НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНИВЕРСИТЕТ УКРАЇНИ

«КИЇВСКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»

Інститут Прикладного Системного Аналізу

Кафедра Системного Проектування

Звіт з розрахунково-графічної роботи

З курсу

«Нанотехнології у інформаційних технологіях»

Виконала:

Студенка 3-го курсу

Групи ДА-81

Желєзнова В.С.

Київ – 2021

Завдання:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Назва теми | Література | Сторінки | Примітки |
| 10 | Bell states | [3] | 136 - 149 |  |

Література:

1. Nanoelectronics and Nanosystems . From Transistors to Molecular and Quantum Devices. KarZ F. Gaser Peter Glösekötter Jan Dienstuhl. © Springer-Verlag Berlin Heide1berg 2004
2. Explorations in Quantum Computing Colin P. Williams 2nd edition: © Springer-Verlag London Limited 2011 , pp 740
3. Quantum Computer Science An Introduction. N. David Mermi; Cambridge University Press, 2007, pp. 237
4. A First Introduction to Quantum Computing and Information.Bernard Zygelman : Springer International Publishing, 2018, pp243
5. Problems & Solutions in Quantum Computing & Quantum Information. Willi-Hans Steeb, Yorick Hardy : World Scientific Publishing Company,2004, pp. 262

6.1 Стан Белла (двохкубітовий стан)

У цій главі ми розглядаємо деякі елементарні теоретичні протоколи квантової інформації, які часто зустрічаються в контексті квантових обчислень, хоча вони також мають застосування в більш широкій області квантової обробки інформації. Оскільки вони використовують лише невелику кількість квантових бітів, всі вони принаймні в одній лабораторії, на відміну від будь-яких більш тривіальних і нетипових прикладів протоколів, які ми розглядали в попередніх розділах.

(6.1)

У більшості цих прикладів використовується стан переплутаних 2-х кубіт,

Цей стан можна призначити двом кубітам, кожен у стані , застосувавши до одного з них Адамара, а потім використовувати його як контрольний кубіт для cNOT (контрольоване заперечення), який націлений на інший (Рисунок 6.1 (а)):

(6.2)

Ми узагальнюємо (6.2), дозволяючи оригінальній парі непереплутаних кубітів знаходитись у будь-якому з чотирьох обчислювальних станів 2-х кубіт (Рисунок 6.1 (b)):

(6.3)

Оскільки чотири стани є ортонормованою множиною, а логічні елементи Адамара та cNOT є унітарними, чотири переплутані стани також є ортонормованою множиною, що називається базисом Белла для вшанування пам’яті фізика Джона С. Белла, який виявив у 1964 р. один із найнезвичайніших про переплутані стани 2-х кубіт. Ми розглядаємо потужну 3-кубітову версію теореми Белла в розділі 6.6.

Якщо ми перепишемо (6.3) як

(6.4)

і згадаємо, що **HX = ZH** і що або **Z** на контрольному кубіті, або **X** на цільовому кубіті комутується з cNOT, тоді маємо

(6.5)

як показано на рисунку 6.2. Це показує, що інші стани Белла отримані з перевернувши один з кубітів, змінивши + на -, або змінивши обидва. Звичайно, це також можна отримати безпосередньо з (6.3), дозволивши Адамару та cNOT діяти на кожен з чотирьох варіантів для пари *xy.*

Тепер ми розглянемо кілька простих протоколів, у яких важливу роль відіграють деякі або всі стани Белла (або, у розділі 6.6, їх узагальнення 3х кубіт).

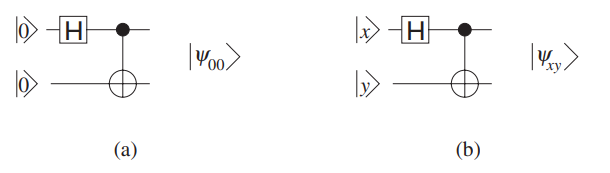


Рисунок 6.1

(a) Схема, яка створює заплутаний стан з незаплутаного обчислювально-базисного стану .

(b) Схема, яка створює чотири ортонормальні переплутані стани Белла з незаплутаного обчислювально-базисного стану .

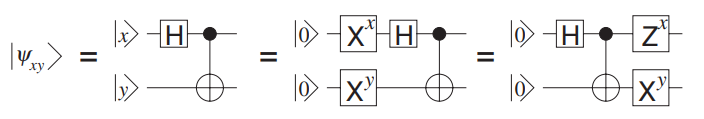


Рисунок 6.2

Стани Белла можна побудувати з шляхом перевертання одного кубіту, змінюючи знак з + на -, або виконавши обидві ці дії.

