin og í sígilda tilfellinu. Nú er eðlilegt að krefjast þess að *normun ástandsins* haldist óbreytt þótt hliðið verki á það (þ.e. skammtabitann). Þetta krefst þess að verkun hliðsins sé einoka aðgerð. Því gildir almennt um skammtahlið að fylkin sem lýsa þeim eru einoka ($A^\dagger A = 1$ ef A er fylki sem lýsir skammtahliði), en það er vissulega uppfyllt í tilfelli NOT aðgerðarinnar.

Nú er hægt að hugsa sér flóknari skammtahlið sem gefa úttak sem er línuleg samantekt eiginástanda. Dæmi um slíkt hlið er $\sqrt{\text{NOT}}$ hliðið

$$\begin{aligned} \sqrt{\text{NOT}} &= \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} . \end{aligned} \quad (5)$$

Nafnið tengist því að tvö raðtengd hlið af þessu tagi jafngilda einu skammta NOT hliði, eins og sést með einfaldri reikniæfingu.

Annað algengt hlið er Hadamard hliðið

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (6)$$

(sem oft er *ranglega* nefnt $\sqrt{\text{NOT}}$), en það breytir

$$|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (7)$$

$$|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (8)$$

og hefur rauntölu–stuðla. Mæling þessara úttaka í grunni $|0\rangle$ og $|1\rangle$ gefur slembiniðurstöðu, þ.e. jafnmiklar líkur eru á að mælingin gefi ástandið $|0\rangle$ og ástandið $|1\rangle$. Við mælinguna fellur skammtabitinn í eiginástand, en ef hann er látinn óáreittur helst hann í línulegri samantekt eiginástandanna. Sígildir bitar hafa ekki þennan eiginleika, þeir geta einungis tekið annað tveggja gilda hverju sinni. Þó notuð sé samskonar fylkjaframsetning er túlkunin ólík í sígilda og skammtatilfellinu. Úttök skammtahliða eru líkindavísar skammtabita meðan úttök sígildu framsetningarinnar gefa ástand bita.

Sem dæmi um samhliðaeiginleika skammtatölva skulum við líta á samanburð tveggja talna. Skoðum rökhlíð, með eitt inntak og eitt úttak, sem samsvarar tvíundarfallinu $f : \{0, 1\} \rightarrow \{0, 1\}$. Verkefnið felst í því að athuga hvort fallið er fasti.

$$f(0) \stackrel{?}{=} f(1) . \quad (9)$$

Með sígildri tölvu væri líkleg röð aðgerða eitthvað á þessa leið,

- reikna $f(0)$ og setja í minni,
- reikna $f(1)$ og setja í minni,
- athuga hvort $f(0)$ sé jafnt og $f(1)$ og setja niðurstöðuna í minni.

Hér þarf því að reikna fallgildið tvisvar til þess að geta sagt hvort útkoman fyrir 0 er jöfn þeirri fyrir 1. Til þess að nýta samhliðaeiginleika skammtareikninga tökum við dálítið öðruvísi á málinu. Við byrjum á að setja inntakið í línulega samantekt sem er summa eða mismunur ástandanna $|0\rangle$ og $|1\rangle$, og beitem Hadamard hliði til þess. Það setur innbitann í ástand $|0\rangle \pm |1\rangle$ þar sem formerkið ræðst af byrjunarstöðu. Gerum síðan ráð fyrir (án þess að hafa áhyggjur af því hér hvernig það er útfært) að við höfum rökhlíð sem jafngildir einoka aðgerð sem veldur fasahliðrun

$$\begin{aligned} \mathcal{F} &= \begin{pmatrix} e^{i\pi f(0)} & 0 \\ 0 & e^{i\pi f(1)} \end{pmatrix} \\ &= \begin{pmatrix} (-1)^{f(0)} & 0 \\ 0 & (-1)^{f(1)} \end{pmatrix} . \end{aligned} \quad (10)$$

