Мирољуб Дугић

ОСНОВЕ КВАНТНЕ ИНФОРМАТИКЕ И КВАНТНОГ РАЧУНАЊА

Природно-математички факултет
Универзитет у Крагујевцу

Мирољуб Дугић

ОСНОВЕ КВАНТНЕ ИНФОРМАТИКЕ И КВАНТНОГ РАЧУНАЊА

Крагујевац 2009

„Информација је физичка“
Ролф Ландауер

ПРЕДГОВОР АУТОРА

Овај уџбеник *намењен је читаоцу који се* по први пут сусреће *са мултидисциплинарном облашћу квантне информатике и квантног рачунања. Избор тема је пао на оне које се не могу заобићи ни у једном приказу, са нагласком на приступ са становишта теоријске физике. Посебност текста лежи у инсистирању на важности самих основа квантне механике за област квантне информатике и квантног рачунања. У вези са тим посебна пажња поклоњена је темама квантног мерења, ансамбалском приступу квантне механике, те месту појма појединачног система у основама квантне механике. Релативно мањи број тема омогућује њихово детаљније, физичко и математичко, представљање са могућношћу проширења садржаја до нивоа професионалног, истраживачког рада заинтересованог читаоца. Ради растерећења текста и лакшег читања, неки детаљи (на пример, неки докази) дати су у додацима на крају текста, као и кроз задатке на крају сваког поглавља – неки од тих задатака су решени, а остали остављени за самостални рад, чиме ће читаоци моћи да провере своје разумевање и савладавање садржаја. Нису решени сви тежи задаци, а неки лаки задаци су решени – из „педагошких“ разлога. Текстови издвојени у оквирима (уоквирени) у главнини текста имају вишеструку сврху. Неки од њих служе као подсетници на садржаје који би читаоцу могли бити познати. Други, пак, издвајају важне ставове и исказе, док трећи (обично мањим фонтом) истичу неке детаље који се при првом читању могу заобићи.*

Прва три поглавља су уводна. Ту су дати основни појмови (и део формализма, посебно формализма квантне механике) који су од непосредног интереса за средишње теме обрађене у поглављима почев од Поглавља IV. *Ипак, текст је писан са намером да читалац не мора трагати по литератури за разјашњењем садржаја,* осим *ако се ради о амбициознијем читаоцу. Наравно, свака критика у овом смислу је добродошла.*

Повремена промена фонта текста који је уоквирен је смишљена као истицање посебно важних места у излагању. Намера аутора је да тиме обезбеди могућност брзог, површног читања само тих делова текста, а да читалац ипак може извући неке корисне информације на теме које се обрађују.

Од велике помоћи у коначном уобличењу овог уџбеника биле су сугестије и мишљење рецензената, др Дејана Раковића и др Владимира Цвјетковића. Пажљиво читање ранијих верзија текста и кометари мр Јасмине Јекнић-Дугић знатно су олакшале рад аутору. Свима њима желим да упутим изразе искрене захвалности. Наравно, за могуће, простале грешке и недостатке текста, аутор је једини одговоран.

У Крагујевцу,
лета Господњег 2009.

ПРЕСЕК САДРЖАЈА

за нестрпљиве

- ***Основна идеја.*** Стања квантног система („квантног хардвера“) користити као ***информатички ресурс***: манипулацијом стања обавити корисна информатичка процесирања.
- ***Основни постулат.*** Поступак (процес) ***квантног мерења*** обезбеђује ***класичну информацију*** о систему (на којем се обавља мерење). Ова информација се тиче података о вредностима физичких величина (опсервабли) и/или стања система.
- ***Општи став.*** Како год били конструисани и коришћени, класични рачунари неће моћи ефикасно да обављају извесне задатке, од којих су неки лаки за обављање помоћу квантних рачунара.

♣ ***Квантни информатички лимит*****:** Чак и када се о систему зна највише што се може, постоји неодређеност (неједнозначност) вредности неких величина (опсервабли) система – квантна неодређеност (релације неодређености).

♥ ***Квантна несепарабилност (сплетеност - entanglement)*****:** Подсистеми сложених (вишечестичних) квантних система не морају имати своја стања.

♦ ***Неважење следећих ограничења класичне информатике*****:**

(а) Разменом једног физичког бита може се разменити *највише један бит* информације.
(б) *Не постоји доказиво поуздан* протокол за размену „тајних кључева“ у протоколима криптографије.
(в) *Израчунавање факторизације великих бројева* и „*дискретног логаритма*“ захтева „*експоненцијално*“ време и/или хардвер.

♠ ***Квантни рачунари посебне сврхе*** рачунски лако ***симулирају сложене квантне системе***, зашта су (било каквом) класичном рачунару потребни експоненцијално велики временски ресурси.

СТРУКТУРА ТЕКСТА

Прва два поглавља су сасвим општа, уводна и намењена су основама теоријске информатике и квантне механике. Читаоци упознати са овим садржајима могу прећи на наредна поглавља којима започиње прави садржај квантне информатике. Треће поглавље је разрада теме мерења у квантној механици и представља унеколико засебан део, иако припада основама квантне механике.

Поглавља IV до VIII представљају неку врсту информатичког читања садржаја стандардног курса нерелативистичке квантне механике, са основним појмовима и припремом за наредна два поглавља. Девето поглавље се тиче неких специфичних квантно-информатичких задатака у ужем смислу теорије квантне информатике. Десето поглавље је посвећено само теми квантног рачунања.

Садржај је прилагођен следећим циљевима: (а) појмовном рашчишћавању информатичке анализе квантне механике, (б) истицању физичких основа разликовања класичне и квантне информације, (в) упознавању са основним протоколима квантне информатике у ужем смислу, (г) упознавању са основама квантног рачунања и елементарних, методских квантних алгоритама. Овиме је успостављена основа за дубље и шире упознавање са сложенијим садржајима чији се списак и садржај непрестано шири, а посебно са квантним протоколима и алгоритмима. Одређене области квантне информатике (као што су: *капацитет информатичког канала*, *поправке грешака* и *fault-tolerant рачунање*, *експериментална квантна информатика*) овде нису представљене, јер би то захтевало много више простора и скренуло пажњу са основа – које су главна тема текста. Коначно, већ сада, садржај свих области квантне информатике запрема читаву једну малу библиотеку која се непрестано обогаћује новим сазнањима. Отуда, као наставак на овај курс, препоручујемо књигу *M. A. Nielsen and I. L. Chuang,"Quantum Computation and Quantum Information"* (*Cambridge University Press, 2000, Cambridge, UK*), која је на нивоу последипломских студија те представља неопходно и незаобилазно штиво за све заинтересоване за професионални и истраживачки рад у области квантне информатике.

Посебна намена овог текста је да послужи као извор за студенте физике (мастер студије) који слушају наставу из предмета квантна информатика на ПМФ у Крагујевцу, али и као подршка сличним курсевима на Електротехничком факултету у Београду и на ПМФ у Нишу.

ОЗНАКЕ И СКРАЋЕНИЦЕ

$\delta_{ij} = \delta_{ji} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$ - *Кронекерова делта*

$\varepsilon_{ijk} \begin{cases} 0, \text{ било која два индекса међусобно једнака} \\ 1, \text{ цикличне пермутације индекса} \\ -1, \text{ антицикличне пермутације индекса} \end{cases}$ - *симбол Леви-Чивита*

$A_{ijk}B_{pjk} \equiv \sum_{j,k} A_{ijk}B_{pjk}$ - пример Ајнштајнове конвенције о сабирању

$\mu_B = e\hbar / 2mc$, e - наелектрисање и m -маса квантне честице, $\hbar = h / 2\pi$, h -Планкова константа, c -брзина светлости у вакууму,

Диракова симболика (нотација)

$|\psi\rangle$ - елемент Хилбертовог простора, стање квантног система

$\langle\psi|\chi\rangle$ - скаларни производ (стања) у Хилбертовом простору

$\hat{A}$ - оператор на Хилбертовом простору

$\langle\psi|\hat{A}|\chi\rangle$ - матрични елемент оператора $\hat{A}$

$W\left(\hat{A}, |\psi\rangle, [\alpha, \beta]\right)$ - вероватноћа да се мерењем опсервабле (ермитског оператора) $\hat{A}$, на ансамблу у стању $|\psi\rangle$, добије резултат у интервалу $[\alpha, \beta]$.

$\Delta\hat{A}$ - стандардно статистичко одступање опсервабле $\hat{A}$

$\hat{\rho}$ - статистички оператор („матрица густине“)

$|\Psi\rangle_{12}$ - стање двочестичног система (честице 1 и 2)

tr_i - „парцијални траг“ („интеграљење степени слободе“ i -те честице сложеног система)

Логичке операције

CNOT (или *XOR*) – искључиво ИЛИ

T - Операција $\pi / 8$

S ($S = T^2$) - Операција $\pi / 4$ - «фаза»

H - Адамарова (*Haddamard*) операција

$C - \hat{U}$ - контролисана (унитарна) операција $\hat{U}$

$X \equiv \hat{\sigma}_x, Y \equiv \hat{\sigma}_y, Z \equiv \hat{\sigma}_z$; $\hat{\sigma}_i$ - Паулијеви оператори

Неке скраћенице

акко – „ако и само ако“

BB84 – Bennett-Brasard криптиографски протокол

CNOT (или *XOR*) – *Controlled-NOT* (или *Exclusive OR*)

КДФТ – Квантни дискретни Фуријеов трансформ

POVM (*Positive Valued Operator Measure*)

ПСКО – потпун скуп компатибилних опсервабли

САДРЖАЈ

I ОСНОВНИ ПОЈМОВИ ТЕОРИЈСКЕ ИНФОРМАТИКЕ
1.1 Појам информације. Шенонова информација
1.2 Подела информатике и општи задаци
1.3 Појам бита и физичка имплементација
1.4 Појам спољашњег шума и корекција грешака
1.5 Појам рачунања и комплексност
1.6 Неки резултати класичне информатичке теорије
1.7 Неки мотиви за развој квантне информатике
1.8 Историјски осврт

II ОСНОВНИ ПОЈМОВИ КВАНТНЕ МЕХАНИКЕ
2.1 Класични фазни простор. Класична реалност
2.2 Основни постулати квантне механике
2.3 Дискусија постулата
2.4 Појам појединачног система
2.5 Релације неодређености
2.6 Принцип комплементарности
2.7 Постулат о квантизацији.
Постулат о степенима слободе
2.8 Унутрашњи степени слободе: Спин
2.9 Постулат о вишечестичним системима.
Паулијев принцип
2.10 Вишечестични систем спинова-1/2
2.11 Квантна динамика
2.12 Појам квантног мерења. Пројекциони постулат
2.13 Напомене и коментари

III КВАНТНА СТАЊА, АНСАМБЛИ И МЕРЕЊЕ
3.1 Општа схема квантних мерења.
Чисти и мешани анасамбли
3.2 Предиктивно мерење
3.3 Потпун скуп компатибилних опсервабли (ПСКО)
3.4 Придруживање стања ансамблу
3.5 Симултана мерења. Квантна неодређеност
3.6 Квантна мешана стања. Лиувилова једначина
3.7 Особине статистичког оператора
3.8 Промена стања услед мерења
3.9 Ансамбалско разликовање стања

IV КВАНТНО МЕРЕЊЕ И КЛАСИЧНА ИНФОРМАЦИЈА. ПРОБЛЕМ МЕРЕЊА
4.1 Квантна стања: класични информатички аспект
4.2 Препарација стања. Квантни информатички лимит
4.3 Проблем мерења
4.4 Различивост квантних стања

V КВАНТНА НЕОДРЕЂЕНОСТ. КВАНТНА НЕСЕПАРАБИЛНОСТ. КВАНТНА НЕЛОКАЛНОСТ
5.1 Класична неодређеност
5.2 Квантна неодређеност
5.3 Квантна несепарабилност (сплетеност –
quantum entanglement*).*
5.3.1 Квантне корелације (квантна несепарабилност)
5.3.2 Квантна нелокалност
5.3.3 Белова неједнакост
5.4 Проблем појединачног система
5.5 Напомена
5.6 Ансамбли* vs. *појединачни системи

VI НЕРАЗЛИЧИВОСТ НЕОРТОГОНАЛНИХ СТАЊА. *No-cloning* ТЕОРЕМ
6.1 Појам клонирања стања
6.2 No-cloning теорем
6.3 No-cloning ⇔ неразличивост неортогоналних стања
6.4 Важна напомена

VII УОПШТЕНА КВАНТНА МЕРЕЊА. ДЕЛИМИЧНА РАЗЛИЧИВОСТ НЕОРТОГОНАЛНИХ СТАЊА
7.1 Ортогонална (пројективна) мерења
7.2 Уопштена мерења
7.3 POVM мерење
7.4 Сводивост уопштених мерења на ортогонална мерења

VIII КЛАСИЧНА *vs.* КВАНТНА ИНФОРМАЦИЈА
8.1 Квантни паралелизам
8.2 Појам квантног бита (кубита)

IX ПРИМЕРИ КВАНТНОГ ИНФОРМАТИЧКОГ ПРОЦЕСИРАЊА
9.1 Квантна телепортација
9.2 Квантно супергусто кодирање

9.3 Квантна криптографија
9.3.1 Интуиција
9.3.2 Идеја
9.3.3 BB84 протокол без шума
9.3.4 Процена присуства Еве
9.3.5 Евине стратегије прикривања
9.3.6 Сигурност тајног кључа
9.4 Осврт

X ОСНОВЕ КВАНТНОГ РАЧУНАЊА
10.1 Појам рачунања. Комплексност
10.2 Појам универзалности рачунања. Реверзибилно рачунање
10.3 Црч-Тјурингова теза. Јака Црч-Тјурингова теза
10.4 Елементарни појам квантног рачунања
10.5 Једнокубитне трансформације
10.6 Двокубитне трансформације. Модел-кола квантног рачунања
10.7 Универзалност модела-кола квантног рачунања
10.8 Дефиниција квантног рачунања
10.9 Примери квантних алгоритама
10.9.1 Појам квантне црне кутије
*10.9.2 Дојчов (*Deutsch*) алгоритам*
*10.9.3 Дојч-Јоса (*Deutsch-Josza*) алгоритам*
*10.9.4 Сајмонов (*Simon*) алгоритам*
10.9.5 Квантни дискретни Фуријеов трансформ
10.9.6 Корисни алгоритми
10.10 Корекција грешака
10.11 Квантни хардвер
10.12 Алтернативни модели квантног рачунања

XI ИНФОРМАТИЧКА ФОРМУЛАЦИЈА ПРОБЛЕМА КВАНТНОГ МЕРЕЊА

XII КВАНТНИ ИНФОРМАТИЧКИ РЕСУРСИ
12.1 Врсте ресурса
12.2 Енергијски захтеви квантног информатичког процесирања

XIII НЕКИ КУРИОЗИТЕТИ КВАНТНЕ ИНФОРМАЦИЈЕ
13.1 Негативна условна ентропија
13.2 Квантни паралелизам: квантне грешке се не морају сабирати

13.3 Услови информатичке изолованости
13.3.1 Адијабатска информатичка изолованост
13.3.2 Декохеренцијом-индуковано суспрезање декохеренције
13.3.3 Информатичка локалност у трочестичном систему
13.3.4 Напомена
13.4 Питање „шта је систем“: информатички аспекти
13.5 Осврт

Додатак 1.1 *Размена сигнала брже од светлости*
Додатак 1.2 *Сводивост класичног реверзибилног рачунања на класично иреверзибилно рачунање*
Додатак 2.1 *Операције са матрицама и детерминантама*
Додатак 2.2 *Хилбертов простор и оператори на њему*
Додатак 2.3 *Релације неодређености: коментари*
Додатак 2.4 *Штерн-Герлахов експеримент*
Додатак 8.1 *Модели кубита*
Додатак 9.1 *Статистички нееквивалентни кубитови*
Додатак 9.2 BB84 *протокол са шумом*
Додатак 10.1 *О реверзибилном рачунању: дисипација енергије*
Додатак 10.2 *Изградња операције „корен из НЕ“*
Додатак 10.3 *О Шоровом алгоритму за факторисање великих бројева*
Додатак 10.4 *О Гроверовом алгоритму претраге базе података*
Додатак 10.5 *Стратегије борбе против декохеренције. Појам корекције грешака*

ЛИТЕРАТУРА

ИНДЕКС АУТОРА

ИНДЕКС ПОЈМОВА

I ОСНОВНИ ПОЈМОВИ ТЕОРИЈСКЕ ИНФОРМАТИКЕ

Теоријска информатика представља математичку и физичку основу *процесирања информација*. У овом кратком и наменском прегледу основа теоријске информатике нагласак је стављен на основне појмове и њихову повезаност, као и нека ограничења класичне теоријске информатике, а све у служби наредних поглавља посвећених основама квантне информатике. За више детаља мора се консултовати одговарајућа литература која је наведена у Оквиру ниже, као и на крају овог поглавља.

1.1 Појам информације. Шенонова информација

Информација је појам који се обично *не дефинише*. Овај појам потиче од свакодневних потреба које подразумевају његове различите употребе. У теоријској информатици отуда постоје и различите „врсте информација“: актуелна, алгоритамска, *Шенонова*, Фишерова, квантна.

Главни *задатак информатике* је *баратање информацијама* (процесирање информација) зашта се сматра да је, у зависности од контекста и/или конкретног задатка, интуитивно јасан појам. У вези са тим су и тумачења различитих *мера информације*. Може се рећи да је за све практичне потребе теоријска информатика заокружен систем искуства и знања.

Елементарни поступци ***кодирања*** (C) и ***декодирања*** (D) порука представљају поступке преписа порука у *формална* слова и речи. На пример, за кодирање слова ***а*** и ***б***, довољно је користити два симбола, два *формална слова*, означимо их са 0 и 1. Тако се кодирање и декодирање може представити:

$$\boldsymbol{а} \xrightarrow{C} 0, \quad \boldsymbol{б} \xrightarrow{C} 1 \tag{1.1}$$

$$0 \xrightarrow{D} \boldsymbol{а}, \quad 1 \xrightarrow{D} \boldsymbol{б}. \tag{1.2}$$

Скуп $\{0,1\}$, тзв. ***бит***, представља *формална слова* од којих се изграђују формалне реченице којима се кодирају жељене поруке. При томе се подразумева да обе (све) стране у комуникацији располажу истим поступцима кодирања и декодирања, за које важи $D = C^{-1}$.

За кодирање три слова, пак, од скупа формалних слова, 0, 1, потребно је повећати број комбинација нула и јединица, нпр.

$$\boldsymbol{а} \xrightarrow{C} 00, \ \boldsymbol{б} \xrightarrow{C} 01, \ \boldsymbol{в} \xrightarrow{C} 10, \tag{1.3}$$

што показује да је за кодирање три слова довољно $2^n = 3 \Rightarrow n = \log_2 3 = 1.58$ симбола (бита) у низу. Наравно, како је број симбола цео број, то је најмање потребно $n = \lceil \log_2 3 \rceil = 2$ симбола; средња заграда указује на најмањи цео број већи од вредности у загради.

Тако се за N слова која чине поруку захтева макар

$$n = \lceil \log_2 N \rceil \tag{1.4}$$

комбинација нула и јединица (формалних слова).

Сви поступци кодирања и декодирања имају исту, овде представљену *идеју*: пресликавања скупова нула и јединица једне дужине, у скупове нула и јединица, у општем случају, друге дужине. Тако се размена порука своди на размену и операције над скуповима формалних слова, формалних речи и реченица, што процесирању информације даје основу *универзалности* у примени.

У понечему, појам информације уопште, па и, тзв., Шенонове информације, није сасвим интуитиван. То је умногоме последица свакодневне чињенице да се исти појам (информације) везује за неке актуелне, текуће догађаје (као, нпр., да ли је *Партизан* победио *Црвену Звезду* са 3 према 0, или са 5 према 1). Теоријска информатика барата прецизним оперативним дефиницијама информације кроз *меру информације* каква је, на пример, тзв., *Шенонова ентропија* (видети оквир ниже). Отуда се у информатици мора опрезно ослањати на интуицију.

Нека је задатак размена садржаја „Горског Вијенца“ између две стране у комуникацији. Тада се његов садржај мора кодирати тиме што ће сва слова азбуке бити кодирана *формалним словима*, нпр., нулама и јединицама. Сходно изразу (1.4), за ово је потребно $n = \lceil \log_2 30 \approx 4.9 \rceil = 5$ нула или јединица. Поента лежи у чињеници да, у реалном комуницирању, није унапред познато која ће се реч (или реченица) у комуникацији појавити. Отуда размена (кодираних) порука има особину ***стохастичности*** – није унапред познато које формално слово, тј., низ формалних слова, ће бити употребљен. Комбинације формалних слова дају симбол x_i (Одељак 1.3), који се може појавити са неком вероватноћом p_i. Зато се каже да пошиљалац поруке представља *извор* поруке којег одликује *стохастичност*.

Посебан задатак за *велико* n је задатак *сажимања (формалних) порука*, чиме се врши уштеда у ресурсима – у броју коришћених нула и јединица. Овај задатак поставио је и решио Шенон (*Shannon 1948, Shannon and Weaver 1963*) у виду теорема који носе његово име. Испоставља се да величина која одређује најмањи број потребних нула и јединица за сажимање врло дугих порука (какав је „Горски Вијенац“) које се још *могу* успешно декодирати, означена са H, и која се назива ***Шенонова ентропија***, има облик:

$$H = -\sum_i p_i \log_2 p_i \tag{1.5}$$

где индекс i пребројава горње симболе x_i. Величина H се још назива и ***Шеноновом информацијом***.

Шенонова ентропија је ***мера (Шенонове) информације***, са два могућа (међусобно комплементарна) тумачења:

(а) H представља меру ***непознавања*** садржаја поруке ***пре*** очитавања поруке,

(б) H представља меру ***добијене*** *информације* ***после*** очитавања поруке.

Овде су очигледне следеће особине Шенонове информације: ако је садржај поруке *унапред познат*, тј., $p_{i_0} = 1$, док $p_i = 0, \forall i \neq i_0$, *нема* никакве *информације* - $H = 0$. А информација је максимална ако $p_i = const.$, што за број N симбола x_i даје $p_i = N^{-1}$, тј. $H = H_{\max} = \log_2 N$.

Формално, дакле, *информација* се представља као *стохастички извор слова*, и за фиксиран скуп слова (симболе x_i, за које се претпоставља да су унапред задати) се *представља скупом вероватноћа,* $\{p_i\}$, које дефинишу израз (1.5), са горе наглашеним тумачењима овог израза.

1.2 Подела информатике и општи задаци

Грубо говорећи, теоријска информатика се може поделити на *Информатику комуникација* и *Теоријско рачунарство*. Прва област подразумева задатке размене кодираних садржаја („информација“) између (макар) две стране, које се уобичајено означавају као *Алиса* и *Боб*. Поред кодирања и декодирања садржаја, средишњи задатак је корекција грешака услед, тзв., *спољашњег шума* (енгл.: *noise*), тј., сметњи које потичу из окружења, а које могу променити (кодирани) садржај размењених порука. Друга област представља математичку формулацију општег задатка *рачунања* (енгл.: *computing, computation*), што подразумева и поступке корекције грешака услед спољашњег шума. Средишњи део теорије рачунања је, тзв., теорија комплексности која се бави захтевима који се тичу *ресурса* неопходних за обављање одређеног израчунавања.

Информатички *ресурси* се могу поделити на *просторне*, *временске* и *енергијске*. Просторни ресурси обично подразумевају број *битова* (Одељак 1.3) неопходних за обављање одређене операције. Временски ресурси подразумевају време[1], T, неопходно за обављање одређене операције. Међусобна зависност ових ресурса, а у контексту датог информатичког задатка, је у средишту интереса теоријске информатике. Енергијски ресурси се тичу енергије потребне за практично обављање процесирања.

Поједностављено речено, теоријска информатика има следеће опште задатке:

(а) дефинисање поступака кодирања и декодирања садржаја порука које се желе разменити између страна у комуникацији,

(б) формулисање *поузданих поступака* за корекцију грешака услед спољашњег шума,

[1] Које се обично исказује бројем неопходних логичких операција.

(в) процену ресурса неопходних за обављање дате *класе* информатичких задатака, као и

(г) дефинисање ограничења информатичког процесирања с обзиром на расположиве информатичке ресурсе.

1.3 Појам бита и физичка имплементација

Математички модел ***бита*** представља скуп од два елемента који, по дефиницији, представљају домен логичких операција *Булове логике (и алгебре)*[2]. Ови елементи се обично означавају са $\{0,1\}$, те овај пар представља један бит информације. Скуп од n битова представља скуп од n нула или јединица. Дакле, у скупу од n битова, сваки бит представљен је једном вредношћу, ***или*** 0, ***или*** 1. У скупу од n битова постоји 2^n комбинација нула и јединица – што представља домен логичких операција за n битова.

Скуп симбола (домен вредности операција) за:

1 бит:
$x_0 = 0$
$x_1 = 1$

3 бита:
$x_0 = 000$
$x_1 = 001$
$x_2 = 010$
$x_3 = 011$
$x_4 = 100$
$x_5 = 101$
$x_6 = 110$
$x_7 = 111$

n битова:
$x_0 = 000...00$
$x_1 = 000...01$
$x_2 = 000...10$
...
$x_{2^n-1} = 111..11$

Свака порука се на једнозначан начин кодира одређеним низом нула и јединица из горе представљених скупова (симбола x_i), у зависности од броја неопходних битова. Прималац поруке мора бити у стању да прочита поруку, што

[2] Булову логику чине, нпр., операције И, ИЛИ, НЕ, итд.

се назива поступком декодирања. Укупан процес кодирања и декодирања мора бити такав да са *великом вероватноћом* омогућује поуздано комуницирање (процесирање информација) на скупу битова када се занемари утицај окружења, тј., спољашњег шума. У идеалном случају, за фиксирани симбол x_i из горњег оквира, фиксирана операција даје једнозначан резултат – детерминистички. При томе, саму информацију карактерише стохастичност (Одељак 1.1).

Класична теорија комуникација се заснива на појму *Шенонове ентропије* – Одељак 1.1 – са очигледном последицом: ако је реч x_i коју одашиље извор информација одређена са вероватноћом 1, тада примањем те речи (тј., поруке) *није примљена никаква информација*[3] ($H=0$). Отуда се од извора информација очекује да има ***стохастички излаз***, као и међусобну ***статистичку независност*[4] *битова у низу*** којима се порука имплементира. Ово је уједно и најважнија претпоставка модела која је од општег важења, како у класичној, тако и у квантној информатици.

Физички, имплементација битова мора испунити ове захтеве. Конкретно, *хардвер* мора бити тако изграђен да физички сигнали који се размењују морају испунити следеће захтеве: *различивост сигнала који имплементирају 0, тј., 1,* затим*, сигнали не смеју бити детерминистички*[5]*,* док *појединачни сигнали у низу морају бити међусобно стохастички независни*. *У пракси* је довољно да ови захтеви буду макар приближно испуњени.

У зависности од задатка, од интереса су и друге врсте ентропије, тј., информације, изграђене на основи Шенонове ентропије, које су представљене у оквиру ниже – без доказа, с обзиром да их ми нећемо користити.

Нека су задате три варијабле, X, Y, Z, представљене скуповима одговарајућих вредности (симбола), $\{x_i\}, \{y_j\}, \{z_k\}$, редом. Тада се могу увести следеће величине.

- Заједничка ентропија:

$$H(X,Y)=\sum_{i,j} p(x_i,y_j)\log p(x_i,y_j),$$

- Условна ентропија:

$$H(X|Y)=H(X,Y)-H(Y)$$

- Међусобна информација:

$$H(X:Y)=H(X)+H(Y)-H(X,Y).$$

Везе између ових величина одређују и неке особине Шенонове ентропије:

(а) $H(X,Y)=H(Y,X), H(X:Y)=H(Y:X)$

[3] Тада се каже да је информатички потенцијал такве поруке једнак нули.

[4] Вредност једног бита у низу не сме да зависи од вредности било којег другог бита у низу.

[5] *Детерминистичке (*непрекидне*) сигнале је могуће размењивати и брже од светлости*! Ово важи и за *појединачне* сигнале (непрекидне, и врло краткотрајне) који имплементирају *битове* (0, или 1). Али *размена информације не може ићи брже од светлости*, јер размена информација подразумева дискретан *скуп* (непрекидних, краткотрајних) сигнала (битова) који међусобно нису корелисани, тј., детерминистички условљени – в. ***Додатак 1.1***.

(б) $H(Y|X) > 0 \Rightarrow H(X:Y) \leq H(Y)$

(в) $H(X) \leq H(X,Y)$ - особина пододитивности

(г) $H(X,Y) \leq H(X) + H(Y)$

(д) $H(Y|X) \leq H(Y) \Rightarrow H(X:Y) \geq 0$,

(ђ) $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$ - јака пододитивност

(е) $H(X|Y,Z) \leq H(X|Y)$.

1.4 Појам спољашњег шума и корекција грешака

У информатичком процесирању могу се појавити две врсте грешака: (1) грешке у обављању појединих *операција* у процесирању (услед несавршености апаратуре, или спољашњег шума), и (2) грешке у појединим *битовима* у симболима x_i (услед спољашњег шума): $0 \to 1$ са вероватноћом p и $1 \to 0$ са вероватноћом $1 - p$ [6].

Прва врста грешака се може математички представити као

$$V' x_i \neq V x_i \qquad (1.6)$$

где је V жељена, а V' практично остварена операција. На срећу, ова врста грешака је релативно безболна. Наиме, добрим баждарењем апаратуре, у контролисаним условима је увек могуће практично постићи да је $V' \approx V$, тј. да важи:

$$p\left(|V' x_i - V x_i| < \varepsilon\right) \approx 1, \qquad (1.7)$$

где p означава вероватноћу, а $\varepsilon << 1$.

Другу врсту грешака, међутим, ***није могуће избећи***. Отуда је посебан задатак теоријске информатике заправо задатак *кориговања грешака*, и овај део информатике се означава као *EEC* ("*error correction codes*") методи – методи корекције грешака; успешност корекције грешака је сама основа високе тачности у раду савремених дигиталних рачунара.

Сви поступци корекције грешака имају исту идеју: утврдити који бит у низу, x_i, је измењен и кориговати његову вредност, и то учинити као *међукорак* у жељеном процесирању информација. Обично је за ово потребно увећати број неопходних битова у односу на број одређен изразом (1.4). Тиме се, ефективно, оперише на већем броју физичких битова него што је бројем-битова-изражена „количина информације". Другим речима, *због присуства шума*, уместо да се барата бројем N физичких битова (који је довољан број с обзиром на информатички задатак, израз (1.4)), *барата се са* M *физичких битова,* $M > N$,

[6] Вероватноћа p је средња вероватноћа. У општем случају, за различите битове у симболу x_i могу се појавити различите вероватноће грешке (промене 0 у 1).

тако да број $M-N$ *битова није информатички користан* – ту је само ради остварења корекције грешака.

1.5 Појам рачунања и комплексност

Неке детаље овде представљеног садржаја могуће је наћи у Одељцима 10.1-10.3, као и у литератури наведеној на крају овог поглавља.

Математички, рачунање представља *пресликавање*, тј. израчунавање вредности неке функције f за задату вредност аргумента („улаз“), a:

$$f : a \to b . \qquad (1.8)$$

Све што обављају рачунари описиво је изразом (1.8).

У теоријском рачунарству се подразумева да поступак рачунања има особину ***алгоритмичности***. То јест, рачунање је уређени низ поступака (основнијих операција). Сам појам алгоритма, интуитивно јасан, има своју формализацију кроз рачунску машину, тзв., *Тјурингову машину*. Тако се у теорији *изједначавају два појма*, појам *алгоритма*, и појам *Тјурингове машине* (в. Чрч-Тјурингову тезу у Одељку 10.3).

Основни задатак теоријског рачунања је направити модел ***универзалног рачунања***, тј., универзалне Тјурингове машине. Универзалност рачунања значи могућност да се:

> *са великом вероватноћом, приближно тачно*[7]*, прорачуна* ***било која*** *функција.*

Савремени дигитални рачунари испуњавају овај услов. Њихов рад заснован је на ***моделу-кола*** рачунања. Наиме, свака операција изграђена је од скупа ***елементарних операција*** (попут изградње материје од елементарних честица). Тај скуп операција мора имати особину универзалности, тј., особину да се комбиновањем елемената *само тог скупа* операција ***може прорачунати било која функција***. Скуп таквих операција – ***елементарних операција универзалног рачунања*** – није једнозначан. Али се испоставља да су, у смислу универзал-ности, сви такви скупови међусобно (рачунски) еквивалентнти. Отуда је довољно у пракси остварити један такав скуп.

> *Један скуп* елементарних операција универзалног класичног рачунања чине логичке операције И, ИЛИ, НЕ, *FANOUT*, *CROSSOVER*; операција ИЛИ је операција «искључиво ИЛИ», док *FANOUT* представља операцију копирања на *додатни бит* (који не улази у скуп од n битова, израз (1.4)), док *CROSSOVER* представља операцију замене вредности два одабрана бита.

[7] Прави напредак теоријског рачунања почиње уочавањем да, *у пракси*, није неопходно, нити да резултат буде тачан (већ само приближно тачан), ни да је вероватноћа његовог појављивања једнака 1 (довољно је да ова вероватноћа буде приближно једнака 1).

Други скуп елементарних операција, занимљиво, чине само операције *FANOUT* и И; са И је означена негација операције И.

Операција ИЛИ је вероватно најважнија операција, како у класичном, тако и у квантном рачунању (видети Одељак 10.7); њена енглеска ознака је *CNOT*, или *XOR*, и означава се симболом „$\oplus$“. Отуда се за њу користи и „збир (битова) модула 2“: $a \oplus b = 1(\text{за различите вредности битова}), 0(\text{за једнаке битове})$.

Средишњи задатак теорије рачунања је задатак *процене потребних ресурса* за рачунање – *просторни ресурси* се обично изражавају бројем потребних битова, n, а *временски ресурси* временом потребним за рачунање, T, у функцији задатог броја битова n. При томе, од интереса су само она израчунавања за која је $n >>> 1$.

Овим задатком се бави, тзв., *теорија комплексности*, која по правилу изражава време T у функцији броја битова n (за $n >>> 1$). Различите функционалне зависности времена од броја битова дефинишу различите класе задатака, по тежини. Тако постоје две основне класе: (а) лаки задаци (полиномска зависност), и тешки задаци (надполиномска зависност). Друга класа задатака се *не може практично обавити* на рачунару, тј., за класичне рачунаре постоје *практично* неизрачунљиве функције – време T постаје непрактично велико за неко велико n; посебан случај је експоненцијална зависност[8] времена од броја битова (нпр. 2^n).

У потрази за што бољим моделом рачунања дошло се до открића, тзв., ***стохастичког рачунања***. Наиме, ово рачунање се заснива на стохастичности улаза, и/или стохастичком избору операције на датом (детерминистичком) улазу. Испоставља се да овај модел рачунања има значајне предности у односу на детерминистичко рачунање (фиксиран улаз и фиксирана операција, у сваком кораку). У терминима Тјурингове машине, овај резултат, који обухвата искуство класичног рачунања у контексту комплексности рачунања, успоставља (в. Јаку Чрч-Тјурингову тезу, Одељак 10.3) да је стохастичка Тјурингова машина ***најбољи могући модел (класичног) рачунања***!

Друго значајно (физичко) откриће је откриће ***реверзибилног рачунања***. Наиме, испоставља се да се све елементарне операције универзалног рачунања у моделу-кола могу остварити физички реверзибилним (без расипања енергије), а математички инвертибилним операцијама – јасно је, инвертибилност операције захтева једнак број улазних (*input*) и излазних (*output*) битова. При томе, класично реверзибилно рачунање се може свести на класично иреверзибилно – видети ***Додатак 1.2***. Занимљиво је истаћи: најмањи број битова за задавање елементарног скупа универзалног реверзибилног рачунања је 3. Примери таквих операција (капија) дати су у Задацима 1.6-1.11 где се види да те, тробитне операције (Тофолијева, у ***Додатку 1.2***, или Фредкинова), свака за себе, представљају скуп елементарних операција универзалног класичног реверзибилног рачунања.

[8] Зато се понекад друга класа задатака назива «експоненцијално тешким».

Тако се сво искуство теорије ***класичног рачунања*** може обухватити моделом ***стохастичког, реверзибилног рачунања*** као ***најбољег и најпогоднијег модела рачунања***, с обзиром на услове комплексности и уштеде енергије у процесирању.

1.6 Неки резултати класичне информатичке теорије

Овде ће бити истакнути *само* они резултати који су од интереса за квантну информатику.

- *Класично кодирање*: разменом једног физичког бита, може се разменити *највише* један бит информације (Шенонове информације).

КОМЕНТАР: испоставља се да се овај резултат нарушава протоколом квантног супергустог кодирања (Одељак 9.2)., када се уместо класичних битова користе посебно припремљени (квантно сплетени - *entangled*) квантни битови – кубитови.

- *Проблем тајности кључа класичне криптографије*: тајну размену порука је могуће обавити (како тврди класична теорија криптографије) уколико је *кључ* за дешифровање поруке познат *само* странама у тој комуникацији. Међутим, тајност кључа није могуће доказиво обезбедити разменом класичних битова.

КОМЕНТАР: Разменом кубитова је могуће обавити и размену *доказиво тајног* кључа, користећи протоколе квантне криптографије (Одељак 9.3).

- *Факторизација великих бројева*: задатак факторисања великих бројева – разбијање на производе простих бројева – је тежак задатак – класа (2) - класичне теорије комплексности.

КОМЕНТАР: Квантни алгоритам Питера Шора (*Shor 1997*; видети и *Nielsen and Chuang 2000*) омогућује практично лако факторисање свих великих бројева. Тако, један тежак задатак класичне теорије комплексности постаје лак задатак квантне теорије комплексности.

1.7 Неки мотиви за развој квантне информатике

Минијатуризација електронских кола је главни задатак и главни покретач брзог развоја савремене (дигиталне) електронике и информатике. Међутим, овај задатак непосредно испоставља два проблема. *Прво*, минијатуризација не може ићи произвољно далеко[9]. Отуда се поставља питање: како изгледа процесирање на физичким системима који се повинују законима квантне[10], а не класичне физике? *Друго*, класично иреверзибилно рачунање подразумева расипање (дисипацију) енергије из физичког склопа који реализује поступак рачунања у околину. Обично, та околина су други, такође корисни, делови

[9] Наравно, граница су квантни системи, молекули, атоми и, фундаментално, елементарне честице.
[10] Испод неких просторних и временских димензија, физички системи почињу да испољавају квантно, а не класично понашање – повинују се квантним, а не класичним законима физике.

микроелектронског склопа, који се зато греју. Отуда, смањењем запремине склопова (као последица минијатуризације) а неумањењем расуте енергије, загревање у систему (нпр., у микрочиповима) може значајно нарасти - до те мере да промени режим рада микроелектронских склопова, тј., рад рачунара. Као својеврстан одговор на изазове ових питања појављује се квантно рачунање, тј., квантни рачунари: они непосредно нуде одговор на прво питање, а чињеницом да представљају модел реверзибилног (мада не-класичног) рачунања, омогућују и значајно смањење дисипације енергије.

Тешким задацима класичне теорије комплексности требало би придружити и задатке рачунарског ***симулирања сложених квантних система***. Наиме, како Фајнман (*Feynman 1982*) показује, симулирање сложених квантних система захтева велике, и просторне, и временске ресурсе, па се нека од тих симулирања *не могу практично* остварити на постојећим, дигиталним рачунарима. Отуда се природно поставља питање: ако класични физички системи нису у стању да обаве ове задатке, шта је са квантним системима (квантним хардвером), који би требало природно да симулирају квантне системе? Од квантних рачунара се очекује одговор на ово питање.

Откриће ***реверзибилног рачунања*** (в. Ландауеров принцип у Одељку 10. 2) је чисто физичко уочавање које није проистекло из теоријских основа заснованих на математичком приступу. Слично је и са открићем неких квантних алгоритама (Одељци 10.9.2 и 10.9.3), који на неочекиван начин проширују математичке основе теорије рачунања. Отуда се интерес, са чисто математичких, помера на, мање-више, чисто физичке задатке у смислу изучавања капацитета израчунавања, а који су исказиви (сада већ) ***квантном теоријом комплексности*** (*Nielsen and Chuang 2000*; *Preskill 1998*).

Поред задатака рачунања, посебан мотив за развој квантне информатике била су открића информатичких поступака која ***није могуће обавити на класичном хардверу*** (тј., помоћу класичних битова), као што су квантно супергусто кодирање (*Bennett and Wiesner 1992*), и размена доказиво тајних кључева у квантној криптографији (*Bennett and Brassard 1984*).

Коначно, практично све природне науке и области технике бележе тренд неке врсте минијатуризације. Зато је за боље разумевање, или боље функционисање и процесирање, пожељно (а понекад и нужно) изучити процесе на тако малим просторно-временским скалама да су то заправо скале на којима долазе до изражаја квантномеханички ефекти и понашање система од интереса (в. Поглавље II). Овај тренд, толико изражен у хемији (физичкој хемији, хемијској физици), савременој биологији (биотехнологији, биоинформатици, биохемији и биофизици), медицини, нанотехнологији и слично, заправо указује на појаву нове врсте технологије – технологије 21. века - која се понекад назива ***квантном технологијом***[11]. Област квантне информатике је истакнута област ових технологија у развоју.

[11] Видети *Milburn 1997*.

Отуда квантна механика постаје *примењена физика* par exellance (*Dugić 2000a*), те њено изучавање постаје потреба и у областима примењене физике 21. века.

1.8 Историјски осврт

Теоријска информатика (посебно рачунање) започиње славним Хилбертовим питањем: „*да ли постоји рачунска машина која може решити сваки математички задатак?*“. Одговор на ово питање је фасцинантан: ***не*** - постоје *неизрачунљиве функције*. Али до овог одговора се дошло после дуге потраге за формализацијом интуитивног појма рачунања, кроз појам алгоритма. *Свођењем поступка рачунања на појам алгоритма* отворена су врата за формализацију овог појма Тјуринговом машином. Формализам рада Тјурингове машине је типично математички задатак који има особину општости, у смислу формулисања теорема (или макар правила) теоријског рачунања који је кулминирао формулисањем теорије комплексности. Напоредо са тим постављене су основе теорије комуникација, у чијој су основи појам Шенонове ентроипије и славни Шенонови теореми.

Савремена теорија рачунања започиње радовима Ролфа Ландауера (*Landauer 1963*, а на основи тога, између осталих, и Пола Бениофа (*Benioff 1980*), као и Чарлса Бенета (*Bennett 1982*)), чиме је успостављена физичка основа, тзв., *реверзибилног рачунања*. Истовремено, ово значи и промену перспективе у вези са процесирањем информација: могућности процесирања информација се изучавају на *физичкој*, уместо на чисто математичкој основи. Круну класичне теоријске информатике чини уочавање да је модел стохастичког, реверзибилног рачунања најбољи модел класичног рачунања.

Основе квантне информатике (у ширем смислу) успостављене су формулацијом, тзв., *no-cloning* теорема (*Wooters and Zurek 1982*), те увођењем појма *модела-кола квантног рачунања* од стране Дејвида Дојча (*Deutsch 1985*). На основи овог модела убрзо је развијен модел *универзалног рачунања у моделу-кола* квантног рачунања. Први значајни квантни алгоритми Шора (*Shor 1997*) и Гровера (*Grover 1997*), те откриће квантне криптографије (*Bennett and Brasard 1984*) и квантне телепортације (*Bennett et al 1993*), успоставили су основу за широк теоријски (али и експериментални) развој квантне информатике. Квантно рачунање у моделу-кола кулминира у моделу тзв. *fault-tolerant* квантног рачунања, које одликује имуност на грешке[12]. Откриће овог модела започето је пионирским радом Питера Шора (*Shor 1995*), а даље настављено радовима Дејвида Готесмана (*Gottesman 1998*), те Ендрјуа Стина (*Steane 1996*), да поменемо само неке истраживаче[13].

[12] Прецизније: корекција грешака у току рачунања обезбеђује робусност процесирања (слично класичним поступцима корекције грешака) спрам спољашњег шума.

[13] Овим пресеком нису обухваћене неке области квантне информатике које нису предвиђене Садржајем.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

За све теме изложене у овом поглављу консултовати *Nielsen and Chuang 2000*.

- У вези са задацима кодирања и декодирања, Шеноновим теоремима (и особинама Шенонове ентропије), ограничењима класичне комуникације, консултовати: *Csiszar and Korner 1982*.
- У вези са основама теорије комплексности консултовати: *Papadimitriou 1994*.
- У вези са историјским развојем области квантне информатике консултовати: *Nielsen and Chuang 2000*
- У вези са квантним технологијама консултовати: *Milburn 1997*; *Dugić 2002a*.

Неки Интернет ресурси:

- http://arXiv.org , под опцијом *квантна физика*, quant.ph/ архива.
- http://physics.kg.ac.yu/Prezentacija/Prezentacije%20zaposlenih/Miroljub%20Dugic/Kvantno%20racunanje/

па даље: нађи линкове под опцијом: „*Неки корисни линкови*“.

ЗАДАЦИ:

1.1 Дискутовати важност захтева универзалности за процесирање информација.

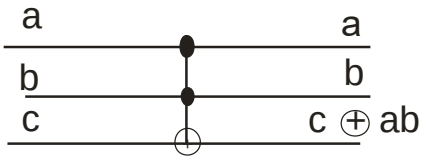
1.2 Скупом од 5 битова кодирати слова азбуке, и написати израз „квантна информатика“.

1.3 Генерисати (нпр. *бацањем новчића*) случајни избор вредности за један бит, који са једнаком вероватноћом даје вредност 0, или 1. На основи тога генерисати све (различите) низове од 5, а затим од 50 битова. За сваки скуп обавити следеће: упоредити број низова у којима је број нула и јединица приближно једнак са онима у којима то није случај. Уочити да са повећањем броја битова у низу ($50 > 5$) расте број првог скупа – све је више „типичних“ низова са приближним бројем нула и јединица. (Напомена: ово уочавање се строго заснива у лимесу $N \to \infty$, што је уочавање које лежи у основи Шенонових теорема.)

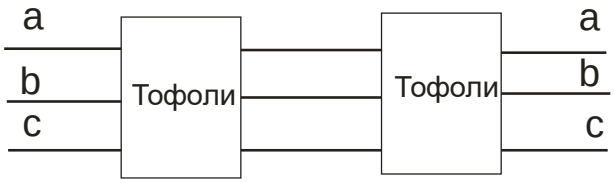
1.4 Извор информација описан је расподелом вероватноћа $p_n = \left(\frac{1}{3}\right)^n, n = 1,2,3,\ldots,N-1$. У низу од N симбола, колико је p_N? Израчунати Шенонову ентропију за случајеве: $N = 2,10$ и $N \to \infty$?

1.5 Користећи операције *FANOUT* и И, изградити логичке операције И, ИЛИ, НЕ, *FANOUT, CROSSOVER*.

1.6 Логичко коло на слици је, тзв., Тофолијевих капија, ***Додатак 1.2***. За вредност $c=1$ доказати да ова капија ради као НЕИ$\equiv$<u>И</u> за прва два бита, а да за вредности $a=1, c=0$, ова капија остварује FANOUT (тј. копирање вредности 2. бита на трећи).



1.7 Доказати да је Тофолијева капија инверзна сама себи (тј., реверзибилна), тј. да двоструко деловање Тофолијеве капије враћа почетне вредности битова, као на слици:



1.8 Који од три бита у Тофолијевој капији треба, и како, фиксирати да би Тофолијева капија остварила CNOT (XOR) – тј. „искључиво-ИЛИ“ операцију?

1.9 Која операција постаје Тофолијева капија за $a=b=1$?

1.10 Фредкинова капија је тробитна капија: $(a,b,c)\to(a',b',c)$ таква да за $c=0$ оставља прве битове неизмењене, док за $c=1$, вредности прва два бита се међусобно замењују. Доказати: (а) да је Фредкинова капија реверзибилна, (б) $a=1, b=0$ истовремено остварује НЕ, тј., c на првом биту, као и копирање (FANOUT) трећег бита на други, (в) да се број јединица (број битова једнак 1) сачувава овом операцијом.

НАПОМЕНА: Особина конзервативности, тачка (в) задатка, носи физичку интуицију у смислу физичке имплементације ове капије – све познате физичке интеракције и процеси (осим, можда, процеса квантног мерења) на физичким системима су повратни (реверзибилни).

1.11 Којим избором улазних, и којих излазних битова Фредкинове капије се остварују И, НЕ, CROSSOVER?

НАПОМЕНА: Када се овима дода још CNOT и FANOUT, добије се један скуп елементарних операција универзалног класичног рачунања. Тако је и Фредкинова капија, сама за себе (баш као и Тофолијева) јединствена (*тро*битна) капија универзалног, реверзибилног класичног рачунања.

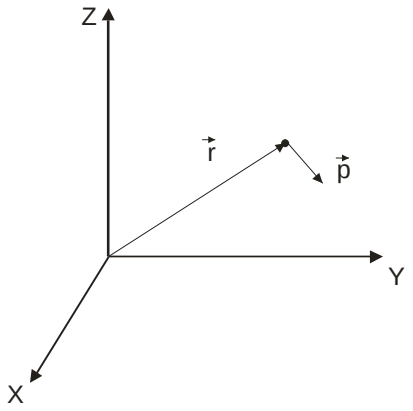
II ОСНОВНИ ПОЈМОВИ КВАНТНЕ МЕХАНИКЕ

У овом поглављу представљени су само они елементи основа квантне механике који су од интереса за област квантне информатике. За више детаља у овом смислу консултовати литературу на крају овог поглавља.

2.1 Класични фазни простор. Класична реалност

Основни физички појам је појам ***стања***. Познавање стања физичког система повлачи и познавање вредности свих физичких величина у класичној физици, као и одговор на питање временске промене стања, као и вредности физичких величина у току времена.

Стање *материјалне тачке* дефинисано је паром вектора, вектора положаја и импулса, $(\vec{r}, \vec{p})$. За скуп од N материјалних тачака, стање је дефинисано као скуп вектора положаја и импулса свих материјалних тачака („честица“) система, $(\vec{r}_i, \vec{p}_i, i = 1,2,..., N)$. Векторски простор у којем овај скуп величина (тј. стање система) представља *тачку*, назива се *класични фазни простор стања*. Подпростор овог простора је, тзв., конфигурациони простор, што је векторски простор положаја – у којем је тачка дефинисана скупом $(\vec{r}_i, i = 1,2,...., N)$, што је на Сл. 2.1 представљено за једну честицу ($N = 1$).



Сл. 2.1 Вектор положаја, $\vec{r}$, и импулса, $\vec{p}$, једне материјалне тачке у датом референтном систему. То је стандардни, тродимензионални Еуклидски простор положаја – „конфигурациони простор“.

ДЕФ. 2.1: Под ***класичном реалношћу*** се подразумева ничим условљено постојање стања и вредности физичких величина физичког система у сваком тренутку времена.

Решавањем једначина кретања (Њутнових, Даламберових, Хамилтонових, Лагранжеових) за систем честица, као решења се добијају једнозначне функције времена датих физичких величина. Основни пар („конјугованих“) величина, $\vec{r}$ и $\vec{p}$, представљене као функције времена:

$$\vec{r} = \vec{r}(t),\ \vec{p} = \vec{p}(t)\,, \qquad (2.1)$$

задовољавају критеријум класичне реалности: ова решења диференцијалних једначина кретања нису ничим условљена, и за унапред познате услове под којима се систем налази, су једнозначна. Како су све физичке величине класичне механике функције овог пара величина, то се *исти став тиче свих физичких величина сваког класично-механичког система*.

Тако се може рећи да се реални физички системи (објекти) у класичној механици моделују скупом параметара (маса, наелектрисање и сл.), и скупом вектора положаја и импулса, тј., фазним простором као простором стања. Отуда се, ефективно, међусобно ***идентификују два појма***, појам ***стања***, и појам вредности ***основног скупа величина*** („варијабли“) положаја и импулса, $\vec{r}$ и $\vec{p}$.

Имајући у виду израз (2.1), класична реалност се у физичким моделима састоји у *једнозначности трајекторије* (како у фазном простору, тако и у сваком његовом подпростору – на пример конфигурационом простору) *сваке честице система*, за унапред познате физичке услове. Наравно, ако ти услови нису једнозначно познати, онда ни трајекторије нису једнозначно, већ само са неком вероватноћом, познате. Али ове вероватноће *не нарушавају особину класичне реалности* стања (вредности физичких величина[1]): ако важе услови S, тада ће решења (2.1) која одговарају овим условима бити стопостотно остварена[2].

