Квантови компютри: до къде сме стигнали?

Дж. Бененти, Дж. Касати

Квантовата механика оказа изключително влияние – както върху технологиите, така и върху обществото. За да разберем това твърдение е достатъчно да споменем създаването на транзистора – вероятно най-забележителното измежду безброй многото други приложения на квантовата механика. Лесно е да се види също така огромното въздействие на компютрите върху всекидневния живот. Важността на компютрите е толкова голяма, че е подходящо да се каже, че днес ние живеем в информационната ера. Тази информационна революция стана възможна благодарение създаването на транзисторите, т.е. благодарение обединението между науката за компютрите и квантовата физика. Днес това обединение предлага съвършено нови възможности и обещава вълнуващ напредък както във фундаменталната наука, така и в технологичните приложения. Тук ние имаме предвид факта, че квантовата механика може да се използва за обработка и обмен на информация.

Миниатюризацията ни предоставя един интуитивен начин да разберем защо в близкото бъдеще квантовите закони ще станат важни за компютризацията. Растежът на произвеждащата компютри индустрия върви ръка за ръка с намаляването на размерите на интегралните схеми. Тази миниатюризация е необходима за увеличаване на изчислителната мощност, т.е. на броя на операциите с плаваща запетая за секунда (флопс), които може да извърши един компютър. През 50-те години на миналия век компютрите, използващи технология основана на вакуумни радиолампи, можеха да извършват от порядъка на 10^3 операции с плаваща запетая в секунда, докато днес съществуват суперкомпютри, чиято мощност е повече от 10 терафлопса (10^{13} флопса). Както вече отбелязахме, този изключителен растеж на изчислителната мощност стана възможен благодарение на напредъка в миниатюризацията, който може да се опише количествено със закона на Мор. Този закон е резултат от забележителното наблюдение, направено от Гордън Мор през 1965 г.: броят на транзисторите върху един чип на интегрална схема се удвоява всеки 18 – 24 месеца. Този експоненциален растеж не е започнал да се насища и законът на Мор е все още валиден. Понастоящем границата е приблизително 10^8 транзистора на чип и типичният размер на елементите е от порядъка на 100 нанометра. Като екстраполираме закона на Мор може да оценим, че около 2020 година за складиране на 1 бит информация ще е необходим елемент с размерите на атом. Оттук нататък квантовите ефекти неизбежно ще станат определящи.

Може да се очаква обаче, че освен квантовите ефекти, и други фактори може да доведат до нарушаване на закона на Мор. На първо място, има известни икономически съображения. Наистина, цената на съоръженията, които произвеждат чипове, също расте експоненциално с времето. Въпреки това, важно е да се разберат максималните ограничения, налагани от квантовата механика. Дори да успеем да преодолеем икономическите ограничения чрез пробив в технологиите, квантовата физика поставя фундаментални ограничения върху размерите на елементите на интегралните схеми. Първият въпрос, който трябва да се обсъди, е кое е по-подходящо: да се намаляват транзисторите на силициева основа до достигане на техните физически граници, или вместо това да се развиват алтернативни устройства като квантови точки, едноелектронни транзистори или квантови превключватели (?). Обща черта на всички тези устройства е, че всички те са от мащабите на нанометър и следователно при тях квантовите ефекти играят решителна роля.

Дотук ние говорихме за квантови превключватели, които могат да заместят изградените върху силиций транзистори и вероятно да бъдат свързани така, че да изпълняват класическите алгоритми, основани на Булевата логика. От тази гледна точка квантовите ефекти представляват просто неизбежни корекции, които следва да се вземат предвид поради нанометровите размери на елементите. *Един квантов компютър предоставя радикално различно предизвикателство*: целта е да се направи машина, основана на квантовата логика, т.е. машина, която може да обработва информацията и да извършва логически операции в съответствие със законите на квантовата механика.

