Чи виправдана така кількість назв одного і того ж фізичного явища? Нехтування у назвах єдиної фізичної природи вільного ЕМВ та гіперолізація однієї з багатьох властивостей, якою підмінюється справжня назва теплового, оптичного, рентгенівського, радіаційного і космічного електромагнітного випромінювання нерідко призводить до спотвореного розуміння сутності єдиного явища – вільного електромагнітного випромінювання з різною частотою коливань, яку можна ще трактувати як швидкість формування повного коливання електромагнітної хвилі.

1. Біленко І.І. Фізичний словник.– 2-е вид., перероб. і допов. – К.: Вища школа, 1993.– 319 с. 2. Шеннон К. Работи по теории информации и кибернетике. - М.: ИЛ, 1963 – 829 с. 3. Бриллюэн Л. Научная неопределенность и информация. – М.: Мир, 1966 – 271 с. 4. Бриллюэн Л. Наука и теория информации. – М.: Физмат., 1960.– 329 с. 5. Шилейко А.В., Кочнев В.Ф., Химушин Ф.Ф. Введение в информационную теорию систем.– М.: Радио и связь, 1985. – 280 с. 6. Игнатов В.А. Теория информации и передачи сигналов: Учебник для ВУЗов.– 2-е изд., перераб. и доп. – М.: Радио и связь, 1991.– 280 с. 7. Тарасенко Ф.П. Введение в курс теории информации. - Томск, Изд. Томского университета, 1963.– 240 с. 8. Сколник М. Введение в технику радиолокационних систем. - М.: Мир, 1965.– 748 с. 9. Ребане К.К. Енергия, ентропия, среда обитания. - М.: Знание, 1985.– 64 с. 10. Дверняков В.С. Солнце – жизнь, енергия.– К.: Наукова думка, 1986.– 112 с. 11. Айламазян А.К., Стась Е. Информатика и теория развития.– М.: Наука, 1989.– 174 с.

УДК 621.378

Піотр Марецкі
Вища школа інформатики та управління, м. Бєльско-Бяла (Польща)

МАТЕМАТИЧНІ МОДЕЛІ ЕЛЕМЕНТІВ КВАНТОВОЇ ІНФОРМАТИКИ

Ця стаття присвячена математичному опису фізичних процесів, які лежать в основі т.зв. “квантових обчислень” – нового напряму в науці, який виник і розвивається протягом двох останніх десятиліть, і відразу став об’єктом міждисциплінарних досліджень. Якщо квантові обчислення ляжуть в основу побудови квантових комп’ютерів, вони спричинять революційний переворот в теорії інформації.

The paper is devoted to a mathematic description of the physic processes in the new branch of science called “Quantum Computing”. The branch emerged quite recently (last two decades) and immediately focused quite interdisciplinary research. It provides a powerfull tools which – if implemeuted – would truly revolutionize the theory of information.

Сучасна квантова теорія інформації займається питаннями перетворення інформації за допомогою мікроскопічних систем, які описує квантова механіка. Аналогічно як підставою існування класичної теорії інформації є наука про електрику, яка пояснює принцип дії електронних приладів, так підставою квантової теорії інформації є квантова

механіка, яка пояснює принцип дії пристроїв, що перетворюють квантову інформацію. Поведінка квантових систем є настільки дивовижною та несподіваною, що для її розуміння та обґрунтування необхідно побудувати та проаналізувати відповідні математичні моделі.

1. Спін як аналог біта. Математичний опис стану спіна. Квантові системи, які практично реалізують квантові алгоритми, використовують мікрочастинки. Часто квантова інформація кодується станом окремого електрона чи йона. В класичній інформатиці прийнято бітовий (двійковий) запис, тобто вважають, що на виході логічного елемента появляється “0” або “1”. Щоб знайти квантовий еквівалент для такої ситуації уявимо собі систему, що складається з електрона у зовнішньому магнітному полі. У досить грубому наближенні електрон можна вважати обертовим зарядом, який має магнітний момент (аналогічний до стрілки компаса). Виявляється, що квантовий характер електрона проявляється у тому, що його магнітний момент, який називатимемо далі спіном, може бути спрямований або згідно з напрямом поля, або проти напряму поля. Отже, існують лише два стани спіна. Стан спрямування спіна згідно з напрямом електромагнітного поля позначатимемо $|0\rangle$, а протилежний стан – $|1\rangle$. Це є аналогією класичного біта. Стан спіна називатимемо q бітом.

Стан спіна електрона у зовнішньому електромагнітному полі описуватимемо за допомогою нормованого вектора у n-вимірному просторі Гільберта H, для якого задана база (найчастіше ортонормальна), тобто сукупність n взаємно перпендикулярних векторів одиничної довжини.