2.2 Основни постулати квантне механике

Квантну механику одликује одсуство визуализација физичких система и процеса који су карактеристични за класичну физику, као што је Сл. 2.1. Штавише, појмови *стања* и *вредности физичких величина* (варијабли) више нису исто. Коначно, квантна механика је инхерентно статистичка дисциплина – о физичким догађајима (резултатима мерења) се говори само у терминима вероватноће, и *само изузетно* у терминима појма класичне реалности уведеног Деф. 2.1.

За разумевање садржаја основних постулата неопходно је предзнање основа Хилбертових простора – видети ***Додатке 2.1 и 2.2***.

ПОСТУЛАТ О СТАЊИМА: Свако стање квантног система представљено је једним елементом неког Хилбертовог простора. Важи и обрнуто: сваки елемент датог Хилбертовог простора је једно могуће стање квантног система. При томе, ако важи једнакост:

$$|\chi\rangle = e^{i\delta}|\psi\rangle, \qquad (\text{П}.1)$$

тада се два стања $|\chi\rangle$ и $|\psi\rangle$ имају сматрати истим квантним стањем, за сваку „фазу“ δ.

[1] Такве физичке величине се онда називају *варијаблама*.

[2] Ако има више могућих физичких услова, има и више могућих решења (2.1), од којих се у сваком појединачном случају остварује *само једно* од њих.

ПОСТУЛАТ О ОПСЕРВАБЛАМА: Свакој класичној варијабли физичког система A се једнозначно придружује један ермитски оператор (опсервабла) $\hat{A}$ који делује над датим Хилбертовим простором – простором стања квантног система. Важи и обрнуто: свака ермитска опсервабла која делује над датим простором стања је, у принципу, једна физичка величина (варијабла) коју је могуће измерити одређеним мерним поступком.

ПОСТУЛАТ О ВЕРОВАТНОЋАМА: Вероватноћа да се мерењем опсервабле $\hat{A}$ на систему у стању $|\psi\rangle$ добије резултат који лежи у интервалу $[\alpha,\beta]$ (што може бити и отворен, или полуотворен интервал) израчунава се по формули:

$$W(\hat{A},|\psi\rangle,[\alpha,\beta]) = \langle\psi|\hat{P}_{[\alpha,\beta]}(\hat{A})|\psi\rangle\,. \qquad (\text{П.2})$$

На левој страни (П.2) стоји ознака за вероватноћу мерења, а са десне стране је спектрална мера опсервабле $\hat{A}$ за интервал $[\alpha,\beta]$, $\hat{P}(\hat{A})_{[\alpha,\beta]}$.

Упутно је дати следеће напомене (детаљно представљене у ***Додатку 2.2***). Свако ***стање*** $|\psi\rangle$ Хилбертовог простора – простора стања – се може *једнозначно разложити* у линеарну суперпозицију стања из неког ортонормираног базиса (ОНБ)[3], $\{|\phi_i\rangle, \langle\phi_i|\phi_j\rangle = \delta_{ij}, i,j = 1,2,3,4,\dots\}$:

$$|\psi\rangle = \sum_i c_i\,|\phi_i\rangle, \text{ где } c_i = \langle\phi_i|\psi\rangle. \qquad (2.2)$$

Услов нормираности стања $|\psi\rangle$, $\langle\psi|\psi\rangle = 1$, еквивалентан је услову

$$\sum_i |c_i|^2 = 1. \qquad (2.3)$$

Сваки ермитски оператор, $\hat{A}$, једнозначно је представљен својом ***спектралном формом***:

$$\hat{A} = \sum_n a_n \hat{P}_n\,, \qquad (2.4)$$

где *реални бројеви* a_n представљају својствене вредности оператора $\hat{A}$ које се ***могу добити мерењем*** ове опсервабле, док $\hat{P}_n$ представљају *својствене пројекторе* (на својствене подпросторе) ове опсервабле, уз услов *једнозначног* придруживања $a_n \to \hat{P}_n$ и ортогоналности пројектора:

$$\hat{P}_n\hat{P}_m = \delta_{nm}\hat{P}_n\,. \qquad (2.5)$$

Спектрална мера оператора $\hat{A}$ за интервал[4] вредности (α,β), за случај чисто дискретног спектра вредности ове опсервабле, $\{a_n, n = 1,2,3,4,\dots\}$, дефинисана је збиром пројектора:

---

[3] За ознаке видети стр. iv.

[4] Који може бити и полу-отворени, или затворени интервал.

$$\hat{P}_{(\alpha,\varepsilon)} = \sum_{a_n \in (\alpha,\varepsilon)} \hat{P}_n \,, \qquad (2.6)$$

где се сумирање врши само за оне својствене вредности које падају у задати интервал (α,β).

2.3 Дискусија постулата

Стање квантног система је елемент Хилбертовог простора стања и не може се (за разлику од класичне механике) идентификовати са опсерваблама које представљају физичке величине, јер опсервабле представљају операторе (пресликавања) на простору стања – на које се односи посебан постулат.

У поређењу са класичном механиком, квантна механика има схизоидну основу: појам квантног *стања* је *одвојен* од појма квантне *величине* („опсервабле“), док је то у класичној физици обједињено појмом тачке у фазном простору. Класично, познавање стања одређује, и то једнозначно, вредности свих физичких величина датог система; то је, формално, последица чињенице да су све физичке величине заправо аналитичке функције на фазном простору. Квантномеханички, пак, познавање стања не одређује вредности физичких величина (опсервабли) – иначе не би био потребан посебан постулат о опсерваблама, баш као што нешто слично и не постоји у класичној механици. Отуда се намеће очекивање: ако једном стању не одговара једнозначна вредност неке опсервабле, онда је нужни елемент квантномеханичке теорије појам вероватноће. То јест, ако се, за једнозначно дефинисано стање, мерењем не мора добити само једна вредност неке опсервабле, онда квантно мерење на систему мора имати одлике стохастичности – баш у складу са трећим постулатом.

Основни и општи задатак квантне механике је прорачун вероватноћа догађаја (резултата мерења) и очекиваних (средњих) вредности опсервабли. Тада се подразумева да је стање система познато (у сваком тренутку – видети Одељак 2.11).

Постулат о вероватноћама имплицира да се стање система заправо тиче ***ансамбла*** *– скупа, по нечему идентичних, међусобно неинтерагујућих физичких система*. Ово следи на основи чињенице да појам вероватноће има смисла само на ансамблу, тј., на скупу идентично обављених мерења на свим елементима ансамбла. Тако, ако у ансамблу има N идентично припремљених система (елемената ансамбла), мерење неке опсервабле у општем случају даје исту, i-ту вредност, на скупу од N_i понављања мерења. При томе, како захтева теорија вероватноће, мора важити:

$$N = \sum_i N_i \,,$$

док стандардна дефиниција вероватноће i-тог резултата мерења, p_i, захтева важење лимеса:

$$p_i = \lim_{N\to\infty} \frac{N_i}{N},$$

што води испуњењу услова позитивности и нормираности расподеле вероватноћа, $\{p_i\}$:

(а) $p_i \geq 0, \forall i$,
(б) $\sum_i p_i = 1$.

Полазећи од статистичке дефиниције средње (очекиване) вредности опсервабле $\hat{A}$ у стању $|\psi\rangle$, $\langle\hat{A}\rangle = \sum_n a_n W(\hat{A}, |\psi\rangle, a_n)$, лако се доказује:

$$\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle. \qquad (2.7)$$

Ако стање $|\psi\rangle$ није својствено за опсерваблу $\hat{A}$, онда важи $W(\hat{A}, |\psi\rangle, a_n) < 1$, $\forall n$, то јест, постоји више могућих резултата мерења. Тада се уводи мера *неодређености* (неједнозначности) вредности опсервабле $\hat{A}$ за систем у стању $|\psi\rangle$, *стандардним одступањем*, $\Delta\hat{A}$, дефинисаним изразом:

$$\Delta\hat{A} = +\sqrt{\left\langle\left(\hat{A} - \langle\hat{A}\rangle\right)^2\right\rangle} = +\sqrt{\langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2}, \qquad (2.8)$$

где се сва усредњавања односе на $|\psi\rangle$.

За вредност a опсервабле $\hat{A}$ за коју важи $W(\hat{A}, |\psi\rangle, a) = 1$, или, еквивалентно, $\Delta\hat{A} = 0$ у стању $|\psi\rangle$, се каже да је „оштра вредност".

2.4 Појам појединачног система

Сваки квантни ансамбл се састоји из појединачних система (појединачних елемената ансамбла). Физички, то су елементи на којима се врши мерење и који међусобно не интерагују. Сви елементи ансамбла су на исти начин препарирани (па су у том смислу идентични) и на сваком од њих се обавља (макроскопски гледано) исти поступак мерења. *Оперативно*, појединачни елемент ансамбла је сваки појединачни резултат мерења. Стање појединачног система квантног ансамбла није унапред познато, иако је познато стање ансамбла. Међутим, ако се систем налази у неком („чистом") стању $|\psi\rangle$ (в. Одељак 3.4, а као контраст Одељак 3.6), што је (према Постулату о стањима) елемент Хилбертовог простора стања, тада је стање и сваког појединачног елемента (система) у ансамблу једнозначно одређено. Ово је успостављено следећим постулатом.

ПОСТУЛАТ О ПОЈЕДИНАЧНИМ СИСТЕМИМА: Нека је неки ансамбл у („чистом") стању $|\psi\rangle$. Ако је вероватноћа да се мерењем неке опсервабле $\hat{A}$ на

ансамблу у том стању добије резултат из неког интервала $[a,b]$ једнака јединици, тада мерење на сваком појединачном елементу ансамбла нужно даје исти резултат, то јест важи једнакост:

$W(\hat{A},|\psi\rangle,[a,b])=1 \Leftrightarrow$

$\{$резултат мерења у интервалу $[a,b]$ је апсолутно сигуран догађај$\}$

Другачије исказано: сваки елемент ансамбла који се налази у стању $|\psi\rangle$, и сам се налази у истом квантном стању. Овај постулат је од суштинског значаја за квантну информатику, у којој се барата појединачним системима (тзв., кубитовима).

2.5 Релације неодређености

Средишњи појам квантне механике јесу релације неодређености. Ради се о теорему – последици основних постулата – чије физичко значење не само да не престаје да привлачи пажњу истраживача, већ је у извесном смислу и један од средишњих физичких појмова квантне информатике.

ТЕОРЕМ 2.1: Нека су $\hat{A}$ и $\hat{B}$ две опсервабле на Хилбертовом простору стања система. Нека је стање $|\psi\rangle$ такво да припада домену обеју ових опсервабли, као и домену њиховог комутатора. Тада важи неједнакост:

$$\Delta\hat{A}\cdot\Delta\hat{B}\geq\frac{1}{2}\left|\left\langle\left[\hat{A},\hat{B}\right]\right\rangle\right|, \tag{2.9}$$

при чему $\left\langle\left[\hat{A},\hat{B}\right]\right\rangle\equiv\langle\psi|\left[\hat{A},\hat{B}\right]|\psi\rangle$, а на левој страни се појављују стандардна одступања опсервабли у истом стању $|\psi\rangle$.

□ Доказ: Користићемо добро познату Шварцову неједнакост: $\left|\langle u|v\rangle\right|^2\leq\langle u|u\rangle\langle v|v\rangle$, која важи за било која два вектора $|u\rangle$ и $|\mathrm{v}\rangle$ сваког векторског простора. Сада, уводећи ознаке: $\hat{A}'=\hat{A}-\left\langle\hat{A}\right\rangle$ и $\hat{B}'=\hat{B}-\left\langle\hat{B}\right\rangle$, где се усредњавање опсервабли врши у стању $|\psi\rangle$, дефинисаног условима теорема, згодно је увести нове дефиниције. Наиме, дефинисањем $|u\rangle\equiv\hat{A}'|\psi\rangle$ и $|v\rangle\equiv\hat{B}'|\psi\rangle$, непосреедно се примењује Шварцова неједнакост:

$$\left|\langle\psi|\hat{A}'\hat{B}'|\psi\rangle\right|^2\leq\langle\psi|\hat{A}'^2|\psi\rangle\langle\psi|\hat{B}'^2|\psi\rangle. \tag{2.10}$$

Како $\hat{A}'\hat{B}' = \frac{1}{2}\left(\hat{A}'\hat{B}' + \hat{B}'\hat{A}'\right) + \frac{1}{2}\left(\hat{A}'\hat{B}' - \hat{B}'\hat{A}'\right)$, то се лева страна израза (2.10) може преписати у облик[5]:

$$\left|\langle\psi|\hat{A}'\hat{B}'|\psi\rangle\right|^2 = \frac{1}{4}\left|\langle\psi|\left\{\hat{A}', \hat{B}'\right\}|\psi\rangle\right|^2 + \frac{1}{4}\left|\langle\psi|\left[\hat{A}', \hat{B}'\right]|\psi\rangle\right|^2. \qquad (2.10а)$$

Памтећи дефиниције опсервабли, сменом у израз (2.10), добија се:

$$\langle\psi|\hat{A}'^2|\psi\rangle\langle\psi|\hat{B}'^2|\psi\rangle = \left(\Delta\hat{A}\right)^2\left(\Delta\hat{B}\right)^2 \geq \frac{1}{4}\left|\langle\psi|\left[A', B'\right]|\psi\rangle\right|^2. \qquad (2.10б)$$

Сада, како важи једнакост $\left[\hat{A}', \hat{B}'\right] = \left[\hat{A}, \hat{B}\right]$, добијена је неједнакост:

$$\left(\Delta\hat{A}\right)^2 \cdot \left(\Delta\hat{B}\right)^2 \geq \frac{1}{4}\left|\left\langle\left[\hat{A}, \hat{B}\right]\right\rangle\right|^2, \qquad (2.10в)$$

што је други запис релације неодређености, израз (2.9). ■

Уочити да за стања која нису у пресеку домена оператора наведених у теорему, релације неодређености не морају да важе. Као драстичан пример у овом смислу се појављују ситуације у којима квантни објекти нису више на располагању, нпр., за мерење, као у случају *детекције квантних честица* (нпр., фотона на застору), у ком случају квантне честице „нестају" – бивају захваћене од стране средине којом се њихово присуство детектује. Отуда следи и непримењивост релација неодређености – самом чињеницом да није познато стање квантних честица које су детектоване[6].

Специјалан случај релација неодређености су релације за опсервабле положаја и импулса, $\hat{x}, \hat{p}$. Како важи $[\hat{x}, \hat{p}] = i\hbar$, сменом комутатора у израз (2.9) води славним Хајзенберговим релацијама неодређености:

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{\hbar}{2}. \qquad (2.10')$$

Само у овако једноставним случајевима – када се са десне стране у изразу (2.9) налази константа (умножак јединичног оператора) – има смисла исказ: *са смањењем стандардног одступања (неодређеност) једне опсервабле, увећава се стандардно одступање(неодређеност) друге.*

Задатак *физичког тумачења релација неодређености* је један од средишњих задатака квантне механике. У вези са тим би требало истаћи: у изразу (2.9) се појављују стандардна одступања која, као и све статистичке величине,

---

[5] Овде је коришћена чињеница да $\langle\psi|\left\{\hat{A}', \hat{B}'\right\}|\psi\rangle$ представља реалан, а $\langle\psi|\left[\hat{A}', \hat{B}\right]|\psi\rangle$ чисто имагинаран број, па је квадрат модула $\left|\langle\psi|\hat{A}'\hat{B}'|\psi\rangle\right|^2$ просто збир квадрата реалног и имагинарног дела комплексног броја $\langle\psi|\hat{A}'\hat{B}'|\psi\rangle$.

[6] Детекција квантних честица спада у тзв. *непоновљива мерења* (Одељак 3.1). Дакле, релације неодређености не важе за непоновљива (*nonrepeatable*) мерења.

имају смисла само у контексту (квантног) ансамбла. Отуда није очигледно (и није ни јасно) да ли релације неодређености носе икакав садржај у контексту појединачних система, тј., појединачних елемената квантног ансамбла.

Једно погрешно тумачење релација неодређености:
Историјски, релације неодређености најчешће су тумачене на следећи, *погрешан*, начин: „мерење опсервабле $\hat{A}$ са тачношћу $\Delta\hat{A}$ производи (узрокује) неодређеност опсервабле $\hat{B}$ у износу, најмање, $\Delta\hat{B}$ (тако да је задовољен израз (2.9))". Доказ погрешности овог става је предмет Задатка 2.10. Овде само још напомена: доказ има ансамбалску основу, те се исти доказ тим пре тиче појединачних елемената ансамбла - за које иначе и није јасно како би им се могла придружити статистичка одступања.

Отуда је згодно посебно нагласити: постоји читав низ непоузданих, па и нетачних тумачења релација неодређености, од којих се већина тиче процеса мерења[7] – *Хербут 1984.*

Ансамбалско тумачење релација неодређености:

Поделимо један ансамбл у стању $|\psi\rangle$ на два подансамбла. На основи Одељка 2.4, сваки од тих подансамбала биће у истом стању, $|\psi\rangle$. Измеримо на једном подансамблу опсерваблу $\hat{A}$, а на другом опсерваблу $\hat{B}$. Тада Теорем 3.1 гарантује важење релације (2.9) за стандардна одступања опсервабли $\hat{A}$ и $\hat{B}$, која се прорачунавају на основи мерења на два подансамбла, оба у стању $|\psi\rangle$.

Изван ансамбалске интерпретације, израз (2.9) не говори много о процесу мерења. Са друге стране, анализа процеса мерења (в. Поглавље III) не повезује процес мерења са релацијама неодређености на једнозначан начин[8] (видети и ***Додатак 2.3***). Отуда је веза ових двеју великих тема основа квантне механике *предмет тумачења (интерпретације)*, и једно такво, широко прихваћено, тумачење је предмет следећег одељка.

2.6 Принцип комплементарности

Већ основни постулати квантне механике компромитују интуицију засновану на појмовима класичне физике. У извесном смислу, садржај квантне

[7] Веза релација неодређености и мерења није једнозначно успостављена – осим у мери у којој је то успостављено у оквирима ансамбалског тумачења релација неодређености – из разлога што је (Задатак 2.10) процес мерења динамички процес, док је у (2.9) време фиксирано. Сама тема мерења запрема добар део ове књиге, а посебно у Поглављима III, IV и VII.
[8] Неке варијације на тему специјалних случајева који могу унети забуну у контекст тумачења релација неодређености представљене су у ***Додатку 2.3***.

информатике и рачунања представља примену физичких основа, тј., тумачења (интерпретације) квантномеханичке теорије.

У историји тазвоја квантне механике у овом смислу посебно место заузима, тзв., Копенхагенска школа (копенхагенско тумачење) квантне механике у чијој основи је, тзв., принцип квантне комплементарности.

Принцип комплементарности успоставља постојање међусобнио *искључивих* мерских ситуација, у смислу да мерење одређене врсте може у потпуности елиминисати могућност обављања неких других мерења у истом поступку, симултано, и то у принципу. Тако, мерење неке опсервабле $\hat{A}$, по овом принципу, онемогућује добијање једнозначне вредности неке њој некомпатибилне (некомутирајуће) опсервабле $\hat{B}$ у истом мерном поступку (истовремено). Као формални израз ове искључивости, *успоставља принцип комплементарности*, појављују се релације неодређености – наравно, у *ансамбалском* контексту. При томе, не ради се о ограничењима практичне врсте, тј., о слабостима апаратура у поступку мерења, већ се тиче свих могућих мерских поступака, како год били смишљени.

Принцип комплементарности успоставља и следећи *пропис*: у свакој мерској ситуацији треба оштро разликовати објекат мерења од мерног инструмента (апарата). При томе, физички систем који је у једној мерској ситуацији био апарат, у некој другој мерској ситуацији може бити део (подсистем) објекта мерења. Комплементарност се сада појављује као ограничење на пренос закључака на различите мерске ситуације.

Поступак мерења је средишњи извор проблема у тумачењу квантне механике – што се очитује потребом за успостављањем посебног постулата (трећег постулата) квантне механике. Отуда је овде дата једна описна формулација принципа комплементарности а на терену поступка квантног мерења. Општије формулације (нпр., везане за дуалност талас-честица) овог принципа се могу наћи на другим местима (в., нпр., Хербут 1984, Марић 1986).

Интуитивно, принцип комплементарности успоставља границу у самим могућностима истовременог мерења неких опсервабли – а што је тема Поглавља III.

2.7 Постулат о квантизацији. Постулат о степенима слободе.

Пренос класичних варијабли у квантни контекст, а у складу са постулатом о опсерваблама, захтева посебан пропис. Тај *пропис* дат је у Оквиру испод, а на основи њега (и без његове експлицитне примене) разматрамо и *вишедимензионалне* квантне системе.

Овим постулатом успостављају се општи прописи преноса физичких модела из контекста класичне у контекст квантне физике, и представља једну од основних и најважнијих рецептура у оперативном раду у оквирима формализма квантне механике.

ПОСТУЛАТ О КВАНТИЗАЦИЈИ: Свакој класичној варијабли физичког система једнозначно се придружује један ермитски оператор (који делује над простором стања тог система) у складу са следећим скупом правила:

(1) основни скуп варијабли постаје основни скуп опсервабли – степени слободе и њима канонски коњугованих импулса,

(2) $\alpha A+\beta B\to\alpha\hat{A}+\beta\hat{B}$, за произвољне реалне бројеве α,β,

(3) $AB\to\frac{1}{2}(\hat{A}\hat{B}+\hat{B}\hat{A})$ - симетризовани производ

(4) $[A,B]_{PB}\to-\frac{i}{\hbar}[\hat{A},\hat{B}]$,

(5) Пресликавања у тачкама 3 и 4 одликује математичка непрекидност.

Са десне стране су ермитске опсервабле. Индекс „*PB*“ означава „Пуасонову заграду“ (в. *Мушицки 1984*), а средња заграда код оператора означава комутатор – видети ***Додатак 2.2***. Основу примене овог постулата одређује следећи постулат квантне механике.

ПОСТУЛАТ О СТЕПЕНИМА СЛОБОДЕ: Сваком степену слободе физичког система придружује се један простор стања, H_i. Укупни простор стања, H, квантног система дефинише се као тензорски производ простора стања појединачних степени слободе, $H=\otimes_i H_i$.

Дакле, постулат о степенима слободе формално уводи просторе стања за дате класичне степене слободе система. Ти простори стања, који се тичу појединих степена слободе, постају *фактор простори* (***Додатак 2.2***) укупног простора стања система:

$H=\otimes_n H_n$.

Над фактор просторима стања сада делују опсервабле које се, на основи класично задатих степена слободе, квантују у складу са претходним постулатом. Све опсервабле система које делују над укупним простором стања су сада аналитичке функције основног скупа опсервабли (тј., степена слободе и њима коњугованих импулса – баш како је то и у класичној аначлитичкој механици).

Ако је $\left\{\left|\varphi^{(n)}{}_i\right\rangle\right\}$ један ОНБ фактор простора H_n, тада се сваки елемент укупног простора стања[9], $|\Psi\rangle\in H$, може записати у општем облику:

$$|\Psi\rangle=\sum_{i,j,k,\ldots}\alpha_{ijk\ldots}\left|\varphi^{(1)}{}_i\right\rangle\otimes\left|\varphi^{(2)}{}_j\right\rangle\otimes\left|\varphi^{(3)}{}_k\right\rangle\ldots \qquad (2.11)$$

[9] Један ОНБ укупног простора стања је $\left\{\left|\varphi^{(1)}{}_i\right\rangle\otimes\left|\varphi^{(2)}{}_j\right\rangle\otimes\left|\varphi^{(3)}{}_k\right\rangle..\right\}$, када се узму у обзир *све* комбинације индекса *i,j,k,…*.

2.8 Унутрашњи степени слободе: Спин

Неки експерименти, попут славног Штерн-Герлаховог експеримента (***Додатак 2.4***), указују на тешкоће објашњења неких квантних ефеката када се модел ефекта заснива на стандардним (просторним, „спољашњим“) степенима слободе – када урачунавање свих могућности за објашњење ефекта, а које се моделују на скупу опсервабли вектора положаја и импулса једног вишечестичног система, није довољно за објашњење неких ефеката. Тада је неизбежна претпоставка о постојању нових, од опсервабли положаја и импулса независних, „унутрашњих“ степена слободе. Објашњење Штерн-Герлаховог експеримента уследило је на основи увођења унутрашњег степена слободе названог ***спин***.

Спин је „унутрашња“ особина квантне честице чија се (временски независна) вредност, s, феноменолошки утврђује. На основи ове вредности изграђује се одговарајући простор стања, H_s. Укупни простор стања честице се уводи као тензорски производ $H_o \otimes H_s$, где је са H_o означен „орбитални“ простор стања над којим делују опсервабле положаја и импулса, $\hat{r}$ и $\hat{p}$ („спољашњи степени слободе“); спин није функција било које од ових опсервабли.

Векторска опсервабла спина, $\hat{S}$, ***уводи се по аналогији са опсерваблом момента импулса,*** $\hat{L} = \hat{r} \times \hat{p}$ и, по дефиницији, није функција нити $\hat{r}$, ни $\hat{p}$. Њено увођење је неопходно: Штерн-Герлахов експеримент не може бити објашњен нити класичном, ни квантном физиком, заснованим на „спољашњим степенима слободе“. Отуда се спину прилази као унутрашњој особини квантне честице чија се вредност феноменолошки утврђује за сваку честицу посебно. Испоставља се да су дозвољене, или полубројне ($s = (2k+1)/2$), или целобројне (ненегативне) вредности спина. Честице са полубројним спином називају се *фермионима*, а честице са целобројним спином *бозонима*.

У формализму:

1. уводи се опсервабла спина, $\hat{\vec{S}} = \left(\hat{S}_x, \hat{S}_y, \hat{S}_z\right)$, чије компоненте (*по аналогији са моментом импулса*) задовољавају комутационе релације:
$\left[\hat{S}_i, \hat{S}_j\right] = i\hbar\varepsilon_{ijk}\hat{S}_k$,
при чему ε_{ijk} представља, тзв., симбол Леви-Чивита и користимо, тзв., Ајнштајнову конвенцију (индекс који се понавља у производу указује на сабирање по том индексу);

2. ова опсервабла делује над спинским (фактор-) простором стања, H_s, који је за вредност спина $s = 1/2$ дводимензионални простор стања, и један базис је, нпр., $\left\{\left|\pm\right\rangle_z\right\}$, својствени базис $\hat{S}_z$: $\hat{S}_z\left|\pm\right\rangle_z = \pm\frac{\hbar}{2}\left|\pm\right\rangle_z$;

3. задовољене су следеће, симултане својствене једнакости (број s је квантни број спина):

$$\hat{\vec{S}}^2\left|sm_s\right\rangle=\frac{3}{4}\hbar^2\left|sm_s\right\rangle \qquad \left|1/2,\pm1/2\right\rangle\equiv\left|\pm\right\rangle_z;$$
$$\hat{S}_z\left|sm_s\right\rangle=m_s\hbar\left|sm_s\right\rangle, s=1/2, m_s=\pm1/2$$

4. уводи се векторска Паулијева опсервабла, $\hat{\vec{\sigma}}=\{\sigma_i, i=1,2,3\}$, дефинисана једнакошћу $\hat{\vec{S}}=\frac{\hbar}{2}\hat{\vec{\sigma}}$. Компоненте овог оператора, тзв., Паулијеви оператори, задовољавају следећу алгебру:

$$\left[\hat{\sigma}_i,\hat{\sigma}_j\right]=2i\varepsilon_{ijk}\hat{\sigma}_k$$
$$\left\{\hat{\sigma}_i,\hat{\sigma}_j\right\}=2\delta_{ij}$$
;

5. у $\hat{\sigma}_z$ репрезентацији Паулијеви оператори се репрезентују Паулијевим матрицама:

$\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$; циклична замена индекса репрезентације ($y\to z\to x$) води цикличној замени индекса репрезентационих матрица.

Физички, (*а по аналогији са моментом импулса*) спин честице дефинише магнетни диполни момент, $\hat{\mu}_s=-g_s\mu_B\hat{\vec{S}}$ (g_s је фактор који се феноменолошки утврђује), који у спољашњем (класичном) магнетном пољу магнетне индукције $\vec{B}$ уводи потенцијалну енергију спинског магнетног дипола, $\hat{V}_s=-\hat{\vec{\mu}}_s\cdot\vec{B}$.

Детаљно увођење спина, докази свих релација и горе наведених детаља се могу наћи у свим уџбеницима; видети, нпр., *Хербут 1984.*

2.9 Постулат о вишечестичним системима. Паулијев принцип

Ако се физички систем састоји из скупа од N квантних честица, тада се простор стања таквог, сложеног, система посебно дефинише.

ПОСТУЛАТ О ВИШЕЧЕСТИЧНИМ СИСТЕМИМА:
Свакој (i -тој) квантној честици у систему се придружује један простор стања, H_i. Простор стања H сложеног система је дефинисан као тензорски производ стања појединачних квантних честица, $H=\otimes_i H_i$.

Број степена слободе појединачних квантних честица у сложеном систему може бити произвољан. Отуда простор стања сложеног система може математички представљати уистину сложену структуру.

Од свих врста сложених система, од највећег интереса су системи, тзв., *неразличивих (идентичних) честица*. „Неразличивост“ заправо подразумева једнакост свих основних параметара честица у скупу, као што су маса, наелектрисање, спин. А у контексту квантне механике, од посебног значаја је спин квантних честица.

Наиме, у зависности од вредности спина (s), скупу идентичних честица се могу придружити различити простори стања. *Пропис* који то успоставља је заправо феноменолошко правило које има за последицу, тзв., Паулијев принцип искључења.

Честице целобројног спина (0, 1, 2, 3, ..) називају се *бозонима*, док се честице полубројног спина (1/2, 3/2, 5/2,...) називају *фермионима*. Поменуто феноменолошко правило успоставља да простор стања идентичних бозона чине искључиво *симетрична* стања. За фермионе, исто правило успоставља да простор стања идентичних фермиона чине само *антисиметрична* стања.

Симетричност и антисиметричност су особине вектора стања у односу на *пермутацију честица*. Наиме, ако заменимо два *бозона*, стање скупа идентичних бозона се не сме променити. За *фермионе*, пак, пермутација пара честица успоставља предзнак „минус“ као последицу: $|\psi\rangle \xrightarrow{\text{пермутација}} -|\psi\rangle$. За пар идентичних бозона, *симетрично* стање је дато изразом:

$$\frac{1}{\sqrt{2}}\left(|\psi\rangle_1|\chi\rangle_2 + |\chi\rangle_1|\psi\rangle_2\right). \qquad (2.12)$$

Дакле, два идентична бозона се могу наћи у једном од два могућа стања, ψ или χ, а због идентичности честица, не знамо који бозон је у којем стању. Формално, бозоне бројимо индексима 1 и 2, а њихова идентичност се огледа у постојању „корелисаног стања“; да је, пак, стање система „некорелисано“, $|\psi\rangle_1|\chi\rangle_2$, тада би стање првог бозона у пару било ψ, а другог χ, те би разликовање квантних стања омогућило разликовање квантних честица.

За пар фермиона, *антисиметрично* стање је дато са:

$$\frac{1}{\sqrt{2}}\left(|\psi\rangle_1|\chi\rangle_2 - |\chi\rangle_1|\psi\rangle_2\right). \qquad (2.13)$$

Пермутација честица (тј., замена индекса 1 и 2, или, еквиваленето, стања ψ и χ), води промени предзнака у изразу за коначно стање пара фермиона. Као непосредна последица антисиметричности уочава се: једнакост стања, $\psi = \chi$, имплицира једнакост нули за стање укупног система (пара фермиона), што заправо значи да таква стања у скупу идентичних фермиона не могу постојати. Та забрана да се било која два фермиона у скупу идентичних фермиона могу наћи у истом стању је позната као феноменолошко правило атомске физике познато под називом „Паулијев принцип“. И то правило тиче се било којег броја идентичних фермиона, не само пара фермиона као у горњем примеру.

Горе-поменуто правило о просторима стања сада успоставља да се у суперпозицији

$$\sum_i c_i|\varphi_i\rangle$$

за скуп идентичних бозона могу наћи само и искључиво симетрична стања $|\varphi_i\rangle$, док се за скуп фермиона у суми могу наћи искључиво и само антисиметрична стања $|\varphi_i\rangle$. Изградња таквих стања за вишечестичне системе идентичних бозона, или фермиона, се непосредно уопштава на основи израза (2.12), или (2.13), и може се наћи у литаратури (в. *Хербут 1984*).

Коначно, важно је истаћи да се горе представљено правило о просторима стања идентичних бозона и фермиона тиче чак и система у којем нема (или се не разматра) међусобна интеракција квантних честица – дакле, све једнако важи и за „идеални гас“ бозона, или фермиона. Међуделовање (интеракција) у систему је додатни услов који овде није разматран. Тиме смо желели да посебно истакнемо значај принципа неразличивости (идентичности) за квантне честице, с обзиром на чињеницу да „корелисаност“ стања (2.12), тј. (2.13), *није* последица интеракције међу честицама сложеног система – корелисаност стања сложеног система као последица интеракције подсистема је предмет задатка 2.9.

НАПОМЕНА: Феноменолошко правило идентичности се не примењује на сваки скуп идентичних честица. На пример, последица овог правила, Паулијев принцип, се не може применити на све електроне у свемиру, иако би се на први поглед то могло претпоставити на основи горње дискусије. Паулијев принцип се тиче, нпр., скупа електрона у *једном* атому, али не и електрона који припадају *различитим* атомима – *осим* ако атоми чине један молекул. Тако се говори и о „тачности“ важења Паулијевог принципа, тј., општије, о *тачности феноменолошког правила о идентичности квантних честица*. У пракси, применљивост овог правила се успоставља за сваку физичку ситуацију понаособ. Нпр., Паулијев принцип важи за све електроне у једном молекулу (или једном атому), као и у једном „комаду“ метала (када чине „електронски гас“). Слично, сви атоми хелијума у датом делу запремине течног хелијума чине скуп идентичних бозона – што представља квантномеханичку основу, тзв., Бозе-Ајнштајнове кондензације, као теоријске основе суперфлуидности течног хелијума.

2.10 Вишечестични систем спинова-1/2

Нека је задат скуп „спинова“, сваки спин 1/2. Конкретно, то значи да нас не занимају „спољашњи“ степени слободе, већ само спински степени слободе скупа квантних честица. Тада је, сходно Постулату у степенима слободе (како спољашњим, тако и унутрашњим), простор стања таквог скупа заправо тензорски производ простора стања појединих спинова, $\otimes_i H_i$, где је сваки H_i простор стања једног спина 1/2, описан у Одељку 2.8.

У зависности да ли се тај скуп спинова тиче међусобно идентичних, или неидентичних квантних честица, правила рада су различита – у првом случају, има се примењивати Постулат о идентичним честицама.

Размотримо овде други случај који је од интереса за квантну информатику и рачунање.

Тада је опште стање таквог скупа дато обликом:

$$\sum_{i,j,k,\ldots} c_{ijk\ldots}|i\rangle_1|j\rangle_2|k\rangle_3\ldots,$$

где $i, j, k, \ldots$ могу узети вредности $\pm 1/2$ – видети Одељак 2.8. Ако спинови међусобно *не интерагују*, тада су дозвољена и некорелисана стања $|i\rangle_1 |j\rangle_2 |k\rangle_3 \ldots$, у којима је познато стање сваког спина у систему. Ако уведемо ознаке $|1/2\rangle \equiv |0\rangle, |-1/2\rangle \equiv |1\rangle$ за сваки спин у скупу, тада ОНБ система спинова којег чине искључиво некорелисана стања се може краће записати. Нпр., за скуп од N таквих спинова, може се писати:

$$
\begin{aligned}
&|0\rangle_1 |0\rangle_2 \ldots |0\rangle_{N-1} |0\rangle_N \equiv |00\ldots00\rangle \equiv |0\rangle \\
&|0\rangle_1 |0\rangle_2 \ldots |0\rangle_{N-1} |1\rangle_N \equiv |00\ldots01\rangle \equiv |1\rangle \\
&|0\rangle_1 |0\rangle_2 \ldots |1\rangle_{N-1} |1\rangle_N \equiv |00\ldots11\rangle \equiv |2\rangle \qquad (2.14) \\
&\ldots \\
&|1\rangle_1 |1\rangle_2 \ldots |1\rangle_{N-1} |1\rangle_N \equiv |11\ldots1\rangle \equiv |2^N - 1\rangle
\end{aligned}
$$

Тада се свако стање таквог система може представити, у општем случају, у облику:

$$\sum_{i=0}^{2^N-1} c_i |i\rangle , \qquad (2.15)$$

где индекс i пребројава елементе горњег базиса у ознакама (2.14).

2.11 Квантна динамика

За кватни систем који не међуделује ни са једним физички системом и највише се може наћи у неком спољашњем пољу (електричном, магнетном и сл.) се каже да представља *изоловани*[10] квантни систем. За такве, изоловане квантне системе, успоставља се постулат о „закону кретања“ који описује и одређује динамику система – тј., промену његовог стања у времену. Због подвојености стања од опсервабли, постоји еквивалентни запис закона кретања изолованих система у терминима опсервабли, што се назива „Хајзенберговом сликом“. Закон кретања (динамика) система у терминима стања се назива „Шредингеровом сликом“.

Динамика система се успоставља следећом рецептуром[11]: (а) квантизацијом класичне Хамилтонове функције добија се опсервабла енергије (Хамилтонијан) система $\hat{H}$, који се (б) замењује у операторски израз

$$\hat{U} = exp\{-i\hat{H}(t - t_0)/\hbar\} \qquad (2.16)$$

за све „*конзервативне*“ системе, дефинисане условом $\partial\hat{H}/\partial t = 0$. Тада се промена стања у времену може описати једнакошћу

---

[10] У новијој литератури се користи и израз „затворени“ (енгл: *closed*).

[11] У строгој формулацији квантне механике, рецептура следи из, тзв., Постулата о закону кретања - видети *Хербут 1984.*

$$|\psi(t)\rangle = \hat{U}|\psi(t_0)\rangle\,, \tag{2.17}$$

или, еквивалентно, нестационарнаом *Шредингеровом једначином*:

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = \hat{H}|\psi(t)\rangle. \tag{2.18}$$

За конзервативне системе Шредингерова једначина (2.18) се своди на решавање својственог проблема (в. ***Додатак 2.2***) хамилтонијана:

$$\hat{H}|\psi_n\rangle = E_n|\psi_n\rangle\,, \tag{2.19}$$

где се не појављује време као параметар. Ова једначина се назива „стационарном“ Шредингеровом једначином. Временска зависност у стањима, решењима Шредингерове једначине (2.18), се појављује кроз фазни фактор, тј., дефинишу се „стационарна стања“ (искључиво за конзервативне системе) у облику:

$$exp\{-itE_n/\hbar\}|\psi_n\rangle, \tag{2.20}$$

где је стављено $t_0 = 0$ (само за конзервативне системе, за које је *време хомогено* - сви временски тренуци су међусобно равноправни - дозвољен је овај избор почетног тренутка).

Познавање стања система у једном тренутку успоставља ***једнозначно стање тог система у сваком каснијем тренутку***, што је по свом садржају заправо физичка ***каузалност***. Промена стања у времену је једнозначна и инвертибилна (реберзибилна), јер оператор промене стања у времену, $\hat{U}$, је унитаран: $\hat{U}^{+} = \hat{U}^{-1}$.

2.12 Појам квантног мерења. Пројекциони постулат

Поступак квантног мерења је физички процес који од објекта мерења (тј., од квантног система на којем се врши мерење) чини *неизоловани* („*отворени*“) квантни систем. Наиме, свако мерење подразумева *међуделовање* објекта мерења и мерног инструмента („апарата“). То међуделовање није типа „спољашњег поља“. Отуда се квантно мерење не описује Шредингеровом једначином, већ се резултати мерења (интеракције објекта и апарата) описује постулатом о вероватноћама мерења.

Важно је истаћи: процес мерења је динамички процес, у којем се систему придружују почетно и коначно стање, у различитим (имплицитним дискусији) временским тренуцима[12].

Од свих врста мерења (видети Поглавље III) од посебног интереса су, тзв., *предиктивна* мерења. То су *поновљива* мерења (после обављеног мерења објекат мерења се може припремити за неко друго мерење) за која је *познато коначно*

[12] Отуда и тешкоће у тумачењу релација неодређености (Одељак 2.5) у терминима процеса мерења – релације неодређености се тичу стања фиксираног у времену.

стање објекта мерења (стање после мерења). Ако је мерена опсервабла чији је спектрални облик дат изразом (2.4) и ако је добијена вредност a_n, тада, тзв., *Пројекциони постулат* (*von Neumann 1955*), за предиктивна мерења успоставља да је коначо стање $|\chi^{(n)}\rangle$ после мерења дато изразом:

$$|\chi^{(n)}\rangle = \left(\langle\psi|\hat{P}_n|\psi\rangle\right)^{-1/2}\hat{P}_n|\psi\rangle\,. \qquad (2.21)$$

Пројекциони постулат успоставља могућност да кажемо у ком стању се после мерења налази квантни систем – и то када нас занима само један резултат мерења. Општија ситуација је описана у Поглављу III. Тако се предиктивним мерењем може припремити („препарирати“) жељено стање квантног система, обављањем предиктивног мерења описаног изразом (2.21).

2.13 Напомене и коментари

Основни постулати квантне механике се тичу сваког, *ма како сложеног система*. Задатак изучавања сложених система, у смислу анализе квантног понашања *подсистема*, је посебан задатак и делимично је представљен у Одељку 5.3.

Стање квантног система, $|\psi\rangle$, не представља ни „честицу“, ни „талас“, већ *квантни систем* чије понашање (на пример: или честично, или таласно) зависи од услова под којима се систем налази. Отуда нема места визуелизацији физичких система и процеса, попут оне дате на Сл. 2.1.

Квантна механика познаје неодређеност „мерену“ стандардним одступањима опсервабли, тј., релацијама неодређености. У извесном смислу, ова неодређеност – квантна неодређеност – је у средишту пажње квантне информатике.

Квантна механика барата двема врстама динамике (промене стања у времену). *Једна* је описана Шредингеровом једначином, има особину повратности (реверзибилности), и тиче се „изолованог“ система; по својој природи је каузална. *Друга* врста динамике описана је процесом мерења и постулатом о вероватноћама мерења и тиче се објекта мерења (који није изолован, већ интерагује са мерним инструментом).

У поређењу са класичном механиком, Одељак 2.1, квантна механика се чини врло необичном теоријом. Али зато је рецептура њене примене *концепцијски* једноставна: „само“ треба пратити постулате и рецепте прорачуна динамике, тј., вероватноћа мерења на систему.

У извесном смислу, квантна информатика представља примену самих *основних* принципа квантне механике у контексту задатака процесирања информације.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- За основе теорије Хилбертових простора користити одличну књигу *Vujičić 2008.*
- За основе квантне механике консултовати *Хербут 1984* (посебно препоручујемо за детаље, физичке и формализма, спина-1/2), *Messiah 1976.*
- За основе квантне теорије мерења консултовати *von Neumann 1955, Хербут 1984, Дугић 2004.*

Овде изложени приступ основама квантне механике сличан је приступу изложеном у *Nielsen and Chuang 2000.*

ЗАДАЦИ:

2.1 За скуп пројектора $\{\hat{P}_i\}$ проверити односе између пројектора који морају бити задовољени да би следећи оператори такође били пројектори:
(а) $\hat{P}_i + \hat{P}_j$,
(б) $\hat{P}_i\hat{P}_j$.

Решење: (а) $\left(\hat{P}_i + \hat{P}_j\right)^2 = \hat{P}_i^2 + \hat{P}_j^2 + \hat{P}_i\hat{P}_j + \hat{P}_j\hat{P}_i = \hat{P}_i + \hat{P}_j + \hat{P}_i\hat{P}_j + \hat{P}_j\hat{P}_i$, одакле следи да ортогоналност пројектора, $\hat{P}_i\hat{P}_j = \delta_{ij}\hat{P}_j$, што важи и за под (б).

2.2 Доказати еквивалентност следећих исказа за пар опсервабли:
(а) опсервабле $\hat{A}$ и $\hat{B}$ међусобно комутирају,
(б) сви својствени пројектори опсервабле $\hat{A}$ комутирају са свим својственим пројекторима опсервабле $\hat{B}$.

2.3 Задата је опсервабла својом спектралном формом: $\hat{A} = \sum_n a_n\hat{P}_n$. Доказати да за сваку аналитичку функцију f важи: $f(\hat{A}) = \sum_n f(a_n)\hat{P}_n$.

Решење: Представимо аналитичку функцију f преко реда: $f\left(\hat{A}\right) = \sum_n \alpha_n\hat{A}^n$. Сменом спектралне форме опсервабле $\hat{A}$ у овај израз добија се:

$$f\left(\hat{A}\right) = \sum_n \alpha_n\left(\sum_i a_i\hat{P}_i\right)^n = \sum_{n,i} \alpha_n {a_i}^n\hat{P}_i = \sum_i\left(\sum_n \alpha_n {a_i}^n\right)\hat{P}_i = \sum_i f\left(a_i\right)\hat{P}_i,$$

где је коришћена особина ортогоналности и идемпотентности пројектора.

2.4 Решити Шредингерову једначину за слободну честицу ван поља. Доказати дискретност вредности импулса (и енергије) ако се кретање честице просторно ограничи на област чија је једна димензија реда величине неке константе L. (Једноставности ради, започети са једнодимензионалном „честицом“.)

Решење: У, тзв., координатној репрезентацији (Додатак 2.2, Хербут 1984), оператор импулса постаје изводни оператор: $-i\hbar\frac{d}{dx}$ за једнодимензионални систем. Квадрат импулса се отуда репрезентује као $-\hbar^2\frac{d^2}{dx^2}$. Тако Шредингерова једначина за слободну честицу масе m добија облик:

$$-\frac{\hbar^2}{2m}\frac{d^2}{dx^2}\psi(x)=\frac{p^2}{2m}\psi(x). \qquad (2a)$$

Ограничавање области кретања слободне честице на димензију L се може записати као *гранични услови*: $\psi(x=-L/2)=0=\psi(x=L/2)$. Како су решења једначине (2а) заправо експоненцијелне функције, $C\exp(ixp/\hbar)$, то гранични услови испостављају једнакости:

$$exp(-iL\cdot p/2\hbar)=0=exp(iLp/2\hbar), \qquad (2б)$$

што се мора обавити независно за синусне и косинусне чланове ($e^{ix}=\cos x+i\sin x$), $\sin x=0=\cos x$ за $x=-L/2,L/2$. Отуд лако следе закључци: за косинусне функције важи $kL=\frac{n\pi}{2}, n=1,3,5,\ldots$, док за синусне важи исто, али за парно $n=2,4,6,\ldots$, одакле $E_n=\frac{\hbar^2}{2m}k_n^2=\frac{\hbar^2\pi^2}{8mL^2}n^2, n=1,2,3,4,5,\ldots$. Уопштења на више димензија су непосредна.

2.5 Доказати „инваријантност трага“, тј., да је за задат оператор $\hat{A}$, $tr\hat{A}$ јединствен број који не зависи од избора базиса по којем се „траг“ израчунава.

Решење: $tr\hat{A}\equiv\sum_n\langle n|\hat{A}|n\rangle$. Изаберимо други ОНБ, $\{|\alpha\rangle\}$, у истом Хилбертовом простору. Запишимо д.с. израза за траг као $\sum_n\langle n|\hat{I}\hat{A}\hat{I}|n\rangle$. Декомпонујмо сада идентичне операторе по новом базису и заменимо у овај израз да добијемо:

$$\sum_{n,\alpha,\alpha'}\langle n|\alpha\rangle\langle\alpha|\hat{A}|\alpha'\rangle\langle\alpha'|n\rangle=\sum_{\alpha,\alpha'}\langle\alpha|\hat{A}|\alpha'\rangle\sum_n\langle\alpha'|n\rangle\langle n|\alpha\rangle=\sum_{\alpha,\alpha'}\langle\alpha|\hat{A}|\alpha'\rangle\delta_{\alpha\alpha'}=\sum_\alpha\langle\alpha|\hat{A}|\alpha\rangle.$$

Тиме је доказ завршен.

2.6 У израз за стање (2.13) ставити:

$$|\psi\rangle=\frac{1}{\sqrt{13}}\begin{pmatrix}2\\3i\end{pmatrix},|\chi\rangle=\frac{1}{\sqrt{13}}\begin{pmatrix}3\\-2i\end{pmatrix},$$

и израчунати (в. ***Додатак 2.2***) парцијални траг по првом подсистему за стање сложеног система задато изразом (2.13).

Решење: Стање (2.13) је сада задато као $|\Psi\rangle=\frac{1}{13\sqrt{2}}\left(\begin{pmatrix}2\\3i\end{pmatrix}_1\otimes\begin{pmatrix}3\\-2i\end{pmatrix}_2-\begin{pmatrix}3\\-2i\end{pmatrix}_1\otimes\begin{pmatrix}2\\3i\end{pmatrix}_2\right)$. Задатак је да израчунамо $tr_1|\Psi\rangle\langle\Psi|$. Како показује следећи задатак, избор базиса за прорачун парцијалног трага је произвољан. Зато ћемо одабрати баш базис из поставке задатка, ${}_1\langle\psi|\Psi\rangle\langle\Psi|\psi\rangle_1+{}_1\langle\chi|\Psi\rangle\langle\Psi|\chi\rangle_1$, што у матричном запису постаје:

$$\frac{1}{26}\begin{pmatrix}2 & -3i\end{pmatrix}\frac{1}{13}\left(\begin{pmatrix}2\\3i\end{pmatrix}_1\otimes\begin{pmatrix}3\\-2i\end{pmatrix}_2-\begin{pmatrix}3\\-2i\end{pmatrix}_1\otimes\begin{pmatrix}2\\3i\end{pmatrix}_2\right)\left[\frac{1}{13}\left(\begin{pmatrix}2\\3i\end{pmatrix}_1\otimes\begin{pmatrix}3\\-2i\end{pmatrix}_2-\begin{pmatrix}3\\-2i\end{pmatrix}_1\otimes\begin{pmatrix}2\\3i\end{pmatrix}_2\right)\right]^+\begin{pmatrix}2\\3i\end{pmatrix}_1+$$

$$\frac{1}{26}\begin{pmatrix}3 & 2i\end{pmatrix}\frac{1}{13}\left(\begin{pmatrix}2\\3i\end{pmatrix}_1\otimes\begin{pmatrix}3\\-2i\end{pmatrix}_2-\begin{pmatrix}3\\-2i\end{pmatrix}_1\otimes\begin{pmatrix}2\\3i\end{pmatrix}_2\right)\left[\frac{1}{13}\left(\begin{pmatrix}2\\3i\end{pmatrix}_1\otimes\begin{pmatrix}3\\-2i\end{pmatrix}_2-\begin{pmatrix}3\\-2i\end{pmatrix}_1\otimes\begin{pmatrix}2\\3i\end{pmatrix}_2\right)\right]^+\begin{pmatrix}3\\-2i\end{pmatrix}_1= \quad (2в)$$

$$\frac{1}{26}\left(\begin{pmatrix}3\\-2i\end{pmatrix}_2{}_2\begin{pmatrix}3 & 2i\end{pmatrix}+\begin{pmatrix}2\\3i\end{pmatrix}_1{}_2\begin{pmatrix}2 & -3i\end{pmatrix}\right)=\frac{1}{2}\left(\frac{1}{\sqrt{13}}\begin{pmatrix}3\\-2i\end{pmatrix}_2\frac{1}{\sqrt{13}}{}_2\begin{pmatrix}3 & 2i\end{pmatrix}+\frac{1}{\sqrt{13}}\begin{pmatrix}2\\3i\end{pmatrix}_1\frac{1}{\sqrt{13}}{}_2\begin{pmatrix}2 & -3i\end{pmatrix}\right)=$$

$$\frac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}_2$$

2.7 Доказати да операција „узимања парцијалног трага“ има особину независности од базиса по којем се врши узимање трага.

2.8 Задат је „двочестични оператор“ $\hat{A}_1\otimes\hat{B}_2$. Ако је спектрална форма $\hat{A}_1=\sum_m a_m\hat{P}_{1m}$, доказати важење једнакости:

$$\exp\{-i\alpha\hat{A}_1\otimes\hat{B}_2\}=\sum_m\hat{P}_{1m}\otimes\exp\{-i\alpha a_m\hat{B}_2\},\ \alpha\in R.$$

Упутство: користити резултат Задатка 2.3.