Квантова логика

Елементарната единица за квантова информация е *кубитът* (квантовият аналог на класическия бит) и един квантов компютър може да се разглежда като една многобитова система. Физически един кубит е система с две нива, подобно на двете състояния на спина на една частица със спин 1/2, на състоянията на вертикална и хоризонтална поляризация на един фотон или на две нива на един атом.

Класическият бит е система, която може да съществува в две различни състояния, които се използват за представяне на 0 и 1, т.е. на отделна двоична цифра. Единствените възможни действия (гейтове) в такава система са тъждественост (0→0, 1→1) и НЕ (0→1, 1→0). За разлика от това един квантов бит (кубит) представлява квантова система с две нива, описвана в двумерно комплексно хилбертово пространство. В това пространство може да се избере двойка нормирани и ортогонални

помежду си квантови състояния, наречени $|0\rangle$ и $|1\rangle$, които представят стойностите 0 и 1 на класическия бит. Тези две състояния представляват основата за пресмятанията. Съгласно с *принципа на суперпозицията*, всяко състояние може да бъде представено във вида:

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

където амплитудите α и β са комплексни числа, удовлетворяващи условието за нормировка $|\alpha|^2 + |\beta|^2 = 1$.

Набор от n кубита е известен като *квантов регистър* с размерност n. Неговата вълнова функция принадлежи на едно 2^n-мерно комплексно хилбертово пространство. Докато състоянието на един n-битов класически компютър се описва в двоични означения чрез едно число $k \in \{1, 2, \ldots, 2^{n-1}\}$,

(2) $$k = k_{n-1}2^{n-1} + \ldots k_1 2 + k_0,$$

където $k_0, k_1, \ldots k_{n-1} \in \{0, 1\}$ са двоични цифри, то състоянието на един n-кубитов квантов компютър е:

(3) $$|\psi\rangle = \sum_{k=0}^{2^n-1} C_k \,|\, k\rangle,$$

където $|\, k\rangle \equiv |\, k_{n-1}\rangle \ldots |\, k_1\rangle |\, k_0\rangle$, а $|k_j\rangle$ е състоянието на j-тия кубит и

$$\sum_{k=0}^{2^n-1} |\, C_k\,|^2 = 1.$$

Равенство (3) демонстрира ясно принципа на суперпозицията: докато в n класически бита може да се запише само едно число k, квантовият n-кубитов регистър може да бъде както в съответното състояние $|k\rangle$, така и в една суперпозиция. Ние обръщаме внимание на факта, че броят на състоянията на базиса в тази суперпозиция може да достигне 2^n, т. е. расте експоненциално с увеличаването на n. Принципът на суперпозицията разкрива нови възможности за изчисления. Когато извършваме пресмятания с класически компютър, различните входни данни изискват отделни действия. За разлика от това, един квантов компютър може да прави едновременно пресмятания с експоненциално растяща входяща информация (?). Тъкмо този огромен паралелизъм е основа за мощта на квантовите компютри.

За разбиране предимствата на квантовите пред класическите компютри е важно също така да се подчертае ролята на *преплитането*. Преплитането е най-вълнуващата и най-противоречаща на интуицията проява на квантовата механика, наблюдавана в сложни квантови системи: то означава наличие на нелокални връзки между

измервания, извършени върху отдалечени една от друга частици. След като две класически системи са взаимодействали, всяка от тях се намира в добре дефинирано индивидуално състояние. За разлика от това, след като две квантови частици са взаимодействали, казано най-общо, те повече не могат да се описват независимо една от друга. Ще бъде налице чисто квантова връзка между две такива частици, независимо от разстоянието, което ги разделя. Примери за дву-кубитови преплетени състояния представляват четирите състояния на т. нар. базис на Бел $|\phi^{\pm}>=\frac{1}{2}(|00>\pm|11>)$ и $|\psi^{\pm}>=\frac{1}{2}(|01>\pm|10>)$. Измерването на състоянието на поляризация на единия кубит незабавно променя състоянието на другия, независимо от разстоянието между тях. В класическата физика няма преплитане. Следователно, за да представим суперпозицията на 2^n нива чрез класически вълни, тези нива трябва да принадлежат на същата система. Наистина, никога не може да се направи суперпозиция от класически състояния на различни системи. По такъв начин, за да се представи *n*-кубитовото състояние (3) чрез класически вълни е необходима единична система с 2^n нива. Ако Δ е типичното разстояние между две съседни енергетични нива, необходимата енергия за пресмятане е $\Delta 2^n$. Следователно количеството физични ресурси, необходими за пресмятането, растат също експоненциално с *n*. За разлика от това, поради преплитането, в квантовата физика една обща суперпозиция от 2^n нива може да бъде представена с помощта на *n* кубита. Следователно в този случай количеството на физичните ресурси (енергията), необходими за пресмятането, растат само линейно с *n*.