Síðan beitem við Hadamard hliðinu aftur. Heildarvörpunin er þá

$$H\mathcal{F}H \quad (11)$$

og við skoðum hvað verður um inntaksástandið $|0\rangle$.

$$\begin{aligned} |0\rangle &\xrightarrow{H} [|0\rangle + |1\rangle] \\ &\xrightarrow{\mathcal{F}} \left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \right] \\ &\xrightarrow{H} \left[(-1)^{f(0)}(|0\rangle + |1\rangle) \right. \\ &\quad \left. + (-1)^{f(1)}(|0\rangle - |1\rangle) \right], \quad (12) \end{aligned}$$

burt séð frá föstum sem margfalda heildarástandið. Svipað á við um inntakið $|1\rangle$ nema þar munar einu formerki. Við endum þannig með hreint $|0\rangle$ ástand ef $f(0) = f(1)$, en hreint $|1\rangle$ ástand ef $f(0) \neq f(1)$. Stöðu úttaksbitans getum við mælt og þar með fengið niðurstöðu með því að reikna fallgildið aðeins einu sinni. Þetta algrím er kennt við Duetsh [7, 9]. Aðferðina er einfalt að útvíkka og heimfæra á fall sem verkar á N bita inntak. Í sígilda tilfellinu eru 2^N möguleg gildi á inntaki og þarf jafnmarga útreikninga til þess að þekkja öll fallgildin. Einfalt er að sýna að formlega má setja skammtabita í línulega samantekt eiginástanda og með einni aðgerð fá skammtaástand sem inniheldur upplýsingar um öll fallgildin [5, 6].

3. Skammtatölvur; hagnýting og hindranir

Í stuttu máli má segja að skammtatölvur séu safn samtengdra skammtabita sem stillt er í ákveðið upphafsástand. Einoka aðgerðir verka á bitana og safnið þróast í tíma og lokaástandið er lesið. Lesturinn fer fram með *mælingu* á skammtakerfinu, þ.a. niðurstaðan er líkindadreifing. Dreifingin inniheldur upplýsingar um lausn verkefnis sem við getum ekki látið okkur dreyma um að leysa með sígildri tölvu.

Vandamál eru gjarnan flokkuð eftir því hversu hratt lausnartíminn (eða aðgerðafjöldinn) vex með fjölda svigrúmsvídda. Ef aðgerðafjöldinn s fyrir eitt-hvert gefið algrím vex eins og margliða í fjölda svigrúmsvídda, þ.e. samkvæmt $s = a_0 + a_1L + a_2L^2 + \dots + a_nL^n$ þar sem L er fjöldi inntaksbita og n er stig margliðunnar, er sagt að algrímið falli í flokk P (frá e. polynomial). Verkefni af þessu tagi eru sögð “leysanleg”, þótt auðvitað sé það afstætt! Ef skrefafjöldinn vex sem veldisfall fellur algrímið í flokk “erfiðra verkefna” og eru þau svo til óleysanleg fyrir mjög stór inntök. Sem dæmi um þess háttar verkefni er hermun á skammtakerfi, leitun í gagnagrunni og talnaþáttun.

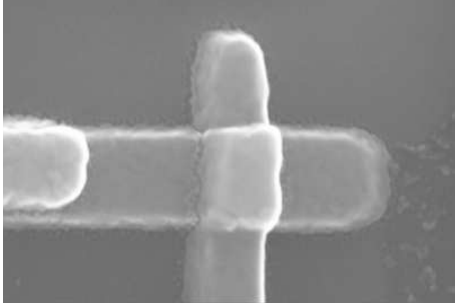
Hagkvæmasta þekkta algrímið til þáttunar talna með fleiri en 100 tölustafi kallast “general number field

