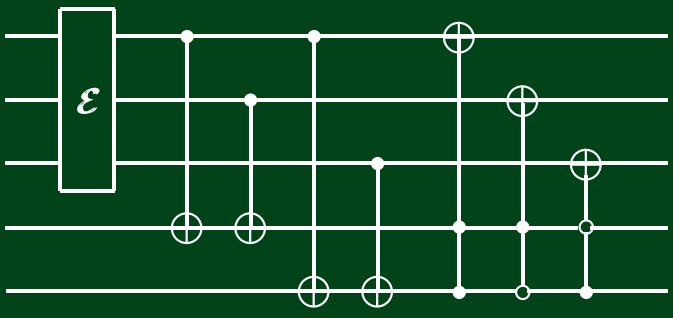
Т. КРОХМАЛЬСЬКИЙ

ВСТУП ДО КВАНТОВИХ ОБЧИСЛЕНЬ



Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Т. Є. Крохмальський

ВСТУП ДО КВАНТОВИХ ОБЧИСЛЕНЬ

Навчальний посібник

Львів
2018

УДК 530.145(075.8)
ББК 22.31я73
К 83

Рецензенти: д-р фіз.-мат. наук, проф. Ю. В. Козицький
(Університет Марії Кюрі-Склодовської в Любліні, Польща);
д-р фіз.-мат. наук, проф. Б. А. Лукіянець
(Національний університет "Львівська Політехніка")
д-р фіз.-мат. наук, ст.н.с. В. М. Симулик
(Інститут електронної фізики НАН України);

Рекомендовано
до друку Вченою радою Львівського національного університету
імені Івана Франка.
Протокол №15/2 від 24 лютого 2016 р.

Крохмальський Т. Є.
К 83 Вступ до квантових обчислень: Навчальний посібник. — Львів : ЛНУ імені Івана Франка, 2018. — 204 с.
ISBN 978-617-10-0362-0.

У посібнику висвітлено засадничі ідеї та поняття теорії і фізики квантових обчислень — одного з розділів квантової інформатики. Розглянуто квантовий процесор (комп'ютер) як квантовий регістр (ізольована система квантових бітів), на який послідовно діє квантова схема, складена з квантових логічних елементів (вентилів), що виконує програму обчислення деякої функції. Наведено приклади ефективних квантових алгоритмів. Розглянуто декілька відомих проектів фізичної реалізації квантових процесорів.

Для студентів, аспірантів фізико-математичних спеціальностей університетів, викладачів та науковців.

In this textbook, the basic ideas and concepts of the theory and physics of quantum computations — one branch of quantum information — are discussed. A quantum processor (computer) as a quantum register (isolated system of quantum bits) on which a quantum scheme (which consists of quantum logical elements (gates)) acts successively while performing calculation of a certain function is considered. Examples of suggested earlier effective quantum algorithms are presented. A few known projects of physical realization of quantum processors are considered.

The textbook is meant for students and post-graduates of physics and mathematics as well as for teachers and researchers.

УДК 530.145(075.8)
ББК 22.31я73

ISBN 978-617-10-0362-0

Зміст

Передмова

Розвиток технологій наукових досліджень мікросвіту та створення необхідних для цього приладів і устаткування дали змогу сьогодні маніпулювати окремими мікрочастинками і безпосередньо спостерігати різноманітні квантові ефекти. Водночас поглибилися теоретичні дослідження основ квантової механіки, що зумовило появу низки нових теоретичних розділів, як-от квантові обчислення, квантова криптографія, квантова теорія інформації, квантова телепортація та ін. Останнім часом ці розділи об'єднують в єдину дисципліну — квантову інформатику.

Теоретичні і експериментальні дослідження квантових обчислень породжують надію на побудову квантових процесорів, які дадуть змогу реалізувати спеціально створені квантові алгоритми з експонентним прискоренням в порівнянні з відповідними класичними.

Курси квантових обчислень чи квантової інформатики, як навчальні дисципліни, ввійшли до програм багатьох університетів країн Америки та Європи. Запроваджують також навчальні та дослідницькі спеціалізації з квантової інформатики.

Мета курсу — ознайомлення студентів з основами теорії і фізики квантових обчислень.

У першому розділі наведено основні положення і факти квантової механіки в обсязі, необхідному для подальшого викладу. У другому розділі розглянуто модель спіну 1/2, яка є засадничою моделлю для опису квантових обчислень. Третій розділ знайомить з основами класичних обчислень, обчислюваністю і складністю алгоритмів. У четвертому розділі описано базові "конструктивні" елементи квантового процесора (комп'ютера) — квантові біти, квантовий регістр, квантові логічні елементи (вентилі) та

засади функціонування квантових процесорів. Розглянуто деякі відомі квантові алгоритми. Описано квантові шуми в процесорах та методи усування їхнього впливу. У наступних розділах висвітлено проекти фізичної реалізації квантових процесорів — ансамблевий процесор на ядерних спінах великих органічних молекул, розчинених у рідинах, що керуються методами ядерного магнітного резонансу та процесор на лінійних пастках Пауля. Розглянуто також адіабатичний комп'ютер, збудований з квантових бітів, реалізованих надпровідниковими інтерферометрами.

Для вивчення запропонованого матеріалу потрібне знання університетських курсів квантової механіки та загальної фізики.

Автор глибоко вдячний І.О. Вакарчуку і В.М. Ткачуку за надання можливості читання цього курсу та плідні предметні дискусії з квантової інформатики. Щиро дякую також рецензентам Ю.В. Козицькому, Б.А. Лукіянцю та В.М. Симулику за критичне прочитання навчального посібника і важливі зауваження.

Вступ

Людина виконує обчислення дуже повільно і при цьому часто помиляється. Першим механічним пристроєм, який допомагав робити арифметичні дії, був абак, винайдений приблизно у 6 ст. до н.е. Від нього походять різноманітні рахівниці. У середині 17 ст. винайдено арифмометри — механічні пристрої із зубчатих коліс, які з деякими вдосконаленнями використовували майже до кінця 20 ст. Арифмометри самостійно виконували чотири арифметичні операції точно в десятковій основі. В першій половині 19 ст. англійський математик Чарльз Беббідж запропонував проект механічної різницевої цифрової обчислювальної машини, яка давала змогу обчислювати функції, апроксимуючи їх многочленами у методі скінченних різниць. Дослідникові вдалося збудувати тільки частину своєї машини, і аж 1991 року відтворено копію різницевої машини №2, виставлену в лондонському Музеї науки, яка бездоганно реалізувала задум автора. Однак головною заслугою Чарльза Беббіджа є ідея його аналітичної машини, яка була вже універсальною обчислювальною машиною і стала прообразом сучасних комп'ютерів. У 1941 р. німецький інженер Конрад Цузе сконструював першу електричну (релейну) машину Z3 із двійковим численням, яке запропонував Ляйбніц. Однак ця машина ще не була універсальною. У 1946 р. група дослідників фірми IBM (США) створила першу електронну обчислювальну машину ENIAC на електронних лампах. Такі машини були громіздкі та споживали дуже багато енергії.

Перша в Україні лампова ЕОМ із архітектурою фон Ноймана була збудована С.О. Лебедєвим у 1951 р. Архітектура фон Ноймана була розроблена групою вчених США за участі фон Ноймана у 1944-46 рр. і з того часу її використовують в усіх комп'ютерах.

ЕОМ другого покоління з'явилися у 1960 роках, у них електронні лампи замінили довговічними, компактними і енергоекономними транзисторами. Це вже були справді універсальні машини загального призначення. Комп'ютери третього (приблизно 1964 р.) і четвертого (приблизно 1970 р.) поколінь компонувалися з інтегральних мікросхем, кожна з яких містила багато тисяч напівпровідникових елементів (діодів, транзисторів і т.п.). Відтоді почався сучасний етап розвитку ЕОМ.

Зменшення розмірів елементів мікросхем (напр., транзисторів) підлягає відкритому емпірично в 1965 році Г.Муром (G.Moore — співзасновник компанії Intel) закону, згідно з яким кількість елементів на одиниці площі мікросхеми подвоюється кожних 24 місяці, тобто за експонентним законом. У 22 nm технології на одному кристалі мікросхеми розміщується понад два мільярди транзисторів. Закон Мура діє вже понад 45 років, однак, якщо розміри транзистора досягнуть розмірів атома, то його дія припиниться. Дослідники висловлюють передбачення, що закон Мура втратить силу з економічних причин, оскільки вартість технології також зростає експонентно, а час окупності нових технологій помітно збільшується. І справді впровадження 22 (2011) і 14 (2014) nm технологій відбулося з помітним відхиленням від закону Мура.

Отже, виникає запитання: чи будуть комп'ютери виконувати класичні алгоритми, якщо їхні базові елементи підлягатимуть квантовим, а не класичним законам? На початку 1980 років П.Беньоф довів існування гамільтоніанів, які забезпечать еволюцію квантової системи, яка відтворює класичне обчислення.

Приблизно тоді ж Р. Фейнман звернув увагу на те, що для систем із L частинок, кожна із яких може перебувати в m станах, треба $m^L = 2^{L \log_2 m}$ комірок пам'яті для запису всіх власних значень. Це означає експонентну залежність об'єму пам'яті комп'ютера і часу розрахунку від розміру системи. Р. Фейнман запропонував використати цю властивість для імітації станів інших квантових фізичних систем.

Із праць Д.Дойча 1985 року розпочався етап розвитку проектів квантових комп'ютерів (процесорів), які можуть суттєво перевершити класичні в ефективності обчислень.

Розділ 1

Елементи квантової механіки

З часів Галілея фізичні системи описують в термінах спостережуваних величин, числові значення яких встановлюють в процесі вимірювання зіставленням з відповідними загальновизнаними еталонами. В макроскопічних масштабах ці числа сприймаються як дійсні, тобто, вони творять неперервну множину. Теоретично спостережувана величина може характеризуватися кількома числами, які формують математичний об'єкт певної тензорної вимірності. Фізичні закони зміни цих спостережуваних записують рівняннями для відповідних математичних об'єктів. Їхні числові значення (як виміряні, так і теоретично спрогнозовані) залежать від **системи відліку** і тому характеризують не саму фізичну систему, а пару "фізична система–система відліку".

Дослідження в мікроскопічних масштабах виявили, що вимірювання деяких спостережуваних призводить до дискретних наборів їхніх значень, що назвали *квантуванням*, а системи з такими властивостями — *квантовими*. Численні спроби сформулювати фізичні закони в термінах безпосередньо вимірюваних значень виявилися безуспішними. Вихід знайдено в запровадженні цілком іншого опису стану і зображення спостережуваних.

Опис квантової системи запропоновано будувати у відповідному *просторі станів*, утвореному множиною функцій певного типу, який залежить від фізичної природи системи, а спостережувані — зображати *операторами* у цьому просторі. Зіставлення теоретично прогнозованих і експериментально вимірюваних значень задається *теоремами про вимірювання* і є суттєво складнішим, ніж у класичному описі. Прийняте в класичних вимірюваннях припущення про допустимість як завгодно малих масшта-

бів еталонів для квантових систем не справджується через співмірність еталонів із досліджуваними системами. Під час вимірювання виникає сильна взаємодія фізичної системи з "приладом", яка формує спільний заплутаний стан, тому результат вимірювання знову характеризує пару "фізична система–система відліку", з тим, що до "системи відліку" треба включити і вимірювальний "прилад".

Квантовий опис, по суті, прогнозує тільки результати вимірювань, тому твердження про те, що "система перебуває в стані" чи "її характеристики мають значення", варто відносити до **опису** системи, а не до її **абсолютних властивостей**.

Ізольована квантова система може перебувати в *чистому* чи *змішаному* станах. Чистий стан описують вектором (точніше, променем) у просторі станів системи. Множина (скінченна чи нескінченна) систем у чистому стані утворює *чистий ансамбль*. Вимірювання деякої динамічної характеристики (спостережуваної) в такому ансамблі дає набір дискретних значень, розподілених відповідно. Якщо ж вимірювання на всіх системах чистого ансамблю дає одне й те ж значення, то такий чистий стан називається *власним* станом цієї спостережуваної. Встановлено, що один і той самий власний стан може відповідати не одній, а кільком спостережуваним, тобто вимірювання кількох спостережуваних у цьому чистому ансамблі дає певне значення для кожної з них. Максимальний набір спостережуваних, що мають спільну множину власних станів, задає *повний опис системи*. Такий набір встановлюється експериментально, кількість спостережуваних у ньому дорівнює кількості ступенів свободи системи. Конкретний чистий стан позначається набором *квантових чисел* — числових значень спостережуваних, що задають повний опис системи.

У просторі станів системи спостережувані зображають лінійними ермітовими операторами, збудованими так, щоб спектри їхніх власних значень збігалися із спектрами значень, отриманими під час вимірювання. Всі оператори спостережуваних, які утворюють повний опис, повинні мати спільні власні функції, котрі описують відповідні власні стани, а отже — комутувати між собою.

Після вимірювання спостережуваної в чистому ансамблі, для якої цей чистий стан не є власним, може виникнути ансамбль си-

стем, кожна з яких перебуває в одному з власних станів спостережуваної. Вага кожного власного стану пропорційна квадрату модуля амплітуди ймовірності цього стану. Такий ансамбль називають *змішаним*. Змішаний ансамбль можна приготувати як із довільних (не обов'язково ортогональних) чистих станів системи з вагою, яка залежить від способу приготування, так і з довільних змішаних станів. Важливо, щоби після приготування кожна система ансамблю залишалася ізольованою. Стан такого ансамблю є *некогерентною суперпозицією* чистих станів, його описують *матрицею густини* в просторі станів системи, але не вектором (променем). Вимірювання спостережуваних, що дають повний опис цих систем у чистому стані, в даному випадку призводять до розподілу результатів із дисперсією, яку не можна звести до нуля.

Зміна станів ізольованих систем (у чистих та змішаних ансамблях) є наслідком гамільтонової часової еволюції чи процесів вимірювання. Часову еволюцію описують унітарним перетворенням вектора стану чи матриці густини, яке генерується гамільтоніаном системи через рівняння Шредингера чи рівняння Ліувілля.

Квантові стани фізичних систем, які взаємодіють із оточенням чи є підсистемами більших (складених) систем, описуються *редукованими* матрицями густини, і не зображаються змішаним ансамблем. Часові зміни підсистеми складеної системи чи системи, що взаємодіє з оточенням, вже не є унітарними. Таку еволюцію можна, зокрема, описати (дискретними) *квантовими перетвореннями* з відповідними *супероператорами*, що діють на редуковану матрицю густини. Формалізм квантових перетворень є досить загальним і дає змогу описувати також унітарні перетворення, процеси вимірювання і неунітарну еволюцію підсистем. Для ґрунтовнішого вивчення квантової механіки можна рекомендувати праці [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

1.1 Стани і вектори

Чисті стани ізольованих (замкнутих) мікроскопічних систем у квантовій механіці описують векторами лінійного простору $\mathcal{H}$ над полем комплексних чисел $\mathbb{C}$, які, за Діраком [3], позначають $|\psi\rangle$ і

називають *кет-векторами*. Лінійність простору означає, що для довільних $|\psi_1\rangle$, $|\psi_2\rangle \in \mathcal{H}$ і $c_1, c_2 \in \mathbb{C}$ існує вектор

$$|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle \in \mathcal{H}.$$

Це є вираженням фізичного *принципу суперпозиції*: якщо ізольована система може перебувати в станах $|\psi_1\rangle$ чи $|\psi_2\rangle$, то вона може перебувати і в стані їх *когерентної суперпозиції* $|\psi\rangle$. Вектор $c\,|\psi\rangle$ описує той самий стан, що і вектор $|\psi\rangle$. У лінійному просторі $\mathcal{H}$ існує нульовий вектор $\mathbf{0}$ такий, що для довільного $|\psi\rangle \in \mathcal{H}$

$$|\psi\rangle + \mathbf{0} = \mathbf{0} + |\psi\rangle = |\psi\rangle\,.$$

Вектори $|\psi_1\rangle, |\psi_2\rangle \ldots |\psi_N\rangle$ називаються лінійно незалежними якщо рівність

$$c_1 |\psi_1\rangle + c_2 |\psi_2\rangle + \ldots + c_N |\psi_N\rangle = \mathbf{0}$$

виконується тільки за умови $c_1 = c_2 = \ldots = c_N = 0$. Максимальна кількість N лінійно незалежних векторів простору $\mathcal{H}$ називається *вимірністю* цього простору[1]. Далі розглядатимемо тільки системи зі станами в скінченновимірних просторах $N{<}\infty$.

У просторі $\mathcal{H}$ можна ввести скалярний (внутрішній) добуток $\langle\varphi|\psi\rangle$ із такими властивостями:

а) ермітова симетрія

$$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*\,;$$

б) лінійність

$$|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle\,, \qquad \langle\varphi|\psi\rangle = c_1 \langle\varphi|\psi_1\rangle + c_2 \langle\varphi|\psi_2\rangle\,;$$
$$|\varphi\rangle = c_1 |\varphi_1\rangle + c_2 |\varphi_2\rangle\,, \qquad \langle\varphi|\psi\rangle = c_1^* \langle\varphi_1|\psi\rangle + c_2^* \langle\varphi_2|\psi\rangle\,;$$

в) позитивність

$$\langle\psi|\psi\rangle \in \mathbb{R}, \quad \langle\psi|\psi\rangle \geq 0,$$

притому, що рівність виконується тільки для $|\psi\rangle = \mathbf{0}$. Скалярний добуток, виражений через компоненти векторів, має вигляд:[2]

$$|\psi\rangle = \sum_i a_i |e_i\rangle, \quad |\phi\rangle = \sum_j b_j |e_j\rangle, \quad \langle\psi|\phi\rangle = \sum_j a_j^* b_j$$

[1] Над полем дійсних чисел вимірність цього простору дорівнюватиме $2N$.

[2] У математиці використовують також інші означення скалярного добутку, коли $\langle\psi|\phi\rangle = \sum_{j=1}^N a_j b_j^*$ чи $(\mathbf{a}, \mathbf{b}) = \sum_{j=1}^N a_j b_j$ (див., напр. [12, 13]).

(Комплексно-спряжені числа будемо позначати символом *, а ермітово-спряжені об'єкти — символом †.)

Об'єкти $\langle\psi|$, за Діраком, називають (див., напр.[3]) *бра-векторами*, вони є спряженими до $|\psi\rangle$ кет-векторів ($\langle\psi| = |\psi\rangle^\dagger$) і утворюють спряжений до $\mathcal{H}$ векторний простір, у якому можна побудувати опис системи, цілком еквівалентний опису в $\mathcal{H}$.

Нормою (довжиною) вектора $|\psi\rangle$ називають додатне дійсне число

$$||\psi\rangle| = \sqrt{\langle\psi|\psi\rangle} > 0. \tag{1.1}$$

Норма вектора має такі властивості:

$$|c\cdot|\psi\rangle| = |c|\cdot||\psi\rangle|,\ |\langle\varphi|\psi\rangle| \le ||\psi\rangle|\cdot||\varphi\rangle|,$$
$$||\psi\rangle + |\varphi\rangle| \le ||\psi\rangle| + ||\varphi\rangle|.$$

Оскільки $c\,|\psi\rangle$ для всіх $c{\neq}0 \in \mathbb{C}$ описують той самий фізичний стан, то прийнято вибирати c так, щоб $\langle\psi|\psi\rangle = 1$. Такі нормовані вектори з врахуванням фазового множника $\exp(i\alpha)$ називаються *променями* у векторному просторі, і саме вони описують чисті стани ізольованих систем.

Норма вектора (1.1) дає змогу запровадити *відстань між векторами* як норму вектора їх різниці:

$$D\left(|\psi\rangle, |\varphi\rangle\right) = ||\psi\rangle - |\varphi\rangle| = \sqrt{\langle\psi|\psi\rangle + \langle\varphi|\varphi\rangle - 2\mathrm{Re}\langle\psi|\varphi\rangle}, \tag{1.2}$$

яка має властивості:

$$D\left(|\psi\rangle, |\varphi\rangle\right) = D\left(|\varphi\rangle, |\psi\rangle\right),\ D\left(|\psi\rangle, |\psi\rangle\right) = 0,$$
$$D\left(|\psi\rangle, |\varphi\rangle\right) \le D\left(|\psi\rangle, |\chi\rangle\right) + D\left(|\chi\rangle, |\varphi\rangle\right).$$

Відстань між нормованими векторами спрощується до виразу;

$$D\left(|\psi\rangle, |\varphi\rangle\right) = ||\psi\rangle - |\varphi\rangle| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle\psi|\varphi\rangle}.$$

Очевидно, що тоді $D(|\psi\rangle, |\psi\rangle){=}0$, $D(|\psi\rangle, -|\psi\rangle){=}2$.

Відстань між векторами (1.2) породжує метрику векторного простору і робить його метричним простором. Однак вона неправильно описує відстань між станами системи, оскільки відстань

між векторами, що належать одному променю $|\varphi\rangle = \exp(i\alpha)|\psi\rangle$ і описують той самий стан,

$$D\left(|\psi\rangle, |\varphi\rangle\right) = \sqrt{2}\sqrt{1-\cos\alpha} = 2\left|\sin\frac{\alpha}{2}\right|,$$

загалом відмінна від нуля. Питання відстані між станами розглядають, зокрема, у працях [9, 11].

Два вектори $|\psi\rangle$ і $|\varphi\rangle$ називають ортогональними, якщо

$$\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle = 0.$$

У просторі $\mathcal{H}$ можна знайти N взаємно ортонормованих векторів $|e_i\rangle$ і спряжених до них $\langle e_i|$ $(i = 1, \ldots N)$

$$\langle e_i|e_j\rangle = \delta_{ij}, \tag{1.3}$$

які утворюють *базис* у цьому просторі, тобто, за допомогою них можна виразити будь-який вектор із $\mathcal{H}$ і спряжений до нього

$$|\psi\rangle = \sum_{i=1}^{N} c_i\,|e_i\rangle\,, \qquad \langle\psi| = \sum_{j=1}^{N} c_j^*\,\langle e_j|\,, \tag{1.4}$$

що для нормованих векторів дає

$$\langle\psi|\psi\rangle = \sum_{i,j=1}^{N} c_i c_j^*\,\langle e_j|e_i\rangle = \sum_{i,j=1}^{N} c_i c_j^*\delta_{ij} = \sum_{i=1}^{N}|c_i|^2 = 1. \tag{1.5}$$

Остання властивість називається *умовою повноти* (базису, в даному випадку) або *рівністю Парсеваля*, вона є узагальненням теореми Піфагора.

Зауважимо, що відстань між двома ортонормованими векторами $D\left(|\psi\rangle, |\varphi\rangle\right) = \sqrt{2}$.

N вимірний лінійний простір векторів $|\psi\rangle$ зі скалярним добутком $\langle\varphi|\psi\rangle$, повний за нормою (1.5) у квантовій механіці називають *простором станів системи*[3]. У математиці такі простори відомі також як *унітарні*.

[3] Лінійні векторні простори вимірності $N \to \infty$ називають гільбертовими.

Координати (компоненти) c_i вектора $|\psi\rangle$ в (1.4) можна виразити як скалярні добутки

$$c_i = \langle e_i|\psi\rangle\,, \qquad c_i^* = \langle\psi|e_i\rangle,$$

тому (1.5) можна записати як:

$$\langle\psi|\psi\rangle = \sum_{i=1}^{N} |\,\langle e_i|\psi\rangle\,|^2 = \sum_{i=1}^{N} \langle\psi|e_i\rangle\,\langle e_i|\psi\rangle\,.$$

Координати $c_j{=}\langle e_j|\psi\rangle$ вектора $|\psi\rangle$ в базисі $|e_j\rangle$ називають *амплітудами ймовірності*, їхні квадрати модуля $|\langle e_j|\psi\rangle|^2$ дорівнюють ймовірності знайти у систему в базисному стані $|e_j\rangle$ при проективному вимірюванні. Стовпець, складений із амплітуд ймовірності, називають *хвильовою функцією* (в даному базисі).

Якщо фізична система складається з підсистем A і B, стани яких належать до просторів $\mathcal{H}_A$ і $\mathcal{H}_B$ відповідно, то стан складеної системи AB лежить у просторі станів, що є тензорним добутком просторів $\mathcal{H}_{AB}{=}\mathcal{H}_A{\otimes}\mathcal{H}_B$. Ортонормований базис у цьому просторі можна побудувати як множину всіх тензорних добутків базисних векторів кожного з підпросторів $|e_{ij}\rangle_{AB}{=}|a_i\rangle_A{\otimes}|b_j\rangle_B$. Вимірність простору станів цієї складеної системи дорівнює $N_{AB}{=}N_AN_B$. За цим правилом легко збудувати простір станів системи, складеної з довільної кількості складових.

1.2 Спостережувані й оператори

У просторі станів можна ввести лінійне перетворення $\mathbf{A}$, що переводить вектор $|\psi\rangle \in \mathcal{H}$, загалом, в інший вектор $|\varphi\rangle \in \mathcal{H}$

$$|\varphi\rangle = \mathbf{A}\,|\psi\rangle\,. \tag{1.6}$$

Лінійність означає, що

$$\mathbf{A}(c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle) = c_1\mathbf{A}\,|\psi_1\rangle + c_2\mathbf{A}\,|\psi_2\rangle$$
$$(c_1\mathbf{A}_1 + c_2\mathbf{A}_2)|\psi\rangle = c_1\mathbf{A}_1|\psi\rangle + c_2\mathbf{A}_2|\psi\rangle.$$

Такі лінійні перетворення називають *лінійними операторами*. Розкладемо вектори $|\psi\rangle$ і $|\varphi\rangle$ за базисом (1.3)

$$|\varphi\rangle = \sum_{l=1}^{N} b_l \, |e_l\rangle \,, \qquad |\psi\rangle = \sum_{j=1}^{N} c_j \, |e_j\rangle \,,$$

тоді вираз (1.6) можна записати:

$$\sum_{l=1}^{N} b_l \, |e_l\rangle = \sum_{j=1}^{N} \mathbf{A} \, |e_j\rangle \, c_j. \tag{1.7}$$

Помноживши вираз (1.7) зліва на $\langle e_i|$, отримаємо

$$b_i = \sum_{j=1}^{N} \langle e_i| \, \mathbf{A} \, |e_j\rangle \, c_j = \sum_{j=1}^{N} A_{ij} c_j$$

матричне зображення оператора $\mathbf{A}=[A_{ij}]$ та векторів станів $|\varphi\rangle$ і $|\psi\rangle$, де $A_{ij} \equiv \langle e_i| \, \mathbf{A} \, |e_j\rangle$ — матричні елементи оператора $\mathbf{A}$, $b_i \equiv \langle e_i|\varphi\rangle$, $c_j \equiv \langle e_j|\psi\rangle$ — координати векторів $|\varphi\rangle$ і $|\psi\rangle$ у базисі $|e_i\rangle$ відповідно. Величини A_{ij}, b_i, c_j є комплексними числами.

Ермітово спряжений до $\mathbf{A}$ оператор $\mathbf{A}^\dagger$ вводять за правилом:

$$\langle \varphi| \, \mathbf{A} \, |\psi\rangle = \langle \psi| \, \mathbf{A}^\dagger \, |\varphi\rangle^* \,.$$

Вибравши вектори $|\varphi\rangle = |e_i\rangle$ і $|\psi\rangle = |e_j\rangle$, знаходимо зв'язок між матричними елементами операторів $\mathbf{A}$ і $\mathbf{A}^\dagger$ в цьому базисі

$$A_{ij} \equiv \langle e_i| \, \mathbf{A} \, |e_j\rangle = \langle e_j| \, \mathbf{A}^\dagger \, |e_i\rangle^* \equiv (A^\dagger_{ji})^*$$

чи

$$A^\dagger_{ij} = A^*_{ji},$$

якщо ж $A^*_{ij} = A_{ji}$, то $A^\dagger_{ij} = A_{ij}$, і тоді кажуть, що оператор дорівнює своєму спряженому $\mathbf{A} = \mathbf{A}^\dagger$. Такі оператори називають *самоспряженими* чи *ермітовими*. Оператори (матриці), для яких виконується $\mathbf{A} = -\mathbf{A}^\dagger$, називають *антиермітовими* чи *косоермітовими*. Довільну квадратну матрицю можна однозначно зобразити як суму ермітової і антиермітової. Добуток ермітових матриць $\mathbf{AB}$ є ермітовою матрицею тільки за умови $\mathbf{AB} = \mathbf{BA}$. Для довільної квадратної матриці $\mathbf{A}$ сума $\mathbf{A}+\mathbf{A}^\dagger$ і добуток $\mathbf{A}\mathbf{A}^\dagger, (\mathbf{A}^\dagger\mathbf{A})$ є ермітовими матрицями.

Вектори $|a_i\rangle$, дія на які оператора $\mathbf{A}$ зводиться до множення на комплексне (загалом) число a_i, називають *власними векторами* цього оператора, а числа a_i — його *власними значеннями*. Рівняння

$$\mathbf{A}\,|a_i\rangle = a_i\,|a_i\rangle$$

називають рівнянням на власні значення і власні вектори, його задовольняють також вектори $c\,|a_i\rangle$, де c — довільне комплексне число. Власні значення a_i самоспряженого оператора $\mathbf{A}$ є дійсними, а власні вектори $|a_i\rangle$, що відповідають різним власним значенням, є ортогональними. Матриці (оператори), в яких $a_i > 0, (a_i \geq 0)$, називаються додатно (невід'ємно) визначеними. Сукупність усіх (із врахуванням кратності) власних значень називається *спектром* відповідної матриці. Власні значення косоермітової матриці є уявними числами.

Якщо деякому власному значенню a_i відповідає m власних векторів $|a_i, k\rangle$, $k{=}1 \ldots m(i)$, таке власне значення називається $m(i)$-кратно виродженим. В цьому випадку кількість різних власних значень $\tilde{N}$ є меншою за вимірність простору N і $\sum_{i=1}^{\tilde{N}} m(i) = N$. Власні вектори вироджених станів ермітової (загалом, простої) матриці завжди можна ортогоналізувати до всіх інших власних векторів і отримати повну ортонормовану систему.

Вектори простору станів описують стани ізольованої фізичної системи, а самоспряжені оператори описують фізичні величини, що характеризують систему, тобто спостережувані. Вимірювання в експерименті фізичної величини, якій відповідає самоспряжений оператор $\mathbf{A}$, завжди призведе до значення, яке збігається з одним із власних значень цього оператора. Якщо ж вимірювання в чистому ансамблі дають одне й теж значення, то це значить, що система перебуває в стані, який є власним для цієї спостережуваної, а вектор цього стану є власним вектором її оператора. Згідно з означенням, спостережувані з набору, що задає повний опис, мають спільні власні стани, отже, відповідні їм оператори повинні мати спільні власні вектори. Такі оператори є переставними, тобто комутативними.

Два оператори комутують, якщо результат їхньої послідовної дії на довільний вектор не залежить від порядку дії, тобто

$$\mathbf{AB}\,|\psi\rangle = \mathbf{BA}\,|\psi\rangle\,,$$

тоді пишуть $\mathbf{AB} = \mathbf{BA}$.

Особливим (виділеним) оператором є *гамільтоніан* — оператор повної енергії фізичної системи, який разом з усіма переставними з ним операторами (інтегралами руху) задає її повний опис. Зображення векторів стану у базисі власних векторів гамільтоніана називається *енергетичним зображенням*.

Одночасне вимірювання фізичних величин (тобто вимірювання спостережуваних у чистому ансамблі), оператори яких не комутують, завжди призводить до результатів, що розподілені з певною дисперсією. Середньоквадратичні відхилення значень операторів таких спостережуваних:

$$\langle(\mathbf{A} - \langle\mathbf{A}\rangle)^2\rangle, \qquad \langle\mathbf{A}\rangle \equiv \langle\psi|\mathbf{A}|\psi\rangle$$

в деякому стані $|\psi\rangle$ пов'язані *співвідношенням невизначеності* із середнім значенням

$$\langle(\mathbf{A} - \langle\mathbf{A}\rangle)^2\rangle\langle(\mathbf{B} - \langle\mathbf{B}\rangle)^2\rangle \geq \frac{1}{4}\langle\mathbf{C}\rangle^2 \tag{1.8}$$

їх комутатора $\mathbf{C}$

$$[\mathbf{A}, \mathbf{B}] \equiv \mathbf{AB} - \mathbf{BA} = i\mathbf{C},$$

який також є ермітовим оператором, якщо $\mathbf{A}$ і $\mathbf{B}$ — ермітові. Із виразу (1.8) легко отримати співвідношення невизначеності Гайзенберга для операторів імпульсу і координати.

1.3 Унітарні оператори

Унітарними називають лінійні оператори $\mathbf{U}$, дія яких не змінює норму вектора

$$\begin{aligned} |\psi'\rangle &= \mathbf{U}\,|\psi\rangle\,, \qquad \langle\psi'| = \langle\psi|\,\mathbf{U}^\dagger \\ \langle\psi'|\psi'\rangle &= \langle\psi|\,\mathbf{U}^\dagger\mathbf{U}\,|\psi\rangle = \langle\psi|\psi\rangle\,. \end{aligned}$$

Це можливе, якщо $\mathbf{U}^\dagger\mathbf{U}{=}\mathbf{I}$, тобто $\mathbf{U}^\dagger{=}\mathbf{U}^{-1}$. Тут і далі $\mathbf{I}$ — одиничний оператор. Унітарні оператори зображають унітарними ма-

трицями. Побудувати матрицю оберненого оператора до унітарного дуже легко — достатньо її транспонувати і виконати комплексне спряження елементів. Унітарна матриця з дійсними елементами є ортогональною матрицею і зображає ортогональний оператор. Власні значення унітарного оператора за модулем дорівнюють одиниці, тобто, мають вигляд $e^{i\alpha}$, де α — деякі дійсні числа.

Нехай $\{|a_i\rangle\}$ і $\{|b_i\rangle\}$ — два різні повні ортонормовані базиси, тоді унітарний оператор $\mathbf{U}=\sum_{i=1}^{N}|a_i\rangle\langle b_i|$ виконує перехід між ними, тобто, $|a_j\rangle=\mathbf{U}|b_j\rangle$ чи $\sum_j|b_j\rangle\langle b_j|=\mathbf{U}^\dagger\left(\sum_i|a_i\rangle\langle a_i|\right)\mathbf{U}=\mathbf{I}$. Це дає змогу зобразити довільний вектор стану в різних базисах

$$|\psi\rangle=\sum_{j=1}^{N}\langle a_j|\psi\rangle|a_j\rangle=\sum_{j=1}^{N}\langle b_j|\psi\rangle|b_j\rangle, \tag{1.9}$$

тому легко знайти зв'язок між координатами

$$\langle a_i|\psi\rangle=\sum_{j=1}^{N}\langle a_i|b_j\rangle\langle b_j|\psi\rangle,$$

що є тривіальним наслідком повноти базису. Однак звідси випливає, що скалярні добутки $\langle a_i|b_j\rangle$ є елементами унітарної матриці, яка перетворює координати вектора в базисі $\{|b_i\rangle\}$ в координати цього вектора в базисі $\{|a_i\rangle\}$, а спряжений оператор здійснює обернене перетворення. Вираз (1.9) свідчить, що довільний чистий стан можна багатьма способами зобразити суперпозицією інших чистих станів. Такі суперпозиції є частковим випадком *когерентної суперпозиції* чистих, не обов'язково ортогональних, станів

$$|\psi\rangle=\sum_{j=1}^{n}c_j|\varphi_j\rangle,$$

де $n\le N$, а $\sum_{i,j=1}^{n}c_i^*c_j\langle\varphi_i|\varphi_j\rangle=1$.

Якщо одночасно з унітарним перетворенням векторів виконати унітарне перетворення оператора $\mathbf{UAU}^\dagger$, то його власні значення не зміняться. Якщо два (або більше) набори операторів, що задають повний опис системи, пов'язані певним унітарним перетворенням, то ці набори дають еквівалентні описи (є еквівалентними). Такі унітарні перетворення не змінюють стану системи, а встановлюють зв'язок між різними зображеннями, які вибирають

із огляду на зручність опису. До таких перетворень належать і переходи між різними системами відліку.

Однак унітарні оператори можуть описувати і зміну стану системи, зокрема, часову еволюцію ізольованих систем у чистому чи змішаному стані, таку еволюцію називають унітарною.

1.4 Проекційні оператори

Вимірювання є фізичним процесом, який може змінювати стан квантової системи, і цю зміну не завжди можна описати перетворенням у просторі станів. Якщо вимірювання вдається зобразити оператором, то такий оператор завжди буде неунітарним.

Певний клас вимірювань, які називають *проекційними* чи *проективними вимірюваннями*, можна формалізувати, запровадивши в просторі станів системи *проекційні оператори*.

Розклад вектора $|\psi\rangle$ (1.4) можна інтерпретувати як суму його проекцій на базисні вектори $|e_i\rangle$ за допомогою проектора (проекційного оператора, оператора проектування) на стан $|e_i\rangle$

$$\mathbf{P}_{e_i} \equiv |e_i\rangle \langle e_i| \,, \tag{1.10}$$

тобто

$$|\psi\rangle = \sum_{i=1}^{N} \mathbf{P}_{e_i} |\psi\rangle \,. \tag{1.11}$$

Оператори проектування задовольняють умову ортогональності

$$\mathbf{P}_{a_i}\mathbf{P}_{a_j} = \mathbf{P}_{a_i}\delta_{ij}. \tag{1.12}$$

Вони є самоспряженими $\mathbf{P}_{a_i}{=}\mathbf{P}_{a_i}^{\dagger}$, що безпосередньо випливає з означення (1.10), їхні власні значення рівні 0 або 1. Проектори на один стан називають *одновимірними* (*лінійними*).

Проекційні оператори на підпростір ортонормованих векторів $|a_i, k\rangle$ $(k = 1, \ldots, m(i))$ $m(i)$-кратно вироджених власних значень оператора $\mathbf{A}$ мають вигляд:

$$\mathbf{P}_{a_i} = \sum_{k=1}^{m(i)} |a_i, k\rangle \langle a_i, k| \,, \tag{1.13}$$

вони задовольняють умову (1.12).

Розбивши весь спектр оператора $\mathbf{A}$ на підмножини $\Omega_l = \{a_j\}$, які не перетинаються $\Omega_{l_1} \cap \Omega_{l_2} = \emptyset$, простір $\mathcal{H}$ можна поділити на підпростори h_l, утворені як лінійні оболонки базисних векторів $|a_j\rangle$ $a_j \in \Omega_l$, тоді проектор на підпростір h_l має вигляд:

$$\mathbf{P}_{h_l} \equiv \sum_{a_j \in \Omega_l} |a_j\rangle \langle a_j| .$$

Вираз (1.11) можна задати оператором

$$\mathbf{P}_a = \sum_{i=1}^{N} |a_i\rangle \langle a_i| = \mathbf{I}, \tag{1.14}$$

який, очевидно, є одиничним $\mathbf{I}$. Цей розклад називають також *ортогональним розкладом одиниці*, він є ще одним вираженням повноти базису (тут $\{|a_i\rangle\}$).

Розклад вектора в базисі, збудованому з ортонормованих власних векторів вироджених станів, записують так само через відповідний проекційний оператор (1.13)

$$|\psi\rangle = \sum_{i=1}^{\tilde{N}} \mathbf{P}_{a_i} |\psi\rangle = \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m(i)} |a_i, k\rangle \langle a_i, k| \psi\rangle,$$

зрозуміло, що для цього проектора вираз $\sum_{i=1}^{\tilde{N}} \mathbf{P}_{a_i} = \mathbf{I}$ також є ортогональним розкладом одиниці.

Оператор $\mathbf{Q} = \mathbf{I} - \mathbf{P}$ називається *ортогональним доповненням* проекційного оператора $\mathbf{P}$.

За допомогою проекційних операторів можна довільний оператор записати у *власному* (*спектральному*) зображенні

$$\mathbf{A} = \sum_{i=1}^{N} a_i |a_i\rangle \langle a_i| = \sum_{i=1}^{N} a_i \mathbf{P}_{a_i}, \tag{1.15}$$

його легко отримати, використавши ортогональний розклад одиниці (1.14) $\mathbf{IAI}$. Для оператора з виродженими власними значеннями спектральний розклад є цілком аналогічним:

$$\mathbf{A} = \sum_{i=1}^{\tilde{N}} a_i \mathbf{P}_{a_i} = \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m(i)} a_i |a_i, k\rangle \langle a_i, k|$$

Спектральне зображення оператора (1.15) є частковим випадком спектрального розкладу *простих* матриць [46].

Очевидно, що матриця оператора у власному зображенні є діагональною. Оператор $\mathbf{A}$, для якого виконується умова $\mathbf{A}^\dagger\mathbf{A} = \mathbf{A}\mathbf{A}^\dagger$, називається *нормальним*, ермітові та унітарні оператори є нормальними. Матриці нормальних операторів також називаються нормальними. Набір власних векторів нормальної матриці $\mathbf{A}$ є ортонормованим і збігається з набором власних векторів матриці $\mathbf{A}^\dagger$. Власні значення, що відповідають тому самому власному вектору, є комплексно спряженими. Матриці $\mathbf{A}$ і $\mathbf{A}^\dagger$ можна звести до діагонального виду $\mathbf{\Lambda}$ і $\mathbf{\Lambda}^*$ унітарною матрицею, складеною із власних векторів. Добуток $\mathbf{A}\mathbf{A}^\dagger = \mathbf{A}^\dagger\mathbf{A}$ є ермітовим оператором. Спектральне зображення нормальної матриці має вигляд (1.15).

Спектральне зображення оператора дає змогу отримати

$$\mathbf{A}^k = \sum_{i=1}^{N} a_i^k |a_i\rangle\langle a_i|. \tag{1.16}$$

Із розкладу в ряд Тейлора функції $f(x)$ знаходимо вираз для функції від простої матриці, що є матрицею того ж розміру:

$$f(\mathbf{A}) = \sum_{i=1}^{N} f(a_i)|a_i\rangle\langle a_i|, \tag{1.17}$$

яка існує, якщо існує функція $f(a_i)$ для всіх a_i. Зауважимо, що в означення (1.17) входять всі власні функції оператора $\mathbf{A}$ навіть ті, для яких $a_i = 0$ аби існувала функція $f(0)$. Тоді як у розклад (1.16) реальний вклад дають тільки функції, що відповідають відмінним від нуля власним значенням. Простір, утворений такими функціями, називають *носієм ермітового оператора* $\mathbf{A}$.

Означення функцій від загальніших матриць є складнішою задачею (див., напр. [46]).

1.5 Унітарна еволюція квантових систем

Картина Шредингера. Часова еволюція ізольованої квантової системи або чистого ансамблю в просторі станів у шредингеровій картині задають постулативно (диференціальним) рівнянням Шредингера для вектора стану

$$i\hbar\frac{d}{dt}\,|\psi(t)\rangle = \mathcal{H}\,|\psi(t)\rangle\,, \tag{1.18}$$

в якому $\mathcal{H}$ — оператор Гамільтона (гамільтоніан) є самоспряженим оператором повної енергії системи. Оператори спостережуваних у цій картині (формі динаміки) залишаються незмінними. Далі сталу $\hbar = h/(2\pi)$ покладемо рівною одиниці і запишемо рівняння (1.18) у вигляді:

$$\frac{d}{dt}\,|\psi(t)\rangle = -i\mathcal{H}\,|\psi(t)\rangle\,.$$

Інфінітизимальну зміну вектора стану у випадку незалежного від часу гамільтоніана виразимо

$$|\psi(t+dt)\rangle \approx \mathbf{U}(dt)\,|\psi(t)\rangle$$

через оператор унітарної інфінітизимальної еволюції

$$\mathbf{U}(dt) \approx \mathbf{I} - i\mathcal{H}dt, \qquad \mathbf{U}^\dagger(dt) \approx \mathbf{I} + i\mathcal{H}dt,$$
$$\mathbf{U}(dt)\mathbf{U}^\dagger(dt) = \mathbf{U}^\dagger(dt)\mathbf{U}(dt) = \mathbf{I} + O(dt^2).$$

Еволюція ізольованої системи або чистого ансамблю за скінченний проміжок часу у випадку, коли гамільтоніан не залежить від часу, описують унітарним оператором еволюції

$$\mathbf{U}(t) = \lim_{n\to\infty}\left(\mathbf{I} - i\mathcal{H}\frac{t}{n}\right)^n = \exp(-i\mathcal{H}t), \quad \mathbf{U}^\dagger(t) \equiv \exp(i\mathcal{H}t)$$
$$|\psi(t)\rangle = \mathbf{U}(t)\,|\psi(0)\rangle = \exp(-i\mathcal{H}t)\,|\psi(0)\rangle\,. \quad (1.19)$$

Запишемо довільний вектор початкового стану ізольованої системи в енергетичному зображенні:

$$|\psi(0)\rangle = \sum_j c_j\,|E_j\rangle\,, \quad \mathcal{H}\,|E_j\rangle = E_j\,|E_j\rangle\,,$$

тоді еволюцію такої системи можна описати виразами:

$$|\psi(t)\rangle = \exp(-i\mathcal{H}t)\,|\psi(0)\rangle = \exp(-i\mathcal{H}t)\sum_j c_j\,|E_j\rangle$$
$$= \sum_j c_j \exp(-iE_jt)\,|E_j\rangle \sim \sum_j c_j|\tilde{E}_j\rangle.$$

Останнє співвідношення виражає еквівалентність усіх базисних векторів відносно фазового множника, всі вони належать до одного (базисного) променя. Тобто, початкова суперпозиція базисних

променів у процесі еволюції ізольованої системи залишається незмінною. Зовсім інакшою є еволюція підсистем складеної системи.

Картина Гайзенберга. Унітарна еволюція системи в картині Гайзенберга переноситься на оператори спостережуваних, а вектори стану залишаються незмінними. Така еволюція здійснюється тими ж унітарними операторами (1.19), що і в картині Шредингера

$$\mathbf{A}(t) = \mathbf{U}^{\dagger}(t)\mathbf{A}(0)\mathbf{U}(t),$$

або в диференціальній формі

$$i\frac{d}{dt}\mathbf{A}(t) = \mathbf{A}(t)\mathcal{H} - \mathcal{H}\mathbf{A}(t) = [\mathbf{A}(t), \mathcal{H}]\,.$$

Такий опис еволюції стосується як чистих, так і змішаних ансамблів — для останніх незмінною залишається матриця густини.

Картина Дірака (зображення взаємодії). Зображення взаємодії зручно використовувати тоді, коли гамільтоніан системи можна записати як суму двох доданків

$$\mathcal{H} = \mathcal{H}^{(0)} + \mathcal{H}^{(1)}(t),$$

а для першого з них $\mathcal{H}^{(0)}$ відомо повний розв'язок задачі на власні функції і власні значення, тобто, відомо оператор еволюції $\mathbf{U}(t) = \exp(-i\mathcal{H}^{(0)}t)$. Тоді рівняння Шредингера для вектора стану $|\psi(t)\rangle = \exp(-i\mathcal{H}^{(0)}t)|\psi_{int}(t)\rangle$ переходить у рівняння:

$$i\frac{d}{dt}|\psi_{int}(t)\rangle = \mathcal{H}^{(1)}_{int}(t)|\psi_{int}(t)\rangle,$$
$$\mathcal{H}^{(1)}_{int}(t) \equiv \exp\left(i\mathcal{H}^{(0)}t\right)\mathcal{H}^{(1)}(t)\exp\left(-i\mathcal{H}^{(0)}t\right).$$

1.6 Змішаний ансамбль

Розглянемо ізольовану систему з простором станів $\mathcal{H}$ вимірності N, яка може перебувати, зокрема, в станах $|\varphi_i\rangle,\ 1 \le i \le n,\ n \le N$ нормованих, але не обов'язково ортогональних. Згідно принципу суперпозиції система може бути і в чистому стані, що є когерентною суперпозицією цих станів

$$|\psi\rangle = \sum_{i=1}^{n} c_i |\varphi_i\rangle,$$

$$\langle\psi|\psi\rangle = \sum_{i,j=1}^{n} c_i c_j^* \langle\varphi_j|\varphi_i\rangle = \sum_{l=1}^{N} \Big| \sum_{i=1}^{n} c_i f_{il} \Big|^2 = 1, \tag{1.20}$$

де використано розклад векторів $|\varphi_i\rangle$ за повним ортонормованим базисом $|\varphi_i\rangle = \sum_{j=1}^{N} f_{ij}|e_j\rangle$.

Нехай маємо набір $K (K \gg N)$ однакових систем, k_i з яких перебувають у стані $|\varphi_i\rangle$, очевидно, що $\sum_{i=1}^{n} k_i = K$. Якщо кількість систем прямує до нескінченності $K \to \infty$, то $k_i/K \to w_i$, тоді частку систем w_i в стані $|\varphi_i\rangle$ можна інтерпретувати як ймовірність знайти довільно взяту систему в цьому стані. Такий набір систем називають *змішаним ансамблем*, його стан не можна зобразити вектором (променем) стану, а тільки *оператором* (*матрицею*) *густини*, який у цьому випадку має вигляд:

$$\boldsymbol{\rho} = \sum_{i=1}^{n} w_i |\varphi_i\rangle\langle\varphi_i|, \quad w_i > 0, \quad \sum_{i=1}^{n} w_i = 1. \tag{1.21}$$

Матриця густини має такі властивості:

1) ермітовості: $\boldsymbol{\rho} = \boldsymbol{\rho}^\dagger$,

2) одиничності сліда: $\mathrm{Sp}\,(\boldsymbol{\rho}) \equiv \sum_{k=1}^{N} \langle e_k|\boldsymbol{\rho}|e_k\rangle = \sum_{i=1}^{n} w_i = 1$,

3) додатновизначеності: $\langle\chi|\boldsymbol{\rho}|\chi\rangle = \sum_{i=1}^{n} w_i |\langle\chi|\varphi_i\rangle|^2 > 0$ для довільного $|\chi\rangle$.

З означення (1.21) зауважуємо, що матриця густини позбавлена неоднозначності, пов'язаної з фазовим множником, характерної для вектора стану.

Розклавши вектори $|\varphi_i\rangle$ як в (1.20), отримаємо зображення матриці густини в цьому базисі:

$$\boldsymbol{\rho} = \sum_{i=1}^{n} w_i \sum_{j,l=1}^{N} f_{ij} f_{il}^* |e_j\rangle\langle e_l| = \sum_{j,l=1}^{N} \rho_{jl} |e_j\rangle\langle e_l|,$$

де матриця $[\rho_{ij}]$ є ермітовою, $\rho_{ii} \geq 0$, $\sum_{i=1}^{N} \rho_{ii} = 1$. Перехід до іншого ортонормованого базису буде звичайним унітарним перетворенням.

Матриця густини системи з N–вимірним простором станів містить не більше ніж N^2 дійсних параметрів.

Опис за допомогою матриці густини є досить загальним, він передбачає, зокрема, і опис чистого стану, для якого

$$\boldsymbol{\rho} = |\psi\rangle\langle\psi| = \sum_{i,j=1}^{n} c_i c_j^* \, |\varphi_i\rangle\langle\varphi_j| \tag{1.22}$$

має очевидну характерну властивість *ідемпотентності*

$$\boldsymbol{\rho}^2 = |\psi\rangle\langle\psi||\psi\rangle\langle\psi| = \boldsymbol{\rho}.$$

В повному ортонормованому базисі

$$\boldsymbol{\rho} = \sum_{l,m=1}^{N} \rho_{lm} |e_l\rangle\langle e_m|, \qquad \rho_{lm} \equiv \sum_{i,j=1}^{n} c_i c_j^* f_{il} f_{jm}^*,$$

ця властивість має форму $[\rho_{lm}]^2{=}[\rho_{lm}]$. У змішаному стані матриця густини не є ідемпотентною $\boldsymbol{\rho}^2{\neq}\boldsymbol{\rho}$ чи $[\rho_{lm}]^2{\neq}[\rho_{lm}]$.

Припустимо тепер, що стани $|\varphi_i\rangle$ є ортогональними, тоді в цьому зображенні матриця густини змішаного стану (1.21) буде діагональна, а матриця густини чистого стану (1.22) міститиме позадіагональні інтерференційні елементи. Варто зауважити, що цілком некогерентна суміш (1.21) станів $|\varphi_i\rangle$ за допомогою унітарного перетворення може бути зображена як частково когерентна суміш інших станів, тобто, міститиме позадіагональні інтерференційні члени, але її не можна зобразити цілком когерентною суперпозицією (чистим станом).

Матриця густини, як і всі інші ермітові оператори, у власному зображенні є діагональною

$$\boldsymbol{\rho} = \sum_{i=1}^{N} \lambda_i \, |\lambda_i\rangle \, \langle\lambda_i| \, ,$$

а її власні значення, внаслідок (1.21), задовільняють умови

$$0 \leq \lambda_i \leq 1, \qquad \sum_{i=1}^{N} \lambda_i = 1.$$

Однак власні стани матриці густини не мають важливого фізичного змісту, більш того, одна й та ж матриця густини може бути зображена кількома діагональними виразами. Це пов'язано з неоднозначністю утворення змішаних станів, які можуть формуватися як чистими, так і різними змішаними станами. Довільний змішаний ансамбль можна утворити безліччю способів з інших змішаних і чистих ансамблів. При цьому між цими зображеннями існують певні співвідношення.

Нехай той самий змішаний стан можна зобразити різними некогерентними суперпозиціями, тобто,

$$\boldsymbol{\rho} = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| = \sum_{j=1}^{m} q_j |\varphi_j\rangle\langle\varphi_j|, \tag{1.23}$$

де ваги задовольняють звичайним умовам $0 < p_i < 1$, $\sum_{i=1}^{n} p_i = 1$; $0 < q_j < 1$, $\sum_{j=1}^{m} q_j = 1$, а кількість станів n і m не обов'язково рівна. Таке зображення можливе тільки для станів, пов'язаних унітарним перетворенням

$$\sqrt{p_i}|\psi_i\rangle = \sum_j U_{ij}\sqrt{q_j}|\varphi_j\rangle, \quad \sqrt{p_i}\langle\psi_i| = \sum_j \sqrt{q_j}\langle\varphi_j|U^{\dagger}_{ji}, \tag{1.24}$$

де $1 \le j \le m$, якщо $m > n$ і $1 \le j \le n$, якщо $m \le n$, меншу множину векторів доповнюють нульовими векторами. Справді, нехай виконуються співвідношення (1.24), тоді

$$\begin{aligned}\sum_i p_i |\psi_i\rangle\langle\psi_i| &= \sum_i \sum_{j_1} U_{ij_1}\sqrt{q_{j_1}}|\varphi_{j_1}\rangle \sum_{j_2} \sqrt{q_{j_2}}\langle\varphi_{j_2}|U^{\dagger}_{j_2 i} \\ &= \sum_{j_1, j_2} \sqrt{q_{j_1} q_{j_2}}|\varphi_{j_1}\rangle\langle\varphi_{j_2}| \sum_i U^{\dagger}_{j_2 i} U_{ij_1} = \sum_j q_j |\varphi_j\rangle\langle\varphi_j|.\end{aligned}$$

Нехай тепер для оператора густини виконується співвідношення (1.23), яке, запровадивши позначення $|\tilde{\psi}_i\rangle \equiv \sqrt{p_i}|\psi_i\rangle$ і $|\tilde{\varphi}_i\rangle \equiv \sqrt{q_i}|\varphi_i\rangle$, запишемо так:

$$\boldsymbol{\rho} = \sum_{i=1}^{n} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{j=1}^{m} |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|. \tag{1.25}$$

З іншого боку оператор густини, як будь-який ермітів оператор, можна зобразити як спектральний розклад

$$\boldsymbol{\rho} = \sum_{k=1}^{l} \lambda_k |k\rangle\langle k| \equiv \sum_{k=1}^{l} |\tilde{k}\rangle\langle\tilde{k}|, \quad 0 < \lambda_k < 1,$$

де $|\tilde{k}\rangle \equiv \sqrt{\lambda_k}|k\rangle$ — ненормовані взаємно ортогональні вектори. Нехай вимірність l носія оператора густини і кількості векторів у розкладах (1.23) чи (1.25) співвідносяться $l < m < n$. Якщо деякий вектор $|\chi\rangle$ із простору станів системи є ортогональним до всіх власних векторів оператора густини $\langle\chi|k\rangle = 0$, то він ортогональний і до всіх векторів $|\psi_i\rangle$ і $|\varphi_j\rangle$, оскільки

$$0 = \langle\chi|\boldsymbol{\rho}|\chi\rangle = \sum_{i=1}^{n} \langle\chi|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\chi\rangle = \sum_{i=1}^{n} |\langle\chi|\tilde{\psi}_i\rangle|^2.$$

Отже, вектори $|\psi_i\rangle$ і $|\varphi_j\rangle$ належать до носія оператора густини і їх можна розкласти за ортогональним базисом $|k\rangle$

$$|\tilde{\psi}_i\rangle = \sum_{k=1}^{l} c_{ik} |\tilde{k}\rangle,$$

а це дає змогу записати вирази (1.23) і (1.25) у вигляді:

$$\sum_{k=1}^{l} |\tilde{k}\rangle\langle\tilde{k}| = \sum_{k_1 k_2} \sum_{i=1}^{n} c_{ik_1} c^*_{ik_2} |\tilde{k}_1\rangle\langle\tilde{k}_2|.$$

Оскільки оператори $|\tilde{k}_1\rangle\langle\tilde{k}_2|$ лінійно незалежні, то $\sum_{i=1}^{n} c_{ik_1} c^*_{ik_2} = \delta_{k_1 k_2}$. Прямокутна матриця $[c_{ik}]$, $1 \leq i \leq n$, $1 \leq k \leq l$ складається з l ортонормованих стовпців вимірності n і $l < n$. Її можна доповнити $n-l$ стовпцями, ортогональними між собою і до всіх заданих стовпців. Отримана квадратна $n \times n$ матриця $[V_{ik}]$ буде унітарною. Множину із l власних векторів $|k\rangle$ доповнюють $n-l$ нульовими векторами. Аналогічну $m \times m$ матрицю $[W_{jk}]$ можна отримати для набору векторів $\{|\varphi_j\rangle\}$, що дає змогу отримати зв'язок

$$|\tilde{\psi}_i\rangle = \sum_k V_{ik} \sum_j W^\dagger_{kj} |\tilde{\varphi}_j\rangle = \sum_j \sum_k V_{ik} W^\dagger_{kj} |\tilde{\varphi}_j\rangle = \sum_j U_{ij} |\tilde{\varphi}_j\rangle$$

як унітарне перетворення.

Розглянемо тепер унітарну еволюцію ізольованої системи, що перебуває в змішаному стані. З означення оператора густини легко встановити, що його зміна в картині Шредингера задається диференціальним *рівнянням Ліувіля*:

$$i\frac{d}{dt}\boldsymbol{\rho}(t) = [\mathcal{H}, \boldsymbol{\rho}] = \mathcal{H}\boldsymbol{\rho} - \boldsymbol{\rho}\mathcal{H}. \tag{1.26}$$

Для систем із незалежним від часу гамільтоніаном зміну за скінченний проміжок часу можна описати унітарним оператором

$$\boldsymbol{\rho}(t) = \mathbf{U}(t)\boldsymbol{\rho}(0)\mathbf{U}^{\dagger}(t) = \exp(-i\mathcal{H}t)\boldsymbol{\rho}(0)\exp(i\mathcal{H}t) \tag{1.27}$$

Зауважимо, що стан, який є некогерентною суперпозицією власних станів гамільтоніана $\boldsymbol{\rho}(0) = \sum_i w_i |E_i\rangle\langle E_i|$, не змінюється з часом $\boldsymbol{\rho}(t) = \boldsymbol{\rho}(0)$. Нескладно записати рівняння Ліувіля для унітарної еволюції матриці густини ізольованої системи в картині взаємодії

$$\begin{aligned} i\frac{d}{dt}\boldsymbol{\rho}_{int}(t) &= \mathcal{H}^{(1)}_{int}(t)\boldsymbol{\rho}_{int}(t) - \boldsymbol{\rho}_{int}(t)\mathcal{H}^{(1)}_{int}(t), \\ \boldsymbol{\rho}(t) &\equiv \exp\left(-i\mathcal{H}^{(0)}t\right)\boldsymbol{\rho}_{int}(t)\exp\left(i\mathcal{H}^{(0)}t\right). \end{aligned} \tag{1.28}$$

Позначення тут ті ж, що і в попередньому підрозділі.

Зрозуміло, що рівняння унітарної еволюції (1.26) – (1.28) стосуються описаних вище як чистих, так і змішаних станів, оскільки вони відповідають станам чистих та змішаних ансамблів **ізольованих** систем. Хоча підсистема великої системи також перебуває в змішаному стані (у своєму підпросторі), однак її часова еволюція не є унітарною і потребує значно складнішого опису.

Суттєва відмінність між чистим і змішаним станами полягає в тому, що для чистого стану можна знайти повний набір спостережуваних, кожна з яких має точне власне значення, а в змішаному стані жодна зі спостережуваних не має точного значення і характеризується тільки середнім значенням. Тому й кажуть, що чистий стан є інформаційно повнішим, ніж змішаний.

Змішаними ансамблями зручно описувати різноманітні системи, наприклад, пучки неполяризованих фотонів, множини станів

ядерних спінів молекул, множини збуджених атомів, що випромінюють некогерентне світло та багато інших об'єктів. Зображення матриці густини найчастіше використовують у квантовій статистичній механіці для опису станів макроскопічних систем. Далі розглянемо утворення змішаного ансамблю в результаті селективних проективних вимірювань деякої спостережуваної.

Квантова система з початково чистого стану під впливом взаємодії з оточенням переходить у змішаний стан, такий процес називають *декогеренцією*. Встановлено, що цей процес відбувається тим швидше чим більша система.