В заключение: поради суперпозицията и преплитането един квантов компютър би могъл по принцип да доведе до експоненциална бързина в сравнение с класическите компютри. Следващият въпрос е как да се осъществи един квантов компютър. За целта трябва да сме в състояние да контролираме развитието във времето на много-кубитовото състояние, описващо квантовия компютър. Доколкото връзката с околната среда може да се пренебрегне, това развитие се управлява от уравнението на Шрьодингер. Известно е, че в един класически компютър определен малък брой от елементарни логически гейтове дава възможност за изпълняване на всяко сложно пресмятане. Това е много важно: то означава, че когато сменим задачата, не е необходимо да променяме компютърния хардуеър. За щастие, същото свойство е налице и за квантовия компютър. Оказва се, че всяко унитарно преобразование на много-кубитовата система може да се разложи на унитарни квантови гейтове,

действащи на единичен кубит и един подходящ квантов гейт, действащ на два кубита, например контролирано-НЕ гейт (CNOT). Този дву-кубитен CNOT-гейт се определя както следва: той преобразува |00> в |00> , |01> в |01>, |10> в |11> и |11> в |10>. Както при класическия XOR гейт, гейтът CNOT преобръща състоянието на втория кубит (целевия), ако първият (контролиращ) кубит е в състояние |1> и не прави нищо, ако първият кубит е в състояние |0>. Лесно се вижда, че CNOT може да създава преплетени състояния. Така например, ако приложим CNOT към непреплетеното състояние $\frac{1}{\sqrt{2}}(|0>+|1>)|0>$, получаваме състоянието на Бел $\frac{1}{\sqrt{2}}(|00>+|11>)$.

Квантови алгоритми

Както видяхме, мощността на квантовите компютри се дължи на присъщия им *квантов паралелизъм*, свързан с принципа на суперпозицията. На обикновен език това означава, че квантовият компютър може да обработва едновременно голям брой класически входни данни. Същевременно обаче не е лесно да се получи полезната информация от изходното състояние. Проблемът се дължи на факта, че в известен смисъл тази информация е скрита. Всяко квантово пресмятане приключва с проектиращо (?) измерване в базиса на пресмятането. Резултатът от измерването е по принцип вероятностен и вероятностите за различните резултати се определят от основните принципи на квантовата механика. Съществуват обаче квантови алгоритми, които ефективно извличат полезната информация.

През 1994 г. Питър Шор предложи един квантов алгоритъм, който решава ефективно проблема за първичната факторизация [3]: да се намерят простите множители на едно сложно положително нечетно число N. Това е централен проблем в компютърната наука и се предполага, без да е доказано, че за един класически компютър е трудно да намери простите множители. Алгоритъмът на Шор решава успешно проблема за разлагане на прости множители с $O((n^2 \log n \log\log n))$ елементарни квантови гейта, където $n = \log N$ е броят битове, необходими за кодиране входящата информация N. Следователно този алгоритъм осигурява експоненциално подобряване на скоростта за пресмятане в сравнение с всеки познат класически алгоритъм. Наистина, най-добрият класически алгоритъм, филтъра за полето на числа, изисква $\exp(O(n^{1/3}(\log n)^{2/3}))$ операции. Струва си да се отбележи, че съществуват криптографски системи, например RSA, които днес са широко използвани и които се основават на предположението, че не съществуват ефективни алгоритми за решаване проблема за

разлагане на прости множители. Следователно алгоритъма на Шор, ако се реализира от един голямо мащабен квантов компютър, ще пробие криптографската система RSA.