sieve” og krefst sú aðferð $s \sim \exp((\frac{64}{9}n)^{1/3}(\ln n)^{2/3})$ reikniðgerða fyrir n stafa tölu [10]. Þar sem þáttunarverkefnið reynist svo erfitt fyrir stórar tölur er það notað í lykilorð. Notandi velur sér lykilorð sem tákna t.d. einhverjar tvær stórar prímtölur. Prímtölurnar eru margfaldaðar saman og úr verður tala sem allir notendur geta nálgast. Til að komast að lykilorðinu þyrftu aðrir misheiðarlegir notendur að komast yfir töluna og þátta hana í prímpætti, nokkuð sem er órænhæft að gera á sígildum tölvum *ef tölurnar sem um ræðir eru valdar nógu stórar*. Þáttun stórra talna er dæmi um verkefni þar sem skammtatölvur gætu komið að góðum notum. Peter Shor setti fram algrím fyrir skammtatölvu sem gæti þáttað n -stafa tölur í $s \sim (\ln(n))^3$ skrefum [11].

Það er þó hægara sagt en gert að byggja skammtatölvuna til þess að framkvæma alla þessa reikninga. Þar til fyrir nokkrum árum síðan höfðu menn ekki skýra mynd af því hvaða kröfur þyrfti að gera til skammtakerfis sem hægt væri að nota í skammtatölvu. Það var ekki fyrir en árið 2000 að DiVincenzo setti fram 5 skilyrði sem (hagnýt) skammtatölva þarf að uppfylla [12]:

- Hún verður að vera *skalanlegt* eðlisfræðilegt kerfi með vel skilgreindum skammtabitum.
- Upphafsstaða allra skammtabita þarf að vera stillanleg.
- Kerfið verður að vera skammtafræðilega samfasa (e. coherent) mun lengur en tímann sem tekur að framkvæma eina aðgerð.
- Þarf að innihalda nokkur mikilvægustu skammtahliðin til aðgerða á skammtabitum.
- Staða allra skammtabita þarf að vera mælanleg að loknum reikningum.

Með skalanleika er hér átt við að með fleiri skammtabitum verði tölvan fær um að fást við stærri reikniverkefni. Sumar þessara krafna virðast einfaldar við fyrstu sýn, en enginn hægðarleikur er að uppfylla þær allar í einu og sama kerfinu. Miklar framfarir hafa orðið á síðastu 5 árum og við færumst óðum nær því að geta smíðað frumstæðar skammtatölvur. Menn hafa leitað meðal ýmissa skammtakerfa að hentugu skalanlegu kerfi, sem gæti uppfyllt flest eða öll hin skilyrðin líka. Erfiðasti hjallinn í flestum kerfum er stuttur samfasatími (e. coherence time), en $1 \mu s$ hefur þó náðst. Takist ekki að halda ástandinu samfasa týnast upplýsingar og reikniðgerðin mistekst.

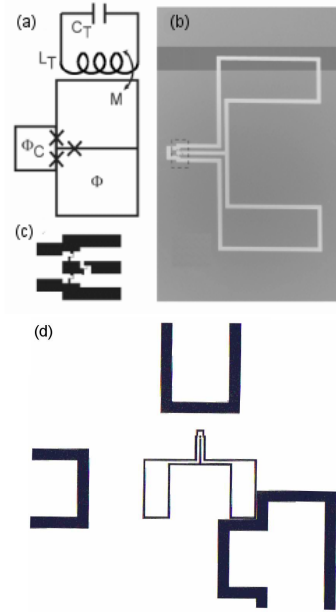


Mynd 2. 200×200 nm Al/Al₂O₃/Al Josephson-skeyti.