6.2 Квантова криптографія

За десять років до відкриття Шором, що квантові обчислення становлять загрозу для безпеки RSA шифрування, було відзначено, що кубіти (хоча цього терміну тоді не існувало) запропонували зовсім іншу і доказово надійну основу для обміну секретних повідомлень.

З усіх можливих застосувань квантової механіки для обробки інформації, квантова криптографія, мабуть, є найбільш перспективною щоб бути практичною технологією. Цьому є декілька причин. Перш за все, вона працює кубіт на кубіт. Єдиними відповідними логічними елементами є невелика кількість простих 1-кубітних логічних елементів. Взаємодія між парами кубітів, подібна до опосередкованих логічними елементами cNOT, не грає жодної ролі, принаймні в найпростіших версіях протоколу.

Крім того, у реальних реалізаціях квантової криптографії фізичні кубіти надзвичайно прості. Кожен кубіт – це один фотон світла. Стан кубіта – це стан лінійної поляризації світла. Якщо стани та описують фотони з вертикальною та горизонтальною поляризацією, то стани та описують фотони, поляризовані діагонально, або на 45°, або на -45° по вертикалі. Фотони в будь-якому з цих чотирьох поляризаційних станів можуть бути отримані різними способами, найпростіше (якщо не найефективніше), посилаючи слабкий промінь світла через відповідний орієнтований поляроїдний фільтр. Після підготовки фотона в його початковому поляризаційному стані, він немає необхідності в подальшому маніпулюванні, окрім як в підсумку виміряти його горизонтально-вертикальну або діагональну поляризацію, наприклад, направивши його через відповідним чином орієнтований двопроменезаломлюючий кристал і побачивши, в якому промені він виходить, або побачивши, чи проходить він через інший відповідним чином орієнтований поляроїдний фільтр. Фотони можна ефективно захистити від сторонніх взаємодій, направивши їх через оптичне волокно, де вони можуть переміщатися зі швидкістю світла зі зберіганням поляризації.

Цю процедуру можна розглядати як найпростіше можливе квантове обчислення. Спочатку кубіту присвоюється початковий стан, посилаючи його через 1-кубітові вимірювальні логічні елементи. Потім застосовуються або не застосовуються 1-кубітні унітарні логічні елементи (в залежності від того, чи повинне бути наступне вимірювання поляризації в тому самому напрямку, що і перше). І, нарешті, кубіт посилається через другий 1-кубітовий вимірювальний логічний елемент.

Користь легко переміщуваних одиночних кубітів для секретних комунікацій зрозуміла з одного важливого криптографічного факту: Аліса і Боб можуть мати невзламуваний код, коли вони сумісно використовують нещодавно створені ідентичні рядки випадкових бітів, названі одноразовими кодовими блоками. Якщо у них обох є такі однакові випадкові рядки, то Аліса може прийняти своє повідомлення у вигляді довгого рядка з нулів та одиниць, і перетворити його в побітову двомодульну суму (також названу ексклюзивною або XOR) з випадковим рядком нулів або одиниць тієї ж довжини, взятої з її одноразового кодового блока. Перевертання чи неперевертання кожного біта когерентного повідомлення в залежності від того, чи дорівнює відповідний біт випадкового рядка 0 чи 1, перетворює повідомлення в інший випадковий рядок. (Якщо це не очевидно, уявіть процес як перевертання чи не перевертання кожного біта випадкового рядка в залежності від того, чи дорівнює відповідний біт когерентного повідомлення 0 чи 1). Ніхто не може відновити вхідний рядок, не знаючи випадкового рядка, використаного для його кодування, тому тільки Боб може декодувати повідомлення. Він це робить шляхом застосування XOR до беззмістовного рядка з нулів та одиниць, отриманого від Аліси, зі своєю особистою копією випадкового рядка, яку вона використовувала для кодування. Рядок, який він отримує таким шляхом це , де M – повідомлення, S – випадковий рядок, а – закодоване повідомлення від Аліси. Оскільки , Боб відновлює вхідне повідомлення.

Проблема з одноразовими кодовими блоками полягає у тому, що їх можна використовувати лише один раз. Якщо підслуховуючий пристрій (Єва) отримує два повідомлення, закодованих одним і тим же блоком, то вона може взяти XOR двох закодованих повідомлень. Випадковий рядок, використаний для кодування двох повідомлень, випадає з процесу, залишаючи XOR двох незакодованих повідомлень. Але XOR двох змістовних повідомлень в поєднанні зі звичайними прийомами злому, заснованими на частоті букв, може бути використаний (з більшою точністю, ніж це потребується для одного повідомлення) для розділу та декодування обох текстів. Тому для забезпечення повної безпеки Аліса і Боб повинні постійно оновляти свій одноразовий кодовий блок новими ідентичними випадковими рядками бітів.