1.7 Складені системи

Розглянемо деяку ізольовану систему, що складається з двох підсистем A і B. Її простір станів є тензорним добутком просторів цих підсистем $\mathcal{H}{=}\mathcal{H}_A{\otimes}\mathcal{H}_B$ вимірності $N{=}N_AN_B$. У випадку, коли підсистеми не взаємодіють між собою, і кожна з них перебуває в чистому стані, вектор стану цілої системи є тензорним добутком векторів станів підсистем

$$|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B. \tag{1.29}$$

Якщо хоча б одна підсистема перебуває в змішаному стані, то описувати цілу систему треба в термінах матриці густини, яка є тензорним добутком матриць густини цих невзаємодіючих підсистем

$$\boldsymbol{\rho} = \boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B. \tag{1.30}$$

Такі стани цілої складеної системи називають *сепарабельними*[4].

Стани, які не можна зобразити як прямий добуток (1.29) чи (1.30), називають *заплутаними* станами підсистем A і B чи *несепарабельними* станами цілої системи. Заплутування є наслідком кореляцій між підсистемами, зумовленими їхньою взаємодією.

[4]Сепарабельність станів квантових систем не треба плутати із сепарабельністю гільбертового простору. Гільбертів простір є сепарабельним, якщо в ньому можна запровадити зліченний базис. Майже всі гільбертові простори, які розглядаються в квантовій механіці, є сепарабельними.

Нехай $|a_i\rangle$ і $|b_j\rangle$ — базиси в $\mathcal{H}_A$ і $\mathcal{H}_B$ відповідно, тоді вектор довільного чистого стану в $\mathcal{H}$ можна розкласти:

$$|\psi\rangle = \sum_{i=1}^{N_A}\sum_{j=1}^{N_B} c_{ij}\,|a_i\rangle \otimes |b_j\rangle\,, \qquad \sum_{i=1}^{N_A}\sum_{j=1}^{N_B} |c_{ij}|^2 = 1. \tag{1.31}$$

А матриця густини цього чистого стану має такий розклад у вибраному базисі:

$$\boldsymbol{\rho} = |\psi\rangle\langle\psi| = \sum_{i_1,j_1}\sum_{i_2,j_2} c_{i_1 j_1} c^*_{i_2 j_2}\,|a_{i_1}\rangle\,\langle a_{i_2}| \otimes |b_{j_1}\rangle\,\langle b_{j_2}|.$$

Якщо підсистеми взаємодіють між собою, то стан окремої підсистеми вже не можна описати вектором стану, оскільки підсистеми не є ізольованими. Такі стани підсистем є змішаними і описують їх за допомогою *редукованих операторів густини*

$$\begin{aligned}\boldsymbol{\rho}_A &= \mathrm{S}p_B\left(|\psi\rangle\,\langle\psi|\right) = \sum_{i_1,i_2}\sum_{j} c_{i_1 j} c^*_{i_2 j}\,|a_{i_1}\rangle\,\langle a_{i_2}|\,,\\ \boldsymbol{\rho}_B &= \mathrm{S}p_A\left(|\psi\rangle\,\langle\psi|\right) = \sum_{j_1,j_2}\sum_{i} c_{i j_1} c^*_{i j_2}\,|b_{j_1}\rangle\,\langle b_{j_2}|\,.\end{aligned} \tag{1.32}$$

Змішаний стан виникає у разі усереднення саме унаслідок заплутування станів підсистем A і B.

Кожен із операторів густини (1.32) є

1) самоспряжений $\boldsymbol{\rho}_A^\dagger = \boldsymbol{\rho}_A$;

2) додатновизначений, справді для довільного $|\varphi\rangle_A$

$$_A\langle\varphi|\,\boldsymbol{\rho}_A\,|\varphi\rangle_A = \sum_{j=1}^{N_B} |\sum_{i=1}^{N_A} c_{ij A}\,\langle\varphi|a_i\rangle\,|^2 > 0;$$

3) $\mathrm{Sp}\,(\boldsymbol{\rho}_A) = 1$.

Додатновизначеність цього оператора густини означає, що його власні значення $0{\leq}\lambda_i{\leq}1$, а з властивості 3) слідує $\sum_{i=1}^{N_A}\lambda_i{=}1$.

Загалом, якщо ізольована система перебуває у стані з матрицею густини $\boldsymbol{\rho}$, редуковані матриці густини підсистем A чи B отримують аналогічно

$$\boldsymbol{\rho}_A = \mathrm{Sp}_B(\boldsymbol{\rho}), \qquad \boldsymbol{\rho}_B = \mathrm{Sp}_A(\boldsymbol{\rho}),$$

вони задовольняють наведені вище умови 1)–3).

Матриці густини (1.21) і (1.32) описують суттєво відмінні стани: перша — змішані стани ансамблю ізольованих систем, тоді як друга — змішані стани якоїсь однієї підсистеми великої системи, такі стани називають *невласними змішаними станами*. Часова еволюція цих різних типів змішаних станів суттєво відмінна.

Розглянемо побіжно структуру операторів фізичних величин складеної системи. Здебільшого оператори мають *адитивний* характер, тобто, формально їх записують як суму

$$\mathbf{G} = \mathbf{G}_A + \mathbf{G}_B$$

хоча точніше їх треба писати як *кронекерову суму*

$$\mathbf{G} = \mathbf{G}_A \otimes \mathbf{I}_B + \mathbf{I}_A \otimes \mathbf{G}_B,$$

де $\mathbf{G}$, $\mathbf{G}_A$, $\mathbf{G}_B$ — оператор деякої величини цілої системи і її складових відповідно. Оператори $\mathbf{G}_A$ та $\mathbf{G}_B$ залежать тільки від змінних відповідних підсистем. Особливу структуру має гамільтоніан

$$\mathcal{H} = \mathcal{H}_A \otimes \mathbf{I}_B + \mathbf{I}_A \otimes \mathcal{H}_B + \mathcal{H}_{AB},$$

який окрім гамільтоніанів підсистем містить доданок $\mathcal{H}_{AB}$, що описує взаємодію між ними. Якщо ж взаємодія відсутня, то гамільтоніан також є кронекеровою сумою. Гамільтоніани кожної підсистеми залежать тільки від її внутрішніх змінних та, можливо, від зовнішніх класичних полів. Частина гамільтоніану, що описує взаємодію, залежить від змінних обидвох підсистем.

Нехай $g_i^A, |g_i^A\rangle, 1 \le i \le n$ та $g_j^B, |g_j^B\rangle, 1 \le j \le m$ — власні значення і власні вектори операторів $\mathbf{G}_A$ та $\mathbf{G}_B$ відповідно, тоді власними значеннями оператора $\mathbf{G}$ будуть nm чисел $g_i^A + g_j^B$, а власними векторами — nm тензорних добутків $|g_i^A\rangle \otimes |g_j^B\rangle$. (Див., напр. [46]) Це справедливо для невзаємодіючих систем A і B.

Проектор на стан $g_i^A + g_j^B$ цілої системи має вигляд:

$$\mathbf{P}_{ij} = |g_i^A\rangle \otimes |g_j^B\rangle\langle g_j^B| \otimes \langle g_i^A| = \mathbf{P}_i^A \otimes \mathbf{P}_j^B,$$

тобто, проектор на власний стан оператора, що є кронекеровою сумою, записують як кронекерів добуток проекторів на власні стани

кожного з доданків. За індукцією це правило можна поширити на довільну кількість доданків (підсистем).

Проектори на стани однієї з підсистем у просторі цілої системи записують:

$$\mathbf{P}_i^A \otimes \mathbf{I} \qquad \text{чи} \qquad \mathbf{I} \otimes \mathbf{P}_j^B.$$

Зауважимо, що у разі проектування на несепарабельні стани цілої системи (на стани Белла, напр.) проектори не можна записати як тензорний добуток.

Із розкладу (1.31) можна отримати *зображення Шмідта* для вектора чистого стану:

$$|\psi\rangle = \sum_{k=1}^{K} \lambda_k |\tilde{a}_k\rangle |\tilde{b}_k\rangle,$$

де $|\tilde{a}_k\rangle$ та $|\tilde{b}_k\rangle$ — ортонормовані набори векторів у просторах станів систем A і B відповідно. Ці набори є унікальними для кожного вектора $|\psi\rangle$. Число K дорівнює рангу матриці $\mathbf{C} = [c_{ij}]$ коефіцієнтів розкладу (1.31), λ_k^2 — власні значення матриці $\mathbf{C}\mathbf{C}^\dagger$, що є додатними. Доведення ґрунтується на теоремі про *сингулярний розклад* довільної комплексної матриці [12].

Матрицю $\mathbf{C} \in M_{m,n}$ ($M_{m,n}$ — множина комплексних матриць $m \times n$, m, n — кількість рядків і стовпців відповідно), рангу K можна зобразити так:

$$\mathbf{C} = \mathbf{V}\mathbf{\Lambda}\mathbf{W}^\dagger,$$

де $\mathbf{V} \in M_{m,m}$ і $\mathbf{W} \in M_{n,n}$ — унітарні матриці. Матриця $\mathbf{\Lambda} = [\lambda_{ij}] \in M_{m,n}$ така, що $\lambda_{ij} = 0, i \neq j; \lambda_{11} \geq \lambda_{22} \geq \ldots \geq \lambda_{KK} > \lambda_{K+1K+1} = \ldots = \lambda_{qq} = 0,\ q = \min\{m, n\}$. Числа $\{\lambda_{ii}\} \equiv \{\lambda_i\}$ є невід'ємні квадратні корені з власних значень матриці $\mathbf{C}\mathbf{C}^\dagger$ і, тому, визначені однозначно. Стовпці матриці $\mathbf{V}$ — власні вектори матриці $\mathbf{C}\mathbf{C}^\dagger$, а стовпці матриці $\mathbf{W}$ — власні вектори матриці $\mathbf{C}^\dagger\mathbf{C}$; обидві системи векторів впорядковано згідно розташування власних значень λ_i^2. Якщо $m \leq n$ і всі власні значення матриці $\mathbf{C}\mathbf{C}^\dagger$ різні, то матриця $\mathbf{V}$ визначена з точністю до правого діагонального множника $\mathbf{D} = \mathrm{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)$, де всі θ_i — дійсні числа; іншими словами, якщо $\mathbf{C} = \mathbf{V}_1\mathbf{\Lambda}\mathbf{W}_1^\dagger = \mathbf{V}_2\mathbf{\Lambda}\mathbf{W}_2^\dagger$, то $\mathbf{V}_2 = \mathbf{V}_1\mathbf{D}$. Якщо $m \leq n$, то матриця $\mathbf{W}$ завжди визначена неоднозначно; якщо $m = n$, матриця $\mathbf{V}$ фіксована і матриця $\mathbf{C}$ невироджена, то вибір матриці $\mathbf{W}$ однозначний. При $n \leq m$ твердження щодо єдиності матриць $\mathbf{V}$ і

$\mathbf{W}$ можна отримати, застосовуючи показане вище до матриці $\mathbf{C}^\dagger$. Для дійсної матриці $\mathbf{C}$ всі три матриці $\mathbf{V}, \mathbf{\Lambda}, \mathbf{W}$ можна вибрати дійсними. (Доведення див. в [11, 12].)

Тоді розклад (1.31) можна записати у вигляді:

$$|\psi\rangle = \sum_{i=1}^{N_A}\sum_{j=1}^{N_B}\sum_{k=1}^{K} V_{ik}\lambda_k W_{kj}|a_i\rangle|b_j\rangle = \sum_{k=1}^{K}\lambda_k|\tilde{a}_k\rangle|\tilde{b}_k\rangle,$$

де вектори

$$|\tilde{a}_k\rangle = \sum_{i=1}^{N_A} V_{ik}|a_i\rangle, \qquad |\tilde{b}_k\rangle = \sum_{j=1}^{N_B} W_{kj}|b_j\rangle$$

утворюють ортонормовані, але не обов'язково повні, системи, які, внаслідок унікальності кожної матриці $\mathbf{C}$, також є унікальними для кожного $|\psi\rangle$.

Кількість відмінних від нуля *сингулярних чисел* матриці $\mathbf{C}$ — власних чисел λ_k матриці $\sqrt{\mathbf{C}\mathbf{C}^\dagger}$ називають *числом Шмідта*. Воно дорівнює рангу K матриці $\mathbf{C}$ і характеризує ступінь заплутаності станів підсистем, чим більше число Шмідта — тим більша заплутаність станів.

З розкладу Шмідта можемо отримати такі зображення редукованих матриць густини підсистем A і B

$$\boldsymbol{\rho}_A = \mathrm{Sp}_B|\psi\rangle\langle\psi| = \sum_{k=1}^{K}\lambda_k^2\,|\tilde{a}_k\rangle\langle\tilde{a}_k|,$$

$$\boldsymbol{\rho}_B = \mathrm{Sp}_A|\psi\rangle\langle\psi| = \sum_{k=1}^{K}\lambda_k^2\,|\tilde{b}_k\rangle\langle\tilde{b}_k|,$$

в яких вони мають однакові власні значення.

Розклад Шмідта уможливлює процедуру "очищення" змішаного стану деякої системи, **формально математично** зобразивши її як підсистему ізольованої системи, що перебуває в чистому стані [10, 11]. Нехай така матриця густини діагональна в станах $|\varphi_i\rangle$

$$\boldsymbol{\rho} = \sum_{i=1}^{n} p_i\,|\varphi_i\rangle\langle\varphi_i|, \qquad p_i > 0, \qquad \sum_{i=1}^{n} p_i = 1,$$

то, очевидно, що вектор чистого стану "подвоєної" системи

$$|\psi\rangle = \sum_{i=1}^{n} \sqrt{p_i}\ |\varphi_i\rangle \otimes |\varphi_i\rangle \tag{1.33}$$

дасть ту саму матрицю густини як редуковану матрицю густини підсистеми цієї фіктивної розширеної системи.

Зображення Шмідта є зручним підходом у дослідженні складених квантових систем.

1.8 Квантові вимірювання

Розглянемо набір (ансамбль) K ізольованих фізичних систем, кожна з яких перебуває в тому самому чистому стані $|\psi\rangle$ (*чистий* чи *когерентний* ансамбль). В кожній окремій системі вимірюємо величину, яка в просторі станів описується оператором $\mathbf{A}$. Допустимо, що ці вимірювання в просторі станів можна описати на основі *постулату про проекційні вимірювання* (вимірювання фон Ноймана), який стверджує, що кожне вимірювання буде давати якесь одне власне значення a_i з ймовірністю

$$w(a_i) = \langle\psi|\mathbf{P}_{a_i}|\psi\rangle$$

і переводити окрему систему ансамблю у стан, який відрізняється від стану $|a_i\rangle$ тільки фазовим множником. Цю зміну стану запишемо як дію проекційного оператора

$$|\psi\rangle \longrightarrow \frac{\mathbf{P}_{a_i}\,|\psi\rangle}{\sqrt{\langle\psi|\,\mathbf{P}_{a_i}\,|\psi\rangle}}. \tag{1.34}$$

Такий перехід із стану $|\psi\rangle$ в стан $|a_i\rangle$ називають також *редукцією вектора стану* (*хвильової функції, хвильового пакету*).

Коли a_i позначає вироджений стан, то перехід відбувається в стан, який описується суперпозицією відповідних власних векторів згідно з проекційним оператором (1.13).

Якщо із всього ансамблю виділяємо (фіксуємо) тільки компоненту із певним значення a_i, а компоненти з іншими власними

значеннями відкидаємо, то таке вимірювання називається *селективним*. Зрозуміло, що з усіх K систем у стан (1.34) перейде тільки $k_i \approx w(a_i)K$ систем. Решта будуть відкинуті, наприклад, поглинуті середовищем.

Нехай вимірювання проводять так, що системи в станах із заданим a_i просторово розділяють між окремими "комірками" і підраховують кількість систем у кожній "комірці". Після K вимірювань отримаємо набір систем, k_i ($\sum_{i=1}^{N} k_i{=}K$) яких зафіксовано в стані $|a_i\rangle$, $i = 1, \ldots, N$. Як відомо (М.Борн), ймовірність отримати значення a_i дорівнює квадрату модуля проекції вектора $|\psi\rangle$ на власний стан $|a_i\rangle$

$$\lim_{K\to\infty} \frac{k_i}{K} = w(a_i) = |\,\langle a_i|\psi\rangle\,|^2 = \langle\psi|a_i\rangle\,\langle a_i|\psi\rangle = \langle\psi|\mathbf{P}_{a_i}|\psi\rangle.$$

В результаті описаного вище вимірювання можна обчислити середнє значення величини $\mathbf{A}$ після K експериментів

$$\langle\mathbf{A}\rangle_K = \frac{1}{K}\sum_{i=1}^{N} k_i a_i. \tag{1.35}$$

Якщо $K \longrightarrow \infty$, то

$$\langle\mathbf{A}\rangle{=}\langle\mathbf{A}\rangle_{K\to\infty}{=}\lim_{K\to\infty}\sum_{i=1}^{N}\frac{k_i}{K}a_i{=}\sum_{i=1}^{N}w(a_i)a_i{=}\sum_{i=1}^{N}a_i|\,\langle a_i|\psi\rangle\,|^2$$
$$=\sum_{i=1}^{N}a_i\,\langle\psi|a_i\rangle\,\langle a_i|\psi\rangle = \langle\psi|\sum_{i=1}^{N}a_i\,|a_i\rangle\,\langle a_i|\,|\psi\rangle = \langle\psi|\,\mathbf{A}\,|\psi\rangle.$$

Описане вище вимірювання перетворило набір K систем в чистому стані $|\psi\rangle$ в набір систем, k_i яких перебувають в одному з власних станів $|a_i\rangle$. Повторне вимірювання тієї ж спостережуваної в отриманому наборі дасть той самий результат і вже не переведе отриманий набір в інший стан. Отже, весь ансамбль перейшов у зовсім інший стан порівняно з початковим чистим станом $|\psi\rangle$, тобто, виник *змішаний ансамбль*, у якому кожен набір із k_i систем, що відповідають заданому значенню a_i, утворює свій чистий ансамбль. Середнє, отримане при повторному вимірюванні

збігається з (1.35), однак запишемо його в дещо іншій формі

$$\langle \mathbf{A} \rangle_K = \sum_{i=1}^{N} \frac{k_i}{K} a_i = \sum_{i=1}^{N} \frac{k_i}{K} \langle a_i | \mathbf{A} | a_i \rangle$$

$$= \sum_{j=1}^{N} \langle e_j | \boldsymbol{\rho}_K \mathbf{A} | e_j \rangle = \mathrm{Sp}(\boldsymbol{\rho}_K \mathbf{A}) = \mathrm{Sp}(\mathbf{A} \boldsymbol{\rho}_K),$$

де запроваджено величину

$$\boldsymbol{\rho}_K \equiv \sum_{i=1}^{N} \frac{k_i}{K} |a_i\rangle \langle a_i| , \tag{1.36}$$

яку можна називати оператором (матрицею) густини скінченного змішаного ансамблю з K систем.

У границі $K \to \infty$ отримуємо матрицю густини нескінченного змішаного ансамблю

$$\boldsymbol{\rho} = \sum_{i=1}^{N} w(a_i) |a_i\rangle\langle a_i|.$$

Операція обчислення сліду (шпура) деякого оператора $\mathbf{A}$ означає підрахунок суми його діагональних елементів у довільному ортонормованому базисі

$$\mathrm{Sp}(\mathbf{A}) \equiv \sum_{j=1}^{N} \langle e_j | \mathbf{A} | e_j \rangle, \qquad \mathrm{Sp}(\sum_k \mathbf{A}_k) = \sum_k \mathrm{Sp}(\mathbf{A}_k).$$

Значення сліду не залежить від вибору базису сумування.

Матриця густини (1.36) описує змішані ансамблі, отримані селективним проективним вимірюванням у чистому ансамблі спостережуваної, яка задається оператором $\mathbf{A}$. Такий самий змішаний ансамбль отримаємо (з тими ж матрицями густини), якщо будемо вимірювати будь-яку іншу сумісну з $\mathbf{A}$ спостережувану.

Матриця густини змішаного ансамблю, отриманого вимірюванням спостережуваної $\mathbf{A}$, є діагональною

$$\boldsymbol{\rho} = \sum_{i=1}^{N} \langle a_i | \psi \rangle \langle \psi | a_i \rangle |a_i\rangle \langle a_i|$$

у базисі власних функцій цієї спостережуваної.

Середні значення деякої спостережуваної $\mathbf{B}$ до вимірювання величини $\mathbf{A}$ і після її вимірювання відповідно будуть

$$\langle \mathbf{B} \rangle = \mathrm{Sp}\,(\mathbf{B}\boldsymbol{\rho}) = \sum_{i,j=1}^{N} \langle a_i|\psi\rangle\langle\psi|a_j\rangle\langle a_j|\mathbf{B}|a_i\rangle,$$

$$\langle \mathbf{B} \rangle' = \mathrm{Sp}\,(\mathbf{B}\boldsymbol{\rho}) = \sum_{i=1}^{N} \langle a_i|\psi\rangle\langle\psi|a_i\rangle\langle a_i|\mathbf{B}|a_i\rangle.$$

Якщо оператори спостережуваних $\mathbf{A}$ і $\mathbf{B}$ комутують, то середні $\langle \mathbf{B} \rangle$ і $\langle \mathbf{B} \rangle'$ рівні, тобто вимірювання величини $\mathbf{B}$ в чистому стані чи після вимірювання величини $\mathbf{A}$ дає той самий результат. Для некомутативних $\mathbf{A}$ і $\mathbf{B}$ результати будуть різними.

Акцентуємо на важливості підрахунку (фіксуванні) кількості систем k_i в стані a_i після проектування. Пояснимо це на прикладі проектування на два стани $|a_1\rangle$ і $|a_2\rangle$. Якщо підрахувати кількість систем у цих станах, а потім звести їх в одну систему, то отримаємо її в змішаному стані з матрицею густини

$$\rho_K = \frac{1}{k_1 + k_2} \left(k_1 |a_1\rangle\langle a_1| + k_2 |a_2\rangle\langle a_2| \right),$$

тобто, в *некогерентній* суперпозиції станів $|a_1\rangle$ і $|a_2\rangle$.

Якщо ж після проектування не рахувати кількість систем у кожному стані, а знову звести їх в одну систему, то вона буде в стані

$$|\varphi\rangle = \frac{(\mathbf{P}_1 + \mathbf{P}_2)\,|\psi\rangle}{\sqrt{\langle\psi|\,(\mathbf{P}_1 + \mathbf{P}_2)\,|\psi\rangle}} = \frac{\langle a_1|\psi\rangle|a_1\rangle + \langle a_2|\psi\rangle|a_2\rangle}{\sqrt{|\langle a_1|\psi\rangle|^2 + |\langle a_2|\psi\rangle|^2}},$$

який є *когерентною* суперпозицією станів $|a_1\rangle$ і $|a_2\rangle$, тобто, чистим станом. Використання в останньому виразі не двох, а всіх власних станів оператора $\mathbf{A}$ призводить до розкладу початкового стану за цими станами. Але при цьому не відбулося вимірювання! Це значить, що у вимірюванні суттєвим є підрахунок (фіксування) кількості систем у кожному власному стані під час формування змішаного стану після вимірювання. Перехід із чистого стану в змішаний є неунітарним переходом.

Експериментально процес проективного вимірювання розділяється на два: спектральне розділення станів, яке здійснюється *аналізатором* і на детектування, яке виконує *детектор*. Саме детектування впливає незворотно на систему і фіксує її в певному стані [7], що і призводить до формування змішаних станів.

У підході матриці густини проективний постулат формулюється так: (селективне) проективне вимірювання з (*одновимірним* чи *лінійним*) оператором проектування $\mathbf{P}_{a_k}$ з ймовірністю $p(a_k)$=Sp$(\mathbf{P}_{a_k}\boldsymbol{\rho})$ переводить систему із стану $\boldsymbol{\rho}$ у стан

$$\boldsymbol{\rho}' = \frac{\mathbf{P}_{a_k}\boldsymbol{\rho}\mathbf{P}_{a_k}}{\mathrm{Sp}(\mathbf{P}_{a_k}\boldsymbol{\rho})}.$$

Нехай початковий стан був чистим і у вимірювальному базисі описуваний матрицею густини $\boldsymbol{\rho} = |\psi\rangle\langle\psi| = \sum_{i,j=1}^{N} c_i c_j^* |a_i\rangle\langle a_j|$. Після вимірювання він перейшов у чистий стан

$$\boldsymbol{\rho}' = \frac{|c_k|^2 |a_k\rangle\langle a_k|}{|c_k|^2} = |a_k\rangle\langle a_k|.$$

Якщо початковий стан є некогерентною сумішшю станів вимірювального базису $\boldsymbol{\rho} = \sum_{i=1}^{N} w_i |a_i\rangle\langle a_i|$, то таке ж вимірювання призведе до того ж результату

$$\boldsymbol{\rho}' = \frac{w_k |a_k\rangle\langle a_k|}{w_k} = |a_k\rangle\langle a_k|.$$

Проектування на підпростір станів $\{|a_1\rangle, |a_2\rangle\}$, тобто, вимірювання з проекційним оператором $\mathbf{P}$=$\mathbf{P}_{a_1}$+$\mathbf{P}_{a_2}$ знову переводить початково чистий стан у чистий

$$\boldsymbol{\rho}' = \frac{(c_1|a_1\rangle + c_2|a_2\rangle)(c_1^*\langle a_1| + c_2^*\langle a_2|)}{|c_1|^2 + |c_2|^2},$$

тоді як початково змішаний стан $\boldsymbol{\rho} = \sum_i w_i |a_i\rangle\langle a_i|$ вже переходить у змішаний

$$\boldsymbol{\rho}' = \frac{w_1 |a_1\rangle\langle a_1| + w_2 |a_2\rangle\langle a_2|}{w_1 + w_2}. \tag{1.37}$$

Однак, якщо проектувати чистий стан на кожен стан $|a_1\rangle, |a_2\rangle$ зокрема, тобто, фіксувати їх окремо, то частина чистого ансамблю пропорційна (чи система з ймовірністю)

$$\mathrm{Sp}\left(\mathbf{P}_{a_1}|\psi\rangle\langle\psi|\mathbf{P}_{a_1} + \mathbf{P}_{a_2}|\psi\rangle\langle\psi|\mathbf{P}_{a_2}\right) = |\langle a_1|\psi\rangle|^2 + |\langle a_2|\psi\rangle|^2$$

перейде у змішаний стан

$$\boldsymbol{\rho}' = \frac{\mathbf{P}_{a_1}|\psi\rangle\langle\psi|\mathbf{P}_{a_1}+\mathbf{P}_{a_2}|\psi\rangle\langle\psi|\mathbf{P}_{a_2}}{\mathrm{Sp}\,(\mathbf{P}_{a_1}|\psi\rangle\langle\psi|\mathbf{P}_{a_1}+\mathbf{P}_{a_2}|\psi\rangle\langle\psi|\mathbf{P}_{a_2})} = \frac{|\langle a_1|\psi\rangle|^2|a_1\rangle\langle a_1|+|\langle a_2|\psi\rangle|^2|a_2\rangle\langle a_2|}{|\langle a_1|\psi\rangle|^2+|\langle a_2|\psi\rangle|^2}.$$

Якщо ж початковий стан був змішаний $\boldsymbol{\rho}=\sum_i w_i|a_i\rangle\langle a_i|$, то після вимірювання з ймовірністю w_1+w_2, отримаємо змішаний стан (1.37), той самий, що і під час проектування на підпростір $\{|a_1\rangle, |a_2\rangle\}$.

Останні вирази легко узагальнити на таке ж вимірювання довільної частини спектра (чи всього спектра) оператора $\mathbf{A}$: частина ансамблю пропорційна до (чи окрема його система з ймовірністю) $p = \mathrm{Sp}\,(\sum_k \mathbf{P}_{a_k}\boldsymbol{\rho}\mathbf{P}_{a_k})$ перейде у стан

$$\boldsymbol{\rho} \to \boldsymbol{\rho}' = \frac{\sum_k \mathbf{P}_{a_k}\boldsymbol{\rho}\mathbf{P}_{a_k}}{\mathrm{Sp}\,(\sum_k \mathbf{P}_{a_k}\boldsymbol{\rho}\mathbf{P}_{a_k})}, \tag{1.38}$$

де суми беруться по відповідній частині (чи всьому) спектру.

Нехай система початково перебуває в одному з власних станів $|c_i\rangle$ деякої величини $\mathbf{C}$. Після вимірювання всіх власних значень спостережуваної $\mathbf{B}$, несумісної з $\mathbf{C}$, система перейде в стан

$$\boldsymbol{\rho} = \sum_k \mathbf{P}_{b_k}|c_i\rangle\langle c_i|\mathbf{P}_{b_k} = \sum_k |\langle b_k|c_i\rangle|^2|b_k\rangle\langle b_k|.$$

Виміряємо тепер власне значення a_j спостережуваної $\mathbf{A}$, несумісної з $\mathbf{B}$. Величина

$$p(c_i, a_j)=\mathrm{Sp}(\boldsymbol{\rho}\mathbf{P}_{a_j})=\sum_k |\langle a_j|b_k\rangle|^2|\langle b_k|c_i\rangle|^2=\sum_k |\langle a_j|\mathbf{P}_{b_k}|c_i\rangle|^2 \tag{1.39}$$

визначає ймовірність переходу системи зі стану $|c_i\rangle$ в стан $|a_j\rangle$ у процесі з проміжним вимірюванням всього спектра спостережуваної $\mathbf{B}$. Без проміжного вимірювання ймовірність цього переходу визначалася б за правилами

$$\langle c_i|\mathbf{P}_{a_j}|c_i\rangle = |\langle a_j|c_i\rangle|^2 \quad \text{чи} \quad \mathrm{Sp}\left(\mathbf{P}_{a_j}|c_i\rangle\langle c_i|\mathbf{P}_{a_j}\right) = |\langle a_j|c_i\rangle|^2.$$

Увівши оператор, що описує проміжне вимірювання $\boldsymbol{\mathcal{P}}_b$, і оператор *неселективного* вимірювання $\boldsymbol{\mathcal{M}}_{a_j}(b)$ (див. [5])

$$\mathcal{P}_b = \sum_{k=1}^{N} e^{i\phi(b_k)} |b_k\rangle\langle b_k|, \qquad \boldsymbol{\mathcal{M}}_{a_j}(b) = \mathbf{P}_{a_j}\mathcal{P}_b, \tag{1.40}$$

де $\phi(b_k)$ — цілком випадкова фаза, якої набуває вектор стану $|b_k\rangle$ при його детектуванні, ймовірність $p(c_i, a_j)$ (1.39) можна обчислити за правилами одного вимірювання, тобто,

$$\begin{aligned} p(c_i, a_j) &= \langle c_i|\boldsymbol{\mathcal{M}}^{\dagger}_{a_j}(b)\boldsymbol{\mathcal{M}}_{a_j}(b)|c_i\rangle = \langle c_i|\mathcal{P}^{\dagger}_b\mathbf{P}_{a_j}\mathcal{P}_b|c_i\rangle \\ &= \sum_{k_1,k_2} e^{-i\phi(b_{k_1})}e^{i\phi(b_{k_2})}\langle c_i|b_{k_1}\rangle\langle b_{k_1}|a_j\rangle\langle a_j|b_{k_2}\rangle\langle b_{k_2}|c_i\rangle \\ &= \sum_{k}\langle c_i|b_k\rangle\langle b_k|a_j\rangle\langle a_j|b_k\rangle\langle b_k|c_i\rangle = \sum_{k}|\langle a_j|\mathbf{P}_{b_k}|c_i\rangle|^2 \end{aligned}$$

чи

$$\begin{aligned} p(c_i, a_j) &= \mathrm{Sp}\left(\boldsymbol{\mathcal{M}}_{a_j}(b)|c_i\rangle\langle c_i|\boldsymbol{\mathcal{M}}^{\dagger}_{a_j}(b)\right) \\ &= \mathrm{Sp}\left(\mathbf{P}_{a_j}\mathcal{P}_b|c_i\rangle\langle c_i|\mathcal{P}^{\dagger}_b\mathbf{P}_{a_j}\right) = \sum_{k}|\langle a_j|\mathbf{P}_{b_k}|c_i\rangle|^2 \end{aligned}$$

прийнявши, що сума хаотичних фаз $e^{-i\phi(b_{k_1})+i\phi(b_{k_2})} = \delta_{k_1k_2}$ [5].

Оператори $\mathcal{P}_b$ є унітарними, а не проекційними, як могло б здатися на перший погляд

$$\mathcal{P}^{\dagger}_b \neq \mathcal{P}_b, \quad \mathcal{P}^2_b \neq \mathcal{P}_b, \quad \mathcal{P}^{\dagger}_b\mathcal{P}_b = \mathcal{P}_b\mathcal{P}^{\dagger}_b = \mathbf{P}_b = \mathbf{I}.$$

Описані неселективні вимірювання (1.39), (1.40) є композицією унітарного перетворення та проекційного вимірювання. Тому в квантовій фізиці розглядають і вимірювання загального виду [10, 11], щодо яких проекційні є частковим випадком. Такі вимірювання в просторі станів зображаються *операторами вимірювання* $\{\mathbf{M}_m\}$, де індекс m позначає результат, ймовірність отримати який обчислюють за формулою

$$p(m) = \langle\psi|\mathbf{M}^{\dagger}_m\mathbf{M}_m|\psi\rangle. \tag{1.41}$$

У деяких випадках кінцевий стан після вимірювання можна визначити подібно як у проективному вимірюванні

$$|\psi\rangle \to \frac{\mathbf{M}_m|\psi\rangle}{\sqrt{\langle\psi|\mathbf{M}^{\dagger}_m\mathbf{M}_m|\psi\rangle}}. \tag{1.42}$$

Оператори вимірювання задовольняють *умову повноти*

$$\sum_m \mathbf{M}_m^\dagger \mathbf{M}_m = \mathbf{I},$$

тобто, сума імовірностей усіх результатів дорівнює одиниці

$$\sum_m p(m) = \sum_m \langle\psi|\mathbf{M}_m^\dagger \mathbf{M}_m|\psi\rangle = 1.$$

Селективне вимірювання з оператором $\mathbf{M}_m$ системи, що описується матрицею густини $\boldsymbol{\rho}$, дає значення m з ймовірністю $p(m)$ і при цьому переводить її у стан

$$\boldsymbol{\rho}' = \frac{\mathbf{M}_m \boldsymbol{\rho} \mathbf{M}_m^\dagger}{\mathrm{Sp}\left(\mathbf{M}_m \boldsymbol{\rho} \mathbf{M}_m^\dagger\right)}, \qquad p(m) = \mathrm{Sp}\left(\mathbf{M}_m \boldsymbol{\rho} \mathbf{M}_m^\dagger\right). \tag{1.43}$$

Вимірювання усіх значень $\{m\}$ переведе систему у стан

$$\boldsymbol{\rho}' = \sum_m \mathbf{M}_m \boldsymbol{\rho} \mathbf{M}_m^\dagger. \tag{1.44}$$

Саме за правилами (1.43) можна знайти перехід у кінцевий стан після неселективного вимірювання, вибравши $\mathbf{M}_m = \boldsymbol{\mathcal{M}}_{a_j}(b)$.

Дехто з авторів (напр. [11]) формулює постулат про вимірювання на основі узагальнених операторів вимірювання $\{\mathbf{M}_m\}$, а не проекційних операторів $\{\mathbf{P}_m\}$. Загальне вимірювання можна зобразити послідовністю унітарного перетворення і проективного вимірювання в складеній системі (див., напр. [6, 11]).

Проекційні вимірювання є частковим випадком вимірювань (1.41), (1.42). Проекційні оператори мають властивості $\mathbf{P}_m^\dagger = \mathbf{P}_m$ і $\mathbf{P}_{m_1}\mathbf{P}_{m_2} = \mathbf{P}_{m_1}\delta_{m_1 m_2}$, які означають ортогональність і виражають їхню відтворюваність. Тобто, повторне проекційне вимірювання дасть той самий результат, що і попереднє, тоді як вимірювання (1.41), (1.42) такої властивості не мають, оскільки в загальному випадку $\mathbf{M}_m^2 \neq \mathbf{M}_m$, вони також не є ортогональними $\mathbf{M}_{m_1}\mathbf{M}_{m_2} \neq \mathbf{M}_{m_1}\delta_{m_1 m_2}$.

Нехай задано набір $\{|\varphi_i\rangle\}$ нормованих, але неортогональних векторів у просторі станів деякої системи такий, що довільний вектор у ньому можна розкласти за цим набором

$$|\psi\rangle = \sum_i |\varphi_i\rangle\langle\varphi_i|\psi\rangle,$$

тобто, цей набір утворює базис, який може бути і переповнений. Останній вираз можна записати і у термінах проекційних операторів $\mathbf{\Pi}_i = |\varphi_i\rangle\langle\varphi_i|$, які, однак, не є ортогональними:

$$\mathbf{\Pi}_i^2 = \mathbf{\Pi}_i, \quad \mathbf{\Pi}_i^\dagger = \mathbf{\Pi}_i, \quad \mathbf{\Pi}_i\mathbf{\Pi}_j = |\varphi_i\rangle\langle\varphi_i|\varphi_j\rangle\langle\varphi_j| \neq \delta_{ij}\mathbf{\Pi}_i$$

Принципово важливим в інформатиці (не тільки квантовій) є можливість зображати (записувати, передавати) символи певними фізичними станами, які можна достовірно розрізняти (щоб не плутати символи). Зрозуміло, що в квантовій інформатиці для цього необхідно використовувати набори ортонормованих станів, справді, якщо $|\psi_i\rangle$ є ортонормованими, то їх легко розрізнити за допомогою проекційних операторів $\mathbf{P}_i = |\psi_i\rangle\langle\psi_i|$

$$\langle\psi_j|\mathbf{P}_i|\psi_j\rangle = \delta_{ij}.$$

Достовірно розрізнити неортогональні стани $|\varphi_i\rangle$ вимірюванням

$$\langle\varphi_j|\mathbf{\Pi}_i|\varphi_j\rangle = |\langle\varphi_i|\varphi_j\rangle|^2 \quad \text{чи} \quad \langle\varphi_j|\mathbf{P}_i|\varphi_j\rangle = |\langle\psi_i|\varphi_j\rangle|^2$$

не вдається. При малих відхиленнях від ортогональності, коли $|\langle\varphi_i|\varphi_j\rangle| \ll 1$ чи $|\langle\psi_i|\varphi_j\rangle| \ll 1$ для $i \neq j$, багатократним повторенням можна досягти статистично достовірного розрізнення.

У багатьох випадках не вдається з'ясувати, в який стан переходить система після вимірювання, а тільки знайти ймовірність стану, в якому вона була до вимірювання. Такі вимірювання зображаються невід'ємно визначеними операторами $\mathbf{\mathcal{M}}_m$ з правилом обчислення вказаної ймовірності:

$$p(m) = \langle\psi|\mathbf{\mathcal{M}}_m|\psi\rangle \quad \text{чи} \quad p(m) = \mathrm{Sp}\left(\mathbf{\mathcal{M}}_m\boldsymbol{\rho}\right),$$

що задовольняють умову $\sum_m \mathbf{\mathcal{M}}_m = \mathbf{I}$, тобто, дають змогу знайти ймовірності всіх можливих станів, індексованих величиною m. Оператори $\mathbf{\mathcal{M}}_m$ називають POVM–елементами, а весь набір $\mathbf{\mathcal{M}}_m$— POVM (Positive Operator-Valued Measure), тобто, позитивнозначною операторною мірою. Загальні вимірювання (1.41), (1.42) також можна віднести до POVM, якщо означити $\mathbf{\mathcal{M}}_m = \mathbf{M}_m^\dagger\mathbf{M}_m$.

Загальне квантове вимірювання на підсистемі A складеної системи описують оператором $\mathbf{M}_m \otimes \mathbf{I}$, який згідно (1.43) із ймовірністю $\mathrm{Sp}((\mathbf{M}_m \otimes \mathbf{I})\boldsymbol{\rho}(\mathbf{M}_m^\dagger \otimes \mathbf{I}))$ переводить матрицю густини $\boldsymbol{\rho}$ в

$$\boldsymbol{\rho}' = \frac{(\mathbf{M}_m \otimes \mathbf{I})\boldsymbol{\rho}(\mathbf{M}_m^\dagger \otimes \mathbf{I})}{\mathrm{Sp}((\mathbf{M}_m \otimes \mathbf{I})\boldsymbol{\rho}(\mathbf{M}_m^\dagger \otimes \mathbf{I}))} = \frac{(\mathbf{M}_m \otimes \mathbf{I})\boldsymbol{\rho}(\mathbf{M}_m^\dagger \otimes \mathbf{I})}{\mathrm{Sp}_A(\mathbf{M}_m \boldsymbol{\rho}_A \mathbf{M}_m^\dagger)}.$$

Звідси легко отримати

$$\boldsymbol{\rho}'_A = \frac{\mathbf{M}_m \boldsymbol{\rho}_A \mathbf{M}_m^\dagger}{\mathrm{Sp}_A(\mathbf{M}_m^\dagger \mathbf{M}_m \boldsymbol{\rho}_A)},$$

тобто, результати вимірювання підсистеми складеної системи можна обчислити за допомогою її редукованої матриці густини. Заплутування з оточенням призводить до змішування станів системи, тому розрізняти їх можна тільки в статистичному сенсі.

Докладніше з квантовими вимірюваннями можна ознайомитися у працях [5, 6, 10, 11].

1.9 Неунітарні перетворення відкритих систем

Головною передумовою функціонування квантового комп'ютера є унітарність еволюції станів квантового регістру, яка забезпечується тільки повною його ізоляцією. Така ізоляція недосяжна, тому треба дослідити можливість виконання квантових обчислень за умови квантового шуму, спричиненого впливом оточення. Це зручно робити *методом квантових перетворень*, який створено для опису неунітарної еволюції підсистем великої системи.

Якщо ізольована система перебуває в чистому або змішаному стані, то її еволюцію описують унітарними перетворенням, і в ній можливі проективні вимірювання.

Нехай фізична система складається з двох підсистем: *основної системи* (S) і *оточення* (env). Її стани описують у термінах матриці густини. У разі унітарної еволюції (за скінченний проміжок часу) цілої системи (основна+оточення) матриця густини основної системи зазнає квантових перетворень

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}(\boldsymbol{\rho}),$$

які за відсутності оточення зводяться до унітарних перетворень:

$$\mathcal{E}(\boldsymbol{\rho}) = \mathbf{U}\boldsymbol{\rho}\mathbf{U}^{\dagger}.$$

Унітарний характер еволюції основної системи зберігається і тоді, коли в процесі перетворення підсистеми не взаємодіють. Якщо початковий стан цілої системи буде $\boldsymbol{\rho}{=}\boldsymbol{\rho}_S{\otimes}\boldsymbol{\rho}_{env}$, і оператор унітарного перетворення $\mathbf{U}{=}\mathbf{U}_S{\otimes}\mathbf{U}_{env}$, то після перетворення основна система перейде в стан:

$$\boldsymbol{\rho}'_S = \mathcal{E}(\boldsymbol{\rho}_S) = \mathrm{Sp}_{env}(\mathbf{U}\boldsymbol{\rho}\mathbf{U}^{\dagger})$$
$$= \mathbf{U}_S\boldsymbol{\rho}_S\mathbf{U}_S^{\dagger}\,\mathrm{Sp}_{env}(\mathbf{U}_{env}\boldsymbol{\rho}_{env}\mathbf{U}_{env}^{\dagger}) = \mathbf{U}_S\boldsymbol{\rho}_S\mathbf{U}_S^{\dagger}.$$

Розглянемо тепер випадок, коли початковий стан системи описують оператором густини $\boldsymbol{\rho}{=}\boldsymbol{\rho}_S{\otimes}|e\rangle\langle e|$, де $|e\rangle\langle e|$ — (чистий нормований) початковий стан оточення, а $|e_k\rangle$ — базисні вектори в просторі станів оточення. Тоді унітарна еволюція при взаємодії основної системи з оточенням зумовить квантове перетворення основної системи, яке описують *супероператором* чи *зображенням операторною сумою* (*зображенням Крауса*):

$$\boldsymbol{\rho}'_S = \mathcal{E}(\boldsymbol{\rho}_S) = \mathrm{Sp}_{env}\left(\mathbf{U}(\boldsymbol{\rho}_S \otimes |e\rangle\langle e|)\mathbf{U}^{\dagger}\right)$$
$$= \sum_k \langle e_k|\mathbf{U}(\boldsymbol{\rho}_S \otimes |e\rangle\langle e|)\mathbf{U}^{\dagger}|e_k\rangle = \sum_k \mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}_k^{\dagger}, \qquad (1.45)$$

де

$$\mathbf{E}_k = \langle e_k|\mathbf{U}|e\rangle \quad — \qquad (1.46)$$

елементи перетворення $\mathcal{E}(\boldsymbol{\rho}_S)$ — матриці в просторі станів основної системи, отримані як середні за векторами стану оточення від матриці унітарного перетворення всієї системи. Якщо після дії на всю систему оператора унітарного перетворення зробити унітарне перетворення тільки станів оточення, тобто, подіяти на стани всієї системи оператором $\mathbf{I}_S{\otimes}\mathbf{V}$, то елементи "нового" перетворення будуть пов'язані з елементами "старого" співвідношенням:

$$\mathbf{F}_k = \langle e_k|(\mathbf{I}_S \otimes \mathbf{V})\mathbf{U}|e\rangle = \langle e_k|\mathbf{I}_S \otimes \mathbf{V}\sum_j |e_j\rangle\langle e_j|\mathbf{U}|e\rangle$$
$$= \sum_j \langle e_k|\mathbf{V}|e_j\rangle\langle e_j|\mathbf{U}|e\rangle = \sum_j V_{kj}\mathbf{E}_j. \qquad (1.47)$$

Оскільки унітарне перетворення $\mathbf{V}$ оточення не зачіпає основної системи, тобто, не впливає на квантове перетворення, що вже відбулося, то це означає, що одне й те ж перетворення $\boldsymbol{\mathcal{E}}(\boldsymbol{\rho})$ можна описати різними операторними сумами з різними елементами перетворення (*неоднозначність зображення операторною сумою*). Таке ж співвідношення (1.47) можна отримати, перейшовши до іншого базису оточення $\langle e_k| = \sum_i V^*_{ik}\langle e'_i|$. Інакше можна сказати, що два квантові перетворення $\boldsymbol{\mathcal{F}}$ і $\boldsymbol{\mathcal{E}}$ рівні між собою ($\boldsymbol{\mathcal{F}} = \boldsymbol{\mathcal{E}}$), якщо їхні елементи задовольняють умову (1.47).

З унітарності оператора $\mathbf{U}$ випливає співвідношення повноти для елементів перетворення $\sum_k \mathbf{E}^\dagger_k\mathbf{E}_k = \mathbf{I}$. Такі перетворення називають *квантовими перетвореннями, що зберігають слід*. Загальне квантове вимірювання (1.44) також є варіантом квантового перетворення, що зберігає слід.

Оператор густини $\boldsymbol{\rho}'$, отриманий після квантового перетворення, що зберігає слід, задовольняє всі умови, якщо їх задовольняє оператор густини $\boldsymbol{\rho}$ початкового стану:

$$
\begin{aligned}
&1)\ \text{ермітовість } \boldsymbol{\rho}'^\dagger_S = \sum_k \mathbf{E}_k\boldsymbol{\rho}^\dagger_S\mathbf{E}^\dagger_k = \sum_k \mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k = \boldsymbol{\rho}'_S,\\
&2)\ \text{одиничний слід } \mathrm{Sp}_S\boldsymbol{\rho}'_S = \mathrm{Sp}_S\left(\sum_k \mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k\right) = 1,\\
&3)\ \text{додатність } {}_S\langle\psi|\boldsymbol{\rho}'_S|\psi\rangle_S = \sum_k ({}_S\langle\psi|\mathbf{E}_k)\boldsymbol{\rho}_S(\mathbf{E}^\dagger_k|\psi\rangle_S) \geq 0. \qquad (1.48)
\end{aligned}
$$

Нехай після унітарної еволюції за скінченний проміжок часу ми провели селективне вимірювання за допомогою проектора $\mathbf{P}_k = |e_k\rangle\langle e_k|$ на стани оточення:

$$
\begin{aligned}
&\mathrm{Sp}_{env}\Big((\mathbf{I}_S\otimes\mathbf{P}_k)\mathbf{U}(\boldsymbol{\rho}_S\otimes|e\rangle\langle e|)\mathbf{U}^\dagger(\mathbf{I}_S\otimes\mathbf{P}_k)\Big)\\
&\qquad = \langle e_k|\mathbf{U}(\boldsymbol{\rho}_S\otimes|e\rangle\langle e|)\mathbf{U}^\dagger|e_k\rangle = \mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k,
\end{aligned}
$$

яке зафіксувало основну систему з ймовірністю $p(k)$ в стані (нормованому):

$$
(\boldsymbol{\rho}'_S)_k = \frac{\mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k}{\mathrm{Sp}_S\left(\mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k\right)}, \qquad p(k) = \mathrm{Sp}_S\left(\mathbf{E}_k\boldsymbol{\rho}_S\mathbf{E}^\dagger_k\right).
$$

Це дає змогу трактувати вираз (1.45) для редукованої матриці, отриманої в результаті таких вимірювань,

$$\boldsymbol{\rho}'_S = \boldsymbol{\mathcal{E}}(\boldsymbol{\rho}_S) = \sum_k \mathbf{E}_k \boldsymbol{\rho}_S \mathbf{E}_k^\dagger = \sum_k p(k)(\boldsymbol{\rho}'_S)_k$$

як випадкову (з ймовірністю $p(k)$) заміну стану $\boldsymbol{\rho}_S$ основної системи на стан $(\boldsymbol{\rho}'_S)_k$ під впливом оточення, що дуже схоже з дією шуму на класичні інформаційні канали. Тому квантові перетворення, які описують процеси квантового шуму, в квантовій інформатиці називають *квантовими каналами з шумом*.

Вище ми розглядали випадок чистого початкового стану оточення, тепер з'ясуємо, як модифікується зображення операторною сумою для початкового стану цілої системи виду $\boldsymbol{\rho}_S \otimes \boldsymbol{\rho}_{env}$. Запишемо вираз для матриці густини оточення в її власному зображенні $\boldsymbol{\rho}_{env}{=}\sum_j \lambda_j |\lambda_j\rangle\langle\lambda_j|$, $\lambda_j > 0$, $\sum_j \lambda_j{=}1$. Квантове перетворення основної системи при унітарній еволюції цілої і загального вимірювання всієї системи $\mathbf{M}_m$ можна виразити:

$$(\boldsymbol{\rho}'_S)_m{=}\boldsymbol{\mathcal{E}}_m(\boldsymbol{\rho}_S){=}\mathrm{Sp}_{env}\Big(\mathbf{M}_m\mathbf{U}(\boldsymbol{\rho}_S{\otimes}\boldsymbol{\rho}_{env})\mathbf{U}^\dagger\mathbf{M}_m^\dagger\Big){=}\sum_{jk}\mathbf{E}_{jk}^{(m)}\boldsymbol{\rho}_S\mathbf{E}_{jk}^{(m)\dagger},$$

де

$$\mathbf{E}_{jk}^{(m)} = \sqrt{\lambda_j}\langle e_k|\mathbf{M}_m\mathbf{U}|\lambda_j\rangle \quad — \tag{1.49}$$

елементи перетворення $\boldsymbol{\mathcal{E}}_m$. Якщо ж вимірювання не проводиться, то $\mathbf{M}_m{=}\mathbf{I}$, і тоді отримаємо квантове перетворення, зумовлене тільки взаємодією між підсистемами. Кількість власних векторів матриці густини оточення завжди менша або рівна вимірності його простору станів N_{env}, а вимірність основної системи також завжди скінченна, тому індекси в (1.49) можна перевпорядкувати так, що цей вираз набере вигляду (1.46), тобто, два індекси j,k замінити одним. Це ще одне свідчення неоднозначності зображення квантового перетворення операторною сумою, яка є наслідком того, що різні фізичні механізми впливу оточення можуть призводити до одного й того ж квантового перетворення основної системи, а, отже, несуттєво, яким є початковий стан оточення — чистим чи змішаним. Тому, аналізуючи ефекти квантового шуму,

нема потреби досліджувати причини і механізми впливу, а досить з'ясувати всі наслідки їхньої дії на основну систему, тобто, встановити всі можливі квантові перетворення основної системи і створити ефективні механізми для їхнього усування.

Усіх квантових перетворень є скінченна кількість (унаслідок скінченної кількості станів основної системи) і цікавим є питання про те, якої мінімальної вимірності має бути простір станів оточення, щоби при унітарному перетворенні цілої системи в основній системі можна було реалізувати всі квантові перетворення? Виявляється, що кількість елементів квантового перетворення $\mathbf{E}_k$ не перевищує N^2 (N — вимірність простору станів основної системи), тобто вимірність простору станів оточення, яке викликає всі квантові перетворення в основній системі при унітарному перетворенні цілої системи, не перевищує N^2 (див., напр. [11]). Це і зрозуміло, бо кількість елементів матриці густини N–вимірного простору станів дорівнює N^2.

Цей висновок може здатися дивним, оскільки вираз (1.46) можна записати за допомогою базисних векторів оточення:

$$\mathbf{E}_k = \langle e_k|\mathbf{U}|e\rangle = \sum_{j=1}^{N_{env}} c_j \langle e_k|\mathbf{U}|e_j\rangle = \sum_{j=1}^{N_{env}} c_j \mathbf{E}_{kj},$$

де кількість усіх елементів $\mathbf{E}_{kj}$ дорівнює N_{env}^2 і значно перевищує N^2, однак, виявляється, що більшість із них дорівнює нулю і суттєво різних між ними є не більше, аніж N^2.

Розділ 2

Квантові біти. Модель спіну s=1/2

Основним алфавітом, який використовують у класичній інформатиці є двійковий алфавіт, що складається з двох "букв" 0 і 1, які і утворюють один біт інформації. Фізично він реалізується системою, що може перебувати в двох стійких станах, які легко розрізнити. Мікроскопічний, суттєво квантовий аналог такої системи, що може перебувати в двох (відносно) стійких станах $|0\rangle$ і $|1\rangle$, а також у суперпозиційному стані

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle , \qquad c_0, c_1 \in \mathbb{C} \tag{2.1}$$

називається *квантовим бітом*. Скорочено будемо називати його *квабітом*, хоча частіше використовують термін *кубіт*. Для достовірного розрізнення зображуваних символів стани квабіта повинні бути ортогональними.

Отже, **квантовий біт — це дворівнева квантова система, станами якої можна керувати.**

Двовимірний простір квабіта $\mathcal{H}$ містить континуум станів (2.1), тоді як простір класичного біта складається лише з двох станів.

Сукупність достатньо великої кількості пов'язаних між собою квабітів утворює *квантовий регістр*.

Когерентну зміну станів квабітів і, загалом, квантових регістрів, виконують за допомогою зовнішніх впливів, здебільшого часовозалежних класичних полів, які, за аналогією з класичним випадком, називають *квантовими логічними елементами* (КЛЕ) чи *квантовими вентилями*.

Квабітами, квантовими регістрами і КЛЕ називають як їхнє зображення в просторі станів, так і фізичну реалізацію.

Побудова фізичного пристрою, який би реалізував квантовий біт, і був придатний для формування квантових регістрів, достатньо великих для ефективного перетворення інформації, є принциповою проблемою квантових обчислень сьогодні.

Моделлю, яка дає змогу описати функціонування квантових пристроїв для перетворення інформації, є модель спіну s=1/2. До неї можна звести більшість цікавих для квантової інформатики фізичних систем як мікроскопічних, так і макроскопічних, якщо останні виявляють квантові властивості, як, наприклад, надпровідні системи. Такі моделі називають *псевдоспіновими*.

У цьому розділі розглянуто простий квантово-механічний опис будови квантових бітів, а також формування одноквабітових КЛЕ імпульсами гармонічного магнітного поля та двоквабітових КЛЕ, що формуються також за допомогою міжспінової взаємодії.

2.1 Модель спіну s=1/2

Спіновими моделями s=1/2 називають системи частинок зі спіном s=1/2, координатні частини хвильових функцій яких є постійними або несуттєвими в аналізованих процесах.

Спін s=1/2 описують трьома просторовими координатами, оператори яких задовольняють комутаційні співвідношення

$$[\mathbf{s}^x, \mathbf{s}^y] = i\hbar\mathbf{s}^z,$$

де індекси (x, y, z) утворюють циклічну перестановку. Експериментально встановлено, що $\mathbf{s}^z$ компонента спіну може мати власні значення $\hbar/2$ і $-\hbar/2$, відповідні власні вектори позначимо $|\uparrow\rangle$ і $|\downarrow\rangle$. Вибравши їх за базис у просторі станів спіну $\mathcal{H}$, довільний вектор можна утворити як суперпозицію

$$|\psi\rangle = c_\uparrow |\uparrow\rangle + c_\downarrow |\downarrow\rangle .$$

Зобразимо цей вектор як вектор-стовпець, який далі позначатимемо

$$|\psi\rangle = \begin{bmatrix} c_\uparrow \\ c_\downarrow \end{bmatrix}$$

і називатимемо спінором. Базисні вектори в спінорному зображенні мають вигляд:

$$|\uparrow\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |\downarrow\rangle = \begin{bmatrix}0\\1\end{bmatrix},$$

вони є ортонормованими. В цьому базисі оператори компонент спіну $\mathbf{s}^\alpha = \hbar\boldsymbol{\sigma}^\alpha/2$ зображають матрицями Паулі:

$$\boldsymbol{\sigma}^x = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \qquad \boldsymbol{\sigma}^y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}, \qquad \boldsymbol{\sigma}^z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}.$$

Ці самоспряжені оператори задовольняють співвідношення:

$$(\boldsymbol{\sigma}^\alpha)^2 = \mathbf{I}_2 = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \ \boldsymbol{\sigma}^x\boldsymbol{\sigma}^y = i\boldsymbol{\sigma}^z, \ (x,y,z); \qquad \left[\boldsymbol{\sigma}^\alpha, \boldsymbol{\sigma}^\beta\right]_+ = 2\mathbf{I}\delta_{\alpha,\beta}.$$

Якщо спін перебуває у власному стані $|\uparrow\rangle$ оператора $\boldsymbol{\sigma}^z$ з власним значенням $+1$, то стверджують, що спін спрямований уздовж осі z.

Покажемо, що власні вектори оператора

$$(\vec{m}\vec{\boldsymbol{s}}) = \frac{\hbar}{2}(\vec{m}\vec{\boldsymbol{\sigma}}) = \frac{\hbar}{2}\begin{bmatrix}\cos\theta & e^{-i\varphi}\sin\theta\\ e^{+i\varphi}\sin\theta & -\cos\theta\end{bmatrix} \tag{2.2}$$

описують спін, зорієнтований у координатному просторі вздовж ($\lambda = +\hbar/2$) одиничного вектора

$$\vec{m} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta) \tag{2.3}$$

або назустріч йому ($\lambda = -\hbar/2$). У спінорному зображенні власні вектори оператора (2.2) мають вигляд:

$$\lambda_+ = +\frac{\hbar}{2}, \ |\psi_+(\vec{m})\rangle = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{+i\varphi}\sin\frac{\theta}{2}\end{bmatrix} = \cos\frac{\theta}{2}\,|\uparrow\rangle + e^{+i\varphi}\sin\frac{\theta}{2}\,|\downarrow\rangle,$$
$$\lambda_- = -\frac{\hbar}{2}, \ |\psi_-(\vec{m})\rangle = \begin{bmatrix}-e^{-i\varphi}\sin\frac{\theta}{2}\\ \cos\frac{\theta}{2}\end{bmatrix} = -e^{-i\varphi}\sin\frac{\theta}{2}\,|\uparrow\rangle + \cos\frac{\theta}{2}\,|\downarrow\rangle. \tag{2.4}$$

Поворотом на кут θ навколо одиничного вектора (див. рис. 2.1)

$$\vec{n} = (-\sin\varphi, \cos\varphi, 0) \tag{2.5}$$

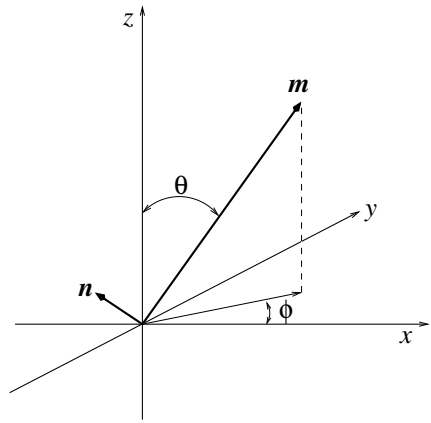


Рис. 2.1: Поворот осі z до напряму вектора $\vec{m}$

у тривимірному евклідовому просторі вектор $\vec{m}' = (0, 0, 1)$, спрямований вздовж осі z, суміщається з вектором $\vec{m}$ (2.3).

У просторі станів спіну s=1/2 поворот у тривимірному координатному просторі на кут θ навколо довільного одиничного вектора $\vec{n}$ описується унітарним оператором (тут покладено $\hbar = 1$)

$$\mathbf{R}(\vec{n}, \theta) = e^{-i\theta(\vec{n}\vec{s})} = e^{-i\frac{\theta}{2}(\vec{n}\vec{\boldsymbol{\sigma}})} = \mathbf{I}\cos\frac{\theta}{2} - i(\vec{n}\vec{\boldsymbol{\sigma}})\sin\frac{\theta}{2}.$$

Спряжений оператор можна отримати заміною

$$\mathbf{R}^\dagger(\vec{n}, \theta) = \mathbf{R}(\vec{n}, -\theta) = \mathbf{R}(-\vec{n}, \theta).$$

Оператор повороту навколо вектора (2.5) на кут θ зобразимо:

$$\mathbf{R}(\vec{n}, \theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -e^{-i\varphi}\sin\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}.$$

Легко перевірити, що

$$\mathbf{R}(\vec{n}, \theta)\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{bmatrix}, \qquad \mathbf{R}(\vec{n}, \theta)\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -e^{-i\varphi}\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{bmatrix},$$

а також

$$\mathbf{R}(\vec{n}, \theta)\boldsymbol{\sigma}^z\mathbf{R}(\vec{n}, -\theta) = \mathbf{R}(\vec{n}, \theta)(\vec{m}'\vec{\boldsymbol{\sigma}})\mathbf{R}(\vec{n}, -\theta) = (\vec{m}\vec{\boldsymbol{\sigma}})$$

оскільки $\boldsymbol{\sigma}^z = (\vec{m}'\vec{\boldsymbol{\sigma}})$, де $\vec{m}' = (0,0,1)$.