4. Segulflæðisskammtabiti

Sá flokkur skammtakerfa sem mestar vonir eru bundnar við og vel hefur orðið ágennt með, byggir á rásum sem innihalda Josephson-skeyti. Josephson-skeyti eru tveir ofurleiðarar sem eru aðskildir með þunnu einangrandi lagi sem Cooperpör geta smogið í gegnum ef þannig ber við. Dæmigerð Josephson-skeyti sjást á mynd 2). Þessi kerfi eru flokkuð eftir hlutfalli rýmdarorku (e. charging energy), $E_C = (2e)^2/2C$ þar sem C er rýmd Josephson-skeytanna, og Josephson-orku $E_J = I_c\Phi_0/2\pi$ þar sem I_c er markstraumur ofurleiðaranna og $\Phi_0 = h/2e$ er segulflæðisskammtur (sjá [13]). Við höfum mestan áhuga á tilfallinu $E_J \gg E_C$, en þá er skammtabitinn kallaður segulflæðisskammtabiti (e. flux based qubit, sjá [13, 14, 15]). Þessi flokkur skammtakerfa hefur þann kost að með stórsæjum breytum, t.d. rýmd, spani og rafstraumi, má hafa áhrif á Hamiltonvirkja kerfisins með mikilli nákvæmni. Þannig má breyta sætni orkustiga, stilla skammtabitann í vel þekkt ástand og verka svo á hann með einoka virkja með stórsæjum breytum.

Undanfarið ár höfum við verið í samstarfi við rannsóknahóp hjá IBM í New York sem er að vinna með segulflæðisskammtabita. Á mynd 3 er sýnd teikning af skammtabitanum ásamt fæðilínunum (e. transmission line) sem notaðar eru til þess að breyta og/eða lesa ástand bitans. Breiðu línurnar eru fæðilínur en bitinn sjálfur hefur tvær stórar lykkjur sem víxlverka stærðar sinnar vegna sterklega við fæðilínurnar. Straumur í fæðilínunni neðst til hægri veldur segulflæði Φ í hægri lykkju bitans, en fæðilínan til vinstri er látin sveiflast á fastri tíðni til þess að stablilisera bitann. Efst í myndinni er önnur fæðilína sem víxlvekar veikar við “hjarta” bitans, þ.e. litlu lykkjuna sem inniheldur tvö Josephson skeyti, og veldur segulflæðinu Φ_c í



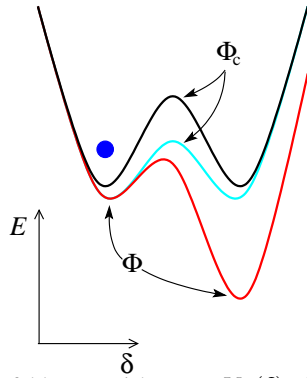
Mynd 3. (a) Teikning af skammtabita IBM og sveifilslíkani fæðilínu. Krossar tákna Josephson skeyti. (b) Rafeindasmásjármynd af skammtabitanum. Hann er um 0.5 mm að lengd og 0.4 mm á breidd. (c) Gríma sem notuð er til að rækta Josephson skeytin. Hvert skeyti er 250×250 nm² að flatarmáli. (d) Teikning af skammtabitanum ásamt fæðilínunum (sjá mynd 5) sem víxlverka við skammtabitann með segulflæði. Efsta fæðilínan og sú neðst til hægri sjá um stýringu og sú síðarnefnda einnig um aflestur. Allar fæðilínurnar eru úr níóbíum (Nb) sem ofurleiðir við 9.3 K, en skammtabitinn er gerður úr áli (Al) sem verður ofurleiðandi við 1.18 K.

henni. Straumur rétt/rangisælis í litlu lykkjunni skilgreinir skammtaástandin tvö sem byggt er á.

Nákvæm lýsing á Hamiltonvirkja kerfisins (skammtabitans og nánasta umhverfis, þ.e. fæðilínanna) er allviðamikil verk [16]. Við látum nægja hér að segja að Hamiltonvirkinn er eins og fyrir eind með massa sem ákvarðast af rýmd kerfisins, í fjórvíðu mætti. Í þessu stóra fasarúmi er til svæði þar sem líta má á mættið V_Q sem tvöfaldan mættisbrunn í einni vídd sem fall af fasabreytu sem við köllum δ

$$V_Q(\delta, t) = -h_2(t)\delta^2 + h_4\delta^4 + a(t)\delta \quad (13)$$

Hér er t tími. Mættinu má stjórna með Φ og Φ_c . Φ stýrir orkumismun mættisbrunnanna í gegnum stærðina a og Φ_c stýrir hæð þröskuldsins á milli þeirra með stærðinni h_2 (sjá mynd 4). h_2 getur tekið bæði jákvæð