Проблема безпечного обміну такими випадковими рядками може здаватися ідентичною початковій проблемі обміну змістовними повідомленнями в безпечному режимі. Але в цей момент квантова механіка приходить на допомогу і надає цілковито безпечний засіб для обміну ідентичними послідовностями випадкових бітів. Зробіть паузу, аби насолодитися цією ситуацією. Ніхто ще не придумав, як використовувати квантову механіку, аби забезпечити безпечний засіб для прямого обміну змістовними повідомленнями. Безпечний обмін можливий лише тому, що послідовності бітів випадкові. На перший погляд можна подумати, що немає нічого більш даремного, ніж така передача інформації. Дивно те, що людська винахідливість в поєднанні з людською збоченістю змогла винайти умови, яких необхідність приховувати інформацію від третьої сторони фактично забезпечує ціль для такого даремного в інших випадках обміну випадкових рядків бітів.

Схема, що дозволяє це зробити, відома як BB84 за іменами її винахідників, Чарльза Беннета і Жиля Брассара, які опублікували цю ідею у 1984 році. Аліса посилає Бобу довгу послідовність фотонів. Для кожного фотона Аліса випадковим чином обирає тип поляризації фотона (горизонтально-вертикальний чи діагональний) і в рамках кожного типу випадковим чином обирає стан поляризації фотона – одне з двох ортогональних станів, пов’язаних з цим типом поляризації. На мові кубітів Аліса надсилає Бобу довгу послідовність кубітів, випадково обраних в одному з чотирьох станів: (поляризований горизонтально), (поляризований вертикально), (поляризований діагонально вздовж 45°) чи (поляризований діагонально вздовж -45°).

Повертаючись з мови фотонної поляризації до більш звичної нам квантово-обчислювальної мови, ми ділимо чотири рівновірогідних типи кубітів, які Аліса надсилає Бобу, на дві категорії: зі станом або , які ми називаємо кубітами типу-1, та станом чи , які ми називаємо кубітами типу-Н. По мірі надходження кожного кубіта Боб випадковим чином вирішує, чи відправити його безпосередньо через вимірювальні логічні елементи чи застосувати Адамара і тільки потім відправити його через вимірювальні логічні елементи. Ми називаємо ці два варіанти вимірюваннями типу-1 та типу-Н. Необхідно, аби кубіти індивідуально ідентифікувалися – наприклад, по послідовності їх надходження, - аби Аліса і Боб могли порівняти, що кожен з них знає про кожний.

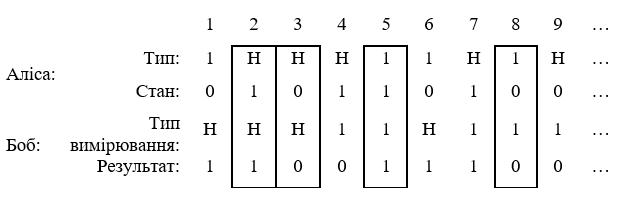
Коли Боб виміряв усі кубіти таким чином, Аліса повідомляє йому по незахищеному каналу, які з кубітів, які вона йому відправила, були типу 1, а які типу Н. Але вона не повідомляє, який з двох можливих станів вона підготувала в кожному типі: або для кубітів типу 1 та чи для кубітів типу Н. Для тих кубітів (приблизно половина з них), для яких випадковий вибір Боба типу вимірювання співпадає з випадковим вибором Аліси, Боб дізнається з результатів свого вимірювання фактично випадковий біт -0 або 1 – який Аліса йому відправила. Для тих кубітів (друга половина), для яких вибір типу вимірювання Боба не співпадає з вибором Аліси, результат його вимірювання повністю не корельований з вибором біту Аліси і нічого про нього не повідомляє. Це показано на рисунку 6.3.

Рисунок 6.3

Квантова криптографія. Для кожного кубіта, який вона посилає Бобу, Аліса випадковим чином вирішує, в якому типі стану його підготувати (тип **1** означає та тип **Н** означає ) і в якому стані цього типу (х = 0 або 1). Для кожного кубіту, отриманого ним від Аліси, Боб випадковим чином вирішує застосовувати (Н) чи ні (1) логічний елемент Адамара перед вимірюванням. В тих випадках (близько половини, обрамлені прямокутниками), для яких обраний Бобом тип вимірювання такий самий, як обраний Алісою стан, вони отримують ідентичні випадкові біти. Коли їх вибір відрізняється, вони не отримують корисної інформації.

Нарешті Боб повідомляє Алісі по незахищеному каналу зв’язку, які з кубітів він піддав зміні таким типом, який співпадає з її вибором типу – тобто які кубіти були такого типу, який забезпечує їх однакові випадкові біти. Вони відкидають некорисну половину своїх даних, для яких тип вимірювання Боба відрізнявся від типу, який підготувала Аліса. Потім, вони можуть побудувати свої одноразові кодові блоки з однакових рядків випадкових бітів, які вони отримали.