Наприклад, для двовимірного H-простору (тобто одного q біта) базою є вектори $|0\rangle$ і $|1\rangle$.

Станом квантової системи називаємо вектор u простору Гільберта H одиничної довжини, (для якого скалярний добуток (u,u)=1. Очевидно, що базові стани спіна $|0\rangle$ і $|1\rangle$ є станами квантової системи, оскільки за означенням вони нормовані до 1. Прикладом інших станів квантової системи є: $\psi = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ та $\chi = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Перевірка показує, що $(\psi,\chi)=0$, тобто ці стани є ортогональними.

Зауважимо, що квантова еволюція, тобто зміна стану квантової системи в часі мусить зберігати властивість нормованості до 1. Інтуїтивно уявляємо, що еволюція повинна бути типу “обороту”, оскільки лише обертання не змінює довжини векторів. Ця властивість зумовлює те, що квантова еволюція завжди буде оборотна, тобто обчислення квантових комп’ютерів на відміну від класичних завжди будуть оборотними. Наприклад, класична операція AND не є оборотною, оскільки не можна однозначно визначити значення вхідних бітів, якщо відоме значення вихідного біта.

Очевидно, що у квантовій теорії інформації розглядають системи багатьох q бітів. Щоб квантові обчислення мали яке-небуть практичне значення, необхідно мати квантові системи з станами біля 100 qбітів. У цьому випадку квантові обчислення виявились би у декілька разів швидшими від обчислень на звичайних комп’ютерах.

Розглянемо простір Гільберта двох qбітів. Математичним апаратом, який описує простір станів двох незалежних спінів, є простір Гільберта $H_{(2)}=H\otimes H$, або т. зв. тензорний добуток односпінових просторів Гільберта. У просторі Гільберта $H_{(2)}$ задана ортонормальна база: $e_1=|0\rangle\otimes|0\rangle$; $e_2=|0\rangle\otimes|1\rangle$; $e_3=|1\rangle\otimes|0\rangle$; $e_4=|1\rangle\otimes|1\rangle$.

Скалярний добуток у просторі $H_{(2)}$ задається для $\psi,\chi \in H_{(2)}$ (де $\psi=\psi_1\otimes\psi_2$; $\chi=\chi_1\otimes\chi_2$) у вигляді: $(\psi,\chi)=(\psi_1,\chi_1)\cdot(\psi_2,\chi_2)$. Хоч усі стани у вигляді $\psi_1\otimes\psi_2$ належать просторові $H_{(2)}$,

проте не всі двоспінові стани можна звести до такого самого вигляду. Дійсно, оскільки базовими векторами є e_1, ... e_4, то всі лінійні комбінації цих векторів нормовані до 1 є станами двоспінової системи. Зокрема, нормованим є вектор

$$\psi = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + (|1\rangle \otimes |1\rangle). \quad (1)$$

Стани у вигляді $\psi_1 \otimes \psi_2$ мають чітку фізичну інтерпретацію: система двох спінів знаходиться у такому стані, якщо перший спін знаходиться у стані ψ_1, а другий – у стані ψ_2.

Проте аналіз показує, що не існує таких ψ_1 та ψ_2, тензорний добуток яких дав би стан (1). Дійсно, довільні вектори односпінового простору можна записати у вигляді: $\Psi_1 = \alpha|0\rangle + \beta|1\rangle$; $\Psi_2 = \gamma|0\rangle + \delta|1\rangle$. Їх тензорний добуток дорівнює: $\Psi_1 \otimes \Psi_2 = \alpha\gamma|0\rangle \otimes |0\rangle + \alpha\delta|0\rangle \otimes 1 + + \beta\gamma|1\rangle \otimes |0\rangle + \beta\delta|1\rangle \otimes |1\rangle$.

Щоб цей стан був еквівалентним станові (1), мусять виконуватись умови: $\alpha\gamma = 1/\sqrt{2};\ \alpha\delta = 0;\ \beta\gamma = 0;\ \beta\delta = 1/\sqrt{2}$. Можна переконатись, що ці умови є суперечливими.

Отже, існують такі стани в системі двох спінів, які не можна інтерпретувати окремо як стани першого та другого спіна. Іншими словами, не можна говорити про стан першого спіна, не згадуючи про другий спін. Стани є взаємозв'язані між собою – це ускладнені (заплутані) стани. Систему треба розглядати в цілому, не розділюючи її на частини, оскільки проста сума її частин не відповідає цілості.