2.9 На стање „двочестичног система“, $|\phi\rangle_1|\chi\rangle_2$, применити оператор задат у претходном задатку и доказати важење једнакости:

$$\exp\{-i\alpha\hat{A}_1\otimes\hat{B}_2\}|\phi\rangle_1|\chi\rangle_2=\sum_i c_i|\psi_m\rangle_1|\chi_m(\alpha)\rangle_2,$$

за стања $|\psi_m\rangle_1$ својствена за $\hat{A}_1$. Како су дефинисана стања $|\chi_m(\alpha)\rangle_2$? Физички коментарисати резултат ако $\alpha=t/\hbar$, где је t време.

Решење: Прво, разложимо стање $|\phi\rangle_1$ по неком својственом базису $\hat{A}_1$: $|\phi\rangle_1=\sum_m|\psi_m\rangle_1$. Сменом овог израза у некорелисано почетно стање, а на основи претходног задатка, следи:

$$\exp\{-i\alpha\hat{A}_1\otimes\hat{B}_2\}\sum_m|\psi_m\rangle_1|\chi\rangle_2=\sum_{m'}\hat{P}_{1m'}\otimes\exp\{-i\alpha a_{m'}\hat{B}_2\}\sum_m|\psi_m\rangle_1|\chi\rangle_2.$$

Како се пројектори и својствена стања заправо тичу опсервабле $\hat{A}$, то важи: или $\hat{P}_{1m'}|\psi_m\rangle_1=0$, или $\hat{P}_{1m'}|\psi_m\rangle_1=1$. Отуда д.с. непосредно добија тражени облик, уз дефиницију: $|\chi_m(\alpha)\rangle_2=\exp\{-i\alpha a_{m'}\hat{B}_2\}|\chi\rangle_2$. Наравно, ако је $\alpha=t/\hbar$, онда доказани израз представља израз ***временске еволуције сложеног система***, тј. формирање сплетености услед интеракције подсистема 1 и 2, а све под претпоставком да за ***сложени систем важи Шредингерова једначина***.

2.10 Доказати погрешност једног тумачења релација неодређености Одељка 2.5.

Решење: израз (2.21) за стање $|\psi\rangle$ на којем је вршено мерење опсервабле $\hat{A}$, успоставља коначно стање $|\chi\rangle$, које је ствојствено за $\hat{A}$. „Погрешно тумачење“ заправо успоставља однос

стандардних одступања опсервабле $\hat{A}$ у *почетном* стању $|\psi\rangle$ и неке опсервабле $\hat{B}$ у *коначном* стању $|\chi\rangle$ – што је у супротности са формулацијом Теорема 2.1, где се појављује само једно стање. Дакле, иако се квантним мерењем мења стање (видети Одељак 3.8 за детаље), та промена стања није мерена релацијама неодређености.

III КВАНТНА СТАЊА, АНСАМБЛИ И МЕРЕЊЕ

Већина задатака квантне механике почиње реченицом типа: „ако се систем (тј., ансамбл) налази у стању $|\psi\rangle$ ...“. Али то отвара питање повезивања, тј., ***придруживања стања ансамблу*** (који се остварује у лабораторији). Одговор на питање овог придруживања је основна тема овог поглавља.

3.1 Општа схема квантних мерења. Чисти и мешани анасамбли

Постулат о вероватноћама мерења успоставља да је: (*1*) квантно мерење обављено на систему у унапред познатом стању, и да (*2*) стохастичност мерења подразумева обављање мерења на (квантном) ***ансамблу***. Тако се у квантној механици подразумева да се мерење обавља на скупу од N идентично (макроскопски, лабораторијски идентичних) копија система које међусобно не интерагују. И припрема копија (појединачних система на којима се обавља мерење), и сам поступак мерења се обављају на исти начин за сваки појединачни систем. У лимесу $N \to \infty$, такав скуп представља ***квантни ансамбл***. Статистичке фреквенције сваке измерене вредности, у лимесу $N \to \infty$, израз (2.8), дају расподелу вероватноћа за обављено мерење, $\{p_i\}$, која се може упоредити са теоријским предвиђањем, израз (П.2).

У зависности од начина обављања, квантна мерења могу се поделити по више критеријума. *Први критеријум* се тиче начина обављања мерења, и ту се разликују мерења која одговарају *ансамблима просторног* и *временског типа*. Просторни ансамбл подразумева да сви елементи ансамбла истовремено бивају објектима мерења. Временски ансамбл подразумева мерење на појединачним системима у одређеном временском следу. Реална мерења су комбинација ова два. *Други критеријум* се тиче резултата мерења. Ако је од интереса само један могући резултат мерења, онда се ради о, тзв., *селективном мерењу*. Ако је од интереса већи број резултати мерења, ради се о, тзв., *неселективном мерењу*. *Трећи критеријум* се тиче стања објекта мерења после обављеног мерења. Ако је после обављеног мерења објекат мерења и даље на располагању за мерење, онда се ради о *поновљивим* мерењима. Ако то није случај, онда се ради о *непоновљивим мерењима, у којима објект мерења „нестаје“* – као у детекцији квантних честица (на пример, на застору, или у Гајгер-Милеровом бројачу). Посебан пример поновљивих мерења су, тзв., *предиктивна* мерења (Одељак 3.2), у којима је познато стање објекта *после мерења*. Посебан пример непоновљивих мерења су *ретроспективна* мерења у којима се добијене информације о објекту мерења тичу времена *пре* обављеног мерења (на пример: коју путању је квантна честица имала пре детекције на застору).

Нека је ансамбл сачињен од N појединачних система (елемената ансамбла). Нека је у питању мерење неке опсервабле $\hat{A}$ са чисто дискретним спектром вредности, $\{a_i\}$. Тада се у мерењу ове опсервабле, у општем случају, добија резултат a_i у N_i понављања мерења на ансамблу. При томе:

$$\sum_i N_i = N\,, \tag{3.1}$$

док

$$p_i = \lim_{N\to\infty} \frac{N_i}{N} = W\left(\hat{A}, |\psi\rangle, a_i\right),\ \sum_i p_i = 1\,, \tag{3.2}$$

представља вероватноћу добијања ове вредности. Подскуп почетног ансамбла на којем је добијена вредност a_i, уколико је дозвољен лимес $N_i \to \infty$, представља *подансамбл* коначног ансамбла – ансамбла који је добијен после обављеног мерења. За такав подансамбл, који одговара селективном мерењу (једна вредност a_i), се каже да је ***„чист“ (под)ансамбл***. Коначни ансамбл у којем се налазе резултати свих N мерења, и који се састоји из „чистих“ (под)ансамбала, се назива ***„мешаним“***. Симболично представљено, чисти подансамбли, S_i, су смешани у коначном, укупном, мешаном ансамблу:

$$S = \cup_i S_i\,, \tag{3.3}$$

који одговара неселективној варијанти мерења опсервабле $\hat{A}$. Чистим ансамблима се придружују чиста („кохерентна“[1]) стања (што су елементи Хилбертовог простора стања), док се мешаним ансамблима придружују, тзв., мешана („некохерентна“) стања.

3.2 Предиктивно мерење

Посебна врста поновљивих мерења, предиктивно мерење, има особину да је ***коначно стање ансамбла после мерења једнозначно познато*** – за детаље видети Одељак 3.8.

ДЕФ. 3.1 Поновљиво квантно мерење произвољне опсервабле $\hat{E}$ назива се ***предиктивним (мерењем 1. врсте)*** уколико за сваку измерену вредност опсервабле, на ансамблу у било ком почетном стању $|\psi\rangle$, важе следећи услови[2]:

(*i*) израз (3.2) за вероватноће мерења,

(*ii*) по престанку мерења, поновљено мерење исте опсервабле на чистом ансамблу S_k (којем одговара измерена вредност E_k у селективној варијанти мерења) би апсолутно сигурно (дакле, са вероватноћом 1) дало резултат E_k,

(*iii*) ако је нека опсервабла, $\hat{F}$, која комутира са мереном опсерваблом $\hat{E}$, имала једнозначну (оштру) вредност пре мерења, имаће ту исту, једнозначну вредност и после мерења опсервабле $\hat{E}$.

---

[1] Ово је назив, а не посебна врста стања. Постоје и *кохерентна стања*, тј. стања са *минималном неодређеношћу*, која се не смеју побркати са овим термином.

[2] *Herbut 1969, 1974.*

3.3 Потпун скуп компатибилних опсервабли (ПСКО)

Опсервабла $\hat{A}$ чије су *све својствене вредности недегенерисане* се назива *потпуном (комплетном) опсерваблом*. Наравно, то не мора бити случај – и у пракси је правило да су макар неке својствене вредности опсервабле дегенерисане. Али одређени скуп таквих, „не-комплетних“ опсервабли, може бити уопштење комплетне опсервабле. Такав скуп међусобно компатибилних опсервабли се назива *потпуним (комплетним) скупом компатибилних опсервабли (ПСКО)*.

Свака опсервабла $\hat{A}$ одређена је спектралном формом, нпр., типа:

$$\hat{A} = \sum_i a_i \hat{P}_i \,, \tag{3.4}$$

при чему својствени пројектор $\hat{P}_i$ дегенерисане вредности (a_i) једнозначно одговара не-једнодимензионалном својственом подпростору, H_i; при томе, $tr\hat{P}_i = \dim H_i$. Јасно је: да би се смањио број димензија својствених подпростора H_i, неопходно је придодати друге опсервабле које би додатно разложиле подпросторе H_i. А за то је потребно додати компатибилне опсервабле. Тако опсервабли $\hat{A}$ треба придодати њој компатибилну опсерваблу $\hat{B}$ чији би својствени подпростори разложили подпросторе H_i, а онда, ако је то потребно, пару $\left(\hat{A},\hat{B}\right)$ придодати њима компатибилну опсерваблу $\hat{C}$, и читав поступак обављати док сви подпростори H_i не буду разложени на једнозначне, једнодимензионалне подпросторе – баш као у случају комплетне опсервабле.

Овим поступком се добија *једнозначни заједнички својствени базис* за дати ПСКО[3], $\left(\hat{A},\hat{B},\hat{C},...\right)$:

$$\begin{aligned}
&\hat{A}\left|a_i,b_j,c_k,...\right\rangle = a_i\left|a_i,b_j,c_k,...\right\rangle \\
&\hat{B}\left|a_i,b_j,c_k,...\right\rangle = b_j\left|a_i,b_j,c_k,...\right\rangle \\
&\hat{C}\left|a_i,b_j,c_k,...\right\rangle = c_k\left|a_i,b_j,c_k,...\right\rangle \\
&...
\end{aligned} \tag{3.5}$$

где је јасно да је свако заједничко својствено стање једног ПСКО-а једнозначно одређено неком комбинацијом својствених вредности опсервабли из тог ПСКО. При томе, и то је важно уочити, неке комбинације својствених вредности опсервабли из датог ПСКО-а не одговарају ни једном заједничком својственом стању. Скуп стања $\left\{\left|a_i,b_j,c_k,...\right\rangle\right\}$ представља један ортонормирани базис (ОНБ) у укупном простору стања, $H = \sum_i{}^{\oplus} H_i$. Тај базис је *једнозначни* заједнички

[3] Важно је уочити да једна опсервабла може припадати различитим ПСКО-овима.

својствени базис опсервабли из датог ПСКО. На овај начин се уопштава комплетна опсервабла, која има једнозначан својствени базис.

Наравно, важи и следеће: свако чисто стање је једнозначно (као једнодимензионални подпростор) одређено скупом својствених вредности опсервабли из неког ПСКО. Отуда и ***пропис за придруживање стања ансамблу, и обрнуто***: сваки чисти ансамбл се налази у чистом стању, неком $|\phi\rangle$, које је одређено (једнозначним) скупом својствених вредности опсервабли из неког ПСКО. А како се то остварује, одговориће нам следећи одељак.

3.4 Придруживање стања ансамблу

Свако селективно предиктивно мерење даје једнозначно познато коначно стање (чистог под-)ансамбла. Тако, и истовремено („симултано“), селективно предиктивно мерење *свих* опсервабли из неког ПСКО даје, као резултат, једнозначно познато, коначно, чисто стање. То је уједно и ***пропис*** за ***придруживање стања ансамблу*** (и обрнуто), као и поступак припреме (препарације) ансамбла: *обави се симултано, селективно предиктивно мерење свих опсервабли из неког ПСКО, и добијени ансамбл се налази у једнозначно одређеном, чистом стању*. За доказ видети израз (2.21) и његово уопштење у Одељку 3.8. Препарација ансамбла се врши у свим експериментима, те је разматрана врста мерења заправо фундаментални појам квантне механике, како теоријске, тако и експерименталне.

3.5 Симултана мерења. Квантна неодређеност

ТЕОРЕМ 3.1: За сваки скуп опсервабли из неког ПСКО, $\left\{\hat{A},\hat{B},\hat{C},..\right\}$, постоји (једнозначна) опсервабла $\hat{E}$, која је *комплетна* опсервабла, тако да важи:

$$\hat{A}=\hat{A}(\hat{E}),\hat{B}=\hat{B}(\hat{E}),\hat{C}=\hat{C}(\hat{E}),\ldots, \tag{3.6}$$

што подразумева функционалну зависност свих опсервабли из ПСКО, од комплетне опсервабле $\hat{E}$.

Одмах важи следећа, лако доказива последица: $e_n \leftrightarrow \left\{a_i,b_j,c_k,...\right\}$, где су e_n својствене вредности опсервабле $\hat{E}$, док се вредности у великој загради тичу израза (3.5).

Сада је очигледно: мерењем опсервабле $\hat{E}$, тј., добијањем неке вредности e_n, ***истовремено су измерене и све опсервабле из датог ПСКО***. То је истовремено и могућност *симултаног (истовременог) мерења* ***било ког пара*** *међусобно компатибилних опсервабли*. Наиме, сваки пар међусобно компатибилних опсервабли је подскуп неког ПСКО. А симултана меривост свих опсервабли неког ПСКО је овде, макар у принципу, успостављена.

Међутим, ***некомутирајуће опсервабле се, у општем случају, не могу истовремено мерити***[4]. Таква мерења су могућа *ако и само ако* се систем налази у неком заједничком својственом стању некомпатибилних опсервабли, у којем *обе опсервабле имају оштре вредности* које се мерењем могу утврдити. У општем случају, међутим, оштрој (једнозначној) вредности једне опсервабле $\hat{E}$, којој одговара стање $|\psi_k\rangle$, одговара *скуп вредности* друге опсервабле, $\hat{F}$, којима одговара својствени (под)базис те друге опсервабле, $\{|\varphi_n\rangle\}$. У математичком запису:

$$|\psi_k\rangle = \sum_n \alpha_{kn} |\varphi_n\rangle , \tag{3.10}$$

одакле следи да је вероватноћа мерења опсервабле $\hat{F}$ у стању $|\psi_k\rangle$ *различита од јединице* – неједнозначност вредности опсервабле $\hat{F}$ у стању $|\psi_k\rangle$, које је својствено за опсерваблу $\hat{E}$. Као меру (квантне) неодређености ове опсервабле могуће је користити њено стандардно одступање, израз (2.8):

$$\Delta\hat{F} = \sqrt{\langle\psi_k|\left(\hat{F} - \langle\psi_k|\hat{F}|\psi_k\rangle\right)^2|\psi_k\rangle} . \tag{3.11}$$

Отуда мерење једне опсервабле повлачи, у општем случају, неједнозначност („необављено мерење“) неке, њој некомутирајуће, опсервабле. Неодређеност (неједнозначност вредности) такве опсервабле представља *квантну неодређеност вредности ове опсервабле у датом (почетном) стању*, чији је формални облик дат изразом (3.11); пуно значење квантне неодређености је дато у Одељку 4.2.

3.6 Квантна мешана стања. Лиувилова једначина

Израз (3.3) уводи појам мешаних стања. Подсетимо се садржаја тог појма.

Ако стање ансамбла није једнозначно познато, онда се оно описује неком расподелом вероватноћа за стања из неког скупа. На пример, нека су стања из скупа $\{|\psi_i\rangle\}$, и нека су одговарајуће вероватноће дате расподелом вероватноћа, тј., скупом вероватноћа, $\{W_i\}$. Физички, то значи да из датог (мешаног) ансамбла, са вероватноћом W_i, можемо одабрати елемент који се налази у стању $|\psi_i\rangle$. Поставља се питање математичког описа мешаног ансамбла, то јест *стања* мешаног ансамбла.

Израз (3.3) казује да је „статистичка тежина“ подансамбла S_i (који је у чистом стању $|\psi_i\rangle$) у ствари вероватноћа W_i. Израчунајмо сада вероватноћу да се, мерењем на целом (мешаном) ансамблу, добије вредност a_n неке опсервабле $\hat{A}$. Тада се мерење „састоји“ од следећих, међусобно независних догађаја: (а) избора

[4] Под „мерењем“ подразумевамо предиктивна мерења.

елемента из једног од чистих (смешаних) подансамбала S_i, и (б) добијања вредности a_n на том, случајно одабраном, подансамблу S_i. За међусобно независне догађаје, елементарни рачун вероватноће успоставља да је укупна вероватноћа производ појединих, а за више таквих могућности, та вероватноћа је збир таквих производа:

$$W(\hat{A},\text{мешани ансамбл},a_n)=\sum_i W_i\cdot W\left(\hat{A},|\psi_i\rangle,a_n\right), \tag{3.12}$$

где смо користили ознаке Поглавља II. Сменом израза (П.2), десна страна израза (3.12) постаје:

$$\sum_i W_i\langle\psi_i|\hat{P}_n|\psi_i\rangle=tr\left(\hat{\rho}\hat{P}_n\right), \tag{3.13}$$

где је оператор $\hat{\rho}$, тзв., ***„статистички оператор“***, дефинисан изразом:

$$\hat{\rho}=\sum_i W_i|\psi_i\rangle\langle\psi_i|. \tag{3.14}$$

За ортогонална[5] стања $|\psi_i\rangle$, израз (3.14) је истовремено и спектрални облик статистичког оператора[6]. А следеће уочавање говори о томе да овај оператор представља ***стање мешаног ансамбла***.

Наиме, израз (П.2) се може преписати у облик:

$$W\left(\hat{A},|\psi\rangle,a_n\right)=\langle\psi|\hat{P}_n|\psi\rangle=tr\left(|\psi\rangle\langle\psi|\hat{P}_n\right), \tag{3.15}$$

у којем се чисто стање $|\psi\rangle$ појављује у облику пројектора, $|\psi\rangle\langle\psi|$, као специјалан случај оператора $\hat{\rho}$: ако је статистичка тежина неког подансамбла једнака јединици (као у изразу (3.15)), тада су све остале статистичке тежине једнаке нули – што је по дефиницији чисто стање. Формално:

$$\hat{\rho}=\sum_i W_i|\psi_i\rangle\langle\psi_i|\xrightarrow{W_{i_0}=1}\hat{\rho}=1\cdot|\psi_{i_0}\rangle\langle\psi_{i_0}|\equiv|\psi_{i_0}\rangle\langle\psi_{i_0}|. \tag{3.16}$$

Дакле, израз (3.14) је формално *уопштење случаја чистог ансамбла*, те статистички оператор представља стање мешаног ансамбла.

Сада је лако доказати да се очекиване вредности неке опсервабле $\hat{B}$, на ансамблу у мешаном стању $\hat{\rho}$, израчунавају по изразу:

$$\langle\hat{B}\rangle_{\hat{\rho}}=tr\left(\hat{\rho}\hat{B}\right), \tag{3.17}$$

где индекс $\hat{\rho}$ наглашава да се ради о мешаном ансамблу.

Шредингерова једначина за мешана стања се назива Лиувиловом једначином, и њен облик је дат изразом:

---

[5] Што је увек случај у предиктивном мерењу.

[6] Који се понекад назива и „матрицом густине“ („*density matrix*“) – *Blum 1981*.

$$i\hbar \frac{d\hat{\rho}(t)}{dt} = \left[\hat{H}, \hat{\rho}\right]. \qquad (3.18)$$

ДОКАЗ: На основи Шредингерове једначине, израз (2.18), следи да се адјунговани вектор стања мења у времену у складу са:

$$-i\hbar \frac{d\langle\psi(t)|}{dt} = \langle\psi(t)|\hat{H}, \qquad (3.19)$$

што важи за свако стање у суми (3.14). Сменом израза (2.18) и (3.19) у израз (3.14), лако следи Лиувилова једначина, израз (3.18).

Решавањем једначине (3.18) добија се временска промена стања мешаног ансамбла, а отуда и могућност израчунавања вероватноћа мерења и средњих вредности опсервабли система у сваком тренутку времена.

3.7 Особине статистичког оператора

Уочимо следеће особине статистичког оператора:
(а) све његове својствене вредности су ненегативне[7]: $W_i \geq 0, \forall i$,
(б) $tr\hat{\rho} = 1$,
(в) $\hat{\rho}^2 = \hat{\rho} \Rightarrow \hat{\rho}$ је чисто стање.

□ ДОКАЗ: Став (а) следи по дефиницији – видети горње вероватноће W_i, и Зад. 3.6.
Став (б) следи на основи уочавања: $tr\hat{\rho} = tr\sum_i W_i |\psi_i\rangle\langle\psi_i| = \sum_i W_i tr|\psi_i\rangle\langle\psi_i| = \sum_i W_i = 1$.
Став (в) следи на основи уочавања да, с обзиром на дефиницију (3.14), $\hat{\rho}^2 = \sum_i W_i^2 |\psi_i\rangle\langle\psi_i|$, одакле $tr\hat{\rho}^2 = tr\hat{\rho} = 1$ може бити испуњено *акко* једна статистичка тежина, $W_{i_0} = 1$, баш као у изразу (3.16). ■

Сада се статистички оператор може користити као ***општи формализам за стања квантних ансамбала***, с обзиром да особине (а)-(в) важе и за чиста, и за мешана стања, тј., ансамбле; ове разликујемо помоћу критеријума тачке (в). Формулација квантне механике у терминима статистичког оператора је елегантна и заснива се на дефиниционим особинама, тачке (а)-(в), као и на изразима (3.14)-(3.19).

Разликовање чистих и мешаних ансамбала:
Поред формалног записа, тачке (в), разликовање чистих и мешаних *ансамбала* има и свој *оперативни*, физички вид. Размотримо као пример два стања,

$$|\psi\rangle = \sum_i C_i |i\rangle,$$

$$\hat{\rho} = \sum_i |C_i|^2 |i\rangle\langle i|.$$

[7] Што остаје на снази и када су смешана неортогонална стања. Доказ овога је предмет Задатка 3.6.

За ова стања се каже, када се међусобно упоређују, да представљају, редом, *кохерентну*, и *некохерентну мешавину* (чистих) стања $|i\rangle$ (отуда се чиста стања понекад називају и „кохерентним мешавинама“). Када су у питању опсервабле за које је базис $\{|i\rangle\}$ својствени базис, вероватноће мерења и средње вредности тих опсервабли су исте *за оба ансамбла*, $|\psi\rangle$ и $\hat{\rho}$. Међутим, ова два ансамбла се *могу разликовати* мерењем било које опсервабле, $\hat{B}$, за коју горњи базис није својствен, тј., за коју важи $\left[\hat{B},\hat{\rho}\right]\neq 0$. Доказ ове тврдње је предмет Задатка 3.7.

Скуп свих оператора који задовољавају особине (а) и (б) чини, математички, тзв., σ*-конвексну структуру*. Наиме, свака линеарна комбинација статистичких оператора, $\{\hat{\rho}_p\}$, који задовољавају тачке (а) и (б), и сама задовољава те услове:

$$\hat{\rho}=\sum_p \lambda_p\hat{\rho}_p \text{ , ако и само ако } \sum_p \lambda_p = 1, \tag{3.20}$$

што се лако може доказати. Дакле, скуп статистичких оператора који се линеарно мешају по пропису (3.20), представља *математички затворену структуру* са особинама (а)-(в). Ове особине су за квантну информатику од основног значаја.

3.8 Промена стања услед мерења

ТЕОРЕМ 3.2: *Селективно предиктивно* мерење неке опсервабле $\hat{A}$ на *чистом* ансамблу у стању $|\varphi\rangle$, ако је резултат мерења a_n, преводи почетни ансамбл у стање:

$$|\psi_n\rangle=\frac{\hat{P}_n|\varphi\rangle}{\langle\varphi|\hat{P}_n|\varphi\rangle^{1/2}}, \tag{3.21}$$

где је $\hat{P}_n$ својствени пројектор мерене опсервабле за својствену вредност a_n.

ТЕОРЕМ 3.3: *Селективно предиктивно* мерење неке опсервабле $\hat{A}$ на *мешаном* ансамблу у стању $\hat{\rho}$, ако је резултат мерења a_n, преводи ансамбл у стање:

$$\hat{\rho}'=\frac{1}{tr\left(\hat{\rho}\hat{P}_n\right)}\hat{P}_n\hat{\rho}\hat{P}_n. \tag{3.22}$$

ТЕОРЕМ 3.4: *Неселективно предиктивно мерење* неке опсервабле $\hat{A}$ на ансамблу[8] у стању $\hat{\rho}$ преводи почетни ансамбл у стање:

$$\hat{\rho}''=\sum_n \hat{P}_n\hat{\rho}\hat{P}_n\ . \tag{3.23}$$

[8] Сходно реченом у Одељку 3.7, ансамбл може бити и чист, иако се користимо статистичким оператором.

У историји квантне теорије мерења, изрази (3.21)-(3.23) су познати као „пројекциони постулат“ (*von Neumann 1955*). На основи ДЕФ. 3.1, пак, изрази (3.21)-(3.23) следе као последице. За доказе упућујемо на оригиналну литературу, *Herbut 1969, 1974*, видети и Хербут 1984.

Сада је јасна улога и важност предиктивних мерења: после мерења, систем (објект мерења) не само да преживљава (и то, приближно, сваки поједи-начни елемент ансамбла), већ је и једнозначно познато коначно стање ансамбла на којем је вршено мерење – што је од основног значаја у квантној информатици.

3.9 Ансамбалско разликовање квантних стања

Поред принципијелног, формалног разликовања чистих квантних стања помоћу појма ПСКО, поставља се питање оперативног *разликовања чистих* ансамбала, тј., стања. На овом месту се истиче још један аспект проблема појединачних система (појединачних елемената ансамбла).

Придруживање стања појединачном систему (Постулат о појединачном систему) на први поглед као да указује да је могуће утврдити у ком стању се налази дати појединачни систем, или да се утврди у ком од два (унапред задата) стања се појединачни систем налази. Ниједно није могуће, и то *у принципу*, учинити – видети, Одељке 6.2 и 6.3.

Са друге стране, пак, придруживање стања ансамблу омогућује, макар у принципу, да се мерењем подесне опсервабле на ансамблу могу разликовати два (унапред задата) стања. Логика доказа – видети задатак 3.14 – је следећа: једини подаци којима, у контексту ансамбала, у квантној механици оперативно баратамо су расподеле вероватноћа које следе мерењем на ансамблу. Иако дата расподела вероватноћа за дату опсервablу не може једнозначно одредити стање ансамбла, могуће је, мерењем погодне опсервабле, разликовати (унапред задата) стања, самом чињеницом што различита стања, по дефиницији, дају различите расподеле вероватноћа резултата мерења макар једне опсервабле система.

Праћењем исте логике лако се доказује и могућност *разликовања мешаних* стања ансамбла – Задатак 3.14.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- *Хербут 1984* (посебно за доказе израза за промену стања при мерењу, као и везу са пројекционим постулатом)
- *d'Espagnat 1971*
- *Дугић 2004* (посебно за основе теорије мерења и формализам статистичког оператора)
- *Kraus 1983* (исцрпни формализам статистичког оператора)

ЗАДАЦИ:

3.1 Како се може показати да релације неодређености не важе за ретроспективна мерења? Дати пример.
Упутство: утврдити да висока тачност одређивања положаја детектоване честице, нпр., на целулоидној траци, не искључује високу тачност одређивања импулса те честице.

3.2. Доказати једнозначност придруживања $e_n \leftrightarrow \{a_i, b_j, c_k, ...\}$, у ознакама Од. 3.5.

3.3. Доказати важење израза (3.13).

3.4. Доказати израз (3.17).

3.5. Полазећи од израза (3.19) доказати важење Лиувилове једначине, израз (3.18).

3.6. Задат је мешани ансамбл: смешана су стања $|+\rangle_z$ са вероватноћом 5/6, $|+\rangle_x$ са вероватноћом (статистичком тежином) 1/12, и стање $|-\rangle_y$, са вероватноћом 1/12. Наћи спектралну форму оператора стања овог ансамбла, посебно ненегативност својствених вредности статистичког оператора. Израчунати фон Најманову ентропију тог стања. (Видети и напомену у оквиру у Одељку 5.1)

3.7. За стања $|\psi\rangle = \sum_i C_i |i\rangle$ и $\hat{\rho} = \sum_i \| C_i \|^2 |i\rangle\langle i|$ доказати да су очекиване вредности опсервабле $\hat{B}$ у овим стањима једнаке *акко* важи $\left[\hat{\rho}, \hat{B}\right] = 0$.

Решење: Очекивана вредност опсервабле $\hat{B}$ у чистом стању има облик $\sum_{i.j} C_i C_j * \langle i|\hat{B}|j\rangle$, док за мешано стање се добија $\sum_i |C_i|^2 \langle i|\hat{B}|i\rangle$. Двострука сума у првом изразу постаје једнострука (као у другом), *акко* су смешана стања (стања $|i\rangle$) својствена стања опсервабле $\hat{B}$ - што је остављено читаоцу на проверу.

3.8. Доказати да услов (3.20) задовољава услов за σ *-конвексну структуру*.

3.9. Израчунати стандардно одступање опсервабле $\hat{S}_x$ у мешаном стању задатом у задатку 3.6.

3.10. У тродимензионалном Хилбертовом простору задато је стање матрицом колоном: $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix}$, а једна опсервабла, у истој репрезентацији, матрицом $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Наћи очекивану вредност ове опсервабле у задатом стању.
Решење: Очекивана вредност је у матричном запису дата матричним производом:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & -i\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ i\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & -i\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ -i\end{pmatrix}=0. \qquad (3а)$$

3.11. У четвородимензионалном Хилбертовом простору задат је статистички оператор матрицом $\frac{1}{8}\begin{pmatrix}0 & 1 & i & -2i\\ 1 & 1 & 0 & 3\\ -i & 0 & 5 & -1\\ 2i & 3 & -1 & 2\end{pmatrix}$. У истој репрезентацији задат је неки оператор матрицом $\begin{pmatrix}1 & -1 & 2 & i\\ -1 & 0 & 0 & 3\\ 2 & 0 & 0 & 1/2\\ -i & 3 & 1/2 & 0\end{pmatrix}$. Наћи стандардно одступање за ову опсерваблу у задатом мешаном стању.

Решење: Стандардно одступање опсервабле дато је општим изразом (2.8). Према општим изразима Одељака 3.6 и 3.7, за мешано стање $\hat{\rho}$ важе следеће дефиниције: $\langle \hat{A}^2\rangle = tr\hat{\rho}\hat{A}^2$, $\left(\langle \hat{A}\rangle\right)^2 = \left(tr\hat{\rho}\hat{A}\right)^2$. Смењујући ове изразе у (2.8), па онда и задате матричне репрезентације, добија се за квадрат стандардног одступања задате опсервабле:

$$\frac{1}{8}tr\left(\begin{pmatrix}0 & 1 & i & -2i\\ 1 & 1 & 0 & 3\\ -i & 0 & 5 & -1\\ 2i & 3 & -1 & 2\end{pmatrix}\begin{pmatrix}7 & -1+3i & 2+i/2 & -2+i\\ -1-3i & 10 & -1/2 & -i\\ 2-i/2 & -1/2 & 17/4 & 2i\\ -2-i & i & -2i & 41/4\end{pmatrix}\right)-$$
$$\left(\frac{1}{8}tr\left(\begin{pmatrix}0 & 1 & i & -2i\\ 1 & 1 & 0 & 3\\ -i & 0 & 5 & -1\\ 2i & 3 & -1 & 2\end{pmatrix}\begin{pmatrix}1 & -1 & 2 & i\\ -1 & 0 & 0 & 3\\ 2 & 0 & 0 & 1/2\\ -i & 3 & 1/2 & 0\end{pmatrix}\right)\right)^2. \qquad (3б)$$

Даљи прорачун је могуће олакшати прорачуном *само дијагоналних елемената* матрица чији се траг тражи, јер „tr “ представља збир дијагоналних елемената у датој репрезентацији. Тај збир, како стоји у Задатку (2.5), не зависи од репрезентације. По правилима матричног множења, дијагонални елементи следе као производи колона и врста истог реда. Тако, за први члан у горњем изразу, дијагонални чланови су, редом: $-5/2+3i$, $9+6i$, $85/4$, $37/4-9i$. Њихов збир, подељен са 8, даје први члан у горњем изразу: 37/8. За други члан се добија 121/64. Отуда следи да је тражено стандардно одступање: $\sqrt{37/4-121/64}\approx 4.42$.

3.12. Упадни сноп атома у Штерн-Герлаховом експерименту је припремљен у стање $|+\rangle_y$. Магнет је постављен дуж x-осе. Наћи коначно стање, као и вероватноћу добијања резултата $\hbar/2$ мерења пројекције спина.

Решење: Мерена опсервабла је $\hat{S}_x$. Почетно стање се може развити по базису мерене опсервабле као: $|+\rangle_y = \frac{1+i}{2}|+\rangle_x + \frac{1-i}{2}|-\rangle_x$. Сада, израз (2.21), тј. (3.21) непосредно дају, за дати резултат (селективно мерење) коначно стање $|+\rangle_x$, као и вероватноћу ${}_x\langle +|+\rangle_y = \left|\frac{1+i}{2}\right|^2 = \frac{1}{2}$.

3.13. Израчунати матрицу која представља коначно стање ансамбла у неселективној варијанти мерења разматраном у задатку 3.12. За то стање израчунати статистичко одступање опсервабле $\hat{S}_y$. (Уочити губљење почетне оштре вредности за $\hat{S}_y$, услед мерења $\hat{S}_x$ - што је последица некомпатибилности, $\left[\hat{S}_x, \hat{S}_y\right] \neq 0$ - видети Одељак 4.4.)

Решење: Према изразу (3.23), коначно, мешано стање (за неселективно мерење) је облика:

$$\hat{\rho} = \hat{P}_{+x}\hat{\rho}'\hat{P}_{+x} + \hat{P}_{-x}\hat{\rho}'\hat{P}_{-x}, \qquad (3в)$$

где се појављују пројектори који одговарају двама могућим резултатима мерења, $\pm\hbar/2$. Како су обе својствене вредности недегенерисане, оба пројектора су дијаде, тј. $\hat{P}_{\pm x} = |\pm\rangle_x\langle\pm|$. Како је почетно стање, $\hat{\rho}' = |+\rangle_y\langle+|$, то резултат претходног задатка лако даје коначно стање:

$$\hat{\rho} = \frac{1}{2}|+\rangle_x\langle+| + \frac{1}{2}|-\rangle_x\langle-|. \qquad (3г)$$

3.14. Доказати постојање опсервабле за коју ће два, по претпоставци различита, квантна стања $|\psi\rangle$ и $|\varphi\rangle$ дати различите расподеле вероватноћа дискретних вредности те опсервабле. Уопштити на (ансамбалску) различивост мешаних стања.

Решење: Одаберимо неку опсерваблу $\hat{A}$ чије је једно својствено стање за неку недегенерисану вредност a баш стање $|\psi\rangle : \hat{A}|\psi\rangle = a|\psi\rangle$; тада $W(\hat{A}, |\psi\rangle, a) = 1$. Ако су стања различита, важи $|\langle\psi|\varphi\rangle| < 1$. Отуд следи $W(\hat{A}, |\varphi\rangle, a) = |\langle\psi|\varphi\rangle|^2 < 1$. Неједнакост вероватноћа, $W(\hat{A}, |\psi\rangle, a) \neq W(\hat{A}, |\varphi\rangle, a)$, успоставља оперативну различивост чистих стања на ансамблу. Читаоцу остављамо уопштење овог доказа на ансамбалско разликовање мешаних стања.

3.15. Један фотон пада на полупропусно огледало масе M. Користећи законе одржања импулса и енергије за двочестични систем „фотон + огледало“, записати стање овог система. Посебно размотрити случај $M \to \infty$.

Решење: У двочестичном систему закон одржања импулса успоставља следећи пропис: ако је фотон прошао кроз огледало, његов импулс се није променио, као ни огледала, а ако се фотон одбио, онда и огледало трпи узмак, тако да је укупни импулс сачуван. Запишимо ово у терминима стања двочестичног система: $|\vec{p}\rangle_{foton}|0\rangle_{ogledalo}$, и $|\vec{p}'\rangle_{foton}|\vec{p}''\rangle_{ogledalo}$, редом, тако да $\vec{p}' + \vec{p}'' = \vec{p}$. Како је огледало полупропустљиво, укупно стање овог система је сплетено:

$$\frac{1}{\sqrt{2}}\left(|\vec{p}\rangle_{foton}|0\rangle_{ogledalo} + |\vec{p}'\rangle_{foton}|\vec{p}''\rangle_{ogledalo}\right). \qquad (3д)$$

Закон одржања (кинетичке) енергије гласи: $\frac{1}{2m}p'^2 + \frac{1}{2M}p''^2 = \frac{1}{2m}p^2$. У *лимесу* $M \to \infty$, други члан са л.с. тежи нули, одакле следи $p' \to p$. Сменом овог у л.с. закона одржања импулса се добија $|\vec{p}' + \vec{p}''| \leq p' + p'' \approx p + p''$, што, с обзиром на д.с. закона одржања, следи да импулс огледала тежи нули, $p'' \to 0$ – огледало не трпи узмак, тј., *његово стање се не мења*. У овом лимесу, дакле, стање (3д) добија облик:

$$\frac{1}{\sqrt{2}}\left(\left|\vec{p}\right\rangle_{foton}+\left|\vec{p}'\right\rangle_{foton}\right)\left|0\right\rangle_{ogledalo}, \qquad (3\hbar)$$

што физички одговара ситуацији у којој *огледало* представља *спољашње поље* за фотон – баш како је то случај у интерференционим експериментима у оптици. Фотон сада представља изоловани систем за којег огледало представља спољашње поље у смислу прописа за интерференцију путања фотона (упоредити са ***Додатком 10.2***). Тј., у овом лимесу, *двочестични* систем постаје *једночестични*.

IV ПРЕПАРАЦИЈА СТАЊА И КЛАСИЧНА ИНФОРМАЦИЈА. ПРОБЛЕМ МЕРЕЊА

Мерење опсервабле $\hat{A}$ на појединачном систему у стању $|\Psi\rangle$ има као резултат неку вредност a_n из скупа могућих вредности. Познавање те вредности је ***класична информација*** о мереној опсервабли.

Резултат појединачног мерења је врста информације која се понекад назива актуелном. Скуп таквих мерења на ансамблу остварује један класични извор информација у смислу Одељка 1.1; овде[1] је Шенонова ентропија одређена расподелом вероватноћа мерења, $p_i = W(\hat{A}, |\psi\rangle, a_i)$.

4.1 Квантна стања:класични информатички аспект

Свако *чисто стање* одговара неком (фиксираном) скупу вредности опсервабли из неког (не нужно једнозначног) ПСКО (в. Одељак 3.3). Означимо стање својствено за $\hat{A}$ (за вредност a_n) са $|\varphi_n\rangle$, а неки одговарајући ПСКО са $\{\hat{A}, \hat{B}, \hat{C}, ...\}$. Тада, *информатички*:

$$|\varphi_n\rangle \Leftrightarrow \{a_n, b^{(n)}{}_p, c^{(n)}{}_q, ...\} \tag{4.1}$$

где се појављују вредности опсервабли из тог ПСКО.

Мешано стање носи ***класичну неодређеност*** – ***недовољно познавање*** вредности опсервабли из неког ПСКО. На пример, нека су смешана стања из скупа $\{|\varphi_n\rangle\}$, са вероватноћама p_n. Тада се ансамбл налази у стању $\hat{\rho} = \sum_n p_n |\varphi_n\rangle\langle\varphi_n|$. Физички, то значи да *сваки елемент* ансамбла ***има одређено стање***, неко из скупа могућих, али да нама није познато у ком стању се *који елемент* налази. Сходно (4.1), *информатички*, мешано стање се може представити:

$$\hat{\rho} = \sum_n p_n |\varphi_n\rangle\langle\varphi_n| \Leftrightarrow \{(a_n, b^{(n)}{}_p, c^{(n)}{}_q, ...; p_n) \Leftrightarrow (|\varphi_n\rangle; p_n)\}. \tag{4.2}$$

То јест, сваком елементу ансамбла се може придружити један скуп вредности опсервабли из неког ПСКО, али то придруживање није унапред задато, тј., не знамо који скуп вредности треба придружити којем елементу ансамбла, те се придруживање одређује вероватноћама.

[1] Што не мора бити дискретна вредност, већ и неки интервал вредности.

4.2 Препарација стања. Квантни информатички лимит

Предиктивним селективним мерењем опсервабле $\hat{A}$ *једнозначно је познат* ***и*** *резултат мерења (нпр., оштра вредност опсервабле),* ***и*** *коначно стање ансамбла*. Сходно (3.21), за неко *чисто почетно* стање, предиктивно селективно мерење води такође чистом коначном стању – што представља поступак ***препарације стања***, тј., ансамбла. За различита *почетна чиста* стања, $|\psi\rangle$ и $|\chi\rangle$, и коначни ансамбли су различити, $\hat{P}|\psi\rangle \neq \hat{P}|\chi\rangle$, за дегенерисану (измерену) вредност a_n. За недегенерисано (измерено) a_n, како је лако показати на основи (3.21), у општем случају важи $\hat{P}|\psi\rangle = \exp(i\alpha)\hat{P}|\chi\rangle$. Тако да коначно стање ансамбла (стање у које желимо да препарирамо ансамбл) *не би зависило од почетног*, потребно је обавити симултано селективно предиктивно мерење опсервабли из одређеног ПСКО (или, еквивалентно, мерење комплетне опсервабле). Имајући ово у виду, сада се непосредно дефинише и препарација (чистог) ансамбла на *почетном мешаном* ансамблу (видети Задатак 4.2). Укупно: да *коначно чисто стање* не би зависило од почетног (чистог или мешаног стања), довољно је обавити селективно предиктивно мерење недегенерисане вредности (или, еквивалентно, симултано предиктивно селективно мерење опсервабли из неког ПСКО).

Алтернативни поступак за препарацију ансамбла је, тзв., *филтрирање* ансамбла. Наиме, помоћу „филтера“ се из почетног ансамбла издвајају само они елементи који задовољавају одређени критеријум. Овај поступак није једнак процесу мерења, а често се користи у пракси – нпр., анализатор поларизације фотона издваја фотоне само одређене поларизације. Наравно, у таквом случају, један део почетног ансамбла је „уништен“ (неки фотони су апсорбовани од стране анализатора), тј., „нестао“ је баш као у квантним мерењима друге врсте (непоновљивим мерењима, Одељак 3.1).

Израз (4.1) носи ***класичну информацију*** о вредностима опсервабли из неког ПСКО, као и о (коначном) стању система о којем је реч. Ту нема неодређености, тј., мањка информација: и a_n, и $|\varphi_n\rangle$ су ***једнозначно*** (са вероватноћом 1) познати. Истовремено, и вредности свих опсервабли које су (аналитичке) функције опсервабли из ПСКО су једнозначно познате.

Управо речено је добро познато у класичној физици: једнозначне вредности варијабли положаја и импулса (тј., стање система) једнозначно одређују вредности *свих* варијабли система – које су аналитичке функције основних, канонски конјугованих варијабли. Недовољно познавање вредности положаја и импулса може да повлачи и недовољно познавање свих других варијабли. Дакле, нема суштинске разлике између информација о вредностима класичних варијабли и горе-анализованих информација представљених изразима (4.1) и (4.2). Отуда се ове информације називају класичним. А за дубљу анализу видети Поглавље V.

Међутим, у квантној механици постоје опсервабле које *не комутирају* са макар неком опсерваблом из ПСКО. Тада, нужно, постоји опсервабла система за коју неко стање $|\varphi_n\rangle$ није својствено. Као што знамо (видети израз (2.8)), таквој опсервабли се не може придружити једнозначна („оштра“) вредност на ансамблу у стању $|\varphi_n\rangle$. *Међутим, ова врста неодређености није «класична»*, и детаљно ће бити обрађена у Одељку 5.2.

Оно што овде желимо истаћи је следећа чињеница: ***чиста стања су носиоци максималне класичне информације о систему***.

Наиме, за свако чисто стање важи: све што се о систему (у том стању) може знати – а то су једнозначне, оштре (са вероватноћом 1) вредности опсервабли из неког ПСКО, израз (4.1) – је познато; имамо све могуће класичне информације о систему у том стању[2]. При томе, опсервабле које не комутирају са макар по једном опсерваблом из датог ПСКО се карактеришу неодређеношћу (ненултим стандардним одступањем). Отуда квантну механику карактерише постојање границе у могућностима информатичког описа система – иако знамо све што се може знати о систему, ипак постоје неодређености (недостатак информација) које се не могу заобићи, а квантитативно се испољавају кроз релације неодређености, израз (2.9). Дакле, ове принципијелне неодређености стављају границу на могућност поседовања/добијања класичних информација о квантном систему, што се назива *квантним информатичким лимитом*.

4.3 Проблем мерења

Квантна механика барата ***двема врстама промене стања у времену***.

Прва врста промене стања је каузална (унитарна, реверзибилна) и описана је Шредингеровом једначином:

$$|\Psi(t)\rangle = \hat{U}(t,t_0)|\Psi(t_0)\rangle, \hat{U}^+ = \hat{U}^{-1}. \tag{4.3}$$

Међутим, *квантно мерење* је **a priori *стохастично***, тј., води промени стања која се у неселективној варијанти може описати као:

$$|\Psi\rangle \to \{(a_i, p_i) \Leftrightarrow (|\varphi_i\rangle, p_i)\}\ , \tag{4.4}$$

тј., општије, изразима (3.21)-(3.23). Памтећи (3.23), израз (4.4) гласи:

$$|\Psi\rangle = \sum_i c_i|\phi_i\rangle \to \hat{\rho} = \sum_i |c_i|^2 |\phi_i\rangle\langle\phi_i|. \tag{4.5а}$$

Наравно, селективна варијанта одговара промени стања објекта мерења која одговара резултату мерења a_n :

$$|\Psi\rangle = \sum_i c_i|\phi_i\rangle \to |\phi_n\rangle. \tag{4.5б}$$

[2] Различита (чиста) стања одређују различите ПСКО-ове.

ПРОБЛЕМ МЕРЕЊА:
Промена стања (еволуција у времену) (4.4), тј. (4.5а,б), ***није у складу са Шредингеровом једначином. Који је онда закон кретања за квантно мерење?***
Овај проблем је још увек отворен.

Интуитивна парадоксалност процеса мерења у селективној варијанти огледа се у следећем уочавању (Задаци 3.16 и 3.17): мерење опсервабле на стању које није њено својствено стање обезбеђује класичну информацију о вредности те опсервабле и *успоставља класичну реалност* те, мерењем-добијене, вредности (a_n), али, у општем случају, на уштрб класичне информације, тј., класичне реалности вредности (b) неке опсервабле ($\hat{B}$) из ПСКО који одређује почетно стање ($|\psi\rangle$: $\hat{B}|\psi\rangle = b|\psi\rangle$). Другим речима, квантно мерење „ствара“ класичну реалност (кроз добијање класичне информације) измерене вредности (нпр., a_n) мерене опсервабле, истовремено „уништавајући“ класичну реалност (класичну информацију) вредности (нпр., b) неких опсервабли које не комутирају са мереном опсерваблом ($\left[\hat{A}, \hat{B}\right] \neq 0$).

4.4 Различивост квантних стања

Квантно мерење успоставља класичну информацију о вредности мерене опсервабле, као и о коначном стању ансамбла. При томе се подразумева ***различивост резултата мерења***: када мерни инструмент покаже вредност a_n , у идеалном случају (без метролошке грешке мерења), то није ни једна друга вредност опсервабле. Другим речима: мерни инструмент („апарат“) не брка вредности – разликује их. Отуда се и за информације везане за вредности мерене опсервабле каже да су различиве. Ово има и свој формални вид. Нека су, по дефиницији, две вредности опсервабле $\hat{A}$, a_n и a_m , међусобно различиве. Тада се њихова ***различивост формално дефинише*** условом ортогоналности одговарајућих својствених стања (или, еквивалентно, пројектора), $|\varphi_n\rangle, |\varphi_m\rangle$ (или $\hat{P}_n, \hat{P}_m$):

$$\begin{aligned} &\langle \varphi_n | \varphi_m \rangle = 0, n \neq m \\ &\hat{P}_n \hat{P}_m = 0, n \neq m \end{aligned} \qquad (4.6)$$

Особина различивости стања и разликовање вредности варијабли се подразумева у класичној физици. Али у квантној механици израз (4.6) има посебну важност и непосредно физичко значење: мерењем опсервабле $\hat{A}$ на ансамблу у стању $|\varphi_n\rangle$ које је својствено за $\hat{A}$, резултат мерења је a_n , и то у идеалном случају (занемарујемо метролошку грешку) са вероватноћом 1. Другим речима: стање $|\varphi_n\rangle$ не може дати вредност a_m , $\forall m \neq n$. И то је пуно ***оперативно значење појма различивости*** вредности опсервабли (тј., стања) у квантној

механици. Истовремено, то је и *носилац различивости (класичних) информација о квантном систему* – о вредностима опсервабли (тј., стањима), добијених мерењем. А значај ове напомене постаће јаснији у Поглављу VI.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- У вези са проблемом мерења консултовати *Дугић 2004, Хербут 1984, Wheeler and Zurek 1983.*
- Интернет претраге започети фразом "*quantum measurement*".

ЗАДАЦИ

4.1 Анализирати произвољну препарацију ансамбла који је у једном од почетних чистих стања, $|\psi\rangle$, или $|\chi\rangle$.

Решење: Израз (3.21) за недегенерисану вредност a_n (тада је пројектор $\hat{P}_n = |\varphi_n\rangle\langle\varphi_n|$) даје:

$$\frac{1}{\langle\psi|\hat{P}_n|\psi\rangle^{1/2}}\hat{P}_n|\psi\rangle = \frac{\langle\varphi_n|\psi\rangle}{|\langle\varphi_n|\psi\rangle|^2}|\varphi_n\rangle = \exp(i\delta)|\varphi_n\rangle,$$

и аналогно за стање $|\chi\rangle$. Дакле, коначна стања се разликују само по „фази. За дегенерисану вредност ова једнакост, у општем случају, више не важи:

$\hat{P}_n|\psi\rangle = \sum_i \langle\varphi_i^{(n)}|\psi\rangle|\varphi_i^{(n)}\rangle \neq \sum_i \langle\varphi_i^{(n)}|\chi\rangle|\varphi_i^{(n)}\rangle = \hat{P}_n|\chi\rangle$, где $\hat{P}_n = \sum_{i=1}^{g_n}|\varphi_i^{(n)}\rangle\langle\varphi_i^{(n)}|$.

4.2 Показати да израз (3.22) даје *препарацију чистог* ансамбла за *почетни мешани* ансамбл под условом да је измерена недегенерисана вредност a_n неке опсервабле $\hat{A}$.

Решење: Израз (3.22) представља мешано стање, означимо га са $\hat{\rho}'$. Ако је измерена недегенерисана вредност, тада је пројектор $\hat{P}_n$ који се појављује у (3.22) заправо дијада, $\hat{P}_n = |\varphi_n\rangle\langle\varphi_n|$. Сменом овог у (3.22) следи за коначно стање, после предиктивног селективног мерења (добијени резултат је a_n):

$$\left(tr\hat{\rho}\hat{P}_n\right)^{-1}\sum_k w_k\langle\varphi_n|\chi_k\rangle\langle\chi_k|\varphi_n\rangle|\varphi_n\rangle\langle\varphi_n| = |\varphi_n\rangle\langle\varphi_n|,$$

где последња једнакост следи на основи једнакости: $\left(tr\hat{\rho}\hat{P}_n\right)^{-1}\sum_k w_k\langle\varphi_n|\chi_k\rangle\langle\chi_k|\varphi_n\rangle = 1$.

4.3 Доказати да (4.4) није у складу са Шредеингеровом једначином.

Решење: Унитарна еволуција стања (Шредингерова једначина) сачувава „чистоћу" стања. То јест, ако је почетно стање чисто, унитарна еволуција води такође чистом стању – у очигледној противуречности са процесом мерења, израз (4.4), тј., (4.5а). Доказ сачувања „чистоће стања": $\hat{\rho}(t) = |\psi(t)\rangle\langle\psi(t)| = \hat{U}|\psi(t_0)\rangle\langle\psi(t_0)|\hat{U}^+ = \hat{U}\hat{\rho}(t_0)\hat{U}^+$. Сада,

$\hat{\rho}^2(t) = \hat{U}\hat{\rho}(t_0)\hat{U}^+\hat{U}\hat{\rho}(t_0)\hat{U}^+ = \hat{U}\hat{\rho}^2(t_0)\hat{U}^+ = \hat{\rho}(t)$, јер $|\psi(t_0)\rangle\langle\psi(t_0)| = \hat{\rho}(t_0) = \hat{\rho}^2(t_0)$. За селективно мерење, израз (4.5б) очигледно нарушава Шредингерову једначину, која је каузална (коначно стање је јединствено).