Ви можете дивуватися, чому Боб не чекає, аби вирішити який тип вимірювання виконати на кожному кубіті, доки він не дізнається, який тип фотона обрала Аліса, тим самим подвоюючи кількість співпадаючих випадкових бітів. Це могло б бути дійсно розумною стратегією, якщо б Боб міг зберігати кубіти, отримані від Аліси. Однак зберігати окремі фотони зі зберіганням поляризації достатньо складно. Для здійсненної квантової криптографії сьогодні, Боб повинен приймати рішення та вимірювати поляризацію кожного фотону по мірі надходження.

Причина, по якій Аліса випадковим чином варіює тип кубіта, який вона надсилає Бобу, є забезпечення безпеки від підслуховуючих пристроїв. Якби Аліса посилала всі кубіти одного типу, то підслуховуючий пристрій, Єва, могла б отримати ту саму інформацію, що і Боб, не будучи виявленим. Якби, наприклад, Аліса і Боб домовились, що усі кубіти будуть типу 1, а Єва би дізналася про це, вона могла б перехватити кожен кубіт до того, як він дійде до Боба, і послати його напряму через вимірювальний логічний елемент, не змінюючи його стану, а потім надіслати його (або інший кубіт, який вона підготувала в стані, який вона тільки-но дізналася) Бобу. Таким чином, вона також може отримати випадковий біт, який надсилає Аліса і який Боб у результаті отримує, коли робить своє вимірювання типу 1. Ніщо в протоколі не дасть Бобу підказки про те, що Єва прослуховує його. Але роблячи кожен кубіт таємно та випадково типу 1 чи типу Н, Аліса позбавляє Єву такої стратегії.

Найкраще, що може зробити Єва, як і Боб, це виконати вимірювання типу 1 чи типу Н випадковим чином. При цьому вона обов’язково виявляє свою присутність. Боб і Аліса можуть визначити, що Єва порушила безпеку їх бітів, пожертвувавши деякими ніби ідентичними випадковими бітами, які вони отримали з кубітів, що були оброблені однаковим чином. Вони беруть зразок цих бітів і перевіряють (по незахищеному каналу), чи дійсно вони співпадають, як ще було б при відсутності прослуховування. Якщо Єва перехоплює кубіти, довільно роблячи власні вимірювання типу 1 чи типу Н, перш ніж надіслати їх Бобу, то приблизно для половини корисних кубітів її вибір буде відрізнятися від спільного вибору Аліси і Боба. Приблизно в половині цих випадків втручання Єви призведе до того, що результат вимірювання Боба не буде співпадати з тим, що надіслала йому Аліса. Якщо, наприклад, Єва виконує вимірювання кубіта типу 1, який Аліса підготувала у стані , то вона обов’язково змінить його стан на один чи інший з двох станів або . У будь-якому випадку, якщо Боб виконає Адамара перед вимірюванням, він отримає результат 0 тільки в половині випадків.

Таким чином, якщо Єва систематично перехоплює кубіти, результат Боба не буде співпадати з вибором Аліси приблизно для четвертої частини їх вибірки. Це попереджує їх про те, що передача не була безпечною. Якщо усі дані вибірки будуть співпадати, за винятком крихітної частини, то вони можуть встановити верхню межу долі бітів, які Єва змогла перехопити, що дозволить їм зробити обґрунтоване судження про безпеку, з якою вони можуть використовувати біти, що залишились.

Чи зможе Єва впоратися з більш складною атакою, яка включає в себе перехват кожного кубіта Аліси та обробку його на квантовому комп’ютері, який відновлює його початковий стан, перш ніж відправити його Бобу? Це усунуло б можливість того, що її підслуховування буде розкрито Бобу. Але вимога, щоб кубіт Аліси був повернений в початковий стан, так же виключає можливість того, що Єва дізнається щось корисне, по причинам, схожим на попередній доказ теореми про відсутність клонування.

Нехай чотири можливих стани кубіта Аліси: , та . Нехай це початковий стан *n* кубітів в комп’ютері Єви, нехай **U** буде *(n+1)*-кубіт унітарне перетворення, яке комп’ютер виконує на своїх кубітах та кубітах Аліси. Оскільки кубіт Аліси повинен вийти з початкового стану, ми маємо

(6.6)

Єві доведеться розробити **U**, який дасть чотири , стани яких дозволять їй, шляхом подальшої обробки та вимірювання, отримати корисну інформацію про те, яке з чотирьох станів було. Але унітарні перетворення зберігають внутрішні добутки, тому

(6.7)

Так як та для , випливає що

(6.8)

Оскільки внутрішній добуток двох нормалізованих станів може дорівнювати 1, тільки якщо вони ідентичні, з (6.8) випливає що

(6.9)

Ціна, яку платить Єва за усунення усіх слідів підслуховування, полягає в тому, що результуючий стан її квантового комп’ютера не може нічого розповісти їй про чотири можливих стани кубіта Аліси.