2. Операції над квантовими станами. Приступаючи до розгляду операцій, за допомогою яких можна створювати квантові алгоритми, враховуємо умови, які повинна задовольняти кожна операція, а саме: кожен стан квантової системи є нормований до 1 і, крім того, будь-які операції над квантовими системами не можуть змінювати довжини векторів.

Математичним відповідником терміну "операція" є поняття оператора – лінійного відображення, яке ставить у відповідність елементам простору Гільберта елементи цього ж простору. Позначатимемо оператори великими літерами A, U, R …

Важливе значення мають т. зв. унітарні оператори, які мають таку властивість: нехай $A: H \to H$ так, що для кожного $\psi \in H$ $A\psi \in H$. Оскільки операції мусять зберігати норму станів, то має виконуватись умова: $||A\psi|| = 1$. Отже, $(A\psi, A\psi) = (\psi, \psi)$.

Відомо, що кожний унітарний оператор є оборотним, тому можемо уточнити властивість оборотності:

Твердження 1. Кожна операція на квантовій системі описується унітарним оператором і як така завжди є оборотною.

Зручною формою представлення операторів є матричеве представлення.

Твердження 2. Кожний оператор можна записати у вигляді:

$$A = a_{00}|0\rangle \cdot \langle 0| + a_{01}|0\rangle \cdot \langle 1| + a_{10}|1\rangle \cdot \langle 0| + a_{11}|1\rangle \cdot \langle 1|, \quad (2)$$

причому коефіцієнти a_{ij} є комплексними числами, а дія оператора полягає у тому, що довільні вектори у вигляді $\alpha|0\rangle + \beta|1\rangle$ реалізуються шляхом утворення скалярних добутків згідно з правилом $|0\rangle \cdot \langle 0|$ діючи на $|\psi\rangle = |0\rangle \cdot (|0\rangle, \psi)$.

Згідно з наведеним твердженням кожен оператор можна охарактеризувати чотирма комплексними числами, записаними у вигляді матриці

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}.$$

Можна показати, що найпростішому унітарному операторові ідентичності I (дія якого є такою: $\psi=\psi$), відповідає одинична матриця

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

а унітарному операторові R множення на фазовий кут α відповідає матриця

$$R=\begin{pmatrix}e^{j\alpha} & 0\\ 0 & e^{j\alpha}\end{pmatrix}.$$

Цікавим унітарним оператором є оператор X Паулі, якому відповідає т. зв. матриця Паулі:

$$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Можна переконатись, що згідно з (2), справедливими є співвідношення: $X|0\rangle = |1\rangle$; $X|1\rangle = |0\rangle$, які є очевидним аналогом класичної операції заперечення (NOT).

Відомі також інші оператори Паулі:

$$Y=\begin{pmatrix}0 & -j\\ j & 0\end{pmatrix}; \qquad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

В принципі кожний унітарний оператор відповідає експериментально реалізованій операції в квантових системах. Якщо система є дворівневою (як у випадку спіна електрона), то квантові операції називатимемо квантовими елементами (вентилями) аналогічно як класичні логічні елементи.

Іншим унітарним оператором (квантовим елементом) є оператор Адамара, якому відповідає матриця $\hat{H}$

$$\hat{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.$$

Діючи оператором Адамара на основний стан $|0\rangle$, отримуємо: $\hat{H}\,|0\rangle = \psi$, аналогічно знаходимо: $\hat{H}\,|1\rangle = \chi$. Отже, інтерпретація елемента Адамара є такою: а) діючи на базові стани $|0\rangle$ та $|1\rangle$, елемент $\hat{H}$ створює суперпозицію станів ψ, χ; б) діючи на суперпозицію ψ, χ елемент H створює базові стани $|0\rangle, |1\rangle$.

Перевага квантових обчислень над класичними полягає у можливостях використання станів типу суперпозиції, які дозволяє створювати елемент Адамара. Більше того, стає можливою реалізація вимірювальних пристроїв, які дозволяють визначити чи система знаходиться в суперпозиції ψ, чи в ортогональній до неї суперпозиції χ. Діючи на стан квантової системи елементом Адамара, а відтак контролюючи чи знаходиться вона у стані $|0\rangle$, ефективно контролюємо чи була вона раніше в стані ψ.

Еволюція квантової системи характеризує неперервну часову залежність стану системи. Еволюція мусить бути задана за допомогою унітарних операторів, тобто таких, які зберігають довжину векторів. Звідси випливає означення: еволюція квантових систем є однопараметричною групою унітарних операторів. Параметром еволюції є час t.