4.4 Полазећи од дефиниције (4.6), *дефинисати* неразличивост квантних стања. Упоредити са тачком (в) Одељка 6.1 и Одељка 6.3.

V КВАНТНА НЕОДРЕЂЕНОСТ. КВАНТНА НЕСЕПАРАБИЛНОСТ. КВАНТНА НЕЛОКАЛНОСТ

5.1 Класична неодређеност

Већ је више пута истакнуто: недовољно познавање вредности опсервабли (или стања система), то јест ***недостатак класичних информација о њима***, се назива ***класична неодређеност*** вредности опсервабли (тј., стања).

На пример, у неселективном мерењу опсервабле $\hat{A}$ чија су својствена стања $|\varphi_n\rangle$ и својствене вредности a_n, у мешаном ансамблу после мерења се налазе елементи (појединачни системи на којима је извршено мерење) којима се могу придружити различите вредности опсервабле (па отуда и различита коначна стања), што се формално представља (еквивалентно (4.2)):

$$\{a_n, p_n\},\ \sum_n p_n = 1. \tag{5.1}$$

При томе се подразумева:

(а) вредности опсервабле $\hat{A}$ су ***међусобно различиве***, $a_n \neq a_m \Rightarrow n \neq m$

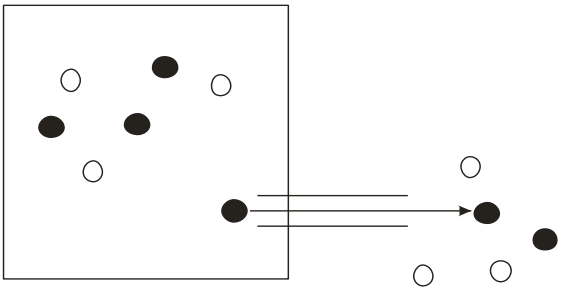
(б) $p_n \neq 1, \forall n$.

Тако се ***класична неодређеност***, која се тиче ансамбла описаног изразом (5.1), у формализму представља мешаним стањем:

$$\hat{\rho} = \sum_n p_n |\varphi_n\rangle\langle\varphi_n|, \tag{5.2}$$

које одсликава ***недостатак (класичне) информације о вредности мерене опсервабле (тј. стања система) у ансамблу након мерења.***

Појмовно, садржај класичне неодређености, изрази (5.1), тј., (5.2), је ***исти као и у класичној ситуацији представљеној на Сл. 5.1***.



Сл. 5.1 У непрозирној кутији су беле и црне куглице. Те куглице могу да изађу из кутије и задатак је одредити вероватноћу појављивања белих/црних куглица (појављивање је заправо *чин мерења* – мерења боје куглица). При томе, и ***то је кључно***, у класичној физици је ***увек случај***: ***и*** у кутији, ***и*** ван ње, свака појединачна

куглица ***има*** (***класично реално***) боју - та боја је ***или*** бела, ***или*** црна, и ***није условљена (не мења се) мерењем***.

Боја куглица у кутији на Сл. 5.1 је *класично-реално одређена* (Деф. 2.1) – она постоји независно од било чега другог, и пре, и после мерења, и није условљена поступком (или исходом) мерења. Ово је тривијалан исказ у класичној физици и тиче се стања (5.2). Наиме, као и у кутији, сваки елемент мешаног ансамбла има *класично-реално одређено стање* ($|\varphi_n\rangle$ са вероватноћом p_n), што је имплицитно у изразу (5.1). То је, појмовно, *и садржај израза* (5.2).

Зато се каже да је класична неодређеност – тј., недостатак информације (о стањима, вредностима величина) – ***субјективног, информатичког карактера*** и не тиче се неких *a priornih* особина система, већ само недовољног познавања стања система и вредности његових варијабли/опсервабли. Отуда је класична неодређеност ***практичне природе***, а не принципијелна граница у могућности стицања информација путем мерења[1].

Класична неодређеност се мери (Болцман-Гибс-Шеноновом) ***ентропијом***:

$$H = -\sum_n p_n \log p_n \,,\ \sum_n p_n = 1 . \tag{5.3}$$

За квантни систем у стању (5.2) уводи се ***фон Најманова ентропија***:

$$S = -tr\left(\hat{\rho}\log\hat{\rho}\right), \tag{5.4}$$

која се после прорачуна трага своди на израз (5.3), при чему сада горње вероватноће p_n постају својствене вредности оператора стања $\hat{\rho}$:

$$\hat{\rho} = \sum_n p_n |\varphi_n\rangle\langle\varphi_n|, \langle\varphi_m|\varphi_n\rangle = \delta_{mn} . \tag{5.5}$$

Очигледно важи: ако $p_n \neq 1, \forall n$ (што важи за сва мешана стања), да тада

$$S > 0 . \tag{5.6}$$

По дефиницији (Одељак 1.1), *што је већа ентропија, мање је познавање стања (вредности варијабли којима та стања одговарају) система*. Отуда и два екстрема:

- Минимум ентропије $S = 0$, одговара чистом квантном стању.
- Максимум ентропије одговара случају мешаног стања: $p_n = const, \forall n$.

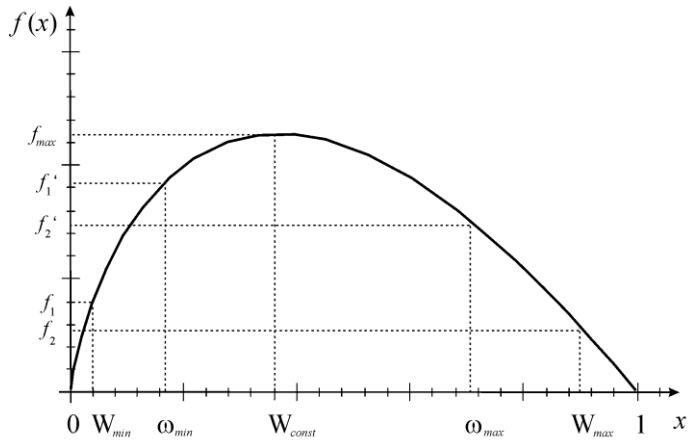
□ ДОКАЗ: Прво за чисто стање. Наравно, чисто стање је специјалан случај мешаног, када је једна вероватноћа једнака 1, а све остале једнаке нули:

$$\hat{\rho}_{чисто} = 1\cdot|\Psi\rangle\langle\Psi| + 0\cdot\sum_{i\neq\Psi}|i\rangle\langle i| . \tag{5.7}$$

[1] За разлику од информатичког лимита квантне механике, Одељак 4.2, који је *ствар принципа*.

Сменом вероватноћа из (5.7) у (5.3) непосредно следи $S = 0$ (уз конвенцију $0 \cdot \log 0 = 0$).

Друго, за мешана стања користићемо график Сл. 5.2.



Сл. 5.2. График функције $-x \ln x$ на интервалу $[0,1]$.

Уочити да су вертикале заправо вредности $-p_n \log p_n$ које се сабирају у изразу (5.3). А збир расте са приближавањем вертикала средини, што одговара случају $p_n = \frac{1}{N}$, при чему важи услов $\sum_{n=1}^{N} p_n = 1$. Овде на слици $N = 2$. ■

Друга мера класичне неодређености је *стандардно одступање*. Ова величина за опсерваблу $\hat{A}$ у ансамблу у стању $\hat{\rho}$ дата је изразом (упоредити са изразом (2.8)):

$$(\Delta_\rho \hat{A})^2 = \left\langle \hat{A}^2 \right\rangle_\rho - \left\langle \hat{A} \right\rangle_\rho^2 = tr\left(\hat{\rho}\hat{A}^2\right) - \left(tr\left(\hat{\rho}\hat{A}\right)\right)^2.$$

Подсетимо се (Одељак 3.6): мешано стање (ансамбл) се не мора тицати само ортогоналних стања. Један ансамбл могу чинити и *неортогонална стања* (што су својствена стања некомутирајућих опсервабли)[2]. Означимо та стања са $|\chi_i\rangle$, а њихове „статистичке тежине“ са p_i. Тада се том ансамблу, по дефиницији (Одељак 3.6), придружује стање $\hat{\rho} = \sum_i p_i |\chi_i\rangle\langle\chi_i|$, уз памћење да $\langle\chi_i|\chi_j\rangle \neq \delta_{ij}$. Сада, решавањем својствене једначине за овако дефинисано $\hat{\rho}$ се добија спектрални облик типа (5.5) ***за који***, сада, важи све горе речено – (5.3) и (5.4). Отуда дефиниција ансамбла (кроз задато мешање стања)

[2] Видети задатак 3.7 и један пример у Задатку 3.8.

једнозначно одређује стање мешаног ансамбла. Али обрнуто не стоји: (5.5) *се може тицати и мешавине неортогоналних стања*.

5.2 Квантна неодређеност

Нулта ентропија чистог квантног стања квантитативно потврђује напред изнет став (Одељак 4.2) да *чиста стања носе максимум класичних информација о систему* (кроз вредности опсервабли из неког ПСКО). Остаје питање како тумачити неодређеност неке опсервабле $\hat{\Lambda}$ за коју задато чисто стање није својствено.

Класично-информатички то изгледа парадоксално, јер ***имамо максимум информација о систему*** (ентропија стања $S = 0$), а опет ***постоји неодређеност***, мерена ненултим статистичким одступањем, $\Delta\hat{\Lambda}$, опсервабле $\hat{\Lambda}$ у датом ***чистом стању***.

Означимо чисто стање са $|\Psi\rangle$, а својствена стања опсервабле $\hat{\Lambda}$ са $|\chi_n\rangle$. Тада, наравно, може се писати:

$$|\Psi\rangle = \sum_n c_n|\chi_n\rangle. \tag{5.8}$$

Са друге стране, класична неодређеност вредности опсервабле $\hat{\Lambda}$ се описује мешаним стањем, нпр. :

$$\hat{\rho} = \sum_n |c_n|^2 |\chi_n\rangle\langle\chi_n|. \tag{5.9}$$

Сада, како се лако доказује (Одељак 3.7 и Задатак 3.7),

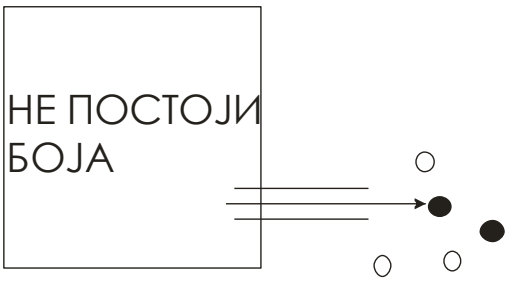
$$|\Psi\rangle\langle\Psi| \neq \hat{\rho}, \tag{5.10}$$

морамо закључити: неодређеност опсервабле $\hat{\Lambda}$ у чистом стању $|\Psi\rangle$ није класичне природе (која се описује мешаним стањем $\hat{\rho}$), већ је типична за квантну механику и отуда је „квантна неодређеност“. Другим речима, ***квантна неодређеност није субјективне (информатичке) природе***, тј., последица недостатка информације, већ ***услед принципијелног постојања границе*** у могућности познавања вредности опсервабли система – као последица некомпатибилности (изражено квантним информатичким лимитом, Одељак 4.2).

ЈЕДНА ПАРАЛЕЛА: У интерференционим експеримента у оптици се понекад спекулира о физичкој ситуацији у којој би свака замишљена честица светлости (фотон) имала одређену путању. Из ове претпоставке се лако изводи закључак да на заклону не би било интерференције. И обрнуто, када има интерференције, *нема смисла говорити о путањама замишљених фотона.* Тако се изводи закључак да у интерференционим експериментима *нема смисла* говорити о путањи фотона.

О квантној неодређености упутно је говорити као о ставу који успоставља да ***у стању*** $|\Psi\rangle$ ***нема смисла*** говорити о вредностима опсервабле $\hat{\Lambda}$. ***Информатички***: у стању $|\Psi\rangle$ ***не постоји*** *a priorna* ***класична информација о вредностима опсервабле*** $\hat{\Lambda}$. (Наравно, мерењем се добија та информација, али се ситуација (после мерења) обрће: вредности мерене опсервабле сада носе класичну информацију, док вредност опсервабле за коју је почетно стање, $|\Psi\rangle$, својствено, то више не важи – Одељак 4.3.)

Дакле, као контраст класичне неодређености, Сл. 5.1, квантна неодређеност се може представити као на Сл. 5.3.



Сл.5.3 Куглице у кутији (*пре мерења*) ***немају боју*** као физичку особину – ***квантна неодређеност боје***; тј., не постоји *a priorna* информација о боји куглице ***у кутији*** – стање куглица у кутији је неко чисто стање, $p_B^{1/2}|B\rangle + p_C^{1/2}|C\rangle$. ***Мерењем,*** пак (што је овде излазак и уочавање боје куглице), свака појединачна куглица ***добија боју*** (што је садржај класичне информације о боји). Изван кутије (*после мерења*) је мешани ансамбл (смешане, ***класично-реално постојеће боје***, које су међусобно ***различиве***) па је стање куглица ($|B\rangle, |C\rangle$ - бела, црна) изван кутије мешано, тј., постоји ***класична неодређеност*** боје куглица: $\hat{\rho} = p_B|B\rangle\langle B| + p_C|C\rangle\langle C|$ - баш као у изразу (4.5).

Сада се лако може доказати *важење квантне неодређености* и за *мешана стања* - али у односу на стања која су својствена за неку опсерваблу ($\hat{B}$) која не комутира са оператором стања ($\hat{\rho}$), $\left[\hat{\rho}, \hat{B}\right] \neq 0$ – Задатак 5.2.

ЈЕДНА ИЛУСТРАЦИЈА: Рећи „електрон[3] у водониковом атому ***има*** (класично реално) одређени положај са густином вероватноће $\rho(\vec{r})$“ ***имплицира класичну неодређеност положаја***:

$$\hat{\rho} = \int d^3\vec{r}\,\rho(\vec{r})|\vec{r}\rangle\langle\vec{r}|. \qquad (5.11a)$$

[3] Ово се тиче *ансамбла*. Када су у питању појединачни електрони, видети Одељак 5.4.

Међутим, из теорије водониковог атома ми *знамо* да су стања електрона у атому *чиста стања*, за која важи израз:

$$|\psi\rangle = \int d^3\vec{r}\psi(\vec{r})\,|\vec{r}\rangle, \qquad |\psi\rangle\langle\psi| \neq \hat{\rho}, \tag{5.11б}$$

те за положај електрона (у сваком атому) важи квантна неодређеност: ***електрон у атому нема положај*** (па отуда ни било какву путању), и то ***у принципу***[4]. Штавише, ***нема никаквог смисла*** говорити о „вредности“ положаја и/или импулса електрона у атому, баш као што у интерференцијама у оптици нема никаквог смисла говорити о путањи фотона (видети изнад).

5.3 Квантна несепарабилност (сплетеност – quantum entanglement)

Квантна неодређеност је универзална особина чистих квантних стања и опсервабли за које та стања нису својствена. За ***сложене*** квантне системе, поред ове, постоји још једна врста неодређености, названа ***квантна несепарабилност*** (или ***квантна сплетеност***[5] - “*entanglement*”).

Размотримо двочестични систем, 1+2. Његов простор стања је, по постулату о стањима сложеног система,

$$H = H_1 \otimes H_2, \tag{5.12}$$

а један ОНБ је $\left\{\left|\varphi_i\right\rangle_1 \otimes \left|\chi_j\right\rangle_2\right\}$, те се свако стање може записати као:

$$|\Psi\rangle_{12} = \sum_{i,j} c_{ij}|\phi_i\rangle_1 \otimes \left|\chi_j\right\rangle_2, \tag{5.13}$$

где се са д.с. (5.13) појављују елементи ОНБ-ова у H_1 и H_2, редом. Међутим, за свако стање сложеног система постоји и посебног-облика форма, успостављена следећим теоремом.

ТЕОРЕМ 5.1 (***Шмитова канонска форма***): За свако стање $\left|\Psi\right\rangle_{12}$ «двочестичног» система се може дефинисати «*редуковани статистички оператор*» првог система изразом $\hat{\rho}_1 = tr_2\left|\Psi\right\rangle_{12\ 12}\left\langle\Psi\right|$, где је «$tr_2$» операција узимања парцијалног[6] трага по неком базису простора стања 2. честице. Нека је (неједнозначна) спектрална форма $\hat{\rho}_1$:

$$\hat{\rho}_1 = \sum_k r_k \left|\varphi_k\right\rangle_{1\ 1}\left\langle\varphi_k\right|. \tag{5.14а}$$

Тада се може писати:

$$\left|\Psi\right\rangle_{12} = \sum_k r^{1/2}{}_k \left|\varphi_k\right\rangle_1 \otimes \left|\chi_k\right\rangle_2 \ , \tag{5.14б}$$

---

[4] Недавни експерименти са креирањем (семи)класичних путања електрона (*Maeda et al 2005*) у атому су својеврсна илустрација реченог: тек спољашњим утицајем се могу створити такве, „краткоживеће“ путање.

[5] Алтернативно: *у*плетеност.

[6] Видети ***Додатак 2.2***.

где су стања $\left|\chi_k\right\rangle_2$ својствена стања «редукованог статистичког оператора» другог система:

$$\hat{\rho}_2 = \sum_k r_k \left|\chi_k\right\rangle_{2\ 2}\left\langle\chi_k\right| \equiv tr_1 \left|\psi\right\rangle_{12\ 12}\left\langle\psi\right|. \qquad (5.14в)$$

Ако се сума у (5.14б) своди на само један члан, тада је стање сложеног система ***сепарабилно (некорелисано)***, неко $\left|\varphi_k\right\rangle_1 \left|\chi_k\right\rangle_2$, и у том стању, по дефиницији, ***сваки подсистем има одређено стање***, $\left|\varphi_k\right\rangle_1, \left|\chi_k\right\rangle_2$, редом.

Доказ теорема даћемо имплицитно – кроз коментаре, као и кроз *алгоритамски поступак за препис произвољног стања у ШКФ*; потпун доказ дат је, нпр., у *Хербут 1984.*

Истакнимо, прво, да оператори (5.14а,в) имају посебне одлике: изразима (5.14а,в) дате су њихове спектралне форме, те је $\{r_k\}$ заједнички скуп својствених вредности. Због (очигледне) једнозначне везе $\left|\varphi_k\right\rangle_1 \leftrightarrow \left|\chi_k\right\rangle_2$, дегенерације ових својствених вредности су идентичне за оба оператора.

За свако $\left|\Psi\right\rangle_{12}$ ***алгоритам преписа у ШКФ*** је следећи:

(а) Израчуна се $\hat{\rho}_1 = tr_2 \left|\Psi\right\rangle_{12\ 12}\left\langle\Psi\right|$; $tr_1\hat{\rho}_1 = tr_1 tr_2 \left|\Psi\right\rangle_{12\ 12}\left\langle\Psi\right| = tr_{12}\left|\Psi\right\rangle_{12\ 12}\left\langle\Psi\right| = 1$.

(б) Реши се својствена једначина за $\hat{\rho}_1$, одакле следе својствене вредности r_k и својствени подпростори. Узме се један својствени базис за $\hat{\rho}_1$, $\left\{\left|\varphi_k\right\rangle_1\right\}$.

(в) За свако (неједнозначно одабрано) стање $\left|\varphi_k\right\rangle_1$ једнозначно се дефинише (ненормирани) вектор $r_k^{1/2}\left|\chi_k\right\rangle_2$, тако да ${}_2\left\langle\chi_k\middle|\chi_{k'}\right\rangle_2 = \delta_{kk'}$. Дакле, добијен је један ОНБ за други подсистем, $\left\{\left|\chi_k\right\rangle_2\right\}$. Тиме су дефинисани сви елементи ШКФ датог стања. Стања $\left|\chi_k\right\rangle_2 \equiv {}_1\left\langle\varphi_k\middle|\Psi\right\rangle_{12}$, где се појављује *парцијални скаларни производ*[7] стања из H_1 и стања из укупног простора H.

НАПОМЕНА: Само ако је $\hat{\rho}_1$ (а тиме – в. горе – и $\hat{\rho}_2$) комплетна опсервабла, добијена ШКФ је једнозначна.

Вероватноће мерења и средње вредности опсервабли подсистема 1, тј., 2, се израчунавају по већ познатим изразима:

$$\left\langle\hat{A}_1\right\rangle = tr_1\left(\hat{A}_1\hat{\rho}_1\right) \qquad (5.15)$$

$$\left\langle\hat{B}_2\right\rangle = tr_2\left(\hat{B}_2\hat{\rho}_2\right). \qquad (5.16)$$

□ ДОКАЗ: Према 3. постулату квантне механике о вероватноћама, следи:

[7] Видети ***Додатак 2.2***.

$$\left\langle \hat{A}_1 \right\rangle = tr_{12}\left(\hat{A}_1 \otimes \hat{I}_2 \left| \Psi \right\rangle_{12\ 12} \left\langle \Psi \right| \right) = {}_{12}\left\langle \Psi \left| \hat{A}_1 \otimes \hat{I}_2 \right| \Psi \right\rangle_{12} =$$

$$\sum_{i,j} C_i^* C_j \, {}_1\left\langle i \left| \hat{A}_1 \right| j \right\rangle_{1\ 2} \left\langle i \left| j \right. \right\rangle_2 = \sum_i \left| C_i \right|^2 {}_1\left\langle i \left| \hat{A}_1 \right| i \right\rangle_1 = \quad ,$$

$$\sum_k {}_1\left\langle k \right| \left(\sum_i \left| C_i \right|^2 \left| i \right\rangle_{1\ 1} \left\langle i \right| \hat{A}_1 \right) \left| k \right\rangle_1 \equiv tr_1\left(\hat{A}_1 \hat{\rho}_1 \right)$$

где је $\hat{\rho}_1 = \sum_i \left| C_i \right|^2 \left| i \right\rangle_{1\ 1} \left\langle i \right|$, и све аналогно за опсервабле система 2. ■

Са становишта ***класичне информатике,*** ова ситуација је ***парадоксална***: укупни систем, 1+2, се налази у чистом стању, те је његова ентропија једанака нули:

$$S_{\left| \Psi \right\rangle_{12}} = 0, \tag{5.17}$$

док су ***ентропије стања подсистема ненулте***:

$$S_{\hat{\rho}_i} = \sum_n r_n \ln r_n \neq 0, i = 1,2. \tag{5.18}$$

То јест, *о укупном систему знамо највише што можемо* (памтећи постојање квантног информатичког лимита), док *о подсистемима*, који га сачињавају, *имамо мањак информација*!

Кључно уочавање је следеће: ***редуковани статистички оператори нису стања квантних подсистема***, већ само математичка погодност – као у изразима (5.15) и (5.16). Наиме, из исказа «стање првог подсистема је $\hat{\rho}_1$, а стање другог подсистема је $\hat{\rho}_2$» следи, по дефиницији[8], да је «стање укупног система $\hat{\rho}_1 \otimes \hat{\rho}_2$ ». Међутим, како важи (Задатак 5.3):

$$\left| \Psi \right\rangle_{12} \left\langle \Psi \right| \neq \hat{\rho}_1 \otimes \hat{\rho}_2 \tag{5.19}$$

то стоји горњи закључак. Отуда се редуковани статистички оператори називају и ***мешавинама друге врсте***[9], да би се разликовали од правих мешаних стања[10] (нпр., (5.5)) која су стања система и последица су (субјективног) недостатка информација.

Дакле, мешавине друге врсте нису последица (субјективног) недостатка информација. Због (5.19), ***нема смисла говорити о појму стања подсистема сложених квантних система*** – осим уколико је стање сложеног система типа д.с. израза (5.19). Информатички: у чистом сплетеном стању не постоји *a priorna* информација о стању подсистема, и то као ствар принципа, а не услед субјективног недостатка информација о стањима подсистема.

[8] Што је уопштење дефиниције из Одељка 2.9 и дефиниције у Одељку 2.10.
[9] Енгл.: *improper mixtures.*
[10] Енгл.: *proper mixtures.*

Ова, нова, неодређеност – непостојање стања подсистема – је нови спецификум квантне механике, потпуно непознат класичној физици. Да бисмо се у ово уверили, проанализирајмо мерење неке опсервабле, нпр., првог подсистема.

Одаберимо опсерваблу $\hat{A}_1$ чија су својствена стања баш она у изразу (5.14б). Нека је измерена вредност неко a_n. Тада, како се може показати (израз (3.21)), коначно стање сложеног система 1+2 после селективног мерења је

$$|\varphi_n\rangle_1 |\chi_n\rangle_2, \tag{5.20}$$

и то *увек са истим индексом* (n) стања оба подсистема**.** Дакле, мерењем опсервабле првог, практично смо увек измерили и неку опсерваблу другог подсистема, чија су својствена стања $|\chi_n\rangle_2$ из исте канонске форме (5.14б). И овиме смо уочили две ствари: *прво*, постојање ***корелација стања (вредности одређених опсервабли) подсистема***, и, *друго*, ово ***без увођења било каквих ограничења у смислу просторног растојања између подсистема***. Размотримо ова два уочавања.

5.3.1 Квантне корелације (квантна несепарабилност)

Прво, и у класичној физици постоје корелације вредности физичких величина, па отуда и корелације стања. Парадигма класичних корелација су *закони одржања*. Али горње корелације нису тог типа[11]. Наиме, класичне корелације стања подразумевају да ***сваки пар у ансамблу има одређено стање***, и да су стања ***у пару*** међусобно корелисана: $|\varphi_n\rangle_1 |\chi_n\rangle_2$. Ако постоји више могућих избора за стања (више вредности индекса n), тада се сваком индексу n мора придружити нека вероватноћа p_n, што по дефиницији (3.12) води мешаном стању сложеног система:

$$\hat{\rho}_{12} = \sum_n p_n |\varphi_n\rangle_1 |\chi_n\rangle_{2\ 1}\langle\varphi_n|_2 \langle\chi_n| = \sum_n p_n |\varphi_n\rangle_{1\ 1}\langle\varphi_n| \otimes |\chi_n\rangle_{2\ 2}\langle\chi_n|. \tag{5.21}$$

Међутим, како стоји (задатак 5.6):

$$|\Psi\rangle_{12\ 12}\langle\Psi| \neq \hat{\rho}_{12}, \tag{5.22}$$

то ни ***уочене корелације у стању*** $|\Psi\rangle_{12}$ ***не могу бити класичне*** (које су описане изразом (5.21)). Зато се и говори о ***квантним корелацијама*** (стања, тј., вредности опсервабли подсистема) у чистом (***„корелисаном“***) стању $|\Psi\rangle_{12}$ сложеног квантног система.

[11] Закони одржања и даље важе, али они овде нису у првом плану.

Информатички: у стању $|\Psi\rangle_{12}$ нема *a priorne* информације о стањима ***парова подсистема***; штавише, о ***стањима парова подсистема нема ни смисла говорити*** – у пуној аналогији са квантном неодређеношћу (Одељак 5.1). Са друге стране, добијање информације о једном подсистему увек повлачи добијање неке информације о другом подсистему, али без позивања на класичне корелације у сложеном систему. Укупно, ове особине сложеног квантног система се називају ***квантном несепарабилносиħу,*** или понекад ***квантном сплетеношћу*** (енгл.: *"quantum entanglement"*). Оправдање овим изразима стиже од интуиције која се заснива на уочавању да, иако целина има стање, о стањима подсистема, као и парова подсистема се може говорити само условно – ако је (као после мерења на једном подсистему) познато стање једног подсистема, *онда је нужно познато и стање другог* – то јест, о *особинама (информацијама о) једног подсистема нема смисла говорити без фиксирања особина другог, и обратно*! Тако се мора рећи: код сложених квантних система ***целина има одређене особине*** (нпр., одређено стање), док ***подсистеми (као ни парови подсистема) немају*** a priori ***задате особине*** – што се понекад назива ***квантним холизмом*** («нераздељивошћу целине»).

У чистим сплетеним квантним стањима *појединачни подсистеми* немају одређено стање – в. израз (5.19).

У чистим сплетеним квантним стањима *појединачни парови* подсистема немају одређено стање – в. израз (5.22), што је специјални случај квантне неодређености, тј., израза (5.10).

Особина (5.19) се назива *квантном несепарабилношћу*, тј., квантним *холизмом*.

5.3.2 Квантна нелокалност

Друго, променом стања мерењем – које успоставља коначно стање, нпр., (5.20) – се, нужно, успостављају класичне информације о стањима (и вредностима опсервабли) о оба подсистема, и ***за то нема никаквих просторних ограничења***. Наиме, два подсистема се могу налазити и произвољно далеко један од другог, а ефекат (тј., промена стања) се изражава изразом (5.20) без увођења било каквог посебног ограничења. Мерењем се успоставља стање целине, израз (5.20), у којем су ***истовремено*** одређена стања оба подсистема, независно на ком растојању се они налазе. Дакле, квантна несепарабилност има и особину ***нелокалности***, у смислу да није неопходно било какво дејство са једног на други подсистем, а да би се успоставило стање (5.20) и у њему садржана квантна корелација стања подсистема. Зато се каже да до промене стања долази тренутно.

Информатички: добијање информације о једном подсистему имплицира истовремено стицање одређене информације и о другом подсистему, без потребе за дејством (интеракцијом) између два подсистема, или било каквом додатном акцијом споља (као што би било мерење на 2. подсистему). *Довољно је извршити*

мерење на једном подсистему и очитавањем на инструменту (добијањем класичне информације о једном подсистему) *аутоматски је и* ***тренутно*** *позната одговарајућа информација о другом,* ***произвољно удаљеном подсистему*** – што се још зове и ***дистантне корелације*** (Хербут 1984).

Уочена нелокалност има и свој прецизан физички вид: горе речено важи (*Aspect et al 1982*, Нобелова награда а физику за 2022. годину) и за мерења која се обављају на оба подсистема, али у временском интервалу (једно мерење у односу на друго), τ, које је краће од времена потребног светлости (тј., неком физичком дејству) да стигне од једног до другог подсистема. Тада се каже да су све операције на подсистемима (у релативистичком смислу) *локалне*, а да је уочени ефекат – појављивање коначног стања (5.20) – ипак нелокалан.

.

5.3.3 Белова неједнакост

Физичка ситуација: пар честица, 1 и 2, налазе се удаљене једна од друге и на свакој од њих се, ***локално***, могу мерити неке једночестичне опсервабле, Q, R и S, T, редом. Нека су могуће вредности ових варијабли ± 1. Уведимо величину:

$$QS + RS + RT - QT\,. \tag{5.23}$$

Нека су све ово ***класичне варијабле***. Тада се може показати да важи *Белова* (*Bell 1964, Clauser et al 1969*) неједнакост:

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle \le 2\,. \tag{5.24}$$

□ ДОКАЗ: Израз (5.23) је облика

$$(Q+R)S + (R-Q)T\,, \tag{5.25}$$

па с обзиром на могуће вредности варијабли, ***или*** $Q+R=0$, ***или*** $R-Q=0$ следи:

$$QS + RS + RT - QT = \pm 2\,. \tag{5.26}$$

Ако *нису познате вредности ових варијабли, тада се мора рачунати средња вредност*:

$$\begin{aligned}\langle QS + RS + RT - QT\rangle &= \langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = \\ \sum_{q,r,s,t=\pm 1} p(q,r,s,t)(qs + rs + rt - qt) &\le \sum_{q,r,s,t=\pm 1} p(q,r,s,t)\cdot 2 = 2\end{aligned} \tag{5.27}$$

где $p(q,r,s,t)$ представља вероватноћу за избор вредности варијабли. ■

Имплицитне ***претпоставке*** доказа су:
(а) Класична реалност (неусловљено постојање) вредности свих варијабли оба подсистема, у сваком тренутку,
(б) Локалност, тј., да мерење на једној честици не условљава резултат било којег мерења на другој честици.

Ми већ знамо да услови (а) и (б) не важе за чиста стања сложеног квантног система. Поставља се питање: да ли тада важи и Белова неједнакост? Зато прорачунајмо све као и горе, али када имамо посла са ***квантним опсерваблама*** и ансамблом у стању, нпр., $|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|+\rangle_{1z}|-\rangle_{2z} - |-\rangle_{1z}|+\rangle_{2z})$ – ознаке Одељка 2.8.

Дефинишимо следеће опсервабле за два кубита (1 и 2), редом:

$$\hat{Q} = \hat{\sigma}_z, \hat{R} = \hat{\sigma}_x,$$
$$\hat{S} = \frac{-\hat{\sigma}_z - \hat{\sigma}_x}{\sqrt{2}}, \hat{T} = \frac{\hat{\sigma}_z - \hat{\sigma}_x}{\sqrt{2}}. \qquad (5.28)$$

Уочимо да све ове опсервабле имају исти скуп својствених вредности, ± 1.

Како се лако може показати:

$$\left\langle \hat{Q} \otimes \hat{S} \right\rangle = \frac{1}{\sqrt{2}} = \left\langle \hat{R} \otimes \hat{S} \right\rangle = \left\langle \hat{R} \otimes \hat{T} \right\rangle = -\left\langle \hat{Q} \otimes \hat{T} \right\rangle, \qquad (5.29)$$

што даје:

$$\left\langle \hat{Q}\hat{S} \right\rangle + \left\langle \hat{R}\hat{S} \right\rangle + \left\langle \hat{R}\hat{T} \right\rangle - \left\langle \hat{Q}\hat{T} \right\rangle = 2\sqrt{2} > 2 \ ! \qquad (5.30)$$

Дакле, ***не важи Белова неједнакост***!!!

Ово непосредно говори о неважењу макар једне од претпоставки (а) и (б). Ми смо већ дали аргументе за ове ставове, али Белова неједнакост на свој начин то и потврђује. Штавише, Белова неједнакост представља ***квантитативни критеријум*** у овом смислу. Приступајући *сплетеним квантним стањима као информатичком ресурсу,* Белова неједнакост успоставља квантитативни ***критеријум квантне сплетености, као и квантне нелокалности***: ње *има* ако је *нарушена* Белова неједнакост!

НАПОМЕНА: Испоставља се да постоје уопштења квантне нелокалности (тзв. „без-сигналне кутије“ – *non-signaling boxes*, *Popescu and Rorlich 1992*). Иако физички није јасно како би стања која одговарају тим нелокалностима била остварена, може се рећи да *природа допушта и „јачу“ нелокалност* од оне коју смо упознали у вези са квантним сплетеним стањима.

Отуда *сплетеност* и *нелокалност* нису исто. Сплетеност (непостојање стања подсистема, и парова подсистема) се квантификује различитим величинама и нема универзалне, канонске мере сплетености – в., нпр., *Mancini and Tombesi 2003*, *Horodecki 2001*. Са друге стране, нелокалност (горња тачка (б)) се обично квантификује нарушењем Белове неједнакости. При томе, нарушење Белове неједнакости (за сложене квантне системе, а не уопштене системе у смислу горње напомене) води и закључку да је сложени систем у сплетеносм стању; обрнуто, пак не важи.

5.4 Проблем појединачног система

Постулат о појединачним системима (Одељак 2.4) се непосредно уопштава на мешана стања. Наиме, ако знамо да је мешани ансамбл у стању $\hat{\rho} = \sum_i W_i |i\rangle\langle i|$, тада се уобичајено сматра да се може рећи да је и сваки елемент тог ансамбла у истом стању $\hat{\rho}$, са истом интерпретацијом: сваки елемент ансамбла се реално налази у неком стању $|i\rangle$, али ми не знамо у ком од тих стања, па се класична неодређеност стања (Одељак 5.1) преноси (уопштава) и на сваки појединачни елемент ансамбла у стању $\hat{\rho}$.

Ово уопштење ***није строго успостављено*** (нпр., у виду постулата). Постоје формулације квантне механике у којима оно не мора важити[12]. Међутим, све док се налазимо на *терену* квантне механике Поглавља II, чини се да ово уопштење *нема алтернативу*. Отуда се чини и да се појмови квантне неодређености и квантне сплетености[13] (формулисани на нивоу појма ансамбла) једнако тичу и појединачног квантног система.

Општи однос елемената ансамбла и читавог ансамбла је предмет врло суптилних истраживања која овде нећемо наводити (видети у вези са релацијама неодређености, Одељак 2.5). Овде још желимо да нагласимо да је појам појединачног система заправо слабо место – па, у извесном смислу, и *проблем* – стандардне формулације квантне механике и да би истраживања која у средиште пажње узимају појединачне системе заправо овде могла да доведу до значајног доприноса основама квантне механике.

5.5 Напомена

Квантна механика, поред класичне неодређености (која се представља мешаним стањима), уводи ***две нове врсте неодређености***:

(I) *Квантну неодређеност* као општу карактеристику свих чистих стања (ма како простих, или сложених) система; ова неодређеност није последица недовољног познавања (мањка класичних информација) система, већ је последица квантне некомпатибилности (релација неодређености) и исказује се постојањем *квантног информатичког лимита*.

(II) *Квантну несепарабилност* (сплетеност), што је одлика стања сложених квантних система; овде се неодређеност тиче непостојања стања (и вредности опсервабли) подсистема који чине сложени систем, изражено квантним корелацијама и квантном нелокалношћу.

На први поглед, ово је, информатички, лоша вест.

Међутим, мање-више сви задаци квантне информатике се заснивају на следећем питању: ***да ли се ове врсте неодређености могу искористити за корисна информатичка процесирања***?

---

[12] На пример, у тзв., теоријама «скривених варијабли».

[13] Али *не* и интерпретације релација неодређености за појединачни систем – видети Одељак 2.5 и ***Додатак 2.3***.

5.6 Ансамбли vs. *појединачни системи*

Стандардна формулација квантне механике (Поглавље II) истиче стохастичност процеса мерења као инхерентну особину квантних система. Отуда је ансамбалски приступ квантној механици природан. Свеједно, то отвара питање (често постављано, нпр., у Одељцима 2.4, 2.5, 3.9, 5.4) статуса појединачног система у оквирима квантне теорије. Ово питање је од посебног значаја за квантну информатику и рачунање, јер је задатак у овој области заправо *манипулација појединачним* квантним системима (Нобелва награда за фзику за 2012. годину). . Наравно, када год се користи појам вероватноће, тада се има у виду замисао да би се разматрани поступци (описани вероватноћом) заправо могли понављати на ансамблу, и да се одговарајуће вероватноће тичу таквог ансамбла.

Питање	**Ансамбл**	**Појединачни систем**
Важи ли појам вероватноће?	+	-
Важе ли релације неодређености?	+	?
Може ли важити квантна неодређеност (неважење класичне реалности)?	+	+
Може ли важити квантна несепарабилност и нелокалност?	+	+
Може ли важити класична неодређеност (увођењем мешаних стања)?	+	+
Може ли се утврдити („измерити“) квантно стање?	+ (путем, тзв., томографије стања, која овде није представљена)	- (*No-cloning* теорем, Одељак 6.2)
Могу ли се разликовати произвољна квантна стања?	+	- (*No-cloning* теорем, Одељак 6.2; делимично разликовање стања помоћу *POVM* мерења, Одељак 7.3)

Табела 5.1 Дефиниција „појединачног система“ дата је у Одељку 2.4. *No-cloning* теорем дат је у Одељку 6.2. *POVM* мерења дата су у Одељку 7.3. Квантна томографија стања није представљена у овој књизи.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- У вези са Беловом неједнакошћу (тј., са Беловим неједнакостима) потражити на *Интернету* под опцијом "*Bell inequalities*".
- За уопштења Белове неједнакости на вишечестичне системе в. *Greenberger, Horne and Zeilinger 1989, Žukowski and Brukner 2002.*
- У вези са општијим нелокалностима од квантномеханичке садржане у сплетеним стањима претраживати на Интернету под "*nonsignaling boxes*".

ЗАДАЦИ

5.1 Доказати квантну неодређеност опсервабле $\hat{B}$ у стању $\hat{\rho}$, која не комутира са оператором стања $\hat{\rho}$.

Решење: Исказ „вредности неке опсервабле $\hat{B}$ ($\hat{B}=\sum_n a_n|\varphi_n\rangle\langle\varphi_n|$) су класично неодређене" воде, по дефиницији (Одељак 3.6), закључку да је стање система мешано стање типа $\hat{\rho}=\sum_n p_n|\varphi_n\rangle\langle\varphi_n|$, одакле следи $\left[\hat{B},\hat{\rho}\right]=0$. Дакле, ако није испуњена комутативност[14], тада ни неодређеност опсервабле $\hat{B}$ у стању $\hat{\rho}$ није класичне, већ квантне природе и потиче од квантне неодређености опсервабле $\hat{B}$ у стањима $|\varphi_n\rangle$ смешаним у $\hat{\rho}$.

5.2 Доказати израз (5.19).

Решење: у чистом стању (5.14б) постоје корелације стања подсистема. Прецизније, за опсервабле $\hat{A}_1$ и $\hat{B}_2$ чија су својствена стања $|\varphi_k\rangle_1$ и $|\chi_k\rangle_2$, редом, лако се може показати: $W\left(\hat{A}_1,\hat{B}_2;|\Psi\rangle_{12};a_i,b_j\right)=0$, ако $i\neq j$ 'упоредити са изразом (5.20). Међутим, у стању $\hat{\rho}_1\otimes\hat{\rho}_2$ нема никаквих корелација , тј., у општем случају, $W\left(\hat{A}_1,\hat{B}_2;|\Psi\rangle_{12};a_i,b_j\right)\neq 0$.

5.3 Доказати израз (5.20).

Решење: непосредно следи на основи примене израза (3.21).

5.4 Доказати израз (5.21).

Упутство: у аналогији са (3.12)-(3.14).

5.5 Доказати израз (5.22).

Упутство: у аналогији са Задатком 3.7, размотрити вероватноће за резултате мерења, нпр., неке опсервабле $\hat{A}_1\otimes\hat{B}_2$, такве да $\left[\hat{A}_1,\hat{\rho}_1\right]\neq 0\neq\left[\hat{B}_2,\hat{\rho}_2\right]$.

5.6 Исказати квантну неодређеност и сплетеност у терминима појединачног система.

---

[14] Подсетимо се: ако $A\Rightarrow B$, тада је B потребан услов за A. Овде: комутативност је потребан услов за интерпретацију мешаног стања као носиоца класичне неодређености вредности опсервабле $\hat{B}$. Како комутативност није испуњена, то нема класичне, већ квантне неодређености.

VI НЕРАЗЛИЧИВОСТ НЕОРТОГОНАЛНИХ СТАЊА. *No-cloning* ТЕОРЕМ

Квантна информатика барата ***појединачним системима*** – или ***појединачним скуповима*** квантних система; у другом случају, један скуп система је један појединачни елемент (замишљеног) ансамбла. Многи задаци који се тичу квантних стања и мерења се морају додатно дефинисати, с обзиром на то да се стања обично (мада не нужно) приписују ансамблима.

Један такав задатак је и задатак разликовања стања појединачног система. У Одељцима 3.9 и 4.4 дискутовали смо различивост ансамбала, тј., стања која се тичу ансамбала. Међутим, када су у питању појединачни системи (тј., поједини елементи ансамбла), задатак разликовања стања се усложњава. Наиме, на појединачном систему можемо добити *само један резултат мерења*, па је потребно на основи њега[1] разликовати стања.

Ако су стања *унапред позната* и задатак је да их мерењем разликујемо, треба разликовати две врсте ове ситуације. Прво, ако се ради о ортогоналним стањима, довољно је обавити погодно мерење (опсервабле чија су то својствена стања) па различивост, израз (4.6), заједно са Постулатом о појединачним елементима ансамбла, гарантује различивост стања и на нивоу појединачних мерења. Друго, квантна механика познаје и неортогонална стања. Све док се та стања могу разликовати на ансамблима (видети Одељак 3.5), на појединаначним системима то *није могуће*. И то је тема овог поглавља.

6.1 Неразличивост неортогоналних стања

Квантна механика нас учи[2]:

(а) Не постоји опсервабла (еримитски оператор) чија би својствена стања била међусобно неортогонална. Отуда мерењем било које опсервабле није могуће (разликовањем резултата мерења) разликовати било која два неортогонална стања.

(б) Свака два неортогонална стања су својствена за неке, међусобно некомутирајуће опсервабле. Како, пак, у општем случају не постоји поступак којим би се симултано измериле некомутирајуће опсервабле (у смислу добијања оштрих вредности обеју опсервабли), то не постоји ни мерење овог типа којим би се разликовала неортогонална стања.

(в) Нека су *задата* неортогонална стања $|\varphi\rangle$ и $|\chi\rangle$, и нека је стање $|\chi\rangle$ својствено стање неке опсервабле $\hat{B}$ за својствену (једноставности ради, недегенерисану) вредност b. Тада се ***појединачним*** мерењем опсервабле $\hat{B}$ на систему у стању

[1] Понављањем мерења реализује се део ансамбла.
[2] Тачке (а) и (б) се тичу и ансамбала.

$|\varphi\rangle$ може добити вредност b са вероватноћом $|\langle\chi|\varphi\rangle|^2 > 0$, одакле би се, у том (појединачном) мерењу, ***могао извући погрешан закључак*** да је пре мерења (појединачни) систем био у стању $|\chi\rangle$.

Отуда се мора извући следећи закључак: ***не постоји мерење на појединачном систему којим би се, са вероватноћом 1, разликовала неортогонална стања***.

Не може се пренагласити: овде разматрани задатак разликовања стања не треба бркати са задатком (Одељак 3.9) ***разликовања ансамбала***.

Задатак разликовања ансамбала је другачији: имамо два *одвојена ансамбла* у *унапред познатим* (може и неортогоналним) *стањима*, и прорачуни вероватноћа мерења неке опсервабле су различити за те ансамбле. Тада је довољно извршити одабрано мерење на једном ансамблу и упоређивањем са теоријским предикцијама за различите ансамбле утврдити о којем ансамблу је реч.

Једна идеја за разликовање стања: за један појединачни систем у низу (нпр., фотон) *копирати* стање фотона произвољан број пута и тако *направити ансамбл*[3]. Тада је, за унапред задата стања $|\varphi\rangle$ и $|\chi\rangle$, могуће разликовати ансамбле и тако утврдити о којем стању (када је у питању тај, појединачни (и сваки други у низу) систем) је реч.

6.2 Појам клонирања стања

У класичној информатици користи се операција *COPY* (или *FANOUT*, када се користе додатни битови). Њоме се копира, тј. «*клонира*», стање система којим се обрађују информације. Схематски, стање система A се клонира у складу са пресликавањем:

$$(S_A, 0_B) \to (S_A, S_B), \tag{6.2}$$

где је индексом B означен физички систем на којег се копира стање система A. Наравно, ова операција подразумева постојање машине за клонирање којом се ова операција обавља, али је стање те машине занемарено у изразу (6.2).

Препис у квантни формализам је непосредан:

$$|\varphi\rangle_A |0\rangle_B \to |\varphi\rangle_A |\varphi\rangle_B . \tag{6.3}$$

Ако је могућ поступак (6.3), могуће је произвољно понављање истог поступка на произвољном броју система:

[3] Постоји алтернатива прављењу ансамбла (видети Теорем 6.2).

$$|\varphi\rangle_A|0\rangle_B|0\rangle_C \ldots \rightarrow |\varphi\rangle_A|\varphi\rangle_B|0\rangle_C \ldots \rightarrow |\varphi\rangle_A|\varphi\rangle_B|\varphi\rangle_C \ldots . \qquad (6.4).$$

Ово је једна формална дефиниција квантног клонирања. Уочити да клонирање (овде дефинисано) није стохастички процес[4], већ се трансформације стања (6.3) и (6.4) одвијају ***са вероватноћом 1***. При томе, и почетно, и коначно стање су јединичне норме, одакле (видети ***Додатак 2.2*** за доказ) закључујемо да ове трансформације одговарају ***унитарним операцијама*** на простору стања.

Али испоставља се да такав поступак није могућ!

6.3 No-cloning теорем

ТЕОРЕМ 6.1: Квантно клонирање, операција (6.3) (тј. (6.4)), произвољног стања се не може обавити, у принципу.

□ ДОКАЗ: Претпоставимо супротно. Тада је могуће, једном машином која формално оперише као *унитарни* оператор, клонирати два различита, неортогонална стања, $|\varphi\rangle$ и $|\chi\rangle$, за која важи $\langle\varphi|\chi\rangle \neq \begin{cases} 0 \\ 1 \end{cases}$. У формалном запису, клонирање ових стања гласи:

$$\begin{aligned} \hat{U}|\varphi\rangle_A|0\rangle_B &= |\varphi\rangle_A|\varphi\rangle_B \\ \hat{U}|\chi\rangle_A|0\rangle_B &= |\chi\rangle_A|\chi\rangle_B \end{aligned} . \qquad (6.5)$$

Међутим, скаларни производи левих и десних страна у (6.5) воде једнакости: $\langle\varphi|\chi\rangle = \langle\varphi|\chi\rangle^2$, одакле следи да $\langle\varphi|\chi\rangle = \begin{cases} 0 \\ 1 \end{cases}$, у супротности са полазном претпоставком. ■

Из доказа теорема се види да нема забране клонирања за међусобно ортогонална стања ($\langle\varphi|\chi\rangle = 0$), као ни за тривијални случај $|\varphi\rangle = |\chi\rangle$. Зато, физички, теорем успоставља ***немогућност клонирања произвољног*** стања система. Прецизније речено: нису забрањене конструкције машина које би клонирале стања из неког *посебног, унапред задатог скупа* стања, већ се успоставља ***непостојање универзалне, унитарне, машине за клонирање***.

У формализму: могу постојати посебно конструисани (не нужно унитарни) оператори $\hat{U}$ за клонирање унапред одабраног скупа стања, али *не постоји универзални оператор* (универзална унитарна операција, трансформација стања, $\hat{U}$) којом би се клонирало произвољно, непознато стање из Хилбертовог простора стања система.

[4] Супротно: имали бисмо посла са стохастичким клонирањем, тј. клонирање би било успешно са неком вероватноћом – упоредити са Одељком 7.3.

И ето једног проблема: практично најчешће коришћену операцију из класичне информатике, *COPY*, не можемо применити на квантна стања.

6.4 No-cloning $\Leftrightarrow$ *неразличивост неортогоналних стања*

ТЕОРЕМ 6.2: *No-cloning* теорем је еквивалентан ставу о неразличивости неортогоналних стања.

□ ДОКАЗ*:* Претпоставимо да имамо универзалну машину за клонирање. Тада можемо, у складу са (6.4), да клонирамо произвољна, неортогонална стања, $|\varphi\rangle$ и $|\chi\rangle$, у складу са рецептом:

$$|\varphi\rangle \xrightarrow{\text{клонирање}} |\varphi\rangle|\varphi\rangle|\varphi\rangle...|\varphi\rangle \equiv \left|\varphi^{(n)}\right\rangle, \tag{6.6}$$

$$|\chi\rangle \xrightarrow{\text{клонирање}} |\chi\rangle|\chi\rangle|\chi\rangle...|\chi\rangle \equiv \left|\chi^{(n)}\right\rangle. \tag{6.7}$$

Тиме смо добили *сложени систем* (а не ансамбл[5]) од n подсистема, у стањима дефинисаним десним странама израза (6.6) и (6.7).

Сада, због:

$$\lim_{n\to\infty}\left|\left\langle\varphi^{(n)}\middle|\chi^{(n)}\right\rangle\right|^2 = \lim_{n\to\infty}\left|\langle\varphi|\chi\rangle\right|^{2n} = 0, \tag{6.8}$$

за довољно велико n (довољно велики број[6] клонираних стања, тј., подсистема), стања $\left|\varphi^{(n)}\right\rangle$ и $\left|\chi^{(n)}\right\rangle$ представљају (приближна) својствена стања неке опсервабле система од n подсистема. Отуда се мерењем ове опсервабле на сложеном систему, у принципу, могу (са занемарљивом грешком) разликовати ова стања, $\left|\varphi^{(n)}\right\rangle$ и $\left|\chi^{(n)}\right\rangle$, а отуда и неортогонална стања $|\varphi\rangle$ и $|\chi\rangle$ од којих је клонирање почело. Овиме смо доказали импликацију:

могућност клонирања $\Rightarrow$ *могућност разликовања неортогоналних стања* . (6.9)

Обрнуто, ако је могуће разликовати неортогонална стања, тада је могуће, са информацијом о стању, даље задати препарацију произвољног скупа подсистема у то стање, што је, ефективно, клонирање. Ово илуструје Слика 6.11.