Акцентуємо на одній властивості такого перетворення спінорів

$$\mathbf{R}(\vec{n}, 2\pi) = -\mathbf{I}$$

при повороті спіну на кут 2π спінор змінює знак. Для окремого спіну цей ефект неспостережуваний унаслідок довільності фазового множника, але в системі спінів ця зміна знака є суттєвою.

Отже, стан спіну $s{=}1/2$ в його просторі станів $\mathcal{H}$ однозначно пов'язаний із одиничним вектором у тривимірному координатному просторі (вектором Блоха). Сфера, яку утворюють кінцеві точки цього одиничного вектора, називається сферою Блоха. Сфера Блоха є дуже зручною інтерпретацією станів одного спіну, однак подібної геометричної інтерпретації для двох і більше спінів побудувати не вдається.

Треба пам'ятати, що вектор, пов'язаний із спіном, є тільки зручною інтерпретацією спінорів (2.4) і зовсім не означає, що спін "має" точні значення всіх компонент одночасно. Результати вимірювання їхніх значень задовольняють умову невизначеності (1.8).

2.2 Матриця густини одного спіну

Нехай спін перебуває у стані $|\psi_+(\vec{m})\rangle$ (2.4), тоді матриця густини цього чистого стану має вигляд:

$$\begin{aligned}\boldsymbol{\rho}_+ = |\psi_+(\vec{m})\rangle\langle\psi_+(\vec{m})| &= \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2}\end{bmatrix}\begin{bmatrix}\cos\frac{\theta}{2} & e^{-i\varphi}\sin\frac{\theta}{2}\end{bmatrix}\\ &= \frac{1}{2}\begin{bmatrix}1+\cos\theta & e^{-i\varphi}\sin\theta\\ e^{i\varphi}\sin\theta & 1-\cos\theta\end{bmatrix} = \frac{1}{2}\left[\mathbf{I} + (\vec{m}\vec{\boldsymbol{\sigma}})\right].\end{aligned}$$

Матриця густини спіну у власному стані оператора $(\vec{m}\vec{\boldsymbol{\sigma}})$ із власним значенням $\lambda{=}-1$ зображається подібно:

$$\boldsymbol{\rho}_- = |\psi_-(\vec{m})\rangle\langle\psi_-(\vec{m})| = \frac{1}{2}\left[\mathbf{I} - (\vec{m}\vec{\boldsymbol{\sigma}})\right].$$

Оскільки для одиничного вектора виконується рівність $(\vec{m}\boldsymbol{\sigma})^2{=}\mathbf{I}$, то очевидним є співвідношення $\boldsymbol{\rho}_\pm^2 = \boldsymbol{\rho}_\pm$.

Розглянемо змішаний ансамбль, у якому окрему систему з імовірністю w_+ можна знайти в стані $|\psi_+(\vec{m})\rangle$ і з ймовірністю w_- — в стані $|\psi_-(\vec{m})\rangle$ ($0 \le w_+, w_- \le 1$, $w_+ + w_- = 1$). Його матриця густини дорівнює:

$$\boldsymbol{\rho}=w_+\boldsymbol{\rho}_+ + w_-\boldsymbol{\rho}_- = \frac{1}{2}\left[\mathbf{I} + (w_+ - w_-)(\vec{m}\vec{\boldsymbol{\sigma}})\right] = \frac{1}{2}\left[\mathbf{I} + (\vec{m}'\vec{\boldsymbol{\sigma}})\right].$$

Для цієї матриці

$$\boldsymbol{\rho}^2 = \frac{1}{4}\left[\mathbf{I} + (w_+ - w_-)^2\mathbf{I} + 2(w_+ - w_-)(\vec{m}\vec{\boldsymbol{\sigma}})\right] \neq \boldsymbol{\rho},$$

оскільки

$$|\vec{m}'|^2 = (w_+ - w_-)^2 < 1.$$

Якщо кожному чистому стану зіставити одиничний вектор $\vec{m}$, то всій множині чистих станів буде відповідати сфера Блоха з радіусом, що дорівнює одиниці. Усім змішаним станам відповідає внутрішній простір сфери Блоха — куля $0 \le |\vec{m}|^2 < 1$. Матриця густини одного спіну, загалом, залежить від трьох дійсних параметрів (координат вектора $\vec{\mathbf{m}}$), в чистому стані вона (як і вектор стану) залежить тільки від двох параметрів.

Чистий стан спіну s=1/2 від змішаного відрізняється тим, що повертанням вимірюваних приладів можна знайти напрям, проекція на який дорівнює $\hbar/2$, тобто, ймовірність знайти спін в стані $|\psi_+(\vec{m})\rangle$ дорівнює 1. Для змішаних станів це неможливо, ймовірність буде завжди < 1.

Будь-який змішаний стан можна безліччю способів утворити з двох інших станів (змішаних і чистих). Нехай

$$\boldsymbol{\rho}(\vec{n}_j) = \frac{1}{2}\left[\mathbf{I} + (\vec{n}_j\vec{\boldsymbol{\sigma}})\right] \quad —$$

чисті стани спінів спрямованих уздовж $\vec{n}_1$ і $\vec{n}_2$ (див. рис. 2.2), тоді можна сформувати змішаний стан

$$\boldsymbol{\rho}(\vec{n}) = \gamma\boldsymbol{\rho}(\vec{n}_1) + (1-\gamma)\boldsymbol{\rho}(\vec{n}_2), \tag{2.6}$$

де $0 \le \gamma \le 1$ і $\gamma/(1-\gamma) = |BC|/|AC|$. Із чистих станів, визначених векторами $\vec{n}_1$ і $\vec{n}_2$, відповідним вибором γ можна утворити

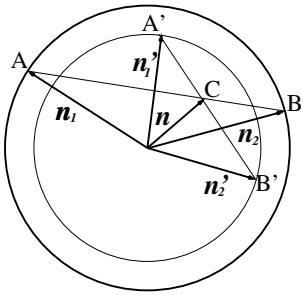


Рис. 2.2: Змішані стани можна утворити безліччю способів

довільний змішаний стан $\boldsymbol{\rho}(\vec{n})$, кінець вектора $\vec{n}$ якого лежить на відрізку AB.

Цей стан можна утворити і зі змішаних станів $\boldsymbol{\rho}(\vec{n}_j')$

$$\boldsymbol{\rho}(\vec{n}) = \gamma'\boldsymbol{\rho}(\vec{n}_1') + (1-\gamma')\boldsymbol{\rho}(\vec{n}_2'),$$

де $0 \le \gamma' \le 1$ і $\gamma'/(1-\gamma') = |B'C|/|A'C|$.

Підмножина елементів лінійного простору, які задовольняють вираз (2.6), називають опуклою підмножиною. Отже, оператори густини змішаних станів утворюють опуклу підмножину N-вимірного простору станів. Чисті стани не можна виразити формулою (2.6) — вони є крайніми точками цієї підмножини.

2.3 Еволюція стану одного спіну в магнітному полі

Досі в цьому розділі ми розглядали стани моделі s=1/2 і їхні зміни формально, не пов'язуючи з процесами, які їх реалізують. Для опису процесів формування квантового біта і керування його станами розглянемо більш реалістичну модель спінів ядер окремих атомів у складі великих органічних молекул, які є достатньо добре ізольовані, щоб формувати квантовий біт, і водночас доступні для керування їхніми станами.

Гамільтоніан частинки зі спіном s=1/2 в зовнішньому магнітному полі $\vec{B}$, при несуттєвості руху в координатному просторі,

запишемо [1]

$$\mathcal{H} = -g\mu\vec{\mathbf{s}}\vec{B},$$

де μ — магнетон і g–фактори відповідної частинки. Для електрона, протона і нейтрона вони мають такі значення:

$$g_e \approx -2\left(1+\frac{\alpha}{2\pi}-0.327\frac{\alpha^2}{\pi^2}\right), \quad g_p \approx 2.792782, \quad g_n \approx -1.913139,$$
$$\mu_e = \frac{|e|\hbar}{2m_e c} = \mu_B, \quad \mu_p = \frac{m_e}{m_p}\mu_B, \quad \mu_n \approx \mu_p; \qquad \vec{\mathbf{s}} = \frac{1}{2}\vec{\boldsymbol{\sigma}}.$$

(α=$e^2/\hbar c$≈1/137 — стала тонкої структури, μ_B — магнетон Бора)

Розгляньмо магнітне поле, яке є суперпозицією поля сталого величиною B_0, скерованого вздовж осі z, і змінного в площині xy величиною b. Вектор змінного поля в початковий момент часу був спрямований уздовж осі x_0 лабораторної системи відліку та обертається за годинниковою стрілкою, якщо $\omega > 0$, і — проти годинникової стрілки, якщо $\omega < 0$

$$\vec{B} = (b\cos\omega t, -b\sin\omega t, B_0), \qquad |B_0| \gg |b|.$$

Гамільтоніан спіну в такому полі має вигляд:

$$\mathcal{H} = -g\mu\vec{\mathbf{s}}\vec{B} = -\frac{\hbar\omega_0}{2}\boldsymbol{\sigma}^z - \frac{\hbar\Omega_0}{2}\left(\cos\omega t\boldsymbol{\sigma}^x - \sin\omega t\boldsymbol{\sigma}^y\right),$$

де

$$\omega_0 \equiv \frac{g\mu B_0}{\hbar}, \qquad \Omega_0 \equiv \frac{g\mu b}{\hbar} \quad -$$

частоти, які іноді називають частотами Лармора, хоча відрізняються від них множниками Ланде. Зрозуміло, що $|\omega_0| \gg |\Omega_0|$.

Для початку розглянемо тільки стале поле B_0, поклавши b=0

$$\mathcal{H} = -\frac{\hbar\omega_0}{2}\boldsymbol{\sigma}^z.$$

У цьому випадку спін має два власні стани:

$$E_- = -\frac{\hbar\omega_0}{2}, \quad |\uparrow\rangle \equiv |0\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix}; \qquad E_+ = +\frac{\hbar\omega_0}{2}, \quad |\downarrow\rangle \equiv |1\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix},$$

коли спін спрямований уздовж поля z (стан $|\uparrow\rangle$), і в протилежному напрямі (стан $|\downarrow\rangle$). Частота переходу між цими станами дорівнює ω_0. Це частковий випадок добре відомого розщеплення Зеемана.

Щоби дослідити часову еволюцію спіну в постійному магнітному полі, побудуємо унітарний оператор еволюції в картині Шредингера. Користуючись рівнянням

$$i\hbar\frac{d}{dt}|\psi\rangle = \mathfrak{H}|\psi\rangle$$

знаходимо

$$\mathbf{U} = e^{i\frac{\omega_0 t}{2}\boldsymbol{\sigma}^z} = \mathbf{I}\cos\frac{\omega_0 t}{2} + i\boldsymbol{\sigma}^z\sin\frac{\omega_0 t}{2} = \begin{bmatrix} e^{i\frac{\omega_0 t}{2}} & 0 \\ 0 & e^{-i\frac{\omega_0 t}{2}} \end{bmatrix}.$$

Якщо в початковий момент часу спін був спрямований уздовж вектора $\vec{m}(0) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$, то в момент часу t він буде в стані

$$\begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i(\varphi-\omega_0 t)}\sin\frac{\theta}{2} \end{bmatrix},$$

тобто, буде скерований у напрямі

$$\vec{m}(t) = (\sin\theta\cos(\varphi-\omega_0 t), \sin\theta\sin(\varphi-\omega_0 t), \cos\theta).$$

Отже, спін регулярно прецесує навколо напряму поля (тобто навколо осі z) з постійним кутом θ, частота цієї прецесії ω_0 залежить від величини магнітного поля B_0 і гіромагнітного відношення $g\mu$ частинки зі спіном.

Однак, якщо початково спін був спрямований уздовж постійного поля (осі z) і θ=0, тобто, був приготований у стані $|0\rangle$ з енергією E_-, то прецесія не відбувається і спін залишається в цьому стані. Так само спін не змінює свого стану $|1\rangle$ з енергією E_+ (θ=π) під дією сталого магнітного поля, спрямованого вздовж осі z. Отже, ці стани є стаціонарними і можуть формувати квабіт $\{|0\rangle, |1\rangle\}$.

Повернімось тепер до випадку змінного магнітного поля. Знайдемо оператор еволюції з рівняння Шредингера

$$i\frac{d}{dt}|\psi\rangle = \left[-\frac{\omega_0}{2}\boldsymbol{\sigma}^z - \frac{\Omega_0}{2}(\cos\omega t\boldsymbol{\sigma}^x - \sin\omega t\boldsymbol{\sigma}^y)\right]|\psi\rangle,$$

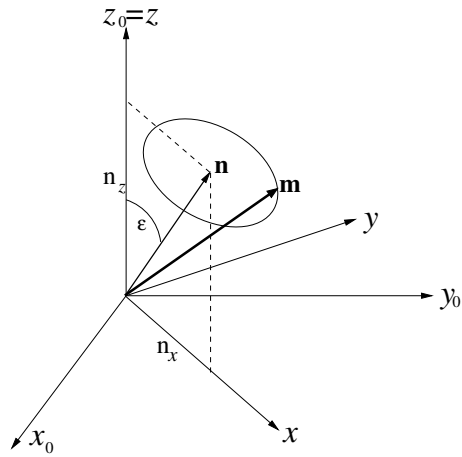


Рис. 2.3: Рух спіну навколо напряму ефективного поля в системі відліку, що обертається

для цього перейдемо до системи відліку, що обертається разом із магнітним полем, за допомогою унітарного оператора

$$\mathbf{U}_R = e^{i\omega t\boldsymbol{\sigma}^z/2}, \qquad |\psi\rangle = \mathbf{U}_R\,|\psi_r\rangle\,. \tag{2.7}$$

Легко встановити, що

$$\mathbf{U}_R^+\boldsymbol{\sigma}^x\mathbf{U}_R = \cos\omega t\boldsymbol{\sigma}^x + \sin\omega t\boldsymbol{\sigma}^y,$$
$$\mathbf{U}_R^+\boldsymbol{\sigma}^y\mathbf{U}_R = \cos\omega t\boldsymbol{\sigma}^y - \sin\omega t\boldsymbol{\sigma}^x.$$

У новій системі відліку рівняння Шредингера має вигляд:

$$i\frac{d}{dt}\,|\psi_r\rangle = -\left[\frac{\omega_0-\omega}{2}\boldsymbol{\sigma}^z + \frac{\Omega_0}{2}\boldsymbol{\sigma}^x\right]|\psi_r\rangle\,.$$

Гамільтоніан у системі відліку, що обертається

$$\mathcal{H}_r = -\hbar\left[\frac{\omega_0-\omega}{2}\boldsymbol{\sigma}^z + \frac{\Omega_0}{2}\boldsymbol{\sigma}^x\right]$$

не залежить від часу, тому еволюцію спіну в змінному магнітому

полі в цій системі відліку можна описати унітарним оператором

$$\mathbf{U}_r = e^{i\left[\frac{\omega_0-\omega}{2}\boldsymbol{\sigma}^z+\frac{\Omega_0}{2}\boldsymbol{\sigma}^x\right]t} = e^{i\frac{\Omega t}{2}(\vec{n}\vec{\boldsymbol{\sigma}})}$$
$$= \mathbf{I}\cos\frac{\Omega t}{2} + i\,(\vec{n}\vec{\boldsymbol{\sigma}})\sin\frac{\Omega t}{2}, \qquad (2.8)$$

де введено координати одиничного вектора, навколо якого обертається спін

$$n_x = \sin\varepsilon = \frac{\Omega_0}{\Omega}, \quad n_y = 0, \quad n_z = \cos\varepsilon = \frac{\omega_0-\omega}{\Omega},$$
$$\Omega = \sqrt{(\omega_0-\omega)^2+\Omega_0^2}.$$

У лабораторній системі відліку при цьому перетворенні базисні вектори так змінюються з часом

$$|\psi(t)\rangle = \mathbf{U}_R\mathbf{U}_r|0\rangle$$
$$= e^{i\omega t/2}\left(\cos\frac{\Omega t}{2} + i\sin\frac{\Omega t}{2}\cos\varepsilon\right)|0\rangle - ie^{-i\omega t/2}\sin\frac{\Omega t}{2}\sin\varepsilon|1\rangle,$$
$$|\varphi(t)\rangle = \mathbf{U}_R\mathbf{U}_r|1\rangle$$
$$= ie^{i\omega t/2}\sin\frac{\Omega t}{2}\sin\varepsilon|0\rangle + e^{-i\omega t/2}\left(\cos\frac{\Omega t}{2} - i\sin\frac{\Omega t}{2}\cos\varepsilon\right)|1\rangle. \qquad (2.9)$$

З виразу (2.8) видно, що в системі відліку, що обертається з магнітним полем, спін із частотою Ω обертається навколо вектора $\vec{n}$, який збігається з напрямом деякого ефективного поля. На рис. 2.3 вектор $\vec{m}$ вказує напрям спіну, а (x_0, y_0, z_0) — осі координат лабораторної системи відліку. В лабораторній системі відліку прецесія спіну навколо вектора $\vec{n}$ виглядає як нутація, оскільки в лабораторній системі відліку регулярно "прецесує" вектор $\vec{n}$ (ефективне поле).

Поклавши $\omega = \omega_0$ (умова резонансу), скеруємо це ефективне поле (вектор $\vec{n}$) уздовж напряму змінного магнітного поля, тобто, уздовж осі x системи відліку, що обертається. Тоді в рухомій системі відліку спін регулярно прецесує навколо "сталого поля" $\mathbf{b}$ з частотою $\Omega{=}\Omega_0$. Якщо в цьому випадку початково спін був скерований уздовж сталого поля B_0 (осі z), тобто, перебував у стані $|0\rangle$ з енергією E_-, то за час $t{=}\pi/\Omega$ він змінить напрям на

протилежний, тобто, перейде в стан $|1\rangle$ з енергією E_+ і далі буде осцилювати між станами $|0\rangle$ і $|1\rangle$. Вектор $\vec{m}$ при цьому буде описувати кола в площині yz. Такі періодичні переходи між двома станами під впливом гармонічного зовнішнього поля називають *осциляціями Рабі*, а частоти цих переходів — *частотами Рабі*.

Отже, унітарний оператор $\mathbf{U}_r$ в цьому випадку описує поворот спіну навколо осі x системи відліку, що обертається

$$\mathbf{X}(\varphi) = \mathbf{U}_r = \begin{bmatrix} \cos\frac{\varphi}{2} & i\sin\frac{\varphi}{2} \\ i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix}, \tag{2.10}$$

де $\varphi \equiv \Omega_0 t$. Вибравши тривалість імпульсів такою, щоб $\varphi = \pi/2$ і $\varphi = \pi$, (так звані $\pi/2$, та π-імпульси), отримаємо оператори:

$$\mathbf{X}\left(\pm\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & \pm i \\ \pm i & 1 \end{bmatrix}, \qquad \mathbf{X}\left(\pm\pi\right) = \pm i\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.11}$$

Якщо змінити фазу поля, що обертається, так, щоб у початковий момент часу його вектор був спрямований уздовж осі y

$$\vec{B} = (b\sin\omega t, b\cos\omega t, B_0),$$

то замість оператора (2.10) отримаємо оператор повороту навколо осі y системи відліку, що обертається:

$$\mathbf{Y}(\varphi) = \mathbf{U}_r = \begin{bmatrix} \cos\frac{\varphi}{2} & \sin\frac{\varphi}{2} \\ -\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix}. \tag{2.12}$$

Таке поле призводить до тих самих осциляцій Рабі, тільки вектор $\vec{m}$ тепер описує кола в площині xz рухомої системи координат.

За допомогою $\pi/2$–імпульсів можна сформувати так звані *псевдооператори Адамара*:

$$\mathbf{Y}\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \equiv \mathbf{h}, \quad \mathbf{Y}\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \mathbf{h}^{-1}, \tag{2.13}$$

а за допомогою π-імпульсів — оператори:

$$\mathbf{Y}\left(\pm\pi\right) = \begin{bmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{bmatrix}.$$

Оператори (2.10), (2.11) та (2.13) дають змогу побудувати оператор Адамара (з точністю до фази)

$$\mathbf{H} = -i\mathbf{Y}\left(\frac{\pi}{2}\right)\mathbf{X}(\pi) = -i\mathbf{X}(\pi)\,\mathbf{Y}\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},$$

а також оператор повороту навколо осі z

$$\mathbf{Z}(\varphi) = \mathbf{Y}\left(\frac{\pi}{2}\right)\mathbf{X}(\varphi)\,\mathbf{Y}\left(-\frac{\pi}{2}\right) = \begin{bmatrix}e^{i\varphi/2} & 0\\ 0 & e^{-i\varphi/2}\end{bmatrix}, \qquad (2.14)$$

який є оператором зміни фази (з точністю до загального фазового множника)

$$\mathbf{Z}(\varphi) = e^{i\varphi/2}\begin{bmatrix}1 & 0\\ 0 & e^{-i\varphi}\end{bmatrix} = e^{i\varphi/2}\mathbf{\Phi}(-\varphi).$$

Отже, оператори (2.10) та (2.12) дають змогу побудувати довільний одноквабітовий оператор, що здійснює переходи між усіма станами в просторі станів $\mathcal{H}$ квабіта. Підкреслимо, що ці оператори описують дію імпульсів зовнішнього гармонічного магнітного поля на спін частинки. В методі ядерного магнітного резонансу (ЯМР) вони називаються радіочастотними імпульсами. Зауважимо також, що оператори (2.10), (2.12) та їхні часткові випадки визначені в системі координат, що обертається навколо осі z_0 лабораторної системи відліку. Перехід до лабораторної системи відліку здійснюється унітарним оператором $\mathbf{U}_R$ (2.7), а він залишає незмінними тільки стани $|0\rangle$ та $|1\rangle$ (множить їх на фазовий множник), всі інші стани в лабораторній системі відліку залежать від часу, бо спін, зафіксований у рухомій системі відліку, обертається в лабораторній. Обчислення потребують, щоб у проміжках між дією квантових логічних елементів квабіти не змінювали свого стану. Цю проблему можна розв'язати в той спосіб, що в проміжку між діями квантових вентилів дати змогу квабітам змінювати стан, але так, щоб на початок дії наступного КЛЕ квабіт підійшов у стані, який він мав на момент закінчення дії попереднього КЛЕ. Методи такого фіксування станів розглянемо пізніше.

2.4 Проектування станів спіну

Нехай спін s=1/2 спрямовано вздовж одиничного вектора $\vec{m}$ (2.3), тобто він перебуває у власному стані оператора $(\vec{m}\vec{\boldsymbol{\sigma}})$ з власним значенням $+1$ і власним вектором $|\psi_+(\vec{m})\rangle$. Ймовірність знайти в експерименті, що спін спрямований уздовж осі z, визначають за формулою

$$w_z^{\uparrow} = |\langle\uparrow|\psi_+(\vec{m})\rangle|^2 = \langle\psi_+(\vec{m})|\,\mathbf{P}_z^{\uparrow}\,|\psi_+(\vec{m})\rangle\,,$$

де

$$\mathbf{P}_z^{\uparrow} = |\uparrow\rangle\langle\uparrow| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \quad -$$

проектор на стан $|\uparrow\rangle$. Тоді

$$w_z^{\uparrow} = \begin{bmatrix}\cos\frac{\theta}{2} & e^{-i\varphi}\sin\frac{\theta}{2}\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2}\end{bmatrix} = \cos^2\frac{\theta}{2}.$$

Після такого вимірювання спін із ймовірністю $w_z^{\uparrow}$ перейде у стан

$$\frac{\mathbf{P}_z^{\uparrow}|\psi_+(\vec{m})\rangle}{\sqrt{w_z^{\uparrow}}} = \begin{bmatrix}1\\0\end{bmatrix} = |\uparrow\rangle, \tag{2.15}$$

та з ймовірністю $1 - w_z^{\uparrow} = \sin^2\frac{\theta}{2}$ — в стан $|\downarrow\rangle$, що легко отримати за допомогою проектора на стан $|\downarrow\rangle$

$$\mathbf{P}_z^{\downarrow} = |\downarrow\rangle\langle\downarrow| = \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix},$$

а це дає

$$w_z^{\downarrow} = |\langle\downarrow|\psi_+(\vec{m})\rangle|^2 = \langle\psi_+(\vec{m})|\,\mathbf{P}_z^{\downarrow}\,|\psi_+(\vec{m})\rangle = \sin^2\frac{\theta}{2}.$$

Загалом спін із змішаного стану

$$\boldsymbol{\rho}(\vec{m}) = \frac{1}{2}\left[\boldsymbol{I} + (\vec{m}\vec{\boldsymbol{\sigma}})\right], \quad 0 \le |\vec{m}| < 1$$

після проектування на окремий власний стан $|\varphi_\lambda(\vec{n})\rangle$ оператора $(\vec{n}\vec{\boldsymbol{\sigma}})$ з ймовірністю:

$$w = \mathrm{Sp}\left(\mathbf{P}_\lambda(\vec{n})\boldsymbol{\rho}(\vec{m})\mathbf{P}_\lambda(\vec{n})\right), \quad \mathbf{P}_\lambda(\vec{n}) \equiv |\varphi_\lambda(\vec{n})\rangle\langle\varphi_\lambda(\vec{n})|$$

перейде в чистий стан:

$$\frac{\mathbf{P}_\lambda(\vec{n})\boldsymbol{\rho}(\vec{m})\mathbf{P}_\lambda(\vec{n})}{\mathrm{Sp}\left(\mathbf{P}_\lambda(\vec{n})\boldsymbol{\rho}(\vec{m})\right)} = |\varphi_\lambda(\vec{n})\rangle\langle\varphi_\lambda(\vec{n})|.$$

Проектування чистого стану $\boldsymbol{\rho}(\vec{m}) = |\psi_\mu(\vec{m})\rangle\langle\psi_\mu(\vec{m})|$ переведе його в стан $|\varphi_\lambda(\vec{n})\rangle$:

$$\frac{\mathbf{P}_\lambda(\vec{n})|\psi_\mu(\vec{m})\rangle}{\sqrt{\langle\psi_\mu(\vec{m})|\mathbf{P}_\lambda(\vec{n})|\psi_\mu(\vec{m})\rangle}} = \frac{|\varphi_\lambda(\vec{n})\rangle\langle\varphi_\lambda(\vec{n})|\psi_\mu(\vec{m})\rangle}{|\langle\varphi_\lambda(\vec{n})|\psi_\mu(\vec{m})\rangle|},$$

з точністю до фазового множника. Що є частковим випадком проектування довільного стану $|\psi\rangle$ на довільний стан $|\varphi\rangle$

$$|\psi\rangle \to \frac{|\varphi\rangle\langle\varphi|\psi\rangle}{|\langle\varphi|\psi\rangle|} = e^{i\alpha}|\varphi\rangle.$$

Одночасне ж проектування на обидва стани $|\varphi_{\lambda_1}(\vec{n})\rangle$ і $|\varphi_{\lambda_2}(\vec{n})\rangle$ переводить як чистий, так і змішаний стани у змішаний стан:

$$\boldsymbol{\rho}(\vec{m}) \to \sum_{i=1}^{2} \mathbf{P}_{\lambda_i}(\vec{n})\boldsymbol{\rho}(\vec{m})\mathbf{P}_{\lambda_i}(\vec{n}).$$

Знайдемо тепер результат проектування станів спіну (2.9) після дії радіочастотного імпульсу тривалістю t на базові стани. З ймовірністю:

$$\cos^2\frac{\Omega t}{2} + \sin^2\frac{\Omega t}{2}\cos^2\varepsilon$$

стан $|\psi(t)\rangle$ перейде у стан $|0\rangle$, а стан $|\varphi(t)\rangle$ — у стан $|1\rangle$. Відповідно, з ймовірністю

$$\sin^2\frac{\Omega t}{2}\sin^2\varepsilon$$

стан $|\psi(t)\rangle$ перейде у стан $|1\rangle$, а стан $|\varphi(t)\rangle$ — у стан $|0\rangle$. Знову спостерігаємо осциляції Рабі — при $\sin\varepsilon = 1$ стани $|0\rangle$ і $|1\rangle$ повторюються з періодом $T = 2\pi/\Omega$.

2.5 Двоспінові системи

Досі ми розглядали систему з одного ізольованого спіну. Його стани описують векторами двовимірного простору станів $\mathcal{H}$, в якому за базис вибрано власні вектори z-компоненти оператора спіну

$$|\uparrow\rangle_z \equiv |\uparrow\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |\downarrow\rangle_z \equiv |\downarrow\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

Стани системи, що складається з двох спінів, описують векторами в чотиривимірному просторі станів, який є прямим (тензорним) добутком просторів станів окремих спінів $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. За базис у цьому просторі можна вибрати всі прямі (тензорні) добутки базисних векторів просторів станів окремих спінів, які в матричному зображенні можна записати як прямі (кронекерові) добутки векторів-стовпців (див. Додаток)

$$|\uparrow\rangle_1 |\uparrow\rangle_2 \equiv |\uparrow\rangle \otimes |\uparrow\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad |\uparrow\rangle_1 |\downarrow\rangle_2 \equiv |\uparrow\rangle \otimes |\downarrow\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$
$$|\downarrow\rangle_1 |\uparrow\rangle_2 \equiv |\downarrow\rangle \otimes |\uparrow\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad |\downarrow\rangle_1 |\downarrow\rangle_2 \equiv |\downarrow\rangle \otimes |\downarrow\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}. \qquad (2.16)$$

Подібно будують зображення тензорних добутків матриць операторів, зокрема, компонент спіну

$$\boldsymbol{\sigma}_1^x \boldsymbol{\sigma}_2^x \equiv \boldsymbol{\sigma}^x \otimes \boldsymbol{\sigma}^x = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \otimes \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} = \begin{bmatrix}0 & 0 & 0 & 1\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\1 & 0 & 0 & 0\end{bmatrix},$$
$$\boldsymbol{\sigma}_1^y \boldsymbol{\sigma}_2^y \equiv \boldsymbol{\sigma}^y \otimes \boldsymbol{\sigma}^y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix} \otimes \begin{bmatrix}0 & -i\\i & 0\end{bmatrix} = \begin{bmatrix}0 & 0 & 0 & -1\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\-1 & 0 & 0 & 0\end{bmatrix},$$

$$\boldsymbol{\sigma}_1^z\boldsymbol{\sigma}_2^z \equiv \boldsymbol{\sigma}^z \otimes \boldsymbol{\sigma}^z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\otimes\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}. \quad (2.17)$$

Якщо записувати в добутках оператори і вектори-стовпці окремих спінів так, щоб їхні номери зростали зліва направо, можна індекси номерів упускати, оскільки правило побудови кронекерових добутків гарантує правильну дію операторів і правильне множення відповідних компонент векторів-стовпців.

Окремий (ізольований) спін може взаємодіяти тільки із зовнішнім магнітним полем. Два і більше спінів, розташовані достатньо близько, можуть взаємодіяти також між собою. У реальних системах ця взаємодія має складну фізичну природу. Доволі загальний гамільтоніан L спінів у вузлах одновимірної ґратки із обмінною взаємодією найближчих сусідів у символічному записі такий

$$\mathcal{H} = -\sum_{j=1}^{L} h_j\boldsymbol{\sigma}_j^z + \sum_{j=1}^{L-1}\sum_{\alpha,\beta=\{x,y,z\}} J_j^{\alpha\beta}\boldsymbol{\sigma}_j^\alpha\boldsymbol{\sigma}_{j+1}^\beta,$$

де h_j — зовнішнє магнітне поле, яке діє на спін у вузлі номер j, а $J_j^{\alpha\beta}$ — константи взаємодій між α і β –компонентами спінів на вузлах j і $j{+}1$. Розглянемо анізотропну модель Гайзенберга двох спінів у зовнішньому полі з гамільтоніаном

$$\mathcal{H} = -h_1\boldsymbol{\sigma}_1^z - h_2\boldsymbol{\sigma}_2^z + J^x\boldsymbol{\sigma}_1^x\boldsymbol{\sigma}_2^x + J^y\boldsymbol{\sigma}_1^y\boldsymbol{\sigma}_2^y + J^z\boldsymbol{\sigma}_1^z\boldsymbol{\sigma}_2^z,$$

чи у тензорному записі —

$$\mathcal{H} = -h_1\boldsymbol{\sigma}^z\otimes\mathbf{I} - h_2\mathbf{I}\otimes\boldsymbol{\sigma}^z + \sum_{\alpha=\{x,y,z\}} J^\alpha\boldsymbol{\sigma}^\alpha\otimes\boldsymbol{\sigma}^\alpha. \quad (2.18)$$

Тут позначено $J^{\alpha\alpha}\equiv J^\alpha$. За допомогою виразів (2.17) матрицю цього гамільтоніана в базисі (2.16) можна зобразити:

$$\mathcal{H} = \begin{bmatrix}-h_1-h_2+J^z & 0 & 0 & J^x-J^y\\ 0 & -h_1+h_2-J^z & J^x+J^y & 0\\ 0 & J^x+J^y & h_1-h_2-J^z & 0\\ J^x-J^y & 0 & 0 & h_1+h_2+J^z\end{bmatrix}. \quad (2.19)$$

У загальнішому випадку з цілком анізотропною взаємодією між спінами $J^x \neq J^y \neq J^z$ власні значення і (ненормовані) власні чотирикомпонентні вектори цього гамільтоніана мають вигляд:

$$\lambda_1 = J^z - b, \qquad |\tilde{\lambda}_1\rangle = \frac{-b-h_1-h_2}{J^x-J^y}|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2;$$
$$\lambda_2 = J^z + b, \qquad |\tilde{\lambda}_2\rangle = \frac{b-h_1-h_2}{J^x-J^y}|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2;$$
$$\lambda_3 = -J^z + a, \qquad |\tilde{\lambda}_3\rangle = \frac{a-h_1+h_2}{J^x+J^y}|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2;$$
$$\lambda_4 = -J^z - a, \qquad |\tilde{\lambda}_4\rangle = \frac{-a-h_1+h_2}{J^x+J^y}|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2;$$
$$a \equiv \sqrt{(J^x+J^y)^2+(h_1-h_2)^2}, \quad b \equiv \sqrt{(J^x-J^y)^2+(h_1+h_2)^2}, \quad (2.20)$$

це свідчить, що тоді всі стани є несепарабельними. Після нормування із загальних виразів (2.20) можна знайти окремі часткові варіанти, які наведено нижче.

Найпростішим випадком є модель Ізінга J^x=J^y=0, тоді власні стани двоспінової системи є сепарабельними

$$\lambda_1 = -h_1 - h_2 + J^z, \qquad |\lambda_1\rangle = |0\rangle_1|0\rangle_2;$$
$$\lambda_2 = h_1 + h_2 + J^z, \qquad |\lambda_4\rangle = |1\rangle_1|1\rangle_2;$$
$$\lambda_3 = -h_1 + h_2 - J^z, \qquad |\lambda_2\rangle = |0\rangle_1|1\rangle_2;$$
$$\lambda_4 = h_1 - h_2 - J^z, \qquad |\lambda_3\rangle = |1\rangle_1|0\rangle_2;$$

оскільки частина гамільтоніана, що описує міжспінову взаємодію, комутує із частиною, що відповідає за взаємодію спінів із зовнішнім полем.

В іншому випадку $J^x = J^y = J$

$$\lambda_1{=}{-}h_1{-}h_2{+}J^z,\ |\lambda_1\rangle{=}|0\rangle_1|0\rangle_2; \quad \lambda_2{=}h_1{+}h_2{+}J^z,\ |\lambda_2\rangle{=}|1\rangle_1|1\rangle_2;$$
$$\lambda_3 = a - J^z,$$
$$|\lambda_3\rangle = \frac{1}{\sqrt{2a}}\left(\sqrt{a{-}h_1{+}h_2}|0\rangle_1|1\rangle_2 + \sqrt{a{+}h_1{-}h_2}|1\rangle_1|0\rangle_2\right);$$
$$\lambda_4 = -a - J^z,$$
$$|\lambda_4\rangle = \frac{1}{\sqrt{2a}}\left(\sqrt{a{+}h_1{-}h_2}|0\rangle_1|1\rangle_2 - \sqrt{a{-}h_1{+}h_2}|1\rangle_1|0\rangle_2\right);$$
$$a \equiv \sqrt{4J^2 + (h_1 - h_2)^2},$$

два стани є сепарабельні, а два — заплутані. Ці пари поміняються місцями для $J^x = -J^y$. Зрозуміло, що останні вирази справедливі і для ізотропної моделі Гайзенберга $J^x = J^y = J^z = J$.

Коли зовнішнє поле відсутнє ($h_1 = h_2 = 0$) гамільтоніан (2.19) має власні значення і власні вектори:

$$\begin{aligned}
\beta_1 &= J^z + J^x - J^y, \quad |\beta_1\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\,|\uparrow\rangle + |\downarrow\rangle\,|\downarrow\rangle\right);\\
\beta_2 &= J^z - J^x + J^y, \quad |\beta_2\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\,|\uparrow\rangle - |\downarrow\rangle\,|\downarrow\rangle\right);\\
\beta_3 &= -J^z + J^x + J^y, \quad |\beta_3\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\,|\downarrow\rangle + |\downarrow\rangle\,|\uparrow\rangle\right);\\
\beta_4 &= -J^z - J^x - J^y, \quad |\beta_4\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\,|\downarrow\rangle - |\downarrow\rangle\,|\uparrow\rangle\right);
\end{aligned} \tag{2.21}$$

які утворюють відомий базис Белла, вони описують максимально заплутані стани двох спінів.

2.6 Еволюція двох взаємодіючих спінів

Найпростіше побудувати оператор гамільтонової еволюції, використовуючи його спектральне зображення:

$$\mathbf{U}(t) = \exp(-i\mathfrak{H}t/\hbar) = \sum_j \exp(-i\lambda_j t/\hbar)|\lambda_j\rangle\langle\lambda_j|.$$

Базисні стани двоспінової системи змінюються із часом так:

$$\begin{aligned}
\mathbf{U}(t)|00\rangle &= \mathrm{e}^{-iJ^z t/\hbar}\left[\left(\cos\frac{bt}{\hbar} + i\frac{h_+}{b}\sin\frac{bt}{\hbar}\right)|00\rangle - i\frac{J^-}{b}\sin\frac{bt}{\hbar}|11\rangle\right],\\
\mathbf{U}(t)|11\rangle &= \mathrm{e}^{-iJ^z t/\hbar}\left[\left(\cos\frac{bt}{\hbar} - i\frac{h_+}{b}\sin\frac{bt}{\hbar}\right)|11\rangle - i\frac{J^-}{b}\sin\frac{bt}{\hbar}|00\rangle\right],\\
\mathbf{U}(t)|01\rangle &= \mathrm{e}^{iJ^z t/\hbar}\left[\left(\cos\frac{at}{\hbar} + i\frac{h_-}{a}\sin\frac{at}{\hbar}\right)|01\rangle - i\frac{J^+}{a}\sin\frac{at}{\hbar}|10\rangle\right],\\
\mathbf{U}(t)|10\rangle &= \mathrm{e}^{iJ^z t/\hbar}\left[\left(\cos\frac{at}{\hbar} - i\frac{h_-}{a}\sin\frac{at}{\hbar}\right)|10\rangle - i\frac{J^+}{a}\sin\frac{at}{\hbar}|01\rangle\right].
\end{aligned}$$

$$a \equiv \sqrt{(J^+)^2 + (h_-)^2}, \quad b \equiv \sqrt{(J^-)^2 + (h_+)^2},$$

$$J^\pm \equiv J^x \pm J^y, \quad h_\pm \equiv h_1 \pm h_2. \tag{2.22}$$

Подібно еволюціонують і стани Белла (2.21).

З цих виразів випливає, що еволюція, генерована гамільтоніаном (2.18), розділяє простір станів на два підпростори, до яких належать базисні вектори $\{|00\rangle, |11\rangle\}$ чи $\{|\beta_1\rangle, |\beta_2\rangle\}$ та $\{|01\rangle, |10\rangle\}$ чи $\{|\beta_3\rangle, |\beta_4\rangle\}$, відповідно. Зв'язок між цими підпросторами можна встановлювати описаними вище радіочастотними імпульсами. У кожному з цих підпросторів стани спінів заплутуються, але в моменти часу кратні $T{=}2\pi\hbar/b$ (чи $T{=}2\pi\hbar/a$) вони факторизуються. Якщо ж зовнішні поля (що формують квантові біти) дорівнюють нулю, то ці стани осцилюють між двома базисними.

Розгляньмо тепер перший спін як основну систему, а другий — як оточення, і з'ясуймо вплив заплутування на стани основної системи. Нехай початковим був стан $|00\rangle$, тоді ймовірність знайти перший спін у стані $|0\rangle$ в деякий момент часу дорівнюватиме

$$\langle 00|\mathbf{U}^\dagger(t)\,(|0\rangle\langle 0|\otimes\mathbf{I})\,\mathbf{U}(t)|00\rangle = \cos^2\frac{bt}{\hbar} + \frac{h_+^2}{b^2}\sin^2\frac{bt}{\hbar}.$$

Якщо ж початковим був стан $|0\rangle\otimes\frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle)$, то ймовірність знайти перший спін у стані $|0\rangle$ дорівнюватиме

$$\frac{1}{2}\left(\cos^2\frac{bt}{\hbar} + \frac{h_+^2}{b^2}\sin^2\frac{bt}{\hbar} + \cos^2\frac{at}{\hbar} + \frac{h_-^2}{a^2}\sin^2\frac{at}{\hbar}\right).$$

Обидві ці ймовірності тим ближчі до одиниці, чим більші зовнішні поля $h_\pm$ в порівнянні з міжспіновою взаємодією $J^\pm$, а тому можна стверджувати, що тоді в будь-який момент часу стан двоспінової системи близький до сепарабельного $|0\rangle\otimes|\chi(t)\rangle$, де $|\chi(t)\rangle$ деякий вектор стану другого спіну. Те ж стосується і стану $|1\rangle$.

З виразів (2.22) також випливає, що за умови формування стійких квантових бітів, тобто, $|h_\pm| \gg |J^\pm|$, динаміка моделі Гайзенберга є ефективно близькою до динаміки моделі Ізінга, оскільки у виразах (2.22) можна знехтувати величинами J^x, J^y. Це суттєво спрощує її опис.

Проаналізуємо часову еволюцію двох спінів із взаємодією Ізінга, але в дещо інших термінах. Результати використаємо пізніше для формування двоквабітових вентилів у квантових процесорах на основі ядерного магнітного резонансу.

Вище ми формально вважали, що взаємодія різних спінів із зовнішнім магнітним полем є різною, цього не можна досягти створенням сталого зовнішнього поля різної напруженості, оскільки частинки зі спіном мусять бути дуже близько розташованими, щоби спіни взаємодіяли між собою. Спіни $s{=}1/2$ частинок, поміщених у стале однорідне магнітне поле B_0, будуть мати різні частоти

$$\omega_{01} \equiv \omega_1 = \frac{h_1}{\hbar} = \frac{g_1\mu_1 B_0}{\hbar}, \qquad \omega_{02} \equiv \omega_2 = \frac{h_2}{\hbar} = \frac{g_2\mu_2 B_0}{\hbar}$$

прецесії навколо напряму цього поля, якщо в них будуть різні гіромагнітні відношення. Частину гамільтоніна, що описує між-

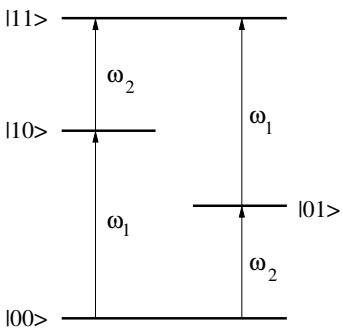


Рис. 2.4: Схема рівнів двоспінової системи без взаємодії

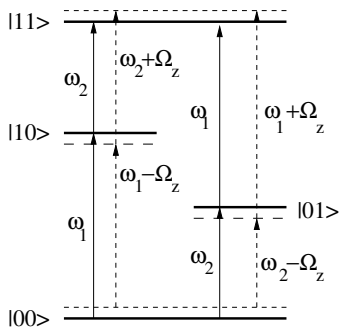


Рис. 2.5: Схема рівнів двоспінової системи із взаємодією

спінову взаємодію, запишемо через відносну частоту:

$$J^z \mathbf{s}_1^z \mathbf{s}_2^z = \frac{\hbar\Omega_z}{2} \boldsymbol{\sigma}_1^z \otimes \boldsymbol{\sigma}_2^z.$$

У реальних фізичних системах частоти прецесії ω_1 чи ω_2 в полі B_0, частоти прецесії в рухомій системі відліку Ω і частоти відносного обертання Ω_z співвідносяться $|\omega_{1,2}| \gg |\Omega| \gg |\Omega_z|$. Гамільтоніан (2.18) такої системи в просторі $\mathcal{H}_{12}{=}\mathcal{H}_1 \otimes \mathcal{H}_2$ зручно записати так:

$$\boldsymbol{\mathcal{H}} = -\frac{\hbar\omega_1}{2} \boldsymbol{\sigma}_1^z \otimes \mathbf{I}_2 - \frac{\hbar\omega_2}{2} \mathbf{I}_1 \otimes \boldsymbol{\sigma}_2^z + \frac{\hbar\Omega_z}{2} \boldsymbol{\sigma}_1^z \otimes \boldsymbol{\sigma}_2^z. \qquad (2.23)$$

Він не залежить від часу, тому оператор еволюції легко отримати:

$$\mathbf{U}_{12}(t) = e^{-\frac{i}{\hbar}\mathcal{H}t} = e^{i\frac{\omega_1 t}{2}\boldsymbol{\sigma}_1^z\otimes\mathbf{I}_2} e^{i\frac{\omega_2 t}{2}\mathbf{I}_1\otimes\boldsymbol{\sigma}_2^z} e^{-i\frac{\Omega_z t}{2}\boldsymbol{\sigma}_1^z\otimes\boldsymbol{\sigma}_2^z} = \left(\mathbf{Z}_1(\omega_1 t)\otimes\mathbf{Z}_2(\omega_2 t)\right)\mathbf{Z}_{12}(\Omega_z t),$$

і виразити його через оператори поворотів:

$$\mathbf{Z}_1(\varphi) = \cos\frac{\varphi}{2}\,\mathbf{I}_1 + i\sin\frac{\varphi}{2}\,\boldsymbol{\sigma}_1^z = \begin{bmatrix} e^{i\varphi/2} & 0 \\ 0 & e^{-i\varphi/2}\end{bmatrix},$$

$$\mathbf{Z}_{12}(\phi) = \cos\frac{\phi}{2}\,\mathbf{I}\otimes\mathbf{I} - i\sin\frac{\phi}{2}\,\boldsymbol{\sigma}^z\otimes\boldsymbol{\sigma}^z = \mathrm{diag}\left[e^{-i\phi/2}, e^{+i\phi/2}, e^{+i\phi/2}, e^{-i\phi/2}\right] \qquad (2.24)$$

з параметрами φ_1=$\omega_1 t$, φ_2=$\omega_2 t$, ϕ=$\Omega_z t$. У матричному зображенні він має вигляд:

$$e^{-\frac{i}{\hbar}\mathcal{H}t} = \mathbf{U}_{12}(t) = \left(\mathbf{Z}_1(\varphi_1)\otimes\mathbf{Z}_2(\varphi_2)\right)\mathbf{Z}_{12}(\phi) = \mathrm{diag}\left[e^{i(\varphi_1+\varphi_2-\phi)/2}; e^{i(\varphi_1-\varphi_2+\phi)/2}; e^{-i(\varphi_1-\varphi_2-\phi)/2}; e^{-i(\varphi_1+\varphi_2+\phi)/2}\right]. \qquad (2.25)$$

Розглянемо тепер як змінюються стани спінів номер 1 і 2, поміщених в стале магнітне поле. Нехай початкові стани спінів такі:

$$|\psi(0)\rangle_1 = |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |\psi(0)\rangle_2 = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i\varepsilon}\sin\frac{\theta}{2}\end{bmatrix}.$$

Після дії оператора $\mathbf{U}_{12}(t)$ (2.25) отримаємо часову залежність станів цих спінів:

$$\mathbf{U}_{12}(t)|\psi(0)\rangle_1|\psi(0)\rangle_2 = e^{i(\varphi_1+\varphi_2-\phi)/2}|\psi(t)\rangle_1|\psi(t)\rangle_2, \qquad (2.26)$$

де

$$|\psi(t)\rangle_1 = |\psi(0)\rangle_1 = |0\rangle, \quad |\psi(t)\rangle_2 = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i(\varepsilon-\varphi_2+\phi)}\sin\frac{\theta}{2}\end{bmatrix}. \qquad (2.27)$$

Якщо ж початковий стан спіну 1 був $|1\rangle$, то результат еволюції буде таким (з точністю до фазового множника)

$$|\psi(t)\rangle_1 = |\psi(0)\rangle_1 = |1\rangle, \quad |\psi(t)\rangle_2 = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i(\varepsilon-\varphi_2-\phi)}\sin\frac{\theta}{2}\end{bmatrix}. \qquad (2.28)$$

Стани (2.26), (2.27), (2.28) записано в лабораторній системі відліку. З цих виразів видно, що стан спіну 1 не змінюється з часом, а спін 2 прецесує навколо напряму магнітного поля. Взаємодія між спінами сповільнює прецесію в першому випадку і прискорює — в другому. Якщо перейти в систему відліку, що обертається разом із спіном 2 (для цього досить покласти в (2.26), (2.27), (2.28) $\varphi_2 = 0$), то спостерігатимемо прецесію спіну 2 навколо напряму спіну 1 в додатному напрямі, якщо спін 1 спрямований у додатному напрямі осі z, і — прецесію у від'ємному напрямі, якщо спін 1 спрямований протилежно.

Тобто, оператор $\mathbf{Z}_{12}(\phi)$ повертає спін 2 навколо спіну 1 на кут ϕ проти годинникової стрілки.

Як бачимо з формул (2.27), (2.28), стани спінів не заплутуються, якщо початково один із них перебуває в стані $|0\rangle$ чи $|1\rangle$. В цьому випадку еволюцію системи двох спінів можна інтерпретувати як рух двох точок по сфері Блоха.

Акцентуємо на одній важливій обставині. Параметри реальних частинок зі спінами є такі, що частоти ω_1 і ω_2 на багато порядків перевищують частоти Ω_z, і тому для формування кутів повороту φ_1 і φ_2, співмірних з ϕ, треба створювати імпульси дуже малої тривалості, а це технічно неможливо. Тому для виконання поворотів навколо осі z використовують не прецесію $\mathbf{Z}_1(\varphi_1)$ (2.24), а послідовності дій (2.14). Тому надалі символами $\mathbf{Z}_1(\varphi_1)$, $\mathbf{Z}_2(\varphi_2)$ і подібними будемо позначати саме послідовності дій (2.14). Реальну ж прецесію усунути неможливо, тому для її нейтралізування використовують методи синхронізації, про які ми вже згадували і які будуть розглянуті пізніше.

Вибравши тривалості імпульсів такими, щоб $\varphi_1{=}\varphi_2{=}\phi{=}\varphi$, отримаємо з (2.25) двоквабітовий оператор фази (з точністю до несуттєвого фазового множника)

$$\begin{aligned}(\mathbf{Z}_1(\varphi)\otimes\mathbf{Z}_2(\varphi))\,\mathbf{Z}_{12}(\varphi) &= e^{i\frac{\varphi}{2}}\mathbf{B}(-2\varphi)\\ &= e^{i\frac{\varphi}{2}}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{-i2\varphi}\end{bmatrix},\end{aligned}$$

звідки:

$$\mathbf{B}(\varphi) = (\mathbf{Z}_1(-\varphi/2) \otimes \mathbf{Z}_2(-\varphi/2))\, \mathbf{Z}_{12}(-\varphi/2).$$

Очевидно, що в операторі $\mathbf{B}(\pi)$ можна вибрати протилежний знак:

$$\mathbf{B}(\pi) = (\mathbf{Z}_1(\pi/2) \otimes \mathbf{Z}_2(\pi/2))\, \mathbf{Z}_{12}(\pi/2).$$

Тоді двоквабітовий оператор **CNOT** матиме таку структуру:

$$\begin{aligned} \mathbf{CNOT} &= (\mathbf{I}_1 \otimes \mathbf{Y}_2\,(-\pi/2))\, \mathbf{B}(\pi)\, (\mathbf{I}_1 \otimes \mathbf{Y}_2\,(\pi/2)) \\ &= (\mathbf{I}_1 \otimes \mathbf{Y}_2\,(-\pi/2))\, e^{i\pi/4}\, (\mathbf{Z}_1\,(\pi/2) \otimes \mathbf{I}_2) \\ &\quad (\mathbf{I}_1 \otimes \mathbf{Z}_2\,(\pi/2))\, \mathbf{Z}_{12}\,(\pi/2)\, (\mathbf{I}_1 \otimes \mathbf{Y}_2\,(\pi/2))\,. \end{aligned} \tag{2.29}$$

Кути $-\varphi$ треба розуміти як $2\pi - \varphi$. Нагадаємо, що оператори $\mathbf{Z}(\varphi)$ насправді є добутком операторів (2.14),

$$\mathbf{Z}\,(\varphi) = \mathbf{Y}\left(\frac{\pi}{2}\right) \mathbf{X}\,(\varphi)\, \mathbf{Y}\left(-\frac{\pi}{2}\right)$$

тобто, формуються трьома послідовними імпульсами гармонічного поля $\mathbf{b}$, а не прецесією навколо осі z, спричиненою сильним постійним полем B_0. Тому час повороту в цьому випадку є набагато більший, аніж час повороту на той самий кут за рахунок прецесії в полі B_0.

Докладніше квантові вентилі розглянемо пізніше.

2.7 Синхронізація квантових вентилів

Як було зауважено раніше, в проміжках часу, коли на квабіт не діє квантовий вентиль (КЛЕ), у даному випадку – радіочастотний імпульс, спін із великою частотою ω_1 прецесує навколо постійного поля B_0. Для того, щоб усунути цей шкідливий природній рух, використовують прийом *рефокусування*, давно відомий у техніці ЯМР. Він ґрунтується на такій властивості операторів $\mathbf{Z}(\omega t)$:

$$\mathbf{X}(\pi)\mathbf{Z}(\omega t)\mathbf{X}(-\pi) = \mathbf{Z}(-\omega t),$$

яку можна сформулювати також у вигляді:

$$\mathbf{X}(\pi)\mathbf{Z}(\omega t)\mathbf{X}(-\pi)\mathbf{Z}(\omega t){=}\mathbf{I} \quad \text{чи} \quad \mathbf{Z}(\omega t)\mathbf{X}(\pi)\mathbf{Z}(\omega t)\mathbf{X}(-\pi){=}\mathbf{I}. \tag{2.30}$$

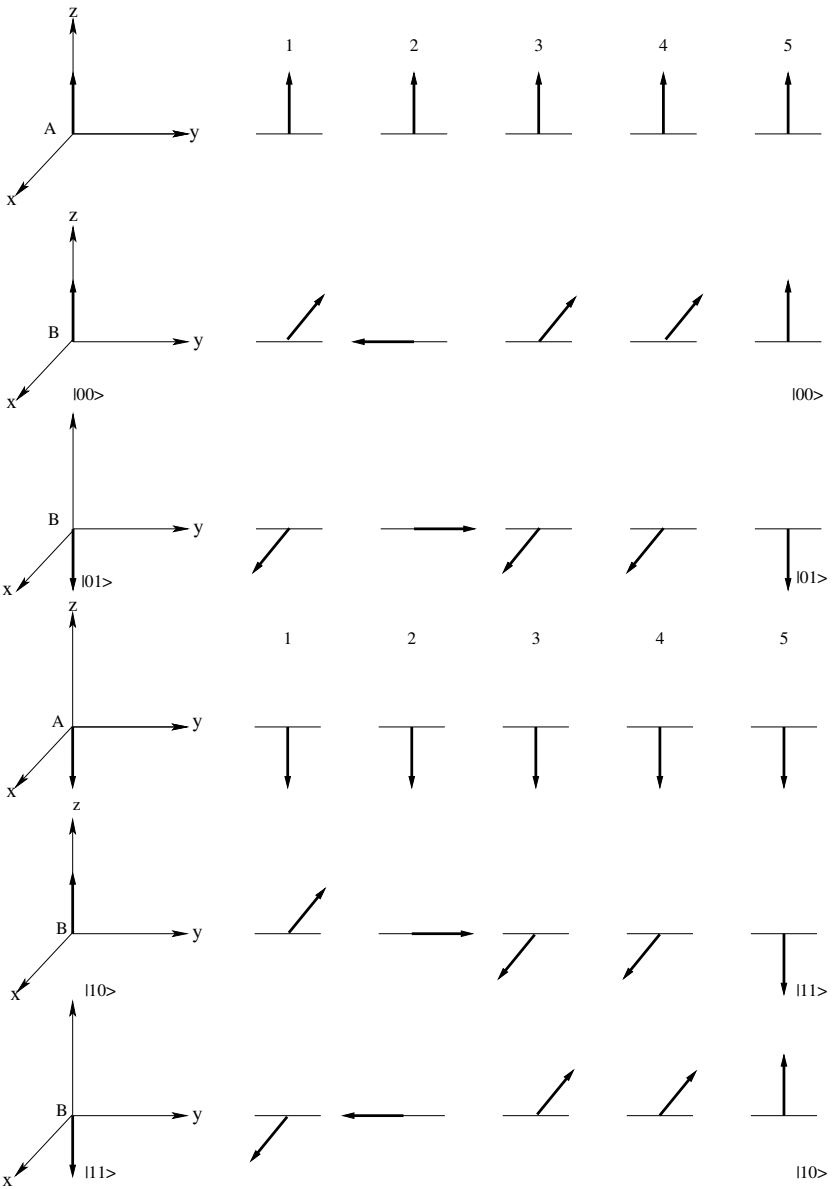


Рис. 2.6: Послідовність дій операторів **CNOT** (2.29) на спіни з різними початковими станами

Зрозуміло, що знак біля π в операторі $\mathbf{X}(\pi)$ несуттєвий, оскільки $\mathbf{X}(\pi) = -\mathbf{X}(-\pi)$. Отже, якщо на початку проміжку "простоювання" спіну подіяти на нього радіочастотним імпульсом $\mathbf{X}(\pi)$, а потім зробити те ж саме в середині цього проміжку, то спін прийде до початку дії наступного квантового вентиля в тому ж стані, в якому він був на кінець попереднього. З виразів (2.30) бачимо, що дію імпульсу $\mathbf{X}(\pi)$ можна перенести з початку проміжку "простоювання" на його кінець.

Подібними властивостями володіє і оператор відносного повороту спінів, зумовленого іхньою взаємодією,

$$\begin{aligned}(\mathbf{X}_1(\pi)\otimes\mathbf{I})\,\mathbf{Z}_{12}(\Omega_z t)\,(\mathbf{X}_1(-\pi)\otimes\mathbf{I}) &= \mathbf{Z}_{12}(-\Omega_z t),\\ (\mathbf{I}\otimes\mathbf{X}_2(\pi))\,\mathbf{Z}_{12}(\Omega_z t)\,(\mathbf{I}\otimes\mathbf{X}_2(-\pi)) &= \mathbf{Z}_{12}(-\Omega_z t).\end{aligned} \qquad (2.31)$$

Якщо на перший вираз у (2.31) подіяти оператором $(\mathbf{I}\otimes\mathbf{X}_2(\pi))$ чи на другий — оператором $(\mathbf{X}_1(\pi)\otimes\mathbf{I})$, то отримаємо:

$$(\mathbf{X}_1(\pi)\otimes\mathbf{X}_2(\pi))\,\mathbf{Z}_{12}(\Omega_z t)\,(\mathbf{X}_1(\pi)\otimes\mathbf{X}_2(\pi)) = \mathbf{Z}_{12}(\Omega_z t),$$

Для формування двоквабітових вентилів треба використовувати відносне обертання спінів, що відбувається завдяки міжспіновій взаємодії, тобто, "чисту" дію оператора $\mathbf{Z}_{12}(\Omega_z t)$, але фізично її можна реалізувати тільки оператором

$$(\mathbf{Z}_1(\omega_1 t)\otimes\mathbf{Z}_2(\omega_2 t))\,\mathbf{Z}_{12}(\Omega_z t), \qquad (2.32)$$

який містить шкідливе швидке обертання генероване дією операторів $\mathbf{Z}_1(\omega_1 t)$ і $\mathbf{Z}_2(\omega_2 t)$. Щоб його усунути, треба на початку (або в кінці) проміжку τ дії оператора (2.32) і в момент $\tau/2$ подіяти короткими імпульсами $\mathbf{X}_1(\pi)\otimes\mathbf{X}_2(\pi)$:

$$\begin{aligned}&(\mathbf{X}_1(\pi)\otimes\mathbf{X}_2(\pi))\left(\mathbf{Z}_1\left(\frac{\omega_1\tau}{2}\right)\otimes\mathbf{Z}_2\left(\frac{\omega_2\tau}{2}\right)\right)\mathbf{Z}_{12}\left(\frac{\Omega_z\tau}{2}\right)\\ &(\mathbf{X}_1(\pi)\otimes\mathbf{X}_2(\pi))\left(\mathbf{Z}_1\left(\frac{\omega_1\tau}{2}\right)\otimes\mathbf{Z}_2\left(\frac{\omega_2\tau}{2}\right)\right)\mathbf{Z}_{12}\left(\frac{\Omega_z\tau}{2}\right) = \mathbf{Z}_{12}\left(\Omega_z\tau\right),\end{aligned}$$

це нейтралізує дію операторів $\mathbf{Z}_1(\omega_1 t)$ і $\mathbf{Z}_2(\omega_2 t)$ і не зіпсує "чистої" дії оператора $\mathbf{Z}_{12}(\Omega_z\tau)$.