Mynd 4. Tvöfaldir mættisbrunnur $V_Q(\delta)$. Orkumismunur brunnanna stjórnast af Φ . Hæð mættisþröskuldsins er stjórnað með Φ_c . Bylgjufall “eindarinnar” lýsir ástandi bitans. Ef þröskuldurinn er nógu lágur lekur bylgjufallið á milli brunnna og er lýst sem línulegri samantekt eiginástanda hvors brunns fyrir sig.

og neikvæð gildi þannig að tvöfalda mættisbrunninum má breyta í einfaldan brunn. Hamiltonvirki kerfisins er í góðri nálgun

$$H = \frac{e^2 Q^2}{2C_Q} + V_Q(\delta, t) + \frac{e^2 q^2}{2C_T} + \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{\varphi^2}{L_T} + \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{M\delta\varphi}{L_Q L_T}. \quad (14)$$

Hér eru fyrstu tveir liðirnir Hamiltonvirki skammtabitans, næstu tveir eru Hamiltonvirki fyrir sveifils nálgun á fæðilínunum og síðasti liðurinn lýsir línulegri víxlverkun milli þessara tveggja hluta kerfisins. Q og q eru hleðsluvirkjar fyrir skammtabitann og fæðilínurnar og leika hér hlutverk skriðþungavirkja, ef við lítum á fasana ϕ og δ sem staðarvirkja: $[\varphi, q] = [\delta, Q] = i$. C_Q og L_Q eru rýmd og span Josephson–skeytanna sem í okkar tilviki eru $C_Q \approx 50$ fF og $L_Q \approx 640$ pH. C_T og L_T eru sambærilegar stærðir fyrir fæðilínurnar. M er gagnspan milli fæðilínanna og skammtabitans. (Til nánari glöggvunar er bent á [15] og [16].) Jöfnur (13) og (14) sýna skýrt að breyta má mættinu V_Q og einstökum liðum Hamilton virkjans og stjórna þannig skammtaástandi bitans með stórsæum stærðum eins og rýmd og spani fæðilínanna eða skammtabitans eða straumum í fæðilínunum sem valda Φ og Φ_c .

IBM hefur undanfarið ár notað skammtabitann sem sýndur er á mynd 3. Nokkur vandamál hafa komið upp með þá útfærslu sem lýst var hér að fram-

an. Erfiðara reyndist að stýra honum og setja í upphafsástand en ætla mátti af hermireikningum. Helstu vandamálín eru talin vera víxlverkun við umhverfissuð og að stýrimerkinn dreifa segulflæði of mikið. Því hönnuðum við nýjan bita og fæðilínur. Vonir standa til að nýja hönnunin bjóði upp á betri stjórnun og verði ekki eins næm fyrir umhverfissuði.

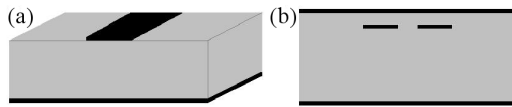
Fjögur atriði voru höfð að leiðarljósi við endurbætur skammtabitans:

- Gagnspan á milli bita og fæðilína verði takmarkað við vel valin svæði og hverfandi annars staðar.
- Útstytting ytra suðs með samhverfu í byggingu bitans.
- Lögum bitans bjóði upp á möguleika á “tengingu” við aðliggjandi bita svo þeir geti víxlverkað þegar við á.
- Lögum bitans gefi hermitíðni sem er miklu hærri en “vinnutíðni” bitans, sem er innan við 10 GHz.

Fæðilínurnar umhverfis skammtabitann á mynd 3 eru svokallaðar “microstrip” línur (mynd 5). Þær flytja merki til og frá bitanum með gagnspani. Straumur í fæðilínunum spanar upp straum í lokuðum lykkjum skammtabitans og öfugt. Þannig má framkvæma lestur og stýra skammtabitannum án þess að hann sé í beinni snertingu við aðra leiðara. Skammtareikingarnir eru gífurlega viðkvæmir fyrir suði og því verður að hanna bæði bitann og fæðilínurnar þannig að merkið komist óhindrað leiðar sinnar á meðan slembisuði og óæskilegu gagnspani er haldið í lágmarki. Víxlverkun skammtabitans við annað umhverfi en fæðilínurnar stýttir samfasatímamann verulega og getur gert hann ónothæfann.