Тиме је доказана импликација:

Могућност разликовања неортогоналних стања $\Rightarrow$ *могућност клонирања*. (6.10)

Укупно, (6.9) и (6.10) успостављају еквиваленцију:

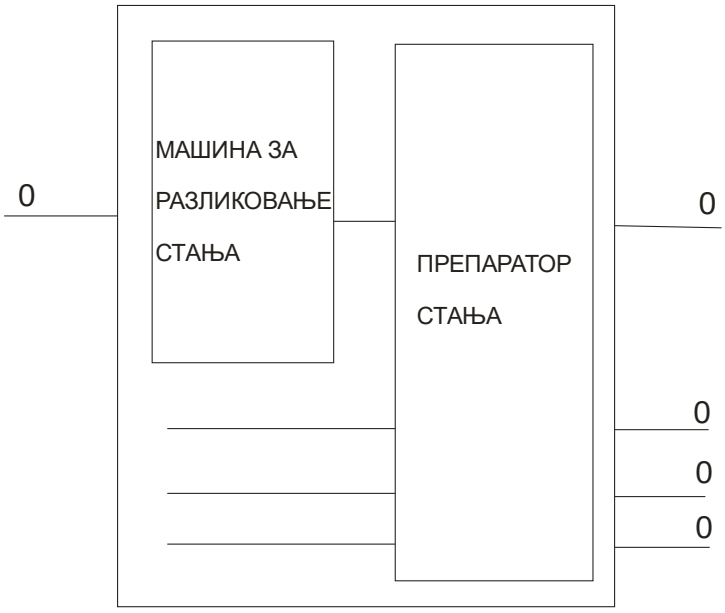
Могућност разликовања неортогоналних стања $\Leftrightarrow$ *могућност клонирања* (6.11)

---

[5] Наравно, ансамбл (овде од n елемената) би био описан стањем $|\varphi\rangle$, тј. $|\chi\rangle$, како је то и описано у Одељку 6.1.

[6] Који још не мора бити довољно велики да би обезбедио ансамбл у смислу претходне фусноте.

а што је логички еквивалентно исказу теорема. ■



Сл. 6.1 Улаз је једно од два неортогонална стања, $|\varphi\rangle \leftrightarrow 0$, или $|\chi\rangle \leftrightarrow 1$; овде је одабрано прво. Помоћу машине за разликовање стања се утврђује о којем стању је реч, и класична информација (или 0, или 1) се прослеђује препаратору. То јест, на основи ове информације се сада, нови, свежи скуп система (кубитова – Одељак 8.2) у произвољним стањима, препарира (в. Одељак 4.2) у стање које је утврдио први апарат. Ефективно, обједињено, „први апарат + препаратор" представљају машину за клонирање.

***Разликовање неортогоналних стања $\Rightarrow$ комуницирање брже од светлости*!**

Нека Алиса и Боб[7] деле пар система у сплетеном стању:

$$|\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2). \qquad (6.11a)$$

Ако Алиса мери свој (под)систем у базису[8] $\{|0\rangle_1, |1\rangle_1\}$, тада и Боб, аутоматски, и *истовремено*, добија свој систем у истом базису (в. израз (5.20)), и то свако стање из базиса са вероватноћом 1/2. Међутим, *комуникација подразумева* контролисани (нестохастички) излаз од стране пошиљаоца (Алисе). Тако, у овој варијанти нема комуникације[9]. Међутим, ако Боб може да разликује неортогонална стања, комуникација брже од светлости је могућа.

[7] Уобичајена имена пара у комуникацији

[8] «*Мерење у базису*» је фраза која означава да се мери опсервабла чији је један својствени базис баш тај, одабрани, базис.

[9] Алиса не може да контролише излаз (овде: резултат свог мерења) са вероватноћом 1.

Наиме, стање $|\Psi^{(-)}\rangle$ се може преписати у облик (што је немогуће за класичне системе, тј., класична стања):

$$|\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_1|-\rangle_2 - |-\rangle_1|+\rangle_2), \qquad (6.11б)$$

где $|\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$. Сада, Алиса може да пошаље поруку сачињену од битова 0 и 1, тако да ове битове кодира мерењима на следећи начин: ако мери у базису $\left\{|0\rangle_1, |1\rangle_1\right\}$, тада је послала бит 0, а ако врши мерење у базису $\left\{|+\rangle_1, |-\rangle_1\right\}$, тада је послала бит 1. Наравно, ако је Алиса послала бит 1, тада је коначно стање Бобовог система једно из базиса $\left\{|+\rangle_2, |-\rangle_2\right\}$. Поента је у следећем: када би Боб био у стању да разликује стања из скупа неортогоналних стања $\left\{|+\rangle_2, |-\rangle_2, |0\rangle_2, |1\rangle_2\right\}$, тј., да разликује Алисина мерења, тада би он једнозначно примио бит Алисине поруке[10]. А порука од Алисе је стигла ***тренутно*** (због квантне нелокалности): чим се заврши Алисино мерење, стање њеног система је *истовремено* успостављено када и стање Бобовог система – дакле, ***брже од било каквог физичког дејства*** - чијим мерењем (накнадним утврђивањем стања свог система) Боб утврђује који бит је добио[11].

Наравно, због немогућности разликовања неортогоналних стања, ни комуникација брже од светлости није могућа.

6.5 Важна напомена

Дакле, за посебне скупове унапред задатих стања, у принципу, није забрањено клонирање стања. Тада је, ако је клонирање могуће, могуће разликовати и неортогонална стања (било користећи (6.6) и (6.7), било користећи једну од ових релација када је реч о ансамблу). Међутим, клонирање посебно одабраних стања је изузетак. ***У општем случају*** ово није могуће обавити, и то је значење *no-cloning* теорема.

У доказу теорема 6.2 је претпостављено да стања нису из неког унапред познатог скупа. Све и да јесу, а не постоји машина за клонирање за тај специјалан скуп стања, резултат теорема стоји као и за непозната стања.

Задатак разликовања стања се тиче ***појединачног система*** (нпр., појединачног фотона или појединачног скупа фотона). Зато ваља још једном нагласити: ***појам вероватноће има смисла само на ансамблу***. Отуда, када кажемо «*да појединачним мерењем опсервабле* $\hat{B}$ *постоји вероватноћа* p_n *да се добије вредност* b_n», то

[10] На пример: Боб је утврдио да је његов систем у стању $|0\rangle_2$, па тада зна да је Алиса мерила у базису $\left\{|0\rangle_1, |1\rangle_1\right\}$, одакле закључује да је Алиса послала бит 0.

[11] Време потребно Бобу за мерење се не урачунава у време потребно за *размену* битова – која се одиграла тренутно (успостављање стања (5.20) је истовремено за оба подсистема).

значи «да се ***у неком појединачном мерењу може појавити вредност*** b_n », али *вероватноћа појављивања овог резултата се мора проверити на ансамблу*.

ЗАДАЦИ

6.1 Доказати Теорем 6.1 када се урачуна и стање машине за клонирање.

6.2 Да ли је забрањено стохастичко клонирање, тј., успешност клонирања са вероватноћом мањом од 1?

6.3 Да ли је забрањено приближно клонирање, тј., добијање стања које није тачно (већ само приближно) једнако почетном?

6.4 Да ли појам вероватноће има смисла на појединачним елементима ансамбла – на „појединачним системима“?
Решење: Суптилно питање! Можда има смисла са чисто математичког становишта. Физички, ипак, чини се да није јасно како би се вероватноћа остварила без неке врсте ансамбла.

VII УОПШТЕНА КВАНТНА МЕРЕЊА. ДЕЛИМИЧНА РАЗЛИЧИВОСТ НЕОРТОГОНАЛНИХ СТАЊА

У Поглављу III добили смо изразе за стања ансамбла после предиктивног мерења. То је последица дефиниције предиктивног мерења (Деф. 3.1).

Међутим, постоји и општији приступ процесу мерења који се заснива на *изразима за коначна стања после мерења*, која се *задају унапред*, дакле као чиниоци *дефиниције* мерења. Ово омогућује уопштења од немале користи у квантној механици и информатици.

7.1 Ортогонална (пројективна) мерења

ДЕФ. 7.1: Под ортогоналним (фон Нојмановим) мерењем опсервабле $\hat{A}$ чија је спектрална форма $\hat{A}=\sum_n a_n\hat{P}_n$, подразумева се поступак који води коначном стању ансамбла (у почетном стању $\hat{\rho}$) задатом следећим изразима:

$$\hat{\rho}\to\left[tr\left(\hat{P}_n\hat{\rho}\right)\right]^{-1}\hat{P}_n\hat{\rho}\hat{P}_n \quad (\textit{селективно мерење}) \tag{7.1}$$

$$\hat{\rho}\to\sum_n\hat{P}_n\hat{\rho}\hat{P}_n \quad (\text{не}\textit{селективно мерење}), \tag{7.2}$$

уз важење услова ортогоналности $\hat{P}_m\hat{P}_n=\delta_{mn}\hat{P}_n$ и потпуности скупа пројектора,

$$\sum_n\hat{P}_n=\hat{I}\ . \tag{7.3}$$

Наравно, ова врста мерења су већ изучена – то су предиктивна мерења Поглавља III, док се овим приступом (дефиницијом) *ставља нагласак на облик промене стања квантног система*. Очигледно је да су промене (7.1) и (7.2) сасвим специјалне.

7.2 Уопштена мерења

ДЕФ. 7.2: Под уопштеним мерењем (или, понекад, само „мерењем“) се подразумева *добијање одређених класичних информација о систему.* Нека су те информације индексиране индексом m. Тада се под мерењем подразумева скуп оператора, $\left\{\hat{M}_m\right\}$, са истим индексима као и информације, који за свако почетно стање ансамбла (система), $|\Psi\rangle$, једнозначно одређује вероватноћу резултата мерења (селективна варијанта) индекса m:

$$p_m=\langle\Psi|\hat{M}_m{}^+\hat{M}_m|\Psi\rangle\,, \tag{7.4}$$

при чему је коначно стање ансамбла задато изразом:

$$\frac{1}{\left\|\hat{M}_m\left|\Psi\right\rangle\right\|^{1/2}}\hat{M}_m\left|\Psi\right\rangle, \tag{7.5}$$

али тако да оператори мерења задовољавају једнакост:

$$\sum_m \hat{M}_m{}^{+}\hat{M}_m = \hat{I}\,. \tag{7.6}$$

Изрази (7.4)-(7.6) су уопштење израза (7.1)-(7.3). Уопштење има два аспекта. Прво, класичне информације се не морају тицати вредности неке опсервабле, већ могу бити општије – како је то углавном случај у класичној информатици (у којој се ретко када информације изражавају вредностима физичких величина). Друго, изрази (7.4)-(7.6) се своде на изразе (7.1)-(7.3) ако важи ортогоналност и ермитичност оператора мерења,
$\hat{M}_m{}^{+} = \hat{M}_m, \hat{M}_m{}^{+}\hat{M}_n = \delta_{mn}\hat{M}_m$.

7.3 POVM мерење

За неке информатичке сврхе довољно је само *делимично* (тј., са довољно високом вероватноћом тачности) *познавање стања појединачних система*. Ова могућност није забрањена *no-cloning* теоремом па је, у складу са тим, и развијена посебна врста, тзв., *Positive Operator Valued Measure* (*POVM*) квантних мерења.

Ова мерења представљају пример уопштених мерења уз једну олакшицу: *не морају бити позната коначна стања система*. Штавише, мерења не морају бити поновљива – што је случај са ретроспективним мерењима која, на овај начин, улазе и у формализам, иако само посредно.

ДЕФ. 7.3: Под *POVM* мерењем се подразумева *уопштено мерење* за које нису важна коначна стања система, а које је дефинисано скупом оператора мерења, $\left\{\hat{E}_m\right\}$, при чему је сваки оператор из скупа *позитиван* оператор[1]. Тада су вероватноће мерења задате изразом:

$$p_m = \left\langle\Psi\left|\hat{E}_m\right|\Psi\right\rangle \tag{7.7}$$

за произвољно почетно стање система, уз услов комплетности:

$$\sum_n \hat{E}_m = \hat{I}\,. \tag{7.8}$$

Упоређујући са ДЕФ. 7.2, намећу се једнакости: $\hat{E}_m = \hat{M}_m{}^{+}\hat{M}_m$, то јест[2] $\hat{M}_m = \sqrt{\hat{E}_m}$.

---

[1] Позитиван оператор (који је ермитски) се дефинише изразом: $\left\langle\psi\left|\hat{E}\right|\psi\right\rangle \geq 0, \forall\left|\psi\right\rangle$.

[2] За сваки позитивни оператор се може дефинисати операција кореновања.

ПРИМЕР: У датом скупу система (или ансамблу) се сваки појединачни систем може наћи у једном од два неортогонална стања, $|\Psi_1\rangle = |0\rangle$, и $|\Psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$. Логика *конструкције оператора мерења* за делимично разликовање ових стања на сваком појединачном елементу скупа је следећа: нека се један оператор мерења тиче догађаја (класичне информације) који је *различив* (ортогоналан) од стања $|\Psi_1\rangle$, а други различив од стања $|\Psi_2\rangle$. Тада, ако добијемо први догађај, означимо оператор са $\hat{E}_1$, знамо да је систем у стању $|\Psi_2\rangle$, и обратно, догађај (резултат мерења) описан оператором $\hat{E}_2$ говори о томе да је систем у стању $|\Psi_1\rangle$. Уведимо стања у складу са овом идејом, $|\Phi_1\rangle \equiv |1\rangle$ и $|\Phi_2\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$. Ако би оператори били дефинисани као $\hat{E}_1 = |\Phi_2\rangle\langle\Phi_2|, \hat{E}_2 = |\Phi_1\rangle\langle\Phi_1|$, тада би важило $\left\|\hat{E}_1 + \hat{E}_2\right\| > \left\|\hat{I}\right\| = 1$, па не важи услов (7.8); еквивалентно, за ове дефиниције оператора мерења важи да вероватноће (за било које стање) задовољавају $p_1 + p_2 > 1$! Зато се, нпр., могу дефинисати оператори мерења следећим изразима:

$$\hat{E}_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|\Phi_1\rangle\langle\Phi_1|,$$
$$\hat{E}_2 = \frac{\sqrt{2}}{1+\sqrt{2}}|\Phi_2\rangle\langle\Phi_2|, \qquad (7.9)$$
$$\hat{E}_3 = \hat{I} - \hat{E}_1 - \hat{E}_2.$$

Уочити: постојање трећег оператора је нужно – то је последица *no-cloning* теорема – и формално следи из услова (7.8). Наравно, ако се мерењем добије резултат описан оператором $\hat{E}_3$, ***ништа није одлучено***, и ***не постоји тражена информација*** о стању система. Вероватноћа таквог догађаја је дата изразом $\langle\Phi_i|\hat{E}_3|\Phi_i\rangle, i = 1,2$.

7.4 Сводивост уопштених мерења на ортогонална мерења

Ортогонална мерења (пројективна мерења, мерења прве врсте, Деф. 3.1) се уобичајено описују у складу са претпоставком да се сложени систем „објект мерења + мерни апарат ($O + A$)“ *може описати Шредингеровом једначином*. Тада дефиниција „уопштеног мерења“ (Деф. 7.2) следи као последица формализма ортогоналних мерења, а не као независан процес мерења. Покажимо ово.

Нека је у складу са Деф. 7.2 задато мерење операторима $\hat{M}_m$ и означимо простор стања објекта мерења са H_O. Придружимо „апарат“ дефинисан простором стања H_A. Формално, запишимо ово – а у складу са Деф. 7.2 - изразом:

$$\hat{U}|\psi\rangle_O|0\rangle_A = \sum_m (\hat{M}_m|\psi\rangle_O)|m\rangle_A, \tag{7.10}$$

где се са д.с. (7.10) појављује неки ортонормирани базис у простору стања апарата, $|m\rangle_A$. Сада се може писати:

$$\begin{aligned} &{}_O\langle\psi|_A\langle 0|\hat{U}^+\hat{U}|\varphi\rangle_O|0\rangle_A = \sum_{m,m'}\langle m|m'\rangle\langle\psi|\hat{M}^+{}_m\hat{M}_{m'}|\varphi\rangle = \sum_{m,m'}\delta_{mm'}\langle\psi|\hat{M}^+{}_m\hat{M}_{m'}|\varphi\rangle = \\ &\langle\psi|\sum_m \hat{M}^+{}_m\hat{M}_m|\varphi\rangle = \langle\psi|\varphi\rangle. \end{aligned} \tag{7.11}$$

Чак ако је избор стања објекта, $|\varphi\rangle_O$, и ограничен на неки подпростор простора стања H_O, израз (7.11) заправо говори о *унитарности* оператора $\hat{U}$. Дакле, макар у принципу, могуће је *унитарном* операцијом $\hat{U}$ обезбедити важење израза (7.10). Отуда је оправдана горе поменута претпоставка да се систем $O+A$ може сматрати објектом Шредингерове еволуције у времену.

Сада, на основи (7.10) лако се уочава: *пројективним* мерењем неке *опсервабле апарата* чији је један својствени базис баш базис $|m\rangle_A$ са д.с. (7.10), у складу са (7.1), стање објекта после мерења као и вероватноћа добијања резултата одређеног индексом m су исти као и у Деф. 7.2.

Физички: „проширењем“ физичког система (овде: објекта мерења, O) на целину ($O+A$) за коју се може задати Шредингерова унитарна еволуција у времену, могуће је сва квантна мерења свести на пројективно мерење.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- У вези са теоријом мерења користити *Дугић 2004, Хербут 1984, d'Espagnat 1971*.
- У вези са *POVM* мерењима користити *Peres 1993*.

ЗАДАЦИ

7.1 За произвољно почетно стање ансамбла, $\hat{\rho} = \sum_i W_i \hat{P}_i$, исписати опште изразе за коначно стање у пројективном мерењу произвољне опсервабле $\hat{A} = \sum_n a_n \hat{\Pi}_n$.

7.2 Наћи коначно стање ансамбла на којем је обављен следећи поступак: за сваки елемент ансамбла се бира један од два поступка, мерење опсервабле $\hat{A}$ са вероватноћом p, или мерење њој некомпатибилне опсервабле $\hat{B}$ са вероватноћом $1-p$.

Решење: према општим правилима Одељка 3.6, добијени мешани ансамбл је мешавина два подансамбла, који одговарају, нпр., неселективним предиктивним мерењима опсервабле $\hat{A}$, са једне, и опсервабле $\hat{B}$, са друге стране. Означимо одговарајуће статистичке операторе са $\hat{\rho}_A$ и $\hat{\rho}_B$, редом, и њихове статистичке тежине у укупном ансамблу – сходно поставци задатка, са p и $1-p$, редом. Тако је стање укупног ансамбла: $\hat{\rho} = p\hat{\rho}_A + (1-p)\hat{\rho}_B$. Ако је почетно стање ансамбла (пре мерења) било $\hat{\sigma}$, тада изрази Одељка 3.8 непосредно дају изразе: $\hat{\rho}_A = \sum_n \hat{P}_n \hat{\sigma} \hat{P}_n$ и $\hat{\rho}_B = \sum_i \hat{\Pi}_i \hat{\sigma} \hat{\Pi}_i$; $\hat{P}$ су својствени пројектори опсервабле $\hat{A}$, док су $\hat{\Pi}_i$ својствени пројектори опсервабле $\hat{B}$. Тако укупно стање коначног ансамбла за разматрану ситуацију има облик:

$$\hat{\rho} = p\sum_n \hat{P}_n \hat{\sigma} \hat{P}_n + (1-p)\sum_i \hat{\Pi}_i \hat{\sigma} \hat{\Pi}_i \,. \qquad (7a)$$

7.3 Доказати $\left\|\hat{E}_1 + \hat{E}_2\right\| > \left\|\hat{I}\right\| = 1$ за пример (7.9).

Решење: без константи које нормирају операторе,
$\hat{E}_1 + \hat{E}_2 = |1\rangle\langle 1| + \left(|0\rangle\langle 0| + |0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0|\right)/2 = |1\rangle\langle 1| + \left(\hat{I} - |0\rangle\langle 1| - |1\rangle\langle 0|\right)/2$.
Отуда $\langle\psi|\left(|1\rangle\langle 1| + \left(\hat{I} - |0\rangle\langle 1| - |1\rangle\langle 0|\right)/2\right)/2|\psi\rangle = \left|\langle 1|\psi\rangle\right|^2 + 1/2 - \mathrm{Re}\left(\langle 0|\psi\rangle\langle\psi|1\rangle\right)$. Како норма вектора подразумева супремум, овде је довољно проценити добијени израз за $|\psi\rangle = |0\rangle$. Тада добијени израз даје вредност 3/2.

7.4 За пример (7.9) израчунати вероватноћу неодлучивог мерења – тј., догађаја који не даје једнозначан одговор на питање стања у којем се појединачни систем налази.
Упутство: ако је почетно стање $|\psi_1\rangle$, тада је вероватноћа $\langle\psi|\left(\hat{I} - \hat{E}_1 - \hat{E}_2\right)|\psi\rangle < 1$, и аналогно за друго стање.

7.5 Изградити *POVM* операторе за разликовање стања $|0\rangle_1|1\rangle_2$ и Беловог стања $\left|\Psi^{(+)}\right\rangle_{12}$ за пар честица чији је, сваке честице, простор стања дводимензионалан.
Упутство: као и у одељку 7.3, уз једнакост: $\hat{I}_{12} = |00\rangle_{12}\langle 00| + |01\rangle_{12}\langle 01| + |10\rangle_{12}\langle 10| + |11\rangle_{12}\langle 11|$, где $|ij\rangle_{12} \equiv |i\rangle_1|j\rangle_2$.

VIII КЛАСИЧНА *vs.* КВАНТНА ИНФОРМАЦИЈА

Класичну информацију карактерише *различивост информација* заснована на *класичној реалности* физичких стања (и вредности варијабли) система на којем се процесирање обавља.

Међутим, класичне системе карактерише и непостојање неортогоналних стања. Отуда и

ПИТАЊЕ: Шта се, ако ишта, може добити ако, као ***информатички ресурс***, користимо квантна стања, уместо класичних?

ОДГОВОР: У овом тренутку није познат потпун и коначан одговор.

ИДЕЈА: Испитати квантни формализам у смислу различитих информатичких задатака са ***нагласком на коришћење специфичности квантних система***, конкретно, коришћење:

(А) Квантне неодређености,
(Б) У сложеним системима коришћење квантне несепарабилности (сплетености, тј., квантних корелација), тј., нелокалности (тренутног релирања стања подсистема после мерења),
(В) Уз уважавање чињенице да се квантно стање не може клонирати (тј., измерити) са вероватноћом 1.

8.1 Квантни паралелизам

Овим уочавањима би требало придружити још једно. Наиме, ***аналогон класичног бита*** су базисни елементи, $|0\rangle$ и $|1\rangle$, неког дводимензионалног простора стања. Али једно стање квантног система је суперпозиција:

$$|\Psi\rangle = a|0\rangle + b|1\rangle . \tag{8.1}$$

Класично, свако процесирање на скупу од n битова одвија се ***сукцесивно***:

$$\begin{aligned} &V(01010010010) \equiv Vx_1 = y_1 \\ &V(10010101010) \equiv Vx_2 = y_2 \\ &..... \\ &V(10101010101) \equiv Vx_N = y_N \end{aligned} \tag{8.2}$$

Међутим, квантна механика познаје линеарне операторе (нпр. унитарне операторе) који задовољавају – по аналогији са (8.1) и (8.2):

$$\hat{V}|\Psi\rangle \equiv \hat{V}\sum_i C_i |x_i\rangle = \sum_i C_i \hat{V}|x_i\rangle = \sum_i C_i |y_i\rangle , \tag{8.3}$$

то јест ***симултано процесирање дуж свих операционих линија из (8.2)***. Другим речима, оно што је рађено у N корака у (8.2), у квантном, (8.3), се уради у ***једном кораку***, ***„паралелно“***. Ова особеност квантног формализма се назива:

(Г) Квантни паралелизам.

Дакле, захваљујући (Г), постоји, макар у принципу, *могућност скраћења извесних информатичких поступака, што је једна од средишњих тема такозване теорије комплексности у теорији рачунања*.

Квантна информација	*vs*	**Класична информација**
Квантни информатички лимит (релације неодређености, тј., некомпатибилност, квантна неодређеност)		Постојање једнозначних вредности *свих варијабли* и *стања* система у сваком тренутку.
$\forall\|\psi\rangle, \exists\hat{B}: \Delta\hat{B} \neq 0$		$\forall B, \exists b, \forall t$
Неразличивост неортогоналних стања, тј., no-cloning теорем (суперпизиција (квантни паралелизам), некомпатибилност, тј., релације неодређености)		Неразличивост класичних стања (или вредности варијабли) је последица *метролошке* грешке. Нулта метролошка грешка води међусобној *различивости свих могућих* стања (и свих вредности свих варијабли) система.
$a_i \xleftarrow{\text{неразличивост}} b_j, \left[\hat{A}, \hat{B}\right] \neq 0$		$a_i \xleftarrow{\text{различивост}} b_j$
***Квантна сплетеност – уплетеност* (*entanglement*)**		Сва стања (ма како сложеног) класичног система су *сепарабилна* – сваки подсистем, у сваком тренутку, *има одређено стање*.
$\|\Psi\rangle = \sum_i C_i \|i\rangle_1 \|i\rangle_2 \neq \|\bullet\rangle_1 \|\circ\rangle_2$		$(\bullet)_1 (\circ)_2$
Квантна нелокалност, т.ј. квантни холизам (квантна сплетеност - *не важи Белова неједнакост*)		Операција на једном подсистему не мора да утиче на просторно удаљене подсистеме истог сложеног система. *Увек важи Белова неједнакост*.
$\|\Psi\rangle = \sum_i C_i \|i\rangle_1 \|i\rangle_2 \xrightarrow{\text{merenje u trenutku t}} \|k\rangle_1 \|k\rangle_2$		

НАПОМЕНА: У поређењу са класичном, квантну информацију одликује читав низ ***ограничења*** (*квантни информатички лимит, немогућност клонирања стања, непостојање стања подсистема сложеног система*). Отуда би се могло учинити да је ово неудобан терен за бављење информатиком. Међутим, ***задатак информатике је баратање информацијама***, а не сама информација. А квантни простор – Хилбертов простор – је много богатији од класичног (в. тачку (Г) и ДЕФ. 8.1).

8.2 Појам квантног бита (кубита)

По аналогији са класичном информатиком уводи се појам ***квантног бита, кубита (qubit)***. Овај модел *физички* је коментарисан у ***Додатку 8.1***, а формална дискусија овог појма је дата у Одељку 10.5.

ДЕФ. 8.1: Под ***кубитом*** се подразумева било који (макар ефективни) дводимензионални простор стања квантног система. Један произвољни, унапред одабрани и фиксирани ОНБ, означен са $|0\rangle$ и $|1\rangle$, који је аналогон класичних битова, назива се ***базисом израчунавања***.

За ***скуп*** физичких кубитова се не узима Паулијев принцип у обзир, тј., кубитови у скупу су међусобно различиви (динамички одвојени – в. Одељак 2.9).

Важно је схватити да се, *по аналогији са класичном информатиком,* подразумева да се све операције (информатичко процесирање) обавља на, и ***тиче се појединачног кубита*** (тј., ***појединачног система*** кубитова), а да се ***појам вероватноће тиче ансамбла.*** При томе, ако имамо скуп кубитова, сви кубитови ***су међусобно различиви*** (не узимају се изменски ефекти у обзир), а тај скуп кубитова ***чини систем***; за довољно велики број кубитова, с обзиром да они не интерагују, тај систем се понекад може (видети Одељак 2.10 и Одељак 9.3.2) третирати и као ансамбл – то зависи од конкретног задатка. Тако, када се говори у терминима вероватноће о, нпр., квантном рачунару, замишља се да се има посла са ансамблом идентичних квантних рачунара.

Међуделовање кубитова у скупу (када се тај скуп *не може* третирати као ансамбл) се најчешће ***спољa изазива*** и ***контролише*** (нпр., спољашњим пољем), чиме се остварују жељене (по правилу, унитарне) ***операције на систему кубитова*** – видети Одељак 10.11.

Отуда квантна информатика доноси изазов за *фундаменталну* квантну механику: мора се подробно изучити садржај квантног формализма на нивоу појединачних система, што представља *задатак контроле појединачних квантних система* у смислу (макар делимичног) познавања стања појединачног система, поступака мерења, контроле и прослеђивања резултата са једног на други појединачни квантни систем, и томе слично.

Додатну потешкоћу у овом смислу представља и чињеница да информатика није изграђена као заокружени систем знања, већ се више ради о *решавању појединачних (или класа сличних) информатичких задатака* – овде са нагласком на оне које је, евентуално*, лакше, или ефикасније обављати (решавати) на квантном „хардверу“*[1]*, него на класичном*.

[1] Класични хардвер су физички *битови*, а кванти су физички *кубитови*.

Ово су општи задаци квантне информатике и најосновнији међу њима су предмет наредна два поглавља.

IX ПРИМЕРИ КВАНТНОГ ИНФОРМАТИЧКОГ ПРОЦЕСИРАЊА

Овде ће бити представљени примери из области квантне информатике у *ужем смислу*. У ширем смислу, квантна информатика обухвата и квантно рачунање, које је предмет следећег поглавља.

Истакнимо још једном основне претпоставке развоја квантне информатичке теорије. Пре свега, ***квантно стање*** (по аналогији са класичном теоријом) се ***третира као информатички ресурс***, са нагласком на специфичности наведене у претходном поглављу – тачке (А)-(Г). По аналогији са класичним битом уводи се појам ***кубита***, или ***систем кубитова, на којем се врши процесирање информација*** непосредним (на пример, унитарним) операцијама. Опет по аналогији са класичним резоновањем, све операције, по правилу, тичу се ***појединачног кубита, тј., појединачног система кубитова,*** за разлику од стандардних експеримената у квантној механици који се обично обављају на ансамблу[1]. Наравно, операције се обављају на ***појединачним кубитима, или појединачном скупу кубитова***, али се све вероватноће (и очекиване вредности) морају проверавати на ***ансамблу*** (ако је то неопходно).

Краће речено: *квантне информатичке операције (по правилу) представљају контролисане операције на једном кубиту, или на једном* скупу *кубитова, у пуној аналогији са класичним случајем, уз коришћење специфичности квантног хардвера (квантна неодређеност, сплетеност, квантни паралелизам) као неке врсте квантног информатичког ресурса*.

У складу са тим су и овде представљени примери квантног информатичког процесирања.

9.1 Квантна телепортација

Забрана клонирања квантних стања је озбиљан хендикеп у поређењу са класичном информатиком. Јер успешно процесирање информација захтева успешан пренос *неизмењених информација* кроз пренос физичких стања у неизмењеном облику. Класично, овај поступак је тривијалан: измери се стање система и та информација се имплементира као стање другог система – *COPY*. Управо то, тј., мерење стања појединачних квантних система, је немогуће – *no-cloning* теорем. Отуда се на први поглед чини да се овиме успоставља озбиљна препрека у поступку процесирања информација на квантним системима. На сву срећу, изнађен је квантни пандан класичног копирања, тзв., *квантна телепортација*.

По правилу, информатички протоколи подразумевају *две стране у комуникацији – Алиса и Боб*. У протоколу квантне телепортације они деле један једини (*појединачни*) пар квантних честица које су квантно корелисане. Свако од

[1] Не може се пренагласити (в. Одељак 8.2): за велики број неинтерагујућих кубитова у скупу, тај скуп се може третирати и као ансамбл (в. Одељак 9.3).

учесника може, на својој честици, тј., на свом кубиту, да обавља произвољна (локална[2]) мерења. Алиса располаже и трећом квантном честицом која има своје, непознато квантно стање. То стање је квантна информација коју треба у ***неизмењеном «облику» пренети Бобу.***

Нека је непознато стање прве честице, које треба телепортовати до Боба, $\left|\Psi\right\rangle_1 = a\left|0\right\rangle_1 + b\left|1\right\rangle_1$. Нека је стање пара честица, 2+3, једно из Беловог базиса (видети ниже), нпр., сплетено стање $\left|\Psi^{(-)}\right\rangle_{23} = 1/\sqrt{2}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)$. Стање укупног система 1+2+3 је (гдегод је могуће не пишемо симбол „⊗“):

$$|\Phi\rangle_{123} = (a|0\rangle_1 + b|1\rangle_1) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3). \qquad (9.1)$$

Уз мало алгебре, стање (9.1) се може преписати у облик:

$$\begin{aligned}\left|\Phi\right\rangle_{123} = \frac{1}{2}\left|\Psi^+\right\rangle_{12}\left(-a\left|0\right\rangle_3 + b\left|1\right\rangle_3\right) + \frac{1}{2}\left|\Psi^-\right\rangle_{12}\left(-a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right) + \\ \frac{1}{2}\left|\Phi^+\right\rangle_{12}\left(-b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right) + \frac{1}{2}\left|\Phi^-\right\rangle_{12}\left(b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right)\end{aligned} . \qquad (9.2)$$

Уочити постојање корелација стања 1. и 2. честице (обе у Алисином поседу) у стању (9.2). Уочити и постојање квантних корелација стања система 1+2 као целине, са стањима треће честице. А стање (9.1) садржи корелације 2. и 3. честице. Ово пребацивање корелација (сплетености) са пара 2+3 на пар 1+2 се назива „заменом сплетености“ (енгл.: *entanglement swapping*). У изразу (9.2), стања сложеног система 1+2 су стања:

$$\begin{aligned}\left|\Psi^\pm\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 \pm \left|1\right\rangle_1\left|0\right\rangle_2\right) \\ \left|\Phi^\pm\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|0\right\rangle_2 \pm \left|1\right\rangle_1\left|1\right\rangle_2\right)\end{aligned} . \qquad (9.3)$$

Ова стања су међусобно ортогонална и чине ОНБ у простору стања два кубита 1+2. Овај базис се назива ***Беловим базисом***, а стања ***Беловим стањима***. Зато се може дефинисати опсервабла система 1+2 чија су ово својствена стања:

$$\hat{B}_{12} = b_1\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + b_2\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + b_3\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + b_4\left|\Phi^-\right\rangle\left\langle\Phi^-\right|. \qquad (9.4)$$

Одељак 5.3 успоставља: из израза (9.2) непосредно следи уочавање да мерењем (одељак 7.1) опсервабле $\hat{B}_{12}$ – дакле мерење обавља само Алиса – једнозначно је познато, после мерења, стање сложеног система 1+2+3. Тако се добија да је мерењем опсервабле $\hat{B}_{12}$ укупни систем у једнозначном коначном стању, у којем *оба подсистема*, (1+2) и 3, имају одређено стање редом:

[2] Мерења на пару кубитоваа, ако нема других кубитова, су нелокална.

$$
\begin{aligned}
b_1 &\Leftrightarrow \left|\Psi^+\right\rangle_{12}\left(-a\left|0\right\rangle_3 + b\left|1\right\rangle_3\right)\\
b_2 &\Leftrightarrow \left|\Psi^-\right\rangle_{12}\left(-a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right)\\
b_3 &\Leftrightarrow \left|\Phi^+\right\rangle_{12}\left(-b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right)\\
b_4 &\Leftrightarrow \left|\Phi^-\right\rangle_{12}\left(b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right)
\end{aligned}
\qquad (9.5)
$$

Али ово уочавање има значајну последицу. Прво, приметимо да су стања треће честице (која после мерења *има своје стање* – није квантно корелисана ни са једним кубитом), повезана унитарним трансформацијама са почетним стањем $\left|\Psi\right\rangle$ на следеће начине:

$$
\begin{aligned}
&\hat{U}_1\left(-a\left|0\right\rangle_3 + b\left|1\right\rangle_3\right) = \left|\Psi\right\rangle_3\\
&\hat{I}\left(-a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right) = -\left|\Psi\right\rangle_3 \equiv \left|\Psi\right\rangle_3\\
&\hat{U}_2\left(-b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right) = \left|\Psi\right\rangle_3\\
&\hat{U}_3\left(b\left|0\right\rangle_3 + a\left|1\right\rangle_3\right) = \left|\Psi\right\rangle_3
\end{aligned}
\qquad (9.6)
$$

ако су матричне репрезентације ових оператора (у репрезентацији базиса израчунавања) дате са:

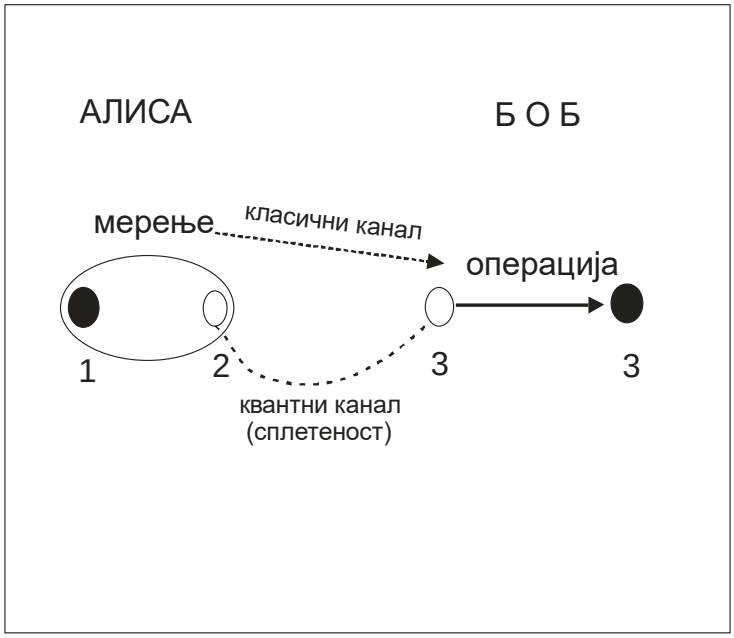
$$
U_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, U_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, U_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (9.7)
$$

Овде је од суштинског значаја приметити да ови оператори, тј., њихове матричне репрезентације, ***не зависе од константи*** a ***и*** b***, то јест, не зависе од почетног стања*** $\left|\Psi\right\rangle$ (које треба телепортовати). При томе, ови оператори су, преко стања на која делују у (9.6а), у ***једнозначној вези са резултатима мерења у (9.5)***. Отуда је јасно: ако би Боб знао који је резултат мерења добила Алиса (неки из скупа b_1, b_2, b_3, b_4), он би само требало да примени одговарајући оператор из (9.7) (одговарајући из скупа $\hat{U}_1, \hat{I}, \hat{U}_2, \hat{U}_3$) и да, сходно (9.6), ***преведе стање трећег кубита у непознато стање*** $\left|\Psi\right\rangle$!

Сада је лако формулисати ***протокол квантне телепортације***: на свом пару кубитова, 1+2, Алиса мери опсерваблу $\hat{B}_{12}$. О томе, ***класичном везом***, обавести Боба. Боб, сада, на основи резултата мерења примени одговарајућу трансформацију на свом, трећем кубиту и коначно стање његовог, трећег, кубита је $\left|\Psi\right\rangle_3$. Тако је непознато стање првог кубита телепортовано на трећи, који је у Бобовом поседу.

Обично се ***трансформација стања услед мерења***, израз (9.5), информатички назива ***квантним каналом***. Класична веза којом Алиса обавештава Боба о

резултату свог мерења назива се ***класичним каналом***, и у складу са овом терминологијом је и схема протокола на Сл. 9.1.



Сл. 9.1 *Квантни канал* је заправо *коришћење квантне сплетености*, које у мерењу једнозначно (и тренутно) релира стања подсистема, израз (9.5). Добивши информацију о мерењу класичним каналом, Боб врши унитарну операцију на 3. кубиту, чиме се стање 3. (Бобовог) кубита преводи у жељено, непознато стање.

На први поглед би се могло учинити да је овиме извршено клонирање стања првог кубита. Међутим, то није тачно. Клонирање подразумева *умножавање стања*, (6.3), тј., (6.4), тј., увећање броја кубита у истом стању. То овде није случај: за било које коначно стање из (9.5), ***у жељеном (непознатом) стању*** $|\Psi\rangle$ ***се налази само 3. кубит***, јер се сложени систем 1+2 налази у квантно сплетеном стању у којем *ниједан подсистем нема своје стање*! (При томе, у реалним експериментима, обично прва два кубита нестају – на њима се врше непоновљива мерења, те чак ни кубитови код Алисе више, физички, не постоје.)

9.2 Квантно супергусто кодирање

У ***класичној*** информатици познато је да ***један размењени физички бит*** (као физички систем) може да пренесе ***највише један бит информације***. Квантно, пак, у погодном протоколу могуће је ***разменом једног физичког кубита*** пренети ***два бита*** класичне информације – *квантно супергусто кодирање*.

Нека Алиса и Боб деле пар кубитова у сплетеном стању:

$$\left|\Psi^{-}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2-\left|1\right\rangle_1\left|0\right\rangle_2\right). \tag{9.8}$$

Одаберимо за Алису следеће трансформације на првом кубиту (који је само њој на располагању):

$$\begin{aligned}
&\hat{I}_1\otimes\hat{I}_2\left|\Psi^{-}\right\rangle_{12}=\left|\Psi^{-}\right\rangle_{12}\\
&\hat{\sigma}_{1z}\otimes\hat{I}_2\left|\Psi^{-}\right\rangle_{12}=\left|\Psi^{+}\right\rangle_{12}\\
&\hat{\sigma}_{1x}\otimes\hat{I}_2\left|\Psi^{-}\right\rangle_{12}=\left|\Phi^{-}\right\rangle_{12}\\
&i\hat{\sigma}_{1y}\otimes\hat{I}_2\left|\Psi^{-}\right\rangle_{12}=\left|\Phi^{+}\right\rangle_{12}
\end{aligned} \tag{9.9}$$

Ако, сада, после одабране трансформације из скупа (9.9), Алиса пошаље свој кубит Бобу, он може да обави мерење опсервабле $\hat{B}_{12}$, израз (9.4), и да из тога једнозначно закључи о којем стању из скупа са д.с. (9.9) се ради. Међутим, ***овиме он стиче два бита класичне информације***, у складу са Табелом 9.1.

Квантно стање	Придружени битови
$\left\|\Psi^{-}\right\rangle_{12}\leftrightarrow b_2$	00
$\left\|\Psi^{+}\right\rangle_{12}\leftrightarrow b_1$	01
$\left\|\Phi^{-}\right\rangle_{12}\leftrightarrow b_4$	10
$\left\|\Phi^{+}\right\rangle_{12}\leftrightarrow b_3$	11

Таб. 9.1 Четири стања из Беловог базиса се класично морају кодирати са најмање два бита.

Тако разменом само једног физичког кубита, Боб (после мерења опсервабле $\hat{B}_{12}$) добија два бита класичне информације. Ово је *класично немогуће*. Уверимо се у ово.

Размотримо класични аналогон. Пре свега, у ***класичном случају нема сплетених стања, а и морамо користити ортогонална стања*** (не постоје неортогонална класична стања). Отуда нам је на располагању само базис израчунавања два кубита: $\left|0\right\rangle_1\left|0\right\rangle_2,\left|0\right\rangle_1\left|1\right\rangle_2,\left|1\right\rangle_1\left|0\right\rangle_2,\left|1\right\rangle_1\left|1\right\rangle_2$. Тада Алиси нису од користи сва четири оператора из (9.9), већ, ефективно, само два, нпр.:

$$\begin{aligned}
&\left|00\right\rangle\xrightarrow{\hat{I}_1\otimes\hat{I}_2}\left|00\right\rangle\\
&\left|00\right\rangle\xrightarrow{\hat{\sigma}_{1x}\otimes\hat{I}_2}\left|10\right\rangle
\end{aligned} \tag{9.10}$$

то јест, добијају се само два стања као резултат, иако је систем двокубитни. Наравно, за пар стања довољан је један бит класичне информације да их

представи, па у класичном случају, (9.10), Таб. 9.2, Боб добија само један бит класичне информације.

Квантно стање	Кодирање класичним битовима
$\|00\rangle$	0
$\|10\rangle$	1

Таб. 9.2 Два стања се могу кодирати паром класичних битова. $|ij\rangle \equiv |i\rangle_1 |j\rangle_2$.

Кључ је у уочавању да су само две трансформације на располагању. Наиме, друга два оператора из (9.9), *на истом почетном стању*, дају:

$$\begin{aligned} |00\rangle &\xrightarrow{\hat{\sigma}_{1z}\otimes\hat{I}_2} |00\rangle \\ |00\rangle &\xrightarrow{i\hat{\sigma}_{1y}\otimes\hat{I}_2} -|10\rangle \equiv |10\rangle \end{aligned} . \qquad (9.11)$$

баш као у (9.10). И све аналогно важи за свако почетно стање $|ij\rangle$. Отуда овај протокол у класичном случају (***без сплетености***) *не нарушава класични резултат са почетка овог одељка*.

НАПОМЕНА: У (9.10) и (9.11) користимо једнакости $\hat{\sigma}_{1x}\otimes\hat{I}_2|0\rangle_1|0\rangle_2 = \left(\hat{\sigma}_{1x}|0\rangle_1 \otimes \hat{I}_2|0\rangle_2\right) = |1\rangle_1|0\rangle_2$, као и $\hat{\sigma}_z|0\rangle = |0\rangle, \hat{\sigma}_z|1\rangle = -|1\rangle$, одакле следе горе коришћени изрази, а на основи израза (Д8.1.3) у ***Додатку 8.1***.

9.3 Квантна криптографија

Задатак криптографије је размена тајних порука. Постоје класични методи (нпр., такозвани, *RSA* систем) који гарантују практично сигурну (безбедну) комуникацију (између *Алисе* и *Боба*), *уколико је обема странама познат тајни кључ за дешифровање, и истовремено, тај кључ није никоме другом познат*, па ни потенцијалном шпијуну, *Еви*.

Управо та претпоставка о тајности „тајног кључа“ је најслабија карика у класичној криптографији. ***Једини задатак квантне криптографије је обезбеђивање тајног кључа***. И управо то се обезбеђује протоколом који ће овде бити изучен, под претпоставком да у комуникацији између Алисе и Боба, осим можда шпијуна Еве, *нема сметњи, тј., „шума“*.

9.3.1 Интуиција

No-cloning теорем гарантује нечитљивост стања кубита (стање се не може измерити). Тако, ако се класична информација имплементира неортогоналним стањима, то ниједан шпијун неће бити у стању да је прочита са сигурношћу, тј.,

са вероватноћом 1. Наравно, уколико се користе само ортогонална стања, тада је то могуће ако Ева зна коју опсерваблу да мери, па учесници у комуникацији морају да користе неортогонална стања.

Зато се може очекивати да ако Алиса шаље Бобу један по један кубит, бирајући стања из неког скупа неортогоналних стања, да тада Ева не може да очита та стања, баш као ни Боб. Али интуиција налаже следеће очекивање: с обзиром да није унапред познато стање која шаље Алиса, свако мерење уноси грешку у коначно стање послатог кубита, те се може очекивати да је та грешка већа уколико се између Алисе и Боба удене Ева са својим покушајем очитавања стања. Ако се, још, та грешка може и детектовати, ***ето начина да се утврди присуство/одсуство Еве у комуникацији***. А тада се већ може смислити поступак за утврђивање заједничког, тајног кључа, једном када су Алиса и Боб сигурни да нема Еве „на траси".

9.3.2 Идеја

Нека Алиса шаље један по један кубит Бобу (укупно N њих). Дакле, *физички систем је један кубит*. Мерења на појединачним кубитовима су статистички независна, па се ефективно низ (али не и *скуп* – што је *систем*) кубитова *може сматрати и ансамблом* (на којем се остварују вероватноће које се тичу појединачних кубитова).

Нека Алиса и Боб унапред договоре (*јавно* – то може да чује и Ева) скупове оператора које ће мерити, произвољно (тајно, и свако за себе) бирајући који од тих, *некомпатибилних оператора*, ће мерити на ком кубиту. И нека је информатички опис тога договорен као у Таб. 9.3.

	Мерење опсервабле $\hat{\sigma}_x$	Мерење опсервабле $\hat{\sigma}_z$
Резултат мерења +1	$\|+\rangle_x \leftrightarrow 00$	$\|+\rangle_z \leftrightarrow 10$
Резултат мерења -1	$\|-\rangle_x \leftrightarrow 01$	$\|-\rangle_z \leftrightarrow 11$

Таб. 9.3 Мерења, коначна стања после мерења, и класично кодирање тих стања, на располагању и Алиси, и Бобу, за сваки кубит у низу. Наравно, $\left|{}_x\langle\pm|\pm\rangle_z\right|^2 = 1/2$.

Ако Алиса бира насумично једно од стања из Таб. 9.3 – тј., врши насумична мерења на сваком кубиту и тиме препарира (в. Одељак 4.2) стање сваког од њих, онда и Ева и Боб немају избора: да би „прочитали" Алисина стања, *они такође морају насумично да врше мерења из истог скупа опсервабли на сваком кубиту*. И, наравно, обоје, са неком вероватноћом, греше. Идеја је да се направи протокол у којем би се та ***грешка услед присуства Еве могла уочити***, и тиме ***детектовати пристуства/одсуство Еве***. Уколико је Ева одсутна, за очекивати је да се лако може утврдити заједнички тајни кључ – и то је срж квантне криптографије.

9.3.3 BB84 протокол без шума

Занемаримо неконтролисане догађаје, тј., „спољашњи шум“.

Мерења опсервабли $\hat{\sigma}_x, \hat{\sigma}_z$ могу да унесу грешку у односу на послати кубит. Нека је стање послатог кубита $|+\rangle_x$. Тада мерење опсервабле $\hat{\sigma}_x$ не мења то стање, те и битови придружени овом стању, 00, остају неизмењени као класична информација о стању из скупа могућих из Таб. 9.3. Међутим, ако је одабрано мерење опсервабле $\hat{\sigma}_z$, тада су могућа коначна стања $|+\rangle_z$ (10), $|-\rangle_z$ (11), оба са вероватноћом 1/2 - Таб. 9.3. Уочити да се погрешним мерењем обавезно мења први бит, а да се други бит мења са вероватноћом 1/2. Сада одаберимо: ***управо од низа других битова се прави тајни кључ***.

BB84 протокол има две фазе.

Прва фаза: На сваком кубиту Алиса стохастички бира мерење једне од двеју задатих опсервабли и прослеђује их Бобу. Наравно, она бележи класичну информацију о одабраном мерењу (један бит, *i*), као и о резултату обављеног мерења (други бит, *j*) у складу са Таб. 9.3. То исто ради и Боб на сваком кубиту добијеном од Алисе. Дакле, свако за себе има парове битова, за сваки физички кубит, $(ij), i = x, z \equiv 0,1,\ j = 1, -1 \equiv 0,1$, што је у једнозначној кореспонденцији са стањима у Таб. 9.3.

Друга фаза има два корака.

Први корак се састоји у јавном комуницирању у којем Боб, *за сваки кубит, јавно* открива које мерење је обавио (тј., свој бит, означимо га са i). Тако Алиса добија информацију о првом биту за сваки кубит. Како погрешан избор води грешци (в. горе), Алиса јавно обавештава Боба где су неслагања у скупу првих битова између њих двоје, и из скупа се бришу сва места (укупно n њих), и код Алисе, и код Боба, где важи $i_A \neq i_B$. Наравно, тада на оба места преостају парови битова за које важи $i_A = i_B$. Ови, преостали, низови других битова се називају ***сировим кључем***, и свако има свој сирови кључ, сачињен од других битова, $\{j_A\}, \{j_B\}$, редом; број битова у сировом кључу је $N - n$.

Други корак представља проверу поклапања других битова, одакле би требало да Алиса и Боб закључе о присуству Еве. Наравно, ако нема шума, а сва погрешна мерења су већ елиминисана (претходним кораком), довољно је *једно једино неслагање у сировом кључу* да се закључи да је Ева прислушкивала – јер (в. горе) иста мерења ($i_A = i_B$) сачувавају оба бита. Наравно, Алиса и Боб не смеју да открију све своје друге битове. Зато они, свако из свог сировог кључа, издвајају m битова, и то такође договоре *јавно*. ***И на тих m битова траже неслагање***. Обоје из својих сирових кључева избришу свих договорених m битова које јавно упоређују. Ако нема ни једног неслагања међу одабраних m битова, постоји велика вероватноћа да Ева није прислушкивала. Тада се остатак сировог кључа

(после елиминације јавно откривених I upore]ivanih m битова) може прогласити ***тајним кључем***. Ако је уочено макар једно неслагање, то је последица Евиног прислушкивања – и нема тајности у комуницирању, те Алиса и Боб морају испочетка.

9.3.4 Процена присуства Еве

Поставља се питање откуд следи закључак о Евином присуству? Друго, са којом вероватноћом Ева може да се прикрије (да остане неоткривена)? Треће, да ли је „тајни кључ“ стварно тајни?