Розділ 3

Класичні обчислення. Обчислюваність. Складність

Багато задач математики, фізики, техніки та інших областей можна розглядати як обчислення функцій: для заданого набору вхідних параметрів (“аргументу”) розраховується вихідний набір параметрів (“значення функції”), тобто будується відображення з одного багатовимірного простору в інший багатовимірний простір. У вужчому сенсі відомі функції елементарні, алгебраїчні, трансцендентні, спеціальні та ін. Разом з іменем, пов’язаним з означенням, вони мають відповідні правила обчислення. Означенням функції можуть бути певні співвідношення, інтеграли, рівняння (алгебраїчні, трансцендентні, диференціальні, інтегральні та ін.). Одну й ту ж функцію можна означити як розв’язок деякого рівняння, як інтеграл, ланцюговий дріб, рекурентне співвідношення і т.п.. Це задає різні алгоритми для її обчислення. Проблема існування функції є проблемою математичного аналізу, а проблема обчислюваності функції належить до області теорії алгоритмів і абстрактних обчислювальних машин.

3.1 Обчислюваність

«Обчислюване дійсне число — дійсне число, для якого існує алгоритм, що знаходить як завгодно точні наближення до цього числа.» [18].

Обчислення виконують за допомогою *алгоритму*, що є послідовністю певних “механічних” дій, правильне виконання яких гарантує достовірний результат незалежно від кваліфікації ви-

конавця. Великі за об'ємом обчислення проводять на технічних пристроях, які називають *обчислювальними машинами* чи *комп'ютерами*. Теоретичною основою (математичною моделлю) обчислювальних машин, як технічних пристроїв (фізичних систем), є *абстрактні обчислювальні машини* (АОМ), які вивчають у *теорії автоматів* і в *теорії алгоритмів*, що є певними математичними системами, в рамках яких описують і аналізують АОМ та алгоритми. Вивчення АОМ дає змогу встановити також граничні можливості реальних обчислювальних машин. Історично першою АОМ і найпопулярнішою, є машина Тюринга (1936). Але функціонально ближчою до сучасних комп'ютерів та інтуїтивно зрозумілішою є ідеалізована машина з необмеженими регістрами (МНР), запропонована Шепердсоном і Стерджисом (1963), тому побіжно розглянемо її [19].

МНР складається з безмежної кількості регістрів, що позначаються через R_1, R_2, R_3, ..., R_j, ..., кожен з яких (R_j) містить деяке невід'ємне ціле число (r_j). МНР змінює вміст регістрів за деякими *командами*, що відповідають найпростішим операціям над числами. Скінченний список команд утворює *програму*. Для МНР визначені такі чотири базові команди:

1. *Команда занулення* $Z(j)$: $r_j := 0$,
2. *Команда додавання одиниці* $S(j)$: $r_j := r_j + 1$,
3. *Команда переадресування* $T(j,m)$: $r_j := r_m$,
4. *Команда умовного переходу*:

$$J(j,m;q): \begin{cases} \text{якщо } r_j = r_m, & \text{переходь на команду за номером } q, \\ \text{якщо } r_j \neq r_m, & \text{виконуй наступну команду}, \\ \text{якщо } q > p, & \text{stop} \end{cases}$$

(p номер останньої команди програми P).

МНР здійснює обчислення згідно програми P, починаючи з деякої початкової конфігурації $\{r_i = a_i\}$ (теоретично i може прямувати до ∞), і закінчує обчислення після скінченного числа кроків у кінцевій конфігурації $\{r_j = b_j\}$. Як правило, розглядають скінченні початкові $\{a_i\}$ та кінцеві $\{b_j\}$ конфігурації $1 \leq i \leq n$ і $1 \leq j \leq m$. Кажуть, що обчислення збігаються, якщо машина зупиняється і розбігаються, якщо машина не зупиняється.

Розглянемо функції $\mathbb{Z}^n \xrightarrow{f} \mathbb{Z}$, де $\mathbb{Z}$ — множина невід'ємних цілих чисел. Відомо, що такі функції складають незліченну множину, тоді як для МНР із чотирьох базисних команд можна збудувати зліченну множину програм [19].

Як тоді окреслити множину функцій, обчислюваних на МНР?

Обчислюваними є *основні* (*базові*) *функції:*

a) нуль-функція $\oslash$ ($\oslash(x) = 0$ для всіх x);

b) функція додавання одиниці $x + 1$;

c) функція проекції U_i^n:

$$U_i^n(x_1, x_2, \ldots, x_n) = x_i;\ 1 \le i \le n,\ n \ge 1.$$

Суперпозиція функцій. Нехай функції $f(y_1, \ldots, y_k)$ і $g_1(\mathbf{x}), \ldots, g_k(\mathbf{x})$, де $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, — є МНР обчислюваними функціями. Тоді і суперпозиція цих функцій $h(\mathbf{x}) \stackrel{def}{=} f(g_1(\mathbf{x}), \ldots, g_k(\mathbf{x}))$ також є МНР обчислюваною функцією.

Рекурсія. Нехай $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, $(x_j, y, z \in \mathbb{Z})$, а $f(\mathbf{x})$ і $g(\mathbf{x}, y, z)$ є функціями. Тоді існує єдина функція $h(\mathbf{x}, y)$, що задовольняє рівняння рекурсії:

$$h(\mathbf{x}, 0) = f(\mathbf{x}),$$

$$h(\mathbf{x}, y + 1) = g(\mathbf{x}, y, h(\mathbf{x}, y)).$$

Якщо $f(\mathbf{x})$ і $g(\mathbf{x}, y, z)$ — МНР обчислювані функції, то і $h(\mathbf{x}, y)$ — також МНР обчислювана функція.

Функції, отримані із базових функцій, суперпозиції і рекурсії, називають *примітивно рекурсивними функціями* [19]. До них належать:

a) $x + y$; b) $x \cdot y$; c) x^y;

d) $x \dot{-} 1$ $(0 - 1 = 0)$; e) $x \dot{-} y = \begin{cases} x - y, & x \ge y, \\ 0, & x \le y; \end{cases}$

f) $\mathrm{sg}(x) = \begin{cases} 1, & x = 0, \\ 0, & x \ne 0; \end{cases}$ g) $\overline{\mathrm{sg}}(x) = \begin{cases} 0, & x = 0, \\ 1, & x \ne 0; \end{cases}$

h) $|x - y|$; i) $x!$;

j) $\min(x, y)$; k) $\max(x, y)$;

l) $\mathrm{rm}(x, y)$ – залишок від ділення y на x $(\mathrm{rm}(0, y) \stackrel{\text{def}}{=} 0)$;

m) $\mathrm{qt}(x,y)$ – частка від ділення y на x $(\mathrm{qt}(0,y) \stackrel{\mathrm{def}}{=} 0)$;

$$\text{n) } \mathrm{div}(x,y) = \begin{cases} 1, & \text{якщо } x|y \ (x \text{ ділить } y), \\ 0, & \text{якщо } x \nmid y \ (x \text{ не ділить } y). \end{cases}$$

o) Скінченна сума і скінченний добуток обчислюваних функцій також є обчислюваною функцією.

За допомогою *оператора мінімізації* μ клас примітивно рекурсивних функцій розширюється до класу *рекурсивних функцій*. Оператор мінімізації μ визначають так: для довільної обчислюваної функції $f(\mathbf{x},y)$ оператор мінімізації $\mu y(f(\mathbf{x},y)=0)$ відбирає найменший розв'язок рівняння $f(\mathbf{x},y)=0$ відносно y. Іншими словами, оператор мінімізації визначає неявно задану функцію $y(\mathbf{x})$.

Функції, визначені на всій множині $\mathbb{Z}$ називають *тотальними*, в іншому випадку – *частковими* [19].

Класом $\mathcal{R}$ *частково рекурсивних функцій* називають найменший клас часткових функцій, що містить базисні функції $\oslash$, $x+1$, U_i^n і замкнутий відносно операцій суперпозиції, рекурсії і мінімізації.

Або, $\mathcal{R}$ – це клас часткових функцій, кожну з яких можна отримати з основних функцій за допомогою скінченного числа операцій суперпозиції, рекурсії і мінімізації [19].

У 30-60-их роках 20 ст. запропоновано інші АОМ і відповідні їм класи обчислюваних функцій, не обов'язково заданих конструктивно:

a) Гедель-Ербан-Кліні (1936): Загальнорекурсивні функції, визначені за допомогою числення рекурсивних рівнянь.

b) Черч (1936): λ–означені функції.

c) Гедель-Кліні (1936): μ–рекурсивні функції і частково рекурсивні функції.

d) Тюринг (1936): Функції, обчислювані машиною Тюринга.

e) Пост (1943): Функції, визначені канонічними дедуктивними системами.

f) Марков (1951): Функції, задані нормальними алгорифмами над скінченним алфавітом.

g) Шепердсон-Стерджис (1963): МНР розраховні функції.

В підсумку цих досліджень було отримано **основний результат**:

Всі ці уточнення поняття обчислюваності призводять до одного й того ж класу обчислюваних функцій $\mathcal{C}(\mathcal{T})$ — класу Тюринга.

Тобто, всі АОМ можуть обчислювати тільки функції з класу $\mathcal{C}(\mathcal{T})$. А реальні ОМ обчислюють функції, що творять підклас у $\mathcal{C}(\mathcal{T})$.

Доведено, що клас $\mathcal{C}(\mathcal{T})$ утворює зліченну множину, тобто, всі обчислювані функції можна перенумерувати натуральними числами $f_i(\mathbf{x})$, $\mathbf{x} = (x_1, \ldots, x_n)$, $n \to \infty$.

Функцію $F(y, \mathbf{x})$ називають *універсальною* функцією певного класу $\{\varphi_j(\mathbf{x})\}$, якщо всі функції цього класу отримуються з неї покладанням $y = j$, тобто, $\varphi_j(\mathbf{x}) = F(j, \mathbf{x})$.

АОМ, яка обчислює універсальну функцію класу $\mathcal{C}(\mathcal{T})$ називається *універсальною* АОМ. Іншими словами, універсальна АОМ моделює всі інші АОМ.

Зрозуміло, що ці означення не можуть претендувати на повноту і строгість, в тому сенсі, який прийнятий в цьому розділі математики. Однак, нашою метою є, радше, встановлення того факту, що не всі функції можуть бути алгоритмічно обчислюваними, і створення хоча б приблизного уявлення про клас обчислюваних функцій. Для докладнішого ознайомлення з проблемою обчислюваності функцій окрім книги [19] (на якій ґрунтується цей підрозділ) рекомендуємо книгу [20].

3.2 Складність алгоритмів

Іншою характеристикою алгоритмів є ефективність, яка показує як алгоритм використовує основні ресурси: час, простір, точність. Під простором розуміють кількість конструктивних елементів ОМ, потрібних для виконання алгоритму.

Алгоритми, які отримують на вході тільки аргументи функції, котру вони обчислюють, із послідовністю команд, що залежить тільки від функції і її аргументу, називають *детермінованими*. Якщо алгоритм на вході, крім аргументу функції, отримує деяку випадкову (напр. числову) послідовність, яка впливає на виконання алгоритму і, як наслідок, — на результат, достовірність якого визначається імовірністю (напр. $P{>}2/3$), називають *імовірніс-*

ними (або *рандомізованими*). До них, зокрема, належать Монте-Карло алгоритми.

Для різних функцій із класу $\mathcal{C}(\mathcal{T})$ використовують різні алгоритми, які працюють з різною ефективністю, що визначається тільки характером функції.

Нехай L – довжина вхідного слова ОМ. Для числа X це буде $L = \log_k(X)$, де k – основа кодування, прийнята в даній ОМ, найчастіше $k = 2$.

1. Алгоритми, які обчислюють функції за час $t \approx cL^m$, належать до класу складності $\mathcal{P}$ (*поліномного*).

2. Алгоритми, які за поліномний час $t = cL^m$ встановлюють чи випадково запропонований розв'язок є істинним ($y = f(\mathbf{x})$), входять до класу $\mathcal{NP}$ (*недетермінованого поліномного*). Відомо, що $\mathcal{P} \subseteq \mathcal{NP}$, існує проблема $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$.

3. Імовірнісні алгоритми належать до класу $\mathcal{BPP}$ (*bounded probability polynomial*), якщо за поліномний час $t = cL^m$ вони дають правильну відповідь $y = f(\mathbf{x})$ з імовірністю $P > P_0$.

4. $\mathcal{PSPACE}$ алгоритми потребують поліномного простору, тобто, пам'яті і числа логічних елементів.

5. $\mathcal{EXPTIME}$ алгоритми потребують експонентного часу виконання $t = c\exp(aL^r)$.

Очевидно, що алгоритми всіх цих класів складності обчислюють функції із класу обчислюваних функцій $\mathcal{C}(\mathcal{T})$.

Приклади.

1. Додавання, множення і ділення двох чисел довжини L потребує часу $t \simeq cL^2 \in \mathcal{P}$.

2. Обчислення найменшого спільного дільника (НСД) за алгоритмом Евкліда потребує часу $t \simeq cL^3 \in \mathcal{P}$.

3. Розпізнавання простоти. Число x просте чи складене? У 2002 році з'ясовано, що ця проблема належить до класу складності $\mathcal{P}$ [25], а $t \simeq cL^k, k \sim 10$.

4. Факторизація. Нехай x – складене, знайти p і q такі, що $x = pq$. Найкращий імовірнісний алгоритм потребує часу $t \simeq c2^{a\sqrt{L\log L}}$. Є алгоритми з оцінкою часу $t \simeq c2^{2L^{1/3}(\log L)^{2/3}}$, яка не доведена [21].

Нехай число x має 130 десяткових знаків, тобто, $L \approx 300$, тоді

час факторизації за другим алгоритмом при швидкодії комп'ютера 10^{12} оп/сек дорівнює 10^{18}сек (42 дні). Якщо ж $L = 600$, то $t \simeq 10^{25}$сек.

5. Алгоритм перетворення Фур'є для класичного процесора належить до класу складності $\mathcal{EXPTIME}$ з часом $t = c\exp(aL)$. Алгоритм швидкого перетворення Фур'є дає поліномне (квадратичне) прискорення $t = c\exp(aL/2)$.

Труднощі квантово-механічних задач ілюструє оцінка із статті [23]: «Для квантово-механічного розрахунку молекули метану треба провести обчислення за методом сіток в 10^{42} точках. Якщо вважати, що в кожній точці треба виконати всього 10 елементарних операцій, і припустити, що всі обчислення відбуваються при наднизькій температурі (T=3·10^{-3}K), то і при цьому розрахунок молекули метану потребує витрат енергії, що виробляється на Землі приблизно за століття.»

Отже, алгоритми (або задачі) можна поділити на легкі і складні. Легкі розв'язуються з поліномним використанням ресурсів, а складні — з експонентним. Зауважимо, що ці властивості алгоритмів проявляються при довгих вхідних словах. Для практичних задач з коротким входом навіть теоретично складні експонентні алгоритми можуть бути цілком ефективними.

У теорії алгоритмів не існує методів теоретичного доведення того, чи для певної задачі можна збудувати ефективний алгоритм. Це можна зробити створенням відповідного алгоритму [21].

Цей підрозділ, в основному, ґрунтується на книзі [21]. Детальніше з теорією алгоритмів можна ознайомитись за книгою [22].

3.3 Алгебра Буля і класичні комп'ютери

Алфавіти і команди АОМ можна реалізувати на алгебрі Буля, а операції алгебри Буля і її змінні, відповідно, можна фізично реалізувати як механічні чи електронні пристрої та їхні стани, що є основою для практичної побудови обчислювальних машин, як технічних пристроїв [24].

Довільне ціле невід'ємне число можна задати у двійковому

зображенні:

$$\mathbf{x} = x_n 2^n + x_{n-1} 2^{n-1} + \ldots + x_1 2 + x_0, \tag{3.1}$$

яке символічно записують:

$$\mathbf{x} = x_n x_{n-1} \cdots x_1 x_0, \tag{3.2}$$

де $x_j = \{0, 1\}$.

Ірраціональні числа зображають:

$$r = A_n 2^n + A_{n-1} 2^{n-1} + \ldots + A_1 2 + A_0 + \sum_{j=1}^{\infty} a_j 2^{-j}, \tag{3.3}$$

і записують:

$$r = A_n A_{n-1} \cdots A_1 A_0, a_1 a_2 \cdots a_j \cdots, \tag{3.4}$$

для раціональних чисел послідовність $\{a_j\}$ є періодичною. Надалі обмежимося розглядом тільки цілих невід'ємних чисел, оскільки всі інші (принаймні з достатньою точністю) можна виразити через них. Вирази (3.1)–(3.4) насправді є позначеннями чисел у двійковому зображенні, а не самими числами. У позиційному записі чисел при основі k використовуються k відмінних між собою символів. Правила виконання арифметичних дій аль-Хорезмі (алгоритми), сформульовані для позначень чисел в десятковому зображенні, чинні для дій з позначеннями чисел в довільному позиційному зображенні і призводять до позначень чисел–результатів цих дій. Розглянемо прості дії з числами (3.1)–(3.2).

$$\mathbf{7}{=}1 \cdot \mathbf{2^2}{+}1 \cdot \mathbf{2^1}{+}1 \cdot \mathbf{2^0}{=}111, \quad \mathbf{4}{=}1 \cdot \mathbf{2^2}{+}0 \cdot \mathbf{2^1}{+}0 \cdot \mathbf{2^2}{=}100; \tag{3.5}$$

а) додавання: $\mathbf{7} + \mathbf{4}{=}\mathbf{11}{=}1 \cdot \mathbf{2^3} + 0 \cdot \mathbf{2^2} + 1 \cdot \mathbf{2^1} + 1 \cdot \mathbf{2^0}{=}1011,$

$$\begin{array}{rr} & 111 \\ + & 100 \\ \hline & 1011 \end{array} \tag{3.6}$$

b) віднімання: $\mathbf{7-4=3}=1\cdot\mathbf{2^1}+1\cdot\mathbf{2^0}=11$,

$$\begin{array}{rr} & 111 \\ - & 100 \\ \hline & 011 \end{array} \tag{3.7}$$

c) множення: $\mathbf{7\times4=28}=1\cdot\mathbf{2^4}+1\cdot\mathbf{2^3}+1\cdot\mathbf{2^2}+0\cdot\mathbf{2^1}+0\cdot\mathbf{2^0}=11100$,

$$\begin{array}{rr} & 111 \\ \times & 100 \\ \hline & 000 \\ & 000 \\ & 111 \\ \hline & 11100 \end{array} \tag{3.8}$$

(Десяткові цифри зображено потовщеними символами.)

З прикладів (3.6)–(3.8) зауважуємо, що ці елементарні операції можна реалізувати фізично, якщо позиції в записі числа замінити дротиками рахівниці, коліщатками, магнітними кільцями чи транзисторами, а значення $0, 1$ — відповідно їхніми станами. Зміна цих станів під час виконання арифметичних операцій повинна відповідати алгоритмам (3.6)–(3.8) та подібним до них.

Хоча еволюція ОМ, як фізичної системи, під час виконання програми і підлягає фізичним законам, однак зміна (еволюція) виділених для зображення чисел станів визначається не фізичними законами, а програмою, яку виконує ОМ.

При виконанні операцій (3.6)–(3.8) використано такі правила:

$0+1=1+0=1, \quad 0+0=1+1=0$ — додавання за модулем 2;

$$0\cdot0=0\cdot1=1\cdot0=0, \qquad 1\cdot1=1.$$

Якщо числам 0 і 1 зіставити булеві змінні $\mathbf{O}$ і $\mathbf{I}$, а операціям $+$ та $\cdot$ зіставити логічні операції OR та AND, то можна виявити повну відповідність:

$$\begin{array}{lcl} 0\cdot0=0 & \leftrightarrow & \mathbf{O} \text{ AND } \mathbf{O}=\mathbf{O}; \\ 0\cdot1=0 & \leftrightarrow & \mathbf{O} \text{ AND } \mathbf{I}=\mathbf{O}; \\ 1\cdot0=0 & \leftrightarrow & \mathbf{I} \text{ AND } \mathbf{O}=\mathbf{O}; \\ 1\cdot1=1 & \leftrightarrow & \mathbf{I} \text{ AND } \mathbf{I}=\mathbf{I}; \end{array}$$

$$\begin{array}{lcl} 0+0=0 & \leftrightarrow & \mathbf{O}\ \ \mathrm{OR}\ \ \mathbf{O}=\mathbf{O}; \\ 0+1=1 & \leftrightarrow & \mathbf{O}\ \ \mathrm{OR}\ \ \mathbf{I}=\mathbf{I}; \\ 1+0=1 & \leftrightarrow & \mathbf{I}\ \ \mathrm{OR}\ \ \mathbf{O}=\mathbf{I}; \\ 1+1=0 & \leftrightarrow & \mathbf{I}\ \ \mathrm{OR}\ \ \mathbf{I}=\mathbf{I}; \end{array} \tag{3.9}$$

за винятком останнього рядка у (3.9), тому замість операції OR у комп'ютерах використовують операцію "виключного" OR (XOR), яка визначена такими правилами:

$$\begin{array}{lcl} 0+0=0 & \leftrightarrow & \mathbf{O}\ \ \mathrm{XOR}\ \ \mathbf{O}=\mathbf{O}; \\ 0+1=1 & \leftrightarrow & \mathbf{O}\ \ \mathrm{XOR}\ \ \mathbf{I}=\mathbf{I}; \\ 1+0=1 & \leftrightarrow & \mathbf{I}\ \ \mathrm{XOR}\ \ \mathbf{O}=\mathbf{I}; \\ 1+1=0 & \leftrightarrow & \mathbf{I}\ \ \mathrm{XOR}\ \ \mathbf{I}=\mathbf{O}. \end{array}$$

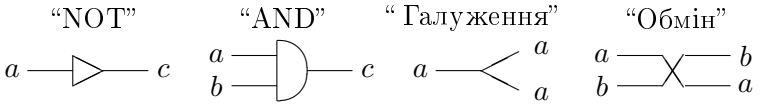
Окрім наведених бінарних, в алгебрі Буля є ще унарна операція заперечення NOT із властивостями:

$$\mathrm{NOT}\ \ \mathbf{I}=\mathbf{O}, \quad \mathrm{NOT}\ \ \mathbf{O}=\mathbf{I}.$$

Алгебри Буля достатньо для виконання дій (3.6)–(3.8) та збудованих із них арифметичних алгоритмів для обчислення всіх обчислюваних функцій.

В електроніці операції алгебри Буля реалізовують як технічні пристрої, які називають логічними елементами або вентилями, позначають їх так:

Доведено, що із скінченної кількості елементів "NOT", "AND", "OR" чи "XOR" можна збудувати скінченну універсальну обчислювальну машину [28]. Класичну обчислювальну машину можна збудувати і з меншої кількості елементів [28]:

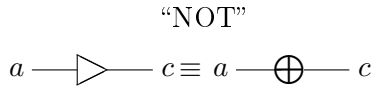


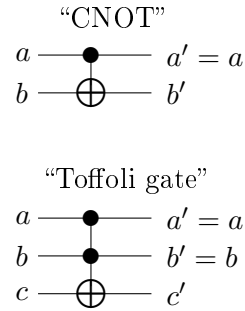
Тут лінії позначають провідники, якими подають стандартні напруги.

3.4 Зворотні обчислювальні машини

Легко зауважити, що одному й тому ж вихідному стану логічних елементів “AND”, “OR” чи “XOR” відповідають декілька вхідних, що свідчить про математичну незворотність цих логічних елементів. Класична обчислювальна машина, складена з незворотних елементів, є незворотною обчислювальною машиною, тобто, така ОМ, запущена в зворотному напрямі, не прийде до початкових даних навіть для детермінованих алгоритмів. З цією незворотністю пов’язували розсіювання тепла в процесі роботи обчислювальної машини, тобто, фізичну незворотність ОМ. Однак Чарльз Беннет (C.Bennet) на початку 80-х років довів, що із зворотних елементів можна збудувати зворотну ОМ, але розсіювання тепла неминуче залишається. Це відбувається під час операції занулення, яка є складовою частиною процесу обчислення. Тобто, як фізична система, класична ОМ є незворотною, іншими словами, не можна виконати математичні обчислення, не збільшивши ентропії в системі ОМ+оточення [28].

У працях Toffoli (1981) було запропоновано набір зворотних логічних елементів:





Логічний елемент "CNOT" (контрольоване "NOT") виконує логічну операцію "XOR".

Останній логічний елемент діє так, що c' =NOT c тільки тоді, коли $a = b = 1$, в інших випадках $c' = c$. Виявляється, що збудувати зворотну ОМ без елемента з трьома лініями ("Toffoli gate") **неможливо**, на противагу до незворотних машин. І навпаки, одного логічного елемента "Toffoli gate" достатньо для побудови зворотної ОМ, тому його називають **універсальним** логічним елементом.

Зрозуміло, що в математичному сенсі (як реалізація машини Тюринга), зворотна ОМ цілком еквівалентна незворотній ОМ.

Розділ 4

Квантовий регістр. Квантові логічні елементи

Головною "структурною" складовою квантового комп'ютера (процесора) є *квантовий регістр* — фізична система, утворена з достатньо великої кількості квантових бітів. Керування станами останніх виконують *квантовими логічними елементами* (*квантовими вентилями*), які в просторі станів регістра описують унітарними операторами. Послідовна дія таких КЛЕ реалізує квантовий алгоритм обчислення. Доведено, що існує базисний набір квантових вентилів, який дає змогу виконати довільне обчислення з потрібною точністю. В цьому розділі розглянемо деякі КЛЕ, які дають змогу такий набір утворити.

4.1 Квантовий регістр

Як і у класичному випадку, числу $\mathbf{x}$ в двійковому записі зіставимо фізичну систему, складену з n квантових бітів, кожен з яких відповідає певній позиції:

$$\mathbf{x} \leftrightarrow |\mathbf{x}\rangle \equiv |x_{n-1}x_{n-2}\ldots x_1x_0\rangle \equiv |x_{n-1}\rangle|x_{n-2}\rangle\ldots|x_1\rangle|x_0\rangle$$
$$\equiv |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \ldots \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle, \quad x_j = \{0,1\}.$$

Таку фізичну систему називають *квантовим регістром*. У базових станах квантових бітів $|0\rangle$ і $|1\rangle$ він визначає всі невід'ємні цілі числа від 0 ($|0\ldots0\rangle_n$) до $2^n{-}1$ ($|1\ldots1\rangle_n$) (арифметику за модулем 2^n в $\mathbb{Z}_n = \{0 \div 2^n{-}1\}$, як і відповідний класичний регістр). Базові стани квантового регістра називатимемо *обчислювальним базисом*. Класичну інформацію у квантовий регістр можна внести як

рядок базових станів квантових бітів регістра. Результат перетворення інформації в квантовому регістрі можна прочитати шляхом вимірювання кінцевого стану регістра в обчислювальному (тепер вже *вимірювальному*) базисі. В процесі роботи *квантовий процесор* буде перетворювати *квантову інформацію*.

Як ізольовану квантову систему його описують вектором стану в просторі станів вимірності 2^n, що є тензорним добутком n просторів станів окремих квабітів:

$$\mathcal{H}^{[n]} = \mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \ldots \otimes \mathcal{H}_0.$$

Оскільки кожній позиції числа ми зіставили відповідний квабіт, то це означає, що чітко розрізняємо квантові біти між собою, а тому хвильова функція не має жодної симетрії відносно перестановок змінних квабітів, тобто, вона не є ні симетричною, ні антисиметричною.

З квантової механіки відомо, що ізольована квантова система може контрольовано змінювати свій стан або в процесі унітарної еволюції, або в результаті вимірювань, тому тільки з таких процесів можна утворити єдиний процес перетворення інформації, записаної в квантовому регістрі. Тут будемо розглядати тільки проекти квантових процесорів із унітарними перетвореннями, хоча є також проекти з використанням вимірювання в процесі обчислення. Отже, обчислення можна записати як унітарне перетворення стану квантового регістра:

$$|\mathbf{x}(t)\rangle = \mathbf{U}(t)\,|\mathbf{x}(0)\rangle\,.$$

Обчислення складається з K кроків тривалістю Δt_j, у кожному з яких квантовий регістр еволюціонує зі своїм гамільтоніаном $\mathcal{H}_j$ і виконує певну дію з алгоритму розрахунку функції:

$$\mathbf{U}(t) = \mathbf{U}_K \mathbf{U}_{K-1} \ldots \mathbf{U}_1.$$

На кожному кроці оператор еволюції $\mathbf{U}_j$ охоплює $1 \div 2$ квабіти. Фізичні перетворення (операції), що описують цими операторами, називають *квантовими логічними елементами* (КЛЕ) чи *квантовими вентилями*, як і самі оператори та їх матриці.

Квантові логічні елементи реалізують унітарні перетворення, які є зворотними, тому вони є аналогами зворотних класичних логічних елементів. Унітарний квантовий комп'ютер є зворотним комп'ютером.

Як і в класичному випадку, існує певний базовий набір КЛЕ, поєднання яких дає змогу збудувати схему для обчислення довільної функції $\mathbf{x} \xrightarrow{f} \mathbf{y}$.

4.2 Одноквабітові вентилі

Нехай квабіт реалізовано на станах спіну s=1/2. Тоді оператор повороту спіну навколо одиничного вектора $\vec{n}$ на кут θ:

$$\mathbf{R}(\vec{n},\theta) = e^{-i\frac{\theta}{2}(\vec{n}\vec{\boldsymbol{\sigma}})} = \mathbf{I}\cos\frac{\theta}{2} - i(\vec{n}\vec{\boldsymbol{\sigma}})\sin\frac{\theta}{2}$$

дає змогу утворити оператор, що переводить спін із довільного стану на сфері Блоха в інший довільний стан[1]. Для цього використовуються такі оператори:
1) оператор повороту навколо осі y, коли $\vec{n} = (0,1,0)$

$$\mathbf{R}_y(\theta) = \mathbf{R}(\vec{n},\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

2) оператор повороту навколо осі z, коли $\vec{n} = (0,0,1)$

$$\mathbf{R}_z(\alpha) = \mathbf{R}(\vec{n},\alpha) = \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix}.$$

З них можна утворити найзагальніший трипараметричний оператор у $\mathbf{SU}(2)$ (групи унітарних перетворень у двовимірному просторі станів, детермінанти матриць яких дорівнюють одиниці)

$$\begin{aligned} \mathbf{W}(0;\alpha,\theta,\beta) &= \mathbf{R}_z(\alpha)\mathbf{R}_y(\theta)\mathbf{R}_z(\beta) \\ &= \begin{bmatrix} e^{-i\frac{\alpha+\beta}{2}}\cos\frac{\theta}{2} & -e^{-i\frac{\alpha-\beta}{2}}\sin\frac{\theta}{2} \\ e^{+i\frac{\alpha-\beta}{2}}\sin\frac{\theta}{2} & e^{+i\frac{\alpha+\beta}{2}}\cos\frac{\theta}{2} \end{bmatrix} \end{aligned} \tag{4.1}$$

[1]Зазвичай у підручниках оператор повороту означають $\mathbf{R}(\vec{n},\theta) = e^{i\frac{\theta}{2}(\vec{n}\vec{\boldsymbol{\sigma}})}$. Цей оператор описує поворот осей координат навколо $\vec{n}$.

Оператор $\mathbf{W}(\delta;\alpha,\theta,\beta) = e^{i\delta}\mathbf{W}(0;\alpha,\theta,\beta)$ дає змогу також будувати унітарні оператори $\mathbf{U}$, для яких $\det(\mathbf{U}) \neq 1$ (група $\mathbf{U}(2)$).

Зауважимо, що найзагальніший одноквабітовий оператор можна записати також формулою:

$$\mathbf{T}{=}a_0\mathbf{I} + a_x\boldsymbol{\sigma}^x + a_y\boldsymbol{\sigma}^y + a_z\boldsymbol{\sigma}^z, \tag{4.2}$$

чи використавши спектральні зображення матриць Паулі

$$\boldsymbol{\sigma}^0 = |0\rangle\langle 0| + |1\rangle\langle 1|,\ \boldsymbol{\sigma}^x = |0\rangle\langle 1| + |1\rangle\langle 0|,$$
$$\boldsymbol{\sigma}^y = i\left(|1\rangle\langle 0| - |0\rangle\langle 1|\right),\ \boldsymbol{\sigma}^z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

у вигляді

$$\mathbf{T}{=}c_{00}|0\rangle\langle 0| + c_{01}|0\rangle\langle 1| + c_{10}|1\rangle\langle 0| + c_{11}|1\rangle\langle 1|. \tag{4.3}$$

Довільні комплексні параметри у виразах (4.2) і (4.3) треба підбирати так, щоб виконувались відповідні умови (унітарності, ермітовості і т.д.) для цих операторів. Зв'язок між параметрами різних виразів (в даному випадку для унітарних операторів) можна отримати з порівняння їхніх явних матричних зображень.

Оператор зміни фази одного квабіта означують так:

$$\boldsymbol{\Phi}(\varphi)\,|x\rangle = e^{i\varphi x}\,|x\rangle, \qquad x = \{0,1\},$$

він має таке матричне зображення:

$$\boldsymbol{\Phi}(\varphi) = \mathbf{W}(\frac{\varphi}{2};\varphi,0,0) = e^{i\frac{\varphi}{2}}\begin{bmatrix} e^{-i\frac{\varphi}{2}} & 0 \\ 0 & e^{i\frac{\varphi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}.$$

Зокрема, $\boldsymbol{\Phi}(\pi) = \boldsymbol{\sigma}^z$.

Введімо оператор Адамара, що переводить базові стани в їх суперпозиції з рівними амплітудами:

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right),$$

чи загальніше:

$$\mathbf{H}|x\rangle{=}\frac{1}{\sqrt{2}}\left(|0\rangle{+}(-1)^x|1\rangle\right){=}\frac{1}{\sqrt{2}}\left(|0\rangle{+}\mathrm{e}^{i\pi x}|1\rangle\right){=}\frac{1}{\sqrt{2}}\sum_{y=0}^{1}\mathrm{e}^{i\pi xy}|y\rangle,$$

де $x, y = \{0, 1\}$. Легко побудувати його матричне зображення:

$$\mathbf{H}{=}\mathbf{W}\Big(\frac{\pi}{2}; 0, \frac{\pi}{2}, \pi\Big){=}\begin{bmatrix}\cos\frac{\pi}{4} & -\sin\frac{\pi}{4}\\ \sin\frac{\pi}{4} & \cos\frac{\pi}{4}\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}{=}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.$$

Розгляньмо тепер одночасну дію операторів Адамара на кожен квабіт квантового регістра, що перебуває в стані $|0\ldots0\rangle_n$

$$\mathbf{H}^{[n]}|0\ldots0\rangle_n = \frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + |1\rangle\right)\left(|0\rangle + |1\rangle\right)\ldots\left(|0\rangle + |1\rangle\right)$$
$$= \frac{1}{2^{\frac{n}{2}}}\sum_{x_{n-1}=0}^{1}\ldots\sum_{x_1=0}^{1}\sum_{x_0=0}^{1}|x_{n-1}\ldots x_1x_0\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{\mathbf{x}}|\mathbf{x}\rangle.$$

Дія n одноквабітових операторів Адамара на кожен із квабітів n–квабітового регістра перевела початковий стан $|0\ldots0\rangle_n$ у стан, що є суперпозицією 2^n станів обчислювального базису, кожен із яких визначає ціле число з області $0 \div 2^n{-}1$. Тобто, такий стан відображає одночасно всі числа з цієї області з однаковою амплітудою.

Цю властивість квантових регістрів називають квантовим паралелізмом, вона є найважливішою з тих, що визначають надефективність квантових процесорів.

Класичні комп'ютери такої властивості не мають, оскільки кожен їхній стан визначає тільки одне число.

Одночасна дія n операторів Адамара на всі квабіти регістра, який перебуває в стані, що визначає число $\mathbf{y}$, переводить його в стан, що задає "суперпозицію" чисел

$$\mathbf{H}^{[n]}|\mathbf{y}\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{x_{n-1},\ldots,x_0=0}^{1}(-1)^{\mathbf{x}\cdot\mathbf{y}}\,|\mathbf{x}\rangle,$$

$$\mathbf{y}\cdot\mathbf{x} \equiv (y_{n-1}x_{n-1} + y_{n-2}x_{n-2} + \ldots + y_1x_1 + y_0x_0) \mod 2. \quad (4.4)$$

На перший погляд це є перетворенням Фур'є, але ця відповідність виникає тільки, якщо $\mathbf{y} = 0$, оскільки при перетворенні Фур'є показник експоненти містить множення $\mathbf{xy} \bmod 2^n$, тоді як множення (4.4) швидше нагадує скалярний добуток за mod 2. Оператор $\mathbf{H}^{[n]}$ ще називають оператором Уолша-Адамара.

Зрозуміло, що квантовий регістр може перебувати і у станах, які є суперпозицією базисних станів із різними амплітудами:

$$|\psi\rangle = \sum_{x_0,\ldots,x_{n-1}} C_{x_0,\ldots,x_{n-1}} |x_{n-1}\ldots x_0\rangle,$$

що задовольняють умову нормування

$$\sum_{x_0,\ldots,x_{n-1}} |C_{x_0,\ldots,x_{n-1}}|^2 = 1.$$

Оператора Адамара й операторів зміни фаз досить, щоб збудувати довільний унітарний одноквабітовий оператор:

$$\mathbf{W}(\delta;\alpha,\theta,\beta)=\mathrm{e}^{i(\delta-\frac{\alpha+\beta-\theta}{2})}\mathbf{\Phi}\left(\alpha-\frac{\pi}{2}\right)\mathbf{H}\mathbf{\Phi}(-\theta)\mathbf{H}\mathbf{\Phi}\left(\beta+\frac{\pi}{2}\right). \qquad (4.5)$$

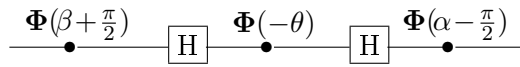
Сукупність усіх квантових логічних елементів, які реалізують дію деякого унітарного оператора, називають *квантовою схемою*. Для спрощення аналізу квантових схем використовують графічні зображення дій квантових вентилів на квабіти, в яких лінія зображає "світову лінію" квабіта, а дія КЛЕ на цей квабіт — відповідним знаком на ній. Наприклад, дію оператора Адамара $\mathbf{H}$ на квабіт $|x\rangle$ графічно зображають так:

$$\mathbf{H}|x\rangle \leftrightarrow |x\rangle \text{ —}\boxed{\text{H}}\text{— } \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle),$$

а дію оператора зміни фази:

$$\mathbf{\Phi}(\varphi)|x\rangle \quad \leftrightarrow \quad |x\rangle \overset{\mathbf{\Phi}(\varphi)}{\text{—}\bullet\text{—}} \mathrm{e}^{i\varphi x}|x\rangle.$$

Загальний оператор $\mathbf{W}((\alpha+\beta-\theta)/2;\alpha,\theta,\beta)$ (4.5) поворотів у $\mathbf{U}(2)$ зображають такою квантовою схемою:

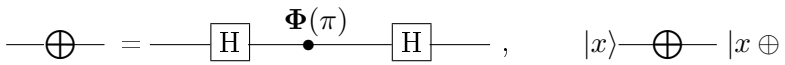


Варто звернути увагу, що знаки КЛЕ на "світових лініях" квабітів розташовані у зворотному порядку порівняно з відповідними операторами, оскільки тут час у схемах зростає зліва направо.

Із (4.1) випливає що, при $\delta = -\alpha = \beta = -\frac{\pi}{2}, \theta = -\pi$ оператор $\mathbf{W}$ стає оператором заперечення, тобто реалізує унарну операцію логічного заперечення **NOT** алгебри Буля:

$$\mathbf{W}(-\pi/2; \pi/2, -\pi, -\pi/2) = \mathbf{NOT} = \mathbf{X} \equiv \boldsymbol{\sigma}^x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\mathbf{X}|0\rangle = |1\rangle, \quad \mathbf{X}|1\rangle = |0\rangle,$$

а його квантова схема спрощується до:



$$|x\rangle \text{—}\oplus\text{—} \; |x \oplus 1\rangle,$$

де

$$\mathbf{\Phi}(\pi) = \mathbf{Z} = \boldsymbol{\sigma}^z.$$

Перед тим, як перейти до конструювання двоквабітових логічних елементів, з'ясуємо з врахуванням співвідношень:

$$\mathbf{R}_y(\theta_1)\mathbf{R}_y(\theta_2) = \mathbf{R}_y(\theta_1+\theta_2), \; \mathbf{R}_z(\alpha_1)\mathbf{R}_z(\alpha_2) = \mathbf{R}_z(\alpha_1+\alpha_2),$$
$$\mathbf{X}\mathbf{R}_y(\theta)\mathbf{X} = \mathbf{R}_y(-\theta), \; \mathbf{X}\mathbf{R}_z(\alpha)\mathbf{X} = \mathbf{R}_z(-\alpha),$$

що для операторів

$$\mathbf{A}{=}\mathbf{R}_z(\alpha)\,\mathbf{R}_y\!\left(\frac{\theta}{2}\right), \quad \mathbf{B}{=}\mathbf{R}_y\!\left(-\frac{\theta}{2}\right)\mathbf{R}_z\!\left(-\frac{\alpha+\beta}{2}\right), \quad \mathbf{C}{=}\mathbf{R}_z\!\left(\frac{\beta-\alpha}{2}\right)$$

справедливо

$$\mathbf{ABC}{=}\mathbf{R}_z(\alpha)\,\mathbf{R}_y\!\left(\frac{\theta}{2}\right)\mathbf{R}_y\!\left(-\frac{\theta}{2}\right)\mathbf{R}_z\!\left(-\frac{\alpha+\beta}{2}\right)\mathbf{R}_z\left(\frac{\beta-\alpha}{2}\right){=}\mathbf{I},$$

а також

$$\mathbf{AXBXC} = \mathbf{W}(0; \alpha, \theta, \beta). \tag{4.6}$$

Тобто, добуток (4.6) реалізує довільне перетворення в $\mathbf{SU}(2)$.

4.3 Двоквабітові вентилі

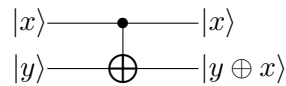
Двоквабітові КЛЕ описують унітарними операторами в просторі станів $\mathcal{H}^{[2]} = \mathcal{H} \otimes \mathcal{H}$, які не можна зобразити тензорним добутком одноквабітових операторів. Найважливішим тут є оператор **CNOT**, дія якого в обчислювальному базисі аналогічна відповідному класичному вентилю, тобто:

$$\mathbf{CNOT}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle,$$

зокрема

$$\mathbf{CNOT}|x\rangle|0\rangle = |x\rangle|x\rangle, \tag{4.7}$$

і може видатися, що порушується теорема про відсутність клонування, але ніякого клонування немає, бо (4.7) істинно тільки для відомих станів $x = 0$ або $x = 1$. Вентиль **CNOT** має таке графічне зображення:



(знак $\oplus$ означає додавання за модулем 2). У базисі $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ матриця оператора **CNOT** має вигляд:

$$\mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

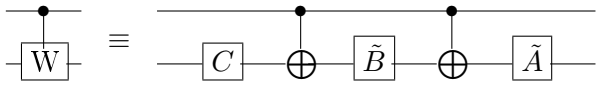
Цей оператор перекидає (заперечує) стан другого квабіта тільки тоді, коли перший квабіт перебуває в стані $|1\rangle$. Такі оператори називають контрольованими (перший квабіт контролює дію на другий квабіт), звідси і назва controlled-NOT. В двоквабітовому просторі станів загальна структура матриці контрольованих операторів є такою:

$$\mathbf{CW} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{W} \end{bmatrix}, \tag{4.8}$$

де $\mathbf{W} = \mathbf{W}(\delta; \alpha, \theta, \beta)$ — означений раніше оператор, а $\mathbf{I}$ і $\mathbf{0}$ одинична та нульова матриці другого порядку. За допомогою операторів **CNOT** та $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ (4.8) запишемо:

$$\mathbf{CW}(0; \alpha, \theta, \beta) = (\mathbf{I} \otimes \mathbf{A})\,\mathbf{CNOT}\,(\mathbf{I} \otimes \mathbf{B})\,\mathbf{CNOT}\,(\mathbf{I} \otimes \mathbf{C})\,,$$

зобразивши квантовою схемою:



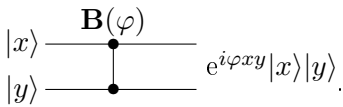
де із зрозумілих причин введено оператори із зворотним порядком дії:

$$\tilde{\mathbf{A}} = \mathbf{R}_y\left(\frac{\theta}{2}\right)\mathbf{R}_z\,(\alpha), \qquad \tilde{\mathbf{B}} = \mathbf{R}_z\left(-\frac{\alpha+\beta}{2}\right)\mathbf{R}_y\left(-\frac{\theta}{2}\right).$$

Матриця іншого КЛЕ – контрольованого зсуву фази – має таку саму загальну структуру:

$$\mathbf{B}(\varphi) = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi}(\varphi) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{i\varphi} \end{bmatrix},$$

із квантовою схемою:



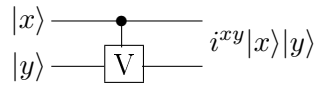
Введімо одноквабітовий оператор

$$\mathbf{V} \equiv \mathbf{\Phi}\left(\frac{\pi}{2}\right) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},$$

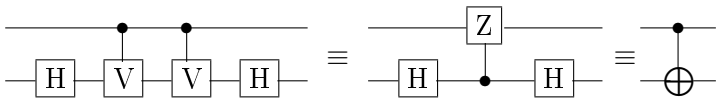
де i — уявна одиниця, та відповідний йому двоквабітовий контрольований оператор

$$\mathbf{CV} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} = \mathbf{B}\left(\frac{\pi}{2}\right),$$

що є частковим випадком оператора $\mathbf{B}(\varphi)$, який зобразимо графічно:



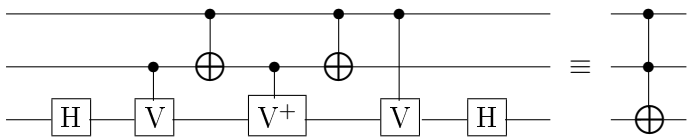
З цього оператора й оператора Адамара збудуємо квантову схему, яка реалізовує оператор **CNOT**:



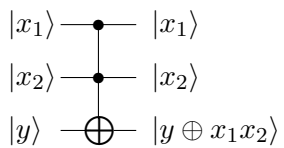
Два внутрішні вентилі в цій схемі можна замінити одним $\mathbf{B}(\pi)$. Різні варіанти утворення одних КЛЕ з інших є важливими, тому що побудувати певний квантовий вентиль за однією схемою в різних фізичних системах не завжди вдається.

4.4 Вентилі для трьох і більше квабітів

Аналогічно із цих двох операторів можна збудувати КЛЕ — квантовий відповідник вентиля Тоффолі з трьома входами і виходами:

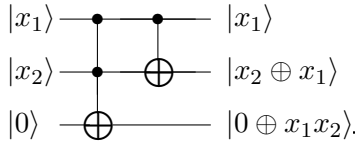


Останній КЛЕ виконує таку ж операцію, як у класичному випадку вентиль Тоффолі:

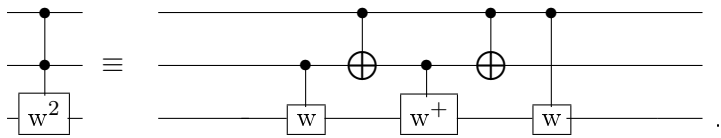


й разом із КЛЕ **CNOT** дає змогу збудувати суматор із перенесен-

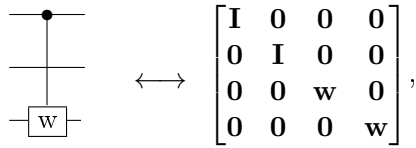
ням у вищий розряд:



Триквабітовий контрольований КЛЕ загального виду можна зобразити квантовою схемою:



Зауважимо, що матриця останнього у цій схемі КЛЕ має таку структуру:



де $\mathbf{I}$ і $\mathbf{0}$ — одинична і нульова матриці розміру 2×2, а $\mathbf{w}$ — матриця довільного оператора із $\mathbf{SU}(2)$.
Вентиль Тоффолі, який позначають $\mathbf{\Lambda}_2(\mathbf{X})$, має матрицю $2^3 \times 2^3$

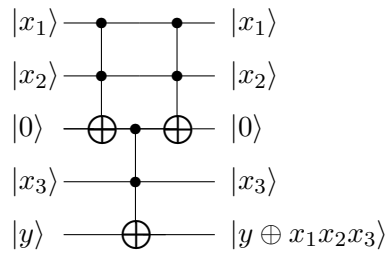
$$\mathbf{\Lambda}_2(\mathbf{X}) = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{X} \end{bmatrix},$$

а матриця $2^{n+1} \times 2^{n+1}$ оператора КЛЕ, який здійснює на $n+1$-ший квабіт дію $\mathbf{W}$, контрольовану всіма попередніми n квабітами, має на діагоналі всі одиниці, крім чотирьох елементів у правому нижньому кутку, де є матриця оператора $\mathbf{W}$, решта її елементів дорівнюють нулю. Такі КЛЕ позначають $\mathbf{\Lambda}_n(\mathbf{W})$. У цих позначен-

нях

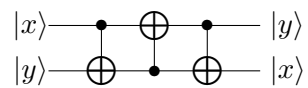
$$\mathbf{CNOT} = \mathbf{\Lambda}_1(\mathbf{X}) = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{X} \end{bmatrix} = \frac{1}{2}\left[(\mathbf{I} + \boldsymbol{\sigma}^z) \otimes \mathbf{I} + (\mathbf{I} - \boldsymbol{\sigma}^z) \otimes \boldsymbol{\sigma}^x\right].$$

Для прикладу зобразимо квантову схему для $\mathbf{\Lambda}_3(\mathbf{X})$, збудовану з трьох $\mathbf{\Lambda}_2(\mathbf{X})$ із використанням додаткового квабіта:



Симетрія відносно входу і виходу цієї схеми, як і всіх інших, пов'язана із вимогою зворотності (унітарності відповідних операторів).

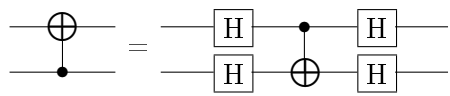
Часто вживаний для побудови квантових мереж квантовий вентиль **SWAP**, який виконує обмін вмістом двох квабітів, так пов'язаний із КЛЕ **CNOT**:



його матриця у спінорному базисі така:

$$\mathbf{SWAP} = \mathbf{CNOT} \cdot \mathbf{CNOT}' \cdot \mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

КЛЕ, що змінює стани першого квабіта під контролем другого, можна реалізувати такою квантовою схемою:



із матричним зображенням:

$$\mathbf{CNOT}' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \frac{1}{2}\left[\mathbf{I} \otimes (\mathbf{I} + \boldsymbol{\sigma}^z) + \boldsymbol{\sigma}^x \otimes (\mathbf{I} - \boldsymbol{\sigma}^z)\right].$$

Детальніше універсальні набори КЛЕ розглянуто у праці [11].

У спрощеному варіанті можна вважати, що:

Квантовий процесор — це квантовий регістр + скінченна схема квантових логічних елементів (КЛЕ), яка, діючи на квантовий регістр, змінює його стани.

Квантове обчислення — це введення квантового регістра в початковий стан + унітарна еволюція квантового регістра під керуванням квантової схеми за скінченний проміжок часу від початкового стану квантового регістра ("входу") до його кінцевого стану ("виходу") + зчитування кінцевого стану квантового регістра.

Для ефективного виконання квантових обчислень необхідно n-квабітовий регістр вводити в довільний початковий стан $|\mathbf{x}\rangle$ за скінченне число кроків $\sim$poly(n).

Зрозуміло, що при одному й тому ж початковому стані унітарна еволюція квантової мережі матиме той самий кінцевий стан (при збереженні квантової когерентності, тобто, за відсутності впливів оточення на роботу квантового процесора). Зчитати кінцевий стан можна тільки виконуючи вимірювання, тобто, проектування на обчислювальний базис. Оскільки між квабітами завжди є взаємодія (необхідна для виконання двоквабітових операцій), а отже — і квантова кореляція, то вектори станів окремих квабітів будуть між собою заплутаними, тому встановити результати обчислення можна лише із статистичного аналізу розподілу результатів вимірювань, отриманих під час багатократного повторення роботи квантового процесора. Достовірною вважають відповідь, знайдену з імовірністю $P{=}1{-}\varepsilon$, $\varepsilon{<}1/3$. Для ефективних обчислень кількість повторів не повинна зростати швидше, ніж $\sim$poly(n).

Проілюструємо це на прикладі проективного вимірювання кінцевого стану регістра. Результатом обчислення буде число, зображене сепарабельними станами квабітів $|\mathbf{k}\rangle{=}|x_{n-1}^{(k)}\rangle|x_{n-2}^{(k)}\rangle\cdots|x_0^{(k)}\rangle$,

однак, внаслідок заплутаності, регістр перебуватиме в стані $|\mathbf{s}\rangle = \sum_{j=0}^{2^n-1} c_j|\mathbf{j}\rangle$. Селективне вимірювання стану кожного квабіта в базисі $\{|0\rangle, |1\rangle\}$ переведе регістр у змішаний стан $\boldsymbol{\rho} = \sum_{j=0}^{2^n-1} |c_j|^2 |\mathbf{j}\rangle\langle\mathbf{j}|$. Повторні обчислення і вимірювання встановлять, що $|c_k| \gg |c_j|, j \neq k$, тобто, найбільш імовірним є стан $|\mathbf{k}\rangle$.

Насамкінець зауважимо, що унаслідок теоретичних досліджень отримано результат:

Клас функцій, обчислюваних квантовим процесором, збігається з класом функцій Тюринга (див., напр. [11]).

4.5 Основні вимоги до квантового процесора

Основні вимоги до фізичних систем реалізації універсального квантового процесора для обчислення функцій із класу Тюринга сформулював Дівінченцо (див., напр. [15]):

1. Реалізація квантових бітів як дворівневих систем, які можна індивідуально ідентифікувати і на які можна діяти квантовими вентилями (квантовими логічними елементами) для зміни квантового стану. Для реалізації повномасштабного квантового регістра з метою втілення всіх переваг, наданих їхньою квантовою природою, необхідні квантові регістри з кількістю квабітів $L > 10^3$.
2. Забезпечення приготування початкового (основного базового) стану регістра (ініціалізації).
3. Збереження квантової когерентності на протязі часу, достатньому для виконання понад 10^4 квантових вентилів. Похибка під час виконання окремої операції повинна бути меншою ніж 10^{-4} для забезпечення дії схем корекції помилок.
4. Існування нелінійної міжквабітової взаємодії для реалізації двоквабітових вентилів. Імпульси, що керують операціями, повинні контролюватися з точністю не меншою ніж 10^{-4}.
5. Здатність забезпечити надійне зчитування результату обчислень (вимірювання кінцевого стану).

Розділ 5

Квантові обчислення. Квантові алгоритми

В цьому розділі розглянуто базиси квантових вентилів і загальну структуру квантового обчислення. Описано основні із створених на даний час ефективних квантових алгоритмів.

5.1 Квантові обчислення

Наведене вище означення квантового обчислення потребує деякого уточнення. Виявляється, що побудувати повний набір КЛЕ для його виконання можна тільки використовуючи розширений квантовий регістр, який, окрім квабітів для запису аргументу, містить також додаткові, необхідні в процесі обчислення. З'ясуємо спосіб обчислення функції $\mathbf{x} \xrightarrow{f} \mathbf{y}$. Формують квантовий регістр довжини $N > n$ у стані $|x_{n-1} \dots x_0\rangle_n \otimes |0 \dots 0\rangle_{N-n}$, потім унітарними перетвореннями в просторі квантового регістра $\mathcal{H}^{[N]}$ його переводять у стан

$$\begin{aligned} |\mathbf{f}(\mathbf{x})\rangle_m \otimes |\mathbf{z}\rangle_{N-m} &= (\mathbf{U}\,|x_{n-1} \dots x_0\rangle_n) \otimes |0 \dots 0\rangle_{N-n} \\ &= \tilde{\mathbf{U}}\left(|x_{n-1} \dots x_0\rangle_n \otimes |0 \dots 0\rangle_{N-n}\right), \end{aligned}$$

і перші m квабітів вимірюють в базисі $\{|0\rangle, |1\rangle\}$. Після багатократного повторення, число, яке отримували з імовірністю $P > 1 - \varepsilon$, визнають за результат обчислення функції.

Зауважимо, що квабіти аргументу та квабіти результату обчислення мають бути мінімально заплутаними з іншими квабітами, інакше це призведе до ускладнення процесу вимірювання!

Для розширеного квантового регістра є два варіанти базису КЛЕ: точний нескінченний та наближений скінченний [14].

Перший складається з нескінченного набору одноквабітових КЛЕ, визначених всіма операторами $\mathbf{W}(\delta;\alpha,\theta,\beta)$ (з усіма можливими значеннями параметрів), та одного двоквабітового КЛЕ (наприклад, **CNOT**). Довільну унітарну $\mathbf{U}$ розміру $2^N\times 2^N$ матрицю в $\mathcal{H}^{[N]}$ можна утворити як добуток $2^N\left(2^N-1\right)/2$ матриць розміру $2^N\times 2^N$ виду (5.1) (див. [14]):

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ \vdots & \dots & \ddots & \dots & \dots & \dots & \dots & \dots & \dots & \vdots \\ 0 & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 & a & b & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 & c & d & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & 0 \\ \vdots & \dots & \dots & \dots & \dots & \dots & \dots & \ddots & \dots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{U}(2). \quad (5.1)$$

Для побудови будь-якого унітарного оператора в $\mathcal{H}^{[N]}$ у точному (нескінченному) базисі необхідна експонентна кількість $\sim 4^N$ базових КЛЕ. (В [11] наведено оцінку $\sim 4^N N^2$).

Перш ніж перейти до встановлення скінченних базисів, означимо унітарний оператор, близький до іншого. Для векторів простору станів введено норму:

$$\| \, |\psi\rangle \, \| \equiv \sqrt{\langle\psi|\psi\rangle}$$

із властивостями:

$$\| \, |\psi\rangle + |\varphi\rangle \, \| \le \| \, |\psi\rangle \, \| + \| \, |\varphi\rangle \, \|, \qquad \|c \, |\psi\rangle \, \| = |c| \| \, |\psi\rangle \, \|. \quad (5.2)$$

На підставі векторної норми введемо підпорядковану їй операторну норму:

$$\|\mathbf{A}\| = \sup \frac{\|\mathbf{A}|\psi\rangle\|}{\||\psi\rangle\|} \equiv \sup \frac{\sqrt{\langle\psi|\mathbf{A}^+\mathbf{A}|\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}},$$

яка окрім властивостей, що випливають із (5.2), має також додаткові властивості:

$$\|c\mathbf{A}\| = |c|\|\mathbf{A}\|, \quad \|\mathbf{A}+\mathbf{B}\| \le \|\mathbf{A}\| + \|\mathbf{B}\|, \quad \|\mathbf{AB}\| \le \|\mathbf{A}\|\|\mathbf{B}\|,$$
$$\|\mathbf{A}^+\| = \|\mathbf{A}\|, \quad \|\mathbf{A}\otimes\mathbf{B}\| = \|\mathbf{A}\|\|\mathbf{B}\|. \quad (5.3)$$

Якщо $\|\tilde{\mathbf{A}}-\mathbf{A}\|\le\delta$, то кажуть, що оператор $\tilde{\mathbf{A}}$ зображає оператор $\mathbf{A}$ з точністю δ. Якщо $\|\tilde{\mathbf{U}}_k-\mathbf{U}_k\|\le\delta_k$, то для добутку унітарних операторів похибка нагромаджується лінійно:

$$\|\tilde{\mathbf{U}}_L\cdots\tilde{\mathbf{U}}_1 - \mathbf{U}_L\cdots\mathbf{U}_1\| \le \sum_{k=1}^{L}\delta_k.$$

І справді, для унітарних попарно близьких операторів із врахуванням властивостей (5.3) маємо:

$$\|\tilde{\mathbf{U}}_2\tilde{\mathbf{U}}_1-\mathbf{U}_2\mathbf{U}_1\| = \|\tilde{\mathbf{U}}_2(\tilde{\mathbf{U}}_1-\mathbf{U}_1)+(\tilde{\mathbf{U}}_2-\mathbf{U}_2)\mathbf{U}_1\| \le \delta_1+\delta_2.$$

Нехай $\mathcal{H}^{[N]}$ — простір станів розширеного квантового регістра, а $\mathcal{H}^{[n]}$ — його підпростір, в якому записано аргумент. Тоді оператор $\mathbf{U}:\mathcal{H}^{[n]}\to\mathcal{H}^{[n]}$ наближується у просторі станів розширеного регістра оператором $\tilde{\mathbf{U}}:\mathcal{H}^{[N]}\to\mathcal{H}^{[N]}$ з точністю δ, якщо для довільного $|\psi\rangle\in\mathcal{H}^{[n]}$ виконується співвідношення:

$$\|\tilde{\mathbf{U}}(|\psi\rangle\otimes|0\ldots0\rangle_{N-n}) - \mathbf{U}|\psi\rangle\otimes|0\ldots0\rangle_{N-n}\| \le \delta\||\psi\rangle\|. \quad (5.4)$$

Ввівши ізометричний оператор розширення простору $\mathbf{Q}:\mathcal{H}^{[n]}\to\mathcal{H}^{[N]}$, що діє за правилом $\mathbf{Q}:|\psi\rangle\to|\psi\rangle\otimes|0\ldots0\rangle_{N-n}$, умову (5.4) запишемо формулою:

$$\|\tilde{\mathbf{U}}\mathbf{Q}-\mathbf{Q}\mathbf{U}\| \le \delta. \quad (5.5)$$

Якщо умову (5.5) задовольняють оператори $\tilde{\mathbf{U}}$ і $\mathbf{U}$, то її задовольняють і $\tilde{\mathbf{U}}^{-1}$ та $\mathbf{U}^{-1}$. Для доведення досить помножити вираз під знаком норми в (5.5) зліва на $\tilde{\mathbf{U}}^{-1}$ і справа на $\mathbf{U}^{-1}$, щоб отримати

$$\|\tilde{\mathbf{U}}^{-1}\mathbf{Q}-\mathbf{Q}\mathbf{U}^{-1}\| \le \delta.$$

Ці твердження про близькість операторів є справедливими і для інших означень норми оператора, важливо, щоби задовольнялись умови (5.3).