Разработени са и други квантови алгоритми. В частност, Гроуер показа, че квантовите компютри могат да бъдат полезни също при решаване на проблема за търсене на един белязан обект измежду неструктурирана база данни от $N = 2^n$ обекта [4]. Най-доброто, което можем да направим в случая с един обикновен компютър, е да тръгнем из базата, докато намерим набелязания обект. Това изисква $O(N)$ операции. За разлика обаче, същата задача може да бъде решена от един квантов компютър със само $O(\sqrt{N})$ операции. В този случай печалбата в сравнение с класическите компютри е квадратична.

Един трети съществен клас квантови алгоритми се отнася до симулиране на физични системи. Добре известно е, че симулирането на квантовия многочастичен проблем с класически компютър е трудна задача, тъй като размерността на Хилбертовото пространство расте експоненциално с увеличаване броя на частиците. Например, ако искаме да симулираме верига от n частици със спин ½, размерността на Хилбертовото пространство е 2^n. По-конкретно състоянието на такава система се определя от 2^n комплексни числа. Както отбелязва Файнман още през 80-те години, ръстът на изискванията към паметта на квантовия компютър е линеен по отношение на n, тъй като самата памет представлява една многочастична квантова система. Това означава, че за симулиране на система от n частици със спин ½ са необходими само n кубита. Следователно един квантов компютър, работещ със само няколко десетки кубита, ще надмине възможностите на класическите компютри. Разбира се, това е вярно само при условие, че намерим ефективни квантови алгоритми за извеждане на полезната информация от квантовия компютър. Още нещо интересно, бе показано, че квантовите компютри могат да бъдат ефективни не само при изследване свойствата на многочастичните системи, но също при изучаване квантовата и класическата динамика на сложни едночастични системи (за едно съвременно ревю вж. напр. [5]).

Първи експериментални постижения

Голямото предизвикателство пред квантовите пресмятания е експерименталното създаване на квантов компютър. За достигане на тази внушителна цел е необходимо да се изпълнят много изисквания. Необходима е съвкупност от квантови системи с две нива, която да може да бъде приготвена, управлявана и измервана по желание.С други

думи нашата цел е да бъдем в състояние да контролираме и измерваме състоянието на многокубитова квантова система. Един полезен квантов компютър трябва да бъде с разумна скала (?), доколкото ние се нуждаем от твърде голям брой кубити, за да извършваме нетривиални пресмятания. С други думи, нуждаем се от квантов аналог на интегралните схеми, използвани в един класически компютър. За да можем да създадем универсална мрежа от квантови гейтове, кубитите трябва да взаимодействат по един контролируем начин. По-нататък, ние трябва да сме в състояние да контролираме развитието на голям брой кубити за времето, необходимо за осъществяване на голям брой квантови гейтове. След като съвкупността от изисквания към изграждането на един квантов компютър са известни, много физични системи могат да бъдат подходящи кандидати за елементи, използвани за създаване на компютъра.

В течните квантови процесори [2], използващи ядрения магнитен резонанс (ЯМР), квантовият хардуеър се състои от течност, съдържаща голям брой (от порядъка на 10^{18}) молекули от даден тип, поставени в силно статично магнитно поле. Кубит представлява спинът на едно ядро в молекулата, а квантовите гейтове се осъществяват посредством резонансни променливи магнитни полета (импулси на Раби (?)), т.е. използва се техниката на ЯМР. Обмяната на квантова информация между ядрата вътре в молекулата се осъществява чрез спин-спин взаимодействия (химични връзки) между съседните атоми. Молекулите се приготвят при термично равновесие при стайна температура. Важно е да се подчертае, че в тези течности състоянието на спина на отделното ядро нито се приготвя, нито се измерва. Напротив – ние измерваме средното състояние на съдържащите се в течността 10^{18} молекули. В опитите с ЯМР бе възможно с помощта на молекули с 3 до 7 кубита да се покажат експериментално няколко квантови алгоритъма, включително алгоритъма на Гроуер, квантовата трансформация на Фурие и алгоритъма на Шор. За нещастие, квантовите пресмятания чрез ЯМР в течности страда от недостатъка, че измерваният сигнал намалява експоненциално с увеличаване на броя на кубитите в една молекула.

