КВАНТНИ РАЧУНАРИ

М. Дугић, Д. Огњановић***

***Институт за физику, Природно-математички факултет, Крагујевац, 34 000 Крагујевац**
****Прва техничка школа, Крагујевац, 34 000 Крагујевац**

Абстракт: Дат је кратак пресек кроз истраживања која се тичу квантних рачунара, са нагласком на физичке основе.

1. КВАНТНА ТЕХНОЛОГИЈА

Технологија XIX века имала је термодинамику као физичку основу. Технологијама XX века доминирале су информатичке технологије са физичком електроником као физичком основом. Технологије XXI века биће, по свему судећи, *квантне технологије*, то јест очекује се да ће физичке основе будуће технологије чинити принципи и закони квантне физике (тј. квантне механике) [1].

Савремени технолошки методи и процедуре бележе продор на микроскопске димензије (испод $1\mu m$). Даљи тренд у овом смислу неминовно намеће потребу примене закона квантне механике за процесе у којима заправо учествују мале групе, па чак *и појединачне квантне честице* (елементарне честице, атоми или молекули). Тако се указују обриси будуће технологије која је већ почела кроз примену тзв. STM (scanning tunneling microscopy) технологије, нанотехнологије (у питању су димензије реда величине $1nm$), квантне оптике и оптоелектронике, физике материјала, а посебно кроз истраживања везана за развој квантне информатике и квантног рачунарства.

Наш задатак је да овде, у кратким цртама, представимо основе квантног рачунања. Више детаља у овом смислу се може наћи на WEB страни посвећеној *Квантном рачунању*, у оквиру WEB презентације Института за физику ПМФ-а у Крагујевцу, на адресама:

http://fizika.pmf.kg.ac.yu
http://www.pmf.kg.ac.yu[1]

2. ФИЗИЧКЕ ОСНОВЕ КВАНТНОГ РАЧУНАЊА

Енглески израз *computing* значи рачунање (израчунавање). Математички, свако рачунање је пресликавање. Физички, рачунање значи промену (трансформацију) стања рачунске машине (то јест рачунара). Класично рачунање (помоћу дигиталних рачунара) представља учинак реда-величине 10^{10} честица. Квантно рачунање је процес који се оснива на учинку (кроз промену стања) *и појединачних* (квантних) честица.

Квантно рачунање се заснива на примени стандардних квантних "парадокса":

♣ Квантна неодређеност (што је физички садржај релација неодређености)

♣ Квантна сплетеност (квантна несепарабилност, entanglement).

[1] Ово је адреса презентације ПМФ-а у Крагујевцу. Зато потражити страну посвећену Институту за физику, па онда ићи на линк *Физика детаљно*, па онда на *Истраживање*.

Дакле, ради се о коришћењу особина квантних честица (фотона, атома или молекула), које немају класичног аналогона. Да се задржимо на разјашњењу ових појмова.

Квантна неодређеност је последица некомутативности квантних опсервабли. На пример, некомутирање опсервабли положаја и импулса успоставља непостојање трајекторије електрона у атому--у супротном, знамо, електрон би у вртњи око језгра емитовао електромагнетно зрачење и пао на језгро. Штавише, може се рећи да електрон у атому *нема одређен положај*, чак ни у принципу! Ово је *строг математички резултат*: ако би електрон имао одређен положај, тада би стандардна решења Шредингерове једначине за водоников атом била неупотребљива. Дакле, *квантна неодређеност значи одсуство (непостојање) вредности физичких величина, у принципу*--за разлику од непознавања тих вредности (када оне постоје), што је класична неодређеност (недовољно познавање стања система)--баш као што не постоје ни "трајекторије" замишљених квантних честица у интерференционим експериментима у оптици.

Квантна сплетеност (несепарабилност) је особина сложених (вишечестичних) квантних система. Наиме, за сложене квантне системе постоје стања у којима "подсистеми" *немају одређено (квантно) стање, чак ни у принципу*.

Дакле, *квантна механика познаје две врсте неодређености*: када је познато квантно стање, неке опсервабле немају одређене вредности, чак ни у принципу, као и ситуације за сложене системе када "подсистеми" немају чак ни (квантно) стање--једино целина има одређено стање.

Основни појам квантног рачунања је ***кубит*** (*qubit*), што је скраћеница од енглеске речи чији превод гласи "квантни-бит". Код класичних рачунара "бит" представља пар могућих стања система, $\{0,1\}$. Квантни бит није скуп стања, већ читав дводимензионални простор стања (аналогон спина ½). Геометријски, класични бит представљен је паром тачака на реалној оси, а кубит читавом кружницом (јединичног полупречника) у равни. Наравно, за користан рачунски рад неопходан је велики број кубита, па је, геометријски, простор стања N кубита заправо 2^N-димензионална хиперсфера јединичног полупречника.

У класичном рачунању, стање система (на пример једног бита) је, увек, или 0, или 1. У квантном то није случај: тачке на горе-поменутој сфери представљају, у општем случају, кохерентну суперпозицију (попут интерференције). Тако, на пример, за скуп битова, стање је увек низ типа $|100111010110..\rangle$. Квантномеханички, међутим, могуће су и суперпозиције (аналогон класичне интерференције):

$$|\Psi\rangle = \alpha_1 |01100..\rangle + \alpha_2 |01101..\rangle + .. \equiv \sum_i \alpha_i |i\rangle, \sum_i |\alpha_i|^2 = 1 \qquad (1)$$

које су носиоци квантне неодређености.