Як було зазначено раніше, довільний одноквабітовий вентиль можна утворити із оператора Адамара $\mathbf{H}$ і оператора зсуву фази $\mathbf{\Phi}(\varphi) = \exp(i\varphi/2)\mathbf{Z}(\varphi)$, де φ довільне дійсне число, яке з точністю до фази достатньо вибирати $0 \le \varphi < 2\pi$. Але фізично реалізувати такі КЛЕ з довільним значенням параметра φ практично неможливо, тому треба знайти спосіб їх побудови з достатньою точністю за допомогою дискретних базових КЛЕ.

Нехай ми уміємо повертати спін навколо осі z на кут $\pi/4$. У просторі станів цьому перетворенню відповідає оператор:

$$\mathbf{Z}(\pi/4) = \exp\left(-i\frac{\pi}{8}\boldsymbol{\sigma}^z\right) = \mathbf{I}\cos\frac{\pi}{8} - i\sin\frac{\pi}{8}\boldsymbol{\sigma}^z.$$

Використовуючи співвідношення

$$\mathbf{H}\boldsymbol{\sigma}^z\mathbf{H} = \boldsymbol{\sigma}^x, \quad \mathbf{H}\boldsymbol{\sigma}^x\mathbf{H} = \boldsymbol{\sigma}^z, \quad \mathbf{H}\boldsymbol{\sigma}^y\mathbf{H} = -\boldsymbol{\sigma}^y, \tag{5.6}$$

з'ясовуємо, що

$$\mathbf{H}\mathbf{Z}(\varphi)\mathbf{H} = \mathbf{X}(\varphi).$$

Запровадьмо оператор:

$$\begin{aligned}\mathfrak{R}(\vec{m},\varphi_0) &= \mathbf{Z}(\pi/4)\mathbf{X}(\pi/4) = \mathbf{Z}(\pi/4)\mathbf{H}\mathbf{Z}(\pi/4)\mathbf{H} \\ &= \mathbf{I}\cos^2\frac{\pi}{8} - i\sin\frac{\pi}{8}\left(\cos\frac{\pi}{8}\boldsymbol{\sigma}^x + \sin\frac{\pi}{8}\boldsymbol{\sigma}^y + \cos\frac{\pi}{8}\boldsymbol{\sigma}^z\right) \\ &= \boldsymbol{I}\cos\frac{\varphi_0}{2} - i\sin\frac{\varphi_0}{2}(\vec{m}\vec{\boldsymbol{\sigma}}) = \exp\left(-i\frac{\varphi_0}{2}(\vec{m}\vec{\boldsymbol{\sigma}})\right)\end{aligned}$$

де

$$\cos\frac{\varphi_0}{2} \equiv \cos^2\frac{\pi}{8}, \quad \vec{m} \equiv \left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)\frac{1}{\sqrt{1+\cos^2\frac{\pi}{8}}},$$

який зображає поворот спіну на кут φ_0 навколо вектора $\vec{m}$. Кут φ_0 є ірраціональним числом за модулем 2π, тому згідно принципу Даламбера [11] добутки $k\varphi_0 \mod 2\pi$, $k = 1, 2, \ldots$ рівномірно заповнюють проміжок $0 \div 2\pi$, а отже для деякого кута $0 \le \varphi < 2\pi$ знайдеться таке k, що $|\varphi - (k\varphi_0 \mod 2\pi)| \le \varepsilon$, тобто за скінченну кількість кроків можна з достатньою точністю наблизитись до довільного кута, що означає близькість таких операторів:

$$||\mathfrak{R}^k(\vec{m},\varphi_0) - \mathbf{R}(\vec{m},\varphi)|| \le \delta.$$

Використовуючи (5.6), утворимо новий оператор

$$\mathbf{H}\mathfrak{R}(\vec{m},\varphi_0)\mathbf{H}=\mathfrak{R}(\vec{m}',\varphi_0),$$

який виконує повороти на той самий кут, але навколо іншого вектора $\vec{m}'=(m_z,-m_y,m_x)$ не колінеарного до $\vec{m}$. За допомогою трьох поворотів навколо двох ортогональних векторів можна збудувати довільний одноквабітовий оператор, у випадку поворотів навколо неортогональних векторів таких поворотів може виявитися більше. Однак довільний одноквабітовий оператор можна з точністю δ наблизити скінченною кількістю поворотів, здійснюваних операторами $\mathfrak{R}(\vec{m},\varphi_0)$ і $\mathfrak{R}(\vec{m}',\varphi_0)$, причому кількість цих кроків оцінюється згідно теореми Соловея-Кітаєва $\sim\log^a(1/\delta)$, де стала $a\approx 2$ (див. [11]). Якщо для побудови деякої точної складної квантової схеми використано m точних елементів (одно- і двоквабітових), то для апроксимації її з точністю δ треба використати $\sim m\log^a(l/\delta)$ дискретних базових КЛЕ [11]. Як уже було зазначено, для побудови точної квантової схеми довільного точного унітарного оператора в просторі станів $\mathcal{H}^{[n]}$ n-квабітового регістра потрібно $\sim 4^n$ одно- і двоквабітових КЛЕ. Отже, квантову схему такого довільного унітарного оператора можна з точністю δ наблизити квантовою схемою з $\sim 4^n\log^a(4^n/\delta)$ дискретних базових КЛЕ. (У праці [11] наведено також оцінку $\sim 4^n n^2\log^a(4^n n^2/\delta)$).

Базис КЛЕ називається повним, якщо будь-який унітарний оператор можна з довільною точністю зобразити квантовою схемою в цьому базисі [14] у просторі станів розширеного регістра.

Доведено (див., зокрема, [11, 14]), що скінченні базиси $\mathcal{Q}=\{\mathbf{H},\mathbf{\Phi}(\pi/2),\mathbf{\Phi}(\pi/4),\mathbf{\Lambda}_1(\mathbf{X})\}$ і $\mathcal{Q}=\{\mathbf{H},\mathbf{V},\mathbf{\Lambda}_1(\mathbf{X}),\mathbf{\Lambda}_2(\mathbf{X})\}$, де

$$\mathbf{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ \mathbf{V}=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix},\ \mathbf{\Phi}(\varphi)=\begin{bmatrix}1 & 0\\ 0 & \exp(i\varphi)\end{bmatrix},$$

$$\mathbf{\Lambda}_1(\mathbf{X})\equiv\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

є повними.

Вперше повний базис $\mathcal{Q}=\{\mathbf{X},\mathbf{\Lambda}_2(\mathbf{R})\}$, де $\mathbf{R}=-i\exp(i\pi\alpha\mathbf{X})$ (α— ірраціональне), запропонував D.Deutsch (див., напр. [14]).

Оцінки складності алгоритмів, виконуваних унітарними операторами, які збудовані у цих базисах в $\mathcal{H}^{[n]}$, дають експонентні часи ($K \sim 4^n$), що свідчить про неефективність цих алгоритмів, але треба звернути увагу, що йдеться про **довільний** унітарний оператор. Це і зрозуміло, бо у загальному випадку квантові унітарні перетворенні можна реалізувати тільки експонентно складними алгоритмами. Квантові процесори можуть дати експонентне прискорення тільки для **деяких алгоритмів**, коли експонентно складні класичні алгоритми стають поліномними.

5.2 Квантові алгоритми

Для аналізу запропонованих квантових алгоритмів, зручно розділити квантовий регістр на два: регістр аргументу $|x\rangle_n$ і регістр значень функції $|y\rangle_m$, упускаючи для простоти додаткові квабіти. Тоді обчислення функції можна зобразити:

$$|x\rangle_n|y\rangle_m \stackrel{f(x)}{\to} |x\rangle_n|y \oplus f(x) \bmod 2^m\rangle_m$$

або

$$|\mathbf{x}\rangle|0\rangle \stackrel{f(\mathbf{x})}{\to} |\mathbf{x}\rangle|f(\mathbf{x})\rangle.$$

На сьогодні створено досить незначну кількість проектів квантових схем для ефективного (поліномного) обчислення тих чи інших обчислюваних функцій. Квантова надефективність може виявлятися не обов'язково у обчисленні самих функцій, а у дослідженні деяких їхніх властивостей. Тому, здебільшого, далі вважатимемо, що нам доступна квантова (під)схема, яка обчислює деяку функцію $f(\mathbf{x})$. Задача полягає у тому, щоби добудувати до неї нову квантову схему, яка б дала змогу ефективно (в поліномний час чи з поліномним числом КЛЕ) провести дослідження властивостей функції $f(\mathbf{x})$, яке на класичному комп'ютері обходиться експонентними затратами.

Розглянемо тепер декілька прикладів відомих сьогодні квантових алгоритмів, які ілюструють надефективність квантових процесорів.

Перетворення Фур'є широко використовують у багатьох фундаментальних і прикладних дослідженнях. Хоча квантове перетворення Фур'є не можна застосовувати безпосередньо через проблеми створення стану регістра, до якого його застосовують, а також проблеми прочитання результатів, воно необхідне як проміжна операція в інших обчисленнях [11].

5.3 Квантове перетворення Фур'є

Дискретне перетворення Фур'є функції $f(\mathbf{x})$, де $\mathbf{x}$ — ціле число з проміжку $\mathbf{x} \in \mathbb{Z}_n = \{0 \div 2^n - 1\}$, можна записати у вигляді:

$$\tilde{f}(\mathbf{x}) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{Z}_n} \mathrm{e}^{i2\pi \mathbf{x}\mathbf{y}/2^n} f(\mathbf{y}).$$

Для його виконання потрібно не менше ніж $K{=}2^{2n}$ операцій (для 2^n значень фур'є-образу $\tilde{f}(\mathbf{x})$ треба обчислити 2^n значень виразу під знаком суми). Скориставшись властивостями експоненти, в цьому виразі доданки під знаком суми можна перегрупувати і цим кількість операцій скоротити до $K{\approx}2^n n$. Хоча ці алгоритми є експонентно складними, вони мають широке застосування, оскільки практичні труднощі виникають тільки для дуже великих n.

Квантовий алгоритм перетворення Фур'є D.Coppersmith запропонував у 1994 році. Розгляньмо спочатку перетворення Фур'є чотириквабітового числа, записаного в квантовому регістрі (точніше, перетворення стану квантового регістра, в якому записано деяке число, в стан суперпозиції з амплітудами, визначеними експонентними множниками перетворення Фур'є).

Згадаймо, що число $\mathbf{x}$ у двійковому зображенні за модулем 2^n має вигляд

$$\mathbf{x} = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \ldots + x_1 2^1 + x_0 2^0 = \sum_{j=0}^{n-1} x_j 2^j,$$

($x_j = \{0, 1\}$) тоді добуток двох чисел (за модулем 2^n) можна за-

писати

$$\mathbf{xy} = \sum_{j=0}^{n-1} x_j 2^j y_0 + 2\sum_{j=0}^{n-2} x_j 2^j y_1 + 2^2 \sum_{j=0}^{n-3} x_j 2^j y_2 + \dots$$
$$+2^{n-3}\big(x_2 2^2 + x_1 2 + x_0\big) y_{n-3} + 2^{n-2}(x_1 2 + x_0) y_{n-2} + 2^{n-1} x_0 y_{n-1}.$$

Поділимо отримане число на 2^n (за модулем 2^n)

$$\begin{aligned}\frac{\mathbf{xy}}{2^n} &= \left(\frac{x_{n-1}}{2} + \frac{x_{n-2}}{2^2} + \dots + \frac{x_2}{2^{n-2}} + \frac{x_1}{2^{n-1}} + \frac{x_0}{2^n}\right) y_0 \\ &+ \left(\frac{x_{n-2}}{2} + \frac{x_{n-3}}{2^2} + \dots + \frac{x_2}{2^{n-3}} + \frac{x_1}{2^{n-2}} + \frac{x_0}{2^{n-1}}\right) y_1 \\ &+ \left(\frac{x_{n-3}}{2} + \frac{x_{n-4}}{2^2} + \dots + \frac{x_2}{2^{n-4}} + \frac{x_1}{2^{n-3}} + \frac{x_0}{2^{n-2}}\right) y_2 + \dots \\ &+ \left(\frac{x_2}{2} + \frac{x_1}{2^2} + \frac{x_0}{2^3}\right) y_{n-3} + \left(\frac{x_1}{2} + \frac{x_0}{2^2}\right) y_{n-2} + \frac{x_0}{2} y_{n-1}.\end{aligned}$$

На рисунку 5.1 зображено квантову схему перетворення Фур'є чотирирозрядного двійкового числа, далі стане зрозумілим, як розбудувати цю схему для n-розрядного числа.

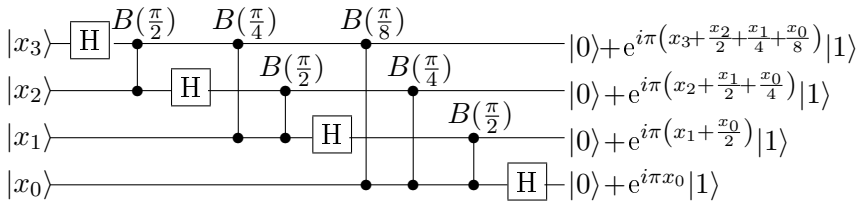


Рис. 5.1: Схема перетворення Фур'є стану чотириквабітового регістра

Перш ніж ознайомитися з дією квантової схеми для виконання квантового перетворення Фур'є, пригадаймо, як діють її окремі елементи: оператор Адамара діє на окремий квабіт:

$$\mathbf{H}|x_j\rangle = |0\rangle + e^{i\pi x_j}|1\rangle,$$

а оператор зміни фази в цій схемі — на два квабіти:

$$\mathbf{B}(\varphi)|x_k\rangle|x_j\rangle = e^{i\varphi x_k x_j}|x_k\rangle|x_j\rangle.$$

(Поки що множники $1/\sqrt{2}$ будемо упускати.) Позначивши індексами біля значків операторів КЛЕ номери квабітів, на які вони діють, еволюцію квантової схеми запишемо так:

$$
\begin{aligned}
|\mathbf{x}\rangle\equiv|x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{H}_3} \left(|0\rangle+\mathrm{e}^{i\pi x_3}|1\rangle\right)|x_2\rangle|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{B}_{32}(\frac{\pi}{2})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}\right)}|1\rangle\right)|x_2\rangle|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{H}_2} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi x_2}|1\rangle\right)|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{B}_{31}(\frac{\pi}{4})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi x_2}|1\rangle\right)|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{B}_{21}(\frac{\pi}{2})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}\right)}|1\rangle\right)|x_1\rangle|x_0\rangle \xrightarrow{\mathbf{H}_1} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}\right)}|1\rangle\right) \\
\left(|0\rangle+\mathrm{e}^{i\pi x_1}|1\rangle\right)|x_0\rangle \xrightarrow{\mathbf{B}_{30}(\frac{\pi}{8})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}\right)}|1\rangle\right) \\
\left(|0\rangle+\mathrm{e}^{i\pi x_1}|1\rangle\right)|x_0\rangle \xrightarrow{\mathbf{B}_{20}(\frac{\pi}{4})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}+\frac{x_0}{4}\right)}|1\rangle\right) \qquad (5.7) \\
\left(|0\rangle+\mathrm{e}^{i\pi x_1}|1\rangle\right)|x_0\rangle \xrightarrow{\mathbf{B}_{10}(\frac{\pi}{2})} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}+\frac{x_0}{4}\right)}|1\rangle\right) \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_1+\frac{x_0}{2}\right)}|1\rangle\right)|x_0\rangle \xrightarrow{\mathbf{H}_0} \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}+\frac{x_0}{4}\right)}|1\rangle\right) \\
\left(|0\rangle+\mathrm{e}^{i\pi\left(x_1+\frac{x_0}{2}\right)}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{i\pi x_0}|1\rangle\right) \\
=\sum_{y_0}\mathrm{e}^{i\pi\left(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)y_0}|y_0\rangle\sum_{y_1}\mathrm{e}^{i\pi\left(x_2+\frac{x_1}{2}+\frac{x_0}{4}\right)y_1}|y_1\rangle \\
\sum_{y_2}\mathrm{e}^{i\pi\left(x_1+\frac{x_0}{2}\right)y_2}|y_2\rangle\sum_{y_3}\mathrm{e}^{i\pi x_0y_3}|y_3\rangle \\
=\sum_{\mathbf{y}}\mathrm{e}^{i2\pi\frac{\mathbf{xy}}{2^4}}|\mathbf{y}\rangle.
\end{aligned}
$$

Зауважимо, що порядок позицій розрядів числа-результату є зворотним порівняно з числом-аргументом.

Загалом квантове перетворення Фур'є

$$|\mathbf{x}\rangle \stackrel{\mathbf{QFT}}{\longrightarrow} \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}} \mathrm{e}^{i2\pi \frac{\mathbf{xy}}{2^n}} |\mathbf{y}\rangle \tag{5.8}$$

переводить n-квабітовий квантовий регістр у стан, що є суперпозицією з амплітудами, які дорівнюють коефіцієнтам перетворення Фур'є. З рис. 5.1 та із перетворень (5.7) легко зрозуміти, як розширити схему для квантового перетворення Фур'є n-розрядного числа і встановити, що така схема буде мати $n(n+1)/2$ КЛЕ.

Допустимо, що ми перевели квантовий регістр у суперпозиційний стан із амплітудами, які є значеннями деякої функції $f(\mathbf{x})$, а потім виконали квантове перетворення Фур'є регістра аргументу:

$$\sum_{\mathbf{x}} f(\mathbf{x})|\mathbf{x}\rangle \stackrel{\mathbf{QFT}}{\longrightarrow} \sum_{\mathbf{x}} f(\mathbf{x}) \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}} \exp(i2\pi \frac{\mathbf{xy}}{2^n})|\mathbf{y}\rangle = \sum_{\mathbf{y}} \tilde{f}(\mathbf{y})|\mathbf{y}\rangle,$$

тоді нові амплітуди станів будуть фур'є-образами функції $f(\mathbf{x})$

$$\tilde{f}(\mathbf{y}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}} f(\mathbf{x}) \exp\left(i2\pi \frac{\mathbf{xy}}{2^n}\right).$$

Звичайно, зчитування цих амплітуд є проблемою, але у випадках, коли перетворення Фур'є є проміжною операцією в обчисленнях, переваги квантового алгоритму є безперечними. Квантовий процесор виконує перетворення Фур'є функції за $K = n(n+1)/2$ кроків, тобто, з поліномними затратами часу, тоді як алгоритми для класичного регістра є експонентно складними.

Виконаємо в (5.8) обернене квантове перетворення Фур'є (та сама схема, але з від'ємними кутами в $\mathbf{B}(\varphi)$)

$$|\mathbf{y}\rangle \stackrel{\mathbf{QFT}^{-1}}{\longrightarrow} \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{z}} \mathrm{e}^{-i2\pi \frac{\mathbf{yz}}{2^n}} |\mathbf{z}\rangle.$$

Тоді (5.8) можна записати як:

$$|\mathbf{x}\rangle \xrightarrow{\mathbf{QFT}} \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}} \mathrm{e}^{i2\pi \frac{\mathbf{xy}}{2^n}} |\mathbf{y}\rangle \xrightarrow{\mathbf{QFT}^{-1}} \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}} \mathrm{e}^{i2\pi \frac{\mathbf{xy}}{2^n}} \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{z}} \mathrm{e}^{-i2\pi \frac{\mathbf{yz}}{2^n}} |\mathbf{z}\rangle$$
$$= \sum_{\mathbf{z}} \frac{1}{2^n} \sum_{\mathbf{y}} \mathrm{e}^{i2\pi \frac{(\mathbf{x}-\mathbf{z})\mathbf{y}}{2^n}} |\mathbf{z}\rangle = \sum_{\mathbf{z}} \delta_{\mathbf{x},\mathbf{z}} |\mathbf{z}\rangle = |\tilde{\mathbf{x}}\rangle.$$

Останні дві рівності умовні, вони означають, що вимірювання квантового регістра у тому стані, у якому він опинився після прямого і оберненого квантового перетворення Фур'є, з великою ймовірністю дасть значення числа $\mathbf{x}$, яке в ньому було початково записано.

5.4 Задача Дойча-Йожи

Задача Дойча — історично перша, яка засвідчила, що деякі експонентно складні для класичних комп'ютерів задачі, на квантових процесорах можна розв'язати з поліномними затратами. Задача полягає у визначенні до якого класу належить функція — вона стала чи збалансована. В першому варіанті Дойч сформульовав її для бінарного аргументу. Коли

$$f(0) = f(1) = 0 \quad \text{або} \quad f(0) = f(1) = 1$$

функцію називають сталою, а коли

$$f(0) = 0, f(1) = 1 \quad \text{або} \quad f(0) = 1, f(1) = 0$$

то — збалансованою. Пізніше Дойч і Йожа (R.Jozsa) узагальнили цю задачу на довільний аргумент $\mathbf{x}$ з області $\mathbb{Z}_n$, при тому, що сама функція приймає два значення $\{0, 1\}$. В цьому випадку функція називають сталою, якщо для всіх значень аргументу вона набуває значення 0 або 1, і — збалансованою, якщо для однієї половини значень аргументу вона набуває значення 0, а для іншої половини — значення 1. Щоб з'ясувати, до якого класу належить така функція, за допомогою класичного процесора треба виконати 2^n обчислень її значень. За допомогою квантового процесора цю

перевірку можна виконати тільки один раз обчисливши функції $f(\mathbf{x})$. Для цього будують регістр аргументу з n квабітів і регістр значень функції з одного квабіта, з початковим станом:

$$|0\ldots0\rangle_n|1\rangle,$$

далі на кожен квабіт діють оператором Адамара, що призводить до такої суперпозиції:

$$\sum_{\mathbf{x}}|\mathbf{x}\rangle(|0\rangle-|1\rangle).$$

Потім обчислюють функцію $f(\mathbf{x})$:

$$\sum_{\mathbf{x}}|\mathbf{x}\rangle(|f(\mathbf{x})\rangle-|1\oplus f(\mathbf{x})\rangle)=\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})}|\mathbf{x}\rangle(|0\rangle-|1\rangle),$$

і знову на кожен квабіт аргументу діють оператором Адамара:

$$\mathbf{H}^{[n]}|\mathbf{y}\rangle=\frac{1}{2^{\frac{n}{2}}}\sum_{x_{n-1},\ldots,x_0=0}^{1}(-1)^{\mathbf{x}\cdot\mathbf{y}}\,|\mathbf{x}\rangle,$$

$$\mathbf{y}\cdot\mathbf{x}\equiv(y_{n-1}x_{n-1}+y_{n-2}x_{n-2}+\ldots+y_1x_1+y_0x_0)\bmod 2,$$

що призводить до результату

$$\sum_{\mathbf{x},\,\mathbf{y}}(-1)^{f(\mathbf{x})+\mathbf{x}\cdot\mathbf{y}}|\mathbf{y}\rangle(|0\rangle-|1\rangle).$$

Нарешті вимірюють значення числа $\mathbf{y}$, записаного в регістрі аргументу. Якщо $\mathbf{y}$=0, то $f(\mathbf{x})$ є сталою, оскільки інакше амплітуда стану $|0\ldots0\rangle$ дорівнювала б нулю, бо для половини значень аргументу $f(\mathbf{x})=0$, а для половини значень аргументу $f(\mathbf{x})=1$,

$$\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})}=0,$$

якщо ж $\mathbf{y}\neq 0$, то $f(\mathbf{x})$ є збалансованою, інакше амплітуда стану $|\mathbf{y}\rangle$ дорівнювала б нулю

$$\sum_{\mathbf{x}}(-1)^{\mathbf{x}\cdot\mathbf{y}}=0.$$

Для функції $f(\mathbf{x})$=$\mathbf{a}\cdot\mathbf{x}$, вимірювання дає $\mathbf{y}$=$\mathbf{a}$.

В цьому обчисленні ми два рази використали оператор $\mathbf{H}^{[n]}$ ($2n$ одноквабітових операцій) і один раз обчислили функцію $f(\mathbf{x})$ проти 2^n її обчислень, необхідних у класичному випадку.

5.5 Визначення періоду функції

Нехай задана функція $f\colon \mathbb{Z}_n \xrightarrow{f} \mathbb{Z}_n$, про яку відомо, що вона має період $\mathbf{r}$, $f(\mathbf{x}+\mathbf{r}) = f(\mathbf{x})$, такий, що $2^{n-1} < \mathbf{r} < 2^n - 1$ і треба знайти його значення. Побудуємо два регістри з n квабітів кожен, подіємо на кожен квабіт регістра аргументу оператором Адамара, після чого обчислимо функцію f:

$$|0\ldots0\rangle_n|0\ldots0\rangle_n \xrightarrow{\mathbf{H}^{[n]}} \sum_{\mathbf{x}} |\mathbf{x}\rangle|0\ldots0\rangle_n \xrightarrow{f} \sum_{\mathbf{x}} |\mathbf{x}\rangle|f(\mathbf{x})\rangle, \qquad (5.9)$$

далі виміряємо число, записане в регістрі значень функції, що дасть деяке $f(\mathbf{k})$, а обидва регістри перейдуть у стан

$$(|\mathbf{k}\rangle + |\mathbf{k}+\mathbf{r}\rangle)|f(\mathbf{k})\rangle.$$

Такий результат ми отримали тому, що після обчислення функції в (5.9) регістри аргументу і значення функції перебували в заплутаному (скорельованому) стані і вимірювання регістра значень функції зафіксувало стан регістра аргументу у вигляді суперпозиції станів, що відповідають двом значенням аргументу, для яких функція має те саме значення $f(\mathbf{k})$. Вимірювання розплутало стани регістрів аргументу і значень функції!

Застосуймо $\mathbf{H}^{[n]}$ до регістра аргументу

$$\begin{aligned}&\sum_{\mathbf{y}} \left[(-1)^{\mathbf{k}\cdot\mathbf{y}} + (-1)^{(\mathbf{k}+\mathbf{r})\cdot\mathbf{y}}\right] |\mathbf{y}\rangle \otimes |f(\mathbf{k})\rangle \\ &= \sum_{\mathbf{y}} (-1)^{\mathbf{k}\cdot\mathbf{y}} \left[1 + (-1)^{\mathbf{r}\cdot\mathbf{y}}\right] |\mathbf{y}\rangle \otimes |f(\mathbf{k})\rangle.\end{aligned}$$

Вимірювання числа $\mathbf{y}$, записаного в регістрі аргументу, дасть

$$\mathbf{y}\cdot\mathbf{r} = 0.$$

Повторивши вимірювання m разів, отримаємо систему m лінійних рівнянь для $\mathbf{r}$, яку розв'яжемо на класичному комп'ютері за допомогою алгоритмів поліномної складності.

Тут ми m разів двічі виконували $\mathbf{H}^{[n]}$ і одне вимірювання, всього $2nm$ одноквабітових операцій, m обчислень функції і m вимірювань, а також розв'язування m лінійних рівнянь. У класичному випадку нам довелося б 2^n разів обчислювати функцію.

5.6 Алгоритм Шора факторизації чисел

Алгоритм Шора для факторизації чисел за допомогою квантового процесора привернув велику увагу до проекту створення квантового комп'ютера. Це пов'язано з тим, що він дає змогу ефективно зламати широковживаний шифр RSA (див. Додаток).

Нехай $N{=}PQ$ — складене число ($N \leq 2^n$), P і Q — невідомі прості числа. Ці дільники є серед найбільших спільних дільників чисел N і $(a^{r/2} \mod N){\pm}1$, де r — період послідовності $a^j \mod N$, $j = 0, 1, 2, \ldots$. Величину r називають порядком числа a за модулем N ($a^r \mod N = 1$). Складність цього алгоритму в тому, що треба щонайменше r разів обчислити функцію a^j.

Збудуємо два регістри: регістр значень функції довжини n ($N \leq 2^n$) і регістр аргументу довжини m ($M = 2^m$), такої що $m \gg n$. Занулимо обидва регістри, потім перетвореннями Адамара переведемо регістр аргументу в суперпозиційний стан, після чого виберемо число $a < N$ взаємно просте з N і обчислимо функцію: $a^{\mathbf{x}} \bmod N$

$$|0\ldots0\rangle_m|0\ldots0\rangle_n \xrightarrow{\mathbf{H}^{[m]}} \sum_{\mathbf{x}} |\mathbf{x}\rangle|0\rangle_n \xrightarrow{a^{\mathbf{x}} \bmod N} \sum_{\mathbf{x}} |\mathbf{x}\rangle|a^{\mathbf{x}} \bmod N\rangle.$$

Виміряємо значення функції:

$$(|\mathbf{k}\rangle + |\mathbf{k}+\mathbf{r}\rangle + \cdots + |\mathbf{k}+l\mathbf{r}\rangle)|a^{\mathbf{k}}\rangle = \sum_{j=0}^{l} |\mathbf{k}+j\mathbf{r}\rangle|a^{\mathbf{k}}\rangle$$

і виконаємо перетворення Фур'є регістра аргументу

$$\sum_{\mathbf{y}}\sum_{j=0}^{l}\exp\left[\frac{2\pi i(j\mathbf{r}+\mathbf{k})\mathbf{y}}{M}\right]|\mathbf{y}\rangle|a^{\mathbf{k}}\rangle$$
$$=\sum_{\mathbf{y}}\frac{\exp\left[2\pi i\mathbf{r}\mathbf{y}l/M\right]-1}{\exp\left[2\pi i\mathbf{r}\mathbf{y}/M\right]-1}\exp\left[2\pi i\mathbf{k}\mathbf{y}/M\right]|\mathbf{y}\rangle|a^{\mathbf{k}}\rangle.$$

Виміряємо $\mathbf{y}$, при цьому найбільш імовірним є результат, для якого виконується співвідношення $\mathbf{r}\mathbf{y}/M=b$, де b деяке ціле число. Оскільки $\mathbf{y}$ і M нам відомі, то побудуємо відношення $\mathbf{y}/M$ і замінимо його дробом $\frac{\mathbf{y}}{M}\approx\frac{D}{d}$, де $d<N$. Перевіримо, чи $a^d \bmod N=1$, якщо ні — то повторюємо алгоритм, якщо ж так — то запишемо $r_1=d$. Після багатократного повторення отримаємо набір $r_1,r_2,\ldots$, мінімальне число з цього набору і буде шуканим періодом r (порядком числа a за модулем N). Тоді обчислимо $(a^{r/2} \bmod N)\pm 1$. Застосування алгоритму Евкліда дасть значення співмножників числа N.

Доведено [14], що квантовий алгоритм Шора факторизації числа N має поліноміальну складність $n^3(\log n)^k$, k=const, тоді як відомий класичний алгоритм є експонентно складним з часом виконання $t\sim\exp\left(\sqrt{\ln N\ln\ln N}\right)$ [21].

5.7 Алгоритм пошуку Гровера

Нехай задана функція $\mathbb{Z}_n\xrightarrow{F}\mathbb{Z}_m$ така, що $F(\boldsymbol{\omega})=\boldsymbol{a}$. Для заданого $\boldsymbol{a}$ треба знайти $\boldsymbol{\omega}$. Здебільшого говорять, що треба знайти стан $\boldsymbol{\omega}$, позначений символом $\boldsymbol{a}$, тобто інтерпретують задачу як пошук у неструктурованій (невпорядкованій) базі даних.

Побудований на квантовому регістрі "оракул" на запитання: чи $\mathbf{x}=\boldsymbol{\omega}$? обчислює функцію $F(\mathbf{x})$ і відповідає 1, якщо $F(\mathbf{x})=\mathbf{a}$, і 0, якщо $F(\mathbf{x})\neq\mathbf{a}$, тобто, обчислює функцію $f_{\boldsymbol{\omega}}(\mathbf{x})=\delta_{\boldsymbol{\omega},\mathbf{x}}$. Алгоритм пошуку Гровера діє так:

1) перевести квантовий регістр у початковий стан:

$$|0\ldots0\rangle_n|1\rangle,$$

2) подіяти оператором Уолша-Адамара $\mathbf{H}^{[n+1]}$, що дасть:

$$\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right),$$

3) обчислити функцію $f_{\boldsymbol{\omega}}(\mathbf{x})$ (звернутися до "оракула")

$$\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle\frac{1}{\sqrt{2}}\left(|f_{\boldsymbol{\omega}}(\mathbf{x})\rangle-|1\oplus f_{\boldsymbol{\omega}}(\mathbf{x})\rangle\right)=$$
$$\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}(-1)^{f_{\boldsymbol{\omega}}(\mathbf{x})}|\mathbf{x}\rangle\otimes\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right), \tag{5.10}$$

та, ігноруючи квабіт значень функції, записати:

$$\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}(-1)^{f_{\boldsymbol{\omega}}(\mathbf{x})}|\mathbf{x}\rangle=\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle-\frac{2}{\sqrt{N}}|\boldsymbol{\omega}\rangle, \tag{5.11}$$

що еквівалентно дії оператора

$$\mathbf{U}_{\boldsymbol{\omega}}=\mathbf{I}-2|\boldsymbol{\omega}\rangle\langle\boldsymbol{\omega}|$$

на стан

$$|\mathbf{s}\rangle\equiv\frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle.$$

У цих виразах $\mathbf{I}$ — одиничний оператор у просторі станів аргументу $\mathcal{H}^{[n]}$, $N=2^n$.

Перетворення (5.10) і (5.11) треба розуміти так, що відповідь "оракула" змінює фазу на π тільки в шуканому стані (хоча він і залишається невідомим). На інші стани оператор $\mathbf{U}_{\boldsymbol{\omega}}$ діє як оператор дзеркального відбиття відносно стану $|\boldsymbol{\omega}^{\perp}\rangle$.

Оскільки стан $|\boldsymbol{\omega}\rangle$ є одним із станів суперпозиції $|\mathbf{s}\rangle$, то косинус кута між цими векторами:

$$\sin\theta=\sin(\pi/2-\beta)=\cos\beta=\langle\mathbf{s}|\boldsymbol{\omega}\rangle=\frac{1}{\sqrt{N}}$$

дуже мала величина, отже вектори $|\boldsymbol{\omega}\rangle$ і $|\mathbf{s}\rangle$ є майже перпендикулярними. Ідея Гровера полягає в тому, щоби повернути стан регістра аргументу $|\mathbf{s}\rangle$ так, аби він став майже паралельним до $|\boldsymbol{\omega}\rangle$.

Тоді вимірювання стану аргументу і дасть шукане значення виділеного (поміченого) числа $\boldsymbol{\omega}$ з ймовірністю, близькою до одиниці. Гровер запропонував процедуру такого повороту, яка складається з деякої кількості кроків, у кожному з яких відбувається поворот на кут 2θ, який виконує оператор:

$$\mathbf{R}_G = \mathbf{U}_\mathbf{s}\mathbf{U}_{\boldsymbol{\omega}},$$

де введено оператор дзеркального відображення відносно вектора $|\mathbf{s}\rangle$ (його іще називають оператором дифузії):

$$\mathbf{U}_\mathbf{s} = 2|\mathbf{s}\rangle\langle\mathbf{s}| - \mathbf{I}.$$

Прямою дією оператора $\mathbf{R}_G$ на стан $|\mathbf{s}\rangle$ із врахуванням:

$$\langle\mathbf{s}|\mathbf{s}\rangle = 1, \qquad \langle\boldsymbol{\omega}|\boldsymbol{\omega}\rangle = 1, \qquad \langle\mathbf{s}|\boldsymbol{\omega}\rangle = \frac{1}{\sqrt{N}}$$
$$|\mathbf{s}\rangle\langle\mathbf{s}|\,|\boldsymbol{\omega}\rangle = \frac{1}{\sqrt{N}}|\mathbf{s}\rangle, \quad |\boldsymbol{\omega}\rangle\langle\boldsymbol{\omega}|\,|\mathbf{s}\rangle = \frac{1}{\sqrt{N}}|\boldsymbol{\omega}\rangle$$

можна встановити, що:

$$|\mathbf{s}_1\rangle = \mathbf{R}_G|\mathbf{s}\rangle = \left(1 - \frac{4}{N}\right)|\mathbf{s}\rangle + \frac{2}{\sqrt{N}}|\boldsymbol{\omega}\rangle,$$
$$|\mathbf{s}_2\rangle = \mathbf{R}_G|\mathbf{s}_1\rangle = \mathbf{R}_G^2|\mathbf{s}\rangle = \left(1 - \frac{12}{N} + \frac{16}{N^2}\right)|\mathbf{s}\rangle + \frac{4}{\sqrt{N}}\left(1 - \frac{2}{N}\right)|\boldsymbol{\omega}\rangle.$$

Звідси

$$\sin\theta_1 = \cos\beta_1 = \langle\boldsymbol{\omega}|\mathbf{s}_1\rangle = \frac{3}{\sqrt{N}} - \frac{4}{N\sqrt{N}} = \sin 3\theta,$$
$$\sin\theta_2 = \cos\beta_2 = \langle\boldsymbol{\omega}|\mathbf{s}_2\rangle = \frac{5}{\sqrt{N}} - \frac{20}{N\sqrt{N}} + \frac{16}{N^2\sqrt{N}} = \sin 5\theta.$$

Після k кроків отримаємо:

$$\sin\theta_k = \langle\boldsymbol{\omega}|\mathbf{s}_k\rangle = \langle\boldsymbol{\omega}|\mathbf{R}_G^k|\mathbf{s}\rangle = \sin(2k+1)\theta.$$

Поклавши $\sin\theta_k \approx 1$, знайдемо:

$$(2k+1)\theta \approx \frac{\pi}{2}.$$

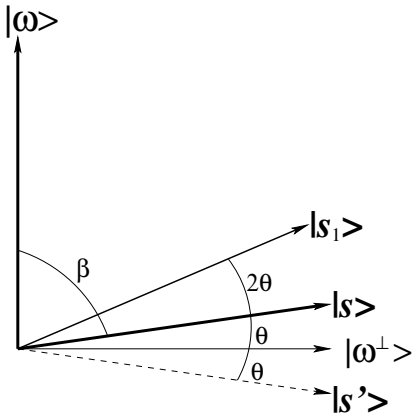


Рис. 5.2: Повороти Гровера

Тобто, після $k \approx \frac{\pi}{4}\sqrt{N}$ кроків квантовий регістр перейде у стан, що з ймовірністю близькою до 1 буде відповідати шуканому числу $\boldsymbol{\omega}$, яке ми знайдемо, вимірявши стан квантового регістра. Нагадаємо, що $N = 2^n$, де n — довжина вхідного слова. Отже квантовий алгоритм Гровера дає змогу за $\sim \sqrt{N}$ кроків знайти позначений елемент у невпорядкованій базі даних, а відповідний класичний алгоритм потребує в середньому $N/2$ кроків. Очевидно, що квантовий алгоритм буде ефективним лише тоді, коли "оракул" відповідає на запитання за час, що поліномно залежить від довжини вхідного слова, тобто, $\sim \mathrm{poly}(n)$.

Алгоритм Гровера зручно описувати у геометричній інтерпретації. Дія оператора $\mathbf{U}_{\boldsymbol{\omega}}$ на стан $|\mathbf{s}\rangle$ переводить його в стан $|\mathbf{s}'\rangle$, що є дзеркальним відображенням $|\mathbf{s}\rangle$ відносно $|\boldsymbol{\omega}^{\perp}\rangle$ (див. рис. 5.2). Кут між станами $|\mathbf{s}\rangle$ і $|\mathbf{s}'\rangle$ дорівнює 2θ. Наступне дзеркальне відображення $|\mathbf{s}'\rangle$ відносно $|\mathbf{s}\rangle$, виконуване оператором $\mathbf{U}_{\mathbf{s}}$, призводить до стану $|\mathbf{s}_1\rangle$, що є результатом першої ітерації Гровера. Кут між $|\mathbf{s}\rangle$ і $|\mathbf{s}_1\rangle$ дорівнює 2θ, а між $|\mathbf{s}_1\rangle$ і $|\boldsymbol{\omega}^{\perp}\rangle$ дорівнює 3θ. Наступна дія $\mathbf{U}_{\boldsymbol{\omega}}$ на стан $|\mathbf{s}_1\rangle$ переводить його у стан $|\mathbf{s}''\rangle$, що утворює кут 3θ із вектором $|\boldsymbol{\omega}^{\perp}\rangle$ і кут 4θ із вектором $|\mathbf{s}\rangle$. Відображення $\mathbf{U}_{\mathbf{s}}$ переводить вектор $|\mathbf{s}''\rangle$ у $|\mathbf{s}_2\rangle$, що утворює кут 4θ із вектором $|\mathbf{s}\rangle$ і кут 5θ з вектором $|\boldsymbol{\omega}^{\perp}\rangle$. Як ми з'ясували раніше, після k кроків кут між $|\mathbf{s}_k\rangle$ і $|\boldsymbol{\omega}^{\perp}\rangle$ буде $(2k+1)\theta$.

Який результат отримаємо після $k \approx \frac{\pi}{4}\sqrt{N}$ кроків алгоритму Гровера, якщо шуканого числа нема в проміжку $\mathbb{Z}_n$? В цьому випадку "оракул" завжди відповідатиме 0, тобто, не змінюватиме фазу в жодному з чисел із проміжку $\mathbb{Z}_n$, а значить оператор $\mathbf{U}_{\boldsymbol{\omega}} = \mathbf{I}$ і стан $|\mathbf{s}\rangle$ не повертається. Тому вимірювання будуть з однаковою ймовірністю давати всі числа з області визначення заданої функції.

Розгляньмо тепер випадок, коли $F(\mathbf{x}) = a$ виконується не для одного $\mathbf{x} = \boldsymbol{\omega}$, а для r значень $\boldsymbol{\omega}_i$. Тоді "оракул" відповідає "так" для всіх значень $\boldsymbol{\omega}_i$, тобто, переводить квантовий регістр аргументу у стан:

$$\frac{1}{\sqrt{N}} \sum_{\mathbf{x}} \sum_{i=1}^{r} (-1)^{f_{\boldsymbol{\omega}_i}(\mathbf{x})} |\mathbf{x}\rangle = \frac{1}{\sqrt{N}} \sum_{\mathbf{x}} |\mathbf{x}\rangle - \frac{2}{\sqrt{N}} \sum_{i=1}^{r} |\boldsymbol{\omega}_i\rangle,$$

що є еквівалентно дзеркальним відображенням відносно вектора, перпендикулярного до вектора, утвореного всіма невідомими значеннями аргументу,

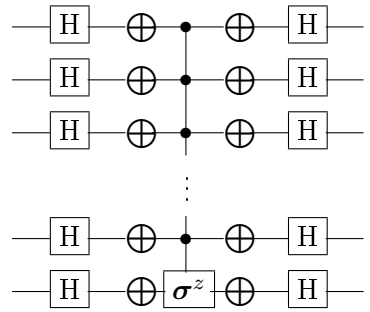
$$|\tilde{\boldsymbol{\omega}}\rangle = \frac{1}{\sqrt{r}} \sum_{i=1}^{r} |\boldsymbol{\omega}_i\rangle$$

у площині, в якій лежать вектори $|\tilde{\boldsymbol{\omega}}\rangle$ і $|\mathbf{s}\rangle$. Ці відображення виконує оператор $\mathbf{U}_{\tilde{\omega}} = \mathbf{I} - 2|\tilde{\boldsymbol{\omega}}\rangle\langle\tilde{\boldsymbol{\omega}}|$ і тепер кут повороту після виконання всіх ітерацій Гровера дорівнюватиме:

$$\sin\theta = \sqrt{\frac{r}{N}}.$$

Отже, після $k \approx \frac{\pi}{4}\sqrt{\frac{N}{r}}$ кроків регістр аргументу з імовірністю близькою до одиниці перейде в стан $|\tilde{\boldsymbol{\omega}}\rangle$, і його вимірювання дасть одне із значень $\boldsymbol{\omega}_i$. Зрозуміло, що у випадку множинності значень $\boldsymbol{\omega}_i$ задача їх визначення суттєво ускладнюється в порівнянні з випадком одного значення $\boldsymbol{\omega}$. Задача ще більше ускладнюється, коли невідомо кількість r шуканих величин, оскільки в цьому випадку невідомо скільки ітерацій треба виконати.

Оператор $\mathbf{U}_{\mathbf{s}}$ можна реалізувати такою квантовою схемою:



де контрольований $\mathbf{\Lambda}_{n-1}(\boldsymbol{\sigma}^z)$ при потребі можна замінити на:

$$(\mathbf{I}_{n-1} \otimes \mathbf{H})\, \mathbf{\Lambda}_{n-1}(\boldsymbol{\sigma}^x)\, (\mathbf{I}_{n-1} \otimes \mathbf{H}).$$

Матриця оператора $\mathbf{\Lambda}_{n-1}(\boldsymbol{\sigma}^z)$ має на головній діагоналі всі елементи, які дорівнюють $+1$ окрім останнього в правому нижньому кутку, який дорівнює -1. Дією операторів $\boldsymbol{\sigma}^x \otimes \boldsymbol{\sigma}^x \otimes \cdots \otimes \boldsymbol{\sigma}^x$ (з двох боків) ця матриця відбивається відносно бічної діагоналі і елемент -1 з правого нижнього кутка переходить у лівий верхній куток. А така матриця зображає оператор $\mathbf{I} - 2|\mathbf{0}\rangle\langle\mathbf{0}|$, який після дії операторів $\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$ (з двох боків) переходить в $\mathbf{I} - 2|\mathbf{s}\rangle\langle\mathbf{s}|$, тобто, в оператор $-\mathbf{U}_{\mathbf{s}}$. Знак мінус не впливає на збільшення амплітуди в кожній ітерації Гровера.

Окрім наведених в цьому розділі алгоритмів створено й інші, зокрема, пов'язані з квантовим перетворенням Фур'є.

Запропоновано також алгоритми, які окрім унітарних операцій передбачають і вимірювання.

Докладніший аналіз квантових алгоритмів висвітлено, зокрема, у працях [11, 14].

Розділ 6

Квантові шуми в процесорах

Досі ми розглядали квантовий процесор як ізольовану систему, еволюція якої є детермінованим процесом, що генерується дією зовнішніх класичних полів і внутрішніх взаємодій, які не руйнують її квантової когерентності. Однак жодна квантова система не може бути цілком ізольованою, з часом вона буде зазнавати зовнішніх впливів і втрачати квантову когерентність. Окрім того, фізична реалізація квантових логічних елементів не є цілком точною, що також призводить до помилок у станах квантового регістра. Виникає питання: чи такі впливи цілком унеможливлюють виконання квантових обчислень? Чи все ж обчислення можна виконувати, передбачивши певні запобіжні заходи? Дослідження переконують у тому, що за достатньо низького рівня квантових шумів можна збудувати певні системи захисту, які забезпечують коректне виконання обчислень.

З такими ж труднощами зіткнулися і розробники класичного процесора, тому спочатку ознайомимося із впливом шуму на передавання класичної інформації. Перешкоди в класичних каналах зв'язку (шум) називають також *завадами*.

6.1 Класичний шум

Нехай певне джерело генерує послідовності символів (текст) із деякого алфавіту, що містить N знаків (це можуть бути, наприклад, літери латинської, кириличної чи якоїсь іншої абетки разом із знаками пробілу, крапки, коми і т.д.). Алфавіт пронумеровано і кожному цілому числу з відрізка $1 \ldots N$ відповідає певний символ, який у вхідному тексті трапляється з частотою (ймовірністю)

$p_i \geq 0$, $\sum_{i=1}^{N} p_i = 1$. Під впливом шуму в каналі зв'язку (каналом зв'язку може бути процес зчитування з диска, шлейф між диском і материнкою, кабель інтернет-мережі, диски, карти пам'яті та ін.) сигнал може змінитися і на виході каналу символ за номером i вже буде сприйнятий як символ за номером j, тобто текст спотворюється і на виході каналу символи з алфавіту вже будуть траплятися з іншою частотою (ймовірністю) $q_i \geq 0$, $\sum_{i=1}^{N} q_i = 1$. Ці ймовірності пов'язані між собою:

$$q_i = \sum_{j=1}^{N} T_{ij} p_j \quad \text{чи у матричній формі} \quad \mathbf{q} = \mathbf{T}\,\mathbf{p}$$

матрицею ймовірності переходу $\mathbf{T}$, яка має властивості: 1) матриця $\mathbf{T}$ є позитивною, тобто, всі її елементи є додатними (інакше може статися, що деякі $q_i < 0$), 2) задовольняє умову повноти, тобто, сума елементів кожного стовпця має дорівнювати одиниці $\sum_i T_{ij} = 1$ (для того, щоб виконувалась умова $\sum_{i=1}^{N} q_i = 1$). Матриця $\mathbf{T}$ є однією з характеристик каналу, елемент матриці T_{ij} визначає ймовірність отримати на виході каналу символ за номером i, якщо на вхід каналу був поданий символ j. Для каналу без шуму матриця $\mathbf{T}$ є одиничною. Передача інформації в каналі може відбуватися в K кроків, тоді матриця ймовірності переходу каналу буде добутком матриць усіх кроків, тобто,

$$\mathbf{T} = \mathbf{T}_K \mathbf{T}_{K-1} \cdots \mathbf{T}_2 \mathbf{T}_1,$$

а кожна з цих матриць задовольняє умови 1)–2). Таку (досить тривалу) послідовність дії шуму трактують як стохастичний процес, при цьому у випадку слабкого шуму припускають, що шумові ефекти на різних кроках є незалежними, а такі стохастичні процеси називають *марковськими*. При слабкому шумі діагональні елементи матриці переходу суттєво більші за позадіагональні.

Важливим каналом зв'язку є *симетричний бінарний* (*двійковий*) *канал*, який передає двосимвольний алфавіт $\{0, 1\}$ із ймовірностями $T_{11} = T_{22} = 1 - p, T_{12} = T_{21} = p$. Зрозуміло, що при $p = 1/2$ канал є цілком зашумленим, бо при посиланні на вхід символу 0(1) на виході з однаковою ймовірністю отримуємо 0 чи 1, тобто, ми не можемо визначити, який символ було надіслано. Дія класичного

шуму в такому каналі призводить до *класичної помилки*, тобто, заміни 0→1 і навпаки 1→0, яка є також і в квантових каналах.

Встановлено, коли рівень шуму в класичному каналі є не дуже високим, то можна створити таку систему захисту інформації, яка цілком усуває його вплив.

Цей захист ґрунтується на *кодуванні*, тобто, додаванні такої кількості надлишкової інформації, яка після пошкодження в каналі, дає змогу відновити закодовану. Хоча методи кодування розроблено для довільних алфавітів [26, 27], далі розглядатимемо тільки бінарний канал.

Створено два принципово відмінні типи кодів: *блокові коди* і *деревоподібні коди* [26, 27], які поділяються на різні види. Для квантових обчислень важливими є блокові коди.

Нехай, через канал зв'язку треба передати текст в деякому алфавіті, кожен із M символів якого зображений послідовністю k бітів. У теорії кодування зазвичай починають із деякої довгої послідовності бітів, яку треба передати через канал із шумом. Цю послідовність розділяють на блоки довжиною k бітів, зрозуміло, що всього різних блоків може бути $M{=}2^k$. Кожному з блоків довжини k зіставляється *кодове слово* довжиною n, $(n{>}k)$, всіх кодових слів є $M{=}2^k$. *Кодом* називають множину всіх кодових слів, яка повинна бути векторним простором, якщо кодові слова інтерпретувати як вектори. Шум у каналі може перетворити їх у 2^n інших слів. Ймовірність того, що жоден символ кодового слова не зміниться дорівнює $K_0 = (1-p)^n$, ймовірність того, що зміниться один біт буде $K_1 = p(1-p)^{n-1}$, два — $K_2 = p^2(1-p)^{n-2}$, i бітів — $K_i = p^i(1-p)^{n-i}$. Якщо $p < 1/2$, то $K_0 > K_1 > K_2 > \ldots > K_n$, а це дає змогу припустити, що слова, найближчі до деякого кодового слова, утворилися саме з нього і прийняти його за вхідне. Близькість двох слів характеризується *віддаллю Хеммінга*, яка дорівнює кількості позицій, що відрізняються між собою. Множину кодових слів треба збудувати так, щоб мінімальна віддаль між кодовими словами d була якнайбільшою. Очевидно, що d буде тим більше, чим більше n, тобто, довгі кодові слова краще захищають інформацію. Однак тут треба шукати оптимум, оскільки збільшення n потребує більшої пропускної здатності каналу зв'язку. Збудовані у такий спосіб блокові коди позначають символами $[k, n, d]$.

Всього різних кодів може бути 2^{n2^k}, а це дуже велике число, тому задача створення доброго коду зі швидкими й ефективними алгоритмами кодування і декодування є складною проблемою захисту інформації від шуму [26, 27].

Коди, які дають змогу тільки встановити, що певне слово перебуває на віддалі $< d-1$ до найближчого кодового називають *кодами, що виявляють помилки.*

Якщо слово перебуває на віддалі t, що задовольняє умову $2t+1 \leq d$, від деякого кодового слова, то з високою ймовірністю можна вважати це кодове слово вхідним. Таке декодування називають *декодуванням із найвищою правдоподібністю.* Коди, які дають змогу це зробити, називають *кодами, що виправляють помилки.* Умова $2t+1 \leq d$ означає, що різні кодові слова a_{enc}, b_{enc} після пошкодження завадами $\mathcal{E}(\cdot)$ не збігаються, тобто виконується *умова виправлення (класичних) помилок*

$$\mathcal{E}(a_{enc}) \neq \mathcal{E}(b_{enc}). \tag{6.1}$$

Якщо ж кількість помилок така, що умова (6.1) не виконується, то виправити помилку не вдасться. Для класичних каналів створено велику кількість різноманітних кодів для різного характеру шумів (див., напр. [26, 27]).

Прикладом простого коду, що виправляє одну помилку, є код повторення $0 \to 000$, $1 \to 111$, із параметрами $[1, 3, 3]$. Дві чи три помилки цей код виправити не може, але їх ймовірність дорівнює $p_e = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$ і, якщо p достатньо мале, то вона суттєво менша ймовірності однієї помилки p незакодованого слова. Код повторення довжини n дає змогу виправити $(n-1)/2$ помилок.

Перш ніж перейти до розгляду задачі захисту в квантових каналах, з'ясуємо характер помилок, які в них викликає шум.

6.2 Квантові перетворення квабіта

У класичних бінарних каналах можлива тільки одна помилка — помилка перекидання біта, яка пов'язана з подоланням певного енергетичного бар'єру між двома станами фізичної системи.

Квантовий біт містить континуум станів, тому він є значно вразливішим до зовнішніх впливів, зокрема, в ньому можливі зміни станів і не пов'язані з обміном енергією, а такі, що викликають дуже малі зміни параметрів суперпозиції, в тому числі, неконтрольованої зміни фази. Однак дослідження виявили, що всі можливі помилки можна звести до кількох, які розглянемо нижче.

Стани квабіта описуємо як стани (псевдо)спіну і геометрично інтерпретуємо їх на сфері Блоха. Загалом оператор густини такий:

$$\boldsymbol{\rho} = \frac{1}{2}\left[\mathbf{I} + \vec{n}\vec{\boldsymbol{\sigma}}\right] = \frac{1}{2}\begin{bmatrix} 1+n_z & n_x - in_y \\ n_x + in_y & 1-n_z \end{bmatrix},$$

де $\mathbf{I}$ — одинична матриця, $\vec{\boldsymbol{\sigma}} = (\boldsymbol{\sigma}^x, \boldsymbol{\sigma}^y, \boldsymbol{\sigma}^z)$, $\vec{n} = (n_x, n_y, n_z)$ — вектор, уздовж якого скеровано спін, $|\vec{n}| = 1$ — для чистих станів і $0 \le |\vec{n}| < 1$ — для змішаних.

Довільне перетворення, що зберігає слід, можна записати:

$$\vec{n} \xrightarrow{\mathcal{E}} \vec{n}' = \mathbf{R}\vec{n} + \vec{c},$$

де $\mathbf{R}$ — дійсна матриця 3×3, $\vec{c}$ — сталий вектор. Такому перетворенню відповідають елементи:

$$\mathbf{E}_k = \alpha_k \mathbf{I} + \sum_{j=\{x,y,z\}} \alpha_{kj} \boldsymbol{\sigma}^j.$$

Це найзагальніше перетворення квабіта, що зберігає слід. Для спіну $s = 1/2$ кількість елементів перетворення не перевищує n^2, тобто, $1 \le k \le n^2 = 4$.

Розглянемо тепер окремі механізми квантових перетворень, чи, як їх іще називають, *квантові канали.*

1. Канал із класичною помилкою описує суттєво квантове перетворення квабіта, яке цілком еквівалентне шуму в класичному бінарному симетричному каналі, тобто з ймовірністю $(1-p)$ квабіт зберігає свій стан, а з ймовірністю p переходить зі стану $|0\rangle$ в $|1\rangle$ і навпаки, зі стану $|1\rangle$ в $|0\rangle$. Квантове перетворення в цьому випадку можна зобразити двома елементами:

$$\mathbf{E}_0 = \sqrt{1-p}\mathbf{I} = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \mathbf{E}_1 = \sqrt{p}\boldsymbol{\sigma}^x = \sqrt{p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

які перетворюють матрицю густини квабіта

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}^x(\boldsymbol{\rho}) = \mathbf{E}_0\boldsymbol{\rho}\mathbf{E}_0^+ + \mathbf{E}_1\boldsymbol{\rho}\mathbf{E}_1^+ = \frac{1}{2}\left(\mathbf{I} + \vec{n}'\vec{\boldsymbol{\sigma}}\right)$$

так, що вектор $\vec{n}$ переходить у $\vec{n}' = (n_x, (1-2p)n_y, (1-2p)n_z)$, тобто, сфера Блоха деформується в еліпсоїд обертання навколо осі x і вироджується у відрізок $[-1, 1]$ осі x при $p = 1/2$.

2. Канал перекидання фази описує суттєво квантове перетворення квабіта, яке не має класичного аналогу. Його елементи, які можна зобразити у вигляді:

$$\mathbf{E}_0 = \sqrt{1-p}\mathbf{I} = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \mathbf{E}_1 = \sqrt{p}\boldsymbol{\sigma}^z = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

перетворюють матрицю густини квабіта

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}^z(\boldsymbol{\rho}) = \mathbf{E}_0\boldsymbol{\rho}\mathbf{E}_0^+ + \mathbf{E}_1\boldsymbol{\rho}\mathbf{E}_1^+ = \frac{1}{2}\left(\mathbf{I} + \vec{n}'\vec{\boldsymbol{\sigma}}\right)$$

у стан із вектором $\vec{n}' = ((1-2p)n_x, (1-2p)n_y, n_z)$, тобто, сфера Блоха деформується в еліпсоїд обертання навколо осі z і вироджується у відрізок $[-1, 1]$ осі z при $p = 1/2$.

3. Канал із фазовою помилкою має такі елементи квантового перетворення:

$$\mathbf{E}_0 = \sqrt{1-p}\mathbf{I} = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{E}_1 = \sqrt{p}\boldsymbol{\sigma}^y = \sqrt{p}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

які перетворюють матрицю густини квабіта

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}^y(\boldsymbol{\rho}) = \mathbf{E}_0\boldsymbol{\rho}\mathbf{E}_0^+ + \mathbf{E}_1\boldsymbol{\rho}\mathbf{E}_1^+ = \frac{1}{2}\left(\mathbf{I} + \vec{n}'\vec{\boldsymbol{\sigma}}\right)$$

у стан із вектором $\vec{n}' = ((1-2p)n_x, n_y, (1-2p)n_z)$, так, що сфера Блоха деформується в еліпсоїд обертання навколо осі y і вироджується у відрізок $[-1, 1]$ осі y при $p = 1/2$.

Розглянуті три перетворення повертають і зменшують довжину всіх векторів, крім тих, які скеровані вздовж осей x, z, y, відповідно, оскільки останні описують стани, що є власними для цих

перетворень. Легко перевірити, що ці перетворення задовольняють умову повноти.

4. Деполяризуючий канал — це таке квантове перетворення, коли з ймовірністю p квабіт переходить у цілком змішаний стан та з ймовірністю $(1-p)$ залишається в початковому стані, тобто,

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}(\boldsymbol{\rho}) = p\frac{1}{2}\mathbf{I} + (1-p)\boldsymbol{\rho} = \frac{1}{2}\left(\mathbf{I} + \vec{n}'\vec{\boldsymbol{\sigma}}\right) \tag{6.2}$$

сфера Блоха змінює радіус в p разів $\vec{n}' = (1-p)\vec{n} = ((1-p)n_x, (1-p)n_y, (1-p)n_z)$, при $p = 1$ спін переходить у цілком змішаний стан. Одним із можливих виборів елементів цього квантового перетворення може бути набір:

$$\mathbf{E}_0 = \sqrt{1 - \frac{3}{4}p}\mathbf{I},\ \mathbf{E}_1 = \frac{\sqrt{p}}{2}\boldsymbol{\sigma}^x,\ \mathbf{E}_2 = \frac{\sqrt{p}}{2}\boldsymbol{\sigma}^y,\ \mathbf{E}_3 = \frac{\sqrt{p}}{2}\boldsymbol{\sigma}^z,$$

який легко можна отримати з (6.2), використовуючи справедливу для квабіта тотожність:

$$\mathbf{I} = \frac{1}{2}\left(\boldsymbol{\rho} + \boldsymbol{\sigma}^x\boldsymbol{\rho}\boldsymbol{\sigma}^x + \boldsymbol{\sigma}^y\boldsymbol{\rho}\boldsymbol{\sigma}^y + \boldsymbol{\sigma}^z\boldsymbol{\rho}\boldsymbol{\sigma}^z\right).$$

Іншим вибором елементів квантового перетворення деполяризуючого каналу може бути набір:

$$\mathbf{F}_0 = \sqrt{1-p}\mathbf{I},\ \mathbf{F}_1 = \sqrt{\frac{p}{3}}\boldsymbol{\sigma}^x,\ \mathbf{F}_2 = \sqrt{\frac{p}{3}}\boldsymbol{\sigma}^y,\ \mathbf{F}_3 = \sqrt{\frac{p}{3}}\boldsymbol{\sigma}^z,$$

який задає перетворення $\boldsymbol{\mathcal{F}}(\boldsymbol{\rho}) = \frac{2}{3}p\mathbf{I} + (1 - \frac{4}{3}p)\boldsymbol{\rho}$, яке набуває вигляду (6.2) після заміни $p \to 3/4p$.

