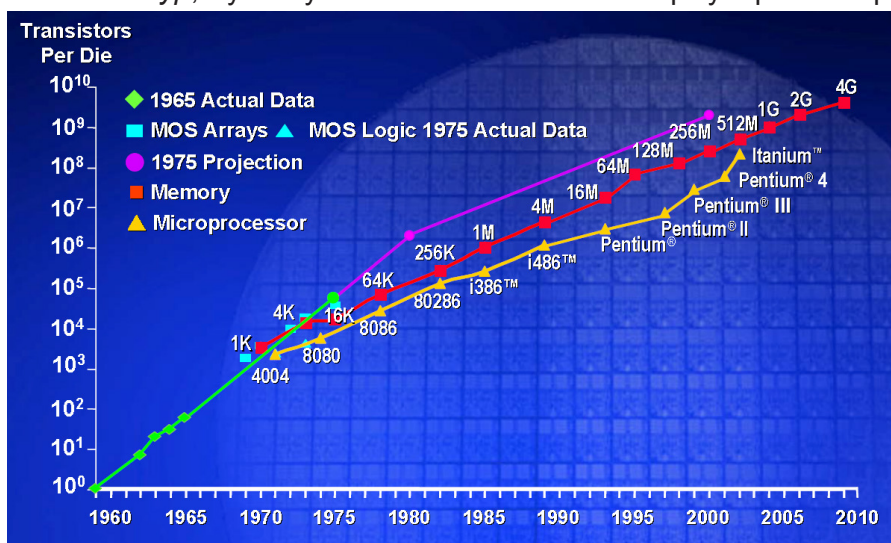


1.3. КВАНТОВИ ИЗЧИСЛЕНИЯ

Забележителна особеност на съвременния етап от развитието на компютърните архитектури е постепенният преход от последователния фоннойманов към паралелния изчислителен модел на *макрониво*¹, както и изследването на възможностите за използване на принципите на квантовата механика за представяне, обработка и пренос на информацията на *микрониво*².

Подобно съвпадение не е случайно. Основните предпоставки са физическите ограничения на използвания класически последователен изчислителен модел, физическите ограничения на полупроводниковата технология, достигнатата степен в познанието за законите на квантово ниво.

На фиг. 1.10 е приведена една от известните илюстрации на *закона на Мур*, публикувана в сайта на *Intel*. Формулиран за пръв



Фиг. 1. 10. Илюстрация на закона на Мур, източник: *Intel Corp.*

1 *Макросветът* се определя като множество от обекти, размерите на които са съпоставими с мащабите на човешките възприятия [В.10].

2 *Микросветът* е множеството обекти, които не могат да се наблюдават непосредствено и за които е характерно квантовото поведение [В.10]. Размерът на тези обекти е в интервала 10^{-10} - 10^{-18} м.

път през 1965 г. от Гордън Мур, той и досега, с малки корекции, определя експоненциалното нарастване на степента на интеграция на полупроводниковите електронни чипове. Редица автори сочат, че действието на този закон ще продължи до около 2040 - 2050 г. [Г.10]. Със спирането на неговото действие ще спре и съществуването на полупроводниковата електроника в днешния ѝ вид. Добре е обаче да се разбира, че става дума не за спиране на съществуването на електрониката, а за невъзможността действието на електронните схеми да продължи да се описва със законите на класическата физика.

Ако законът на Мур се преформулира не чрез броя транзистори, а чрез *характеристичния размер (feature size)* на полупроводниковата технология, се получава фиг. 1.11, еквивалентна на фиг. 1.10. При нея също се използва полулогаритмичен мащаб, като наклонът на теоретичната крива е -12% за година [А.27].

В момента полупроводниковите интегрални схеми имат характеристичен размер от порядъка на 25 - 32 nm и все още се подчиняват на класическите закони на физиката за макросвета³.