Чрез използване техниката на квантовата електродинамика (КЕД) в кухина (резонатор?) [6] станаха възможност експерименти, в които един отделен атом взаимодейства с един отделен мод или с няколко модове на електромагнитното поле в кухината. Двете състояния на един кубит може да се представят от поляризационните състояния на един фотон или от две възбудени състояния на един атом. Техниката на КЕД в кухина дава възможност да се осъществят едно- и двукубитови гейтове и вд частност се оказаха успешни при демонстриране на такива основни особености на

квантовата механика, като преплитането, или при изследване на прехода от квантовия свят към класическата физика.

Направени са и още няколко други предложения за направа на квантов компютър, включително и такива, свързани с квантовата оптика, с охладени атоми в оптични мрежи и твърдотелни системи като квантовите точки и спин в полупроводници. Твърде рано е да се каже кой път ще бъде най-подходящ за изграждане на подходящ (scalable ?) квантов хардуеър. Поради ограниченото място ние се ограничаваме с по-подробно обсъждане на само две предложения, за които напоследък има голям напредък: заловените охладени йони и свръхпроводящите вериги.

Капани за йони

Квантовият хардуеър е както следва: верижка от йони е фиксирана чрез комбинация от статично и променливо електрично полета в линеен капан (известен като капан на Паул, вж. фиг.1). Кубитът представлява отделен йон и две дългоживущи нива на йона съответстват на двете състояния на кубита. Линейната система от йони, задържани в капана, представлява квантовият регистър. Поставянето на всички кубити в начално състояние |0> е възможно, като се използва техниката на оптичното напомпване: когато един йон е в състояние, различно от |0>, той поглъща фотон и излъчва (?), като този процес се повтаря до достигане на нивото |0>. След операциите на квантовото пресмятане състоянието на всеки йон може да се измери чрез детектиране на *квантовите скокове*(?): всеки йон се осветява с лазерна светлина, чиято честота и поляризация са такива, че той поглъща и преизлъчва фотон само, ако е бил в състояние |1>. Обратно, ако йонът е бил в състояние |0>, честотата на лазерната светлина не е резонансна и не предизвиква никакъв преход. По такъв начин регистрирането на флуоресценция свидетелства, че йонът е бил в състояние |1>.

Еднокубитните гейтове се получават чрез адресиране на индивидуалните йони с лазерни импулси с подходящи честота, интензитет и продължителност. Взаимодействията между кубити, които са необходими за осъществяване на контролируеми двукубитови операции, се постигат чрез колективни трептеливи движения на фиксираната верижка от йони. За осъществяване на двукубитният CNOT гейт Чирак и Цолер предлагат следната схема. Квантовото състояние на контролния (?) кубит (йон) се отразява (?) на вибрационното състояние на цялата верижка (известно като *бус-кубит*) с помощта на лазерни снопове, фокусирани върху този йон. Тогава

между бус-кубита и йонът-мишена може да бъде осъществена една гейтова операция. Ще подчертаем, че това е възможно, тъй като йонът-мишена също участва в колективното трептеливо движение. В резултат на това ефектът от лазерния лъч върху кубита-мишена зависи от състоянието на бус-кубита. Накрая, това състояние се отразява обратно върху контролния йон. За отбелязване е, че днес приготвянето на основното състояние на модът на буса може да се осъществи с голяма точност, като се използват лазерните технологии за охлаждане.