Одговоримо на ова питања, једно по једно.

Одговор на прво питање: без присуства Еве, грешка коју (*a priori* – в. доле) прави Боб износи 1/4. Ако, пак, Ева прислушкује сваки кубит, укупна грешка износи 3/8, што је увећање грешке за 50%! Дакле, наша интуиција (Одељак 9.3.1) је потврђена: Евине и Бобове грешке се акумулирају, па се увећањем грешке може открити присуство Еве.

□ ДОКАЗ: *Под **«грешка»** се овде подразумева неслагање* j_A и j_B. Укупна грешка, *пре друге фазе протокола*, представљена је илустрацијама, Илус. 9.1 и Илус. 9.2. На основи њих следе изрази за укупну грешку у два случаја:

(*нема Еве*) $$p_g = p_2 p_5 = \frac{1}{2}\frac{1}{2} = \frac{1}{4}, \tag{9.12}$$

(*Ева прислушкује*) $$p_g^{(Evajeprisutna)} = p_1 p_3 p_7 p_{14} + p_2\left(p_4 p_8 p_{16} + p_5(p_{10} p_{19} + p_{11} p_{20})\right) = \frac{1}{2}1\frac{1}{2}\frac{1}{2} + \frac{1}{2}\left(\frac{1}{2}\frac{1}{2}\frac{1}{2} + \frac{1}{2}\left(\frac{1}{2}\frac{1}{2} + \frac{1}{2}1\right)\right) = \frac{3}{8} \tag{9.13}$$ ■

Овиме смо прорачунали ***укупну грешку***, на ***свих*** N послатих кубита. Претпоставка је да Ева оперише на ***сваком кубиту***. То, наравно, не мора бити случај.

$$\left|+\right\rangle_z \begin{cases} \xrightarrow[p_1(i_B=i_A)=1/2]{\sigma_z} \left|+\right\rangle_z,\ p_3=1=\left|{}_z\left\langle+\right|+\right\rangle_z\right|^2 \\ \xrightarrow[p_2(i_B\neq i_A)=1/2]{\sigma_x} \begin{cases} \left|+\right\rangle_x,\ p_4=1/2=\left|{}_x\left\langle+\right|+\right\rangle_z\right|^2 \\ \left|-\right\rangle_x,\ p_5=1/2=\left|{}_x\left\langle-\right|+\right\rangle_z\right|^2 \end{cases} \end{cases}$$

$$\left|{}_x\left\langle\pm\right|\pm\right\rangle_z\right|^2=\frac{1}{2}$$

Илус.9.1

$$
\left|+\right\rangle_z \begin{cases}
\xrightarrow[p_1(i_B=i_A)=1/2]{\sigma_z} \left|+\right\rangle_z,\ p_3=1=\left|{}_z\langle+|+\rangle_z\right|^2 \begin{cases}
\xrightarrow[p_6(i_B=i_A)=1/2]{\sigma_z} \left|+\right\rangle_z,\ p_{12}=1=\left|{}_z\langle+|+\rangle_z\right|^2 \\
\xrightarrow[p_7(i_B\neq i_A)=1/2]{\sigma_x} \begin{cases}
\left|+\right\rangle_x,\ p_{13}=1/2=\left|{}_x\langle+|+\rangle_z\right|^2 \\
\left|-\right\rangle_x,\ p_{14}=1/2=\left|{}_x\langle-|+\rangle_z\right|^2
\end{cases}
\end{cases} \\
\xrightarrow[p_2(i_B\neq i_A)=1/2]{\sigma_x} \begin{cases}
\left|+\right\rangle_x,\ p_4=1/2=\left|{}_x\langle+|+\rangle_z\right|^2 \begin{cases}
\xrightarrow[p_8(i_B=i_A)=1/2]{\sigma_z} \begin{cases}
\left|+\right\rangle_z,\ p_{15}=1/2=\left|{}_z\langle+|+\rangle_x\right|^2 \\
\left|-\right\rangle_z,\ p_{16}=1/2=\left|{}_z\langle-|+\rangle_x\right|^2
\end{cases} \\
\xrightarrow[p_9(i_B\neq i_A)=1/2]{\sigma_x} \left|+\right\rangle_x,\ p_{17}=1=\left|{}_x\langle+|+\rangle_x\right|^2
\end{cases} \\
\left|-\right\rangle_x,\ p_5=1/2=\left|{}_x\langle-|+\rangle_z\right|^2 \begin{cases}
\xrightarrow[p_{10}(i_B=i_A)=1/2]{\sigma_z} \begin{cases}
\left|+\right\rangle_z,\ p_{18}=1/2=\left|{}_z\langle+|-\rangle_x\right|^2 \\
\left|-\right\rangle_z,\ p_{19}=1/2=\left|{}_z\langle-|-\rangle_x\right|^2
\end{cases} \\
\xrightarrow[p_{11}(i_B\neq i_A)=1/2]{\sigma_x} \left|-\right\rangle_x,\ p_{20}=1=\left|{}_x\langle-|-\rangle_x\right|^2
\end{cases}
\end{cases}
\end{cases}
$$

Илус.9.2

$$\left|+\right\rangle_z \begin{cases} \xrightarrow[p_1=1-\lambda]{NemaEve} \boxed{\begin{array}{l} Ilus.19.1 \\ p_3 = 1/4 \end{array}} \\ \xrightarrow[p_2=\lambda]{Eva} \boxed{\begin{array}{l} Ilus.19.2 \\ p_4 = 3/8 \end{array}} \end{cases}$$

$$p_g = p_1 p_3 + p_2 p_4 = (1-\lambda)\frac{1}{4} + \lambda\frac{3}{8} = \frac{1}{4} + \frac{\lambda}{8} = \begin{cases} \frac{1}{4}, \lambda = 0 \\ \frac{3}{8}, \lambda = 1 \end{cases}$$

Илус.9.3

9.3.5 Евине стратегије прикривања

Прорачун (9.13) се заснива на претпоставци да Ева врши мерење на сваком кубиту. Наравно, то не мора бити случај, и *Ева може да покуша да се прикрије тако што неће вршити мерење на сваком кубиту*. С обзиром да на крају протокола Алиса и Боб не упоређују све друге битове из сировог кључа, већ само m њих, случајно одабраних, постоји вероватноћа да се међу тих m битова не нађе ниједан на којем је Ева обавила мерење. Тада Алиса и Боб могу извући погрешан закључак.

Означимо са λ вероватноћу да је Ева на једном кубиту обавила мерење[3]. Тада је ***укупна грешка*** дата изразом (Илус. 9.3):

$$p_g(\lambda) = (1-\lambda)\, p_g^{(nemaEve)} + \lambda\, p_g^{(Evajeprisutna)} = (1-\lambda)\frac{1}{4} + \lambda\frac{3}{8} = \frac{1}{4} + \frac{\lambda}{8}. \qquad (9.14)$$

Одговор на друго питање: вероватноћа да Ева не буде откривена провером m кубита ***сировог кључа*** износи:

$$p_{prikrivanja} = \left(1 - \frac{\lambda}{4}\right)^m \qquad (9.15)$$

што за $\lambda \approx 1, m = 200$ износи 10^{-25} !!! Дакле, Ева нема практичних шанси да буде неоткривена јер, ако жели да има информације, њено λ не сме бити осетно мање од 1, а тада, за довољно велико m, вероватноћа да не буде уочена је занемарљива!

□ ДОКАЗ *(9.15)*: У сировом кључу нема непоклапања на првом биту – сва мерења од стране Алисе и Боба се поклапају после прве фазе протокола. У сировом кључу има $N-n$ кубитова, где је n број одбачених кубита (у 2. кораку 2. фазе) код којих се њихова мерења не поклапају ($i_A \neq i_B$). У Илус. 9.2 се налазе сва мерења, па се мерења која се тичу сировог кључа (а која у (9.15) разматрамо) добијају одбацивањем непоклапања у Илус. 9.2 по првом биту – тиме се *редефинишу вероватноће*, $p_6 = p_8 = p_{10} = 1$. Тада *вероватноћа грешке на једном кубиту сировог кључа* изгледа:

$$p_g^{siroviključ} = \lambda\left\{p_1 p_3 p_7 p_{14} + p_2\left[p_4 p_8 p_{16} + p_5 p_{10} p_{19} + p_5 p_{11} p_{20}\right]\right\} = \frac{\lambda}{2}\left\{\frac{1}{2}1\frac{1}{2} + \frac{1}{2}1\frac{1}{2}\right\} = \frac{\lambda}{4}$$

Тако вероватноћа да Ева не буде примећена на *једном кубиту* сировог кључа износи $1-\lambda/4$, а на m (случајно одабраних) кубитова сировог кључа $(1-\lambda/4)^m$. ■

9.3.6 Сигурност тајног кључа

---

[3] Овде подразумевамо да су *сви кубитови статистички еквивалентни*, тј., да (с обзиром да међусобно не интерагују) се могу сматрати ансамблом (за довољно велико N). За статистичку нееквивалентност кубитова видети ***Додатак 9.1***.

Сигурност тајног кључа је одређена вероватноћом (9.15): уколико је та вероватноћа мала, тада се може рећи да поклапање Алисиних и Бобових битова у 2. кораку друге фазе протокола говори о неприслушкивању од стране Еве, са вероватноћом $1-p_{prikrivanja}$. То је ***одговор на треће питање*** из Одељка 9.3.4.

BB84 протокол без шума гласи:

1) Алиса насумично бира мерења (а отуда и препарације стања) сваког кубита понаособ и прави свој низ парова битова, $(i_A j_A)$. Прослеђује кубитове, један по један, Бобу.
2) Боб насумично бира мерења на сваком приспелом кубиту и прави сличну листу парова кубита, $(i_B j_B)$.

Свако од њих сада има свој низ од N парова класичних битова којима кодирају квантна стања кубитова.

3) Боб јавно обавештава Алису о свом скупу првих битова, $\{i_B\}$.
4) Алиса упоређује свој скуп (који је само њој познат), $\{i_A\}$, са Бобовим (јавно обзнањеним) подацима, $\{i_B\}$, за сваки кубит посебно. За свако неслагање, јавно обавештава Боба и обоје бришу места где $i_B \neq i_A$. Тако преостају парови битова при чему се на сваком месту (за сваки пар) поклапају први битови.

Сада свако од њих има ***свој сирови кључ***. Сваки кључ има $N'=N-n$ вредности ***за други бит*** (први се поклапају и више нису корисни па се изостављају), где n представља број елиминисаних парова за које су уочена неслагања у првом биту.

5) Алиса и Боб јавно утврђују позиције у својим сировим кључевима, укупно m позиција, које ће јавно упоредити. Нађу ли макар једно неслагање – Ева је прислушкивала. Нема ли неслагања, *Ева није прислушкивала, са вероватноћом* $1-p_{prikrivanja}$.
6) Ако нема неслагања, Алиса и Боб процењују $p_{prikrivanja}$ и заједнички доносе закључак о присуству Еве. Ако су тиме задовољни (Еве нема на «траси», или има занемарљиве информације о битовима), они
7) Утврђују заједнички ***тајни кључ***. То је скуп битова из сировог кључа када се из сирових кључева елиминише m битова утврђених у кораку 5. Број кубита у тајном кључу је $N-n-m$.

9.4 Осврт

У сваком од примера разматраних у 9.1-9.3 уочене су извесне предности информатичког процесирања на кубитовима у односу над класичним битовима. Све

док је квантна телепортација замена за операцију копирања информације, друга два протокола дају очигледне предности у односу на класичне аналогоне. Тако супергусто кодирање ***пробија класично ограничење*** о броју битова класичне информације у комуникацији. Са друге стране, квантна криптографија обавља суштински важан и ***класично неостварљив задатак*** успостављања (размене на растојању) провериво-тајног кључа у криптографским протоколима. Скица истог протокола са урачунавањем грешака услед *спољашњег шума* је дата у ***Додатку 9.2***.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

Има уистину много извора на овде представљене теме. Свеједно, као најбољи и незаменљив водич и извор информација истиче се монографија *Nielsen and Chuang 2000*. Ту се могу наћи и други криптографски протоколи, као и њихова веза са овде представљеним, *BB84*, протоколом.

Претрагу на Интернету могуће је обавити помоћу различитих фраза. За телепортацију то је, обично, *quantum teleportation*, док се за квантну криптографију, поред очекиване, *quantum cryptography*, може користити (по садржају једнако оправдана) фраза *quantum key distribution*.

ЗАДАЦИ

9.1 Доказати једнакост израза у (9.1) и (9.2)
Упутство: поћи од израза (9.2).

9.2 Доказати придруживање (9.5).
Упутство: користити изразе (7.1)-(7.3).

9.3 Доказати важење израза (9.6а).

9.4 Доказати (9.9) и (9.10).

9.5 Доказати (9.9) и (9.10), али за почетна стања: $|01\rangle, |10\rangle, |11\rangle$. То јест, доказати да се класичним путем (коришћењем само *ортогоналних*, некорелисаних (*несплетених*[4]) стања) не може остварити задатак.

[4] Енглески: *un-entangled*.

X ОСНОВЕ КВАНТНОГ РАЧУНАЊА

Посебан део квантне информатике у ширем смислу представља квантно рачунање. Ради се о *теоријском моделу рачунања* према којем би требало да буду изграђени *квантни рачунари* од којих се очекује решавање рачунских задатака који су *практично* нерешиви на било каквим постојећим, класичним рачунарима (дигиталним, неуронским мрежама, и сл.). Овде ће бити представљен основни модел, тзв. ***модел-кола*** (енгл: *circuit model*) квантног рачунања.

10.1 Појам рачунања. Комплексност

Математички, рачунање (*computing, computation*) представља ***пресликавање***

$$f : a \to b, \tag{10.1}$$

где су a и b елементи неке задате математичке структуре (нпр., поља, групе, векторског простора). Други запис (10.1) је:

$$a \xrightarrow{f} b \tag{10.2}$$

као и

$$b = f(a). \tag{10.3}$$

Рачунске машине – рачунари (*computers*) – су физички системи којима се остварује (имплементира) процес рачунања. *Физички*, рачунање представља ***промену стања рачунске машине***, где a и b из израза (10.1)-(10.3) представљају *почетно* и *коначно стање система у датом прорачуну као процесу еволуције система (рачунара) у времену*. Наравно, за сваки рачунски процес мора постојати 1-1 пресликавање између стања машине и елемената апстрактне структуре пресликавања (10.1)-(10.3).

Средишњи део теорије рачунања представља, тзв., ***Теорија комплексности***. Њен основни задатак је *класификовање рачунских задатака по тежини израчунавања – по комплексности*. Комплексност се изражава преко функционалне зависности параметара израчунавања; једна класа увођења комплексности заснива се на зависности времена потребног за израчунавање у функцији броја битова неопходних за решавање дате класе задатака. Тако се задаци деле на *лаке* (време се изражава као неки полином броја битова) и *тешке* (зависност је надполиномска – „експоненцијална“). За велики број битова, сви тешки задаци су *практично нерешиви за класичне рачунаре*. Примери: Навије-Стоксова једначина хидродинамике (проблем турбуленције), факторисање великих бројева, дискретни логаритам.

Поента у квантном рачунању је да су ***неки тешки задаци класичне теорије комплексности лаки (полиномско време) са становишта квантног рачунања***. Пример: Шоров квантни алгоритам за факторисање великих бројева и дискретног логаритма (в. Одељак 10.9.6).

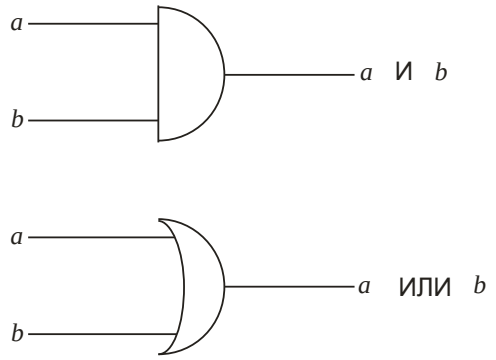
10.2 Појам универзалности рачунања. Реверзибилно рачунање

Како је истакнуто у Одељку 1.5: теоријски модел рачунања је релевантан само ако има особину универзалности.

ДЕФ. 10.1: Под *универзалношћу рачунања* се подразумева модел рачунања који, са *малом вероватноћом грешке*, може, *са произвољно високом тачности*, да израчуна *било коју функцију* (тј., пресликавање). Формално, $p\left(z \approx z_0\right) \approx 1$, где p означава вероватноћу, z резултат рачуна, а z_0 је тачна вредност.

Физички, свака еволуција стања у времену је процес рачунања. Али поента је у захтеву да рачунска машина може, са произвољно великом вероватноћом приближно тачно да прорачуна *било коју функцију*. Могу постојати различити модели универзалног рачунања, али их особина универзалности строго повезује: они су тада сви међусобно, ***рачунски, еквивалентни***. Наравно, за сваки модел постоје задаци који му „леже“, тј., које ефикасније (брже) решава од других модела, али универзалност обезбеђује исту класификацију комплексности задатака за све, међусобно еквивалентне, моделе. Отуда је *довољно реализовати један такав модел у пракси*.

Основне логичке (рачунске) операције код дигиталних (класичних универзалних) рачунара, И и ИЛИ, имају особину неповратности (иреверзибилности) – в. Сл. 10.1. Математички, те операције су неинвертибилне (за ове операције не постоје инверзне операције). Зато се једно време сматрало да не постоји *реверзибилно рачунање*, које подразумева инвертибилне математичке операције; минимум захтева за изградњу таквих операција је да број улаза буде једнак броју излаза, а не као на Сл. 10.1.



Сл. 10.1 Ове операције су математички неповратне, јер нема 1-1 пресликавања између скупа излаза (*output*) и скупа улаза (*input*) представљених линијама, лево и десно, редом, на слици.

Операције И, НЕ-ИЛИ (ИЛИ), НЕ, заједно са помоћним операцијама CROSSOVER и FANOUT чине један (али не и једини могући) скуп ***основних (елементарних) операција универзалног класичног рачунања*** – комбиновањем

само ових операција (логичких „кола“ – откуд потиче назив „***модел-кола***“ рачунања) могу се остварити произвољна пресликавања (израчунавања) на датом скупу битова. Операција CROSSOVER циклично замењује вредности битова, док FANOUT копира стање једног бита на помоћни бит чија се вредност не узима као исход рачунања.

Међутим, фундаментално ***физичко уочавање*** од стране Ландауера отворило је врата следећем закључку:

*Постоји универзално, класично **реверзибилно** рачунање које се физички може остварити реверзибилним процесима. Класично реверзибилно рачунање се може свести*[1] *на класично иреверзибилно, те отуда класични реверзибилни рачунари могу да обаве све као и иреверзибилни – рачунски (у смислу комплексности) су еквивалентни.*

То уочавање се назива ***Ландауеров принцип*** који гласи:

Када рачунар брише један бит информације, минимална енергија која се дисипира у окружење износи $k_B T \ln 2$.

Овај принцип успоставља да се ***само у кораку брисања информација мора трошити (дисипирати у окружење) енергија***, а ***да сви други процеси могу бити (и физички, и математички) реверзибилни***. Практично ограничење коначности меморије захтева брисање информација (попут *reset*-овања код дигиталних рачунара), те нужно, укупно, иреверзибилност (тј., дисипација енергије – ***Додатак 10.1***) се не може избећи. Али *поента је у томе* да основне рачунске операције (аналогони горњих И, ИЛИ, Сл. 10.1) могу имати особину реверзибилности. И заиста, такве операције је могуће конструисати – нпр., Тофолијева (или Фредкинова) капија Одељка 1.5.

На дубљу физичко-информатичку основу *Ландауеровог принципа* указује:

МЕКСВЕЛОВ ДЕМОН. *Други закон термодинамике* (ДЗТД) успоставља немогућност смањења ентропије за изоловани термодинамички систем. Верујући у *стохастичку основу овог закона*, Мексвел (1871. године) је направио *модел у очигледној супротности са овим законом*.

У једној кутији се налази гас у термодинамичкој равнотежи. Кутија је једном преградом подељена на два дела. На прегради се налази помични отвор кроз који могу да пролазе молекули гаса из једног у други део кутије. Мексвел разматра следећу ситуацију: нека се на прегради налази ђаволак који по својој вољи може да отвара и затвара отвор, и тако пропушта молекуле, на пример, један по један. Тада, у принципу, он може да пропушта само брзе молекуле из једног у други део кутије. У дужем оперисању на овај начин, ђаволак ће да наруши термодинамичку равнотежу и смањиће укупну ентропију (изолованог) гаса у кутији, и то ***без вршења рада***.

Иако модел није практично остварив, важан је као нека врста мисаоног експеримента. Решавање овог парадокса има дугу историју, а ***коначно разрешење*** нуди ***Ландауеров принцип***.

Наиме, да би ђаволак могао да обави свој задатак, он мора да мери брзину молекула којег жели да пропусти – тј., мора да *добије (класичну) информацију* о брзини молекула. И то мора да уради за сваки молекул у датом делу кутије. Кључно уочавање је тривијално: да надаље не би грешио (јер молекули су међусобно идентични, и разликују се само по својим брзинама), ђаволак мора да памти информације о сваком обављеном кораку у следу. Те информације

[1] Одељак 1.5 и ***Додатак 1.2***.

морају бити похрањене у *меморији* коју ђаволак мора да консултује у сваком наредном кораку. Међутим, *свака меморија је коначна* (не само практично, већ у принципу) те ће у једном тренутку *ђаволак морати да обрише (reset-ује) меморију*. Сходно ***Ландауеровом принципу***, корак брисања меморије је дисипативан те ***увећава ентропију окружења*** (овде: делова меморије) за најмање $2k_BT$. Тако, ***укупно***, може се показати да смањење ентропије гаса бива надомештено, па чак и преведено у позитиван биланс (пораст) ентропије у укупном систему „гас + меморија", у ***сагласности са*** ДЗТД.

НАПОМЕНА: Мексвелов демон уводи *нераскидивост* појма процесирања информације и основа термодинамике/статистичке механике. Ова интимна веза информатике и основа физике се све чешће тумачи као оправдање тезе (Ландауер) да је информација физички појам („*Information is physical*"). То јест, да се основе, укључујући и ограничења, у могућим поступцима процесирања информације морају тражити у физици, а не у математици – или макар не искључиво у математици. Као ***велика потврда овог става*** појављује се формулисање теорије квантног рачунања (и зачеци квантне теорије комплексности).

10.3 Чрч-Тјурингова теза. Јака Чрч-Тјурингова теза

Сво искуство класичне теорије комплексности обухваћено је следећим, фундаменталним ставовима, тезама.

ЧРЧ-ТЈУРИНГОВА (ЧТ) ТЕЗА: *Класа функција израчунљива на Тјуринговој машини је тачно она класа функција за које бисмо очекивали да су израчунљиве помоћу неког алгоритма.*

Прави развој (математичке) теорије рачунања започео је формализацијом интуитивног појма рачунања. Уведен је појам ***алгоритма*** којим се ***обухвата појам рачунања***. То јест, подразумева се да се ***сваки рачунски поступак заснива на неком (апстрактном појму) алгоритма***. Другим речима: све што се о рачунању може рећи, може се рећи на основи резултата изучавања алгоритма као математичког појма. У овом контексту, Чрч-Тјурингова теза иде даље од интуиције: апстрактни појам алгоритма се формализује кроз рад замишљене машине – Тјурингове машине – те се сада ***успоставља знак једнакости између појмова алгоритма и Тјурингове машине***. Нужно, све што се сада може рећи о рачунању следи из анализе особина Тјурингове машине. То је уједно и садржај Чрч-Тјурингове тезе: ***све што се уопште може израчунати, израчунљиво је на Тјуринговој машини***.

На први поглед, ЧТ теза даје тривијалан исказ. Али оно што она подразумева је заправо шокантно откриће, тј., сазнање. Наиме, као контраст ЧТ тези се појављује појам ***неизрачунљивих функција***!

Баш тако: ***постоје функције које се не могу прорачунати у било каквом алгоритамском поступку, и то у принципу***; пример: *halting problem*. И овај став важи све док је на снази основна парадигма израчунавања – парадигма алгоритма. ЧТ теза успоставља границу између у-принципу-израчунљивих, и у-принципу-НЕизрачунљивих функција!

Отуда се на терену израчунљивих функција, сва комплексност рачунања може дедуковати изучавањем Тјурингове машине. Како, сада, и квантно рачунање

подлеже парадигми алгоритма, ***ЧТ теза успоставља границу израчунљивости и за квантне рачунаре***. То јест, важи став:

> ***Оно што, у принципу, не могу да израчунају класични, не могу да израчунају ни квантни рачунари.***

Широко и обимно искуство у класичној теорији комплексности, а у смислу најбољег модела (класичног) рачунања, обухваћено је следећом тезом.

> ЈАКА ЧРЧ-ТЈУРИНГОВА (ЈЧТ) ТЕЗА: *Било који модел рачунања може се ефикасно симулирати стохастичком Тјуринговом машином уз највише полиномско увећање неопходног броја битова.*

Стохастичка Тјурингова машина је машина са стохастичким излазом (*output*-ом). Ова стохастичност је последица стохастичности алгоритма – било случајног избора улаза (*input*-а), било случајно одабраних логичких (рачунских) операција (из неког скупа унапред задатих операција) за фиксирани улаз. ЈЧТ теза тврди да, ефективно, и у просеку, стохастичка Тјурингова машина представља ***најбољи могући модел рачунања***. И то је ***искуство*** класичне теорије комплексности, укратко и поједностављено исказано.

Међутим, на овом месту се уплићу квантни рачунари, тј., рачунање. Наиме, и опет не-сасвим-прецизно говорећи, квантно рачунање је бољи модел рачунања од класичне стохастичке Тјурингове машине! Дакле, сва је прилика да ***за квантне рачунаре не важи ЈЧТ теза***.

НАПОМЕНЕ: 1. Развој квантних рачунара креће од физике, из квантне механике, и горњи резултат је у прилог ставу да је информација физички појам. Наиме, информатичари сматрају ЈЧТ тезу врхунцем искуства у области теорије комплексности. Разлог томе је помањкање проширивости анализе у смислу изучавања комплексности рачунања. Али, Ландауеров став «*information is physical*» ***отвара потпуно нову стазу у приступу*** – управо оно што недостаје у математичким разматрањима: ***о могућностима и ограничењима рачунања говори (пре свега, ако већ не и искључиво) физика, тј., закони физике*** (*Landauer 1996).* Промена перспективе у теорији комплексности, са класичне на квантну машину, уводи потпуно нови дискурс у теорију и ултимативно је основа горе истакнутог резултата – о надмоћи квантног над класичним рачунањем.

2. Вреди антиципирати: квантно рачунање подразумева ***квантни хардвер***, и има особине *стохастичности и реверзибилности* – дакле обухвата неке од врхунских домета/циљева класичног рачунања. А ипак, ради се о *потпуно новом моделурачунања*.

10.4 Појам квантног рачунања

Само по себи је занимљиво следеће питање: како изгледа (или би могло да изгледа) рачунање на квантном хардверу? То јест, како би се могло обављати рачунање на системима који се повинују законима квантне, а не класичне физике? У извесном смислу, ово питање је у средишту теорије квантног рачунања.

На самом почетку две ствари су јасне: процес мерења на квантном хардверу је *a priori* стохастичан (Одељак 2.2, Постулат о вероватноћама), тако да свако

добијање класичне информације процесом квантног мерења[2] у току квантног рачунања нужно ***чини квантно рачунање стохастичким рачунањем*** – по аналогији са *најбољим класичним рачунањем* (в. ЈЧТ тезу). Друго, све основне квантномеханичке операције су линеарне. А коришћење *унитарних трансформација* би поступак рачунања, макар у том сегменту, учинио ***реверзибилним***. Сваки модел са овим особинама би аутоматски инкорпорирао најбоље и пожељне особине актуелних модела класичног рачунања (стохастичност и реверзибилност).

Дакле, пратећи најновија искуства теорије класичног рачунања, има смисла развијати теоријски модел квантног рачунања са горњим особинама – стохастичности и реверзибилности, али на квантном хардверу.

10.5 Једнокубитне трансформације

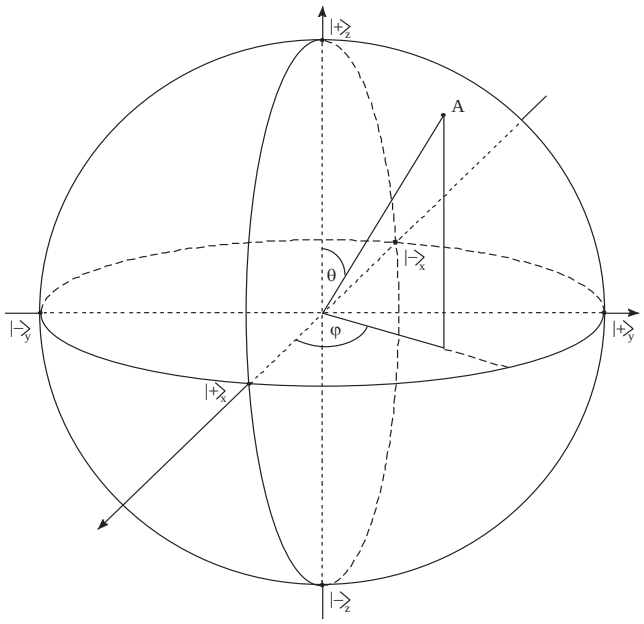
Општи савет развоја квантног рачунања гласи: где год је то могуће, и у мери у којој је то могуће, усвојити опште резоне и методе класичног рачунања.

Поред мотива истакнутог у Одељку 10.4, овај савет пружа и методску основу за физичко-информатичко разграничење класичног и квантног рачунања. Наиме, да би квантно рачунање имало практичног смисла, пожељно је да неке информатичке операције у рачунању обавља ефикасније, а то је, чини се, најлакше уочити/проверити пратећи горњи савет. Јер се праћењем класичних резона непосредно уочава када се од њих мора одустати, као и да је тада поређење двају глобалних модела (класичног и квантног) једноставније.

Тако је и уведен појам ***квантног бита, кубита***, ДЕФ. 8.1. Аналогон класичног бита, пара $(0,1)$, је ***„базис израчунавања“***, један ОНБ у датом простору стања, $\{|0\rangle,|1\rangle\}$. Као што ће то у Одељку 10.8 бити посебно наглашено, информатичко процесирање (па, по претпоставци, и рачунање) искључиво са скупом стања из „базиса израчунавања“ није информатички боље (ефикасније), или слабије (мање ефикасно) од процесирања на пару класичних битова.

Стање једног кубита и све унитарне операције на њему се могу представити графички, тзв., *Блоховом сфером*, Сл. 10.2.

[2] Полазни постулат Поглавља IV.



Сл. 10.2 Тачке у пресецима оса са основним равнима су својствена стања Паулијевих оператора $\hat{\sigma}_i, i = x, y, z = 1, 2, 3$. Тачка A припада сфери. Ротације не сфери одговарају пресликавању стања кубита једно у друго.

За сваки базис $|0\rangle, |1\rangle$ у $2D$ простору стања могу се дефинисати следећи ермитски, и истовремено унитарни оператори:

$$\begin{aligned} \hat{\sigma}_z &= |0\rangle\langle 0| - |1\rangle\langle 1| \\ \hat{\sigma}_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ \hat{\sigma}_y &= i|1\rangle\langle 0| - i|0\rangle\langle 1| \end{aligned} \tag{10.4}$$

где $|0\rangle \equiv |+\rangle_z, |1\rangle \equiv |-\rangle_z$, ознаке Одељка 2.8. Формално, уведени оператори су Паулијеве сигма-матрице, тј., оператори. На основи (10.4) лако је проверити *њихову ермитичност и унитарност*.

Из теорије спина-1/2 добро су познате везе између стања истакнутих на Сл. 10.2:

$$\begin{aligned} \hat{U}_y\left(\frac{\pi}{2}\right)|\pm\rangle_z &= |\mp\rangle_x \\ \hat{U}_x\left(\frac{\pi}{2}\right)|\pm\rangle_z &= |\pm\rangle_y \\ \hat{U}_x(\pi)|\pm\rangle_z &= i|\mp\rangle_z \equiv |\mp\rangle_z \end{aligned} \tag{10.5}$$

где су коришћене ознаке за (унитарни) оператор ротације $\hat{U}_{\vec{n}}(\varphi)$ око осе одређене ортом $\vec{n}$ за угао φ. Свака таква ротација је облика:

$$\hat{U}_{\vec{n}}(\varphi) = \cos\frac{\varphi}{2} + i\hat{\sigma}_n \sin\frac{\varphi}{2}, \tag{10.6}$$

где $\hat{\sigma}_n = \hat{\vec{\sigma}} \cdot \vec{n}$. Последњи израз у (10.5) је еквивалентан једнакости $\hat{\sigma}_x \left|\pm\right\rangle_z = \left|\mp\right\rangle_z$.

Свака ротација (10.6) представља придруживање тачака на Блоховој сфери. Сама Блохова сфера представља геометријски приказ простора стања једног кубита. Отуда се ***скупом ротација на Блоховој сфери исцрпљује скуп могућих, једнокубитних трансформација – под условом да су све трансформације унитарне***.

За уже потребе квантног рачунања, у којима је *почетно* стање једног кубита једно од два стања из базиса израчунавања, згодно је општи запис повезати са Сл. 10.2, то јест дати запис опште ротације ако је почетно стање $\left|0\right\rangle \equiv \left|+\right\rangle_z$:

$$\hat{U}_n(\vartheta,\varphi) = \exp(i\gamma)\left(\cos\frac{\vartheta}{2} + \exp(i\varphi)\hat{\sigma}_n \sin\frac{\vartheta}{2}\right). \tag{10.7}$$

Дакле, ротација (10.7) преводи стање $\left|0\right\rangle$ у неко стање које на Сл. 10.2 одговара тачки A, одређеној угловима (ϑ,φ). Наравно, фаза γ ништа не мења у дефиницији стања добијеног разматраном ротацијом.

Једноставности ради, уведимо скраћено писање: $\hat{\sigma}_z \equiv \hat{Z}, \hat{\sigma}_x \equiv \hat{X}, \hat{\sigma}_y \equiv \hat{Y}$. Сада се може дати теорем чији доказ овде неће бити дат:

ТЕОРЕМ 10.1: Свака једнокубитна трансформација (ротација на Блоховој сфери) се може записати на један од три, међусобно еквивалентна, начина:

(А) $\exp(i\alpha)\hat{A}\hat{X}\hat{B}\hat{X}\hat{C}$, где су $\hat{A},\hat{B},\hat{C}$ три унитарна оператора који задовољавају

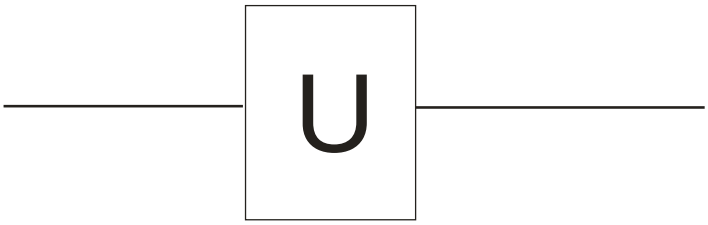
$$\hat{A}\hat{B}\hat{C} = \hat{I} \tag{10.8а}$$

(Б) $\exp(i\alpha)\hat{U}_x(\beta)\hat{U}_y(\gamma)\hat{U}_z(\delta)$, за неке углове β,γ,δ, (10.8б)

(В) $\exp(i\alpha)\hat{U}_n(\beta_1)\hat{U}_m(\gamma_1)\hat{U}_n(\beta_2)\hat{U}_m(\gamma_2)\ldots$ за два неколинеарна орта $\vec{m},\vec{n}$. (10.8в)

Теорем указује на богатство могућих реализација једнокубитних трансформација (ротација на Блоховој сфери). Ингениозност у изналажењу алгоритама се *овде своди на вештину изградње једнокубитних операција*.

Графички, једнокубитна операција $\hat{U}$ се представља као на Сл. 10.3:



Сл. 10.3 Једна линија означава један кубит. Пре операције то је почетно, а после операције, заокружене правоугаоником, је коначно стање једног кубита.

Од посебног значаја је следећи скуп операција:

(*Адамарова трансформација*) $\hat{H} = \frac{1}{\sqrt{2}}\left(\hat{Z} + \hat{X}\right)$. (10.9)

што *у репрезентацији базиса израчунавања* постаје унитарна матрица:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{10.10}$$

(*Операција* $\pi/8$) $T = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(i\pi/4\right) \end{pmatrix}$ (10.11)

(*Операција* $\pi/4$ - *«фаза»*) $S = T^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. (10.12)

Уочити да су сви оператори унитарни, а да је $\hat{H}$ још и ермитски (што, како се лако доказује, повлачи $\hat{H}^2 = \hat{I}$).

10.6 Двокубитне трансформације. Модел-кола квантног рачунања

По аналогији са класичним случајем, скуп од n битова се у квантном случају моделује као скуп од n кубитова. У складу са Постулатом о више-честичним системима, Одељак 2.9, простор стања таквог скупа је дефинисан изразом:

$$H^{(n)} = \otimes_{i=1}^{n} H_i \,. \tag{10.13}$$

Базис израчунавања за скуп од n кубитова уводи се по аналогији са класичним случајем, који представља низ битова, нпр.:

$$01010010110 \rightarrow |0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle,$$

где се подразумева директни (тензорски) производ између суседних стања – стања суседних кубитова. Тако базис израчунавања изгледа:

$$
\begin{aligned}
&|0\rangle \equiv |0\rangle|0\rangle...|0\rangle|0\rangle \\
&|1\rangle \equiv |0\rangle|0\rangle...|0\rangle|1\rangle \\
&... \\
&\left|2^n-1\right\rangle \equiv |1\rangle|1\rangle...|1\rangle|1\rangle
\end{aligned}
\qquad (10.14)
$$

Нас превасходно занима двокубитни систем. Његов базис израчунавања, $|i\rangle, i=0,1,2,3$ дефинисан је скупом (базисом) $|k\rangle_1|l\rangle_2, k,l=0,1$, уз договор $|k\rangle_1|l\rangle_2 \equiv |kl\rangle$. Наравно, на сваком кубиту се могу вршити (локалне) операције, независно од другог, како је то представљено у Одељку 10.5. Те операције (једнокубитне операције) су заправо „једночестичне операције“ из курса квантне механике (Поглавље II).

Овде нас занимају двокубитне операције, тј., операције које, у општем случају, мењају стање *оба* кубита. Од посебног су интереса, тзв., *Контролисане операције*.

Условне (контролисане) операције се дефинишу као двокубитне операције које су на базису израчунавања дефинисане на следећи начин: стање једног (нпр., првог) кубита се не мења при операцији, а стање другог се мења условно (контролисано), *само* ако је стање првог кубита $|1\rangle$. Ако је у питању нека операција $\hat{U}$, тада «контролисано-$\hat{U}$ ($C-\hat{U}$)» се алгебарски (операторски) представља трансформацијама стања из базиса израчунавања:

$$
\begin{aligned}
&|0\rangle_1|\Psi\rangle_2 \to |0\rangle_1|\Psi\rangle_2 \\
&|1\rangle_1|\Psi\rangle_2 \to |1\rangle_1 \otimes \hat{U}_2|\Psi\rangle_2
\end{aligned}
\quad . \qquad (10.15)
$$

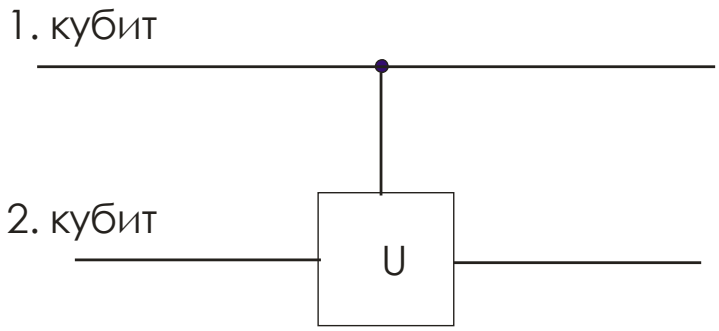
Општија ознака контролисаних операција је $C_1-\hat{U}_2$ где индекс уз «C» указује који је то контролни кубит, а индекс уз операцију $\hat{U}$ указује на кубит на којем (условно) треба обавити операцију. Наравно, ако има више од два кубита у скупу, уопштење ознака је непосредно, $C_i-\hat{U}_j$, са очигледним ознакама. Наравно, сваки кубит у скупу, у принципу, може бити контролни, и сваки може бити «мета» операције. Тако се у изразу (10.15) могу заменити индекси, чиме се мења и улога кубитова у таквој операцији.

Графички, $C_1-\hat{U}_2$ се представља као на Сл. 10.4.

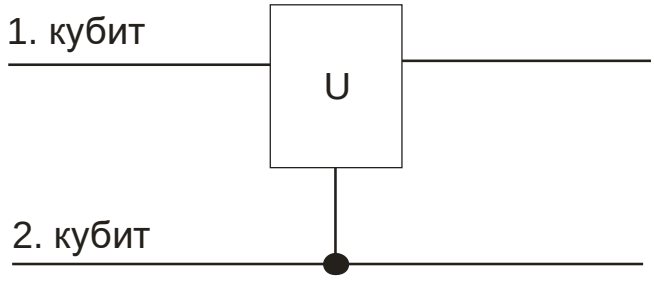
Обрнут случај се представља као на Сл. 10.5.

НАПОМЕНА: Изостављање усправне линије и недостатак тачке на Сл. 10.4,5 значи једнокубитне (неусловљене) операције. Тако, нпр., тада би Сл. 10.5 била представљена у следећој операторској форми:

$$|i\rangle_1|j\rangle_2 \to \hat{U}_1|i\rangle_1 \otimes |j\rangle_2 .$$

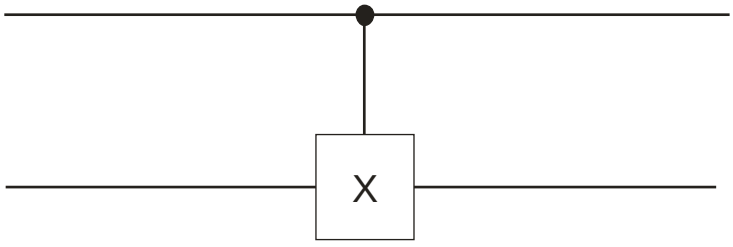


Сл. 10.4 Свака линија означава по један кубит. Тачка указује на контролни кубит (и стање тог кубита се не мења), а условљеност операције на 2. кубиту (кубит „мета“) је означена усправном линијом; $C_1 - U_2$



Сл. 10.5 Овде је други кубит контролни, а мета је први кубит; $C_2 - \hat{U}_1$.

Посебно је корисна, тзв., *CNOT* (*XOR*) трансформација, представљена графички на Сл. 10.6.



Сл. 10.6 Графичка ознака за *CNOT* (*XOR*), што је *у базису израчунавања* „искључиво-ИЛИ“, ИЛИ, операција (Табела 10.1).

Алгебарски, ова операција дата је следећим једнакостима (памтећи да, сходно (10.4), важи $\hat{X}|\pm\rangle_z = |\mp\rangle_z$, тј. $\hat{X}|0\rangle = |1\rangle$ и $\hat{X}|1\rangle = |0\rangle$) *у терминима базиса израчунавања*:

$$\begin{aligned}
&|0\rangle_1|0\rangle_2 \to |0\rangle_1|0\rangle_2 \\
&|0\rangle_1|1\rangle_2 \to |0\rangle_1|1\rangle_2 \\
&|1\rangle_1|0\rangle_2 \to |1\rangle_1|1\rangle_2 \\
&|1\rangle_1|1\rangle_2 \to |1\rangle_1|0\rangle_2
\end{aligned} \quad . \tag{10.16}$$

Табеларно представљено у ознакама класичне логике, (10.16) даје:

1. кубит	2.кубит	Излаз 2. кубита
НЕ	НЕ	НЕ
НЕ	ДА	ДА
ДА	НЕ	ДА
ДА	ДА	НЕ

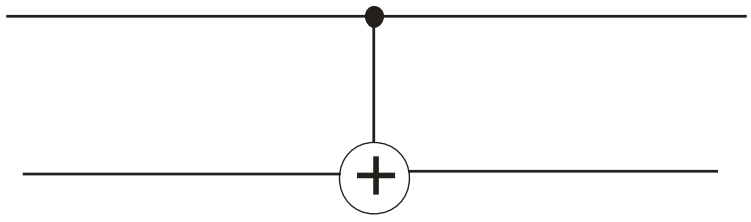
Таб. 10.1 Излаз за други кубит указује на логичко порекло разматране операције као «искључиво или » (*или, или*). Овде: «НЕ» ≡ 0.

Из Таб. 10.1 се види да се ради о добро познатој, класичној логичкој операцији ***«искључиво-ИЛИ»***. Међутим, како се ради о кубитовима, а не класичним битовима, треба бити опрезан. Наиме, ***само на скупу стања из базиса израчунавања*** се може говорити о аналогији са класичном операцијом. Општије, ова операција ***води успостављању квантне сплетености***. На пример:

$$\left(C_1 - \hat{X}_2\right)(a|0\rangle_1 + b|1\rangle_1) \otimes |1\rangle_2 = a|0\rangle_1|1\rangle_2 + b|1\rangle_1|0\rangle_2. \tag{10.16a}$$

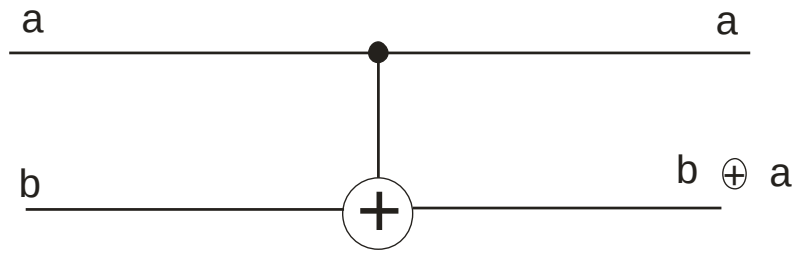
И ово је опште уочавање: *само на базису израчунавања има смисла правити аналогију са класичним операцијама; у општем случају постоје операције које доносе квантне суперпозиције и квантну сплетеност, које су класично потпуно непознате*!

Други, и уобичајени, графички запис истог је:



Сл. 10.7

и преузет је из класичног аналогона, што вреди још једном истаћи: у базису израчунавања, Сл. 10.7, тј., представљена операција (логичко коло), је логички еквивалентно класичном, представљеном на следећој слици:



Сл. 10.8 Класична операција *CNOT* на пару битова.

где $\oplus$ означава „сабирање модула 2“ ($0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$), што је „искључиво-ИЛИ“ из Таб. 10.1.

Главни резултат (класичне) теорије рачунања је откриће постојања ***универзалног скупа елементарних операција*** (Одељак 1.5), чијим се комбиновањем (у алгоритамском следу) може остварити произвољна логичка операција, тј., произвољно пресликавање.

Дакле, поента је у постојању малог броја основних (елементарних) операција чијим комбиновањем се могу изградити све друге операције, у складу са ЧТ тезом – ***модел-кола[3] рачунања***. Поставља се питање да ли је нешто слично могуће и у квантном формализму. Одговор је дат у наредном одељку. Овде ћемо се задржати на неким специфичностима квантног формализма.

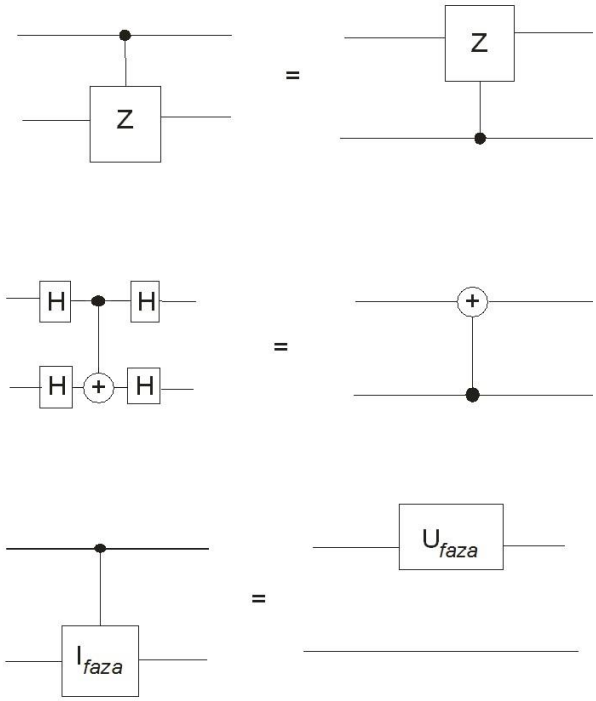
Као што је добро познато, *скуп унитарних оператора на векторском простору чине* ***групу***. Отуда је математичка структура логичких (овде: ***квантно логичких***) операција једноставнија од класичне, и у принципу је боље изучена. У случају једног кубита то је *SU(2)*, а у случају n кубитова то је *SU(* 2^n *)* група.

Због тога је згодно усвојити још један савет из класичне теорије рачунања:

Усвојити модел-кола квантног рачунања и развити га на групно-теоријским особинама скупа унитарних трансформација на скупу од n ***кубитова***.

Прецизније: за сваки број кубитова, n, развити модел на скупу (квантних) логичких операција које треба *третирати као логичка кола, чијим комбиновањем се могу остварити сложења кола*. Питање постојања универзалног скупа елементарних таквих логичких кола остављамо за следећи одељак. Овде ћемо још истаћи пар примера једнакости логичких кола.

[3] Енгл.: *circuit model*.



Сл. 10.9 Операција $I_{faza} = \exp(i\alpha)\hat{I}$, док је у репрезентацији базиса израчунавања $U_{faza} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\alpha) \end{pmatrix}$.

□ Доказ друге једнакости:

Лева страна:

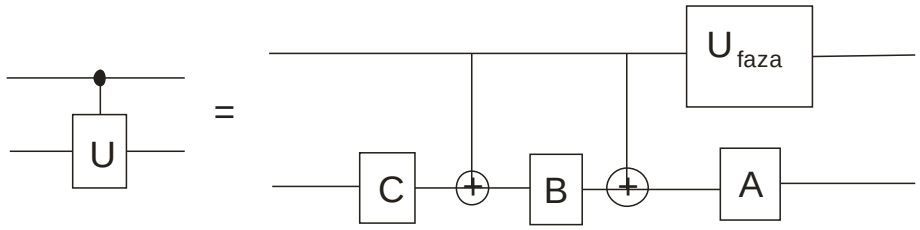
$$\begin{aligned}
&\left(\hat{H}_1 \otimes \hat{H}_2\right)\left(C_1 - \hat{X}_2\right)\left(\hat{H}_1 \otimes \hat{H}_2\right)|0\rangle_1|0\rangle_2 = \\
&\left(\hat{H}_1 \otimes \hat{H}_2\right)\left(C_1 - \hat{X}_2\right)\tfrac{1}{2}(|0\rangle_1 + |1\rangle_1) \otimes (|0\rangle_2 + |1\rangle_2) = \\
&\tfrac{1}{2}\left(\hat{H}_1 \otimes \hat{H}_2\right)(|0\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2 + |1\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2) = \\
&\tfrac{1}{4}(|00\rangle + |01\rangle + |10\rangle + |11\rangle + |00\rangle - |01\rangle + |10\rangle - |11\rangle + |00\rangle - |01\rangle - |10\rangle + \\
&|11\rangle + |00\rangle + |01\rangle - |10\rangle - |11\rangle) = |0\rangle_1|0\rangle_2. \qquad (10.17)
\end{aligned}$$

Десна страна:

$$\left(C_2 - \hat{X}_1\right)|0\rangle_1|0\rangle_2 = |0\rangle_1|0\rangle_2, \qquad (10.18)$$

што важи и за свако почетно стање $|ij\rangle (\equiv |i\rangle_1 |j\rangle_2)$, што остављамо читаоцу за проверу. ■

Графички приказ исказа Теорема 10.1(А) је дат на следећој слици.



Сл. 10. 10

10.7 Универзалност модела-кола квантног рачунања

Упутно је поновити: универзалност рачунања (модела рачунања) значи способност модела да обезбеди, са великом вероватноћом тачности, макар приближан (приближно тачан) резултат. Из практичних разлога је упутно *засновати рачунање на малом скупу елементарних операција*. Тако се долази до појма универзалног скупа елементарних (логичких, рачунских) операција.

У квантном случају, „логичке операције“ су унитарне операције на простору стања скупа кубитова. Отуда ***универзалност квантног рачунања***, као критеријум, заправо успоставља захтев да се, са великом вероватноћом, приближно тачно може остварити ***било која унитарна операција*** на датом скупу кубитова. Испоставља се да се то може остварити *једно-* и *дво-* кубитним операцијама.