Könnun á kostum og göllum nokkurra tegunda fæðilína sýndi að nokkuð óhefðbundin planfæðilína, “dual asymmetric coplanar stripline”, hentar best. Slík lína er sýnd á mynd 5b. Þessi tegund línu er hentug því auðvelt er að smækka hana en halda kennivíðnámínu 50Ω . Einnig er einfalt að skammhleypa línunni til að tryggja að straumhámark verði þar sem línunni liggur að skammtabitannum. Síðast en ekki síst hefur þessi gerð línu hæfilega langseilið segulsvið, sem þýðir að auðvelt er að koma línunni nógu nálægt bitanum til að víxlverkun verði sterk en hröð dvínun dregur úr víxlverkun við aðra hluta rásarinnar.

Endurhönnun skammtabitans er sýnd á mynd 6. Fæðilínunum (grannir fingur ofantil) hefur fjölgað og gefa nú tók á bæði dc og pásuáðri stýringu á Φ og



Mynd 5. (a) Microstrip fæðilína. Leiðarinn og jarðplanið (svart) eru $0.2 \mu\text{m}$ þykkir Nb ofurleiðarar. Á milli þeirra er um $60 \mu\text{m}$ þykkt kísillag (Si). Leiðarinn er $50 \mu\text{m}$ breiður. (b) Þverskurður planfæðilínu (dual asymmetric planar stripline) þar sem tveir leiðarar liggja á milli jarðplana, annar leiðarinn er jarðtengdur. Leiðararnir og jarðplönin eru $0.2 \mu\text{m}$ þykkir Nb ofurleiðarar. Leiðararnir eru $5 \mu\text{m}$ breiðir.

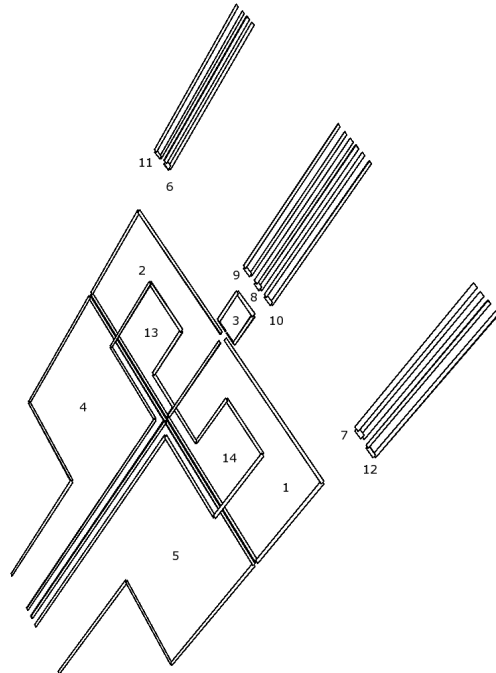
Φ_c . Lestur bitans fer fram með tveimur stórum leiðurum (númer 4 og 5) sem liggja alveg upp að bitanum. Bitinn sjálfur hefur lítið breyst (lykkjur 1 til 3). Bitinn og línurnar eru samhverf um ás eftir miðjunni, svo ytra suð, sem allur bitinn sér, styttest út. Fæðilínur 13 og 14 eru í plani sem er $1 \mu\text{m}$ ofar en aðrar rásir og eru ætlaðar til tengingar við aðliggjandi skammtabita.

Lykkjurnar hafa sjálfspan L_{nn} og eiginrýmd C_{nn} ásamt gagnspani M_{nm} og rýmd C_{nm} til annarra lykkja. Sjálfspan og eiginrýmd í lykkjum skammtabitans ákvarða eigintíðni rásarinnar $\omega_r = 1/\sqrt{C_{nn}L_{nn}}$. Tryggja þarf að eigintíðnin sé miklu hærri en tíðni segulflæðispúlsanna sem örva skammtabitann.