Найбільш природним прикладом еволюції є т. зв. вільна еволюція, яку описує матриця:

$$U_0(t)=\begin{pmatrix}e^{2jt} & 0\\ 0 & e^{jt}\end{pmatrix}.$$

Для кожного значення t матриця є унітарною і, крім того, має властивість $U^{-1}(t)=U(-t)$.

Оскільки $e^{j\pi}=-1$, а $e^{2j\pi}=1$, то $U_0(\pi)=Z$, де Z – оператор Z Паулі. На підставі (2) можемо записати $Z\psi=\chi$, $Z\chi=\psi$. Отже, вільна еволюція неперервно змінює стани ψ і χ.

Різниця між квантовими та класичними системами полягає у тому, що класичні системи, які залишаються вільними, еволюють тривіально, тобто їх стан не змінюється в часі, а вільна еволюція квантових систем неперервно змінює стани ψ і χ.

Іншим прикладом унітарної еволюції є еволюція у присутності зовнішнього електромагнітного поля з частотою достосованою до різниці енергії між базовими станами $|0\rangle$ і $|1\rangle$. Така еволюція задана матрицею

$$U(t)=\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix}$$

Дана матриця є унітарною для кожного моменту часу з огляду на тригонометричну одиницю.

Вибираючи $t=\pi/2$, отримуємо: $U(\pi/2)=-jY$ (де Y – оператор Y Паулі). Відповідно до цього визначаємо: $U(\pi/2)|0\rangle=-|1\rangle$; $U(\pi/2)|1\rangle=0$. Отже, для вибраних моментів часу еволюція веде до "перекидання" спінів.

Еволюція U(t) у поєднанні з $U_0(t)$ дозволяє реалізувати елемент Адамара: діючи послідовно вільною еволюцією $U_0(\pi)$, а відтак $U(\pi/4)$, отримуємо елемент $\hat{H}$: $U(\pi/4)\cdot U_0(\pi)=\hat{H}$.

Проте тут слід згадати, що практична реалізація вищезгаданих елементів пов'язана з певними труднощами. Виявляється, що практично неможливо отримати короткі імпульси з точно визначеними часовими тривалостями і частотами. Чим точніше визначена тривалість імпульсу, тим більше "розмиття" частоти. Це спричинює похибки в реалізації квантових елементів і суттєво ускладнює побудову "квантових комп'ютерів".

3. Дво-qбітові квантові елементи. Оператори дво-qбітові $U:H_{(2)}\rightarrow H_{(2)}$ можна будувати з операторів типу $U=U_1\otimes U_2$, де U_1 та U_2 – одно-qбітові оператори, введені раніше ($U_i=H\rightarrow H$). Оператори вказаного вище типу діють на базові стани дво- qбітового простору (стани e_i) так, що оператор U_1 діє на перший співмножник тензорного добутку (який належить до першого qбіта), а оператор U_2 – на другий: $Ue_2=U_1\otimes U_2(|0\rangle\otimes|1\rangle)=(U_1(|0\rangle)\otimes(U_2(|1\rangle)$. У випадку ускладнених станів дія операторів визначається так: $U(e_0+e_1)=(Ue_0)+(Ue_1)$.

Зазначимо, що аналогічно як існували стани, котрі не можна було представити у вигляді: $\psi\otimes\chi$, так існують оператори (елементи), які не можна представити у вигляді $U=U_1\otimes U_2$. Такі елементи можна записати у вигляді: $U_1\otimes U_2+W_1\otimes W_2$.

Розглянемо дво-qбітовий оператор, який реалізує класичний елемент контрольованого (керованого) заперечення. Покажемо, що він може створювати ускладнені стани із базових станів.

Контрольоване заперечення (CNOT) є дво-бітовим логічним елементом, який має два входи і два виходи, і заперечує другий вхідний біт лише у випадку, коли перший вхідний біт є одиницею. Таблиця істинності елемента CNOT має вигляд:

Вхід		Вихід	
біт 1	біт 2	біт 1	біт 2
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Очевидно, що елемент CNOT є оборотний, тобто він дозволяє визначити значення вхідних бітів на підставі відомих вихідних. Тому, очевидно, існує його квантовий аналог, який теж є оборотним.

Для побудови квантового аналога елемента CNOT використаємо одно-qбітові оператори проекції, які не є унітарними. Оператор P відповідає проекції на стан $|0\rangle$, а оператор P^1 – проекції на стан $|1\rangle$, тобто $P=|0\rangle\cdot\langle 0|$, $P^1=|1\rangle\cdot\langle 1|$. Із даних операторів можна побудувати унітарні одно-qбітові оператори, наприклад: $B=P+jP^1$.

Твердження: квантовим аналогом оператора контрольованого заперечення є $CN=P\otimes I+P^1\otimes X$, де I – оператор ідентичності, X – оператор X Паулі.