Један пример универзалног скупа елементарних квантних логичких операција дат је следећим теоремом.

ТЕОРЕМ 10.2: Скуп {*Адамарова трансформација,* $\pi/8$ *-операција*, *CNOT*} представљају ***универзални скуп елементарних операција модела-кола квантног рачунања*** на било којем броју кубитова.

Појашњења:

(А) За сваки кубит у скупу се дефинишу једнокубитне трансформације из наведеног скупа.
(Б) За сваки пар кубитова у скупу се дефинише *CNOT* операција.
(В) Теорем успоставља да се комбиновањем операција из (А) и (Б), у алгоритамски уређеном следу може, са произвољном тачношћу, остварити произвољна, унитарна операција на скупу од n кубитова.

(Г) Нека је задата жељена унитарна операција на скупу, неко $\hat{U}$. Са $\tilde{\hat{U}}$ означимо операцију добијену по рецепту из (В). Тада израз „са произвољном тачношћу“ значи да важи једнакост:

$$\left\| \left(\hat{U} - \tilde{\hat{U}} \right) |\Psi\rangle \right\| \approx 0, \forall |\Psi\rangle . \qquad (10.19)$$

Другим речима: комбиновањем једнокубитних операција из скупа (не нужно на свим кубитовима) и *CNOT* операције на паровима кубитова (не нужно са свим комбинацијама парова), може се успешно остварити унапред задата операција $\hat{U}$ на било ком скупу кубитова.

□ ДОКАЗ: Доказ следи комбиновањем следећих двају теорема.

ТЕОРЕМ 10.3: Произвољна унитарна матрица на d-димензионалном унитарном векторском простору, може се остварити као *производ „двонивоских“*[4] *матрица* (унитарних матрица). При томе, производи једнокубитних и *CNOT* операција се могу користити за имплементирање произвољног двонивоског оператора (матрице).

ТЕОРЕМ 10.4: Адамарова и $\pi/8$-трансформација се могу користити за имплементирање произвољне једнокубитне операције.

Свака унитарна операција се репрезентује унитарном матрицом. Према Теорему 10.3, свака унитарна матрица се може представити као производ „двонивоских операција“ (матрица). А ове, пак, се могу разбити на производе једнокубитних и *CNOT* операција (наравно, задатих у матричном облику). Коначно, како се свака једнокубитна операција може разбити на производ Адамарове и $\pi/8$-трансформације – Теорем 10.4 – то се, *укупно*, свака унитарна матрица (а тиме и апстрактни унитарни оператор) може представити као уређени производ унитарних операција из скупа наведеног Теоремом 10.2.

Докази Теорема 10.3 и 10.4 захтевају извесне детаље теорије матрица, као и познавање метода теорије комплексности, те овде неће бити дати. ■

ЈЕДНА ИЛУСТРАЦИЈА:
Задат је оператор $\hat{U}$. Према Теорему 10.3, он се може записати као производ $\hat{V}_1\hat{V}_2...\hat{V}_k...$, где су $\hat{V}_i$, тзв., „двонивоске“ операције. Даље, према Теорему 10.3, свака двонивоска операција се може записати као производ једнокубитних и *CNOT* операција, нпр., $\hat{V}_k = \hat{U}^{(k)}{}_{i\alpha} \otimes CNOT_{\beta\gamma} \otimes \hat{U}^{(k)}{}_{j\delta} \otimes ...$, где је једнокубитна трансформација $\hat{U}_{i\alpha}$ i-та операција на α-том кубиту, итд. Коначно, према

[4] Под „двонивоским матрицама“ подразумевају се матрице (произвољне $d \times d$ матрице) које нетривијално делују само кроз две (или мање) своје *врсте*. Примери: $\begin{pmatrix} \alpha & \beta & 0 \\ \gamma & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, и $\begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & d & e \end{pmatrix}$.

Теорему 10.4, свака једнокубитна операција се може представити као производ Адамарове и $\pi/8$-трансформације, $\hat{U}_{i\alpha} = \pi/8 \otimes H \otimes \ldots$. Сада, сменом овога у израз за двонивоске операторе, а ових у израз у којем су у производу двонивоски оператори, јасно је да се сваки унитарни оператор може представити као производ операција уведених Теоремом 10.2.

***Други скупови елементарних операција универзалног модела-кола квантног рачунања*:**
А. Како показује Китајев (*Kitaev 1997*), квантна Тофолијева капија, Адамарова и $\pi/8$-капија чине један скуп елементарних капија.
Б. Како показују Баренко и др (*Barenco et al 1995*), скуп $CNOT$ плус све могуће једнокубитне трансформације такође чине један скуп елементарних капија у моделу-кола универзалног квантног рачунања.

10.8 Дефиниција квантног рачунања

ДЕФ. 10.2: Информатичко процесирање на квантном хардверу са основним скупом универзалних логичких операција Теорема 10.2 назива се квантним рачунањем и састоји се из следећих, општих корака:
(а) обављања, у алгоритамском следу, унитарних операција на неком скупу кубитова,
(б) процеса квантног мерења (најчешће у базису израчунавања).
Резултат завршног мерења на систему представља ***резултат рачунања****.*

Опште особине квантног рачунања су:

(i) *реверзибилност* процеса рачунања, што је последица унитарности основног скупа логичких операција – свих, у сваком поступку (алгоритму), осим корака мерења и брисања информација.

(ii) *стохастичност* као последица мерења на систему, при чему се подразумева велика вероватноћа добијања приближно тачног резултата рачунања.

Као што стоји у Оквиру ниже, квантно рачунање се може свести на класично реверзибилно рачунање. Са друге стране, може се показати (Одељак 1.5) да се класично реверзибилно рачунање може свести на класично иреверзибилно рачунање. Отуда стоји:

Све што, ефикасно, могу да обаве класични, могу и квантни рачунари.

Обрнуто, пак, не стоји. А пуну разлику између двеју врста рачунања могу дати само квантни алгоритми.

Теорем 10.2 гарантује изградивост квантне Тофолијеве капије помоћу једно- и дво- *кубит*них операција, а Задатак 10.3 то и потврђује. Квантна Тофолијева капија (Задатак 10.3) постаје идентична класичној Тофолијевој капији (уведеној у Одељку 1.5, и у ***Додатку 1.2***) у *операисању* ***искључиво*** *на базису*

израчунавања. Наравно, оперисање квантне Тофолијеве капије на суперпозицијама стања из базиса израчунавања води класично непознатим стањима. Надаље имамо у виду само класичну Тофолијеву капију.

Као што је у ***Додатку 1.2*** показано, Тофолијева капија се може користити као основа класичног, универзалног *иреверзибилног* рачунања, а зане-маривањем неких излазних битова (видети основе класичног реверзибилног рачунања, нпр., у *Nielsen and Chuang 2000*), Тофолијева капија остварује и универзално *реверзибилно*, класично рачунање – што подразумева реверзибилне капије и на мањем броју битова од три.

Занимљиво: може се показати (в., нпр., *Nielsen and Chuang 2000*) да једно- и дво- *бит*не реверзибилне операције нису довољне за универзално реверзибилно класично рачунање; за ово (универзално, класично реверзибилно рачунање) је неопходна макар тробитна операција, каква је Тофолијева, или Фредкинова (в. Одељак 1.5)).

Остваривањем *стохастичког* избора улазних битова у Тофолијеву капију, остварује се и *стохастичност рачунања* заснованог на Тофолијевој капији.

Отуда, обједињено: ***квантна Тофолијева капија*** (остварена једно- и дво- *кубит*ним операцијама, Задатак 10.3) која оперише ***искључиво на базису израчунавања*** (чиме постаје еквивалентна класичној Тофолијевој капији), ***може да оствари свако универзално класично рачунање*** – било оно реверзибилно, или не, било оно стохастичко, или детерминистичко.

Упоређујући *довољност једно-* и *дво- кубит*них капија *квантног* рачунања, са једне стране, са *неопходношћу тро-бит*не (нпр., Тофолијеве) капије за универзално реверзибилно *класично* рачунање, са друге стране, поставља се питање: у чему лежи предност квантних капија над класичним, с обзиром да се квантномеханички *не мора* баратати *тро*кубит*ним* капијама?

Помоћу Задатка 10.3 долазимо до одговора. Наиме, уочити да операција $\hat{V}$ у логичком колу у овом задатку има необичну особину: $\hat{V}^2 = \hat{X}$, где, *на базису израчунавања*, важи $\hat{X} = \text{НЕ}$, па у истом базису (аналогону класичних битова) $\hat{V} = \sqrt{\text{НЕ}}$ - *непостојећа једно*бит*на операција*!

Тако, постојање „*корена из НЕ*“ у квантном формализму (у „квантној логици“), а ***као последица квантних суперпозиција*** (то јест, квантног паралелизма)[5], говори о ***богатству квантних операција***, у поређењу са класичним, Буловим логичким операцијама. Отуда је постојање ове операције (*бесмислене* у оквирима класичне Булове логике) ултимативна основа изградње Тофолијеве капије *једно-* и *дво-кубит*ним операцијама.

Другим речима: *непостојање „корена из НЕ“ у* класичном *рачунању* лежи у основи неизградивости Тофолијеве капије помоћу једно- и дво- *бит*них операција.

Занимљиво, „корен из НЕ“ се лако физички остварује, видети ***Додатак 10.2***. И овде се испољава Ландауерова максима „***информација је физичка***“ на делу: *које логичке операције су могуће, треба потражити у физици, тј., у информатичкој анализи физичких теорија*.

[5] Уочити увођење суперпозиција на основи резултата Задатка 10.3:
$\hat{V}|c\rangle = \frac{(1-i)(\hat{I}-i\hat{X})}{2}|c\rangle = \frac{(1-i)}{2}\left(|c\rangle - i|\bar{c}\rangle\right), c = 0,1$.

10.9 Примери квантних алгоритама

Сваки алгоритам подразумева уређен низ логичких (рачунских) операција. Наравно, све операције изграђене су на основном скупу универзалних операција, и један пример таквог скупа у овом смислу дат је Теоремом 10.2.

Овде ће бити представљени основни, најједноставнији квантни алгоритми од историјског значаја за област квантног рачунања. На крају овог одељка биће скренута пажња на актуелне резултате који неће бити детаљно представљени.

10.9.1 Појам квантне црне кутије

Мање-више сви квантни алгоритми (а по угледу на класичне) користе подрутине које се називају „*црним кутијама (ореклима*; ***black boxes, oracles***)“. Ради се о посебно дизајнираним операцијама, тј., пресликавањима унапред задатог типа. Тако, нпр., ако је потребно пресликавање типа неке функције f, класично се одговарајућа црна кутија означава као трансформација (операција) U_f. Могућност изградње такве класичне трансформације гарантује универзалност класичног рачунања. У квантном случају ствари су потпуно аналогне: операција $\hat{U}_f$ се може изградити – то гарантује Теорем 10.2. Деловање квантне операције је *формално идентично класичној* ***на*** *базису израчунавања*.

У већини квантних алгоритама се подразумева постојање такве операције без експлицитне конструкције одговарајућег логичког кола. При томе се, поједностављено (и за многе практичне сврхе, довољно) претпоставља да се ове операције „тренутно одвијају“ – а у прорачуну комплексности алгоритма, по правилу, се *комплексност заснива* на *броју неопходних понављања операција квантних црних кутија*. Наравно, дефиниција операције на базису израчунавања непосредно, и једнозначно, води уопштењу разматране операције, које нема класичног аналогона (в. Пример дат изразом (10.16а)).

*10.9.2 Дојчов (*Deutsch*) алгоритам*

Историјски први, и методски најважнији, је Дојчов алгоритам (*Deutsch 1985*).

ЗАДАТАК: Нека функција f пресликава један бит у један бит; $f:\{0,1\}\to\{0,1\}$. Треба утврдити да ли је пресликавање константно, $f(0)=f(1)$, или је „балансирано“, $f(0)\neq f(1)$.

Класично, *мора се два пута користити (класична) црна кутија*:

$U_f(0)=f(0)$,

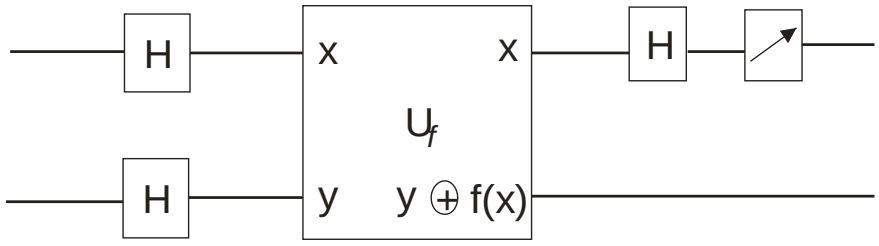
а онда поновити исто, за улаз 1,

$U_f(1) = f(1)$.

Простим упоређивањем добијених вредности обављен је задатак *у два корака*, тј., са два покретања орекла. Квантно се то може обавити у једном кораку, тј., у само једној употреби (квантне) црне кутије.

ИДЕЈА: Ако $f(0) = f(1)$, тада $f(0) \oplus f(1) = 0$, а ако $f(0) \neq f(1)$, тада $f(0) \oplus f(1) = 1$. Искористимо ово за конструкцију квантног алгоритма, наравно, *уз коришћење квантне црне кутије.*

Дејвид Дојч показује да алгоритам који је овде представљен графички испуњава горње захтеве: при чему је довољна *само једна употреба* квантне црне кутије.



Сл. 10.11 Средишњи део графа је квантна црна кутија. Она *на базису израчунавања* оперише баш како то чини класична црна кутија на класичним битовима (тј., класичном биту). Класично, операција је $(x, y) \xrightarrow{U_f} (x, y \oplus f(x))$ – в. (10.21). На крају се врши одређено квантно мерење на првом кубиту, означено косом стрелицом.

Читајући граф Сл. 10.11, ***с лева надесно***, све се може записати у еквивалентну ***операторску (алгебарску) форму***. У ту сврху уочимо алгоритам:

1. Припрема стања два кубита; први кубит чини први, а други кубит други *регистар*, $|0\rangle_1, |1\rangle_2$, редом.
2. На сваком кубиту засебно се обавља Адамарова трансформација.
3. Примена (двокубитне) операције, квантне црне кутије, $\hat{U}_f$.
4. На први кубит се примени Адамарова трансформација.
5. На првом кубиту се обавља одређено квантно мерење.

Запишимо операције за сваки кубит (тј., сваки регистар):

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad (10.20)$$

и дефиницију орекла за базис израчунавања:

$$\hat{U}_f \left|x\right\rangle_1 \left|y\right\rangle_2 = \left|x\right\rangle_1 \left|y \oplus f(x)\right\rangle_2, x, y = 0,1. \tag{10.21}$$

Сада се горњи граф може превести у операторски облик:

1. $\left|\varphi\right\rangle_1 \left|\chi\right\rangle_2 \xrightarrow{\text{препарација стања}} \left|0\right\rangle_1 \left|1\right\rangle_2$
2. $\hat{H}^{(2)} \left|0\right\rangle_1 \left|1\right\rangle_2 \equiv \hat{H}_1 \otimes \hat{H}_2 \left|0\right\rangle_1 \otimes \left|1\right\rangle_2 = \hat{H}_1 \left|0\right\rangle_1 \otimes \hat{H}_2 \left|1\right\rangle_2 = \left|\Psi\right\rangle_{12}$
3. $\hat{U}_f \left|\Psi\right\rangle_{12} = \left|\Phi\right\rangle_{12}$
4. $\hat{H}_1 \otimes \hat{I}_2 \left|\Phi\right\rangle_{12} = \left|\Phi'\right\rangle_{12}$
5. Одређено квантно мерење на систему у стању $\left|\Phi'\right\rangle_{12}$.

Укупно, операторски, граф је облика:

$$\left(\hat{H}_1 \otimes \hat{I}_2\right) \hat{U}_f \left(\hat{H}_1 \otimes \hat{H}_2\right) \left|0\right\rangle_1 \left|1\right\rangle_2. \tag{10.22}$$

Прорачунајмо (10.22).

$$\left(\hat{H}_1 \otimes \hat{I}_2\right) \hat{U}_f \left(\hat{H}_1 \otimes \hat{H}_2\right) \left|0\right\rangle_1 \left|1\right\rangle_2 = \frac{1}{\sqrt{2}} \left(\hat{H}_1 \otimes \hat{I}_2\right) \hat{U}_f \left(\left|0\right\rangle_1 \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right) + \left|1\right\rangle_1 \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right)\right) \tag{10.23}$$

Даљи рачун је лако обавити ако знамо да важи једнакост (10.24) из Оквира ниже.

$$\hat{U}_f \left|x\right\rangle_1 \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right) = (-1)^{f(x)} \left|x\right\rangle_1 \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right). \tag{10.24}$$

□ *Доказ (10.24.).*

На основи (10.21) следи:

$$\hat{U}_f \left|x\right\rangle_1 \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right) = \frac{1}{\sqrt{2}} \left(\left|x\right\rangle_1 \left|0 \oplus f(x)\right\rangle_2 - \left|x\right\rangle_1 \left|1 \oplus f(x)\right\rangle_2\right). \tag{10.25}$$

Размотримо случај $x = 0$.

Тада д.с. (10.25) има облик:

$$\frac{1}{\sqrt{2}} \left(\left|0\right\rangle_1 \left|0 \oplus f(0)\right\rangle_2 - \left|0\right\rangle_1 \left|1 \oplus f(0)\right\rangle_2\right). \tag{10.26}$$

Ако је $f(0) = 0$, израз (10.26) постаје:

$$\frac{1}{\sqrt{2}} \left|0\right\rangle_1 \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right) = (-1)^{f(0)} \frac{1}{\sqrt{2}} \left|0\right\rangle_1 \left(\left|0\right\rangle_2 - \left|1\right\rangle_2\right).$$

Ако је $f(0)=1$, израз (10.26) постаје:

$$-\frac{1}{\sqrt{2}}|0\rangle_1\left(|0\rangle_2-|1\rangle_2\right)=(-1)^{f(0)}\frac{1}{\sqrt{2}}|0\rangle_1\left(|0\rangle_2-|1\rangle_2\right).$$

Аналогни прорачун за $x=1$ даје исти резултат, са $f(1)$ у експоненту, тако да се обједињено добија израз (10.24). ■

Сменом (10.24) у (10.23) се добија:

$$\frac{1}{\sqrt{2}}\left(\hat{H}_1\otimes\hat{I}_2\right)\left((-1)^{f(0)}|0\rangle_1\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2)+(-1)^{f(1)}|1\rangle_1\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2\right)=$$

$$\hat{H}_1\otimes\hat{I}_2\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle_1+(-1)^{f(1)}|1\rangle_1\right)\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2) \qquad (10.27)$$

Нека је $f(0)=f(1)$. Тада (10.27) постаје:

$$\hat{H}_1\otimes\hat{I}_2\frac{1}{\sqrt{2}}(-1)^{f(0)}\left(|0\rangle_1+|1\rangle_1\right)\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2)=$$

$$(-1)^{f(0)}|0\rangle_1\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2) \qquad (10.28)$$

Нека је $f(0)\neq f(1)$. Тада (10.27) постаје:

$$\hat{H}_1\otimes\hat{I}_2\frac{1}{\sqrt{2}}(-1)^{f(0)}\left(|0\rangle_1-|1\rangle_1\right)\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2)=$$

$$(-1)^{f(0)}|1\rangle_1\frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2) \qquad (10.29)$$

Изрази (10.28) и (10.29) су заправо коначни. Јер у овим изразима стања првог кубита (првог регистра) су из базиса израчунавања, и *једнозначно* су везана за жељени резултат: $|0\rangle_1\leftrightarrow f(0)=f(1)$, тј., $|1\rangle_1\leftrightarrow f(0)\neq f(1)$. Тако *мерењем*[6] *неке опсервабле чија су својствена стања стања из базиса израчунавања 1. кубита*, резултат мерења једнозначно води одговору на постављено питање: $+1\leftrightarrow f(0)=f(1)$, $-1\leftrightarrow f(0)\neq f(1)$. А поента је у томе да се квантна црна кутија користи само у једном кораку – двоструко брже него у класичном случају

Алгоритам гласи:

1. Препарација два регистра (сваки са по једним кубитом) у стање $|0\rangle_1|1\rangle_2$

[6] Што се још назива и „мерењем у базису израчунавања“.

2. $\xrightarrow{H^2} \frac{1}{\sqrt{2}}\left(|0\rangle_1 + |1\rangle_1\right)\frac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right)$

3. $\xrightarrow{U_f} \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle_1 + (-1)^{f(1)}|1\rangle_1\right)\frac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right)$

4. $\xrightarrow{H_1 \otimes I_2} \begin{cases} (-1)^{f(0)}|0\rangle_1 \frac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right), f(0) = f(1) \\ (-1)^{f(0)}|1\rangle_1 \frac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right), f(0) \neq f(1) \end{cases}$.

5. Мерење у базису израчунавања првог регистра, $\left\{|x\rangle_1, x = 0,1\right\}$.

*10.9.3 Дојч-Јоса (*Deutsch-Josza*) алгоритам*

Дојч-Јоса алгоритам (*Deutsch and Josza 1992*) је уопштење Дојчовог алгоритма.

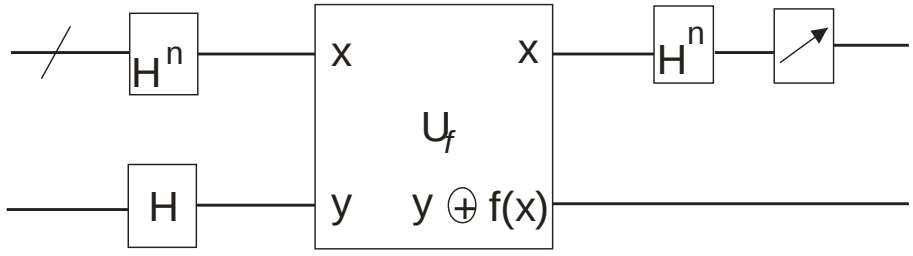
ЗАДАТАК: Задато је пресликавање са скупа од n битова на један бит. Задатак је да се утврди да ли је функција константна, $f(x) = const., \forall x$, или је „балансирана“, тј., да за (приближно) половину могућих улаза даје вредност 0, а за другу половину даје резултат 1.

Формално, пресликавање је $f : \left\{x_1, x_2, ..., x_n\right\} \to \left\{0,1\right\}$, где се скраћено може писати $x \equiv \left\{x_1, x_2, ..., x_n\right\}, x_i = 0,1$.

Физички, јасно је: обрада функције се мора обављати на скупу од макар n кубитова. Дакле, први регистар мора имати макар толико кубитова, док је за други регистар довољно да има један кубит.

Класично, стохастички алгоритми могу дати скраћење од иначе очигледног поступка да се 2^n пута користи класична црна кутија. То скраћење, међутим, није довољно у поређењу са квантним алгоритмом (в. *Nielsen and Chuang 2000*).

Дојч и Јоса предлажу граф (логичко коло) на Сл. 10.12 за овај задатак.



Сл. 10.12 Цртица на првој линији означава да се ради о n кубитова у првом регистру; експонент n означава истовремено обављање Адамарове трансофрмације на свих n кубитова. У другом има само један кубит. На крају се врши одређено мерење на првом регистру.

За рачун нам је потребна следећа једнакост (Задатак 10.4):

$$\hat{H}^{\otimes n}\left|x_1x_2...x_n\right\rangle=\frac{\sum_z(-1)^{x\bullet z}\left|z\right\rangle}{2^{n/2}},\left|z\right\rangle\equiv\left|z_1z_2...z_n\right\rangle,$$

где $x\bullet z=x_1z_1\oplus x_2z_2\oplus...\oplus x_nz_n$, тј., сабирање производа битова по „модулу 2“. За $x=00...0$, наравно, $\hat{H}^{\otimes n}\left|00...0\right\rangle=\frac{\sum_z\left|z\right\rangle}{2^{n/2}}$.

„Сабирање модула 2“ је операција која се за пар битова задаје као „искључиво ИЛИ“: $a\oplus b$ је 0 ако су вредности два бита исте, а 1 у супротном случају. За двобитне стрингове, $a=(a_1,a_2),b=(b_1,b_2)$, множење $a\cdot b\equiv a_1b_1\oplus a_2b_2$, где се појављује обичан производ битова, a_ib_i (без конвенције о сабирању); производ два бита једнак је 1 *акко* су оба бита једнаки 1. Уопштење на вишебитне низове је непосредно, уз правило асоцијативности, нпр.,
$a_1b_1\oplus a_2b_2\oplus a_3b_3\oplus a_4b_4=(a_1b_1\oplus a_2b_2)\oplus a_3b_3\oplus a_4b_4=a_1b_1\oplus(a_2b_2\oplus a_3b_3)\oplus a_4b_4=...$

У пуној аналогији са (10.24) се доказује следећа једнакост:

$$\hat{U}_f\left|x\right\rangle_1\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2-\left|1\right\rangle_2\right)=(-1)^{f(x)}\left|x\right\rangle_1\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2-\left|1\right\rangle_2\right),\qquad(10.30)$$

где се има у виду да је први регистар n-кубитни.

Сада можемо израчунати и коначно стање система 1+2, пре мерења.

$$\left(\hat{H}^{\otimes n}\otimes\hat{I}_2\right)\hat{U}_f\left(\hat{H}^{\otimes n}\otimes\hat{H}_2\right)\left|0\right\rangle_1^{\otimes n}\left|1\right\rangle_2=\left(\hat{H}^{\otimes n}\otimes\hat{I}_2\right)\hat{U}_f\sum_x\frac{\left|x\right\rangle_1}{2^{n/2}}\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2-\left|1\right\rangle_2\right)=$$

$$\left(\hat{H}_1\otimes\hat{I}_2\right)\sum_x\frac{(-1)^{f(x)}\left|x\right\rangle_1}{2^{n/2}}\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2-\left|1\right\rangle_2\right)=\sum_z\sum_x\frac{(-1)^{f(x)+x\bullet z}\left|z\right\rangle_1}{2^n}\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2-\left|1\right\rangle_2\right)\qquad(10.31)$$

Уочити у (10.31): у суми се уз члан $z=0$ налази амплитуда $\sum\frac{(-1)^{f(x)}}{2^n}$; наравно, $\left|z=0\right\rangle_1\equiv\left|0\right\rangle_1^{\otimes n}$.

Сада, ако $f(0)=f(1)$, амплитуда уз $\left|z=0\right\rangle_1\equiv\left|0\right\rangle_1^{\otimes n}$ је ±1. Нужно, тада су све остале амплитуде једнаке нули. Тада се, наравно, (10.31) своди на један члан:

$$|0\rangle_1^{\otimes n}\frac{1}{\sqrt{2}}\left(|0\rangle_2-|1\rangle_2\right). \qquad (10.32)$$

Ако, међутим, $f(0)\neq f(1)$, због претпоставке да је функција „балансирана“, амплитуда уз $|z=0\rangle_1\equiv|0\rangle_1^{\otimes n}$ је једнака нули. Дакле, тада у (10.31) нема члана (10.32).

Ово намеће *идеју* за мерење на првом кубиту које води резултату, *или* $f(0)=f(1)$, *или* $f(0)\neq f(1)$. Наиме, мерењем неке опсервабле на првом регистру чији је својствени базис баш базис израчунавања, постоје само две могућности: *или* вредност која одговара стању (10.32) (што одговара $f(0)=f(1)$), *или* било која друга вредност осим оне која одговара (10.32) (што одговара $f(0)\neq f(1)$). Дакле, да би се појавио резултат $f(0)\neq f(1)$, довољно је да вредност бита за било који кубит првог регистра буде 1. Тиме је задатак решен у *само једној употреби квантне црне кутије*.

Алгоритам гласи:

1. Препарација у стање $|0\rangle_1^{\otimes n}|1\rangle_2$
2. $\xrightarrow{H^{\otimes n}\otimes H_2}\frac{1}{2^{n/2}}\sum_x|x\rangle_1\frac{1}{\sqrt{2}}\left(|0\rangle_2-|1\rangle_2\right)$
3. $\xrightarrow{U_f}\frac{1}{2^{n/2}}\sum_x(-1)^{f(x)}|x\rangle_1\frac{1}{\sqrt{2}}\left(|0\rangle_2-|1\rangle_2\right)$
4. $\xrightarrow{H^{\otimes n}}\frac{1}{2^n}\sum_z\sum_x(-1)^{f(x)+z\bullet x}|x\rangle_1\frac{1}{\sqrt{2}}\left(|0\rangle_2-|1\rangle_2\right)$.
5. Мерење у базису израчунавања првог регистра, $\left\{|x\rangle_1, x=0,1,2\ldots2^n-1\right\}$.

*10.9.4 Сајмонов (*Simon*) алгоритам*

Сајмонов алгоритам (*Simon 1997*) је историјски и методски вишеструко значајан. Прво, то је (поред Дојч-Јосиног) још један формални задатак за који кванти алгоритам даје „експоненцијално убрзање“ у односу на најбољи класични алгоритам. Друго, он показује да, формално мале измене у алгоритму у поређењу са постојећим (нпр., Дојч-Јосиним), омогућују решавање значајно сложенијих задатака. Коначно, Сајмонов алгоритам је нека врста основе за први, прави корисни квантни алгоритам – Шоров алгоритам факторизације великих бројева (видети Одељак 10.9.6).

Сајмонов проблем (којег се тиче алгоритам) указује и на једну значајку, али и неку врсту недостатка, свих квантно-рачунских алгоритама: да би се задатак уопште могао решити, његова поставка мора носити извесна ограничења у погледу функције (пресликавања) која се испитује. Та ограничења („обећања“ програмеру) су већ присутна у горе представљеним алгоритмима. Подсетимо се: у претходним

алгоритмима се гарантује да разматрана функција *има* једну од двеју могућих особина (или константна, или балансирана функција). Без тих „гаранција“ („обећања“), разматрани алгоритми, чини се, не би се ни могли сачинити.

Сајмонов проблем је следећи: задата је нека функција f која пресликава из скупа n битова у скуп n битова – $f:\{0,1\}^n \to \{0,1\}^n$. И за ову функцију постоје „*обећања*“: *постоји* „период“, a, функције, такав да важи $f(x)=f(x\oplus a)$, па је задатак наћи тај период под претпоставком да је једини, тј., *једнозначан*.

Сајмон је сачинио алгоритам који се квантномеханички може сажети следећим изразом:

$$|0\rangle_1|0\rangle_2 \to \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_1|0\rangle_2 \to \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_1|f(x)\rangle_2 \uparrow_2 \frac{1}{\sqrt{2}}\left[|x_0\rangle_1+|x_0\oplus a\rangle_1\right]|f(x_0)\rangle_2 \to$$

$$\to \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}\left[(-1)^{x_0\cdot y}+(-1)^{(x_0\oplus a)\cdot y}\right]|y\rangle_1|f(x_0)\rangle_2 = \frac{1}{2^{(n-1)/2}}\sum_{y:\ a\cdot y=0}(-1)^{x_0\cdot y}|y\rangle_1|f(x_0)\rangle_2 \qquad (10.33)$$

У изразу (10.33): два регистра, сваки од по n кубитова, препариран је у стање $|0\rangle_1|0\rangle_2$; усправна стрелица означава мерење на другом регистру и одговара резултату мерења $f(x_0)$; у прорачуну је коришћена једнакост $(-1)^{(x_0\oplus a)\cdot y}=(-1)^{x_0\cdot y}(-1)^{a\cdot y}$ за производ (у експоненту) „модула 2“, што је операција која, наравно, даје или 0, или 1 као резултат. Детаљно алгоритамско тумачење израза (10.33) је предмет Задатка 10.5.

Десна страна (10.33) садржи суму само по члановима за које $a\cdot y=0$, и то важи за свако y у суми. Отуда је мерењем у базису бројача првог регистра свеједно који ће се резултат (y_i, са истом вероватноћом $2^{n-1}, \forall i$) добити – сваки ће задовољавати исти услов ($a\cdot y_i=0, \forall i$). Понављање истог поступка (сажетог изразом (10.33)) реда величине n пута довољно је за добијање система линеарно независних једначина:

$a\cdot y_1=0$

$a\cdot y_2=0$

.

.

.

$a\cdot y_n=0$

то јест добијање система једначина са нетривијалним решењем (линеарно независним низовима y_i) – што су вредности битова за период a. Дакле, квантни алгоритам користи $O(n)$ коришћења орекла који остварује дато пресликавање f. Најбољи класични алгоритам има још увек експоненцијално много употреба орекла (*Preskill 1998*).

10.9.5 Квантни дискретни Фуријеов трансформ (КДФТ)

Основу корисних алгоритама (в. Одељак 10.9.6) чини, тзв., Квантни Дискретни Фуријеов Трансформ (КДФТ). Ради се о квантном уопштењу класичног дискретног Фуријеовог трансформа.

Вероватно најкориснија класична операција је *дискретни* Фуријеов трансформ (ДФТ). Она се дефинише следећим изразом:

$$x_j \to x_j' = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2i\pi jk/N) x_k \,, \tag{10.34}$$

где су x_i *комплексни бројеви*[7] који представљају компоненте комплексног вектора $x = (x_0, x_1, ..., x_{N-1})$. Израз (10.34) представља, наравно, трансформацију вектора (пресликавање вектора једног у други, $x \to x'$) кроз задате трансформације његових компоненти.

По аналогији се уводи квантни ДФТ (КДФТ):

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2i\pi jk/N) |k\rangle \,, \tag{10.35а}$$

где $\{|j\rangle, j = 0,1,...,N-1\}$ је један ОНБ у простору стања. Наравно, (10.35а) је еквивалентно са:

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} x_k' |k\rangle \,, \tag{10.35б}$$

где се за „амплитуде“ (тј., за константе у развоју по различитим базисима), x_j, x_k', задаје пресликавање (10.35а).

Трансформација (10.35а, б) је ***унитарна***. Доказ (видети и (10.45)):

$$\left|\langle j|j\rangle\right| = \frac{1}{N}\left|\sum_{k,k'} \exp\left(2i\pi j(k-k')/N\right)\langle k|k'\rangle\right| = \frac{1}{N}\left|\sum_{k,k'} \exp\left(2i\pi j(k-k')/N\right)\delta_{kk'}\right| = 1 \,. \tag{10.36}$$

Како само унитарни оператори сачувавају норму вектора у Хилбертовом простору, доказ је завршен. Али отуда постоји и инверзни КДФТ:

$$|k\rangle \to \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp(-2i\pi jk/N) |j\rangle \,. \tag{10.37}$$

[7] Реални бројеви су специјалан случај комплексних бројева.

За систем од n *кубитова,* $N = 2^n$. Тада се израз (10.35) тиче елемената из базиса израчунавања, $\{|i\rangle, i = 0,1,...,2^n - 1\}$. Посебно важан пример је трансформација стања $|0\rangle \equiv \otimes_{i=1}^{n} |0\rangle_i$:

$$|0\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{2^n-1} |k\rangle . \tag{10.38}$$

Задатак је направити квантно логичко коло (орекл) за (10.35). У ту сврху неопходно је увести извесне ознаке дате у раму испод.

Сваком *целом* броју j једнозначно се могу придружити два *биномна* записа:

(1) (***стандардни биномни запис***)

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0 \text{, за } \forall j \in \{0,1,...,2^n - 1\}, \tag{10.39}$$

(2) (***децимални биномни запис***)

$$0.j_l j_{l+1} j_{l+2} ... j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + ... \frac{j_m}{2^{m-l+1}} . \tag{10.40}$$

ПРИМЕР: Број $j = 3$. Нека је $n = 3$. Тада сваки кубит, кроз свој базис израчунавања, $|i\rangle, i = 0,1,$ даје један бит броја $j = 3$. Тада је први запис $j = 3 = (j_1 = 0, j_2 = 1, j_3 = 1) = j_1 2^{3-1} + j_2 2^{3-2} + j_3 2^{3-3} = 0 + 2 + 1 = 3$.
Децимални запис се добија комбинацијом битова $j_i, i = 1,2,3$. На пример, $0.j_1 j_2 \equiv 0.01 = \frac{j_1}{2} + \frac{j_2}{4} = \frac{1}{4}$, а $0.j_1 j_2 j_3 \equiv 0.011 = \frac{j_1}{2} + \frac{j_2}{4} + \frac{j_3}{8} = \frac{3}{8} = \frac{j}{8}$. Уопштење на произвољно n је непосредно.

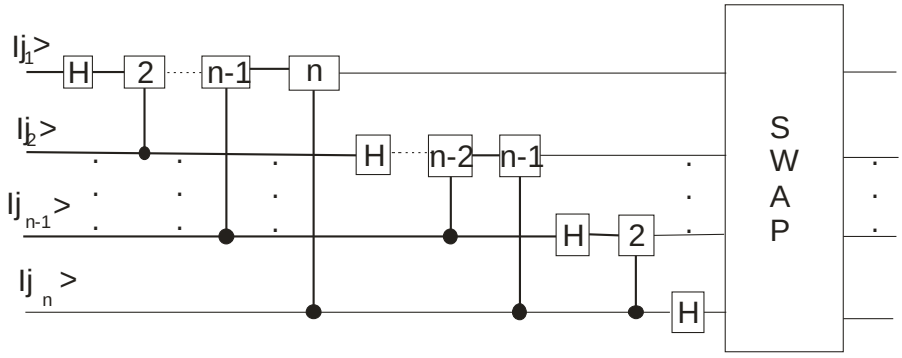
Помоћу записа (10.39) и (10.40) и уз мало пажње, израз (10.35) се може записати у следећем облику:

$$|j\rangle \equiv |j_1 j_2 \dots j_n\rangle \xrightarrow{KDFT}$$
$$\frac{(|0\rangle_n + \exp(2i\pi 0.j_n)|1\rangle_n)(|0\rangle_{n-1} + \exp(2i\pi 0.j_{n-1} j_n)|1\rangle_{n-1}) \dots (|0\rangle_1 + \exp(2i\pi 0.j_1 j_2 \dots j_n)|1\rangle_1)}{2^{n/2}}. \tag{10.41}$$

Израз (10.41) омогућује конструисање логичког кола (орекла - црне кутије) за КДФТ. Ради тога потребно је дефинисати двокубитну унитарну операцију $\hat{R}_k$, која у репрезентацији базиса израчунавања представља операцију дату матрицом:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(2\pi i / 2^k\right) \end{pmatrix}. \tag{10.42}$$

Тада следећи граф представља логичко коло за КДФТ:



Сл. 10.13 Логичко коло са слике имплементира операцију (10.41). Контролисане операције су $C-R_k$, где су двокубитне операције R_k дефинисане изразом (10.42), и индекс k се појављује као број у правоугаоницима – логичким операцијама. Операција *SWAP* обрће редослед вредности кубитова: $SWAP(j_1 j_2 \cdots j_{n-1} j_n) = (j_n j_{n-1} \cdots j_2 j_1)$.

10.9.6 Корисни алгоритми

Дојчов, Дојч-Јоса, па и Сајмонов алгоритам се не тичу корисних рачунских задатака. Они представљају само корисне методске моделе.

Права корист од квантног рачунања тиче се ***класично тешких*** задатака који су ***квантно лаки*** у смислу теорије комплексности, а при томе представљају математичке задатке од ***широке користи***. У овом смислу главни постојећи квантни алгоритам је, тзв., *Шоров квантни алгоритам* факторисања великих бројева (као и израчунавања, тзв., дискретног логаритма). Овај алгоритам даје практично ***експоненцијално убрзање у односу на најбржи класични алгоритам*** факторисања великих бројева. Експоненцијално убрзање у Шоровом алгоритму (***Додатак 10.3***) последица је примене КДФТ .

Овде вреди поменути и Гроверов алгоритам за убрзање претраге „базе података“, који даје $\sqrt{N}$ убрзање у односу на неопходних, класичних, N корака у истој претрази (в. ***Додатак 10.4***).

Отуда се може рећи да се права корист од квантног рачунања тек може очекивати.

10.10 Корекција грешака

Постоје две врсте грешака од интереса, како је већ истакнуто у Одељку 1.4. *Прва врста* тиче се неидеалности операција и/или квантних мерења на систему кубитова. *Друга врста* грешака потиче од утицаја окружења на физичке кубитове на којима се обавља процесирање.

Прва врста грешака је релативно безазлена, јер мале грешке (мала одступања од идеално замишљених операција) воде и малим грешкама у вероватноћама мерења, тј., у коначном резултату рачунања. Ово се може лако доказати. Означимо са $\hat{U}$ жељену, а са $\hat{U}'$ остварену трансформацију, и нека важи $\left|\langle\psi|(\hat{U}-\hat{U}')|\chi\rangle\right| << 1$, за сва нормирана стања $|\psi\rangle, |\chi\rangle$. Тада ће и одговарајуће вероватноће мерења, неке p_n, p'_n, бити приближно једнаке. Наиме, како (Одељак 2.2, израз (П.2)) $p_n = \langle\psi|\hat{U}^{+}\hat{P}_n\hat{U}|\psi\rangle$ и $p'_n = \langle\psi|\hat{U}'^{+}\hat{P}_n\hat{U}'|\psi\rangle$, то се (*уз горњи услов* приближности операција) добија:

$$|p_n - p_n'| = \left|\langle\psi|\hat{U}^{+}\hat{P}_n(\hat{U}-\hat{U}')|\psi\rangle + \langle\psi|(\hat{U}-\hat{U}')^{+}\hat{P}_n\hat{U}|\psi\rangle - \langle\psi|(\hat{U}-\hat{U}')^{+}\hat{P}_n(\hat{U}-\hat{U}')|\psi\rangle\right| \cong$$

$$\left|\langle\psi|\hat{U}^{+}\hat{P}_n(\hat{U}-\hat{U}')|\psi\rangle\right| + \left|\langle\psi|(\hat{U}-\hat{U}')^{+}\hat{P}_n\hat{U}|\psi\rangle\right| = 2\left|\langle\psi|(\hat{U}-\hat{U}')^{+}\hat{P}_n\hat{U}|\psi\rangle\right| \equiv$$

$$2\left|\langle\psi|(\hat{U}-\hat{U}')^{+}\hat{P}_n|\chi\rangle\right| \le 2\left|\langle\psi|(\hat{U}-\hat{U}')^{+}|\chi\rangle\right| << 1$$

(10.43)

Са друге стране, грешке услед утицаја окружења су по правилу неконтролабилне – стохастичке су природе[8]. Методи корекције таквих грешака (*error correction codes*) се заснивају на једноставној идеји: ако се неки бит информације може изгубити услед шума (тј., шум изазива промену стања физичког бита), онда је логично да се уместо једног физичког бита користи скуп[9] физичких битова, како би број битова информације остао сачуван за даље процесирање.

Развијени су и методи квантне корекције грешака. У овом моделу се корекција грешака врши у току поступка рачунања: на систему кубитова се повремено врши одређено квантно мерење, тиме утврди грешка, и коригује се, па се рачунање наставља[10].

Теоријско заснивање поступака поправке грешака, тј., борбе против, тзв., декохеренције, је обимно поље теоријског и практичног истраживања чије представљање захтева значајан простор и представља посебну тему – тзв., *fault tolerant* квантно рачунање – која значајно превазилази овде усвојене оквире представљања основа квантне информатике (за алтернативе методу корекције грешака видети ***Додатак 10.5***).

На крају овог одељка још само истакнимо:

---

[8] Утицај кубитова на окружење се назива декохеренцијом, док се утицај окружења на кубитове назива „квантни шум“ – у оба случаја се губи информација о стању кубитова.

[9] Идеални случај када нема спољашњег шума, наравно, одговара односу: један физички бит за један бит информације.

[10] Процењује се да ће корекција грешака узети до 90% времена рада квантног рачунара, а да ће, опет, у поређењу са класичним, укупна процедура квантног рачунања бити од користи.

Под одређеним *претпоставкама* које се тичу учесталости (и пропагације) *грешака* у хардверу, постоји модел квантног рачунања за који се може рећи да је имун на грешке услед утицаја окружења и који сачувава предности квантног у односу на класично рачунање – тзв., *fault-tolerant* модел рачунања.

10.11 Квантни хардвер

Експериментално изучавање и имплементирање квантних алгоритама се интензивно обавља на различитим физичким основама – различитом квантном хардверу. У оквиру парадигме модела-кола квантног рачунања, основни задаци у дизајнирању квантног хардвера су (*DiVincenzo 2001*):

(А) Дефинисање лако меривих и „контролабилних“ кубитова (једнокубитних унитарних трансформација),
(Б) Лака имплементација $C-NOT$ (наравно, двокубитне) трансформације,
(В) Лако и брзо обављање квантних мерења на скупу кубитова,
(Г) Скалабилност хардвера – што је захтев да увећање броја кубитова (у регистрима) не води драстичним компликацијама у смислу задовољења тачака А-В, као ни нарушењу претпоставки о грешкама у хардверу услед спољашњег шума,
(Д) Могућност непосредног обезбеђивања *додатних кубитова* као простора за рад, који се нити очитавају, нити учествују у утврђивању резултата рачунања (нпр., у поступцима корекције грешака).

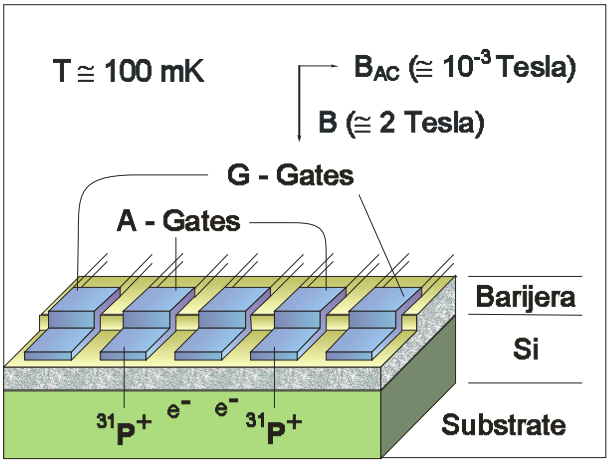
Ови услови и њихова испунљивост се интензивно изучавају на следећим врстама квантног хардвера (видети и ***Додатак 8.1***):

1) фотони (*photons*),
2) атомски и јонски трапови (*atomic, ion traps*),
3) атоми у резонантним електромагнетним пољима у „шупљини“ (*Quantum Electrodynamic Cavity – QED cavities*),
4) квантне тачке (*quantum dots*),
5) Кејнов модел (*Kane's model*),
6) Изменски[11] интерагујући спинови (*exchange interacting spins*), итд.

На Сл. 10.14 представљен је Кејнов предлог (модел) квантног рачунара (*Kane 1998*).

Исцрпно представљање овог дела квантне информатике далеко превазилази оквире уводног курса, а неки извори у овом смислу наведени су на крају овог поглавља.

[11] Тзв., Хајзенбергова интеракција (*Heisenberg*, или *exchange interaction*, у физици чврстог стања) у систему спинова-1/2.



Сл. 10.14 Спинови језгара фосфора-31 су физички кубитови: спинско стање једног језгра представља физички (а без шума и информатички) кубит. Језгра су смештена у ултрачисти *силицијум*, а изнад њих су утиснуте проводне жице које, физичким утицајем на спинове језгара, имплементирају унитарне операције. Манипулација електронима обезбеђује ефективно међуделовање кубитова.

Као и на Сл. 10.14, по правилу, међуделовања у скупу кубитова (којим се успостављају сплетености) се *споља изазивају и контролишу*. Разлог томе је што већина директних физичких интеракција међу кубитовима није згодна за имплементирање потребних унитарних операција на кубитовима.

10.12 Алтернативни модели квантног рачунања

„Модел-кола“ квантно рачунање је само једна парадигма квантног рачунања. Постоје и други модели (парадигме), и у овом тренутку није јасно који од њих – ако иједан – ће и ***практично*** бити користан и остварен.

Пример алтернативе у овом смислу је, тзв., „*Квантно адијабатско рачунање*“ (*Farhi et al 2001, Childs and Farhi 2001*) у којем нема логичких кола и алгоритама који се заснивају на универзалном скупу елементарних операција. Физички, овај модел се заснива на следећој квантномеханичкој идеји: (*адијабатска хипотеза*[12]) квантни систем чији се временски зависан Хамилтонијан *довољно споро мења*, може у сваком тренутку бити у основном стању Хамилтонијана дефинисаног тим тренутком. Испоставља се да таква еволуција стања (нпр., спором променом неког класичног спољашњег поља) квантног система одговара решавању неких рачунски тешких задатака класичне теорије комплексности. Овај модел има читав низ отворених питања везаних за потпуност модела у смислу универзалности, те поступака кориговања грешака, чак ако су и претпоставке адијабатске хипотезе испуњене. Отуда је то још увек непотпун предлог.

[12] Видети, нпр., у *Messiah 1976.*

За разлику од претходне, следећа алтернатива озбиљно конкурише моделу кола квантног рачунања. Ради се о, тзв., „*кластерном*“ квантном рачунању (названог још и: “*one-way*” квантно рачунање *Raussendorf and Briegel 2002*, као и “*measurement-based*” квантно рачунање *Nielsen 2001*), тј., о ингениозном открићу од стране Раусендорфа и Бригела (*Raussendorf and Briegel 2001*). Као и код адијабатског модела, ни овде нема квантних логичких кола која би се сукцесивно примењивала. Ради се о низу међусобно условљених квантних мерења на систему кубитова који је претходно припремљен у високо-сплетено стање. Почетно (високо-сплетено) стање, редослед и избор квантних мерења одређују поступак квантног рачунања. Овај модел је, због мерења, иреверзибилан и има чак и одлике детерминисаности. Уистину има одлике универзалности и врло једноставно репродукује све основне логичке капије које су представљене у Одељку 10. Његова експериментална остварљивост, која је недавно потврђена (*Walther et al 2005,* а псоебно *Lim et al 2006*), могла би водити правом, скалабилном моделу квантног рачунања који би био и економски исплатив.

Закључак овог одељка је очигледан: у овом тренутку није јасно, чак, ни који модел квантног рачунања би се могао испоставити практично користан. Сасвим сигурно, у нарастајућој конкуренцији, главни критеријум у овом смислу биће економска исплативост.

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:

- За детаље у овом Поглављу консултовати књигу *Nielsen and Chuang 2000*, а за ригорознији математички третман *Kitaev et al 2002*. Још једна корисна, општа референца је *Preskill 1998.*
- Изванредан приказ *неизрачунљивих* функција дат је у књизи Пенроуза (*Penrose 1996*).
- Доказ Теорема 10.1 се може наћи, нпр., у књизи *Nielsen and Chuang 2000*.
- Квантни *хардвер* је ваљано представљен у књизи *Nielsen and Chuang 2000*, али брзи развој овог дела области квантне информатике се не може задовољавајуће пратити без претраге путем Интернета, нпр., са упитима “*quantum hardware*”, “(*models of*) *quantum bits (qubits)*” и слично.
- У вези са адијабатским моделом рачунања покренути Интернет претрагу, нпр., под фразом “*adiabatic quantum computation*”.
- У вези са моделом кластерног рачунања покренути претрагу, нпр., под фразом “*cluster quantum computation*”, или “*one-way quantum computation*”, или “*measurement-based quantum computation*”.
- Методи корекције грешака се, на основном нивоу, могу наћи у књизи *Nielsen and Chuang 2000,* као и *Preskill 1998.*

ЗАДАЦИ

10.1 Испитати деловање следећих, „*двонивоских*“, матрица:

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & 0 & \beta \\ 0 & 1 & 0 \\ \gamma & 0 & \delta \end{pmatrix}.$$

Решење:

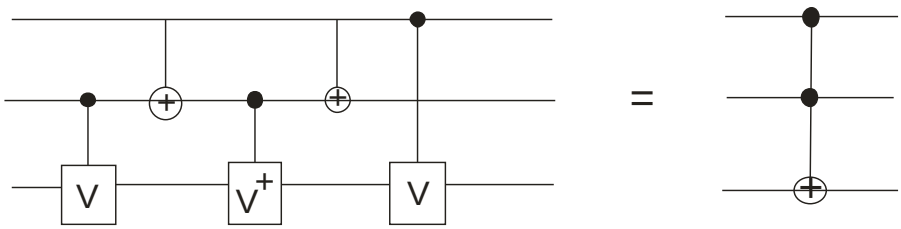
$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} i \\ j \\ k \end{pmatrix} = \begin{pmatrix} ai+bj \\ ci+dj \\ k \end{pmatrix}, \begin{pmatrix} \alpha & 0 & \beta \\ 0 & 1 & 0 \\ \gamma & 0 & \delta \end{pmatrix}\begin{pmatrix} i \\ j \\ k \end{pmatrix} = \begin{pmatrix} \alpha i+\beta k \\ j \\ +\gamma i\delta k \end{pmatrix}. \quad (10a)$$

Уочити непромењеност једне врсте у матрицама-колонама које представљају репрезентације квантних стања. Управо променљивост само две врсте матрице колоне је дефиниција двонивоских матрица.