CNOT-гейтът на Чирак – Цолер е осъществен от групата в Инсбрук [7], която използва два $^{40}Ca^{+}$ йона в линеен капан, които се адресират индивидуално с помощта на лазерни снопове. Общото еднокубитово състояние е кодирано в суперпозиция от основното състояние $S_{1/2}$ и метастабилното състояние $D_{5/2}$ (чието време на живот е приблизително 1 s). Наскоро учени от NIST, Боулдер и от Инсбрук осъществиха *квантова телепортация* между двойка они в капан [8, 9].Телепортацията използва заплитане и осигурява средство за пренос на квантова информация (квантово състояние) от едно място на друго, без пренасяне на физическата система, която носи квантовата информация. Тази възможност би могла да бъде от практически интерес за квантовото пресмятане, например за преноса на квантова информация между различни елементи на квантовия компютър.

Източници на грешки при използването на йони в капан за квантови пресмятания са загряването, дължащо се на случайните флуктуации на електричните полета, флуктуациите на придружаващите ги магнитни полета и лазерният честотен шум. Понастоящем осъществяването на CNOT-гейт чрез поредица от 8 лазерни импулса изисква приблизително 500 μs, докато мащабът на времето за декохерентност (?) е от порядъка на 1 ms. Тук загубата на квантова кохерентност означава разваляне на заложената в квантовия компютър квантовата информация, предизвикано от неизбежната връзка на квантовия компютър със заобикалящата го среда [10]. Изглежда вероятно, че в следващите няколко години, чрез използване на йони, които са по-невъзприемчиви към влиянието на околната среда, ще стане възможно да се приложат десетки гейтове на малък брой йони без да се губи квантовата кохерентност.

Очаква се достигането на голям брой кубити да се осъществи с помощта на мрежа от свързани йонни капани. Комуникациите между тях биха могли да се постигнат посредством чрез обмен на фотон, или чрез прехвърляне на йон от есин капан в друг. В първия случай състоянието на един кубит може да се пренесе от един захванат в капана йон на един фотон и после – от фотона към друг йон, намиращ се в

друг капан. Във втория случай йонният кубит би могъл да се придвижи от един капан до друг чрез прилагането на подходящи електрични полета. Изглежда, че няма фундаментални физични пречки за осъществяване на тези предложения, но остават значителните технологични предизвикателства.

Свръхпроводящи вериги

Бяха направени няколко предложения за изграждане на твърдотелен квантов компютър. Това не е изненадващо, понеже твърдотелната физика през годините разви замисловати технологии, създавайки изкуствени структури и прибори с наномащаби. Твърдотелната физика е в основата на развитието на класическите компютърни технологии и следователно проблемът за по-нататъшното намаляване на мащабите би могъл да намери своето естествено решение в един твърдотелен квантов компютър. Наистина, такъв квантов компютър би могъл да се възползва от производствените техники на микроелектрониката.

Напоследък бе направен забележителен експериментален напредък в използването на свръхпроводящи микроелектронни вериги за конструиране на изкуствени системи с две нива [11]. В свръхпроводниците се образуват т. нар. куперови двойки – два електрона се свързват така, че образуват обект, чиито заряд е два пъти по-голям от заряда на електрона. С помощта на електрично поле куперовата двойка може да се затвори в "кутийка" с размерите на микрометър. В един джозефсоновски контакт кутийката на една куперова двойка, известна като остров, се свързва чрез тънък изолаторен слой (тунелен контакт?) с един свръхпроводящ резервоар (вж. фиг. 2). Куперовите двойки може да преминават от острова в резервоара и обратно посредством тунелен ефект. Те влизат в острова един по един, когато капацитивната връзка на електрода на контролния гейт се променя. Тъй като енергетичните нива на острова са дискретни, при определени експериментални условия двете най-ниски нива |0> и |1> образуват система от две нива, подходяща за кубит. На фиг. 3 е показана една усъвършенствана верига с кутийка на куперова двойка, която действа като кубит. Чрез прилагане на микровълнови импулси на гейтовия електрод чрез този кубит може да бъде реализирана произволна кохерентна суперпозиция $\alpha|0>+\beta|1>$. Възможни са манипулации на еднокубитовите състояния: един микровълнов резонансен импулс с продължителност τ индуцира управляеми Раби-осцилации между състоянията |0> и |1>. Ако стойността на τ е подходяща, може да се осъществи NOT-гейтът (|0> → |1>, |1> → |0>). Един опит с ивици (?) на Рамзей дава също така възможност да се измери мащабът на времето на декохерентност – за тази верига то е около 0,5 μs [12]. Това време е