Класично, увек је једна од горњих константи α једнака јединици, док су све остале једнаке нули. Тада се класично рачунање може представити као трансформација стања: $V_f |i\rangle = |f(i)\rangle$. Међутим, због (1), квантно рачунање познаје трансформације типа $\hat{U}_f \sum_i \alpha_i |i\rangle = \sum_i \alpha_i |f(i)\rangle$, то јест истовремено (паралелно) процесирање дуж свих класичних рачунских "трајекторија"--што се зове *квантни паралелизам*.

Скуп од N кубита се назива регистром. Наспрам тог регистра налази се и други, док систем од два регистра представља сложени квантни систем који се може наћи у

сплетеним (*entangled*) стањима. ***Коришћење стања типа (1) и сплетених квантних стања је сама физичка основа квантног рачунања***.

ПИТАЊЕ: Како се могу користити квантна неодређеност и сплетеност, с обзиром на чињеницу да се свака активност заснива на добро дефинисаним подацима--дакле неопходна је *макар* класична неодређеност?

ОДГОВОР: Процес ***квантног мерења*** обезбеђује информације о опсерваблама и стањима квантних система, то јест на рачун квантне неодређености и сплетености се *уводе класична* (не)одређеност физичких величина и/или квантних стања процесом мерења.

Отуда, ***<u>општи рецепт у квантном рачунању</u>*** представља комбинацију двеју врста поступака: (а) креацију и контролу квантне неодређености и/или сплетености (засноване на познавању почетног стаља система), и (б) вршење одређене врсте квантних мерења.

Ради стицања одређеног физичког осећаја у овом погледу ево једне илустрације. Размотримо усамљени електрон у некој кутији. Ако га нико "не дира" (дакле: нема ни мерења), тада је положај електрона квантно неодређен. Нека се у тренутку t_1 изврши мерење положаја. Тада ће се електрон појавити у некој тачки A, и за интервал мерења Δt_1 прећи (дуж класично-сличне путање) у неку тачку B. По престанку мерења, електрон поново осваја своју основну-квантну--природу. Нека сада буде поновљено исто мерење у неком тренутку t_2 у интервалу Δt_2; електрон ће прећи "пут" од неке тачке C у тачку D. Сада, и то је поента, у неком случају (дакле, са неком вероватноћом), могуће је да ефективна "брзина" електрона задовољава:

$$\frac{\overline{AD}}{t_2 + \Delta t_2 - t_1} > c \qquad (2)$$

где је c брзина светлости у вакууму. Али ово је експлицитно *забрањено у класичној физици*! Информатички: прелаз из тачке A у D представља комуникацију брже од светлости и последица је непостојања положаја изолованог електрона.

Нажалост, вероватноћа оваквог преноса је врло мала, па се у овом моделу не може користити за ефикасну комуникацију брже од светлости. Ипак, основни задаци квантне информатике и рачунања се своде на избор услова под којима је могуће овакве вероватноће учинити разумно великим, а што аутоматски значи--в. (1)--да друге вероватноће постају мале; то јест, *задаци квантне информатике и рачунања подразумевају "прерасподелу" вероватноћа различитих догађаја, при чему су доминантни они догађаји (мерења) који носе корисне информатичко/рачунске резултате*.

3. ИСТРАЖИВАЊЕ

У складу са горњим "рецептом" развијен је математички модел квантних рачунара; прецизније: *модел универзалних квантних рачунских машина*. "Универзалност" значи да једна таква машина може, са великом вероватноћом, са произвољно малом грешком да обави било који прорачун (тј. математичко пресликавање).

Испоставља се да све што могу да израчунају класични, могу и квантни рачунари[2].

Испоставља се да квантни рачунари могу и много више. На пример, за факторисање броја од 400 цифара, батерији од (реда величине) 100 паралелно процесирајућих класичних рачунара неопходно је 10^{10} година[3]. Једном квантном рачунару је довољно мање од три године. Релативна моћ квантних у односу на класичне рачунаре је отворени задатак теоријског рачунарства, и предмет је обимних истраживања [2].

Треба посебно нагласити: оно што, у принципу, не могу да израчунају класични, у принципу не могу ни квантни рачунари!

Експериментална истраживања значајно заостају за теоријским. Вероватно најозбиљнији модел ***хардвера квантног рачунара*** је следећи: у материјал ултрачистог силицијума ^{30}Si постављени су атоми (или језгра) фосфора P^{31}. *Кубит* је реализован кроз (ефективни) *спин појединачног атома (тј. језгра) фосфора*, и таквих кубитова има до-реда-величине 10^6 -- што представља један регистар. Наспрам њега је други регистар, и све је димензија око $200nm$. Изнад кубитова (тј. појединачних атома) постављене су танке жице--извори електричног и магнетног поља. Манипулација тим пољима над атомским спиновима представља физичку трансформацију стања спина (то јест кубита), то јест део процеса рачунања. Комбинације тих поступака (манипулација) представља процес раунања. Главне препреке у реализацији овог хардвера су техничке природе и тичу се, пре свега, тачности у позиционирању атома, тј. жица-носилаца поља. Оптимистички, за неких 20 година би се могли заобићи ови проблеми и кренути у озбиљнији експериментални рад на пољу квантних рачунара.

Једном направљен, прототип квантних рачунара ће дати одговоре на сва основна питања, укључујући и питање да ли математички модели квантних рачунара, у пракси, уопште раде. Али то је ствар будућности

[1] G.J. Milburn, *Schrodinger Machines: Quantum Technology Reshaping Everyday Reality*, New York, 1997
[2] Видети WEB адресе са стране 1.

[2] Непрекидни интервал се увек може апроксимирати скупом малих интервала – у лимесу тачака.
[3] Уочити да је ово једна десетина процењеног века физичког Свемира.