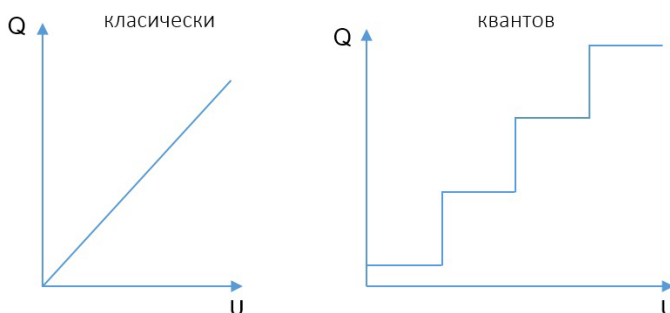
Фиг. 1. 11. Графика на промяната на *характеристичния размер* на интегралните схеми във времето

От фиг. 1.11 се вижда, че до 2020 г. характеристичният размер на интегралните схеми ще намалее до степен, в която ще се засили влиянието на квантовите ефекти. И класическата физика, като апроксимация на законите на квантовата механика, ще стане неприложима в областта на наноелектрониката.

Илюстрация на този феномен е приведена в [А.27]. Намаляването на характеристичния размер на полупроводниковата технология е съпроводено с намаляване на работното напрежение, за да не се надвиши пробивното напрежение на градивния материал.

³ За сравнение, размерът на атома на водорода, определен по най-отдалечената от ядрото електронна орбита, е от порядъка на $0,1 \text{ nm} = 10^{-10} \text{ m}$ [В.13, В.17].

Капацитетът на сферичен кондензатор е $C=4\pi\epsilon_0 r$. Ако радиусът r на кондензатора е 50 nm , капацитетът му ще бъде $5 \cdot 10^{-18} \text{ F}$. Промяната на напрежението върху кондензатора с $0,1 \text{ V}$ ще е свързано с преместването на четири електрона⁴. Посочва се, че описанието на действието на електронните схеми чрез класическата физика, като апроксимация на законите на квантовата механика, е приложимо само до нивото на кохерентност на електроните. Това ниво зависи от градивния материал, обработката и работната температура. Намира се в границите $\sim 0,1 \text{ nm}$ до $\sim 1 \text{ nm}$.



Фиг. 1. 12. Сравнение на волтамперната характеристика на *класически* (вляво) и *квантов* (вдясно) кондензатор

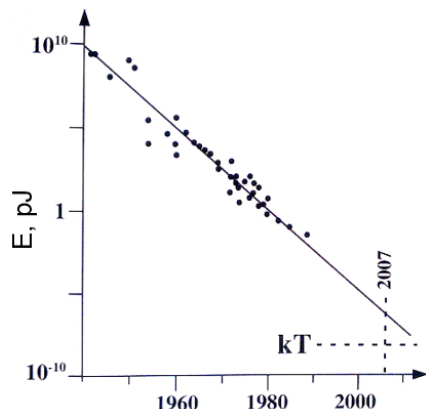
На фиг. 1.12 са сравнени характеристиките на кондензатора, съгласно класическата физика и с отчитане на квантовите ефекти [А.27]. Зарядът на класическия кондензатор е правопрпорционален на приложеното напрежение, докато при квантовия кондензатор, преносът дори на единичен електрон променя скокообразно заряда. С други думи, преходът към квантово ниво изменя начина на работа на електронните схеми, познати от класическата физика и нейните раздели, свързани с теоретичната електротехника и полупроводниковата електроника.

Едновременно с намаляването на характеристикния размер на интегралните схеми, трябва да се намалява и количеството разсейвана от тях енергия (фиг. 1.13). Съгласно *принципа на Ландауер*, всяко необратимо изчисление, е свързано с отделянето на определено количество енергия [А.5, А.11, А.27].

Под логическа обратимост на изчисленията се разбира възможността за взаимнооднозначно изображение на множеството входове в множеството изходи и обратно. Необходимото условие за обратимост е броят изходи да се равнява на броя входове.

От класическите логически елементи (вентили) обратим е само елементът *“НЕ”*, докато елементите *“И”* и *“ИЛИ”* са необратими.