Існує менш практична версія цього криптографічного протоколу, яка, на перший погляд, відрізняється, але залишається такою самою. Припустимо, що існує деякий центральне джерело, який виробляє пари кубітів у заплутаному стані

та потім відправили один член кожної пари Алісі, а інший – Бобу. Можна легко перевірити, що

(6.11)

(6.10)

тому якщо Аліса та Боб виконають вимірювання одного й того ж типу, вони отримають ідентичні випадкові результати.

Це може здатися навіть більш безпечним, ніж перший протокол, оскільки кубіти знаходяться в переплутаному стані до тих пір, доки Аліса та Боб не виконають вимірювання. Корельовані біти – результати вимірювання – навіть не існують до тих пір, доки не буде виконано вимірювання, а це не станеться, доки обидва кубіти не виявляться в безпеці в роздільному володінні Аліси та Боба. Но так відбувається тільки в тому випадку, якщо Єва не перехоплює кубіт. Якщо вона виміряє один біт до того, як він потрапить до Боба чи Аліси, то корельовані біти з’являться в момент її власного вимірювання. Це відбувається пізніше, ніж у першому протоколі (коли кожен біт існує з моменту вимірювання Аліси), але достатньо рано, аби допомогти Єві так само, як і раніше.

Якщо Аліса та Боб вирішили створювати свої ідеально корельовані випадкові біти, завжди виконуючи вимірювання типу 1, то якщо Єва дізнається про це, вона зможе перехопити одного з членів пари з допомогою власних вимірювань типу 1, передчасно розплутавши стан, але таким чином, що вона зможе дізнатися, що представляє собою кожен випадковий біт, не змінюючи при цьому ідеальної кореляції між значеннями, які Аліса та Боб будуть вимірювати згодом. Аліса і Боб можуть захиститися від цієї можливості, якщо кожен з них випадковим чином (і, обов’язково, незалежно) чергує вимірювання типу 1 та типу Н, а потім слідують процедурі, ідентичній тій, яку вони використовували, коли Аліса надсилала Бобу кубіти в певних станах.

Це повертає нас до початкового протоколу, який не використовував переплутані пари. Дійсно, якщо Аліса виміряє свій член переплутаної пари (роблячи чи вимірювання типу 1, чи вимірювання типу Н) до того, як Боб виміряє свій, це еквівалентно тому, що вона надсилає Бобу кубіт з випадково обраним станом, який їй відомо. Різниця лише у тому, що тепер випадковий вибір того, який з двох станів надіслати в рамках кожного типу, здійснюється не Алісою, що кидає монету, а основними законами квантової механіки, котрі гарантують, що результат її власного вимірювання є випадковим.

6.3 Бітова схема зобов’язань

Можна спробувати сформулювати аналогічний протокол для процедури, що називається бітовою схемою зобов’язань. Припустимо, що Аліса хоче переконати Боба у тому, що вона прийняла двійкове рішення до певної дати, але не хоче розкривати це рішення до деякого часу. Вона може зробити це, написав ТАК або НІ на карточці, поклавши карточку в коробку, зачинивши коробку на ключ та відправивши коробку, а не ключ, Бобу. Як тільки коробка опиниться в руках Боба, він може бути впевнений, що Аліса не змінила свого рішення, но доки ключ знаходиться у Аліси, вона може бути впевнена, що Боб не дізнався, яким було це рішення. Коли приходить час розкрити рішення, вона надсилає ключ Бобу, який відкриває коробку та дізнається, що це було за рішення.

Звичайно, Аліса може турбуватися про те, що Боб проникне до ящику іншими способами. Квантова механіка пропонує більш безпечну процедуру (але з екзотичною лазівкою, до якої ми повернемося у найближчий час). Аліса готує велику кількість *n* помічених кубітів. Якщо її відповідь «ТАК», то вона бере кожен кубіт, який випадковим чином знаходиться у стані або . Якщо її відповідь «НІ», то вона готує кожен кубіт випадковим чином у стані чи . У будь-якому випадку, вона записує, які кубіти знаходяться в якому стані, а потім надсилає їх Бобу, який зберігає їх таким чином, аби зберегти як і їх стан, так і їх мітки. (Як зазначалося вище, таке зберігання знаходиться за границями можливостей сучасної технології для поляризованих фотонів).

Якщо у Боба є набір з n кубітів, кожен з яких з рівною ймовірністю знаходиться в одному з двох ортогональних станів , то у Боба немає способу отримати підказку про те, які це два ортогональних стани. Якщо, наприклад, він змінює кожен кубіт, то ймовірність отримати 0 дорівнює

(6.12)

Але

(6.13)

оскільки це сума квадратів модулів амплітуд розкладання в ортогональному базисі, заданому :

(6.14)

Тому . Результати вимірювань Боба повністю випадкові, в незалежності від того, чим насправді є ортогональна пара станів.