5. Канал загасання амплітуди пов'язаний із процесами дисипації енергії в системі, викликаними нестабільністю (квазістабільністю) одного з рівнів квабіта (напр. $|1\rangle$), коли з часом квабіт спонтанно переходить в основний стан (напр. $|0\rangle$). Таке перетворення описують елементами, які задовольняють умову повноти:

$$\mathbf{E}_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad \mathbf{E}_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix},$$

а ймовірність переходу $|1\rangle\to|0\rangle$ γ для спінової моделі пов'язана із спін-ґратковою взаємодією $\gamma{=}1-\exp(-t/T_1)$. Перетворення

$$\mathcal{E}(\boldsymbol{\rho}) = \mathbf{E}_0\boldsymbol{\rho}\mathbf{E}_0^+ + \mathbf{E}_1\boldsymbol{\rho}\mathbf{E}_1^+ = \frac{1}{2}\left(\mathbf{I} + \vec{n}'\boldsymbol{\sigma}\right)$$

деформує $\vec{n}' = \left(\sqrt{1-\gamma}n_x, \sqrt{1-\gamma}n_y, (1-\gamma)n_z + \gamma\right)$ сферу Блоха так, що вона перетворюється в еліпсоїд обертання навколо осі z, центр якого зсувається до точки $|0\rangle$, яка залишається нерухомою при цьому перетворенні.

6. Канал узагальненого загасання амплітуди описує процес дисипації енергії в середовищі зі скінченною амплітудою. Елементи цього перетворення

$$\mathbf{E}_0 = \sqrt{p}\begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{bmatrix}, \quad \mathbf{E}_1 = \sqrt{p}\begin{bmatrix}0 & \sqrt{\gamma}\\ 0 & 0\end{bmatrix},$$
$$\mathbf{E}_2 = \sqrt{1-p}\begin{bmatrix}\sqrt{1-\gamma} & 0\\ 0 & 1\end{bmatrix}, \quad \mathbf{E}_3 = \sqrt{1-p}\begin{bmatrix}0 & 0\\ \sqrt{\gamma} & 0\end{bmatrix}$$

деформують сферу Блоха подібно як і у попередньому випадку:

$$\vec{n}' = \left(\sqrt{1-\gamma}n_x, \sqrt{1-\gamma}n_y, (1-\gamma)n_z + (2p-1)\gamma\right),$$

при $p{=}1$ цей канал діє як попередній. Перші два елементи цього квантового перетворення $\mathbf{E}_0$ і $\mathbf{E}_1$ описують переходи із стану $|1\rangle$ в стан $|0\rangle$, а два наступні елементи $\mathbf{E}_2$ і $\mathbf{E}_3$ описують переходи із стану $|0\rangle$ в стан $|1\rangle$, тобто, процес збудження під впливом температури (в попередньому випадку цього механізму не було). При великих часах $\gamma{=}1$ і $\vec{n}'{=}(0,0,(2p-1))$, тому в системі можна виділити ефективно чистий стан. Для високих температур характерна однакова заселеність рівнів $|0\rangle$ і $|1\rangle$, тобто система перебуває у цілком змішаному стані і $\vec{n}'{=}(0,0,0)$, тобто, $p{=}1/2$. Отже, p описує співвідношення заселеностей рівнів, коли при $p{\le}1/2$ переважають процеси збудження над процесами загасання і навпаки.

7. Канал загасання фази, як і інші квантові перетворення, можна зобразити різними операторними елементами, зокрема:

$$\mathbf{E}_0 = \begin{bmatrix}1 & 0\\ 0 & \sqrt{1-q}\end{bmatrix}, \qquad \mathbf{E}_1 = \begin{bmatrix}0 & 0\\ 0 & \sqrt{q}\end{bmatrix}$$

або

$$\mathbf{F}_0 = (1-p)\mathbf{I}, \qquad \mathbf{F}_1 = \begin{bmatrix} \sqrt{q} & 0 \\ 0 & 0 \end{bmatrix}, \qquad \mathbf{F}_2 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{q} \end{bmatrix},$$

які призводять до того самого результату:

$$\boldsymbol{\rho}' = \boldsymbol{\mathcal{E}}(\boldsymbol{\rho}) = \boldsymbol{\mathcal{F}}(\boldsymbol{\rho}) = \begin{bmatrix} \rho_{00} & (1-q)\rho_{01} \\ (1-q)\rho_{10} & \rho_{11} \end{bmatrix}. \tag{6.3}$$

Загасання фази не пов'язано із втратою енергії, а з певними процесами "розсіяння", якщо ймовірність акту такого "розсіяння" за малий проміжок часу також мала і дорівнює $q{=}\Gamma\Delta t$, тоді за час $t{=}n\Delta t$ відбудеться n таких актів "розсіяння" і сумарне квантове перетворення буде:

$$\boldsymbol{\mathcal{E}}^n(\boldsymbol{\rho}){=}\begin{bmatrix} \rho_{00} & (1-\Gamma t/n)^n\rho_{01} \\ (1-\Gamma t/n)^n\rho_{10} & \rho_{11} \end{bmatrix}$$

а при великих n воно перейде в:

$$\boldsymbol{\mathcal{E}}^{n\to\infty}(\boldsymbol{\rho}) = \begin{bmatrix} \rho_{00} & e^{-\Gamma t}\rho_{01} \\ e^{-\Gamma t}\rho_{10} & \rho_{11} \end{bmatrix}.$$

Отже, з часом відбувається втрата відносної фази власних станів енергії, інтерференційні елементи матриці густини занулюються, і вона стає діагональною, тобто, квабіт переходить у змішаний стан. У спінових системах цей процес пов'язують із спін-спіновою релаксацією, тоді $\Gamma = 1/T_2$, де T_2 — час поперечної релаксації.

Такий процес часто називають *декогеренцією*, хоча це тільки загасання фази, а декоренцією правильно називати всі процеси (зокрема і розглянуті вище квантові канали), які призводять до втрати квантової когерентності.

Повернувшись до зображення станів квабіта на сфері Блоха, із (6.3) зауважуємо, що вектор напряму спіну $\vec{n}$ змінюється на $\vec{n}' = ((1-q)n_x, (1-q)n_y, n_z)$, тобто, як у каналі перекидання фази, і справді антиунітарне перетворення ($\det \mathbf{V} = -1$)

$$\begin{bmatrix} \tilde{\mathbf{E}}_0 \\ \tilde{\mathbf{E}}_1 \end{bmatrix} = \begin{bmatrix} \sqrt{\alpha} & \sqrt{1-\alpha} \\ \sqrt{1-\alpha} & -\sqrt{\alpha} \end{bmatrix} \begin{bmatrix} \mathbf{E}_0 \\ \mathbf{E}_1 \end{bmatrix}$$

призводить до інших елементів цього ж квантового перетворення:

$$\tilde{\mathbf{E}}_0 = \sqrt{\alpha}\mathbf{I}, \qquad \tilde{\mathbf{E}}_1 = \sqrt{1-\alpha}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

де $\alpha = \frac{1}{2}\left(1+\sqrt{1-q}\right)$, що цілком збігається з елементами квантового перетворення каналу перекидання фази. Виявлення цього зв'язку є важливим результатом, оскільки уможливлює використання для квантової корекції помилок у каналі загасання фази тих же засобів, що й у випадку каналу перевороту фази.

6.3 Виправлення помилок

Отже, помилки квантового біта утворюють множину континуальної потужності, однак їх можна поділити на декілька характерних типів. Встановлено (див., напр. [11, 16, 17]), що як і у класичному випадку, коли є тільки одна помилка, можна побудувати квантові коди, які дають змогу не тільки виявляти, але і виправляти помилки. Створені сьогодні підходи є доволі складними, докладно ознайомитися з ними можна, зокрема, у працях [11, 16, 17] і цитованій там літературі. Тут ми проілюструємо ідеї квантового кодування на простих прикладах.

Код повторення з трьох бітів у квантовому випадку називається *триквабітовим кодом*, він так кодує стани $|0\rangle, |1\rangle$

$$|0\rangle \to |000\rangle,\ |1\rangle \to |111\rangle, \qquad \alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle. \quad (6.4)$$

Генерується цей код квантовою схемою з двох квантових вентилів **CNOT**

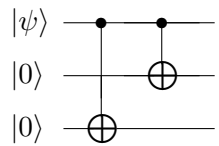


Рис. 6.1: Схема формування коду, що виправляє класичні помилки

Як і класичний трибітовий код повторення, цей код виправляє одну класичну помилку, ймовірність того, що залишилися невиправленими дві і більше помилки дорівнює $p_e = 3p^2 - 2p^3$.

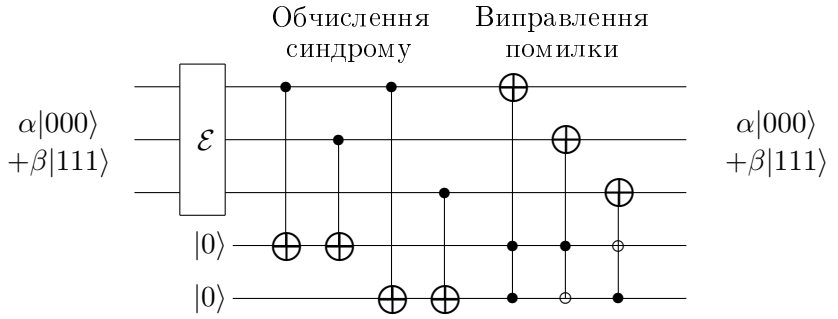


Рис. 6.2: Квантова схема виправлення однієї класичної помилки. Порожні кружечки на схемі означають, що вентиль спрацьовує при стані відповідного квабіта $|0\rangle$.

На рис. 6.2 зображено квантову схему виправлення однієї класичної помилки. Після виходу із каналу, де була зроблена помилка $\mathcal{E}$, виконується *обчислення синдрому* помилки, інколи кажуть *вимірювання синдрому*, яке полягає у виявленні квабіта, стан якого змінився $|0\rangle \rightleftarrows |1\rangle$. Потім відбувається виправлення помилки, коли у виявленому квабіті відновлюється початковий стан $|1\rangle \rightleftarrows |0\rangle$. Ця схема працює і для класичних бітів.

Цікавішим є виправлення помилки в каналі перекидання фази. Для її виявлення і виправлення використовують код, який генерується такою схемою:

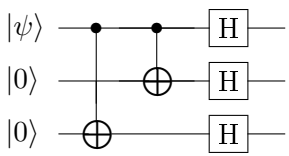


Рис. 6.3: Схема формування коду, що виправляє помилки перекидання фази

і створює такі кодові стани:

$$|0\rangle \to |000\rangle \to |{+}{+}{+}\rangle, \quad |1\rangle \to |111\rangle \to |{-}{-}{-}\rangle,$$
$$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle \to \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle,$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Помилка перекидання фази призводить до класичної помилки на станах $|+\rangle, |-\rangle$, тобто, $|+\rangle \rightleftarrows |-\rangle$. Оскільки оператор Адамара перетворює стани $|0\rangle \rightleftarrows |+\rangle$ і $|1\rangle \rightleftarrows |-\rangle$, то для побудови квантової схеми виправлення помилки перекидання фази досить у схемі для виправлення класичної помилки (рис. 6.2) на початку (перед операторами **CNOT**) і в кінці лінії кожного квабіту коду поставити оператор Адамара. Після такої модифікації схема буде забезпечувати передавання слова $\alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$ без помилок із ймовірністю $P = 1 - 3p^2 + 2p^3$.

Із цих простих триквабітових кодів П.Шор збудував дев'ятиквабітовий код, що виправляє одночасно дві помилки — класичну і помилку перекидання фази. Схему для його генерування можна отримати із схеми на рис. 6.3, приєднуючи до кожної лінії квабіта після оператора Адамара схему генерування коду, що виправляє класичну помилку (рис. 6.1) лінією, що починається квабітом $|\psi\rangle$. Подібно збудовані коди називають *каскадними*. Отримана схема генерує такі кодові стани:

$$|0\rangle \to |000\rangle \to |{+}{+}{+}\rangle \to$$
$$\to 2^{-3/2}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle),$$
$$|1\rangle \to |111\rangle \to |{-}{-}{-}\rangle \to$$
$$\to 2^{-3/2}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).$$

На противагу до триквабітового коду, який дуже подібний до класичного, дев'ятиквабітовий код Шора є значно надійнішим, оскільки він збудований із заплутаних станів, що є стійкими до локального пошкодження.

Схему для виправлення класичних помилок і помилок перекидання фази в коді Шора можна збудувати на підставі схеми рис. 6.2, вона доволі громіздка, тому не будемо її розглядати. Цей код виправляє *всі* квантові помилки одного квабіта [11, 17].

Які ж квантові помилки виправляє певний запропонований квантовий код? Нехай всі його кодові стани, що повинні бути ортонормованими, утворюють векторний простір $\mathcal{QC}$, а $\mathbf{P}$ — проектор на цей простір, тоді, якщо виконується умова:

$$\mathbf{P}\mathbf{E}_\mathbf{i}^\dagger\mathbf{E}_\mathbf{j}\mathbf{P} = \alpha_{\mathbf{ij}}\mathbf{P}, \tag{6.5}$$

де $[\alpha_{ij}]$ — ермітова матриця, то цей код виправляє всі помилки, зумовлені квантовим перетворенням $\mathcal{E}$ з елементами $\mathbf{E}_i$ [11]. Не важко здогадатися, що цей код виправляє також помилки зумовлені шумом із елементами $\mathbf{F}_j = \sum_i \beta_{ji}\mathbf{E}_i$ де $[\beta_{ji}]$ — матриця з комплексних чисел. Оскільки будь-який елемент $\mathbf{E}_i$ можна зобразити лінійною комбінацією матриць Паулі $\boldsymbol{\sigma}^0, \boldsymbol{\sigma}^x, \boldsymbol{\sigma}^y, \boldsymbol{\sigma}^z$, то достатньо встановити виконання умови (6.5) для цих матриць, тобто,

$$\mathbf{P}\boldsymbol{\sigma}_n^\mu\boldsymbol{\sigma}_n^\nu\mathbf{P} = \alpha_{\mu\nu}\mathbf{P}, \tag{6.6}$$

тут n — номер квабіта в коді. Отже, якщо для певного квантового коду виконується умова (6.6), то цей код може виправляти довільну одноквабітову помилку.

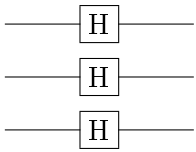
Отже, якщо p — ймовірність помилки в одному квабіті, то квантовий код, що виправляє помилки, дає змогу знизити ймовірність помилки до cp^2 у кожному кодовому стані (слові), де c — стала, залежна від довжини кодового слова.

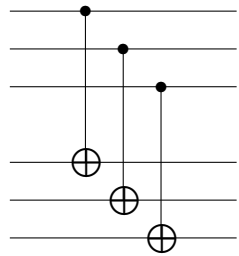
6.4 Обчислення, захищені від помилок

Є два головних джерела помилок у квантовому регістрі під час виконання квантових обчислень — це декогеренція, викликана взаємодією з оточенням, і помилки від неточного виконання квантових вентилів. Квантові схеми виправлення помилок потребують введення у квантовий регістр значної кількості додаткових квабітів і виконання багатьох додаткових квантових вентилів, що призводить до виникнення великої кількості нових помилок. То чи такий спосіб захисту сприятиме виконанню квантових обчислень?

Раніше ми згадували, що набір $\{\mathbf{H}, \mathbf{\Phi}(\pi/2), \mathbf{\Phi}(\pi/4), \mathbf{\Lambda}_1(\mathbf{X})\}$ утворює повний базис квантових вентилів (КЛЕ), який разом із

ініціалізацією та різними операціями вимірювання дають змогу виконати довільне квантове обчислення з наперед заданою точністю. Ці вентилі працюють із окремими (одним чи двома) квабітами. Для роботи із закодованими квабітами треба закодувати КЛЕ. Нижче наведено приклади закодованих квантових вентилів Адамара та **CNOT** на триквабітовому коді. Групу квабітів, що несуть кодовий стан, називають блоком.





Закодований КЛЕ є відмовостійким, якщо під час виконання він породжує не більше однієї помилки в блоці. Двоквабітові вентилі можуть поширювати одну помилку на два квабіти чи породжувати одну або дві помилки, але вони будуть по одній у блоці. Якщо в кожному блоці після кожного квантового вентиля буде діяти схема виправлення помилок, то ймовірність невиправленої помилки буде cp^2, де p — ймовірність виникнення однієї помилки, c — стала, що залежить від довжини кодового слова, кількості компонент закодованого вентиля та інших характеристик ($c > 10^4$) [11]. Схема виправлення помилок також повинна працювати з надійністю cp^2. Отже, обчислення виконуються коректно, якщо ймовірність виникнення однієї помилки менша від порогового значення $p < p_{\text{пор}} = 1/c \sim 10^{-5} \div 10^{-6}$ [11]. Ймовірність невиправленої помилки значно зменшиться, якщо використати *каскадні коди*, тобто, кожен квабіт коду знову закодувати тим самим кодом, тоді ймовірність буде $c(cp^2)^2{=}c^3p^4$, а після каскаду із k рівнів $(cp)^{2^k}/c$.

Порогова теорема [11, 17] стверджує, що ідеальну квантову схему із M вентилів можна моделювати з ймовірністю помилки не більшою ніж ε, використовуючи $O\left(M \log^m \left(\frac{M}{\varepsilon}\right)\right)$ вентилів на апаратурі, компоненти якої вносять помилки з ймовірністю p нижчою деякої порогової $p_{\text{пор}}$ і за розумних припущень стосовно завад на цьому обладнанні.

Розділ 7

Квантовий процесор на основі ЯМР у рідких розчинах

Розглянута вище ідеалізована модель спіну 1/2 у магнітному полі, як квантового біта, найповніше відповідає спіновим станам ядер таких нерадіоактивних ізотопів: ^1H, ^{13}C, ^{15}N, ^{19}F, ^{31}P та деяких інших. Атомні ядра досить добре ізольовані і зазнають незначного зовнішнього впливу. У складі великих органічних молекул вони формують систему квантових бітів, стани яких чітко ідентифікуються за енергетичними рівнями (частотами переходів). Міжспінова взаємодія, необхідна для виконання двоквабітових операцій, формується електронними оболонками. Електронні оболонки впливають також на частоти прецесій ядерних спінів $\omega_{A,(B),\ldots}$ у постійному зовнішньому полі B_0. Тому навіть тотожні ядра в різних положеннях у молекулі мають різні частоти. Цю зміну частоти називають *хімічним зсувом*. Системи з тотожних (але не еквівалентних) ядер називаються *гомоядерними*, з різних — *гетероядерними*. Ядра інших хімічних елементів, що входять до складу молекули, мусять мати частоти, які лежать поза областю частот квабітів. Електронні спіни мають частоти на чотири-п'ять порядків вищі ніж ядерні і, тому їх можна не розглядати.

Всі L ядерних спінів такої молекули і утворюють квантовий регістр. Однієї молекули недостатньо для отримання сигналу, який би можна було зареєструвати приймачами, тому використовують їх розчин при кімнатних температурах із загальною кількістю у квантовому регістрі приблизно $\sim 10^{18}$. Такий квантовий комп'ютер (регістр) називається *ансамблевим*, бо він є змішаним ансамблем спінів, що належать до різних молекул. Це створює певні проблеми в приготуванні початкового стану (*ініціалізації*), вико-

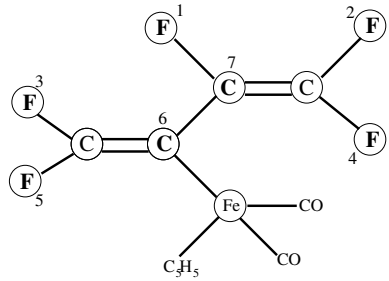


Рис. 7.1: Хімічна структура молекули, використаної в [29] як семиквабітовий квантовий регістр при реалізації алгоритму Шора

нанні обчислень та зчитуванні результату.

Гамільтоніан системи взаємодіючих спінів у середовищі (не обов'язково рідкому), поміщеному в постійне магнітне поле, має вигляд:

$$\mathcal{H} = -\frac{\hbar}{2}\sum_j \omega_j \boldsymbol{\sigma}_j^z + \frac{\hbar}{2}\sum_{j<l} \Omega_{jl}\vec{\boldsymbol{\sigma}}_j\vec{\boldsymbol{\sigma}}_l + \mathcal{H}^D + \mathcal{H}^{env}, \qquad (7.1)$$

де перший доданок визначає взаємодію спінів із полем, другий — обмінну взаємодію між спінами в межах молекули, доданок

$$\mathcal{H}^D = \frac{\hbar}{2}\sum_{j<l} \frac{\gamma_j\gamma_l}{2|\vec{r}_j - \vec{r}_l|^3}\left(\vec{\boldsymbol{\sigma}}_j\vec{\boldsymbol{\sigma}}_l - 3\left(\vec{\boldsymbol{\sigma}}_j\vec{n}_{jl}\right)\left(\vec{\boldsymbol{\sigma}}_l\vec{n}_{jl}\right)\right),\ \vec{n}_{jl} \equiv \frac{\vec{r}_l - \vec{r}_j}{|\vec{r}_l - \vec{r}_j|} \quad (7.2)$$

задає пряму магнітну дипольну взаємодію між спінами з координатами $\vec{r}_j$, $\vec{r}_l$ (попарну взаємодію класичних магнітних диполів), яка сильно залежить від взаємної орієнтації спінів. Останній доданок описує інші взаємодії спінів з оточенням.

Спін-спінові взаємодії призводять до спін-спінової релаксації, що характеризується *часом поперечної релаксації* τ_2, який визначає півширину спектральної лінії $2/\tau_2$. Суттєвий вклад у спін-спінову релаксацію в кристалах вносять магнітні дипольні взаємодії (7.2), тоді як у рідинах, унаслідок швидких обертальних рухів молекул, ці взаємодії усереднюються і їхній вклад зменшується так, що спектральні лінії звужуються на декілька порядків,

Табл. 7.1: Хімічні зсуви частот в полі 11.7 Тл ($\Delta\omega_i$, Hz), часи релаксації ($\tau_i^{(1)}$, $\tau_i^{(2)}$, sec), відносні частоти (Ω_{ij}, Hz) ядерних спінів молекули, зображеної на рис. 7.1. Взято з [29]

i	$\Delta\omega_i$	$\tau_1^{(i)}$	$\tau_2^{(i)}$	Ω_{7i}	Ω_{6i}	Ω_{5i}	Ω_{4i}	Ω_{3i}	Ω_{2i}
1	−22052.0	5.0	1.3	−221.0	37.7	6.6	−114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	−3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	−13.5	41.6	12.9		
4	−4918.7	10.0	1.7	54.1	−5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	−4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						

тобто, τ_2 зростає на декілька порядків. Разом із *часом спін-ґратткової релаксації* τ_1 час поперечної релаксації τ_2 характеризує час перебування системи в когерентному стані, а оскільки $\tau_1 \gg \tau_2$, то останній вважають часом когерентності. В рідких розчинах він може змінюватися від 10^{-2} сек до 10^8 сек, що дає змогу виконати $10^5 \div 10^{14}$ елементарних операцій одноквабітових квантових вентилів.

Як зазначалося раніше, у випадку, коли частоти прецесії спінів у магнітному полі сильно відрізняються, тобто, $|\omega_l - \omega_j| \gg |\Omega_{jl}|$, обмінну міжспінову взаємодію досить розглядати як Ізінгову:

$$\frac{\hbar}{2}\sum_{j<l}\Omega_{jl}\boldsymbol{\sigma}_j^z\boldsymbol{\sigma}_l^z.$$

Квантові вентилі (КЛЕ) в таких системах можна реалізувати, використовуючи методи ядерного магнітного резонансу (ЯМР). Оскільки переходи відбуваються між станами з дуже вузькими спектральними лініями, то такий ЯМР називають *ЯМР з високою роздільною здатністю*.

7.1 Основи методу ядерного магнітного резонансу

Для вивчення зразків методом ЯМР їх вміщують у сильне постійне магнітне поле B_0, скероване вздовж осі z. Воно має бути однорідним по всьому об'єму зразка, щоб забезпечити рівність частот усіх тотожних спінів. Напруженість його має бути якомога вищою, щоб забезпечити велику різницю частот і, внаслідок цього, високу роздільну здатність. Створюють таке поле надпровідниковими електромагнітами, оптимальна його напруженість на сьогодні $\sim 10 \div 12$ Тл (Тесла). Радіочастотні імпульси формуються двома парами соленоїдів, що створюють змінні магнітні поля, скеровані вздовж осей x та y лабораторної системи відліку. Ці ж соленоїди детектують сигнали, зумовлені змінним магнітним полем, генерованим спінами, що релаксують до рівноваги.

Вплив радіочастотних імпульсів на заселеність рівнів. Для розгляду дії радіочастотних імпульсів, використовуваних у ЯМР, до гамільтоніану системи (7.1) треба додати доданок, що описує взаємодію із змінним поперечним полем:

$$\mathcal{H}^{\text{рч}} = -\frac{\hbar}{2}\sum_j \Omega_j \left[f_x(t)\boldsymbol{\sigma}_j^x + f_y(t)\boldsymbol{\sigma}_j^y \right].$$

Якщо частота радіочастотного імпульсу ω збігається з частотою прецесії ω_l спіну l, то із всієї суми суттєвим є тільки доданок з індексом l. В умовах цього резонансу спін здійснює осциляції Рабі, тобто, з частотою Ω_l переходить із рівня $E_l^{(+)}$ на рівень $E_l^{(-)}$ і навпаки. Нехай N_+, N_- — заселеності відповідних рівнів і $N_+ + N_- = N = \text{const}$, тоді:

$$\frac{dN_+}{dt} = N_- w_{(-)\to(+)} - N_+ w_{(+)\to(-)}$$

Оскільки ймовірності вимушених переходів під впливом збурення V у дворівневій системі не залежать від напряму переходу [1]:

$$w = \frac{2\pi}{\hbar}|\langle f|V|j\rangle|^2 \delta(\omega_{fj}) \tag{7.3}$$

тобто, $w_{(+)\to(-)} = w_{(-)\to(+)} = w$, то:

$$\frac{dn}{dt} = -2wn, \qquad n \equiv N_- - N_+ \quad \Longrightarrow \quad n(t) = n(0)e^{-2wt}.$$

Тобто, за час тривалої дії радіочастотного поля, що викликає осциляції Рабі, заселеності рівнів стають однаковими $n \to 0$.

Швидкість поглинання енергії дорівнює:

$$\frac{dE}{dt} = N_- w\hbar\omega - N_+ w\hbar\omega = \hbar\omega w n.$$

Якщо $n > 0$, тобто, заселеність нижчого рівня більша, то відбувається поглинання, якщо ж заселеність вищого рівня більша, $n < 0$, то відбувається випромінювання енергії. За однакової заселеності рівнів n=0 не повинно відбуватися ні поглинання, ні випромінювання, однак експериментально цього не спостерігають, що свідчить про існування також інших механізмів зміни заселеності.

Зміна заселеності рівнів під впливом теплових рухів. Нехай у системі відсутнє резонансне радіочастотне поле, але залишається постійне поле B_0. Візьмемо до уваги взаємодію спінів із середовищем. Вона спричинятиме обмін енергією, унаслідок якого спінова система намагатиметься мінімізувати свою вільну енергію, тобто, якомога більшу кількість спінів перевести у стан із нижчою енергією $E^{(-)}$, що призведе до встановлення термодинамічної рівноваги, коли

$$\frac{N_+^0}{N_-^0} = e^{-\frac{\hbar\omega_l}{kT}}.$$

Нагадаємо, що ми розглядаємо переходи певного спіну l, який ідентифікуємо за частотою ω_l, таких спінів є N — як і великих молекул у системі.

Позначимо ймовірність переходів спіну із стану з меншою енергією в стан із більшою енергією через $w_\uparrow$, а в зворотньому напрямі — через $w_\downarrow$, тоді зміну заселеності опишемо рівнянням:

$$\frac{dN_-}{dt} = N_+ w_\downarrow - N_- w_\uparrow. \tag{7.4}$$

З умови рівноваги отримаємо:

$$\frac{N_+^0}{N_-^0} = \frac{w_\uparrow}{w_\downarrow} = e^{-\frac{\hbar\omega_l}{kT}}.$$

Увівши $N{\equiv}N_+{+}N_-$ і $n{\equiv}N_-{-}N_+$, рівняння (7.4) можна записати:

$$\frac{dn}{dt}=\frac{n_0-n}{\tau_1},\qquad n_0\equiv N\frac{w_\downarrow-w_\uparrow}{w_\downarrow+w_\uparrow},\qquad \tau_1\equiv\frac{1}{w_\downarrow+w_\uparrow}. \tag{7.5}$$

Інтегрування рівняння (7.5) дає релаксаційну залежність різниці заселеностей:

$$n(t)=n_0+Ae^{-t/\tau_1},$$

де τ_1 — час спін-ґраткової релаксації, A — стала інтегрування. Розглянувши дію радіочастотного сигналу разом із спін-ґратковою релаксацією, отримаємо рівняння:

$$\frac{dn}{dt}=-2wn+\frac{n_0-n}{\tau_1}\implies n(t)=n_0\frac{1+2w\tau_1e^{-(2w+1/\tau_1)t}}{1+2w\tau_1},$$

звідки знайдемо рівноважну різницю заселеностей в умовах дії радіочастотного поля і спін-ґраткової релаксації:

$$n^{(0)}=\frac{n_0}{1+2w\tau_1}.$$

Отримана залежність свідчить, що при $2w\tau_1\ll 1$ спін-ґраткова релаксація домінує і радіочастотне поле не може змінити рівноважної заселеності. Ймовірність вимушених переходів w пропорційна до квадрату величини $\vec{b}(t)$ радіочастотного поля (7.3), тому збільшуючи його, можна досягти помітних змін заселеностей.

Детектування релаксації магнітного моменту. Нехай коротким імпульсом магнітний момент M_0 повернуто так, що в початковий момент часу його координати $M_x(0)=M_0\sin\theta$, $M_y(0)=0$, $M_z(0)=M_0\cos\theta$, тоді в наступні моменти часу магнітний момент еволюціонує в зовнішньому полі під впливом спін-спінових та спін-ґраткових релаксаційних процесів:

$$M_x(t){=}M_0\sin\theta\cos\omega_0te^{-t/\tau_2},\ M_y(t){=}M_0\sin\theta\sin\omega_0te^{-t/\tau_2},$$
$$M_z=M_0\cos\theta e^{-t/\tau_1}.$$

У соленоїдах, що генерують радіочастотні імпульсу вздовж осей x та y, детектується сигнал $V(t)$, який є пропорційним до:

$$M^+(t)=M_x(t)+iM_y(t)=M_0\sin\theta e^{i\omega_0t-t/\tau_2}.$$

Фур'є-образ цього сигналу дає змогу виділити частоти ω_0 та оцінити час спін-спінової релаксації τ_2:

$$V(\omega) = \int_0^\infty V(t)e^{-i\omega t}dt \sim M_0 \sin\theta \int_0^\infty e^{i(\omega_0-\omega)t-t/\tau_2}dt$$
$$= M_0 \sin\theta \left(\frac{1/\tau_2}{1/\tau_2^2 + (\omega_0-\omega)^2} + i\frac{\omega_0-\omega}{1/\tau_2^2+(\omega_0-\omega)^2} \right). \qquad (7.6)$$

Перший доданок у (7.6) описує профіль лінії поглинання, а другий — дисперсію. Лоренців профіль лінії поглинання є наслідком надзвичайної простоти моделі процесу поглинання і грубих наближень в його отриманні. З (7.6) бачимо, що максимальний сигнал спостерігається при $\theta = \pi/2$, тобто, після повороту магнітного моменту в площину $x-y$.

7.2 Ініціалізація

Не існує методів для створення повної заселеності якогось із рівнів ($N_- = N$ чи $N_+ = N$), тобто переведення всіх спінів у стан $|0\ldots0\rangle_L$ чи $|1\ldots1\rangle_L$ при кімнатних температурах. Це пов'язано з великими термічними флуктуаціями в порівнянні із енергіями взаємодій спінів із полем, так для поля $B_0 = 11.7$ Тл ларморова частота спіну протона дорівнює $\nu_H = \omega_H/(2\pi) \approx 5 \cdot 10^8$ Hz і відношення:

$$\frac{\hbar\omega_H}{2k_BT} \approx 4 \cdot 10^{-5} \qquad (7.7)$$

є дуже мале. Воно ще менше для ядерних спінів інших елементів, а для відносних частот Ω_{ij} ще на кілька порядків менше. Оскільки молекули в розчині перебувають на великих віддалях і не взаємодіють між собою, то вклад від різних молекул у результуючий сигнал визначають як звичайне середнє, тобто, стан усіх молекул описують матрицею густини однієї молекули в рівноважному стані:

$$\boldsymbol{\rho} = \frac{e^{-\beta\mathcal{H}}}{Z}$$

де $\mathcal{H}$ — гамільтоніан, визначений у (7.1), Z — статистична сума. З огляду на (7.7) у гамільтоніані досить зберегти тільки перший доданок, тоді, позначивши $\alpha_j \equiv \hbar\omega_j/2kT$, матрицю густини можна записати:

$$\begin{aligned}\boldsymbol{\rho} &\approx (\mathbf{I} - \beta\mathcal{H})2^{-L} = \\ = (\mathbf{I} &+ \alpha_1\boldsymbol{\sigma}_1^z \otimes \mathbf{I}_2 \otimes \cdots \otimes \mathbf{I}_L + \alpha_2\mathbf{I}_1 \otimes \boldsymbol{\sigma}_2^z \otimes \mathbf{I}_3 \otimes \cdots \otimes \mathbf{I}_L + \ldots \\ &+ \alpha_L\mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \cdots \otimes \mathbf{I}_{L-1} \otimes \boldsymbol{\sigma}_L^z)\, 2^{-L} \end{aligned} \quad (7.8)$$

оскільки в цьому наближенні $Z = \mathrm{Sp}e^{-\beta\mathcal{H}} \approx 2^L$. Матриця (7.8) є діагональна з елементами близькими до одиниці. Здійснивши $2^L - 1$ циклічних перестановок $\mathbf{P}_j$ всіх діагональних елементів, крім першого, матрицю густини можна виразити як суму $2^L - 1$ доданків:

$$\boldsymbol{\rho}_{eff} = \frac{1}{2^L - 1}\left(\boldsymbol{\rho} + \mathbf{P}_1\boldsymbol{\rho}\mathbf{P}_1^+ + \mathbf{P}_2\boldsymbol{\rho}\mathbf{P}_2^+ + \ldots + \mathbf{P}_{2^L-2}\boldsymbol{\rho}\mathbf{P}_{2^L-2}^+\right). \quad (7.9)$$

Враховуючи, що сума всіх діагональних елементів дорівнює одиниці, цю матрицю можна зобразити:

$$\boldsymbol{\rho}_{eff} = \frac{2^L - 1 - a}{2^L(2^L - 1)}\mathbf{I} + \frac{a}{(2^L - 1)}|0\ldots0\rangle_L\langle 0\ldots0|, \quad (7.10)$$

де перший елемент позначено $a = \sum_{j=1}^{L}\alpha_j$. Стан, який описує матриця (7.10), називають *ефективно чистим* чи *псевдочистим*. У такому стані на всі зовнішні (унітарні) дії система реагує тільки завдяки другому доданку, який описує чистий стан. Такий спосіб приготування початкового стану називають *методом часового засереднення*. Насправді експеримент (обчислення) відбувається $2^L - 1$ разів, кожен раз після виконання оператора перестановки $\mathbf{P}_j$, який реалізується як послідовності операторів **SWAP** і **CNOT**, що діють на відповідні квабіти. Оператори **SWAP** і **CNOT** формуються радіочастотними імпульсами. Після вимірювання результати арифметично усереднюються, що еквівалентно усередненню з матрицею густини (7.9), (7.10). Таке часове засереднення є складною задачею, оскільки потребує $2^L - 1$ обчислень,

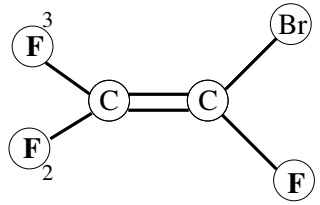


Рис. 7.2: Хімічна структура молекули, використаної в [29] для ілюстрації методу логічної мітки

окрім того, кожен оператор $\mathbf{P}_j$ формується $\sim m^L$ $(m > 2)$ елементарними операціями. Використовуючи те, що діагональні елементи утворені з L величин α_j, для занулення діагональних елементів замість циклічних перестановок можна використати простіші (набагато менш затратні) операції чим суттєво скоротити також кількість експериментів. Докладніше з методом часового засереднення можна познайомитися у працях [11, 15, 29].

Інший метод ініціалізації, який називають *методом логічної мітки*, застосовують до гомоядерних систем. Вперше він був експериментально реалізований L.M.K.Vandersypen та ін. [29] на молекулі, зображеній на рис. 7.2. Квантовий регістр формується ядерними спінами атомів фтору ^{19}F, інші ядра мають нульові спінові моменти. В полі $B_0 = 11.7$ Тл ядерні спіни мають частоти Лармора $\omega_0 \approx 470$ MHz, а різниці частот дорівнюють $\nu_1 - \nu_2 \approx 13.2$ kHz, $\nu_3 - \nu_1 \approx 9.5$ kHz, $\nu_3 - \nu_2 \approx 24.7$ kHz. Відносні ж частоти мають значення $\Omega_{12} = -122.1$ Hz, $\Omega_{13} = 75.0$ Hz, $\Omega_{23} = 53.8$ Hz. Тоді, враховуючи тільки частоти ω_0, матрицю, що описує вклад гамільтоніана в матрицю густини, можна виразити у діагональному вигляді (верхня матриця в (7.11)):

$$\begin{aligned} &\mathrm{diag}[3, 1, 1, -1, 1, -1, -1, -3], \\ &\mathrm{diag}[3, 1, 1, 1, -1, -1, -1, -3]. \end{aligned} \tag{7.11}$$

Після дії операторів $\mathbf{CNOT}_{21}$ і $\mathbf{CNOT}_{31}$ вона переходить у нову діагональну матрицю (нижня матриця в (7.11)), за допомогою якої матрицю густини (позначивши $\alpha \equiv \beta\hbar\omega_0/2kT$) можна запи-

сати так:

$$\boldsymbol{\rho}_{eff} = \frac{1}{2^3}\,[\mathbf{I}+\alpha|0\rangle_1\langle 0|\otimes(\mathbf{I}_2\otimes\mathbf{I}_3+2|00\rangle_{23}\langle 00|) \\ -\alpha|1\rangle_1\langle 1|\otimes(\mathbf{I}_2\otimes\mathbf{I}_3+2|11\rangle_{23}\langle 11|)]\,.$$

З цього виразу бачимо, що стани першого спіну $|0\rangle_1$ і $|1\rangle_1$ фіксують псевдочисті стани другого і третього спінів $|00\rangle_{23}$ і $|11\rangle_{23}$ відповідно. Отже, стани другого і третього спінів формують два квабіти, які можна використати як квантовий регістр, на якому виконувати квантові обчислення, використовуючи квантові вентилі, описані раніше. Для побудови квантових регістрів більших розмірів можна використовувати гомоядерні молекули з більшою кількістю спінів або великі гетероядерні молекули з гомоядерними фрагментами, кожен з яких відповідно відмітивши за процедурою описаною вище. Докладніше про цей метод див. [11, 15, 29].

Ще один метод, який використовували для приведення системи ядерних спінів до початкового стану, називають *методом просторового усереднення*. Його суть полягає в тому, що за допомогою радіочастотних імпульсів градієнта магнітного поля зразок із розчином молекул переводять в неоднорідний стан, який еквівалентний ансамблю псевдочистого стану. Сигнал після імпульсу вимірювання в такому неоднорідному стані еквівалентний сигналу усередненому з матрицею густини псевдочистого стану. Тобто, різні області зразка подібні до різних зразків методу часового засереднення. Радіочастотні імпульси градієнта магнітного поля дають змогу проводити рефазування кожного спіну, і цим гасити шкідливі міжспінові кореляції. Детальніше див. [15].

7.3 Зчитування результату

Якщо після виконання обчислень квантовий регістр містить запис одного числа, тобто, кожен квабіт перебуває або в стані $|0\rangle$ або в стані $|1\rangle$, то спостерігати безпосередньо такий стан неможливо, бо в приймальних соленоїдах спектрометра не індукується жодний сигнал. Тому для вимірювання стану котрогось із квабітів (напр. квабіту l) на нього діють радіочастотним імпульсом (резонансної частоти ω_l), який реалізує квантовий вентиль $\mathbf{Y}\equiv\mathbf{Y}(\pi/2)$,

$\mathbf{Y}^{\dagger}\equiv\mathbf{Y}(-\pi/2)$, тобто, повертають спін із напряму уздовж осі z у напрям вздовж осі x, тобто, в площину $x-y$. Після закінчення дії квантового вентиля спін виконує вільний рух, генерований гамільтоніаном (7.1), що індукує в приймальних соленоїдах сигнал:

$$V(t) = -V_0 \mathrm{Sp}\left(e^{-i\mathcal{H}t/\hbar}\mathbf{Y}_l\boldsymbol{\rho}(0)\mathbf{Y}_l^{\dagger}e^{i\mathcal{H}t/\hbar}\boldsymbol{\sigma}_l^{+}\right), \tag{7.12}$$

де $\boldsymbol{\rho}(0)$ — оператор густини квантового регістра після виконання обчислень, $\boldsymbol{\sigma}_l^{+} \equiv \boldsymbol{\sigma}_l^{x} + i\boldsymbol{\sigma}_l^{y}$, а V_0 — константа, що характеризує конструкцію приймальних соленоїдів спектрометра. Такий спосіб вимірювання називають *методом вільного загасання індукції*. Використовуючи інваріантність сліду оператора щодо циклічної перестановки його співмножників, вираз (7.12) запишемо як:

$$V(t)= -V_0 \mathrm{Sp}\left(\boldsymbol{\rho}(0)\mathbf{Y}_l^{\dagger}\boldsymbol{\sigma}_l^{+}(t)\mathbf{Y}_l\right), \quad \boldsymbol{\sigma}_l^{+}(t)\equiv e^{i\mathcal{H}t/\hbar}\boldsymbol{\sigma}_l^{+}e^{-i\mathcal{H}t/\hbar}. \tag{7.13}$$

Для прикладу обчислимо сигнали для різних кінцевих станів двоквабітового регістра. Нагадаємо його гамільтоніан:

$$\mathcal{H} = -\frac{\hbar\omega_A}{2}\boldsymbol{\sigma}^z\otimes\mathbf{I} - \frac{\hbar\omega_B}{2}\mathbf{I}\otimes\boldsymbol{\sigma}^z + \frac{\hbar\Omega}{2}\boldsymbol{\sigma}^z\otimes\boldsymbol{\sigma}^z, \tag{7.14}$$

тут ми знехтували дипольною магнітною і спін-ґратковою взаємодіями, які призводять до декогеренції, оскільки вважаємо, що обчислення відбулися за час менший від часу когерентності системи. Далі з'ясуємо, як врахувати вплив поперечної релаксації на ширину спектральної лінії сигналу. Розглянемо вимірювання стану спіну A, для якого з виразу (7.13) можна отримати:

$$\boldsymbol{\sigma}_A^{+}(t) = e^{-i\omega_A t}\boldsymbol{\sigma}^{+}\otimes\mathbf{Z}(2\Omega t),$$

$$\mathbf{Y}_A^{\dagger}\boldsymbol{\sigma}_A^{+}(t)\mathbf{Y}_A = e^{-i\omega_A t}\begin{bmatrix} -e^{i\Omega t} & 0 & e^{i\Omega t} & 0 \\ 0 & -e^{-i\Omega t} & 0 & e^{-i\Omega t} \\ -e^{i\Omega t} & 0 & e^{i\Omega t} & 0 \\ 0 & -e^{-i\Omega t} & 0 & e^{-i\Omega t} \end{bmatrix}. \tag{7.15}$$

Тут введено позначення $\boldsymbol{\sigma}_A^{+}\equiv\boldsymbol{\sigma}^{+}\otimes\mathbf{I}$, $\mathbf{Y}_A\equiv\mathbf{Y}\otimes\mathbf{I}$, для спіна B відповідно буде $\boldsymbol{\sigma}_B^{+}\equiv\mathbf{I}\otimes\boldsymbol{\sigma}^{+}$, $\mathbf{Y}_B\equiv\mathbf{I}\otimes\mathbf{Y}$.

Скалярна частина матриці густини дає нульовий сигнал, а відмінний від нуля вклад дає тільки девіація матриці густини, тобто,

частина, яка описує псевдочистий стан. Спершу знайдемо відгук у випадку матриці густини рівноважного стану:

$$\Delta\boldsymbol{\rho} = \frac{1}{4}\begin{bmatrix} \alpha_A+\alpha_B & 0 & 0 & 0 \\ 0 & \alpha_A-\alpha_B & 0 & 0 \\ 0 & 0 & -\alpha_A+\alpha_B & 0 \\ 0 & 0 & 0 & -\alpha_A-\alpha_B \end{bmatrix}. \quad (7.16)$$

Підставивши (7.16) і (7.15) у вираз (7.13), отримаємо:

$$V(t) = V_0\alpha_A e^{-i\omega_A t}\cos\Omega t = V_0\alpha_A e^{-i\omega_A t}\frac{1}{2}\left(e^{i\Omega t}+e^{-i\Omega t}\right).$$

Спектр цього сигналу знайдемо як фур'є-образ з урахуванням часу τ_2 спін-спінової (поперечної) релаксації:

$$V(\omega) = \int_0^\infty V(t)e^{-i\omega t - t/\tau_2}dt$$

$$= \frac{V_0\alpha_A}{2}\left(\frac{1/\tau_2 + i(\omega+\omega_A-\Omega)}{1/\tau_2^2+(\omega+\omega_A-\Omega)^2} + \frac{1/\tau_2 + i(\omega+\omega_A+\Omega)}{1/\tau_2^2+(\omega+\omega_A+\Omega)^2}\right). \quad (7.17)$$

Якщо замість $\omega+\omega_A$ ввести нову змінну ω, то можна побачити, що дійсна частина виразу (7.17) описує два лоренцові піки на частотах $\omega=-\Omega$ і $\omega=\Omega$, які при $\tau_2\to 0$ переходять у дельта-піки $V(\omega) = V_0\alpha_A[\delta(\omega+\Omega)+\delta(\omega-\Omega)]/2$. Якщо зберегти $\omega+\omega_A$, то піки будуть розташовані симетрично відносно ω_A.

Отримаємо вирази для сигналу від конкретних станів. Нагадаємо, що девіація матриці густини в цьому випадку має вигляд $\Delta\boldsymbol{\rho}(0) = \varepsilon|\psi\rangle\langle\psi|/4$, де $|\psi\rangle$ — вектор стану квантового регістра.

Нижче наведено вирази функції $V(t)$ для різних станів квантового регістра

$$|00\rangle \Longrightarrow +v(t)e^{i\Omega t}, \quad |01\rangle \Longrightarrow +v(t)e^{-i\Omega t},$$
$$|10\rangle \Longrightarrow -v(t)e^{i\Omega t}, \quad |11\rangle \Longrightarrow -v(t)e^{-i\Omega t},$$

тут використано позначення $v(t)\equiv V_0\varepsilon e^{-i\omega_A t}/4$. Стани можна ідентифікувати за знаком піка ($|x\rangle_A$) чи положенням піка ($|x\rangle_B$). Вимірюючи тільки стани першого спіну, можна знайти також і стани другого спіну (насправді знаходимо єдиний стан системи двох

спінів). Це зумовлено заплутуванням (скорельованістю) станів в процесі еволюції, породженої взаємодією.

Суперпозиційні стани спіну A вже не так легко ідентифікувати

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle \Rightarrow 0, \quad \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|0\rangle \Rightarrow 0,$$
$$\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)|0\rangle \Rightarrow -iv(t)e^{i\Omega t}, \quad \frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)|0\rangle \Rightarrow iv(t)e^{i\Omega t}. \quad (7.18)$$

Чому стани $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ і $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ дають нульовий сигнал? Ці вектори описують стани спіну A, скерованого уздовж осі x, імпульс $\mathbf{Y}$ повернув їх навколо осі y на $\pi/2$ і скерував уздовж осі z, а такі стани не індукують сигнал в детекторі спектрометра. Вектори $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ і $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ описують стани спіну, скерованого уздовж осі y і їх імпульс $\mathbf{Y}$ не зачепив, тому вони дали сигнал:

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|1\rangle \Rightarrow 0, \quad \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|1\rangle \Rightarrow 0,$$
$$\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)|1\rangle \Rightarrow -iv(t)e^{-i\Omega t}, \quad \frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)|1\rangle \Rightarrow iv(t)e^{-i\Omega t}. \quad (7.19)$$

Вирази для сигналу (7.19) відрізняються від виразів (7.18) тільки частотою, на якій спостерігаються піки.

Вимірювання станів тільки спіну A вже недостатньо для визначення суперпозиційних станів спіну B, тому необхідно проводити вимірювання і над ним. Тобто, для обчислення очікуваного сигналу формулу (7.13) треба записати:

$$V(t) = -V_0 \mathrm{Sp}\left(\boldsymbol{\rho}(0)(\mathbf{Y}^\dagger \otimes \mathbf{Y}^\dagger)(\boldsymbol{\sigma}_A^+ + \boldsymbol{\sigma}_A^+)(t)(\mathbf{Y} \otimes \mathbf{Y})\right),$$

і замість $\boldsymbol{\sigma}_A^+(t)$ використовувати оператор

$$\left(\boldsymbol{\sigma}_A^+ + \boldsymbol{\sigma}_B^+\right)(t) = e^{i\mathcal{H}t/\hbar}\left(\boldsymbol{\sigma}^+ \otimes \boldsymbol{I} + \boldsymbol{I} \otimes \boldsymbol{\sigma}^+\right) e^{-i\mathcal{H}t/\hbar}.$$

Позначивши $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ вектори станів спіну, скерованого уздовж осі x, запишемо вирази для отриманих сигналів:

$$|x_A\rangle|x_B\rangle \Rightarrow [(-1)^{x_A}v_A(t)+(-1)^{x_B}v_B(t)]\cos\Omega t, \ |\pm\rangle|\pm\rangle \Rightarrow 0,$$
$$|x_A\rangle|\pm\rangle \Rightarrow (-1)^{x_A}v_A(t)\exp(\pm i\Omega t),$$
$$|\pm\rangle|x_B\rangle \Rightarrow (-1)^{x_B}v_B(t)\exp(\pm i\Omega t). \quad (7.20)$$

Позначивши аналогічно $|\pm\rangle \equiv (|0\rangle \pm i|1\rangle)/\sqrt{2}$, отримаємо сигнали для деяких станів:

$$\begin{aligned} |x_A\rangle|\pm\rangle &\Longrightarrow v_B(t)\cos(\Omega t) \pm (-1)^{1\oplus x_A} v_A(t)\sin(\Omega t), \\ |\pm\rangle|x_B\rangle &\Longrightarrow v_A(t)\cos(\Omega t) \pm (-1)^{1\oplus x_B} v_B(t)\sin(\Omega t). \end{aligned} \tag{7.21}$$

Означені виразом (7.12) вимірювання належать до описаних в першому розділі POVM–вимірювань, які дають змогу знайти стани системи, у яких вона перебувала до початку вимірювання.

7.4 Томографія квантового стану

Метод вільного загасання індукції дає змогу виконати *томографію квантового стану*, тобто, цілком відтворити матрицю густину. Спочатку розглянемо цей метод на прикладі одного спіну в постійному магнітному полі. Його гамільтоніан має вигляд:

$$\mathcal{H} = -\frac{\hbar\omega_0}{2}\boldsymbol{\sigma}^z.$$

Найзагальніша матриця густини одного спіну визначається трьома дійсними параметрами:

$$\boldsymbol{\rho} = \frac{1}{2}\left(\mathbf{I} + n_x\boldsymbol{\sigma}^x + n_y\boldsymbol{\sigma}^y + n_z\boldsymbol{\sigma}^z\right) = \frac{1}{2}\begin{bmatrix} 1+n_z & n_x - in_y \\ n_x + in_y & 1-n_z \end{bmatrix}.$$

Легко переконатися, що вимірювання сигналу вільного загасання індукції

$$V(t) = V_0 \mathrm{Sp}\left(e^{-i\mathcal{H}t/\hbar}\mathbf{U}\boldsymbol{\rho}\mathbf{U}^+ e^{i\mathcal{H}t/\hbar}\boldsymbol{\sigma}_l^+\right) \tag{7.22}$$

після дії таких операторів, що формуються імпульсами:

$$\begin{aligned} \mathbf{X} \equiv \mathbf{X}\left(\frac{\pi}{2}\right) &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \ \mathbf{X}^+ \equiv \mathbf{X}\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}, \\ \mathbf{Y} \equiv \mathbf{Y}\left(\frac{\pi}{2}\right) &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \ \mathbf{Y}^+ \equiv \mathbf{Y}\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \end{aligned} \tag{7.23}$$

призведе до результатів:

$$\begin{aligned}
\mathbf{U}=\mathbf{I} \quad &\Longrightarrow \quad V(t)=v(t)(n_x+in_y),\\
\mathbf{U}=\mathbf{X} \quad &\Longrightarrow \quad V(t)=v(t)(in_z+n_x),\\
\mathbf{U}=\mathbf{X}^+ \quad &\Longrightarrow \quad V(t)=v(t)(-in_z+n_x),\\
\mathbf{U}=\mathbf{Y} \quad &\Longrightarrow \quad V(t)=v(t)(-n_z+in_y),\\
\mathbf{U}=\mathbf{Y}^+ \quad &\Longrightarrow \quad V(t)=v(t)(n_z+in_y),\\
\mathbf{U}=\mathbf{XY} \quad &\Longrightarrow \quad V(t)=v(t)(-n_z+in_x).
\end{aligned}$$

Тут позначено $v(t)\equiv V_0e^{-i\omega_0t}$. Після перетворення Фур'є числові результати дають змогу знайти три невідомі параметри, що цілком визначають матрицю густини одного спіну.

Для матриці густини змішаного стану одного спіну

$$\boldsymbol{\rho}=\begin{bmatrix} a & 0\\ 0 & 1-a\end{bmatrix}$$

в усіх вимірюваннях отримаємо сигнал $V(t)=\gamma v(t)(a-1/2)$, де γ дорівнює ±1 чи $\pm i$.

Найзагальніша матриця густини двох спінів має 16 елементів, але, внаслідок ермітовості і рівності одиниці сліду, вона залежить від 9 дійсних параметрів. Для відшукання цих параметрів, як і у випадку одного спіну, треба збудувати набір операторів, які можна реалізувати радіочастотними імпульсами, і виконати вимірювання, визначені формулою (7.22), яка в даному випадку набуває вигляду:

$$V(t)=-V_0\mathrm{Sp}\left(e^{-i\mathcal{H}t/\hbar}\mathbf{U}\boldsymbol{\rho}\mathbf{U}^+e^{i\mathcal{H}t/\hbar}\left(\boldsymbol{\sigma}_A^+ +\boldsymbol{\sigma}_B^+\right)\right),$$

де гамільтоніан, що описує еволюцію, заданий виразом (7.14), а оператори $\boldsymbol{\sigma}_A^+$ і $\boldsymbol{\sigma}_B^+$ у двоспіновому просторі зображаються так:

$$\boldsymbol{\sigma}_A^+\equiv\boldsymbol{\sigma}^+\otimes\mathbf{I},\qquad \boldsymbol{\sigma}_B^+\equiv\mathbf{I}\otimes\boldsymbol{\sigma}^+.$$

Виконання таких вимірювань дає змогу отримати систему незалежних лінійних рівнянь для параметрів, що входять у вираз для матриці густини двоспінової системи, і у такий спосіб цілком відтворити її. Поширення методу томографії квантового стану на

системи більшої вимірності призводить до експонентного зростання кількості вимірювань і розмірності систем лінійних рівнянь, тому не може бути ефективним, але є принципово можливим.

Нарешті відзначимо той факт, що описані вимірювання не належать до проективних вимірювань фон Ноймана. В проективних експериментах система переходить у власний стан оператора, який ми вимірювали і власне значення якого отримали в результаті експерименту. Тут же ми дізнаємося стан системи, в якому вона перебувала до експерименту, а кінцевий стан є деяким рівноважним станом, що встановлюється в процесі вільної еволюції (релаксації) після відповідного вимірювального радіочастотного імпульсу, тобто, тут ми маємо справу з POVM–вимірюваннями.

7.5 Переваги і недоліки процесора на основі ЯМР

Проект квантового процесора на рідинному ЯМР розвивався роботами багатьох науковців (див., напр. [15, 29, 30]), в яких було експериментально доведено можливість практичної реалізації ідей квантових обчислень. На невеликих молекулах було виконано ініціалізацію методами часового та просторового усереднення, а також методом логічної мітки. Успішно реалізовано алгоритми Дойча, Гровера і Шора. Виконано квантову томографію одно- та двоспінових систем та впроваджено інші ідеї квантових обчислень. Разом з тим встановлено, що метод реалізації квантового процесора на рідинному ЯМР є безперспективним через експонентне 2^{-L} ослаблення сигналу вільного загасання індукції зі збільшенням числа квантових бітів L в молекулі. Окрім того, збільшення кількості квабітів в молекулі призводить до згущення спектральних ліній, що суттєво утруднює роздільну дію радіочастотних імпульсів на окремі спіни.

Цей розділ в значній мірі ґрунтується на матеріалі роботи [15].

Розділ 8

Квантовий процесор на іонах у пастці Пауля

Квантові біти в такому процесорі реалізуються на двох квазістабільних електронних рівнях позитивно заряджених іонів, поміщених у лінійну пастку Пауля і охолоджених до дуже низьких температур, коли відсутні відносні рухи іонів. Кожен квабіт пов'язаний з окремим іоном, положення якого в просторі відоме. Квантові вентилі формуються імпульсами лазерного випромінювання певної частоти, скерованими на конкретні квабіти, та коливними рухами іонів. Охолодження ланцюжка іонів проводять на основі методів, створених для нейтральних атомів (див., напр. праці [47, 48, 49, 50]).

8.1 Пастка Пауля. Формування іонного ланцюжка

На рисунках 8.1 і 8.2 подано схематичні зображення лінійної пастки Пауля і прикладених в ній напруг. На осі z пастки розташовують позитивно заряджені іони, на кільця подають позитивний заряд напруги U_0, який утримує іони від розбігання вздовж осі z під впливом кулонівського відштовхування. Віддаль між кільцями $\sim 10mm$, радіуси електродів $R' \approx R_0 \approx 1mm$.

З електростатики відомо, що неможливо створити статичний електричний потенціал, в якому заряджена частинка перебувала б у механічній рівновазі (теорема Ірншоу). У пастці Пауля ефективна рівновага формується поєднанням статичних і динамічних електричних полів.