⁴ При стайна температура ($\sim 100 \text{ K}$), термалното напрежение на електрона е приблизително 26 mV .



Фиг. 1. 13. Графика на промяната на количеството разсейвана енергия за логическа операция

Теоретичният минимум на разсейваната от всеки двоичен цифров компютър енергия е $kT \ln 2$ J за всяка конюнкция и дизюнкция⁵. Енергийната граница kT се преодолява единствено при обратимите изчисления, каквито са квантовите.

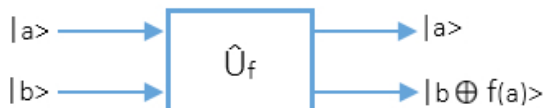
От направените разглеждания става ясно определящото място на физическите ограничения на съвременните цифрови компютри и на съвременната полупроводникова технология за необходимостта от изследвания в областта на квантовите изчисления.

Вторият, не по-малко важен фактор, е вътрешноприсъщият на квантовите изчисления паралелизъм. В неговата основа е възможността едновременно да се обработва суперпозицията на всички стойности на входната величина. При това, *NP*-алгоритмите се редуцират в *P*-алгоритми, т.е. неефективните алгоритми с експоненциална сложност за класическите цифрови компютри се редуцират до ефективни полиномиални квантови алгоритми. Такъв е примерът с първия известен квантов алгоритъм – алгоритъмът на Питър Шор (Peter Shor) от 1994 г. за факторизация на цели числа (разлагане на прости множители) [A.23].

Квантовите изчисления протичат в следната последователност [A.23]. Формира се входното множество *q-битове* (*qubits*). Подава се за обработка към *квантовата верига* (*quantum circuits*), която съдържа група *квантови вентили* (*quantum gates*). Квантовата верига преобразува входното множество *q-битове* в изходно чрез предварително зададена унитарна трансформация⁶. Накрая се

5 Константата на Болцман $k = 1,38 \cdot 10^{-23}$ J/K свързва енергията на отделна частица с температурата. *Характеристичната енергия* kT отговаря на количеството топлина, необходимо за промяна на информационната ентропия (ентропията на Клод Шенон) с 1 nat.

6 Изискването за унитарност на преобразуването, извършвано от



Фиг. 1. 14. Схематично представяне на квантов процесор [A.8]

извършва измерване на изходното за веригата квантово състояние и се извлича резултата от обработката. Така, квантовият процесор отговаря на схемата от фиг. 1.14. За да бъде универсален, на входа му се подават две квантови променливи, представени с кет-векторите $|a\rangle$ и $|b\rangle$. На изхода на квантовия процесор, в резултат на унитарната трансформация \hat{U}_f , се формира изходното състояние

$$|a\rangle \otimes |b\rangle \rightarrow \hat{U}_f |a\rangle \otimes |b\rangle = |a\rangle \otimes |b \oplus f(a)\rangle \quad (1.3.1)$$

където \otimes е тензорното произведение, а \oplus - операция XOR на q -битовете. Тензорното произведение⁷ служи за получаване на q -бит от няколко q -бита с по-малка размерност. Например, ако кет-векторите $|a\rangle$ и $|b\rangle$ са единични q -битове (1-qubit), тяхното тензорно произведение $|a\rangle \otimes |b\rangle = |ab\rangle$ е двоен q -бит (2-qubit).

По определение квантовият бит (q -bit, qubit) е единица информация, описваща двумерна квантова система.

Квантовият бит $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ е вектор от двумерното комплексно Хилбертово пространство \mathbb{C}^2 . Представя се с матрица-стълб с размерност 2 от вида $\begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$, където c_0 и c_1 са комплексни числа, за които е изпълнено условието $|c_0|^2 + |c_1|^2 = 1$. Първият елемент $|c_0|^2$ се разглежда като вероятността⁸ този q -бит да се измери в състояние $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, докато вторият елемент $|c_1|^2$ - като вероятността да се измери в състояние $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Следователно, квантовият бит представлява обобщена информационна единица, а класическият логически бит е неин частен случай. При измерването, квантовият бит автоматично се превръща, т.е. колапсира, в класически бит [A.23].