У додатку Р показано, в більш загальному вигляді, що ніяка інформація, яку Боб може отримати зі свого набору кубітів, не може відрізнити випадок, в якому кожен з них має 50-50 шансів бути у стані або , від випадку, в якому кожен з них має 50-50 шансів бути у стані чи . Боб ніяк не може дізнатися вибір Аліси з кубітів, які Аліса надіслала йому. Він не може зламати замкнений ящик.

(Для неможливості Боба дізнатися вибір Аліси дуже можливо, що, незалежно від того, який цей вибір, вона надсилає йому набір кубітів, кожен з двох можливих станів обирається випадковим чином. Якщо, наприклад, вона надсилає йому рівно кубітів у стані та у стані в деякому випадковому порядку, то з вірогідністю 1 Боб отримає рівну кількість нулів та одиниць при вимірюванні в обчислювальному базисі. Але якщо він виконав перед вимірюванням, результат кожного вимірювання був би випадковим, і ймовірність отримання однакового числа нулів та одиниць при вимірюванні була б дуже мала (асимптотично при великих значеннях *n.* Тому, якби він отримав однакову кількість нулів та одиниць, він міг би бути впевненим, що Аліса надіслала йому фотони у станах та , а не у станах та ).

Коли приходить час Алісі повідомити про свій вибір пари ортогональних станів, вона каже Бобу приблизно наступне: «Моя відповідь була ТАК, тому кожен з кубітів, які я тобі надіслала, були або у стані , або у стані . Аби довести це, я зараз скажу тобі, що я помістила кубіти 1, 2, 4, 6, 7, , … у стан , а кубіти 3, 5, 8, 9, 10, 12, … у стан . Ти можеш підтвердити, що я кажу правду, виміряв кожен кубіт напряму».

Боб виконує прямі виміри та отримує кожен з передбачених Алісою результатів. Якби замість цього Аліса надіслала йому кубіти, стани яких були випадковим чином або , вона змогла би виконати той самий трюк, сказавши Бобу, що саме він виявить, якщо перед кожним зі своїх вимірювань буде використовувати логічний елемент Адамара. Але вона ніяк не зможе виконати цей трюк для вимірювань, яким передують логічні елементи Адамара в першому випадку чи для прямих вимірювань у другому випадку. Найкраще, що вона могла б зробити, якби вона хотіла би обдурити Боба, було б зробити випадкові припущення для кожного з n кубітів їй вдасться обдурити його тільки з ймовірністю . Таким чином, це працює відмінно, та без побоювання, що Боб володіє неочікуваними навичками зламу сейфів.

Але як відмічалося раніше, існує лазівка – фактично, фатальна проблема. Технологічні навички, необхідні для використання цієї лазівки, значно перевершують ті, які вимагаються для наївного протоколу, тому можна уявити собі відрізок часу в ті роки, десятиріччя чи навіть сторіччя, протягом якого наївний протокол може бути дійсно корисним. Але в підсумку він буде небезпечним. Припустимо, що Аліса, невідома Бобу, насправді підготувала n помічених пар у переплутаному стані (6.10), відправивши один з них Бобу, а інший залишила собі. Тоді кубіти, які отримує Боб, не будуть мати власних станів, будучи переплутаними з кубітами, які Аліса залишила собі. Тим не менш, якщо Боб вирішить перевірити деякі з них за допомогою вимірювань, (6.11) гарантує, що результати, які він отримає, не будуть відрізнятися від випадкових результатів, які він отримав би, якщо б Аліса грала чесно. Ніякого натяку на її обман не буде виявлено ні при якому випробуванні, які Боб може провести.

Але тепер, коли приходить час Алісі розкрити свій вибір, якщо вона хоче довести Бобу, що це було «ТАК», вона робить пряме вимірювання на кожному з кубітів, які вона зберегла, та прямо повідомляє Бобу, що він отримає, якщо зробить пряме вимірювання на кожному з парних кубітів. Але якщо вона хоче довести, що це було «НІ», вона застосовує Адамара перед вимірюванням кожного зі своїх кубітів, що дозволяє їй, завдяки тотожності (6.11), сказати Бобу, що він знайде, якщо також застосує Адамара перед вимірюванням своїх власних кубітів. Таким чином, вона може використовувати переплутані пари кубітів, аби обдурити, що в інакшому випадку було б цілковито безпечним протоколом фіксації бітів.