Не наводячи проміжних математичних викладень, подаємо кінцевий результат дії квантового оператора CN на базові стани:

$$CN|0\rangle\otimes|0\rangle=|0\rangle\otimes|0\rangle;\ CN|1\rangle\otimes|0\rangle=|1\rangle\otimes|1\rangle;$$
$$CN|0\rangle\otimes|1\rangle=|0\rangle\otimes|1\rangle;\ CN|1\rangle\otimes|1\rangle=|1\rangle\otimes|0\rangle.$$

Отже, елемент CN діє аналогічно як і логічний елемент CNOT.

Покажемо можливість утворення ускладнених станів. Для цього використаємо елемент CNOT та елемент Адамара. Приймемо, що задано базовий дво-qбітовий стан $e_1=|0\rangle\otimes|0\rangle$. Діючи на перший qбіт елементом Адамара у вигляді $\hat{H}\otimes I$, отримуємо стан $\psi=\frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right]\otimes|0\rangle$. Відтак діючи елементом CNOT на отриманий стан ψ, отримуємо ускладнений стан $CN\psi=\frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle)$.

Отже, існують фізичні процеси, які утворюють ускладнені стани із станів неускладнених. В розглянутому випадку дія елемента на другий qбіт залежатиме від стану першого q біта, тобто спостерігається взаємний вплив qбітів. Розглянемо фізичну інтерпретацію даного явища. Нагадаємо, що зі спіном електрона зв'язаний магнітний момент, який створює навколо себе магнітне поле. Приймемо, що два електрони віддалені від себе на атомну відстань $d=10^{-10}$м. При цьому виявляється, що вплив магнітного моменту першого електрона на другий електрон є настільки сильним, що його можна спостерігати. Наближено можна вважати, що магнітне поле першого електрона векторно додається до зовнішнього поля, яке діє на другий електрон. Залежно від напряму спіна першого електрона це поле або збільшує, або зменшує значення напруженості магнітного поля, впливаючи тим самим на різницю енергії ΔE_2 базових станів другого електрона. Виявляється що цей вплив може спричинити: а) перекидання стану спіна другого електрона, якщо різниця енергії його станів реально дорівнює ΔE_2, тобто якщо стан першого спіна спричинив збільшення локального поля в околі другого електрона; б) незмінність стану спіна, якщо стан першого спіна зменшив різницю енергії рівнів спіна другого електрона.

Отже, маємо перекидання стану спіна другого електрона лише в тому випадку, коли перший електрон перебував у стані $|1\rangle$. Це і є експериментальна реалізація квантового елемента CN.

1. Cempel Cz.: Nanotechnologie, źródła i perspektywy, Nauka 1999, nr 3, Str. 178-186. 2. Grover L.K.: A fast quantum mechanical algorithm for databae search. Proceedings of the 28-th ACM Symposium on Theory of Computations, 1996, pp.212-219. 3. Gershenfield., Chuang L.:

Bulk spin-resonance quantum computation, Science, vol. 275, 1997, pp.350-356. 4. Marecki P.: Quantum Computers – Facts or Fiction, Academy of Computer Science and Management, Bielsko-Biała, 2001, pp.1-25. 5. Marecki P.: The Advantagees of Quantum Computation, Academy of Computer Science and Management, Bielsko-Biała, 2001, pp.-18. 6. Marecki P.: Quantum Gates, Academy of Computer Science and Management, Bielsko-Biała, 2001, pp.1-16. 7. MareckiP.: Quantum Circuits, Academy of Computer Science and Management, Bielsko-Biała, 2001, pp.1-25. 8. Sher P.: Polynomial-time algorithms for factorization and discrete logarithms on a quantum computer. Proceedings of the 35-th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994, P.124-134. 9. Węgrzyn S.: Informatics Science, Archiwum Informatyki Teoretycznej i Stosowanej, tom 11, z.2/1999, s.107-119. 10. Węgrzyn S., Klamka J.: Kantowe systemy informatyki, Instytut Informatyki Teoretycznej i Stosowanej PAN, Gliwice, 2000. 11. Węgrzyn S., Klamka J.: Quantum Computing, Archiwum Informatyki Teoretycznej i Stosowanej, tom 12, z.3/2000, pp.235-246. 12. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki, Studia Informatica, volume 21, number 1, 2000, str.15-45. 13. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki, Nauka, nr 3, 2000, str.71-82. 14. Węgrzyn S., Klamka J.: Informatyka kwantowa i jej miejsce w informatyce jako dyscyplinie naukowej, Studia Informatica, volume 22, number 1, 2001, str.11-27.