Вътрешноприсъщият на квантовите изчисления паралелизъм е във възможността едновременно да се обработва не само единични стойности, а суперпозицията на всички стойности на входната

квантовата верига е свързано с обратимостта на квантовите изчисления.

⁷ Тензорното произведение е известно също като *произведение на Кроникер* [B.9].

⁸ За да не се бъркат с класическите вероятности, тъй като не е задължително да бъдат нормирани, c_0 и c_1 е прието да се наричат амплитуди на вероятностите.



Фиг. 1. 15. Квантов процесор с *EPR* изход [А.8]

величина. Така, квантовият процесор от фиг. 1.15 изчислява едновременно $f(a)$ за всички стойности на a . Суперпозицията съдържа 2^n стойности, които квантовият процесор обработва за време, представляващо полином от n . Като резултат се получава експоненциално нарастване на производителността, спрямо класическата обработка.

Получаваното изходно състояние се определя като *сплетено* (*entangled*). Обозначава се още като *EPR* (Einstein, Podolsky, Rosen) по имената на откривателите на известния квантов парадокс за сплетените елементарни частици. Процесът на формирането на подобно състояние се нарича *сплитане* (*entanglement*). Изпълнява се от схема, наричана *EPR* източник (*EPR source*) или генератор на *състояния на Бел* (*Bell state generator*).

Сплитането е от принципно значение за квантовите изчисления, защото е в основата на квантовата телепортация - единственият начин за пренос на квантова информация на разстояние. За разлика от цифровите компютри, при квантовите не е възможно копирането на съдържанието на квантовите регистри⁹.

Квантовата верига, извършваща унитарната трансформация \hat{U}_f , включва множество *вентили* (*gates*), различавани по размерността на квантовото състояние и по вида на обработката. Част от тези вентили образуват функционално-пълни набори.

Важно множество *1-qubit* квантови вентили $\{I, X, Y, Z\}$ се представят с *матриците на Паули*.

Повторителят I отговаря на единичната матрица $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Вентилът $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ представлява инвертор.

Вентилът $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ извършва фазово завъртане на 180° .

Вентилът $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -iZX$ извършва инверсия и фазово завъртане.

За формиране на суперпозиция се използва *1-qubit* вентил на

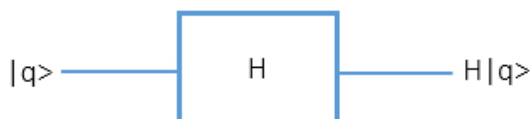
⁹ Това е следствие на теоремата за невъзможност на клонирането на квантовите състояния (*no-cloning theorem*).

Адамар (*Hadamard gate*), описван от матрицата $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Ако например на входа на квантовата верига от фиг. 1.16 се подаде кет-векторът $|0\rangle$, изходното *1-qubit* квантово състояние ще отговаря на положителната суперпозиция на кет-векторите $|0\rangle$ и $|1\rangle$

$$|q\rangle = |0\rangle \rightarrow H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (1.3.2)$$

Аналогично, може да се докаже, че ако на входа на квантовата верига от фиг. 1.16 се подаде кет-векторът $|1\rangle$, на изхода ще се получи отрицателната суперпозиция на кет-векторите $|0\rangle$ и $|1\rangle$, описвана от израза $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

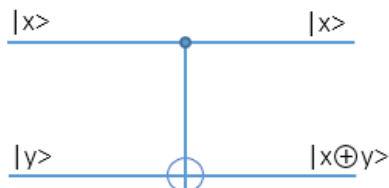


Фиг. 1. 16. Вентилът на Адамар служи за суперпозиция на входния *1-qubit*

Интересен *2-qubit* вентил е управляваният инвертор *CNOT* (*Controlled-NOT gate*, Feynman gate). Сам по себе си той образува функционално-пълно множество. Неговото включване към квантовата верига е показано на фиг. 1.17. Унарното преобразуване, което извършва вентилът *CNOT*, се определя от матрицата

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (1.3.3)$$

Горният вход $|x\rangle$ е управляващ, а долният - $|y\rangle$ се инвертира, ако на управляващия вход е подаден *q*-бита $|x\rangle = |1\rangle$. Така, на изхода на веригата се получава следният *2-qubit* резултат $U_{CNOT}|xy\rangle = |x(x \oplus y)\rangle$.