Аліса може обдурити таким же чином, навіть якщо Боб виміряє свої кубіти (випадковим чином застосовуючи чи не застосовуючи Адамара перед кожним вимірюванням) до того, як вона «розкриє» своє зобов’язання. Якщо вона хоче довести Бобу, що вона надіслала йому «ТАК», вона напряму виміряє кожен зі своїх кубітів та повідомляє Бобу усі свої результати. Він відмічає, що вони дійсно співпадають з усіма результатами, які він знайшов для своїх прямих вимірювань, та переконується, що вона дійсно надіслала йому «ТАК». Аби «довести», що вона надіслала йому «НІ», вона застосовує Адамара перед вимірюванням кожного зі своїх кубітів.

Звичайно, успіх обману Аліси в значній мірі залежить від того, що Боб знає усе про стани 1-кубіт, але ніколи не проходив курс квантової механіки, який навчив би його чомусь про переплутані стану 2-х кубітів. Якщо Боб настільки ж підкований у квантовій механіці, як і Аліса, вони обидва зрозуміють, що протокол фатально небездоганний, оскільки він може бути розрушений переплутаністю.

Саме у цьому контексті відома скарга Ейнштейна про «жахливі дії на відстані» здається доречною. За допомогою остаточного вимірювання своїх членів заплутаних пар, Аліса, здається, перетворює видалені кубіти, що знаходяться у Боба, в ті, як вона оманливо сказала, вона давно надіслала йому, зберігаючи при цьому до останньої хвилини можливість вибору одного з двох видів. Але, звичайно, дії Аліси залежать не стільки від кубітів, що знаходяться у Боба, скільки від того, що вона може сказати йому про те, що він може дізнатися з цих кубітів. Саме ця своєрідна напруга між тим, що є об’єктивним (онтологія) і тим, що відомо (епістемологія), робить квантову механіку таким джерелом захоплення (чи страждань) для філософськи налаштованих людей.

Щось подібне відкриттю Алісою цінності переплутування для омани фактично відбулося в історичному розвитку цих ідей про квантову обробку інформації. Коли вперше був запропонований описаний вище протокол фіксації бітів, було зрозуміло, що переплутані пари можуть бути використані для його руйнування, але були запропоновані більш складні версії, які, як вважалося, були невразливими для обману за допомогою переплутування. Виникли розбіжності щодо того, чи можливо розробити якусь форму передачі бітів, яка могла б бути безпечною, навіть якби переплутування було б повністю експлуатованим. Поточний консенсус полягає у тому, що не існує способу використовувати кубіти в протоколі фіксації бітів, який не може бути переможеним використанням переплутаних станів. Дійсно, було навіть висловлено припущення, що структура квантової механіки може бути однозначно визначена, якщо зажадати, аби вона дозволяла безпечний обмін випадковими рядками бітів, як у квантовій криптографії, але не дозволяла передачу бітів. Нікому не вдалося довести це. Однак здається неправдоподібним, що Бог прийняв би за основоположний принцип замислу те, що певні види таємної діяльності мають бути можливі, а інші – заборонені.

6.4 Квантове щільне кодування

Хоча для визначення стану одного кубіта необхідна нескінченна кількість інформації, немає ніякого способу для того, хто заволодів кубітом, дізнатися, що це за стан, як ми часто відмічали. Якщо Аліса підготує кубіт у стані і відправить його Бобу, все, що він зможе зробити, це використати унітарне перетворення по своєму вибору, а потім виміряти кубіт, отримавши значення 0 чи 1. Після цього стан кубіта буде чи , чи і ніякі подальші вимірювання не зможуть нічого дізнатися про його початковий стан . Найбільше, що Аліса зможе передати Бобу, відправивши йому один кубіт, - це один біт інформації.

Якщо, однак, Аліса має один член переплутаної пари кубітів у стані

(6.15)

а у Боба – інший, то підготувавши відповідним чином свій член пари та відправивши його Бобу, вона зможе передати йому два біти інформації. Для цього вона спочатку застосовує перетворення **1, X, Z** чи **ZX** до свого кубіта, в залежності від того, чи хоче вона надіслати Бобу повідомлення 00, 01, 10 чи 11. Якщо її кубіт зліва в (6.15), то вони перетворюють стан пари в один з чотирьох ортогональних станів Белла (6.5),

Тоді вона надсилає свій кубіт Бобу. Він посилає пару через керовані NOT логічні елементи , використовуючи кубіт, отриманий від Аліси, в якості керування, аби отримати

(6.17)

(6.16)

далі він застосовує перетворення Адамара, аби отримати

(6.18)

Вимірювання двох кубітів дає йому 00, 01, 10 чи 11 – саме те двохбітове повідомлення, яке хотіла передати Аліса.

Цей процес перетворення базису Белла назад в обчислювальний базис - тобто відміна процесу (6.3), за допомогою якого базис Белла був побудований з обчислювального базису – потім вимірювання – це і є процес вимірювання названий «вимірюванням в базисі Белла».