много по-голямо от времето, необходимо за осъществяване на еднокубитов гейт, така че със серия от микровълнови импулси може да се реализира произволна еволюция на системата от две нива. Трябва да се отбележи, че времето, необходимо за еднокубитова операция може да се скъси до 2 ns. Наскоро с помощта на двойка капацитивно свързани свръхпроводящи кубити бе осъществен двукубитов гейт [13].

Перспективи

Да резюмираме, главният дискутиран въпрос е: възможно ли е да се построи полезен квантов компютър, който да бъде по-добър от съществуващите класически компютри при решаване на изчислителни задачи? И ако отговорът е “да”, то кога? Трудностите са огромни. Освен проблемът с декохерентността, трябва да спомена и трудността при намиране на нови и ефективни квантови алгоритми. Ние знаем, че проблемът за разлагане на прости множители може да бъде решен ефективно с квантов компютър, но ние не знаем отговора на следния фундаментален въпрос: Какъв клас от задачи може да бъде решаван ефективно с квантов компютър. Квантовите компютри разкриват прекрасни перспективи, но няма вероятност в близките години те да станат реалност с практическо приложение. Колко време ще бъде необходимо за разработване на съответните технологии? Въпреки че по принцип неочаквани пробиви в технологиите са възможни, трябва да помним огромните усилия, необходими за развитието на технологията на класическите компютри.

Въпреки това даже първите, скромни, демонстрационни опити са забележителни – не само за квантовите пресмятани, но и за проверката на теоретичните принципи на квантовата механика. Доколкото квантовата механика представлява теория, противоречаща на интуицията, в края на краищата би трябвало да очакваме, че експериментите и теоретичните изследвания на квантовите пресмятания ще ни осигурят едно по-добро разбиране на самата квантова механика. Нещо повече, подобни изследвания стимулират контрола на отделни квантови системи (атоми, електрони, фотони и др.). Подчертаваме, че това не са просто лабораторни куриози, а имат интересни технологични приложения. Например, сега е възможно да се направи часовник с един йон, който е по-точен от стандартните атомни часовници. Други предвидими приложения са използването на заплетени състояния за повишаване разделителната способност на оптичната литография и на интерферометричните измервания.

Квантовата механика осигурява също уникално съдействие на криптографията: тя дава възможност на двама партньори в комуникацията да проверят дали предаденото съобщение е било прехванато от подслушвач. В областта на класическата физика това е невъзможно, тъй като по принцип винаги може да се копира информацията, без да се променя съобщението. Противоположно на това, в квантовата механика процесът на измерване, най-общо казано, променя системата от най-общи принципни съображения: това е следствие от принципа на Хайзенберг за неопределеността. Експерименталният напредък в областта на квантовата криптография е впечатляващ [14] и с помощта на оптични кабели с дължина няколко десетки километра вече са демонстрирани квантови криптографски протоколи при скорост на предаване на информацията хиляда бита в секунда.Нещо повече, демонстрирана е безкабелна квантова криптография на разстояние няколко километра. Следователно има всички изгледи в близкото бъдеще квантовата криптография да стане първият квантово-информационен протокол, който да намери търговски приложения.