5. Framtíðarhorfur

Fyrir nokkrum árum tókst vísindamönnum frá Stanford háskóla og IBM að nota algrím Shor's til að þátta töluna 15 [17]. Svarið $3 \times 5 = 15$ kemur engum á óvart, en hér var samt um mikilvægan áfanga að ræða. Reikningarnir voru framkvæmdir á “tölvum” í vökvalausn! Skammtatölvan var sameind með 7 spuna, þar sem hver spuni er skammtabiti. Með NMR mælingum (e. nuclear magnetic resonance) og seglum var spununum stillt upp í upphafsástand og líkindadreifing þeirra mæld eftir viðeigandi aðgerðir. Aðferðin jafngildir því að taka meðaltal yfir marga eins reikninga, þar sem hver sameind er í raun tölva, en til þess að fá nógu stórt merki í NMR mælingu þurfti að mæla safn sameinda. Þessi tilraun varð til þess að áhugi á skammtareikningum margfaldaðist á skömmum tíma.

NMR aðferðin er ekki líkleg til að leiða til stórra skammtatölva, vegna þess að flóknari sameindir þarf til þess að fjölga skammtabitanum, merkisstyrkur fellur sem veldisfall með fjölda spuna, og ekki er hægt að stilla styrk spuna–spuna víxverkunarinnar [6]. Þess



Mynd 6. Endurhönnun skammtabita og fæðilína. Lykkjur 1 til 3 mynda skammtabitann. Fingurnir fyrir ofan bitann (6 til 12) eru fæðilínur sem stjórna straumum í bitalykkjunum. Sumir fingranna flytja DC straum en aðrir flytja 1.5 GHz straumpúlsa. Lykkjur 4 og 5 eru til aflestrar og lykkjur 13 og 14 eru til tengingar við næstu skammtabita og liggja þær í plani sem er um $1 \mu\text{m}$ fyrir ofan aðrar rásir.

vegna er leitað að öðrum kerfum sem uppfylla skilyrði DiVincenzo. Þar koma ofurleiðandi skammtakerfi sterklega til greina. Ekki verður annað séð en að skammtabitinn sem fjallað er um í þessari grein sé vel fallinn til skölunar, en ná þarf betri tókum á stýringu hans. Einnig þarf að skilja betur uppruna suðs sem truflar skammtabitann og finna mótvægisáðgerðir.

Skammtareikningar eru ný leið til að framkvæma reikninga og eru þeir töluvert frábrugðnir tvíundareikningum. Ekki eru enn komin fram mörg algrím sem leyfa skammtatölvum að leysa verkefni betur en gert er með sígildum tölvum. Fleiri algríma er að vænta í framtíðinni, enda eru menn rétt að byrja að átta sig á því hvernig á að nota skammtatölvur til reikninga og hvernig best er að nýta skammtabita sem taka samfelld ástönd — nema þegar mæling er framkvæmd á þeim!

Hér hefur mest verið horft til notkunar skammtatölva til þess að leysa verkefni sem eru óleysanleg

með sígildum tölum. Sá eiginleiki skammtatölva að geta hermt eftir öðrum skammtakerfum er ekki síður mikilvægur. Nú þegar er unnt að herma eftir einföldum frumeindum og jafnvel sameindum. Vonandi verður seinna unnt að herma eftir fjöleindakerfum. Jafnvel þó svo fari að aldrei takist að byggja skammtatölvu er dýpri skilningur á grundvallar skammtafræði mikilvægur ávinningur af rannsóknum á þessu sviði, skilningur sem nýtist á mörgum öðrum sviðum. Sem dæmi má nefna að í þeim kerfum sem eru til skoðunar sem frumeiningar skammtatölva hafa þegar sést Rabi-sveiflur og Ramsey-bylgjuvixlmynstur. Einnig má vænta að þessi kerfi verði notuð til þess að skera úr um mikilvæg deiluefni innan skammtafræðinnar.