Можна безпосередньо продемонструвати, що це працює, за допомогою схем, не вдаючись до аналізу в (6.15) – (6.18). Припустимо, що Аліса представляє два біта *x* та *y*, які вона хоче передати Бобу, як стан обчислювального базису двох кубітів (два верхніх проводи, рисунок 6.4(а)). Якщо у Боба два кубіта від самого початку знаходяться у стані (два нижніх проводи на рисунку 6.4(а)), то схема на рисунку 6.4(а) отримає ці два біти для Боба простим класичним способом, перетворюючи стан справа у стан зліва шляхом прямого з’єднання кубіта з бітом через два cNOT переходи. Процедура містить тільки класичні операції над класично значущими станами. Вона отримує два біти від Аліси до Боба шляхом явної взаємодії між її кубітами та його. Вона буде працювати так само добре і для Cбітів.

Можна перетворити цю пряму класичну процедуру в більш екзотичний квантовий протокол, розширивши cNOT-вентилі у добуток квантових вентилів. Спочатку один із **С** вентилів розширюється у на рисунку 6.4(b). Оскільки **Z**, що діє на керуючий кубіт, комутує з **С** і оскільки **С** є його власною інверсією, ми можемо далі розширити рисунок 6.4(b) до рисунка 6.4(с). Далі ми можемо винести вентилі **Н** і **С** по обидві сторони від у крайні ліву та праву сторони, аби отримати рисунок 6.4(d) до трьох С-вентилів зліва на рисунку 6.4(е), оскільки дія будь-якого з цих наборів полягає у перевертанні цільового кубіта тоді і тільки тоді, коли обчислювально-базисні стани двох керуючих кубітів різняться, залишаючи при цьому стани керуючих кубітів незмінними. Оскільки стан інваріантний під дією **X**, **C** у крайній лівій частині рисунку 6.4(е) діє як тотожність, і рисунок 6.4(е) спрощується до рисунка 6.4(f).

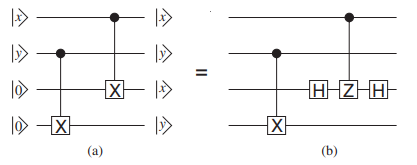
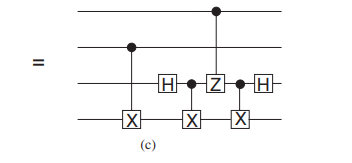
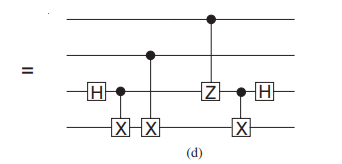
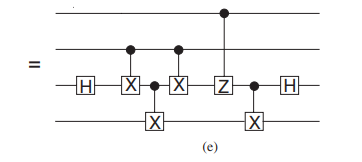


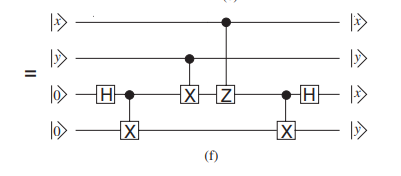
Рисунок 6.4

Теоретична схема виводу квантового протоколу щільного кодування









Той факт, що рисунок 6.4(f) має ту саму дію, що і рисунок 6.4(а), містить увесь зміст протоколу щільного кодування. Пара вентилів зліва на рисунку 6.4(f) діє на стан для отримання заплутаного стану (6.15). Нижній кубіт з цієї пари, кубіт 0, передається Бобу, а верхній, кубіт 1, передається Алісі, яка також володіє двома верхніми кубітами, кубітами 2 та 3. Пара вентилів діє як **1, X, Z** чи **ZX** на кубіт 1 в залежності від того, в якому стані знаходяться кубіти 3 та 2: . Це відтворює перетворення, яке Аліса застосовує до члена переплутаної пари, що знаходиться в її розпорядженні, в залежності від значень двох бітів, які вона хоче передати Бобу. Потім Аліса надсилає Бобу кубіт 1. Кінцева пара справа – це саме те перетворення (6.18), яке Боб застосовує до возз’єднаної переплутаної пари, перш ніж зробити своє вимірювання, яке дає значення *x, y*, які Аліса хотіла передати.

Подібно щільному кодуванню, більшість прийомів квантової теорії інформації, включаючи телепортацію, яку ми розглянемо далі, засновані на тому, що дві чи більше людини обмінюються переплутаними кубітами, підготовленими деякий час назад та ретельно зберігаються у віддалених місцях в очікуванні випадку для їх використання. Хоча підготовка переплутаних кубітів (у вигляді фотонів) та їх передача у віддалені місця була досягнена, поміщення їх у локальне довгочасне сховище, що зберігає переплутаність, залишається складною задачею.