В околі центру пастки (x=0, y=0, z=0) статичний ("зовнішній

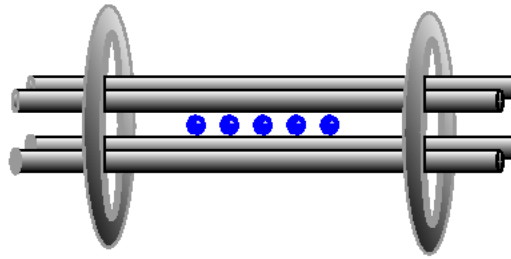


Рис. 8.1: Одна із схем лінійної пастки Пауля [35]

квадрупольний") потенціал, створений кільцями, можна записати:

$$\Phi_s = \frac{kU_0}{z_0^2}\left[z^2 - \frac{x^2+y^2}{2}\right] = \frac{M}{2Q}\Omega_z^2\left[z^2 - \frac{x^2+y^2}{2}\right],$$

де $k \approx 1$ — геометричний фактор, z_0 — віддаль від центру пастки до площини кільця, M — маса іона, Q — заряд іона, $\Omega_z^2 \equiv (2kQU_0)/(z_0^2 M)$ — частота коливань іона в напрямі z у статичному потенціалі Φ_s. Змінна напруга $V_0 \cos\Omega_T t + U_r$, прикладена до циліндричних електродів, створює у центрі пастки ("внутрішній квадрупольний") потенціал:

$$\Phi_r = \frac{1}{2}(V_0 \cos\Omega_T t + U_r)\frac{x^2-y^2}{R_0^2}.$$

Рівняння руху іона в сумарному потенціалі $\Phi{=}\Phi_s{+}\Phi_r$ мають такий вигляд

$$M\frac{d^2x}{dt^2} = -Q\frac{\partial\Phi}{\partial x}, \quad \Longrightarrow \quad \frac{d^2z}{dt^2} + \Omega_z^2 z = 0,$$

$$\frac{d^2x}{d\tau^2} + [a_x + 2d_x\cos(2\tau)]\,x{=}0, \quad \frac{d^2y}{d\tau^2} + [a_y + 2d_y\cos(2\tau)]\,y{=}0, \quad (8.1)$$

де позначено:

$$\tau \equiv \Omega_T t/2, \quad d_x = -d_y = \frac{2QV_0}{M\Omega_T^2 R_0^2},$$

$$a_x \equiv -\frac{4Q}{M\Omega_T^2}\left(\frac{kU_0}{z_0^2} - \frac{U_r}{R_0^2}\right), \; a_y \equiv -\frac{4Q}{M\Omega_T^2}\left(\frac{kU_0}{z_0^2} + \frac{U_r}{R_0^2}\right).$$

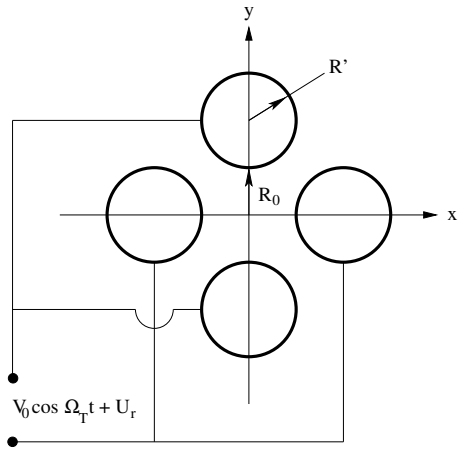


Рис. 8.2: Схема прикладання високочастотної напруги в пастці Пауля

Із рівнянь (8.1) видно, що вздовж осі z іон виконує гармонічний рух із частотою Ω_z. У напрямах x і y його рух описують рівняннями Матьє, які є рівняннями на власні функції та власні значення і мають досить багатий набір розв'язків у різних областях стійкості. Для пастки Пауля між параметрами рівнянь існують співвідношення $|a_{x(y)}| < d^2_{x(y)}/2 \ll 1$, тому можна отримати наближені розв'язки з точністю до $d^2_{x(y)}$:

$$x(t) = A_x \left[\cos\Omega_x t \left(1 + \frac{d_x}{4}\cos\Omega_T t + \frac{d_x^2}{32}\cos 2\Omega_T t + \ldots\right) - \frac{d_x}{4}\sin\Omega_x t \left(\sin\Omega_T t + \frac{d_x}{16}\sin 2\Omega_T t + \ldots\right)\right],$$

$$y(t) = A_y \left[\cos\Omega_y t \left(1 + \frac{d_y}{4}\cos\Omega_T t + \frac{d_y^2}{32}\cos 2\Omega_T t + \ldots\right) - \frac{d_y}{4}\sin\Omega_y t \left(\sin\Omega_T t + \frac{d_y}{16}\sin 2\Omega_T t + \ldots\right)\right],$$

$$\Omega_{x(y)} = \sqrt{a_{x(y)} + \frac{d^2_{x(y)}}{2}}\frac{\Omega_T}{2}. \qquad (8.2)$$

Оскільки $\Omega_{x(y)} \ll \Omega_T$, то з (8.2) випливає, що іон у площині $x-y$ виконує відносно повільні, близькі до гармонічних, коливання з частотами Ω_x, Ω_y, на які накладаються високочастотні Ω_T осциляції малої амплітуди. Відмінність у числових значення частот Ω_x, Ω_y зумовлена сталою напругою U_r. Амплітуди A_x, A_y поперечних коливань є значно меншими за амплітуди поздовжніх, тому поперечними коливаннями зазвичай нехтують при описі механічних рухів іонів у пастці Пауля.

Із врахуванням міжчастинкового кулонівського відштовхування потенціальна енергія іонів у пастці Пауля така [33]:

$$V = \frac{M\Omega_z^2}{2}\left[\sum_{i=1}^{L} z_i^2(t) + \sum_{i\neq j}^{L} \frac{\zeta^3}{|z_i(t) - z_j(t)|}\right], \qquad \zeta^3 \equiv \frac{Z^2e^2}{M\Omega_z^2}.$$

Координати точок рівноваги іонів u_i

$$z_i(t) = z_i^{(0)} + q_i(t), \qquad u_i \equiv z_i^{(0)}/\zeta, \quad i = 1, \ldots, L$$

можна знайти чисельно з умови:

$$\left[\frac{\partial V}{\partial z_i}\right]_{q=0} = 0, \Longrightarrow u_i - \sum_{j=1}^{i-1} \frac{1}{(u_i - u_j)^2} + \sum_{j=i+1}^{L} \frac{1}{(u_i - u_j)^2} = 0.$$

Вони залежать від віддалі z до центру пастки, в континуальному наближенні ця залежність така:

$$s(z) = s_0\left(1 - \frac{z^2}{\ell_0^2}\right)^{-1},$$

де ℓ_0 півдовжина іонного ланцюжка, s_0 — віддаль між іонами в центрі пастки, яка є мінімальною, у праці [15] для неї наведено такі оцінки:

$$s_0(L) \approx 2.018\zeta L^{-0.559}, \qquad s_0(L) \approx 2.29\zeta L^{-0.596}.$$

Ці віддалі між іонами складають величини порядку кількох μm, а амплітуди коливань іонів — порядку $10nm$. Такі віддалі між іонами дають вільний доступ лазерного променя до кожного іона і забезпечують відсутність перекриття електронних хвильових функцій сусідніх іонів, що унеможливлює обмінні взаємодії. Однак

для великих значень L віддаль між іонами може дуже зменшитися, що стане перешкодою для лазерного керування електронними станами іонів. Іонний кристал у пастці Пауля є стійким для невеликих L, зокрема, вдалося експериментально збудувати кристал з $L = 33$ іонів $^{199}Hg^{+}$ [15]. Встановлено, що для довгих ланцюжків $L = 10^3 \div 10^4$ необхідною умовою стійкості є таке співвідношення частот, щоб $\Omega_r/\Omega_z > 0.73L^{0.86}$ [15].

Функція Лагранжа коливних рухів іонів має вигляд [33]:

$$\mathcal{L} = \frac{M}{2}\sum_{i=1}^{L}\dot{q}_i^2 - \frac{M\Omega_z^2}{2}\sum_{i,j=1}^{L}A_{ij}q_iq_j,$$

де позначено

$$\left[\frac{\partial^2 V}{\partial z_i \partial z_j}\right]_{q=0} = M\Omega_z^2 A_{ij}, A_{ij} = \begin{cases} 1+2\sum_{l=1}^{L}|u_i-u_l|^{-3}, & i=j, \\ -2|u_i-u_j|^{-3}, & i\neq j. \end{cases}$$

Матриця $\mathbf{A}$ дійсна, симетрична, невід'ємна і її власні значення мають бути невід'ємні. Власні вектори визначаються рівнянням:

$$\mathbf{A}\mathbf{b}^{(k)} = \lambda_k \mathbf{b}^{(k)}$$

і задовольняють умови ортогональності та повноти:

$$\sum_{k=1}^{L} b_i^{(k)} b_j^{(k)} = \delta_{ij}, \qquad \sum_{j=1}^{L} b_j^{(k_1)} b_j^{(k_2)} = \delta_{k_1 k_2}.$$

Двом найнижчим власним значенням відповідають вектори [33]

$$\lambda_1 = 1,\ \mathbf{b}^{(1)} = \{1,1,\ldots,1\}/\sqrt{L},$$
$$\lambda_2 = 3,\ \mathbf{b}^{(2)} = \{u_1,u_2,\ldots,u_L\}/\left(\Sigma_{i=1}^{L}u_i^2\right)^{1/2}.$$

Очевидно, що всі компоненти власних векторів $k \neq 1$ задовольняють умову $\sum_{i=1}^{L} b_i^{(k)} = 0$.

Введемо нормальні координати (моди)

$$Q_k(t) = \sum_{i=1}^{L} b_i^{(k)} q_i(t).$$

Моду Q_1 називають модою центра мас, а моду Q_2 — дихаючою модою (breathing). Лагранжіан коливних рухів іонів можна виразити через нормальні моди

$$\mathcal{L} = \frac{M}{2}\sum_{k=1}^{L}\left[\dot{Q}_k^2 - \Omega_k^2 Q_k^2\right], \qquad \Omega_k^2 \equiv \lambda_k \Omega_z^2.$$

З нього збудуємо гамільтоніан у термінах канонічно спряжених нормальних координат Q_k та імпульсів $P_k = M\dot{Q}_k$:

$$\mathcal{H} = \frac{1}{2M}\sum_{k=1}^{L} P_k^2 + \frac{M}{2}\sum_{k=1}^{L}\Omega_k^2 Q_k^2.$$

Замінивши в ньому канонічні змінні операторами за правилами

$$Q_k \to \mathbf{Q}_k = i\sqrt{\frac{\hbar}{2M\Omega_k}}\left(\mathbf{a}_k - \mathbf{a}_k^+\right),\ P_k \to \mathbf{P}_k = \sqrt{\frac{M\hbar\Omega_k}{2}}\left(\mathbf{a}_k + \mathbf{a}_k^+\right),$$

з такими комутаційними співвідношеннями $[\mathbf{Q}_{k_1}, \mathbf{P}_{k_2}] = i\hbar\delta_{k_1 k_2}$ та $\left[\mathbf{a}_{k_1}, \mathbf{a}_{k_2}^+\right] = \delta_{k_1 k_2}$, отримуємо квантово-механічний гамільтоніан руху іонів у пастці Пауля:

$$\boldsymbol{\mathcal{H}} = \sum_{k=1}^{L}\hbar\Omega_k\left(\mathbf{a}_k^+\mathbf{a}_k + 1/2\right),$$

де $\mathbf{a}_k^+$ ($\mathbf{a}_k$) — оператори народження (знищення) фонона в стані k. Як і треба було очікувати, це добре відомий гамільтоніан гармонічного осцилятора. В картині Гайзенберга оператори зміщень іонів у нових змінних так залежать від часу:

$$\mathbf{q}_j(t) = e^{i\boldsymbol{\mathcal{H}}t/\hbar}\mathbf{q}_j e^{-i\boldsymbol{\mathcal{H}}t/\hbar} = \sum_{k=1}^{L} b_j^{(k)}\mathbf{Q}_k(t)$$

$$= i\sqrt{\frac{\hbar}{2M}}\sum_{k=1}^{L}\frac{b_j^{(k)}}{\sqrt{\Omega_k}}\left(\mathbf{a}_k e^{-i\Omega_k t} - \mathbf{a}_k^+ e^{i\Omega_k t}\right).$$

Зокрема для моди центра мас останній вираз спрощується:

$$\mathbf{q}_j(t) = i\sqrt{\frac{\hbar}{2ML\Omega_z}}\left(\mathbf{a}e^{-i\Omega_z t} - \mathbf{a}^+ e^{i\Omega_z t}\right), \tag{8.3}$$

де позначено $\mathbf{a}^+ \equiv \mathbf{a}_1^+$, $\mathbf{a} \equiv \mathbf{a}_1$, а $\Omega_1 = \Omega_z$. Він потрібний для опису взаємодії лазерного променя з коливними модами при побудові двоквабітових квантових вентилів.

8.2 Квантові біти. Квантові вентилі

Формування квантових бітів і КЛЕ розглянемо на прикладі іона кальцію $^{40}Ca^+$, який використовували в експериментах з цією метою [35]. За квантовий біт вибирали стани $4^2S_{1/2} \leftrightarrow |0\rangle$ (стаціонарний стан) та $3^2D_{5/2} \leftrightarrow |1\rangle$, інші рівні, показані на рис. 8.3, використовували як допоміжні. Для оперування зі станами цього іона застосовували лазери з довжинами хвиль $729\,nm$ — для переходів $S_{1/2} \leftrightarrow D_{5/2}$, $397\ nm$ — для переходів $S_{1/2} \leftrightarrow P_{1/2}$ і $866\ nm$ — для переходів $P_{1/2} \leftrightarrow D_{3/2}$. Перехід $S_{1/2} \leftrightarrow D_{5/2}$ має квадрупольний характер, тому стан $3^2D_{5/2}$ є досить довговічним $\sim 1.14\ sec$ (квазістаціонарним).

Перед тим, як розглядати керування станами певного іона коротко ознайомимося із описом переходів електрона між двома рівнями під дією лазерного променя. Для цього досить обмежитися наближенням, у якому рух іонів та електронів описується квантово-механічно, а електромагнітне випромінювання лазерів — класично. Тоді еволюція стану електрона в іоні визначається рівнянням Шредінгера:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \left(\mathcal{H}^{(0)} + \mathcal{H}^{(1)}(t)\right)|\psi(t)\rangle, \tag{8.4}$$

де $\mathcal{H}^{(0)}$ — гамільтоніан електрона в іоні без взаємодії із полем лазера, $\mathcal{H}^{(1)}(t)$ — доданок, що задає взаємодію електрона із залежним від часу електромагнітним полем. Будемо вважати цю взаємодію слабкою настільки, що вона не руйнує станів електрона, визначених гамільтоніаном $\mathcal{H}^{(0)}$, а тільки призводить до переходів між ними. Це дає змогу розкласти вектор збуреного стану за векторами незбуреного:

$$|\psi(t)\rangle = \sum_n a_n(t)|\psi_n^{(0)}(t)\rangle, \quad i\hbar\frac{d}{dt}|\psi_n^{(0)}(t)\rangle = \mathcal{H}^{(0)}|\psi_n^{(0)}(t)\rangle,$$

$$|\psi_n^{(0)}(t)\rangle = e^{-iE_nt/\hbar}|\varphi_n\rangle$$

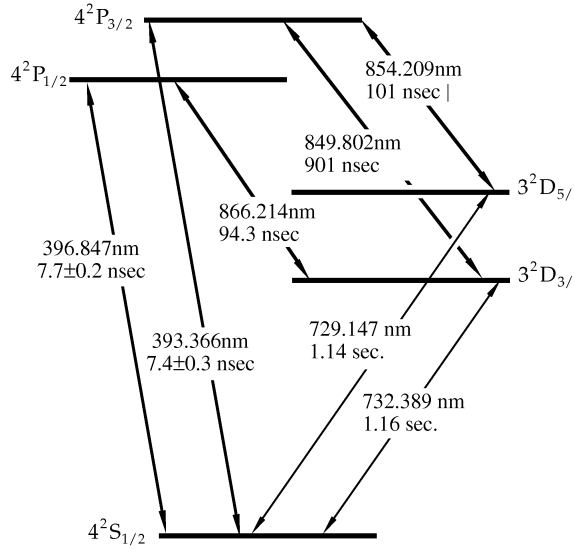


Рис. 8.3: Схема електронних рівнів, які використовують для формування квабіта на іоні $^{40}Ca^+$ (взято з [33])

і отримати рівняння (8.4) у вигляді:

$$i\hbar\frac{d}{dt}a_m(t)=\sum_n \mathcal{H}^{(1)}_{mn}(t)a_n(t), \qquad \mathcal{H}^{(1)}_{mn}(t)\equiv\langle\psi^{(0)}_m(t)|\boldsymbol{\mathcal{H}}^{(1)}(t)|\psi^{(0)}_n(t)\rangle.$$

Для переходів між двома рівнями, за умови $\mathcal{H}^{(1)}_{11}(t)=\mathcal{H}^{(1)}_{22}(t)=0$, це рівняння має таку матричну форму:

$$i\hbar\frac{d}{dt}\begin{bmatrix}a_1(t)\\a_2(t)\end{bmatrix}=\begin{bmatrix}0 & \mathcal{H}^{(1)}_{12}(t)\\ \mathcal{H}^{(1)}_{21}(t) & 0\end{bmatrix}\begin{bmatrix}a_1(t)\\a_2(t)\end{bmatrix}. \tag{8.5}$$

Нехай на іон, розташований у пастці Пауля, перпендикулярно до осі z падає промінь лазера, тоді оператор взаємодії електрона з полем такий:

$$\boldsymbol{\mathcal{H}}^{(1)}(t) = -\vec{\mathbf{p}}\cdot\vec{E}\cos\omega t,$$

де $\vec{\mathbf{p}}$ — оператор дипольного моменту, а $\vec{E}$ — напруженість електричного поля в точці знаходження електрона. Рівняння (8.5) в цьому випадку буде таким:

$$i\hbar\frac{d}{dt}\begin{bmatrix}a_1(t)\\a_2(t)\end{bmatrix}=\frac{1}{2}\begin{bmatrix}0 & F\\F^* & 0\end{bmatrix}\begin{bmatrix}a_1(t)\\a_2(t)\end{bmatrix},$$
$$F\equiv\left(e^{-i(\omega_0-\omega)t}+e^{-i(\omega_0+\omega)t}\right)(p_x-ip_y),$$

де $\omega_0\equiv(E_2-E_1)/\hbar$ — частота випромінювання при переході із стану 2 в стан 1, $p_x-ip_y\equiv-\langle\varphi_1|\vec{\mathbf{p}}\cdot\vec{E}|\varphi_2\rangle$ — середнє значення дипольного моменту помноженого на напруженість електричного поля хвилі.

Якщо в момент часу $t=0$ електрон перебував у стані 1, тобто, $a_1(0)=1, a_2(0)=0$, то під дією короткого імпульсу тривалістю τ електрон перейде у стан:

$$a_1(t)=1,\quad a_2(t)=-i\frac{p_x+ip_y}{\hbar}\int_0^\tau e^{i\omega_0 t}\cos\omega t dt$$
$$=-\frac{p_x+ip_y}{2\hbar}\left[\frac{e^{i(\omega_0+\omega)\tau}-1}{\omega_0+\omega}+\frac{e^{i(\omega_0-\omega)\tau}-1}{\omega_0-\omega}\right].$$

Отже, головний вклад в амплітуду дає доданок з $\omega_0-\omega$, який набуває максимального значення, коли частота лазерного променя збігається з частотою переходу, а доданком з $\omega_0+\omega$ можна знехтувати. В цьому наближенні (*наближенні хвилі, що обертається*) з позначеннями $p_x-ip_y\equiv\langle p\rangle e^{i\phi}$, $\tilde{\omega}_0\equiv\langle p\rangle/\hbar$, $\delta\equiv\omega-\omega_0$ рівняння (8.5) можна записати у вигляді:

$$i\frac{d}{dt}|\chi\rangle=\frac{\tilde{\omega}_0}{2}\begin{bmatrix}0 & e^{i\delta t+i\phi}\\e^{-i\delta t-i\phi} & 0\end{bmatrix}|\chi\rangle. \tag{8.6}$$

Унітарним перетворенням $|\chi\rangle=\mathbf{V}_R(t)|\chi_r\rangle=e^{i\delta t\boldsymbol{\sigma}^z/2}|\chi_r\rangle$ рівняння (8.6) зведемо до форми:

$$i\frac{d}{dt}|\chi_r\rangle=\left(\frac{\delta}{2}\boldsymbol{\sigma}^z+\frac{\tilde{\omega}_0}{2}\boldsymbol{\sigma}^\phi\right)|\chi_r\rangle,\qquad\boldsymbol{\sigma}^\phi\equiv\begin{bmatrix}0 & e^{i\phi}\\e^{-i\phi} & 0\end{bmatrix}$$

звідки легко отримаємо оператор еволюції:

$$\mathbf{V}_r(t)=e^{-i(\delta\boldsymbol{\sigma}^z+\tilde{\omega}_0\boldsymbol{\sigma}^\phi)t/2}=e^{-i\Omega t\vec{n}\vec{\boldsymbol{\sigma}}/2}=\mathbf{I}\cos\frac{\Omega t}{2}-i\vec{n}\vec{\boldsymbol{\sigma}}\sin\frac{\Omega t}{2},$$

де введено позначення:

$$\Omega \equiv \sqrt{\delta^2 + \tilde{\omega}_0^2}, \qquad \vec{n}\vec{\boldsymbol{\sigma}} \equiv \left(\delta \boldsymbol{\sigma}^z + \tilde{\omega}_0 \boldsymbol{\sigma}^\phi\right)/\Omega.$$

Еволюцію вектора стану $|\chi(t)\rangle = \mathbf{V}(t)|\chi(0)\rangle$ описує такий унітарний оператор:

$$\mathbf{V}(t) = \mathbf{V}_R(t)\mathbf{V}_r(t) = e^{i\delta t \boldsymbol{\sigma}^z/2} e^{-i\Omega t \vec{n}\vec{\boldsymbol{\sigma}}/2},$$

у випадку резонансу $\delta = 0$ він спрощується до виразу:

$$\mathbf{V}(\varphi, \phi) = \begin{bmatrix} \cos\frac{\varphi}{2} & -ie^{i\phi}\sin\frac{\varphi}{2} \\ -ie^{-i\phi}\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix}, \tag{8.7}$$

де $\varphi \equiv \tilde{\omega}_0 t$. З цього виразу видно, що із періодом $2\pi/\tilde{\omega}_0$ електрон повертається у початковий стан (з точністю до знаку вектора стану), такі осциляції двостанової системи під дією гармонічної електромагнітної хвилі, як і у випадку ядерного магнітного резонансу, називаються осциляціями Рабі, а частота $\tilde{\omega}_0$ — частотою Рабі.

Оператор (8.7) при $\varphi = \pi$ і $\phi = 0$ з точністю до фазового множника формує квантовий вентиль **NOT**. Загалом цей оператор дає змогу реалізувати всі одноквабітові квантові вентилі (операції $\mathbf{V}$-типу [34]) на іоні за номером j дією лазерного імпульсу:

$$\mathbf{V}_j(\varphi, \pi) = \mathbf{X}_j(\varphi), \qquad \mathbf{V}_j(\varphi, \pi/2) = \mathbf{Y}_j(\varphi),$$
$$\mathbf{Z}(\varphi) = \mathbf{Y}(\pi/2)\mathbf{X}(\varphi)\mathbf{Y}(-\pi/2).$$

Для формування двоквабітових вентилів необхідно включити деяку взаємодію між квабітами. Її може забезпечити колективне збудження моди центра мас [34], коли всі іони переходять у коливний стан. Цього можна досягти, якщо скерувати промінь лазера не перпендикулярно до осі z, а так, щоби він мав складову хвильового вектора κ_z. Тоді при взаємодії іон, на який падає такий промінь, отримає вздовж осі z деякий механічний імпульс, що і призведе до збудження колективної моди. Гамільтоніан взаємодії променя з електроном матиме залежність від координати z:

$$\mathcal{H}^{(1)}(t) = -\vec{\mathbf{p}} \cdot \vec{E}\cos(\omega t + \kappa_z z_j(t)) =$$
$$-\vec{\mathbf{p}} \cdot \vec{E}\cos(\omega t + \kappa_z z_j^{(0)} + \kappa_z q_j(t)).$$

Тоді рівняння (8.5), з урахуванням тільки резонансних $\delta = \omega - \omega_0$, доданків набере вигляду:

$$i\hbar\frac{d}{dt}\begin{bmatrix} a_1(t) \\ a_2(t) \end{bmatrix} = \frac{\langle p\rangle}{2}\begin{bmatrix} 0 & e^{i(\delta t+\phi+\kappa_z z_j^{(0)}+\kappa_z q_j(t))} \\ e^{-i(\delta t+\phi+\kappa_z z_j^{(0)}+\kappa_z q_j(t))} & 0 \end{bmatrix}\begin{bmatrix} a_1(t) \\ a_2(t) \end{bmatrix}, \quad (8.8)$$

тут можна покласти $z_j^{(0)} = 0$, оскільки промінь діє на окремий іон, і цей доданок не вносить відносної фази між різними іонами. Оскільки зміщення $q_j(t)$ дуже малі, то експоненти у (8.8) можна розкласти за доданком $\kappa_z q_j(t)$ з точністю до лінійного члена. Після заміни зміщення на оператор зміщення (8.3) рівняння (8.8) перейде у таке:

$$\begin{aligned} i\frac{d}{dt}|x_j,\xi\rangle = \Big\{ & \frac{\tilde{\omega}_0}{2}\left(S_j^+ e^{i\delta t+i\phi} + S_j^- e^{-i\delta t-i\phi}\right) \\ & -\frac{\tilde{\omega}_0'}{2}\Big[S_j^+ e^{i\delta t+i\phi}\left(\mathbf{a}e^{-i\Omega_z t} - \mathbf{a}^+ e^{i\Omega_z t}\right) \\ & +S_j^- e^{-i\delta t-i\phi}\left(\mathbf{a}^+ e^{i\Omega_z t} - \mathbf{a}e^{-i\Omega_z t}\right)\Big]\Big\}|x_j,\xi\rangle, \end{aligned} \quad (8.9)$$

де позначено $\tilde{\omega}_0 \equiv \langle p\rangle/\hbar$, $\tilde{\omega}_0' \equiv \eta\tilde{\omega}_0/\sqrt{L}$, а $\eta \equiv \kappa_z\sqrt{\hbar/(2M\Omega_z)}$ — параметр Лемба-Діке для іонів у пастці Пауля і лазерних променів з довжинами хвиль $\lambda \approx 500\ nm$ складає величину близьку до $\eta \approx 0.1$ [15], тому $\tilde{\omega}_0' < \tilde{\omega}_0$. Оператори

$$S^+ \equiv |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad S^- \equiv |1\rangle\langle 0| = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

описують переходи між станами $|0\rangle$ і $|1\rangle$. Рівняння (8.9) описує еволюцію вектора стану $|x_j,\xi\rangle$ електрона на іоні j (змінна x_j) разом із коливною модою Q_1 (змінна ξ). Їхню взаємодію описує доданок у квадратних дужках із множником $\tilde{\omega}_0'$. Для збудження фонона необхідне виконання умови резонансу $\delta = \Omega_z$ чи $\delta = -\Omega_z$ (залежно від знаку δ), покладемо для визначеності $\delta = -\Omega_z$. У рівнянні (8.9) збережуться тільки доданки, де в експоненті $\delta + \Omega_z = 0$, а

інші доданки будуть давати дуже малі вклади:

$$i\frac{d}{dt}|x_j,\xi\rangle = \frac{\tilde{\omega}_0'}{2}\left[e^{+i\phi}S_j^+\mathbf{a}^+ + e^{-i\phi}S_j^-\mathbf{a}\right]|x_j,\xi\rangle. \tag{8.10}$$

Це рівняння описує переходи між станами $|0,1\rangle$ і $|1,0\rangle$, а тому розв'язок будемо шукати у такому вигляді:

$$|x,\xi\rangle = c(t)|0,1\rangle + d(t)|1,0\rangle.$$

Підставивши цей вираз у (8.10), отримаємо рівняння для коефіцієнтів:

$$i\frac{d}{dt}\begin{bmatrix}c\\d\end{bmatrix} = \frac{\tilde{\omega}_0'}{2}\begin{bmatrix}0 & e^{i\phi}\\ e^{-i\phi} & 0\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix},$$

яке легко розв'язати:

$$\begin{bmatrix}c(t)\\d(t)\end{bmatrix} = \begin{bmatrix}\cos\frac{\tilde{\omega}_0't}{2} & -ie^{i\phi}\sin\frac{\tilde{\omega}_0't}{2}\\ -ie^{-i\phi}\sin\frac{\tilde{\omega}_0't}{2} & \cos\frac{\tilde{\omega}_0't}{2}\end{bmatrix}\begin{bmatrix}c(0)\\d(0)\end{bmatrix}$$

і отримати унітарний оператор

$$\mathbf{U}(\theta,\phi) = \begin{bmatrix}\cos\frac{\theta}{2} & -ie^{i\phi}\sin\frac{\theta}{2}\\ -ie^{-i\phi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

з параметром $\theta \equiv \tilde{\omega}_0't$. У праці [34] такі операції називають операціями **U**-типу. Ввівши допоміжний рівень, можна реалізувати оператор $\mathbf{U}_j^{(aux)}(\theta,\phi)$, який діє на стани $|0_j,1\rangle$ і $|aux_j,0\rangle$, тобто він діє тільки на стан $|0_j,1\rangle$ квабіта. Оператор $\mathbf{CNOT}_{jl}$, де j — контролюючий квабіт, а l — контрольований, можна виконати такою послідовністю [15, 34]:

$$\mathbf{CNOT}_{jl}=\mathbf{V}_l\Big(\frac{\pi}{2},-\frac{\pi}{2}\Big)\mathbf{U}_j(\pi,\pi)\mathbf{U}_l^{(aux)}(2\pi,\phi)\mathbf{U}_j(\pi,\pi)\mathbf{V}_l\Big(\frac{\pi}{2},\frac{\pi}{2}\Big), \tag{8.11}$$

операторів

$$\mathbf{V}(\pi/2,\pi/2)=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix},\quad \mathbf{V}(\pi/2,-\pi/2)=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix},$$

$$\mathbf{U}(\pi,\pi) = \begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

Останній з них таким чином змінює стани квабіта j і коливної моди v: $\mathbf{U}(\pi,\pi)|0\rangle_j|1\rangle_v = i|1\rangle_j|0\rangle_v$ і $\mathbf{U}(\pi,\pi)|1\rangle_j|0\rangle_v = i|0\rangle_j|1\rangle_v$, на стани $|0\rangle_j|0\rangle_v$ і $|1\rangle_j|1\rangle_v$ він діє як одиничний оператор. А оператор $\mathbf{U}_l^{(aux)}(2\pi,\phi)$ змінює знак тільки у вектора стану $|0\rangle_l|1\rangle_v$. Покажемо детальніше послідовність дії оператора (8.11) на стан $|1\rangle_j|0\rangle_l|0\rangle_v$:

$$
\begin{aligned}
&|1\rangle_j|0\rangle_l|0\rangle_v \\
\xrightarrow{\mathbf{V}_l(\pi/2,\pi/2)}\ &\frac{1}{\sqrt{2}}|1\rangle_j(|0\rangle-|1\rangle)_l|0\rangle_v \xrightarrow{\mathbf{U}_j(\pi,\pi)}\ \frac{i}{\sqrt{2}}|0\rangle_j(|0\rangle-|1\rangle)_l|1\rangle_v \\
\xrightarrow{\mathbf{U}_l^{(aux)}(2\pi,\phi)}\ &-\frac{i}{\sqrt{2}}|0\rangle_j(|0\rangle+|1\rangle)_l|1\rangle_v \xrightarrow{\mathbf{U}_j(\pi,\pi)}\ \frac{1}{\sqrt{2}}|1\rangle_j(|0\rangle+|1\rangle)_l|0\rangle_v \\
&\xrightarrow{\mathbf{V}_l(\pi/2,-\pi/2)}\ |1\rangle_j|1\rangle_l|0\rangle_v.
\end{aligned}
$$

Аналогічно можна показати, що оператор (8.11) так діє на стани:

$$
\begin{aligned}
\mathbf{CNOT}_{jl}|1\rangle_j|1\rangle_l|0\rangle_v &= |1\rangle_j|0\rangle_l|0\rangle_v, \\
\mathbf{CNOT}_{jl}|0\rangle_j|0\rangle_l|0\rangle_v &= |0\rangle_j|0\rangle_l|0\rangle_v, \\
\mathbf{CNOT}_{jl}|0\rangle_j|1\rangle_l|0\rangle_v &= |0\rangle_j|1\rangle_l|0\rangle_v.
\end{aligned} \tag{8.12}
$$

Отже, операцій **V**-типу і **U**-типу достатньо, щоб збудувати довільний унітарний оператор для виконання квантових обчислень на квантовому регістрі, збудованому з іонів у пастці Пауля.

8.3 Зчитування результату

Якщо після закінчення обчислень іон номер j перебуває у стані $|0\rangle_j = |4^2S_{1/2}\rangle$, то, діючи на цей іон лазерним променем із довжиною хвилі $\lambda = 397\ nm$, ми переведемо його в стан $|4^2P_{1/2}\rangle$, з якого він може повернутися в стан $|4^2S_{1/2}\rangle$, випромінивши фотон довжиною хвилі $\lambda = 397\ nm$, або перейти в квазістаціонарний стан $|4^2D_{3/2}\rangle$. Повернути його в стан $|4^2P_{1/2}\rangle$ із стану $|4^2D_{3/2}\rangle$ можна, якщо подіяти лазерним променем із довжиною хвилі $\lambda = 866\ nm$. Оскільки зафіксувати детектором окремий фотон неможливо, то необхідно діяти на цей іон на протязі деякого часу, за який буде випромінено багато фотонів, які детектор зафіксує з великою

ймовірністю. Якщо ж після закінчення обчислень іон перебував у стані $|1\rangle_j = |4^2D_{5/2}\rangle$, то детектор не зафіксує жодного фотона.

8.4 Переваги і недоліки

До переваг квантового процесора на іонах у пастці Пауля слід віднести добре відпрацьовану технологію сповільнення іонів, відносну простоту формування квантових вентилів і зчитування результатів обчислень. Недоліками цього квантового процесора є нестійкість іонного ланцюжка при великих L, практично неможливо досягти $L \approx 10^3 \div 10^4$, сильну декогеренцію через кулонівську взаємодію з оточенням, яка також призводить і до нагрівання іонного кристалу, технічні труднощі компонування пристрою керування в малому просторовому об'ємі.

Цей розділ значною мірою ґрунтується на матеріалі праці [15].

Розділ 9

Квантовий процесор із надпровідникових елементів

Цікавим напрямом пошуку фізичних систем, придатних для створення квантових бітів, є дослідження пристроїв на основі надпровідникових елементів (див., напр. праці [39, 41]). Надпровідність є наслідком переходу макроскопічної кількості електронів у квантовий когерентний стан, який має макроскопічні прояви і дає змогу побудувати пристрої, що можуть формувати макроскопічні квантові стани, зокрема, стани квабіта.

9.1 Деякі властивості надпровідників

Послідовна теорія (низькотемпературної) надпровідності металів і сплавів є достатньо складною (див., напр. праці [36, 37, 38]), але для коректного опису тих властивостей надпровідників, які можна використати для побудови квантового процесора, достатньо обмежитися феноменологічною теорією Гінзбурга-Ландау [36].

Надпровідність спостерігається у металах, в яких при температурах нижчих від критичної T_c виникає щілина в спектрі електронів $\Delta(T)$, залежна від температури. Носіями надпровідного струму є пари електронів (куперівські пари), що мають енергію дуже близьку до енергії Фермі, а імпульси їх взаємно протилежні $\vec{p}$ і $-\vec{p}$. Такі пари утворюються нижче критичної температури T_c внаслідок ефективного притягання, викликаного електрон-фононною взаємодією. Характерним розміром пари є *довжина когерентності* $\xi_0 = \hbar v_F/\Delta(0)\pi$ (v_F — швидкість Фермі, $\Delta(0)$ — щілина в спектрі електронів при нульовій температурі), на від-

далях між електронами більшій від ξ_0 хвильова функція пари починає розмиватися. Надпровідний струм може протікати без прикладання електричного поля, при цьому куперівські пари не розсіюються і не розриваються (якщо зовнішнє магнітне поле менше від критичного H_c). Всі надпровідні електрони надпровідника утворюють єдину когерентну квантову макроскопічну систему, яку в теорії Гінзбурга-Ландау (ГЛ) описують хвильовою функцією $\psi(\vec{r},t) = \sqrt{n_s(\vec{r},t)/2}\exp(i\vartheta(\vec{r},t))$, де $n_s(\vec{r},t)$ — густина носіїв надпровідного струму, $\vartheta(\vec{r},t)$ — фаза хвильової функції. В теорії ГЛ цю хвильову функцію вважають параметром порядку, а оскільки перехід у надпровідний стан є фазовим переходом II роду, то, згідно теорії Ландау, вільна енергія системи електронів провідності (надпровідних і нормальних), коли $\psi(\vec{r},t)$ поволі змінюється в просторі, повинна мати вигляд[1]:

$$\mathcal{F}=\mathcal{F}_n+\int\left\{\frac{\vec{B}^2}{8\pi}+\frac{\hbar^2}{4m}\left|\left(\vec{\nabla}-i\frac{2e}{\hbar c}\vec{A}\right)\psi\right|^2+a|\psi|^2+\frac{b}{2}|\psi|^4\right\}d\vec{r}. \quad (9.1)$$

$\mathcal{F}_n$ — вільна енергія в нормальному стані без поля, $\vec{B}$ і $\vec{A}$ — індукція магнітного поля і векторний потенціал, $a{=}\alpha(T-T_c)$, b — феноменологічні сталі, значення яких у наближенні БКШ такі:

$$\alpha=\frac{6\pi^2T_c}{7\zeta(3)T_F}\approx 7.04\frac{T_c}{T_F},\qquad b=\alpha\frac{T_c}{n_e}. \quad (9.2)$$

Мінімум вільної енергії реалізується на станах (хвильових функціях), для яких варіація функціоналу (9.1) за $\delta\psi^*$ (чи $\delta\psi$)

$$\delta\mathcal{F}=\int\left\{-\frac{\hbar^2}{4m}\left(\vec{\nabla}-i\frac{2e}{\hbar c}\vec{A}\right)^2\psi+a\psi+b|\psi|^2\psi\right\}\delta\psi^*d\vec{r}$$
$$+\frac{\hbar^2}{4m}\oint\left(\vec{\nabla}\psi-i\frac{2e}{\hbar c}\vec{A}\psi\right)\delta\psi^*d\vec{s} \quad (9.3)$$

дорівнюватиме нулю $\delta\mathcal{F}{=}0$, тобто за умови:

$$\frac{1}{4m}\left(-i\hbar\vec{\nabla}-\frac{2e}{c}\vec{A}\right)^2\psi+a\psi+b|\psi|^2\psi=0. \quad (9.4)$$

[1]Насправді в ненульовому магнітному полі перехід у надпровідний стан стає фазовим переходом I роду, але для слабих полів цей розклад залишається в силі.

У випадку $\vec{A}$=0 хвильова функція не залежить від координат, тоді з рівняння (9.4), врахувавши (9.2), отримуємо n_s=$-2n_e(T-T_c)/T_c$ (при T>T_c, зрозуміло, n_s=0).

Мінімізація функціоналу (9.1) за $\vec{A}$ призводить до рівняння:

$$\mathrm{rot}\vec{B} = \frac{4\pi}{c}\vec{j}_s, \quad \vec{j}_s = -i\frac{\hbar e}{2m}\left(\psi^*\vec{\nabla}\psi - \psi\vec{\nabla}\psi^*\right) - \frac{2e^2}{mc}|\psi|^2\vec{A}, \qquad (9.5)$$

де $\vec{j}_s$ — густина надпровідного струму. Рівняння (9.4), (9.5) утворюють повну систему рівнянь Гінзбурга-Ландау. За певних умов, які реалізуються, зокрема, при температурах поблизу T_c, разом із рівняннями Максвела вони досить докладно описують макроскопічні властивості надпровідників.

Прирівнювання до нуля другого доданку в (9.3) (інтегралу по поверхні надпровідника) призводить до крайової умови:

$$\vec{n}\left(\vec{\nabla}\psi - i\frac{2e}{\hbar c}\vec{A}\psi\right) = 0, \qquad (9.6)$$

яка фізично реалізується на границі надпровідника з вакуумом чи (масивним) діелектриком. Ця умова не вимагає, щоби хвильова функція на поверхні дорівнювала нулю. Хвильова функція може поширюватися (в даному випадку у вакуум чи масивний діелектрик) на величину кореляційного радіусу флуктуацій параметра порядку $\xi(T)$=$\hbar/(2\sqrt{m\alpha(T_c-T)})$. Тому для поверхні контакту надпровідника з металами (в тому числі і з надпровідниками) умову (9.6) треба замінити іншою. З рівнянь (9.5) і (9.6) випливає також умова $\vec{n}\vec{j}_s$=0.

Подіявши оператором rot на обидві сторони рівняння (9.5) із врахуванням співвідношень div$\vec{B}$=0 і rot(rot$\vec{B}$)=$\vec{\nabla}(\vec{\nabla}\vec{B}) - \Delta\vec{B}$ за умови $\vec{\nabla}n_s$=0, отримаємо рівняння Лондонів:

$$\Delta\vec{B} = \lambda_L^{-2}\vec{B}, \qquad (9.7)$$

де λ_L=$\sqrt{mc^2/(4\pi e^2 n_s)}$=$\sqrt{mc^2T_c/(8\pi e^2 n_e(T_c-T))}$ — лондонівська глибина проникнення магнітного поля в надпровідник. Розглянемо плаский надпровідник в однорідному зовнішньому магнітному полі, скеруємо вісь z углиб надпровідника, а осі x, y — паралельно

до поверхні. Поле, що проникає углиб надпровідника, може залежати тільки від z. З рівняння $\mathrm{div}\vec{B}=0$ випливає, що $dB_z/dz=0$, а з рівняння (9.7) — $B_z=0$. Тоді розв'язком рівняння (9.7) буде вираз:

$$\vec{B}(z) = \vec{B}(0)e^{-z/\lambda_L}, \tag{9.8}$$

де $\vec{B}(0)$ — вектор паралельний до поверхні. Вираз (9.8) пояснює явище виштовхування магнітного поля з надпровідника (ефект Майсснера). Глибина проникнення λ_L є дуже малою величиною, однак для неї і для кореляційного радіусу флуктуацій параметра порядку повинні виконуватись умови $\xi_0 \ll \xi(T)$ і $\xi_0 \ll \lambda_L$, коли застосовна теорія ГЛ[2]. Струм надпровідних електронів у тонкому приповерхневому шарі називають екрануючим діамагнітним струмом, оскільки генероване ним магнітне поле гасить зовнішнє, що викликає ефект виштовхування, який спостерігається при малих полях, поля вищі від критичних руйнують надпровідність і проникають углиб провідника.

З виразу для густини струму (9.5) можна знайти, що при $T < T_c$ надпровідний струм залежить від температури, як і густина надпровідних електронів n_s:

$$\vec{j_s} = \frac{e\hbar}{2m} n_s \left(\vec{\nabla}\vartheta - \frac{2e}{\hbar c}\vec{A} \right). \tag{9.9}$$

Власне останній вираз є означенням величини n_s, яка не збігається ні з густиною куперівських пар, ні з густиною електронів провідності n_e.

З рівнянь (9.5) і (9.8) випливає, що (у зовнішньому магнітному полі) надпровідний струм протікає тільки в приповерхневій області надпровідника товщиною порядку λ_L, а в глибині густина струму дорівнює нулю. Тоді для масивного кільця з отвором інтеграл від правої частини виразу (9.9) вздовж контура, що про-

[2]Вираз (9.8) описує надпровідники I роду (піппардові) і II роду (лондонівські), тільки в надпровідниках I роду глибина проникнення магнітного поля на кілька порядків більша, і описується іншим рівнянням, але надалі вона дуже мала в макроскопічних масштабах. Для нашої мети ця різниця несуттєва, тому не будемо їх розрізняти.

ходить у глибині кільця і охоплює отвір, дає:

$$\oint \vec{\nabla}\vartheta \, d\vec{l} = 2\pi k, \qquad \oint \vec{A}\, d\vec{l} = \int \mathrm{rot}\, \vec{A}\, d\vec{s} = \int \vec{B}\, d\vec{s} = \Phi,$$

$$\Phi = k\Phi_0, \qquad \Phi_0 = \frac{\pi\hbar c}{|e|} = \frac{hc}{2|e|} \approx 2 \cdot 10^{-7} \text{Гс}\cdot\text{см}^2.$$

Тут $k = 0, \pm 1, \pm 2, \ldots$ ціле число, оскільки фаза хвильової функції при повному обході контура може змінюватися тільки на $2\pi k$, це свідчить про квантування магнітного потоку в отворі кільця з квантом магнітного потоку Φ_0. Відомо також, що повний струм у кільці (інтеграл по поперечному перетину кільця від густини струму) генерує магнітний потік в отворі $LJ/c = \Phi$, де L — коефіцієнт самоіндукції кільця, що призводить до квантування повного надпровідного струму $J_s = kc\Phi_0/L$, квант якого залежить від форми і розмірів кільця.

9.2 Ефект Джозефсона

Якщо у тіло кільця перпендикулярно до осі внесено тонкий шар діелектрика товщиною меншою за кореляційний радіус флуктуацій параметра порядку $\xi(T)$, то хвильові функції з одного краю надпровідника будуть проникати через шар діелектрика в інший шар надпровідника. В цьому випадку крайова умова (9.6) не справджується, а тому, розглядаючи контакт як одновимірну систему, сформулюємо нові умови [36]:

$$\frac{\partial\psi_1}{\partial x} - i\frac{2e}{\hbar c}A_x\psi_1 = \frac{1}{\delta}\psi_2, \qquad \frac{\partial\psi_2}{\partial x} - i\frac{2e}{\hbar c}A_x\psi_2 = \frac{1}{\delta}\psi_1,$$

де ψ_1 і ψ_2 — хвильові функції надпровідних електронів з двох сторін діелектричного шару, а $1/\delta$ — стала, пропорційна проникності останнього. Підставивши ці умови у вираз (9.5), отримаємо густину струму через діелектричний шар:

$$j = j_m \sin(\vartheta_1 - \vartheta_2) = j_m \sin(\varphi), \qquad j_m = \frac{\hbar e}{2m\delta} n_s. \tag{9.10}$$

Її часто записують

$$j = j_0 \sin(\varphi) \tag{9.11}$$

через густину критичного струму [38]:

$$j_0(T) = \frac{\pi\tilde{\Delta}(T)}{2eR_n}\mathrm{th}\frac{\tilde{\Delta}(T)}{2k_BT}, \qquad j_0(0) = \frac{\pi\Delta(0)}{2eR_n}, \tag{9.12}$$

де R_n — опір джозефсонівського переходу для нормальних електронів, а $\tilde{\Delta}(T)\approx 1.74\Delta(0)\sqrt{1-T/T_c}$ — щілина в енергетичному спектрі електронів поблизу T_c, $\Delta(0)\approx 1.764k_BT_c$ — щілина в енергетичному спектрі електронів при $T=0$.

Явище протікання (тунельного) надпровідного струму через тонкий діелектричний шар без прикладання зовнішнього електричного поля теоретично передбачив Джозефсон у 1961 році, його називають стаціонарним ефектом Джозефсона. У цьому випадку інтегрування фази вздовж контуру в глибині надпровідника, який перебуває в зовнішньому магнітному полі, дає умову:

$$\varphi + 2\pi k = 2\pi\frac{\Phi}{\Phi_0} \qquad \text{чи} \qquad \Phi = (\varphi/2\pi + k)\,\Phi_0, \tag{9.13}$$

де $\varphi{=}\theta_1{-}\theta_2$ — різниця фаз хвильової функції на переході Джозефсона.

Якщо ж зовнішнє електричне поле створює на діелектричному шарі різницю потенціалів $V = U_1 - U_2$, то виникає нове явище, яке називають нестаціонарним ефектом Джозефсона, коли тунельний струм стає змінним за напрямом і за часом. Це легко пояснити з умов калібрувальної інваріантності, зв'язок

$$\vartheta(t) = \vartheta(0) + \frac{2e}{\hbar}\int_0^t U(t)dt, \tag{9.14}$$

не змінюється при перетвореннях:

$$U \to U + \frac{1}{c}\frac{\partial\chi}{\partial t}, \qquad \vartheta \to \vartheta + \frac{2e}{\hbar c}\chi.$$

Тоді вираз для струму (9.10) при сталій напрузі буде таким:

$$j = j_0 \sin(\varphi(0) + \omega t), \qquad \omega \equiv \frac{2e}{\hbar}V. \tag{9.15}$$

Енергія кванту випромінювання $\hbar\omega$ точно дорівнює енергії, яку набуває куперівська пара, проходячи різницю потенціалів V. Зауважимо, що прикладання напруги спричиняє також тунельний струм нормальних електронів, але через високий опір діелектричного шару він є дуже малим і ним можна знехтувати.

Умову (9.14) можна записати у диференціальній формі для різниць фаз і потенціалів:

$$\frac{d\varphi}{dt} = \frac{2e}{\hbar}V. \tag{9.16}$$

Відзначимо, що стаціонарний (9.11) і змінний (9.15) тунельні струми Джозефсона є набагато меншими за екрануючі діамагнітні струми в надпровіднику тому, за відповідних умов, ними часто нехтують.

9.3 Надпровідні квантові інтерферометри

Надпровідні квантові інтерферометри часто називають SQUID (superconducting quantum interference devices), їхня дія ґрунтується на ефектах Джозефсона. Використовують їх, зокрема, для високоточних вимірювань напруженості магнітного поля. Розглянемо коротко SQUID на стаціонарному ефекті Джозефсона. Най-

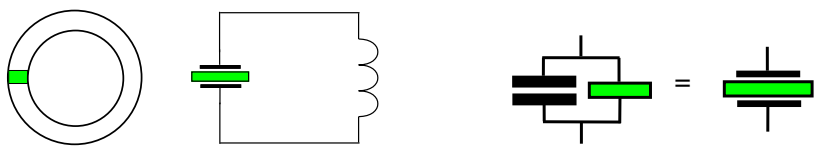


Рис. 9.1: rf-SQUID і його схема. Позначення переходу Джозефсона включає також електричну ємність SQUID

простіший з них rf–SQUID (radio frequency SQUID) складається з одного переходу Джозефсона, в якому діелектричний шар має форму паралелепіпеда (див. рис. 9.1). Якщо такий перехід помістити в магнітне поле, перпендикулярне до більшої вільної грані, і детально врахувати екрануючі діелектричні струми, викликані

магнітним полем (в діелектрику і його околі), то можна встановити, що повний тунельний надпровідний струм крізь діелектричний шар визначається магнітним потоком через поверхню переходу [38]:

$$J = J_{max}\sin(\varphi), \qquad J_{max} = j_0 Y Z \frac{\sin(\pi\Phi_t/\Phi_0)}{\pi\Phi_t/\Phi_0},$$

де Z, Y — висота і ширина діелектричного шару, Φ_0 — квант магнітного потоку, $\Phi_t = B_z Y(d + 2\lambda_L)$ — потік магнітного поля через перехід Джозефсона, а B_z, λ_L, d — напруженість магнітного поля, глибина проникнення магнітного поля в надпровідник і товщина діелектрика відповідно. З останньої формули бачимо, що залежність надпровідного струму від магнітного потоку має такий самий характер як інтенсивність світлового потоку від координати при дифракції на щілині. Надпровідний струм дорівнює нулю, коли потік магнітного поля через перехід кратний кванту магнітного потоку. Такий SQUID дає змогу вимірювати напруженість магнітного поля з точністю $\sim \Phi_0$, підвищити точність вимірювання за допомогою цього SQUID можна, використовуючи високочастотний струм [38].

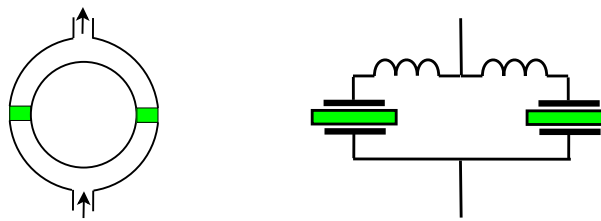


Рис. 9.2: dc-SQUID і його схема

Інший інтерферометр dc–SQUID (direct current SQUID) дає змогу вимірювати потоки з точністю до $\sim 0.001\Phi_0$. Його виготовляють у формі (топологічного) кільця з двома переходами Джозефсона і симетрично розташованих входу і виходу струму (Рис. 9.2). Повний струм у ньому описує такий вираз:

$$J = J_0\left(\sin\varphi_A + \sin\varphi_B\right).$$

Врахувавши, що в цьому випадку інтеграл уздовж контуру у формулі (9.9) дає

$$\varphi_A - \varphi_B = 2\pi\Phi/\Phi_0 + 2\pi k,$$

для фізично однакових контактів зміни фаз на кожному з них можна записати як:

$$\varphi_A = \varphi_0 + \pi\Phi/\Phi_0 + \pi k, \qquad \varphi_B = \varphi_0 - \pi\Phi/\Phi_0 - \pi k,$$

і отримати вираз для повного струму:

$$J = 2J_0 \sin\varphi_0 \cos\left(\pi\Phi/\Phi_0\right).$$

Тут Φ (магнітний потік через кільце) є значно більшим за потоки через переходи Φ_t, якими ми знехтували. З врахуванням цих потоків повний струм через dc–SQUID матиме вигляд:

$$J = 2J_0 \sin\varphi_0 \frac{\sin(\pi\Phi_t/\Phi_0)}{\pi\Phi_t/\Phi_0} \cos(\pi\Phi/\Phi_0).$$

З цього виразу бачимо, що на високочастотні осциляції, пов'язані з потоком через кільце Φ, накладається плавна залежність від потоку через перехід Φ_t, оскільки $\Phi_t \ll \Phi$. Тому чутливість dc–SQUID до зовнішнього поля є значно вищою, ніж у rf–SQUID.

9.4 Квантові біти на основі rf-SQUID

Отже, пристрої, збудовані з надпровідників, можуть працювати в режимах, коли деякі макроскопічні характеристики цих систем квантуються. Чи можна їх використати для побудови квантового біта? Щоб відповісти, треба записати гамільтоніан такої системи у відповідних змінних, проквантувати його і з'ясувати чи система має в макроскопічних змінних такі достатньо тривкі стани, придатні для формування квантових бітів. Треба зважати на обмеженість змісту гамільтоніана, оскільки ми маємо справу із термодинамічною системою і зображення її квантовомеханічною системою може бути тільки наближеним. Але, як свідчать теоретичні й експериментальні дослідження, таке зображення є достатньо адекватним і дає змогу збудувати макроскопічні квантові пристрої з досить тривалим часом когерентності.

Записати гамільтоніан, який був би придатний для опису всіх надпровідникових пристроїв, неможливо, тому розглянемо спочатку найпростіший з них rf-SQUID. Цей приклад допоможе зрозуміти засади побудови гамільтоніанів для складніших систем. Наведемо (якісні) міркування, які дають змогу прояснити походження різних складових шуканого гамільтоніана.

З курсу електрики відомо, що будь-який електричний ланцюг характеризується активним опором R, електричною ємністю C та коефіцієнтом самоіндукції L. Якщо через rf-SQUID протікає струм J, то його можна записати (знехтувавши для спрощення індуктивністю) формулою:

$$J + J_N = C\frac{dV}{dt} + \frac{V}{R} + J_0 \sin\varphi,$$

де J_N — струм, викликаний шумами. Використавши зв'язок між фазою і напругою (9.16), останню формулу можна виразити в змінних фази:

$$J + J_N = C\frac{\hbar}{2e}\frac{d^2\varphi}{dt^2} + \frac{\hbar}{2eR}\frac{d\varphi}{dt} + J_0 \sin\varphi,$$

чи у вигляді:

$$J_N = C\frac{\hbar}{2e}\frac{d^2\varphi}{dt^2} + \frac{\hbar}{2eR}\frac{d\varphi}{dt} - \frac{d}{d\varphi}\left(J_0\cos\varphi + J\varphi\right).$$

Для того, щоб доданки в цьому рівнянні мали розмірність енергії, помножимо його на величину $\alpha = \hbar/(2e)$:

$$\alpha J_N = C\alpha^2\frac{d^2\varphi}{dt^2} + \frac{\alpha^2}{R}\frac{d\varphi}{dt} - \alpha\frac{d}{d\varphi}\left(J_0\cos\varphi + J\varphi\right).$$

Це рівняння описує rf-SQUID у змінних струму і фази із врахуванням шумів і дисипації, що необхідно для дослідження процесів декогеренції. Оскільки ми цікавимося процесами формування квантових рівнів, то впливом шумів (J_N) і дисипації ($d\varphi/dt$) наразі знехтуємо. Тоді останнє рівняння буде рівнянням Лагранжа для "механічної" системи з лагранжіаном

$$\mathcal{L} = \frac{C\alpha^2}{2}\left(\frac{d\varphi}{dt}\right)^2 - U(\varphi), \qquad U(\varphi) = -\alpha\left(J_0\cos\varphi + J\varphi\right).$$

Звідси можна отримати гамільтоніан у змінних заряду і фази:

$$\mathcal{H} = \frac{Q^2}{2C} + U(\varphi).$$

Або з врахуванням індуктивності системи:

$$\mathcal{H}=\frac{Q^2}{2C}+U(\varphi)+\frac{LJ^2}{2} \quad \text{чи} \quad \mathcal{H}=\frac{Q^2}{2C}+U(\varphi)+\frac{(\Phi-\Phi^{ex})^2}{2L}, \qquad (9.17)$$

де Φ — повний магнітний потік через кільце rf-SQUID, Φ^{ex} — потік через кільце, викликаний зовнішнім магнітним полем. Ці вирази насправді визначають вільну енергію rf-SQUID, їх можна отримати простіше, додавши до суми енергій конденсатора та індуктивності $Q^2/2C+LJ^2/2$ вільну енергію надпровідного струму в переході Джозефсона, яку можна знайти як роботу цього струму:

$$\int_{-\infty}^{t} J_s(t)V(t)dt = \alpha \int_{-\infty}^{t} J_0 \sin(\varphi)d\varphi/dt \cdot dt$$
$$= \alpha J_0 \int_0^{\varphi} \sin(\varphi)d\varphi = \alpha J_0 \left(1-\cos\varphi\right).$$

Хоча вирази (9.17) для енергії rf-SQUID ми обґрунтовували теорією Гінзбурга-Ландау, яка найкраще описує надпровідники поблизу температури переходу T_c, однак ці вирази придатні для опису rf-SQUID і для температур значно нижчих від T_c. Більше того, спосіб отримання енергії, коли до електромагнітної енергії кола додається енергія надпровідного струму, поширюється на значно складніші електричні схеми, збудовані з подібних елементів.

Запишемо енергію (9.17) у вигляді:

$$\mathcal{H} = E_C N^2 - E_J \cos\varphi - \alpha J\varphi + E_L \left(\Phi/\Phi_0 - \Phi^{ex}/\Phi_0\right)^2 \qquad (9.18)$$

з параметрами $E_C{=}(2e)^2/2C$, $E_J{=}\alpha J_0{=}L_J J_0^2$, $E_L{=}\Phi_0^2/2L$, де N — число куперівських пар у заряді, акумульованому ємністю джозефсонівського переходу, а L_J — еквівалентна індуктивність надпровідного струму [38, 40, 42, 43] $L_J J_0 = \Phi_0/2\pi$. Якщо $E_L \ll E_C$ і $E_L \ll E_J$, то магнітні потоки не є важливими і останнім доданком в (9.18) можна знехтувати, тоді можливі два варіанти співвідношень параметрів: $E_C{<}E_J$, коли фаза є добре визначена, а заряд

флуктуює, або $E_C{>}E_J$, коли заряд є добре визначеним, а фаза флуктуює. У надпровідниках оператор фази хвильової функції і оператор повної кількості куперівських пар є канонічно спряженими змінними:

$$[\boldsymbol{\varphi}, \mathbf{N}] = i, \ \Rightarrow \ \{\boldsymbol{\varphi}{=}\varphi, \ \mathbf{N}{=}-i\frac{\partial}{\partial\varphi}\} \ \text{ чи } \ \{\mathbf{N}{=}N, \ \boldsymbol{\varphi}{=}i\frac{\partial}{\partial N}\}, \quad (9.19)$$

тобто, пов'язані співвідношенням невизначеності $\Delta N \Delta\varphi \gtrsim 1$. Кількість куперівських пар і фаза хвильової функції є макроскопічними величинами, тому вирази (9.19) дають змогу побудувати опис макроскопічних квантових властивостей систем, складених із надпровідникових елементів.

Вираз (9.18) справедливий тоді, коли можна нехтувати термічними флуктуаціями в системі, тому далі вважатимемо, що енергія термічних збуджень k_BT є значно меншою за кожен із енергетичних параметрів виразу (9.18).

Фазовий квабіт. Цей квабіт реалізується станами rf-SQUID,

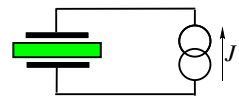


Рис. 9.3: Схема фазового квабіта

до якого приєднано джерело слабкого струму для керування цими станами. rf-SQUID виготовлений так, що виконуються умови $E_L \ll E_C \ll E_J$ і магнітними потоками можна знехтувати, тому добре визначеною змінною є фаза. Тоді виходячи із виразу (9.18), із врахуванням комутаційного співвідношення (9.19) оператор Гамільтона можна записати в змінних фази:

$$\mathcal{H} = -E_C\frac{\partial^2}{\partial\varphi^2} - E_J\cos\varphi - \alpha J\varphi. \quad (9.20)$$

Рівняння на власні функції і власні значення для цього гамільтоніана є досить складним:

$$\left(-E_C\frac{\partial^2}{\partial\varphi^2} - E_J\cos\varphi - \alpha J\varphi\right)|\psi\rangle = E|\psi\rangle \quad (9.21)$$

(без доданка $\alpha J\varphi$ це було б рівняння Матьє) і точно розв'язати його можна тільки чисельно. Однак за певних умов можна знайти аналітично стани з найнижчими енергіями. Потенціальна енер-

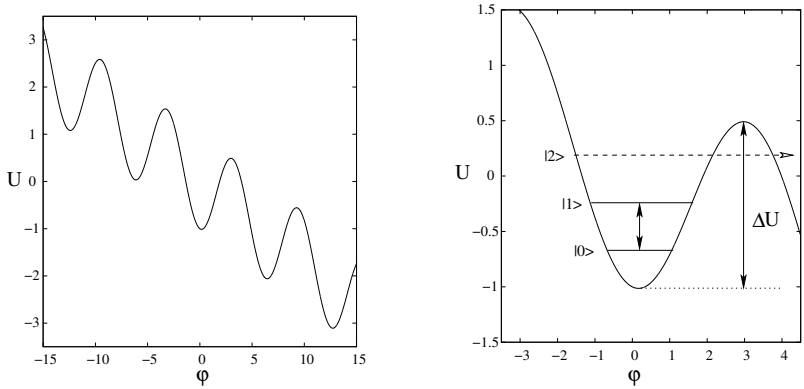


Рис. 9.4: Потенціальна енергія фазового квабіта

гія цього гамільтоніана нагадує "пральну дошку" (див. рис. 9.4). Розглянемо найнижчі енергетичні рівні системи, коли $-\pi\lesssim\varphi\lesssim\pi$. Тоді потенціальну енергію можна розкласти за φ біля мінімуму

$$U=-\alpha\left(J_0\cos\varphi+J\varphi\right)\approx-\alpha J_0\left(\cos\varphi_0+\frac{J}{J_0}\varphi_0\right)+\frac{\alpha J_0}{2}\cos\varphi_0(\varphi-\varphi_0)^2$$

з $\cos\varphi_0=\sqrt{1-J^2/J_0^2}$ і отримати наближене рівняння (9.21):

$$\left(-E_C\frac{\partial^2}{\partial\varphi^2}+\frac{E_J}{2}\cos\varphi_0(\varphi-\varphi_0)^2-E\right)|\psi\rangle=0.$$

Увівши нові безрозмірні змінні $\xi\equiv\sqrt[4]{E_J\cos\varphi_0/2E_C}\varphi$ останнє рівняння можна записати як:

$$\left(\frac{d^2}{d\xi^2}-\xi^2+\varepsilon\right)|\psi\rangle=0,$$

де $\varepsilon=2E/\hbar\omega_p$, $\omega_p\equiv\omega_{0p}\sqrt{\cos\varphi_0}$, $\omega_{0p}\equiv\sqrt{2E_JE_C}/\hbar$. Ми отримали рівняння на власні значення одновимірного гармонічного осцилятора, розв'язки якого добре відомі [1]. Вибравши основний $n=0$ і перший збуджений $n=1$ стани осцилятора за стани квабіта,

$$E_n = \hbar\omega_p\,(n + 1/2)$$

отримаємо гамільтоніан квабіта:

$$\mathcal{H} = -\frac{\hbar\omega_p(s_0)}{2}\boldsymbol{\sigma}^z,$$

із залежною від постійного струму $s_0{=}J/J_0$ частотою, якщо ж додати залежний від часу струм $s(t){=}\Delta J(t)/J_0$ такий, що $|s(t)|{\ll}1$, то гамільтоніан квабіта буде таким (див. [42, 43]):

$$\mathcal{H} = -\frac{\hbar\omega_p(s_0)}{2}\boldsymbol{\sigma}^z - \frac{aE_J}{\sqrt{2}}s(t)\boldsymbol{\sigma}^x,$$

де позначено $a{=}a_0(1-s_0)^{-1/8}$, $a_0{=}\sqrt[4]{2E_C/E_J}$. Перший доданок цього гамільтоніана формує стани квабіта, а другий, залежний від часу, описує переходи між ними.