Þakkir

Höfundar þakka Dr. R.H. Koch fyrir samstarfið. Verkefnið var styrkt af Rannsóknasjóði Vísinda- og Tækniráðs.

Heimildir

- [1] J. Guðmundsson, “Moore’s law forever and ever: The advent of nanoelectronics,” *Technology in Society—Society in Technology*, p. 201, 2005.
- [2] S. Ingvarsson, “Magnetic nanoparticles in composite materials and devices,” *Technology in Society—Society in Technology*, p. 217, 2005.
- [3] C.P. Collier, E.W. Wong, M. Belohradsky, F.M. Raymo, J.F. Stoddart, P.J. Kuekes, R.S. Williams, and J.R. Heath, “Electronically configurable molecular-based logic gates,” *Science*, **285**, p. 391, 1999.
- [4] A. Imre, G. Csaba, L. Ji, A. Orlov, G.H. Bernstein, and W. Porod, “Majority logic gate for magnetic quantum-dot cellular automata,” *Science*, **311**, p. 205, 2006.
- [5] J. Preskill, “Lecture notes for physics 219: Quantum information and computation,” 1998. <http://www.theory.caltech.edu/people/preskill/ph219/#lecture>.
- [6] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, United Kingdom: Cambridge University Press, 2000.
- [7] D. Deutsch, A. Ekert, and R. Lupacchini, “Machines, logic and quantum physics,” 1999. <http://xxx.lanl.gov/abs/math.HO/9911150>.
- [8] A. Clements, *The Principles of Computer Hardware*. Oxford: Oxford University Press, 2000.
- [9] D. Deutsch, “Quantum theory, the church-turing principle and the universal quantum computer,” *Proceedings of the Royal Society of London A*, **400**, pp. 97–117, 1985.
- [10] “General number field sieve,” www.wikipedia.org.
- [11] P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1996. <http://arxiv.org/abs/quant-ph/9508027>.
- [12] D. P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschritte Der Physik*, **48**, p. 771, 2000. <http://arxiv.org/abs/quant-ph/0002077>.
- [13] J.Q. You and F. Nori, “Superconducting circuits and quantum information,” *Physics Today*, **58**, no. 11, p. 42, 2005. <http://arxiv.org/abs/quant-ph/0601121>.
- [14] I. Chiorescu, Y. Nakamura, C.J.P.M. Harmans, and J.E. Mooij, “Coherent quantum dynamics of a superconducting flux qubit,” *Science*, **299**, p. 1869, 2003.
- [15] R.H. Koch, J.R. Rozen, G.A. Keefe, F.M. Milliken, C.C. Tsuei, J.R. Kirtley, and D.P. DiVincenzo, “Low-bandwidth control scheme for an oscillator stabilized Josephson qubit,” 2004. <http://arxiv.org/abs/cond-mat/0411380>.
- [16] G. Burkard, R.H. Koch, and D.P. DiVincenzo, “Multilevel quantum description of decoherence in superconducting qubits,” *Phys. Rev. B* **69**, 064503, 2004.
- [17] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, “Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance,” *Nature*, **414**, p. 883, 2001.

Summary: In this article we give a brief introduction to qubits, quantum gates, and quantum computation. We discuss some problems that are solved more efficiently with quantum than classical computers. We then turn to hardware considerations: How to build a quantum computer starting with the qubits. We focus on a specific solid state implementation of a superconducting flux qubit that is being studied at IBM in Yorktown Heights, NY and discusses some suggested improvements to the design.

Um höfundana: Tryggvi Ingason stundar nám í rafmagnsverkfræði við Háskóla Íslands.

Snorri Ingvarsson er dósent við eðlisfræðiskor Háskóla Íslands.

Raunvísindastofnun Háskólans
Dunhaga 3, IS-107 Reykjavík
tryggvii@hi.is

Móttékin: 23. febrúar 2006