В заключение ще кажем, че все още не е ясно кога ще настъпи времето, когато на бюрото си ще имаме квантов компютър. Това, което е сигурно, е фактът, че е отворено едно вълнуващо и многообещаващо поле за изследвания. Накрая, нека цитираме Шрьодингер [Brit. J. Phyl. Sci. 3, 233 (1952)]: “Ние никога не правим опити с точно един електрон или атом, или (малка) молекула. В мисловните експерименти ние понякога го правим; това винаги влече след себе си абсурдни следствия … Възможността ни да експериментираме с отделни частици е не по-голяма от тази да отглеждаме ихтиозаври в зоологическите градини.” Забележително е, че само 50 години по-късно експериментите с отделни електрони, атоми и молекули са вече рутинна практика в лабораториите по целия свят.

Литература[1]

1. G. Benentiq G. Casati and G. Strini, Principles of Quantum Computation and Information, Vol. I: Basic Concepts (World Scientific, Singapore, 2004).
2. M. A. Nielsenand I. L. Chuang, Quantum computation and quantum information (Cambridge University Press, Cambridge, 2000).
3. G. Benentiq G. Casati and S. Montangero, quant-ph/0402010.
4. J. M. Raimond, M. Brune and S. Haroche Rev. Mod. Phys. 73, 565 (2001).

[1] Въпреки че се споменават в текста, източниците с номера 13 и 14 липсват в списъка на литературата в оригинала. (Бел. прев.)

5. F. Schmidt-Kaler et. al., Nature 422, 408 (2003).

6. M. Riebeet al., Nature 429, 737 (2004).

7. M. D. Barrett et. al., Nature 429, 737 (2004).

8. W. H. Zurek, Rev. Mod. Phys. 75, 715 (2003).

9. Y. Makhlin, G. Schon and A. Shnirman, Rev. Mod. Phys. 73,357 (2001).

10. D. Vion et. al., Science 296, 886 (2002).

11. T. Yamamoto et. al., Nature 425, 941 (2003).

12. N. Gisin et. al.

Превод от Europhysics News: Х. Д.

Текст под фигурите:

Фиг. 1: Схематично представяне на редица от кубити (йони) в линеен капан. Йоните се държат в капан от комбинация от статично и променливо електрични полета. За да се детектира състоянието на йоните, те се осветяват с подходяща лазерен сноп: част от излъчените чрез флуоресценция фотони от йоните се събират с леща и попадат върху една CCD-камера. Долу е показано изображение на “пленените” йони”. (Снимката е предоставена от Райнер Блат от университета в Инсбрук.)

Фиг. 2: Схематично представяне на най-простия вид кубит, реализиран с джозефсоновски контакт: един малък свръхпроводящ остров *n*, в който има излишък (по отношение на някакво отправно ниво) от куперови двойки, е свързан посредством тунелен контакт с капацитет C_j и джозефсоновска енергия на връзката E_j към свръхпроводящия резервоар. Контактът се влияе от напрежението U на гейта с капацитет на гейта C_g.

Фиг. 3: Горе: Схема на свръхпроводяща верига, наречена “квантрониум”, която се държи като система с две нива. Веригата се състои от свръхпроводящ остров (черната точка), свързан с два малки джозефсоновски контакта (кутийките с “X” в тях) в свръхпроводяща затворена верига. Веригата е включена в трети, по-голям джозефсоновски контакт. С E_J и E_{J0} са отбелязани джозефсоновските енергии за кутийката с куперовите двойки и съответно за големия контакт. Броят N на куперовите двойки в острова и свръхпроводящите фази δ и γ са степените на свобода на веригата. Ток I_Φ през намотката създава магнитен поток Φ в затворената верига и се използва за настройка на квантовите енергетични нива. За приготвяне на произволно състояние на

кубита се използват микровълнови импулси $u(t)$, приложени към гейта. Тези състояния се регистрират чрез прилагане на токов импулс $I_b(t)$ към големия контакт и чрез следене на неговото напрежение V(t).

Долу: Снимка на образец, изготвен от алуминий и алуминиев оксид, получена със сканиращ електронен микроскоп. Гейт-електродът е отгоре, а островът е под гейта. Широкият правоъгълник долу представлява големия контакт.