Зарядовий квабіт. Фізично зарядовий квабіт творять два надпровідникові наноострівці, поєднані джозефсонівським переходом з енергією E_J та зарядовою ємністю C_J, які вмонтовані в ланцюг із додатковою ємністю C_g та джерелом напруги V_g (див. рис. 9.5). Енергію, акумульовану одним із острівців, запишемо як:

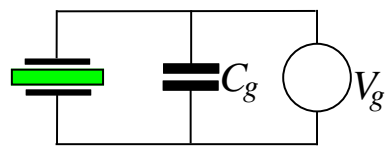


Рис. 9.5: Схема зарядового квабіта

$$\mathcal{H} = \frac{(Q+Q_g)^2}{2(C_J+C_g)} - E_J\cos\varphi = \frac{(2eN+V_gC_g)^2}{2(C_J+C_g)} - E_J\cos\varphi$$
$$= E_C(N-N_g)^2 - E_J\cos\varphi,$$

де $E_C = (2e)^2/2(C_J+C_g)$, N — число куперівських пар, що утворюють заряд на переході Джозефсона, тобто, різниця в числі куперівських пар двох острівців. Воно є малим унаслідок малої ємності джозефсонівського переходу. $N_g = -C_gV_g/(2e)$ — "кількість

куперівських пар", створених зарядом додаткового конденсатора, яке може регулюватися неперервно величинами C_g і V_g.

Увівши оператори кількості куперівських пар $\mathbf{N}$ і фази $\boldsymbol{\varphi}$, можна отримати фізичний гамільтоніан, який описує переходи куперівських пар між острівцями:

$$\mathcal{H} = E_C(\mathbf{N} - N_g)^2 - E_J \cos\boldsymbol{\varphi}. \tag{9.22}$$

Квантовий біт можна утворити з перших власних станів $n = 0$ і $n = 1$ оператора $\mathbf{N}$:

$$\mathbf{N}|n\rangle = n|n\rangle$$

$\{|0\rangle, |1\rangle\}$. Оскільки в цьому базисі

$$\mathbf{N} - N_g = -\left(N_g - \frac{1}{2}\right) - \frac{1}{2}\boldsymbol{\sigma}^z,$$

то перший доданок оператора (9.22) можна записати як:

$$\mathrm{const} E_C \mathbf{I} + E_C\left(N_g - \frac{1}{2}\right)\boldsymbol{\sigma}^z.$$

З огляду на співвідношення $\exp(-i\boldsymbol{\varphi})|n\rangle = \exp(d/dN)|n\rangle = |n+1\rangle$ можна зрозуміти, що другий доданок оператора (9.22) описує переходи між станами $|n\rangle$ (див. [42, 43]):

$$\frac{E_J}{2}\left(|n\rangle\langle n+1| + |n+1\rangle\langle n|\right)$$

тому в базисі $\{|0\rangle, |1\rangle\}$ гамільтоніан (9.22) буде мати вигляд:

$$\mathcal{H} = E_C\left(N_g - \frac{1}{2}\right)\boldsymbol{\sigma}^z - \frac{E_J}{2}\boldsymbol{\sigma}^x.$$

А в базисі $\{|+\rangle, |-\rangle\}$

$$\mathcal{H} = E_C\left(N_g - \frac{1}{2}\right)\boldsymbol{\sigma}^x - \frac{E_J}{2}\boldsymbol{\sigma}^z,$$

тобто, базисні стани $\{|+\rangle, |-\rangle\}$ формуються джозефсонівськими струмами, а переходи між ними регулюються напругою V_g (зміною N_g). Кінцевий стан квабіта визначається вимірюванням V_g.

Зарядовий квабіт є дуже чутливий до впливу зовнішніх зарядів, тому має дуже малий час когерентності, що дуже ускладнює його фізичне застосування. Докладніше із зарядовими квабітами на надпровідникових елементах можна ознайомитися за книгами [15, 39] та наведеними там джерелами.

Потоковий квабіт. Схема цього квабіта на основі rf-SQUID наведена на рис. 9.6. Його енергію запишемо так:

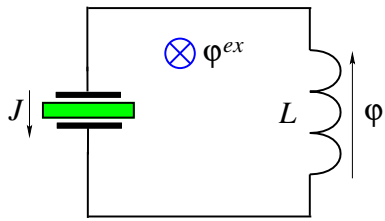


Рис. 9.6: Схема потокового квабіта. $\varphi{\equiv}2\pi\Phi/\Phi_0$, $\varphi^{ex}{\equiv}2\pi\Phi^{ex}/\Phi_0$ [44, 45]

$$\mathcal{H} = E_C N^2 - E_J \cos\varphi + E_L \left(\Phi/\Phi_0 - \Phi^{ex}/\Phi_0\right)^2, \qquad (9.23)$$

де параметри такі $E_C{=}(2e)^2/2\mathrm{C}$, $E_J{=}\alpha J_0$, $E_L{=}\Phi_0^2/2L$ і в даному випадку перебувають у співвідношенні $E_C \ll E_J < E_L$. З виразу (9.23), із врахуванням співвідношень (9.13) і (9.19), можна отримати гамільтоніан в зображенні потоками:

$$\mathfrak{H} = -\frac{\hbar^2}{2C}\frac{\partial^2}{\partial\Phi^2} - E_J \cos\left(2\pi\frac{\Phi}{\Phi_0}\right) + \frac{(\Phi-\Phi^{ex})^2}{2L}$$

чи у фазовому зображенні:

$$\mathfrak{H} = -E_C\frac{\partial^2}{\partial\varphi^2} - E_J\cos\varphi + \left(\frac{\Phi_0}{2\pi}\right)^2\frac{(\varphi-\varphi^{ex})^2}{2L}.$$

Останній гамільтоніан дуже схожий до гамільтоніана фазового квабіта тільки замість доданка із зовнішнім струмом містить доданок з магнітними потоками. Як для фазового, так і для потокового квабіта добре визначеною змінною є фаза, а заряд сильно флуктує.

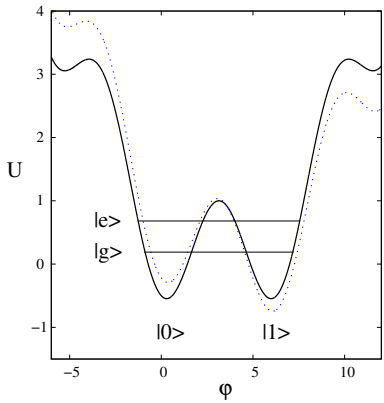


Рис. 9.7: Потенціальна енергія та найнижчі рівні потокового rf-SQUID при $L_J/2L{=}2/(2\pi)^2$, $\varphi^{ex}{=}\pi$ (суцільна лінія), $\varphi^{ex}{=}5\pi/4$ (штрихова лінія)

Різні потенціальні ями відповідають різним орієнтаціям індукованого потоку $\Phi - \Phi^{ex}$, тобто, різним напрямам протікання надпровідного струму. Тому стани, локалізовані в цих ямах, можна було б вибрати за стани квабіта $\{|0\rangle, |1\rangle\}$. Однак, оскільки бар'єр між ямами досить низький, унаслідок квантового тунелювання магнітний потік (і струм) змінює свій напрям, тому такі стани не будуть стабільними. Водночас процес тунелювання спричиняє розщеплення рівня основного стану в симетричному потенціалі ($\varphi_0{=}\pi$ чи $\Phi^{ex}/\Phi_0{=}1/2$) і формує два рівні в кожній із ям, як показано на рис. 9.7. Тому за логічні рівні квабіта можна вибрати $|0\rangle = (|g\rangle + |e\rangle)/\sqrt{2}$, $|1\rangle = (|g\rangle - |e\rangle)/\sqrt{2}$. "Логічний" гамільтоніан квабіта (тобто на базисних станах $\{|0\rangle, |1\rangle\}$) в даному випадку має вигляд:

$$\mathcal{H}_q = -\frac{1}{2}\left(\epsilon\boldsymbol{\sigma}^z + \Delta_q\boldsymbol{\sigma}^x\right), \tag{9.24}$$

де позначено:

$$\epsilon \equiv 2\frac{\langle 1|\Phi - \Phi_0/2|1\rangle}{L}\left(\Phi^{ex} - \frac{\Phi_0}{2}\right), \;\; \Delta_q \equiv \langle e|\mathcal{H}|e\rangle - \langle g|\mathcal{H}|g\rangle.$$

Простий rf-SQUID дає змогу відносно легко реалізувати квабіт, однак він має недоліки, які не можна усунути: 1) параметром роз-

щеплення рівнів Δ_q не можна керувати in situ, 2) цей параметр експонентно чутливий до параметрів SQUID, тобто до коефіцієнта самоіндукції L і критичного струму J_0, тому він непридатний до конструювання квантових схем (див. [44]).

Квантові біти на основі CJJ rf-SQUID Недоліки квабіта на rf-SQUID вдається частково усунути, використавши його вдосконалену схему CJJ rf-SQUID (coupled Josephson-junction rf-SQUID), зображену на рис. 9.8, де в схему rf-SQUID замість переходу Джозефсона введено dc-SQUID (див. [44]).

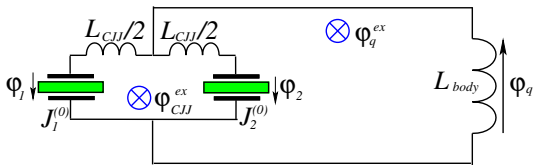


Рис. 9.8: Схема CJJ rf-SQUID квабіта

Таку схему описують гамільтоніаном:

$$\mathcal{H} = \sum_n \left[\frac{Q_n^2}{2C_n} + U_n \frac{(\varphi - \varphi_n^{ex})}{2} \right] - U_q \beta_{eff} \cos(\varphi_q - \varphi_q^0). \qquad (9.25)$$

Тут сумування ведеться за індексами $n = \{q, CJJ\}$, а змінні і параметри цього гамільтоніана так пов'язані із змінними та параметрами пристрою (див. [44]):

$$C_q \equiv C_1 + C_2,\ 1/C_{CJJ} \equiv 1/C_1 + 1/C_2,\quad L_q \equiv L_{body} + L_{CJJ}/4,$$
$$\varphi_n^{ex} \equiv 2\pi \frac{\Phi_n^{ex}}{\Phi_0},\ \varphi_q^0 \equiv 2\pi \frac{\Phi_q^0}{\Phi_0} \equiv -\operatorname{arctg}\left(\frac{\beta_-}{\beta_+} \operatorname{tg} \frac{\varphi_{CJJ}}{2} \right),$$
$$U_n \equiv \left(\frac{\Phi_0}{2\pi} \right)^2 \frac{1}{L_n}\ \beta_\pm \equiv 2\pi \frac{L_q (J_1^{(0)} \pm J_2^{(0)})}{\Phi_0},$$
$$\beta_{eff} \equiv \beta_+ \cos\left(\frac{\varphi_{CJJ}}{2} \sqrt{1 + \left[\frac{\beta_-}{\beta_+} \operatorname{tg} \frac{\varphi_{CJJ}}{2} \right]^2} \right).$$

Квантовий біт формується, як і в rf-SQUID, напрямами магнітного потоку через велике (q) кільце. Його суттєвою перевагою є те,

що параметром тунелювання Δ_q можна керувати, змінюючи зовнішнє магнітне поле Φ^{ex}_{CJJ} в маленькому кільці (CJJ), тобто, in situ виправляти дефекти виготовлення SQUID. Недоліком цього пристрою є асиметрія переходів Джозефсона, тобто, різниця критичних струмів $J_1^{(0)} - J_2^{(0)}$ у різних переходах, яка є дефектом виготовлення і призводить до асиметрії потенціалу, а тому може спричинити вихід за допустимі межі параметрів ϵ і Δ_q у процесі виконання обчислень. Використання CJJ rf-SQUID у невеликих мережах потребує детального контролю його параметрів.

Квантові біти на основі CCJJ rf-SQUID Цю асиметрію CJJ rf-SQUID вдається усунути в CCJJ rf-SQUID (coupled-coupled Josephson-junction rf-SQUID), схема якого зображена на рис. 9.9 (див. [44]). Він утворений із CJJ rf-SQUID за тим самим правилом: замість кожного переходу Джозефсона в схему введені dc-SQUID. Його гамільтоніан такий, як і гамільтоніан (9.25) CJJ rf-SQUID,

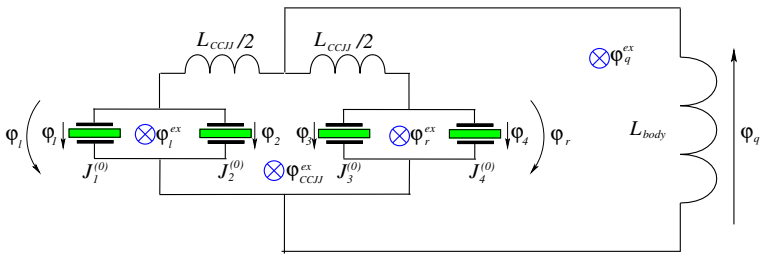


Рис. 9.9: Схема CCJJ rf-SQUID квабіта

тільки змінні і параметри інакше пов'язані із змінними і параметрами фізичної системи (див. [44]). Вибором магнітних потоків у правому і лівому малих кільцях можна досягти симетрії, якої не вдається досягти в процесі виготовлення CJJ rf-SQUID. На основі такого квабіта уже можна будувати великі схеми ($\sim$ 1000 квабітів).

Пов'язування квабітів на основі CJJ rf-SQUID. На рис. 9.10 показано схему індуктивного зв'язку між двома квантовими бітами, яку було запропоновано і випробувано у праці [45]. Дослідження довели, що така схема веде до бажаного гамільтоніана, не вносить

перешкод в роботу окремих квабітів і дає змогу будувати досить великі мережі. “Логічний” гамільтоніан квабіта (9.24) є таким са-

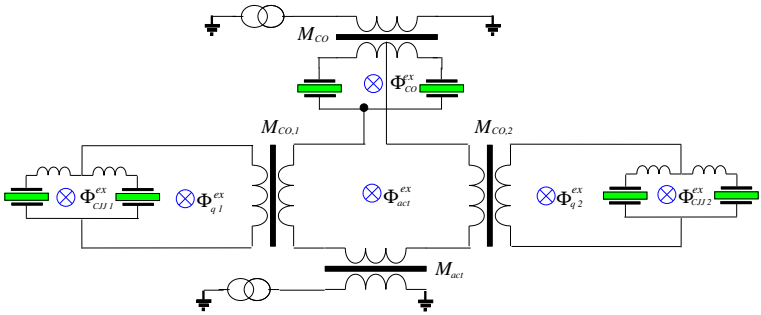


Рис. 9.10: Схема індуктивного зв’язку між двома CJJ rf-SQUID

мим у всіх трьох варіантах. Запропонована схема зв’язку вносить взаємодію між z–компонентами ефективних спінів, якою можна керувати, тоді “логічний” гамільтоніан мережі можна записати у вигляді:

$$\mathcal{H} = -\frac{1}{2}\sum_j \left(\epsilon_j \boldsymbol{\sigma}_j^z + \Delta_j \boldsymbol{\sigma}_j^x\right) + \sum_{i,j} K_{ij}\boldsymbol{\sigma}_i^z\boldsymbol{\sigma}_j^z. \qquad (9.26)$$

Це гамільтоніан квантової моделі Ізінга в зовнішніх полях. Без доданка з x–компонентою його ще називають гамільтоніаном моделі спінового скла.

3JJ–квабіт. Ще одним проектом потокового квабіта, над яким працюють і українські вчені із Харкова, є 3JJ-квабіт, описаний зокрема у праці [39]. Це топологічне кільце з трьома джозефсонівськими контактами — двома однаковими і третім відмінним від них (див. схему на рис. 9.11). Перевагою цього квабіта є малі розміри, що суттєво зменшує вплив зовнішніх електромагнітних полів. Через малу індуктивність доданком із магнітним полем можна знехтувати, тому його енергія пов’язана тільки із джозефсонівським струмом і так виражається через зміну фаз на контактах:

$$U = E_J\left(2 + \gamma - \cos\varphi_1 - \cos\varphi_2 - \gamma\cos\varphi_3\right), \qquad (9.27)$$

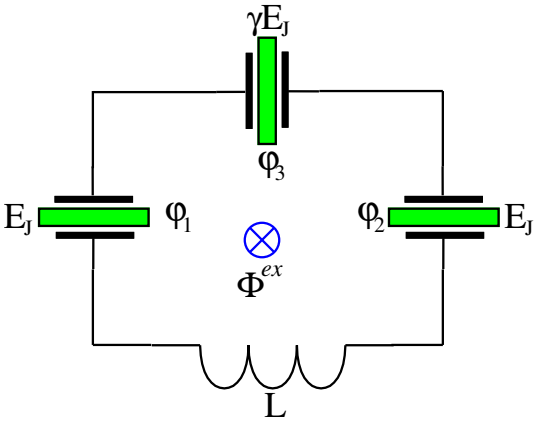


Рис. 9.11: Схема 3JJ–квабіта

а фази в ньому пов'язані з магнітним потоком співвідношенням:

$$\varphi_1 + \varphi_2 + \varphi_3 = 2\pi\frac{\Phi}{\Phi_0} \approx 2\pi\frac{\Phi^{ex}}{\Phi_0} = 2\pi\,(f + 1/2)\,.$$

Увівши нові змінні $\varphi = (\varphi_1 + \varphi_2)/2$, $\theta = (\varphi_1 - \varphi_2)/2$ вираз для енергії (9.27) запишемо:

$$U(\varphi,\theta){=}E_J\,[2{+}\gamma{-}2\cos\varphi\cos\theta{-}\gamma\cos\left(2\pi(f{+}1/2){-}2\varphi\right)]\,. \qquad (9.28)$$

Параметр γ зумовлює відмінність джозефсонівського струму на третьому контакті від цього струму на перших двох, він визначається співвідношенням геометричних розмірів, експериментально встановлене оптимальне значення дорівнює $\gamma \approx 0.8$ (див. [39]).

Потенціал (9.28) в області $-\pi < \theta \leq \pi, -\pi < \varphi \leq \pi$ при $f = 0$, тобто, слабкому магнітному полі $\Phi^{ex} = \Phi_0/2$ має два однакові мінімуми в точках $\theta = 0, \varphi = \pm\arccos(1/2\gamma)$. Його профіль при $\theta = 0$ близький до зображеного на рис. 9.7. Подібно як у потоковому квабіті формуються стани з різними напрямами магнітного поля, але квабіт утворюється на суперпозиційних станах. Згідно тверджень, наведених у праці [39], такі квабіти можна з'єднати керованими індуктивними зв'язками в квантовий регістр, який описують гамільтоніаном (9.26).

Однак експериментально створені на сьогодні квантові біти на основі надпровідникових елементів мають час когерентності порядку кількох мікросекунд (див. [39]), чого недостатньо для побудови реальних квантових процесорів.

9.5 Адіабатичний комп'ютер

Нехай перед нами стоїть задача, розв'язком якої є число, записане в основному стані гамільтоніана

$$\mathcal{H} = -\sum_j h_j \boldsymbol{\sigma}^z + \sum_{i,j} K_{ij} \boldsymbol{\sigma}_i^z \boldsymbol{\sigma}_j^z.$$

Як перевести систему в цей стан? З адіабатичної теореми відомо, що при адіабатичному вмиканні взаємодії система перейде з основного стану гамільтоніана без взаємодії в основний стан гамільтоніана із взаємодією. Якщо ми можемо створити фізичну систему з "логічним" гамільтоніаном, параметри якого залежать від часу

$$\mathcal{H}(t) = -\sum_j h_j(t) \boldsymbol{\sigma}^z + \sum_{i,j} K_{ij}(t) \boldsymbol{\sigma}_i^z \boldsymbol{\sigma}_j^z - \sum_j f(t) \boldsymbol{\sigma}_j^x$$

так, що $h_j(0) = 0, K_{ij}(0) = 0, f(0) = \text{const}$ і $h_j(t \to \infty) = h_j$, $K_{ij}(t \to \infty) = K_{ij}$, $f(t \to \infty) = 0$, причому цей перехід буде адіабатичним, то ми розв'яжемо нашу задачу. Автори праць [41, 44, 45] стверджують, що запропонований ними квантовий процесор, і виконує такий перехід.

Підсумки

Теоретичні дослідження проблеми квантових обчислень, виконані в середині 1990-х — на початку 2000 років, дали змогу з'ясувати, що принципових заборон на створення квантових комп'ютерів (процесорів) квантова механіка не встановлює. Квантове обчислення проходить три важливі етапи: 1) ініціалізацію квантового регістра (приведення його в початковий стан), 2) виконання дії квантових схем, складених із квантових вентилів (квантових логічних елементів), 3) прочитання (вимірювання) кінцевого стану. Квантовий регістр складається з L квантових бітів, що попарно взаємодіють. Квантовий біт — це дворівнева система, станами якої можна керувати за допомогою квантових вентилів (КЛЕ), які реалізуються зовнішніми полями. Квантовий регістр повномасштабного процесора повинен складатися з $L \approx 10^3 \div 10^5$ (а може і більше) квантових бітів. Його захищеність від декогеренції та неточності виконання квантових вентилів повинна бути такою, щоби ймовірність p появи похибки в одному квабіті була меншою від деякого порогового значення $p < p_p \approx 10^{-5} \div 10^{-6}$, тоді застосуванням відповідних квантових кодів і схем виправлення помилок можна забезпечити безпомилкове виконання квантових обчислень. Зауважимо, що наведені числа є наближеними і неостаточними.

Тоді ж було створено кілька квантових алгоритмів (квантове перетворення Фур'є, алгоритм факторизації Шора, алгоритм пошуку Гровера та ін.), які виконуються за час, що поліномно залежить від довжини вхідного слова, тоді як відповідні класичні алгоритми мають експонентну залежність. Створення ефективних квантових алгоритмів є складними та ресурсно затратними задачами і, мабуть, брак остаточної ясності в можливості фізичної реалізації квантового процесора гальмує роботи в цьому напрямі.

Наприкінці 1990 — на початку 2000 років в працях Вандерси-

пена (Vandersypen L.M.K.) зі співавторами на квантовому процесорі на ЯМР у рідинах (із числом квабітів $L \approx 2 \div 7$) було реалізовано відомі на той час квантові алгоритми, чим і підтверджено достовірність теоретичних досліджень та принципову можливість побудови квантового процесора. Однак проект цього процесора виявився тупиковим, оскільки його регістр не може бути масштабований через експонентне за числом квабітів загасання сигналу.

Грубі оцінки часів когерентності та кількості операцій у деяких фізичних системах. (Взято з [11])

Система	τ_K	$\tau_{\text{оп}}$	$n_{\text{оп}}$
Спін ядра	$10^{-2} \div 10^{8}$	$10^{-3} \div 10^{-6}$	$10^{5} \div 10^{14}$
Спін електрона	10^{-3}	10^{-7}	10^{4}
Іонна пастка	10^{-1}	10^{-14}	10^{13}
Електрон – Au	10^{-8}	10^{-14}	10^{6}
Електрон – GaAs	10^{-10}	10^{-13}	10^{3}
Квантова точка	10^{-6}	10^{-9}	10^{3}
Оптичний резонатор	10^{-5}	10^{-14}	10^{9}
НВЧ резонатор	10^{0}	10^{-4}	10^{4}

Головною проблемою є фізична реалізація квантового процесора, тобто, побудова регістра як об'єднання квабітів, що задовольняє згадані вище умови, та створення пристроїв для виконання квантових вентилів. Фізичні квантові біти можна розділити на два типи — ті, які існують в природі (спіни, атоми, фотони та ін.) і ті, які може створити людина (напр. SQUID, квантові точки та ін.). Перші мають очевидну перевагу, оскільки володіють точно визначеними незмінними характеристиками і є ідентичними, тоді як людина може створити тільки макро–, нано–, мезоскопічні об'єкти, у яких не можна досягти точних значень відповідних параметрів, і ці параметри різняться для різних квабітів, що суттєво утруднює опис системи і побудову квантових вентилів.

Окрім розглянутих вище проектів квантових процесорів, було запропоновано декілька інших, з якими познайомимося нижче.

У 1998 р. Б.Кейн (B.Kane) запропонував модель **напівпровідникового ЯМР квантового процесора**, в якому квабіти формую-

ться станами ядерного і електронного спінів стабільних атомів ізотопу фосфору ^{31}P, поміщених в кристал безспінового ізотопу кремнію ^{28}Si поблизу поверхні. Атоми фосфору утворюють певну регулярну структуру, в якій найближчі сусіди взаємодіють через електронні оболонки. На поверхню кристалу наносять тонкий шар діелектрика, а поверх нього над кожним атомом фосфору напилюють металевий електрод. Увесь кристал уміщують в зовнішнє магнітне поле. Змінювати стани квабіта пропонують поданням на електроди електричного поля. Хоча експериментально вдалося досягти дуже великого часу когерентності квабітів навіть при кімнатній температурі, однак проблеми керування станами і забезпечення взаємодії між квабітами, а також ініціалізація та вимірювання кінцевих станів є дуже складними. Складним є також обладнання для виконання всіх цих операцій. Однак дослідження в цьому напрямі тривають. (Детальніше див. [15]).

Запропоновано також проект **квантового процесора на оптичних фотонах**, у якому квабіт формується станами поляризації фотона чи його перебуванням у різних резонаторах (наприклад, $|10\rangle \equiv |0\rangle$ — фотон у першому резонаторі, $|01\rangle \equiv |1\rangle$ — фотон у другому резонаторі). Фазообертач (прозора плоскопаралельна пластина) змінює фазу фотона, тобто, здійснює поворот $Z(\varphi)$ квабіта навколо осі z. Світлоподільник (напівпрозоре дзеркало) виконує поворот $Y(\theta)$ навколо осі y. Взаємодія двох фотонів у нелінійному середовищі Керра дає змогу реалізувати двоквабітовий вентиль $\mathbf{B}(\pi)$ і таким чином утворити базисний набір квантових вентилів. Оскільки нелінійна складова коефіцієнта заломлення середовища Керра є досить мала, то для виконання вентиля $\mathbf{B}(\pi)$ фотони повинні пройти в ньому значну віддаль, а це призводить до збільшення ймовірності їхнього поглинання, а ці труднощі не вдається подолати.

Їх пропонують обійти використанням замість середовища Керра **квантовоелектродинамічного оптичного резонатора**, який утворюється дворівневим атомом, поміщеним в інтерферометр Фабрі-Перо. Багатократне відбивання фотона в інтерферометрі створює високе електричне поле (насправді — високу ймовірність зустрічі з цим фотоном). Одночасна взаємодія двох фотонів з атомним електроном дає змогу, як і в попередньому випадку, реалізувати

двоквабітовий вентиль $\mathbf{B}(\pi)$. Для збільшення ймовірності фотон-фотонної взаємодії необхідно збільшити константу зв'язку атома з полем, а це призводить до швидкого зменшення часу когерентності стану атома, тобто, і когерентності самих фотонів. (Детальніше див., напр. [11]).

Є кілька проектів процесорів (див., напр. [15]), в яких квабіт формується станами електрона в **квантових точках**. В одному з них, запропонованому Т.Танамото в 1999 р., електрон може перебувати в двох різних за розміром квантових точках: більшій з меншою енергією і в меншій із більшою енергією. Електрон може переходити між цими квантовими точками, тунелюючи крізь низький бар'єр. Діючи локально на цей квабіт електричним полем, можна керувати його станом, двоквабітові операції здійснюють, використовуючи кулонівську взаємодію електронів з різних пар квантових точок (квабітів). В іншому варіанті процесора на квантових точках квабіт пропонують формувати станами електронного спіна, якими керують магнітним полем. Недоліком процесорів на квантових точках є дуже малий час когерентності, викликаний далекосяжним характером електричного поля електрона. (Детальніше див. [15]).

Проблема фізичної реалізації квантового процесора є серйозним викликом, який зумовив глибокі наукові дослідження, що поступово розширюються. Зацікавилися цим і в бізнесових колах, зокрема, канадська фірма "D Wave" виготовила і продала не менше ніж два адіабатичні комп'ютери, складені з надпровідникових елементів. Наукові дослідження одного з них, виконані на замовлення компанії "Google", засвідчили, що в процесі його роботи відбувається квантовий процес тунелювання.

Вправи

До розділу 1

Матриці розглядаємо над полем комплексних чисел.

1. Знайти власні значення і власні вектори матриці густини одного спіну $s = 1/2$ $\boldsymbol{\rho} = \frac{1}{2}\left(\mathbf{I} + \vec{\mathbf{n}}\vec{\boldsymbol{\sigma}}\right)$ $|\vec{\mathbf{n}}| \leq 1$. Побудувати її спектральний розклад.
2. Нехай матриця $\mathbf{A}$ має період m, тобто, $\mathbf{A}^m = \mathbf{I}$. Знайти функцію $(\mathbf{I} - \alpha\mathbf{A})^{-1}$ як поліном від $\mathbf{A}$.
3. Нехай $\mathbf{P}^2 = \lambda\mathbf{P}, 0 < |\lambda| < 1$, знайти $(\mathbf{I} - \mathbf{P})^{-1}$ і $e^{\alpha\mathbf{P}}$.
4. Нехай існує функція $f(\mathbf{A})$, показати, що $f(\mathbf{V^{-1}AV}) = \mathbf{V^{-1}}f(\mathbf{A})\mathbf{V}$.
5. Для довільної матриці $\mathbf{A}$ розміру 2×2 знайти всі квадратні корені, тобто, матриці $\mathbf{S}$, для яких $\mathbf{S}^2 = \mathbf{A}$. Для яких $\mathbf{A}$ матриця $\mathbf{S}$ буде ермітовою? Чи всі корені ермітової матриці будуть ермітовими?
6. Записати вираз найзагальнішої унітарної 2×2 матриці. Чи всі корені унітарної матриці будуть унітарними? В чому виявляється відмінність?
7. Знайти всі квадратні корені одиничної 2×2 матриці.
8. Скільки коренів нормальної матриці $\mathbf{A}$ розміром $N \times N$ можна збудувати скориставшись правилом (1.17)? Скільки серед них буде ермітових? Для яких матриць?
9. Знайти власні значення матриці $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Для дійсних a, d встановити умови, за яких: власні значення дійсні, додатні, рівні, одне з них дорівнює нулю, комплексно спряжені.
10. Знайти вираз для $e^{\alpha\mathbf{A}+\beta\mathbf{B}+\gamma\mathbf{C}}$ коли $\mathbf{A}^2{=}\mathbf{B}^2{=}\mathbf{C}^2{=}\mathbf{I}$, а також:

$$\mathbf{AB}+\mathbf{BA}=\mathbf{AC}+\mathbf{CA}=\mathbf{CB}+\mathbf{BC}=\mathbf{0}.$$

Як зміниться результат при чисто уявних параметрах α, β, γ? Знайти відповідні гіперболічні і тригонометричні функції від цієї суми операторів.
11. Спростити оператор $(\mathbf{I}{-}(\alpha\mathbf{A}{+}\beta\mathbf{B}{+}\gamma\mathbf{C}))^{-1}$ за умов попередньої задачі.
12. Знайти вираз для $e^{\alpha\mathbf{A}+\beta\mathbf{B}+\gamma\mathbf{C}}$ коли $\mathbf{A}^2{=}\mathbf{B}^2{=}\mathbf{C}^2{=}\mathbf{I}$, а оператори $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ взаємно комутують при дійсних і уявних параметрах.

До розділу 2

1. У просторі станів спіну $1/2$ знайти матриці поворотів $\mathbf{X}(\varphi)$, $\mathbf{Y}(\varphi)$, $\mathbf{Z}(\varphi)$ навколо відповідних осей і застосувати їх до всіх матриць Паулі, вибравши $\varphi = \pi/2$.
2. Розв'язавши рівняння на власні вектори і власні значення для матриць Паулі, побудувати унітарні оператори, які їх діагоналізують. Застосувати ці унітарні перетворення до інших матриць Паулі і порівняти з результатами попередньої задачі.
3. Знайти умови, за яких гамільтоніан

$$\mathcal{H}=J^x\boldsymbol{\sigma}_1^x\boldsymbol{\sigma}_2^x+J^y\boldsymbol{\sigma}_1^y\boldsymbol{\sigma}_2^y+J^z\boldsymbol{\sigma}_1^z\boldsymbol{\sigma}_2^z+J^{xy}\boldsymbol{\sigma}_1^x\boldsymbol{\sigma}_2^y+J^{yx}\boldsymbol{\sigma}_1^y\boldsymbol{\sigma}_2^x \\ -h_1\boldsymbol{\sigma}_1^z-h_2\boldsymbol{\sigma}_2^z$$

унітарним перетворенням $\mathbf{U}(\alpha)=e^{i\alpha\mathbf{I}\otimes\boldsymbol{\sigma}_2^z}$ можна звести до вигляду

$$\tilde{\mathcal{H}}=\tilde{J}^x\boldsymbol{\sigma}_1^x\boldsymbol{\sigma}_2^x+\tilde{J}^y\boldsymbol{\sigma}_1^y\boldsymbol{\sigma}_2^y+J^z\boldsymbol{\sigma}_1^z\boldsymbol{\sigma}_2^z-h_1\boldsymbol{\sigma}_1^z-h_2\boldsymbol{\sigma}_2^z.$$

Знайти значення параметра цього перетворення і параметри $\tilde{J}^x$ і $\tilde{J}^y$. Доведіть, що унітарні перетворення $\mathbf{U}(\alpha)e^{i\theta\mathcal{H}}\mathbf{U}^\dagger(\alpha)$ і $e^{i\theta\tilde{\mathcal{H}}}$ є еквівалентними.
4. Знайти координати вектора $\vec{n}$, поворот навколо якого на кут ε еквівалентний композиції (4.1), тобто,

$$\mathbf{R}(\vec{n},\varepsilon)=\mathbf{R}_z(\alpha)\mathbf{R}_y(\theta)\mathbf{R}_z(\beta).$$

5. Знайти ймовірність переходу із початкового стану $|c_i\rangle=|0\rangle$ у кінцевий стан $|a_j\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ при прямому проектуванні і при неселективному вимірюванні з проміжними станами $|b_1\rangle=|\psi_+(m)\rangle$, $|b_2\rangle=|\psi_-(m)\rangle$ означеними в (2.4).
6. Знайти оператор еволюції одного спіну у зовнішньому магнітному полі $\vec{B}=(b\sin\omega t, b\cos\omega t, B_0)$.

До розділу 3

1. До якого класу обчислюваних функцій належать функції, обчислювані на квантовому комп'ютері?
2. До якого класу складності належать арифметичні операції?
3. До якого класу складності належить алгоритм перетворення Фур'є на класичному комп'ютері?
4. Оцінити кількість операцій множення у разі обчислення визначника матриці $n\times n$, користуючись означенням, а також методом розкриття за елементами рядка. Якою буде ця величина у разі перетворенні матриці до трикутної форми? (див. [51])

5. Скільки операцій множення і ділення треба виконати у разі розв'язування системи n лінійних алгебраїчних рівнянь із n невідомими методом Гауса?
6. До якого класу складності належать алгоритми розв'язування системи n лінійних алгебраїчних рівнянь із n невідомими методом Гауса і методом Крамера?
7. Оцінити кількість обчислень функції $f(x)$ у процесі знаходження кореня рівняння $f(x) = 0$ методом половинного поділу з абсолютною похибкою ε на відрізку $[a, b]$? Як зміниться ця величина у процесі знаходження m коренів, рівномірно розміщених на цьому ж відрізку?

До розділу 4

1. Записати оператори $\mathbf{R}_y(\theta)$, $\mathbf{R}_z(\alpha)$ в зображеннях (4.2) і (4.3).
2. Записати оператор $\mathbf{W}(...)$ (4.1) в зображеннях (4.2) і (4.3).
3. Записати оператор $\mathbf{B}(\varphi)$ в зображеннях (4.2) і (4.3).
4. Записати матрицю суматора двох чисел із перенесенням у вищий розряд.
5. Згаданий у попередній задачі оператор записати в зображеннях (4.2) і (4.3).
6. Зобразити схему для вентиля Тоффолі з підрозділу (4.4) як добуток операторів.

До розділу 5

1. Наведіть приклади повних дискретних базисів квантових логічних елементів.
2. Скільки квантових вентилів потрібно для здійснення квантового перетворення Фур'є регістру з N квабітами?
3. Чи можна за допомогою квантового перетворення Фур'є знайти період функції?
4. Для чого призначений алгоритм Шора? До якого класу складності він належить?
5. За скільки кроків алгоритм Гровера знайде шукане число в квантовому регістрі довжини L? Чи є оператори Гровера унітарними?

До розділу 6

1. Доведіть, що композиція квантових перетворень в будь-якому каналі є перетворенням з цього ж каналу. Знайти ймовірність таких композицій у каналах із класичною помилкою, перекиданням фази і фазовою помилкою.
2. З огляду на те, що $\boldsymbol{\sigma}^z\boldsymbol{\sigma}^x = i\boldsymbol{\sigma}^y$, чи буде виконуватись співвідношення $\boldsymbol{\mathcal{E}}^z(\boldsymbol{\mathcal{E}}^x(\boldsymbol{\rho})) = \boldsymbol{\mathcal{E}}^y(\boldsymbol{\rho})$?

3. Чи можна композицією квантових перетворень $\mathcal{E}^x, \mathcal{E}^y, \mathcal{E}^z$ реалізувати помилку деполяризуючого каналу?
4. Нехай імовірність p у квантових перетвореннях $\mathcal{E}^x, \mathcal{E}^y, \mathcal{E}^z$ на кожному часовому кроці Δt дорівнює $p = \Gamma\Delta t$. Як зміниться матриця густини спіну $\boldsymbol{\rho} = \frac{1}{2}(\mathbf{I} + \vec{n}\vec{\boldsymbol{\sigma}})$ після m кроків за час $t = m\Delta t$ під впливом цих перетворень? Знайти границю $m \to \infty$. Як залежить енергія системи від часу, якщо її гамільтоніан $\mathcal{H} = -\hbar\omega\boldsymbol{\sigma}^z/2$?
5. Розв'язати попередню задачу для деполяризуючого каналу і каналу загасання амплітуди.
6. Розв'язати задачу (4) для каналу узагальненого загасання амплітуди.
7. В яких каналах система втрачає енергію, а в яких — ні? В яких каналах відбувається декогеренція?

До розділу 7

1. За допомогою формул (2.24) і (2.25) отримати вираз (7.15).
2. Знайти аналогічний вираз для $\boldsymbol{\sigma}_B^+(t) = (\mathbf{I}\otimes\boldsymbol{\sigma}^+)(t)$.
3. Знайти вирази для $(\mathbf{Y}^\dagger\otimes\mathbf{I})\boldsymbol{\sigma}_A^+(t)(\mathbf{Y}\otimes\mathbf{I})$ і $(\mathbf{I}\otimes\mathbf{Y}^\dagger)\boldsymbol{\sigma}_A^+(t)(\mathbf{I}\otimes\mathbf{Y})$.
4. Знайти вирази для $(\mathbf{Y}^\dagger\otimes\mathbf{I})\boldsymbol{\sigma}_B^+(t)(\mathbf{Y}\otimes\mathbf{I})$ і $(\mathbf{I}\otimes\mathbf{Y}^\dagger)\boldsymbol{\sigma}_B^+(t)(\mathbf{I}\otimes\mathbf{Y})$.
5. Знайти вирази для $(\mathbf{X}^\dagger\otimes\mathbf{I})\boldsymbol{\sigma}_A^+(t)(\mathbf{X}\otimes\mathbf{I})$ і $(\mathbf{I}\otimes\mathbf{X}^\dagger)\boldsymbol{\sigma}_A^+(t)(\mathbf{I}\otimes\mathbf{X})$.
6. Знайти вирази для $(\mathbf{X}^\dagger\otimes\mathbf{I})\boldsymbol{\sigma}_B^+(t)(\mathbf{X}\otimes\mathbf{I})$ і $(\mathbf{I}\otimes\mathbf{X}^\dagger)\boldsymbol{\sigma}_B^+(t)(\mathbf{I}\otimes\mathbf{X})$.
7. Вивести формули (7.20).
8. Вивести формули (7.21).

До розділу 8

1. Якими факторами можна досягти стабільності іонного ланцюжка в пастці Пауля?
2. Які коливні моди іонного кристалу в пастці Пауля використовують для формуванні двоквабітових вентилів?
3. Якою є умова виникнення осциляцій Рабі у дворівневому іоні? Якою є частота осциляцій Рабі?
4. В чому полягає наближення хвилі, що обертається?
5. Яким механізмом збуджуються коливання іонного ланцюжка в пастці Пауля?
6. Операціями якого типу $\mathbf{V}$ чи $\mathbf{U}$ формуються одноквабітові вентилі?
7. Вивести формули (8.12).

Додатки

А. Кронекерів добуток матриць

Тензорний добуток векторів і операторів лінійного простору в матричному зображенні реалізується прямим (кронекеровим) добутком матриць.

Прямим (кронекеровим) добутком матриць $\mathbf{A}$ і $\mathbf{B}$ називають матрицю, утворену за правилом:

$$\mathbf{A}\otimes\mathbf{B}=\begin{bmatrix} A_{11}\mathbf{B} & A_{12}\mathbf{B} & \dots & A_{1m}\mathbf{B} \\ A_{21}\mathbf{B} & A_{22}\mathbf{B} & \dots & A_{2m}\mathbf{B} \\ \vdots & & & \vdots \\ A_{n1}\mathbf{B} & A_{n2}\mathbf{B} & \dots & A_{nm}\mathbf{B} \end{bmatrix}.$$

З цього означення випливають такі властивості прямого добутку:

а) $(c\mathbf{A})\otimes\mathbf{B}=\mathbf{A}\otimes(c\mathbf{B})=c(\mathbf{A}\otimes\mathbf{B}), \qquad c\in\mathbb{C},$
б) $(\mathbf{A}+\mathbf{B})\otimes\mathbf{C})=\mathbf{A}\otimes\mathbf{C}+\mathbf{B}\otimes\mathbf{C},$
в) $\mathbf{A}\otimes(\mathbf{B}+\mathbf{C})=\mathbf{A}\otimes\mathbf{B}+\mathbf{A}\otimes\mathbf{C},$
г) $\mathbf{A}\otimes(\mathbf{B}\otimes\mathbf{C})=(\mathbf{A}\otimes\mathbf{B})\otimes\mathbf{C},$
д) $(\mathbf{A}\otimes\mathbf{B})^T=\mathbf{A}^T\otimes\mathbf{B}^T, \quad (\mathbf{A}\otimes\mathbf{B})^\dagger=\mathbf{A}^\dagger\otimes\mathbf{B}^\dagger,$
е) $\mathrm{Sp}(\mathbf{A}\otimes\mathbf{B})=\mathrm{Sp}(\mathbf{A})\,\mathrm{Sp}(\mathbf{B})$.
Відзначимо, що прямий добуток, загалом, не комутативний. Можна також довести, що для матриць відповідних розмірів виконується рівність:

$$(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})=\mathbf{AC}\otimes\mathbf{BD},$$

яка для матриць розміром $m\times m$ ($\mathbf{A}$) і $n\times n$ ($\mathbf{B}$) має такі наслідки:
а) $\mathbf{A}\otimes\mathbf{B}=(\mathbf{A}\otimes\mathbf{I}_n)(\mathbf{I}_m\otimes\mathbf{B}),$
б) $\det(\mathbf{A}\otimes\mathbf{B})=(\det\mathbf{A})^n(\det\mathbf{B})^m,$
в) якщо $\mathbf{A}$ і $\mathbf{B}$ неособливі, то $(\mathbf{A}\otimes\mathbf{B})^{-1}=\mathbf{A}^{-1}\otimes\mathbf{B}^{-1}$
г) якщо $\mathbf{A}_1,\dots,\mathbf{A}_k$ — матриці розміром $m\times m$, а $\mathbf{B}_1,\dots,\mathbf{B}_k$ — матриці розміром $n\times n$, то
$(\mathbf{A}_1\otimes\mathbf{B}_1)(\mathbf{A}_2\otimes\mathbf{B}_2)\cdots(\mathbf{A}_k\otimes\mathbf{B}_k)=(\mathbf{A}_1\mathbf{A}_2\cdots\mathbf{A}_k)\otimes(\mathbf{B}_1\mathbf{B}_2\cdots\mathbf{B}_k).$

Приклади:

1) Прямий добуток вектора-рядка на вектор-стовпець (і навпаки) є комутативний, зокрема для вектора-рядка $\mathbf{a} = \begin{bmatrix} a_1 & a_2 \end{bmatrix}$ і вектора-стовпця $\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$:

$$\mathbf{a} \otimes \mathbf{b} = \begin{bmatrix} a_1 & a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 b_1 & a_2 b_1 \\ a_1 b_2 & a_2 b_2 \end{bmatrix},$$

$$\mathbf{b} \otimes \mathbf{a} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \otimes \begin{bmatrix} a_1 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 b_1 & a_2 b_1 \\ a_1 b_2 & a_2 b_2 \end{bmatrix}.$$

2) Для квадратних матриць 2×2:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix}.$$

Нехай $\varphi(x, y)$ деякий многочлен від x, y з комплексними коефіцієнтами c_{ij}

$$\varphi(x, y) = \sum_{i,j} c_{ij} x^i y^j,$$

а $\mathbf{A}$ і $\mathbf{B}$ — матриці $m \times m$ і $n \times n$ відповідно. Якщо $\lambda_1 \ldots \lambda_m$ і $\mu_1 \ldots \mu_n$ їхні відповідні власні значення, то власними значеннями функції

$$\varphi(\mathbf{A}, \mathbf{B}) = \sum_{i,j} c_{ij} \mathbf{A}^i \otimes \mathbf{B}^j$$

будуть mn чисел $\varphi(\lambda_k, \mu_l)$ [46]. Зокрема, для функції $\varphi(\mathbf{A}, \mathbf{B}) = \mathbf{A} \otimes \mathbf{B}$ власними будуть mn чисел $\lambda_k \mu_l$. Для функції $\varphi(x, y) = x + y$ відповідна матрична функція матиме вигляд

$$\varphi(\mathbf{A}, \mathbf{B}) = \mathbf{A} \otimes \mathbf{I}_n + \mathbf{I}_n \otimes \mathbf{B},$$

її ж власними значеннями будуть mn чисел $\lambda_k + \mu_l$ з власними функціями $|a_k\rangle \otimes |b_l\rangle$, де $|a_k\rangle$ і $|b_l\rangle$ — відповідні власні функції операторів $\mathbf{A}$ і $\mathbf{B}$. Матрицю $\varphi(\mathbf{A}, \mathbf{B})$ називають кронекеровою сумою матриць $\mathbf{A}$ і $\mathbf{B}$.

Б. Шифрування. Криптосистема RSA

Захист важливої інформації (військової, дипломатичної, комерційної та ін.) від третіх осіб (суперників) завжди був життєво важливою задачею. За тисячолітню історію винайдено багато способів перетворення інформації (шифрування) до виду, з якого її неможливо отримати без знання таємного ключа. Найнадійнішою на сьогодні вважається система з цілком випадковим ключем одноразового використання. Ця система могла б працювати так: текст перетворюють у двійкову форму T, потім генерують випадкову двійкову послідовність (ключ) K тієї ж довжини, що і текст у двійковій формі. До T побітово додають за модулем 2 ключ K. Отриманий зашифрований текст S легко розшифрувати, повторно додаючи ключ K до S, але без знання ключа розшифрувати S неможливо. Принципові практичні труднощі застосування цієї схеми полягають у складності генерування чисто випадкових ключів, а також у передаванні їх адресату. Тому подібні методи використовують тільки для дуже важливої інформації. Для шифрування не дуже важливої інформації, а також інформації, таємність якої є актуальною протягом певного часу, використовують методи шифрування, які у процесі дешифрування потребують розв'язування задач, алгоритми яких є експонентно складними [21]. До них, зокрема, належать системи з відкритим ключем.

Серед найпоширеніших сьогодні систем шифрування з відкритим ключем є RSA.

Система шифрування RSA була запропонована 1977 року Рональдом Райвестом, Аді Шаміром та Леонардом Адлеманом. (Однак, пізніше виявилося, що таку систему шифрування спецслужби Великобританії створили наприкінці 60-х років.)

Вибирають два великі прості числа p і q. Для їх добутку $N = pq$ значення функції Ойлера дорівнює

$$\phi(N) = (p-1)(q-1).$$

Далі випадково вибирають елемент e, що не перевищує значення $\phi(N)$ і є взаємно простим з $\phi(N)$. Після цього за алгоритмом Евкліда знаходять обернений елемент d

$$ed \mod \phi(N) = 1.$$

Тоді приймають $\{e, N\}$ — відкритий ключ, d — закритий (таємний) ключ. Інформація зашифровується конфідентами, яким власник таємного ключа d надав відкритий ключ $\{e, N\}$. Шифрування виконують у кілька кроків: спочатку текст переводять у цифрову форму (наприклад, літерам алфавіту зіставляють їх порядкові номери), тоді розділяють на

блоки довжини m, такої щоб $2^m < N$. Тоді кожен із блоків вважають числом B_j, над яким виконують операцію $E(B_j) = B_j^e \mod N$. Зашифровану в такий спосіб інформацію відкрито надсилають власнику таємного ключа, оскільки тільки він може її дешифрувати у такий спосіб:

$$E(B_j)^d \mod N = (B_j^e \mod N)^d \mod N = B_j,$$

тобто виконанням оберненої до шифрування операції. Несанкціонований доступ може отримати той, хто зуміє знайти число Ойлера для N, тобто, факторизувати число N, але це складна задача, оскільки числа p і q вибирають достатньо великими.

Відомо такий алгоритм пошуку співмножників складеного числа N. Вибираємо просте число $a < N$ і будуємо послідовність $a^j \mod N$, $j = 0, 1, 2, \ldots$. Визначаємо період цієї послідовності r. Одним із співмножників числа N буде серед найбільших спільних дільників чисел N, $(a^{r/2} \mod N) + 1$ і $(a^{r/2} \mod N) - 1$. Складною задачею тут є визначення періоду r, бо якщо період відомий, то знаходження найбільших спільних дільників чисел N і $(a^{r/2} \mod N) \pm 1$ за допомогою алгоритму Евкліда є задачею поліномної трудності для класичного процесора.

Розгляньмо процес факторизації числа N=21 на прості множники 3 і 7. Для цього виберімо просте число менше від N=21, наприклад a=5, і побудуймо послідовність $a^j \mod N$, $j = 0, 1, 2, \ldots$. Отримаємо послідовність: $1, 5, 4, 6, 2, 3, 1, 5, 4, 6, 2, 3, \ldots$ з періодом $r = 6$, що дає змогу знайти $a^{r/2} \bmod N = 6$, а також $(a^{r/2} \bmod N) + 1 = 7$, $(a^{r/2} \bmod N) - 1 = 5$. Співмножники числа 21 є серед найбільших спільних дільників чисел 21, 7 і 5, яким є число 7, а другий співмножник отримують діленням, що дає число 3.

Список літератури

[1] *Вакарчук І.О.* Квантова механіка/І.О. Вакарчук// Львів: ЛНУ імені Івана Франка, 2007.—848 с.

[2] *Юхновський І.Р.* Основи квантової механіки/ І.Р. Юхновський// Київ: Либідь, 2002.—392 с.

[3] *Дирак П.А.М.* Принципы квантовой механики/ П.А.М. Дирак //Москва: Наука, 1979.—481 с.

[4] *Нейман Й.* Математические основы квантовой механики/ Й. Нейман//Москва: Наука, 1964.—367 с.

[5] *Кемпфер Ф.* Основные положения квантовой механики/ Ф. Кемпфер// Москва: Мир, 1967.—391 с.

[6] *Садбери А.* Квантовая механика и физика элементарных частиц/ А. Садбери// Москва: Мир, 1989.—488 с.

[7] *Блохинцев Д.И.* Основы квантовой механики/ Д.И. Блохинцев// Москва: Наука, 1976.—664 с.

[8] *Блум К.* Теория матрицы плотности и ее приложения / К.Блум// Москва: Мир, 1983.—248 с.

[9] *Ткачук В.М.* Фундаментальні проблеми квантової механіки/ В.М.Ткачук//Львів: ЛНУ імені Івана Франка, 2011.—144 с.

[10] *Прескилл Дж.* Квантовая информация и квантовые вычисления/ Дж. Прескилл// Т.1— Москва-Ижевск: РХД, 2008.— 464 с.

[11] *Нильсен М.* Квантовые вычисления и квантовая информация/ М.Нильсен, И.Чанг// Москва: Мир, 2006.—824 с.

[12] *Хорн Р.* Матричный анализ/ Р.Хорн, Ч.Джонсон// Москва: Мир, 1989.—655 с.

[13] *Беллман Р.* Введение в теорию матриц/ Р.Беллман// Москва: Наука, 1969.—307 с.

[14] *Китаев А.* Классические и квантовые вычисления/А.Китаев, А.Шень, М.Вялый// Москва: МЦНМО ЧеРо, 1999.—111 с.

[15] *Валиев К.А.* Квантовые компьютеры: надежды и реальность/ К.А. Валиев, А.А. Кокин// Москва-Ижевск: РХД, 2001.— 352 с.

[16] *Прескилл Дж.* Квантовая информация и квантовые вычисления/ Дж. Прескилл// Т.2— Москва-Ижевск: РХД, 2011.— 312 с.

[17] *Кайе Ф.* Введение в квантовые вычисления/ Ф.Кайе, Р.Лафламм, М.Моска//Москва-Ижевск: РХД, 2009.–338 с.

[18] Математическая энциклопедия. Т.1. Москва: Советская энциклопедия, 1977.—1152 с.

[19] *Катленд Н.* Вычислимость. Введение в теорию рекурсивных функций/ Н. Катленд// Москва: Мир, 1983.—256 с.

[20] *Манин Ю.И.* Вычислимое и невычислимое/ Ю.И.Манин// Москва: Советское радио, 1980.—128 с.

[21] *Вербіцький О.* Вступ до криптології/ О.Вербіцький// Львів: ВНТЛ, 1998.—248 с.

[22] *Клакович Л.М.* Теорія алгоритмів/ Л.М. Клакович, С.М. Левицька// Львів: ЛНУ імені Івана Франка, 2015.—162 с.

[23] *Поплавский Р.П.* Термодинамические модели информационных процессов/ Р.П.Поплавский//Усп. физ. наук.—1975.—**115**, №3.—С. 465.

[24] Компьютеры. Справ. руков. в 3 томах. Под ред. Г.Хелмса. Т.1. Москва: Мир, 1986.—416 с.

[25] *Agraval M.* Primes is in $\mathcal{P}$/ M.Agraval, N.Kayal, N.Saxena// Annals of Math.— 2004.— **160**.— P.781–793.

[26] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки/ Р.Блейхут// Москва: Мир, 1986.—576 с.

[27] *Питерсон У.* Коды, исправляющие ошибки/ У.Питерсон, Э.Уэлдон// Москва: Мир, 1976.—593 с.

[28] *Фейнман Р.Ф.* Квантовомеханические ВМ/ Р.Ф.Фейнман// Усп. физ. наук.—1986.—**149**, №8.—С. 671.

[29] *Vandersypen L.M.K.* Experimental quantum computation with nuclear spins in liquid solution/ L.M.K.Vandersypen// www.arXiv.org/ ph-quant/0205193.

[30] *Laflamme R.* Introduction to NMR Quantum Information Processing/ R.Laflamme at al// www.arXiv.org/ quant-ph/0207172.

[31] *Сликтер Ч.* Основы теории магнитного резонанса/ Ч.Сликтер// Москва: Мир, 1981.—448 с.

[32] *Эрнст Р.* ЯМР в одном и двух измерениях/ Р.Эрнст, Дж.Доденхаузен, А.Вокаун// Москва: Мир, 1990.—711 с.

[33] *D.F.V.James* Quantum dynamics of cold trapped ions, with application to quantum computation/ www.arXiv.org/ quant-ph/9702053.

[34] *Hughes R.J.* The Los Alamos trapped ion quantum computer experiment/ R.J.Hughes at al// www.arXiv.org/ quant-ph/9708050.

[35] *Schmidt-Kaler F.* Ground state cooling, quantum state engineering and study of decoherence of ions in Paul traps/ F.Schmidt-Kaler at al// www.arXiv.org/ quant-ph/0003096.

[36] *Лифшиц Е.М.* Статистическая физика./ Е.М.Лифшиц, Л.П.Питаевский// Ч.2. Москва: Наука, 1978.—448 с.

[37] *Де Жен П.* Сверхпроводимость металлов и сплавов/ П. Де Жен// Москва: Мир, 1968.—280 с.

[38] *Тинкхам М.* Введение в сверхпроводимость/ М.Тинкхам// Москва: Атомиздат, 1980.—312 с.

[39] *Омельянчук А.Н.* Квантовые когерентные явления в джозефсоновских кубитах/ А.Н.Омельянчук, Е.В.Ильичев, С.Н.Шевченко// Киев: Наукова думка, 2013.—168 с.

[40] *Orlando T.P., at al.* Superconducting persistent-current qubit. Phys.Rev.B.—1999.—**60**, №22.—P. 15398–15413.

[41] *Johnson M.W.* Quantum annealing with manufactured spins/ M.W.Johnson at al// Nature.—2011.—**473**.—P.194–198.

[42] *Geller M.R.* Quantum computing with superconductors I: Architectures/ M.R. Geller at al// www.arXiv/quant-ph/0603224.

[43] *Makhlin Yu.* Quantum-state engineering with Josephson-junction devices/ Yu.Makhlin, G.Schön, A.Shnirman// Rev. Mod. Phys.— 2001.— **73**.— №2.— P. 357–400.

[44] *Harris R.* Experimental demonstration of a robust and scalable flux qubit/ R.Harris at al// Phys. Rev. B.— 201.0— **81**.— 134510.

[45] *Harris R.* Compound Josephson-junction coupler for flux qubits with minimal crosstalk/R.Harris at al//Phys. Rev. B.–2009.–**80**.–052506.

[46] *Ланкастер П.* Теория матриц/ П. Ланкастер// Москва: Наука, 1978.—280 с.

[47] *Чу С.* Управление нейтральными частицами/ С.Чу// Усп. физ. наук.—1999.—**169**, №3.—С. 274-291.

[48] *Коэн-Тануджи К.Н.* Управление атомами с помощью фотонов/ К.Н.Коэн-Тануджи// Усп. физ. наук.—1999.—**169**, №3.—С.292-304.

[49] *Филипс У.Д.* Лазерное охлаждение и пленение нейтральных атамов/У.Д.Филипс//Усп. физ. наук.—1999.—**169**, №3.—С.305– 322.

[50] *Ровенчак А.А.* Фізика бозе–систем/ А.А.Ровенчак// Львів: ЛНУ імені Івана Франка, 2015.—128 с.

[51] *Шахно С.М.* Чисельні методи лінійної алгебри/С.М. Шахно// Львів: ЛНУ імені Івана Франка, 2007.—245 с.

Предметний покажчик

Навчальне видання

КРОХМАЛЬСЬКИЙ Тарас Євстахійович

Вступ до квантових обчислень

Навчальний посібник

Редактор	**Михайло Коперсако**
Комп'ютерна верстка	**Тарас Крохмальський**
Технічний редактор	**Світлана Сеник**
Формат 60×90 1/16	Умовн. друк. арк. 12.8
Наклад 200 прим.	Зам.

Львівський національний університет імені Івана Франка
вул. Університетська, 1, м. Львів, 79000

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників та розповсюджувачів
видавничої продукції
Серія ДК № 3059 від 13.12.2007 р.

Віддруковано у книжковій друкарні "Коло"
вул. Бориславська, 8, м. Дрогобич, Львівська обл., 82100

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників та розповсюджувачів
видавничої продукції
Серія ДК № 498 від 20.06.2001 р.