Фиг. 1. 17. Означение на универсалният *2-qubit* *CNOT* вентил

От сравнението на матрицата на *1-qubit* инвертиращия вентил *X* с матрицата на *2-qubit* вентил *CNOT*, се получава следното

представяне

$$U_{CNOT} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \quad (1.3.4)$$

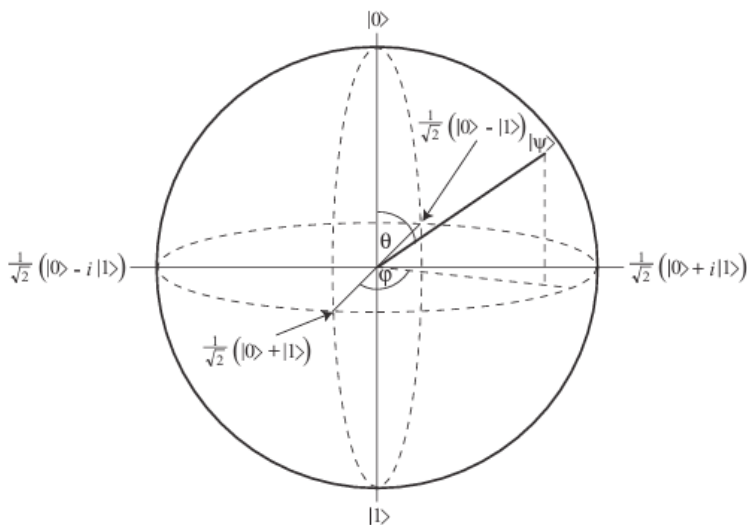
По идентичен начин може да се получат и други управлявани вентили. Например управляваният Z вентил (*Controlled-Z gate*) се определя от матрицата

$$U_{CZ} = \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (1.3.5)$$

Графически квантовият бит $|\psi\rangle$ може да се представи като точка от повърхността на сфера, наричана *сфера на Блох* (*Bloch sphere*, фиг. 1.18) [A.8]. Това е сфера с единичен радиус, всяка точка от повърхността на която отговаря на определено чисто състояние¹⁰. Противоположните точки на сферата отговарят на ортогонални квантови състояния. Северният и южният полюс отговарят съответно на кет-векторите $|0\rangle$ и $|1\rangle$. Най-общо, квантовото състояние

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (1.3.6)$$

съответства на точка от повърхността на сферата на Блох с полярни координати θ и φ .



Фиг. 1. 18. Графично представяне на квантовия бит $|\psi\rangle$

¹⁰ Чисто (*pure state*) се нарича квантово състояние с еднозначно определен вектор. То е частен случай на *смесеното състояние* (*mixed state*) с вероятност 1. Смесените квантови състояния имат вероятностен характер [A.8, A.21, A.II.2].

Представената работа е част от развиващата се в катедра "Компютърни системи и технологии" на Русенския университет "А. Кънчев" тематика за изследване на квантовите явления чрез моделирането им в паралелна изпълнителна среда. Възприетият подход предполага *съвместното разглеждане* на прехода към паралелен изчислителен модел, както на макрониво, така и на квантово ниво.

Разглежда се възможността за *структурно моделиране* на основните квантови явления - поляризация, суперпозиция, сплитане, квантова телепортация, залегнали в основата на квантовите изчисления. При това, паралелният структурен модел е тъждествен на квантовата верига, която извършва преобразуванията на вектора на състоянието.