10.2. Показати да производ две двонивоске матрице не мора бити и сам двонивоска матрица.

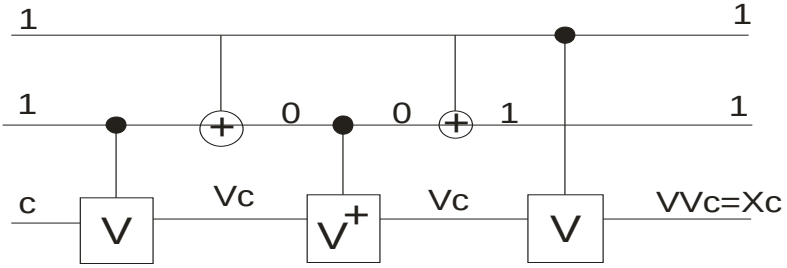
Упутство: помножити двонивоске матрице из претходног задатка и доказати да се не добија двонивоска матрица.

10.3 Доказати једнакост логичких кола на слици:



уз следећу дефиницију једнокубитне операције, $\hat{V} = \frac{(1-i)}{2}\left(\hat{I} - i\hat{X}\right)$. Уочити да коло са десне стране, *делујући на елементе базиса израчунавања*, заправо имплементира Тофолијеву капију (Одељак 1.5 и ***Додатак 1.2***).

Решење: Доказ је дат за један избор почетних вредности кубита (вредности из базиса израчунавања), а све остале комбинације се могу проверити, тј., доказати, на исти начин,



где је коришћено: $\hat{V}\hat{V} = \hat{V}^2 = \hat{X}$. Имајући у виду да за $|c\rangle, c = 0,1$ (базис израчунавања), вредност трећег кубита је: $\hat{X}|c\rangle = |\bar{c}\rangle$, што је у складу са д.с. (дефиниција Тофолијеве капије, Задатак 1.6 у Поглављу I, и ***Додатак 1.2***), где вредност трећег бита износи: $c \oplus 1 \cdot 1 = c \oplus 1 = \bar{c}$.

10.4 Показати ваљаност једнакости:

$\hat{H}^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle$, где је $x \cdot z \equiv x_1 z_1 \oplus x_2 z_2 \ldots \oplus x_n z_n$ и „$\oplus$“ означава сабирање „модула 2“.

Решење: Проверимо прво за један кубит.

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2^{1/2}}\left((-1)^{0\cdot 0}|0\rangle + (-1)^{0\cdot 1}|1\rangle\right),$$
$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2^{1/2}}\left((-1)^{1\cdot 0}|0\rangle + (-1)^{1\cdot 1}|1\rangle\right) \qquad (10б)$$

За два кубита у регистру:

$$\hat{H}_1 \otimes \hat{H}_2 |00\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2 + |1\rangle_2) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle),$$

а на основи једнакости следи

$$\frac{1}{2}\left((-1)^{0\cdot 0\oplus 0\cdot 0}|00\rangle + (-1)^{0\cdot 0\oplus 0\cdot 1}|01\rangle + (-1)^{0\cdot 1\oplus 0\cdot 0}|10\rangle + (-1)^{0\cdot 1\oplus 0\cdot 1}|11\rangle\right) =$$
$$\frac{1}{2}\left((-1)^{0\oplus 0}|00\rangle + (-1)^{0\oplus 0}|01\rangle + (-1)^{0\oplus 0}|10\rangle + (-1)^{0\cdot 1\oplus 0\cdot 1}|11\rangle\right) =$$
$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle);$$
$$\hat{H}_1 \otimes \hat{H}_2 |01\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2 - |1\rangle_2) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle),$$

а на основи једнакости следи

$$\frac{1}{2}\left((-1)^{0\cdot 0\oplus 1\cdot 0}|00\rangle + (-1)^{0\cdot 0\oplus 1\cdot 1}|01\rangle + (-1)^{0\cdot 1\oplus 1\cdot 0}|10\rangle + (-1)^{0\cdot 1\oplus 1\cdot 1}|11\rangle\right) =$$
$$\frac{1}{2}\left((-1)^{0\oplus 0}|00\rangle + (-1)^{0\oplus 1}|01\rangle + (-1)^{0\oplus 0}|10\rangle + (-1)^{0\oplus 1}|11\rangle\right) =$$
$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

и аналогно за све остале комбинације. Уочити да у горњим изразима прво стоји тачан израз, одвојен зарезом од остатка, који је добијен применом једнакости која се доказује.

Мало пажње треба да се уочи да дати израз важи за произвољан број кубитова у регистру.

10.5 У изразу (10.33) растумачити све кораке, тј., водоравне стрелице као унитарне операције. При томе користити резултат претходног задатка, као и општу дефиницију деловања орекла. На основи тога написати алгоритам (по угледу на

алгоритме, корак по корак, за Дојчов или Дојч-Јосин алгоритам), као и нацртати граф – по угледу на Сл. 10.12.

Решење: Користећи резултат Задатка 10.4 и дефиницију деловања орекла (10.30), израз (10.33) заправо одговара следећем алгоритму:

1. Препарација стања $\left|00\right\rangle_{12}$ два регистра, сваки са по n кубитова,

2. $\hat{H}^{\otimes n} \otimes \hat{I}_2$,

3. $\hat{U}_f$,

4. Мерење на 2. регистру, у базису израчунавања,

5. $\hat{H}^{\otimes n} \otimes \hat{I}_2$.

(6. Мерење у базису израчунавања на првом регистру.)

10.6 Доказати да коло са Сл. 10.13 имплементира операцију (10.41).

10.7 На основи Сл. 10.13 конструисати коло које одговара инверзном КДФТ.

XI ИНФОРМАТИЧКА ФОРМУЛАЦИЈА ПРОБЛЕМА КВАНТНОГ МЕРЕЊА

Поступак квантног мерења у квантном информатичком процесирању се, ефективно, користи као *елементарна* логичка операција која, као што је наглашено у Поглављу IV, *доноси класичну информацију*, која је и резултат рачунања. Другим речима: квантно мерење представља „*црну кутију*“ квантне информатике.

За разлику од квантног мерења, егзистенција за све друге „црне кутије“ (Одељак 10.9.1) је гарантована универзалношћу квантног рачунања (Теорем 10.2). При томе, и за разлику од квантног мерења, ове црне кутије су унитарне операције на систему кубитова. Квантно мерење, пак, представља, ефективно, неунитарну (а ефективно и иреверзибилну) трансформацију стања кубита (Одељак 3.8 и 4.3), те се доказ универзалности квантног рачунања нити тиче, ни дотиче „црне кутије квантног мерења“.

Дакле, теорија квантне информатике не доприноси проблему мерења (Одељак 4.3). За ово има више разлога. Прво, неунитарност квантног мерења се не може засновати само на унитарним операцијама (описаним Теоремом 10.2). Друго, механизам процеса мерења се и не поставља као задатак ове теорије: мерење се користи као елементарна операција, напоредо са унитарним операцијама на скупу кубитова. Треће, квантно мерење произвољне опсервабле се може симулирати на квантном рачунару, али (*Nielsen and Chuang 2000*) захтева коришћење самог поступка мерења (на пример, у базису израчунавања). Отуда процес квантног мерења има необичан статус у квантној информатици – статус *„доносиоца одлуке“* (о жељеној информацији о систему), али без познавања механизма процеса мерења, и без могућности да се „доносилац одлуке“ и сам провери, изучи, или опише[1]. Отуда је проблем квантног мерења отворен и у оквирима квантне информатике.

Тако се проблем мерења у оквирима кванте информатике може формулисати на следећи начин:

> *да ли се процес квантног мерења може квантно-информатички описати, али тако да сам процес мерења (неке опсервабле)* не[2] *буде при томе коришћен (у протоколу, или у алгоритму којим се процес мерења описује)?*

Имајући у виду неунитарност процеса мерења (Одељак 3.8 и 4.3 – *Дугић 2004, Wheeler and Zurek 1983, d'Espagnat 1971*), а памтећи универзалност квантног рачунања (Теорем 10.2), *једна могућа стратегија* у разрешавању овог проблема би могла бити следећа. Наиме, чини се да би добар пут у овом смислу могла бити потрага за *новим, фундаменталним законом физике* који лежи у основи иреверзибилности процеса квантног мерења. Формулисање таквог закона би био

---

[1] Ефективно, квантно мерење се овде појављује као нека врста *deus ex machina*.

[2] Коришћење мерења (неке опсервабле) ради симулирања квантног мерења (било које опсервабле), у нашем контексту, била би *circulus viciousus* - логичка (и методска) грешка.

фундаментални научни допринос који би извесно водио преформулацији квантномеханичке, али и теорије квантне информатике. Начин на који би те преформулације биле обављене је нешто о чему се, у овом тренутку, може само спекулирати.

Свеједно, једном формулисан, такав физички закон би представљао физичку динамику коју би ваљало симулирати на (квантном) рачунару. У *овом контексту*, проблем мерења би гласио:

> *да ли процес мерења представља* израчунљив *физички процес, тј., да ли се он може алгоритамски симулирати?*

Занимљиво је спекулирати о могућности да одговор на ово питање буде ***не.*** Како истиче Пенроуз (*Penrose 1996*), а у терминима логичких операција, неизрачунљива операција може бити основа нове врсте рачунања, које нарушава и саму основу познатог теоријског рачунања – Црч-Тјурингову тезу (Одељак 10.3). Као варијација на ову тему, а у смислу дубљег изучавања квантног рачунања, било би занимљиво испитати домете алгоритамског рачунања (које поштује Црч-Тјурингову тезу), али са једном неизрачунљивом операцијом, какво је (по горњој претпоставци) квантно мерење.

Као додатни задатак, у овим контекстима, појављује се задатак давања одговора на следеће питање: зашто (како се чини) не постоји неизрачунљива операција (логичка капија, или орекл) у оквирима класичног рачунања, или, општије, неизрачунљив класично-физички процес[П,3]?

> П: Са чисто физичког становишта, постојање реверзибилног рачунања није изненађујуће.
>
> Сви фундаментални закони квантне физике (па и класичне физике), *са изузетком* закона термодинамике, су реверзибилни. Ово уочавање је у корену проблема „преласка са квантног на класично“ (*Giulini et al 1996, Дугић 2004, Zeh 2007*). Прецизније речено: фундаментални физички закони не подржавају иреверзибилност коју феноменолошки успоставља Други Принцип Термодинамике (ДПТД).
>
> Чини се да се као једини кандидат за (по претпоставци) нови фундаментални закон физике који би имао одлике иреверзибилности појављује процес квантног мерења (*Penorose 1996, Zeh 2007, Giulini et al 1996, Дугић 2004*). А у основи овог процеса би могао бити, тзв., процес декохеренције (горње референце). Отуда би, по претпоставци, процес декохеренције био основа класичности неких физичких система (тј., „класичне информације“), као и феноменолошке иреверзибилности (тј., „стреле времена“ (*Zeh 2007*)). У овом смислу није чудо што (са изузетком процеса које описује ДПТД), у класичној физици нису уочене физичке основе иреверзибилности процеса кје описује ДПТД. Али остаје проблем описа макроскопске иреверзибилности као *последице* једног фундаменталног, микроскопског, иреверзибилносг закона.

Закључимо ове спекулације следећим уочавањем: могућност да квантно мерење буде израчунљив процес (симулабилан на квантном рачунару, и то без употребе било каквог квантног мерења у току симулације) води преформулацији овде уведеног модела-кола квантног рачунања, самом чињеницом да се квантно

[3] Овиме се долази до информатичке поставке проблема, тзв., „преласка са квантног на класично“ (*Giulini et al 1996, Zeh 1999, Дугић 2004*).

мерење (по овој претпоставци) може разложити на једноставније (елементарније) квантно-логичке операције.

Отуда се чини да истраживање на тему информатичког описа квантног мерења не може а да не донесе берићет, како у теоријско-информатичком, тако и у смислу продубљења самих основа квантне механике – у најбољем маниру Ландауерове фразе „*Информација је физичка*“. Ипак, то је само још неуочљива будућност.

XII КВАНТНИ ИНФОРМАТИЧКИ РЕСУРСИ

Коришћење квантних система као хардвера информатичког процесирања отвара неке нове, класично недоступне и неостварљиве могућности. Ова област је још у повоју и прави, зрели резултати се тек очекују. Отуда је за очекивати да ће пуно сагледавање квантноинформатичких ресурса тек добити свој пунији облик. Зато у овом поглављу истичемо основне квантне-информатичке ресурсе.

12.1 Класично непознати ресурси

Физички системи којима се остварују информатички задаци, својим бројем, брзином обављања процесирања, као и енергијом за то неопходном, дефинишу *просторни, временски*, и *енергијски* ресурс информатичког процесирања.

Квантни системи, пак, тј., системи (скупови) кубитова, имају посебне особине корисне за информатичко процесирање. Отуда те особине представљају нове, класично непознате, ресурсе. Једна листа тих, класично непознатих, ресурса је обједињена следећим списком.

(А) ***Неортогоналност квантних стања*** је сама основа успешности криптографског протокола (Одељак 9.3). Подсетимо се: такав информатички учинак (доказиво поуздану размену тајних кључева) *класично*[1] *није могуће обавити.*

(Б) ***Квантна сплетеност*** (*entanglement*) и ***нелокалност*** сама су основа успешности супергустог кодирања (Одељак 9.2), као и представљених квантних алгоритама.

Изучавање информатичких ресурса кроз њихово квантификовање, тј., „мерење“, је основни задатак теоријске информатике – теорија комплексности се само тога заправо и тиче (в. и Одељак 1.5). Када је у питању квантна сплетеност, постоји читава подобласт квантне информатике на тему „мерења“ сплетености. Представљање њених основа далеко превазилази оквире задатка представљања основа квантне информатике, и читалац се упућује на одређену литературу (в. ниже). Напоменимо само да је један део ове области њена подобласт у развоју, тзв., ентанглодинамика (*entanglodynamics*), по угледу на термодинамику. За разлику од термодинамике, у којој је у средишту пажње задатак енергијских ресурса за обављање физичког рада, у ентанглодинамици у средишту пажње су задаци везани за „количину“ сплетености (*entanglementa*) потребних за обављање „информатичког рада“.

Коначно, енергијске потребе за процесирање информацоја су тема за себе, и кратко су представљене у наредном одељку..

[1] Помоћу битова, или, еквивалентно, ортогоналних стања кубитова.

12.2 Енергијски захтеви квантног информатичког процесирања

Енергија неопходна за процесирање информација је *чисто физичка тема*. Један од врхунаца истраживања на ову тему је *Ландауеров принцип* (Одељак 10.2), који успоставља најмањи износ енергије за *брисање* једног бита (класичне) информације – који износи $k_B T \ln 2$. Истовремено, овај принцип је основа уочавања могућности обављања реверзибилног рачунања (када год оно не подразумева потребу за брисањем информације – Одељак 10.2).

Међутим, и реверзибилно процесирање захтева ненулту (макар средњу) почетну енергију битова, тј., физичких система који имплементирају (физички остварују) битове. Ова потреба је прилично интуитивно јасна и илустрована је у Оквиру ниже, а тиче се енергије потребне за промену стања система, тј., за промену вредности битова.

Енергијски ресурс: једна интуитивна опаска

Размотримо кретање једне физичке честице, без преписа у формализам битова – то зависи од конкретног случаја и информатичког задатка који је од интереса.

Промена стања честице, ако је импулс константан, $\left(\vec{r}_1, \vec{p}\right)$, представља физичку основу процесирања информације. Сада, ако се честица нађе у коначном стању $\left(\vec{r}_2, \vec{p}\right)$, иако се њена (овде: укупна) кинетичка енергија, $E = p^2/2m$, не мења, промена стања ће бити бржа уколико је већа брзина, тј., импулс честице – већи импулс, тј. *већа енергија* честице води бржој промени положаја, тј., бржој промени стања честице, а отуда и *бржем процесирању информација*.

У квантном домену, енергијски захтеви се тичу промене *квантних* стања. Тако су од интереса две врсте промена: (а) када су коначно и почетно стање међусобно ортогонални, и (б) када то није случај. За неке од ових случајева се може одредити *доња граница времена* потребног за промену стања, τ, ипак уз извесне суптилности, па и један класично неочекиван резултат.

Прво, може се показати да у случају *ортогоналне* промене стања, случај (а), важи (*Margolus and Levitin 1998*):

$$\tau = \frac{h}{4\left(\left\langle \hat{H} \right\rangle - E_0\right)}, \tag{12.1}$$

где је $\hat{H}$ хамилтонијан (енергија) система, E_0 енергија основног стања (најмања могућа вредност енергије система), док $\left\langle \hat{H} \right\rangle$ представља средњу вредност енергије система у почетном стању. Израз (12.1) потврђује класичну интуицију: већа (овде: средња) енергија честице омогућује бржу промену стања у коначно стање које је ортогонално[2] на почетно.

[2] Па отуда и различиво – Одељак 4.4 – од почетног стања.

Међутим, за једну посебну врсту промене стања типа (б), добија се класично неочекиван резултат.

Наиме, за промену стања која значи *успостављање квантне сплетености*:

$$|\Psi_{почетно}\rangle = |\varphi\rangle_1 \otimes |\chi\rangle_2 = \sum_i C_i |i\rangle_1 \otimes |\chi\rangle_2 \rightarrow |\Psi_{коначно}\rangle = \sum_i C_i |i\rangle_1 \otimes |i\rangle_2 , \qquad (12.2)$$

добија се други израз за минимално време процесирања (*Dugić and Ćirković 2002a*):

$$\tau' \propto \frac{h}{4C(B_1 + B_2)} , \; B_i > 0, \forall i \qquad (12.3)$$

где је C константа („*каплинг константа*“) која одређује јачину интеракције у систему 1+2, а B_i су величине које одређују очекивану вредност Хамилтонијана (енергије) *интеракције*, $\hat{H}_{\text{int}}$. Наиме, ако $\hat{H}_{\text{int}} = C\hat{A}_1 \otimes \hat{B}_2$, таква да опсервабла $\hat{B}_2$ има и позитивне, и негативне својствене вредности[3], тада је почетна средња енергија дата изразом:

$$\langle \Psi_{почетно} | \hat{H} | \Psi_{почетно} \rangle = C_1 \langle \varphi | \hat{A}_1 | \varphi \rangle_1 (B_1 - B_2) . \qquad (12.4)$$

Сада је занимљиво уочити: релативни минимум за τ' – израз (12.3) – одговара једнакости $B_1 = B_2$, а што, с обзиром на (12.4), одговара *нултој почетној (средњој) енергији система*. Наиме, у изразу (12.3) се не појављују други (нпр., кинетички) чланови за енергију, па ни енергија основног стања, E_0 *– време зависи само* од величина које одређују (средњу) вредност *енергије интеракције* два подсистема, 1 и 2.

Дакле, за очекивати је да ће процесирање (12.2) *бити брже* уколико је (релативна[4]) средња вредност[5] интеракције *мања, а најбрже за нулту вредност ове енергије*! Наравно, ово се никако не уклапа у класичну интуицију (в. Оквир у претходном одељку).

ЛИТЕРАТУРА И ДАЉЕ ЧИТАЊЕ:
Сложеност и разноврсност истраживања везаних за сплетеност као ресурс отежава избор мањег броја типичних извора. Читаоцу препоручујемо да на Интернету претражује, нпр., под фразама: *quantum entanglement, quantum resources, entanglodynamics, Bell inequalities*, да поменемо само неке типичне фразе корисне у овом смислу.

- У вези са енергијским ресурсом видети: *Brillouin 1962*; *Landauer1961*; *Margolus and Levitin 1998*; *Dugić and Ćirković, 2002a*.

[3] Типично за скуп (или систем) *кубитова*.

[4] Овде израз „релативна“ указује на произвољност вредности B_i, за које претпостављамо да су једнаке.

[5] Заправо, ради се о апсолутној вредности, $\left|\left\langle \hat{H}_{\text{int}} \right\rangle\right|$, јер за $B_2 > B_1$, $\left\langle \hat{H}_{\text{int}} \right\rangle < 0$.

- У вези са питањем потребности квантне сплетености и нелокалности за постизање надмоћи квантног над класичним рачунањем постоји много референци и отворених питања. Најкраћи начин да се дође до њих је Интернет претрага уз помоћ фраза: „*entanglement + resource*“, „*entanglement + computation*“, „*entanglement + computational + complexity*“.

XIII НЕКИ КУРИОЗИТЕТИ КВАНТНЕ ИНФОРМАЦИЈЕ

Као ни класична, ни „квантна информација“ се не дефинише. Отуда би се могло учинити да би једине разлике између класичне и квантне информације могле бити заправо разлике у ефикасности у процесирању информација.

Све док је ефикасност квантног у поређењу са класичним процесирањем основни мотив за развој области квантне информатике и рачунања, постоје значајне, физичке и формалне разлике двеју информација у неким тачкама које би могле помоћи и у некој врсти дефинисања квантне информације.

Иако се у такво дефинисање овде нећемо упуштати, у овом поглављу циљ нам је да укажемо на неке куриозитете – интуитивне парадоксалности и/или неочекиване особине – квантне информације. Тиме се можда може допринети развоју неке нове, „квантне интуиције“ – у овом тренутку, чини се, тако стране нашој уобичајеној, класичној интуицији.

13.1 Негативна условна ентропија

Класична интуиција успоставља: у сложеном систему $A+B$, природно је очекивати да непознавање подсистема, нпр., подсистема B, не може бити веће од непознавања укупног система $A+B$. У класичној информатици, овај став се може квантификовати Шеноновом ентропијом и на њој изведеним величинама (упореди са Оквиром у Одељку 1.3), каква је, тзв., *условна ентропија*, $H(A|B)=H(A,B)-H(B)$; $H(A,B)$ је ентропија укупног система, а $H(B)$ ентропија подсистема B. Наиме, горња интуиција се формално исказује ненегативношћу условне ентропије, тј., неједнакошћу $H(B)\le H(A,B)$. У квантном контексту, пак, то не мора бити случај.

Фон Најманова ентропија, $S=-tr(\hat{\rho}\ln\hat{\rho})$, је квантни аналогон Шенонове ентропије. На основи ње се уводе све друге мере информације и информатичког процесирања на квантним системима (квантном хардверу). Може се лако показати да условна фон Најманова ентропија може бити *негативна*! То јест, да се о целини (сложеном систему) зна највише што се може знати (у складу са квантним информатичким лимитом, Одељак 4.2), а да се о подсистемима мање зна.

Није, вероватно, изненађење да ово одговара баш ситуацији у којој је сложени систем у чистом стању, и то у сплетеном стању. Тада се лако доказује да је (фон Најманова) ентропија укупног система једнака нули, а да је ентропија било ког подсистема ненулта, што укупно води негативној условној ентропији. Експлицитан доказ реченог је предмет Задатка 13.1. Понекад се квантна информација и дефинише као информација која допушта негативну условну ентропију (*Volovich 2001*).

13.2 Квантни паралелизам: квантне грешке се не морају сабирати

У класичној метрологији, сабирање грешака (при мерењу) је основни постулат. Слично стоје ствари и у класичној информатици – грешке при процесирању се никада не поништавају те су отуда неопходни поступци за отклањање грешака, нпр., у току поступка рачунања.

Међутим, у квантној информатици то не мора бити случај: грешке *услед квантног мерења* се могу поништавати („деструктивно интерферирати“), и то као посебна последица квантног паралелизма.

Пројективна мерења (Одељци 3.2, 7.1) неке опсервабле $\hat{A}_O$ се називају *идеалним*, ако се за систем у својственом стању мерене опсервабле $|n\rangle_O$ добија тачна информација, тј., стање сложеног система „објекат мерења + апарат ($O+A$)“ задовољава једнакост:

$$|n\rangle_O|\chi\rangle_A \xrightarrow{\text{мерење}} |n\rangle_O|\chi_n\rangle_A, \langle\chi_n|\chi_{n'}\rangle = 0, n \neq n' . \qquad (13.1)$$

Како то показују Вигнер (*Wigner 1952*), и Араки и Јанас (*Araki and Yanase 1960*), оваква, идеализована, схема мерења је одржива само за опсервабле које су интеграли кретања – временски независне опсервабле које комутирају са хамилтонијаном система.

Сва реална мерења су неидеална, тј., уместо израза (13.1), у општем случају добија се:

$$|n\rangle_O|\chi\rangle_A \xrightarrow{\text{мерење}} C_1|n\rangle_O|\chi_n\rangle_A + C_2|\eta\rangle_{O+A}, {}_O\langle\chi_n|\chi_{n'}\rangle_O = 0, n \neq n' , \qquad (13.2)$$

где се појављује сплетено стање у сложеном систему. При томе, норма „грешке“, C_2, је утолико мања уколико је мерни апарат „већи“ (*Yanase 1961*), и за макроскопске апарате, та се грешка може и занемарити.

Поступак квантног мерења је незаобилазни део процеса квантног информатичког процесирања. За очекивати је да су „апарати“ који се том приликом користе *мезоскопски* (а не макроскопски) системи, те за њих грешка не мора бити занемарљива. Отуда се намеће задатак изучавања утицаја неидеалности пројективних мерења на квантно информатичко процесирање.

Овај задатак изучен је у *Dugić and Ćirković 2002a*, а као мера ваљаности процесирања (тј., одступања од жељеног стања у процесирању) коришћена је, тзв., *fidelity*, F (нећемо улазити у њено формално дефинисање). Без улажења у детаље, показује се да величина F *– чије смањење* говори о *порасту грешке* – може *порасти* као *последица понављања грешке* у квантном мерењу; поновљено (неидеално) мерење (не нужно исте опсервабле) заправо има „неидеално“ стање (13.2) као почетно. Отуда: понављање грешке услед неидеалности квантног мерења не мора бити деструктивно, тј., *квантне грешке се не морају сабирати*. Усредњена по ансамблу, величина F је једнака нули – у непосредној супротности са усредњењем грешака у класичном мерењу и информатичком процесирању.

Као недвосмислена основа овог неинтуитивног резултата препозната је сплетеност (тј., квантни паралелизам) у сложеном систему $O+A$ (*Dugić and Ćirković 2002a*). Отуда и није чудно што се нешто слично не дешава код класичних физичких и информатичких система.

13.3 Услови информатичке изолованости

Задатак информатичке изолованости једног система од неког другог система, који су оба део веће целине, је у неку руку задатак обрнут свим задацима теоријске информатике: трага се за условима под којима један систем (неки систем A) неће имати информацију о другом систему (о неком систему B).

И у класичном, и у квантном домену то води плаузибилној претпоставци да је потребно „укинути“ међуделовање између система A и B. Иако ови системи (тј., подсистеми неке целине) заправо могу интераговати са неким трећим системом, може се очекивати да би, под неким условима, њихова међусобна неинтеракција могла бити довољна за непреношење информација са система, нпр., B на систем A.

У квантномеханичком контексту, овај задатак се може на први поглед учинити неостваривим – чак ако међусобно и не интерагују, квантни подсистеми могу бити ефективно у интеракцији (индукованој интеракцији) преко неког трећег система (C) са којим оба интерагују. А тада, ефективно, може се очекивати појављивање *сплетености* за ова два подсистема, A и B, тј., појављивање њихове међусобне, ефективне несепарабилности, тј., квантноинформатичке повезаности. Отуда се можда може поверовати интуицији да се у сложеним квантним системима и не мора много водити рачуна о могућности ефективне информатичке изолованости неких подсистема сложеног система (какви су регистри квантних рачунара).

Супротно овом очекивању, овде ће бити указано на постојање, и размотрене три различите врсте информатичке изолованости (локалности) квантних подсистема. *Прва* се тиче *изолованог пара* система A и B који су у међусобној интеракцији. При томе, један од њих (нпр., систем B) нема информацију о другом подсистему, и то важи за сваки тренутак, независно од стања ових система. *Друга* врста се тиче *пара* система *који међуделују* и поступка којим се, *споља* (трећим системом), изазива њихова међусобна, ефективна изолованост у току дугог (али *не* и произвољно дугог) временског интервала; ово „индуковање“ локалности може бити и нежељени, непредвиђени процес у реалном квентном хардверу. *Трећа* врста изолованости се тиче горе описане ситуације: системи A и B међусобно не интерагују, али оба интерагују са неким трећим системом (C) са којим чине изоловану целину. Ниже ће бити размотрене ове врсте изолованости, датим редом.

13.3.1 Адијабатска информатичка изолованост

Размотримо два подсистема, 1 и 2, који међусобно интерагују и као целина представљају изоловани систем (који се описује Шредингеровом једначином). Нека је овај сложени систем (1+2) дефинисан Хамилтонијаном:

$$\hat{H} = \hat{H}_1 + \hat{H}_2 + \hat{H}_{\text{int}}, \tag{13.3}$$

где се појављују сопствени Хамилтонијани ($\hat{H}_i, i = 1,2$) и интеракциони Хамилтонијан који описује њихову међусобну интеракцију, $\hat{H}_{\text{int}}$.

Стандардни је квантномеханички задатак *адијабатског „декупловања“* квантних подсистема, чак и у случајевима у којима су они у међусобној интеракцији, и то независно од стања подсистема.

Ако је подсистем 1 (нпр., електронски систем у молекулу) много мање масе од масе подсистема 2 (нпр., система језгара атома у молекулу), тада се може очекивати следеће. Због релативно велике масе, систем 2 не стиже да прати динамику ситема 1. Са друге стране, систем 1 „види“ стање спорог (инертнијег) система 2 у сваком тренутку и у стању је да му се, „адијабатски“, прилагоди. Отуда се ова интуитивна слика може представити као споро кретање система 2 којем се брзи систем 1 „тренутно“ („адијабатски“) прилагођава.

У квантномеханичком формализму (видети, нпр., *Messiah 1976, Gribov and Mushtakova 2000, Atkins and Friedman 2005*), ова интуиција има и свој прецизни – и даље интуитивно-подобан – израз и облик. Тако, нпр., електрони у молекулу адијабатски прате споро кретање језгара атома који одређују просторну структуру молекула, и то тако да је стање електронског система (систем 1) „тренутно“ одређено стањем језгара (систем 2).

Спори систем 2 (нпр., систем језгара у молекулу), пак, не може да прати кретање брзог система – у молекулима, један „циклус“ спорих језгара је праћен стотинама „циклуса“ брзих електрона. Отуда, од брзог система, спори систем види неко временско и/или ансамбласко *усредњење*, те се динамика спорог система заправо одређује усредњеном динамиком у односу на стање брзог система.

Не улазећи у формализам адијабатске апроксимације, овде ћемо истаћи само основну претпоставку о облику стања сложеног система под адијабатским претпоставкама. Наиме, у нултом нивоу адијабатске апроксимације, сложени систем се тражи у стању облика:

$$\left|\Psi\right\rangle_{12} = \left|\varphi(A_2)\right\rangle_1 \left|\chi\right\rangle_2 + \left|O(\kappa^{3/4})\right\rangle \tag{13.4}$$

где A_2 представља фиксирану вредност неке варијабле $\hat{A}_2$ система 2, која постаје (у адијабатској апроксимацији) *параметар* стања (и динамике) брзог система 1. Мали члан са д.с. (13.4) је одређен параметром $\kappa = m/M$, где је m маса брзог, а M маса спорог подсистема, 1 и 2, редом.

Уочити: у изразу (13.4), сложени систем је приближно у *сепарабилном стању*, у сваком тренутку – сва сплетеност се појављује у малом члану у (13.4). Физички, то одговара *суспрезању сплетености* у сложеном систему, тј., чињеници да је оперативно уочавање последица сплетености мало вероватан догађај, у сваком тренутку.

Подсистем 1 има (параметарски засновану) информацију о подсистему 2, док *обрнуто не стоји*. Отуда се може рећи да је спори систем, адијабатским одсецањем од брзог система, заправо и информатички одсечен од брзог система 1.

13.3.2 Декохеренцијом-индуковано суспрезање декохеренције

Такозвани, декохеренцијом-индуковано суспрезање декохеренције (ДИСД) метод (в. ***Додатак 10.5***, *Dugić 2000*) је оригинално формулисан као поступак за суспрезање декохеренције у квантном хардверу. По свом садржају, овај метод се тиче *међуделујућих* система и тиче се *суспрезања сплетености* међу овим системима – што је заједничко и за адијабатски метод. Са друге стране, он обезбеђује *богатију* информатичку (и физичку) изолованост међуделујућих подсистема, са јединим ограничењем у смислу временског интервала у којем се то може сматрати ваљаним – за разлику од адијабатског модела, овај метод не успоставља изолованост у произвољном тренутку времена.

ДИСД метод разматра трочестични квантни систем $S+B+E$: отворени систем (S) који је у међуделовању са својим окружењем („резервоаром“, „купатилом“, B) и задатак је суспрезање (ослабљење, баш као у адијабатском контексту) слетености, а отуда и, тзв., декохеренције у систему S услед утицаја окружења B. Наравно, претпоставка је да се на овај систем не може применити адијабатска апроксимација.

Метод представља и поступак „инжењерисања купатила“[1], у смислу планираних поступака *над купатилом* B, уз помоћ неког спољашњег, трећег система који се може означити као окружење купатила, E. Претпоставке метода су: окружење E међуделује само са купатилом B, и та интеракција у потпуности доминира динамиком трочестичног система.

Може се показати (*Dugić 2000, 2002c*) да је стање трочестичног система слично по свом облику стању у изразу (13.4), представљено у поједностављеном облику:

$$\left|\Psi\right\rangle_{SBE}=\left|\varphi(t,0_B)\right\rangle\!\!\rangle_S\left|0\right\rangle_B\left|\chi(t)\right\rangle_E+\left|O(|c/C|,t)\right\rangle_{SBE}, \qquad (13.5)$$

где је мали члан са десне стране одређен количником јачина међуделовања c,C између подсистема S и B, тј., B и E, редом. Стање $\left|\chi(t)\right\rangle_E$ носи одређену зависност од стања, а отуда и информације о оба система, S и B, док стање $\left|\varphi(t,0_B)\right\rangle$ носи одређену (параметарску) информацију о стању купатила (*Dugić and*

[1] Енгл.: *Environment engineering.*

Jeknić-Dugić 2009) – баш као у адијабатској локалности. Физички, метод успоставља одређену манипулацију којом се купатило (декохеренцијски-заснованим поступком) присиљава да се у неком тренутку нађе у посебном стању $|0\rangle_B$, тако да се за релативно дуге (али *не и произвољно дуге*) временске интервале, уочавање последица сплетености (присутних у малом члану на д.с. израза (13.5)) може сматрати мало вероватним догађајем. Информатички се појављују два нивоа изолованости. *Први* ниво се тиче изолованости система B од оба подсистема – до на произвољну, горе неистакнуту фазу, његова динамика је „замрзнута" – S и E. *Други* ниво се тиче информатичке одсечености система S од система E (са којим и не међуделује)[2]. При томе, иако систем E може имати информацију о систему S, обрнуто не важи за дужи (али не и произвољно дуги) временски интервал.

13.3.3 Информатичка локалност у трочестичном систему

У трочестичном систему $A+C+B$, само пар (A,B) није у међусобној интеракцији. Поставља се задатак изоловивости система A од система B, која је једносмерна (систему B није забрањено поседовање неке информације о подсистему A), и која важи у сваком тренутку за изоловани сложени систем $A+C+B$.

Општи услови информатичке локалности (изолованости) у овом смислу уведени су од стране Шумахера и Вестморланда (*Schumacher and Westmoreland 2005*). Наиме, ако се један трочестични систем $A+C+B$ као целина може описати унитарном (нпр., Шредингеровом) променом стања, тада *претпоставка* информатичке изоловивости и одсуства интеракције између подсистема A и B има за *последицу* каузалну структуру динамике сложеног система, у смислу да прво међуделују подсистеми A и C, а тек онда подсистеми C и B. Другим речима, под *претпоставком* унитарне динамике сложеног система, ова каузална структура динамике је *потребан услов* информатичке изолованости, тј., прецизније, она *гарантује* одсуство преноса информације са система B на систем A. Обрнуто, пак, не стоји: систем B може имати неку информацију о систему A – дакле, изолованост није двосмерна. Под датим претпоставкама, модел разматран од стране Шумахера и Вестморланда је сасвим општег типа и тиче се многих реалних ситуација у моделу-кола квантног рачунања.

13.3.4 Напомена

Информатичка изолованост није само академска информатичка тема. Поред одређене физичке интуиције (у светлу реченог у ***Додатку 1.1***, физичка и

---

[2] За *произвољно дуг временски интервал* појаве се сплетености, чак, и између подсистема S и E, иако они нису у међусобној интеракцији. Временски интервал за успостављање ове сплетености (тј., корелација стања) је прецизно временски интервал у којем истакнуте локалности имају смисла.

информатичка изолованост су повезаније него што се то уобичајено сматра), она има и сасвим практичних информатичких страна.

На пример, у моделима квантно-рачунарског хардвера[3], већина интеракција међу кубитовима се остварује путем трећег подсистема, који међуделује са оба кубита и тако преноси, тј., успоставља ефективно међуделовање два кубита (в. Одељак 8.2 и Одељак 10.11). У овом смислу се резултати који се тичу информатичке изоловивости појављују као *критеријуми успешности* тих (и свих сличних) поступака.

Отуда горњи примери/модели изолованости нуде и следеће лекције. Прво, типична *временска скала* система који преноси међуделовање не сме бити значајно краћа/дужа од временских скала динамика кубитова (због могуће адијабатичности). Друго, *прејаке локалне интеракције* у трочестичном систему могу условити информатичку изоловивост као у ДИСД схеми. Треће, *каузална схема* трочестичних система представљена у Одељку 13.4.3 може узроковати једносмерну изоловивост појединих делова хардвера (нпр., појединих парова кубитова у регистрима). Ово су, дакле, неки од закључака на које конструктори квантног хардвера морају обратити пажњу, те да би хардвер функционисао онако како је замишљено у теоријским алгоритмима и протоколима.

13.4 Питање „шта је систем“: информатички аспекти

Сваки сложени систем се на различите начине може поделити на подсистеме. Један начин поделе на подсистеме је од непосредног интереса за неке квантноинформатичке протоколе. На пример, у трочестичном систему $1+2+3$ могу се дефинисати различити сложени подсистеми, нпр., $(1+2)+3$, или $1+(2+3)$. Овај начин редефинисања подсистема сложеног система – *прегруписавањем* почетних подсистема – је од интереса у протоколу квантне телепортације, и то за поступак замене сплетености (*entanglement swapping*) – Одељак 9.1. Друга, општија врста редефинисања подсистема има и озбиљније последице.

Истакнимо произвољне *линеарне канонске трансформације*[4] на скупу степени слободе и њима канонски коњугованих импулса (за појмове видети, нпр., *Мушицки 1984*), којима се уводе нови степени слободе и импулси. Тим, новим скупом варијабли, формално се дефинишу и нови подсистеми сложеног система. А у новој дефиницији сложеног система, ствари могу, и физички, и информатички, сасвим другачије стајати (*Dugić and Jeknić 2006, Dugić and Jeknić-Dugić 2008a, Dugić and Jeknić-Dugić 2008b*). Размотримо овде најједноставнији могући сложени систем – водоников атом.

Оригинално, водоников атом (као сложени систем) се дефинише као двочестични систем „електрон + протон (e+p)“. Канонским трансформацијама се уводи *центар маса* атома (CM) и, неизбежно, „релативне координате“, којима се

[3] Видети, нпр., *Nielsen and Chuang 2000*.

[4] Формално тривијалан пример ових трансформација је, горепоменуто, прегруписавање честица.

формално уводи подсистем „*релативна честица*“ (R). Тако је „атом“ подељен на други начин од почетног, а при томе важи: $e+p=$ атом $=CM+R$.

Овај, уобичајени, поступак атомске физике (који формално одговара поступку „сепарације варијабли“, *Хербут 1984*) носи нетривијални информатички садржај.

И квантна стања, и облици Хамилтонијана атома водоника у различитим декомпозицијама на подсистеме су сасвим различитих квантноинформатичких потенцијала.

Кулонова интеракција електрона и протона води сплетености њихових стања, док међусобно неинтераговање центра маса и релативне честице обезбеђује сепарабилно стање за ову декомпозицију атома. Формално, стање атома задовољава једнакост:

$$\sum_i c_i |i\rangle_e |i\rangle_p = |\varphi\rangle_{CM} |nlm_l m_s\rangle_R , \qquad (13.6)$$

где се са д.с. појављују стандардна стационарна стања водониковог атома (одређена добро познатим квантним бројевима n,l,m_l,m_s – в., нпр., *Хербут 1984*) као решења Шредингерове једначине за унутрашње степене слободе – степене слободе система R. У задатку 13.2 ово стање је и прецизније задато. Неинтераговање CM и R има за последицу (Задатак 13.3) да, без спољашњег утицаја (видети за супротно у оквиру ниже), динамика центра маса остаје независна од динамике релативног система, и обратно – тј., стање атома у овој декомпозицији је сепарабилно у сваком тренутку. Наравно, сепарабилна стања су класично-слична (класична физика не познаје сплетеност); а ако се још стања подсистема ограниче на ортонормиране базисе (за сваки фактор-простор стања), тада се процесирање искључиво са овим стањима не може разликовати од класично-информатичког.

Различити облици Хамилтонијана атома успостављају различите трајекторије у простору стања атома (Задатак 13.3), и отуда остварују *различите рачунске процедуре*. У овом смислу, атом није једнозначно дефинисан као квантни рачунар (неуниверзалне сврхе), па ни рачунски потенцијали једног те истог система (атома водоника под датим условима) није једнозначно одређен. Другим речима, различите декомпозиције атома на подсистеме дају сасвим различите потенцијале атома као квантног хардвера, те уочавање/коришћење тих потенцијала зависи искључиво од практичне (оперативне, лабораторијске) приступачности опсервабли различитих подсистема атома. Зато се може рећи да је квантноинформатички потенцијал квантних система *релативна* ствар – све зависи од тога како „посматрамо“ сложени систем – који је дефинисан као скуп подсистема, тј., оперативно, које опсервабле сложеног система су практично доступне.

Различите поделе сложеног система на подсистеме релативизују један од основнх појмова квантне информатике – појам *локалности у дефинисању (под)система* – овај појам је у корену *једно-* или *дво-* кубитних операција Теорема 10.2! Нпр., у водониковом атому: мерења на електрону су локална – уколико то мерење не „додирује“ степене слободе (тј., опсервабле) протона. Али, у терминима

система CM и R, мерења над електроном су сложена – да би се измерио положај електрона потребно је мерити ***нешто*** од положаја ***оба система***, CM *и* R, али не и било шта. Наиме, овакво мерење (тј., мерење положаја електрона) мора бити обављено над системом $CM+R$, али не и над „целим“ системом $CM+R$, који „обухвата“ још и степене слободе протона. Дакле: мерења на електрону су мерења над $CM+R$, али тако да та мерења сачувавају појам локалности – који није очигледан у терминима система $CM+R$; али јесте очигледан у терминима „електрон“ и „протон“. И обрнуто: мерење положаја центра маса атома је мерење над сложеним системом $e+p$, али тако да то мерење не открива релативно растојање ових квантних честица – тј., не открива вредности опсервабле положаја система R. Такво мерење је *локално* у односу на поделу атома као $CM+R$, али се та локалност не види у односу на поделу атома као $e+p$, јер, по аналогији са горњим, ово мерење подразумева мерење *и* на електрону, *и* на протону, али – и то је поента – *не* и мерење *на целом* систему $e+p$; мерење на целом систему $e+p$ је мерење на целом атому, тј., истовремено је и мерење на целом систему $CM+R$ – не заборавимо: $e+p=\text{атом}=CM+R$.

У пракси, чини се, заправо и није увек сасвим јасно која опсервабла и којег подсистема је „непосредно“ мерена. У корену тумачења мерења у овом смислу су наша интуиција и навике, али тумачења поступака не морају увек бити ваљана. Са кубитовима се чини да релативност појма локалности не успоставља нека озбиљнија упозорења, али у општем случају, а посебно у оквирима квантне механике, ова упозорења имају и свој оперативни разлог и смисао.

Квантноинформатичко процесирање на идеалном гасу.

Размотримо идеални гас од N квантних честица. Како показују Задаци 13.2-13.4, на први поглед, такав систем је информатички сиромашан – нема сплетености у систему, а да би се формирала морају се применити спољашњи преносници међуделовања међу честицама гаса. Овај закључак опстаје и у случају примене спољашњег поља на произвољан број честица гаса – за сплетеност (осим ако су честице међусобно идентичне) неопходно је међуделовање у гасу.

Међутим, канонске трансформације (уопштење израза (у зад. 13.2)) потпуно мењају слику и закључке о идеалном гасу.

Наиме, увођење центра маса гаса и релативног система може да понуди сплетеност у новодефинисаним подсистемима. Размотримо најједноставнији случај: примену спољашњег поља само на *једну* честицу гаса – примену неког поља $V\left(\hat{r}_j\right)$ на j-ту честицу гаса. У терминима нове декомпозиције гаса, $CM+R$, ово спољашње поље постаје *интеракциони члан*, јер $\hat{r}_j=\hat{\vec{R}}_{CM}-\sum_m \alpha_{jm}\hat{\rho}_{Rm}$, где индекси CM,R одређују подсистеме атома у декомпозицији $CM+R$. Тако ово спољашње поље за једну декомпозицију (скуп немеђуделујућих честица), постаје интеракција међу подсистемима за другу декомпозицију ($CM+R$), и у тој другој декомпозицији води успостављању сплетености (Задатак 13.4).

Дакле, *неслично стандардним упутствима квантне теорије рачунања*, применом (виртуелно било којег) спољашњег поља на било коју честицу идеалног гаса, погодним избором опсервабли гаса у декомпозицији $CM+R$ може се квантноинформатички користити ресурс којег нуди сплетеност и нелокалност – макар у принципу. У случају $N=2$, овде разматран

поступак је обрнут у односу на стандардни задатак квантномеханичке анализе водониковог атома.

13.5 Осврт

Згодно је на једном месту поређати неке ***особине квантне информације*** које ***немају аналогона*** у класичној информатици и рачунању. Табела ниже то даје као својеврстан пресек садржаја ових основа квантне информатике и квантног рачунања (упоредити са табелом на крају Одељка 8.1).

Квантни ресурси: неодређеност (постојање квантног информатичког лимита)
Квантни ресурси: сплетеност и нелокалност
Квантни ресурси: квантни паралелизам
Забрана клонирања квантних стања = неразличивост неортогоналних стања, *као аспект квантне неодређености*
Негативност условне (фон Нојманове) ентропије, *као аспект квантне сплетенсоти*
Непотребност енергије за формирање квантне сплетености
Деструктивна интерференција грешака (у поновљеним неидеалним мерењима), *као последица квантног паралелизма*
Једно- и дво- кубитна универзалност рачунања
Ефикасни квантни протоколи и алгоритми
Општи наук: информација је физичка

ЗАДАЦИ

13.1 Доказати негативност условне ентропије за сложени систем у чистом, сплетеном стању.

Решење: Условна ентропија дефинисана је изразом $S(A|B)=S(A,B)-S(B)$. Први члан са десне стране представља ентропију сложеног система, док други члан представља ентропију подсистема B. Размотримо произвољно, чисто, сплетено стање $|\psi\rangle_{AB}$ сложеног система $A+B$. Како стоји у изразу (5.17): сваком, једнозначно познатом, чистом стању се придружује нулта (фон Нојманова) ентропија; тј., $S(A,B)=0$. Са друге стране, сходно изразу (5.14а), подсистем B је у мешаном стању (мешавина „друге врсте“), $\hat{\rho}_B = tr_A|\psi\rangle_{AB}\langle\psi|$, за које (израз (5.18)) следи да $S(B)=-tr_B\hat{\rho}_B \ln \hat{\rho}_B > 0$. Отуда непосредно следи: $S(A|B)<0$, у потпуној супротности са класичним аналогоном.

13.2 Дефинисати и анализовати канонске трансформације којима се уводе центар маса и релативна честица атома водоника. Експлицитно записати стања подсистема атома у различитим декомпозицијама, и дати прецизан запис факторисања простора стања атома.

Решење: За атом водоника као двочестични систем ($N = 2$), систем центра маса (CM) и релативни систем (R) се уводе изразима:

$$\hat{\vec{R}}_{CM} = \frac{m_e \hat{\vec{r}}_e + m_p \hat{\vec{r}}_p}{m_e + m_p}, \hat{\vec{\rho}}_R = \hat{\vec{r}}_e - \hat{\vec{r}}_p, \tag{13а}$$

са инверзним релацијама:

$$\hat{\vec{r}}_e = \hat{\vec{R}}_{CM} + \frac{m_p}{m_e + m_p}\hat{\vec{\rho}}_R, \hat{\vec{r}}_p = \hat{\vec{R}}_{CM} - \frac{m_e}{m_e + m_p}\hat{\vec{\rho}}_R, \tag{13а'}$$

где индекси означавају електрон и протон. Стандардна теорија водониковог атома се тиче декомпозиције атома $CM + R$: енергије система R су, прецизно, унутрашње енергије атома за које је феноменолошки уочен (и теоријски утврђен) дискретан спектар вредности. Тако теорија водониковог атома даје сепарабилно стање као на д.с. (13.6), што у координатној рењпрезентацији постаје $\phi(\vec{R}_{CM})\psi_{nlm_l m_s}(\vec{\rho}_R)$. Са друге стране, Кулонова интеракција уводи сплетеност стања електрона и протона. У координатној репрезентацији, систем $e + p$ се налази у стању облика $\sum_i c_i \mu_i(\vec{r}_e)\eta(\vec{r}_p)$. Поента је да, за свако стање атома, Ψ, стоји једнакост (13.6), сада у облику:

$$\sum_i c_i \mu_i(\vec{r}_e)\eta(\vec{r}_p) = \Psi = \phi(\vec{R}_{CM})\psi_{nlm_l m_s}(\vec{\rho}_R), \tag{13б}$$

што је и својеврстан математички запис последица канонских трансформација (13а). Формално, Хилбертов простор стања, H, атома (без спина) се различито факторише за различите декомпозиције, како је и имплицитно у изразима (13.6) и (13б): $H_e \otimes H_p = H = H_{CM} \otimes H_R$. (Уочити да нема много смисла уписивати координатну репрезентацију стању целог атома, Ψ, осим када се зада декомпозиција атома на подсистеме – са леве и десне стране стања Ψ).

13.3 Указати на постојање различитих трајекторија у простору стања атома у току Шредингерове временске еволуције атома као целине.

Решење: Хамилтонијан атома водоника је свакако јединствен оператор, $\hat{H}$, на Хилбертовом простору стања атома водоника. У зависности од дефиниције атома, тј. његове декомпозиције на подсистеме, тај оператор добија различите, добро познате[5], облике:

$$\begin{aligned} \hat{H} &= \hat{T}_e + \hat{T}_p + \hat{V}_{Coul} \\ H &= \hat{T}_{CM} + \hat{H}_R \end{aligned} \tag{13в}$$

где су са $\hat{T}$ означени кинетички чланови (енергије), а $\hat{H}_R = \hat{T}_R - (1/4\pi\varepsilon_0)\left|\hat{\vec{\rho}}_R\right|^{-1}$. Уочити неинтераговање CM и R атома – „сепарација варијабли“. Ово неинтераговање има и важну последицу: унитарни оператор временске еволуције атома као целине, $\hat{U}$, дат изразом:

[5] *Хербут 1984.*

$$\hat{U} = \exp\left(-it\hat{H}/\hbar\right), \tag{13г}$$

у другој декомпозицији се може декомпоновати:

$$\hat{U} = \exp\left(-it\hat{H}/\hbar\right) = \hat{U}_{CM} \otimes \hat{U}_R = \exp\left(-it\hat{H}_{CM}/\hbar\right) \otimes \exp\left(-it\hat{H}_R/\hbar\right). \tag{13д}$$

Тривијалан је задатак доказати да два подсистема, CM и R, међусобно независно еволуирају у времену, и да је стање атома (без спина) у овој декомпозицији увек сепарабилно:

$$\chi\left(\vec{R}_{CM}, t\right)\varphi\left(\vec{\rho}_R, t\right). \tag{13ђ}$$

Сада је из (13ђ) јасно: протицање времена успоставља две независне трајекторије у фактор-просторима стања, H_{CM} и H_R. За пар електрон-протон, те трајекторије су квантно корелисане. Отуда динамика генерисана једним те истим Хамилтонијаном, $\hat{H}$, има сасвим различите физичке трајекторије, а отуда и информатичке путање, тј., садржаје у терминима различитих подсистема једног те истог система – водониковог атома.

13.4 Доказати успостављање сплетености за идеални гас у пољу.

Решење: Идеални гас је скуп неинтерагујућих честица које међусобно нису везане нити једна другој ограничавају кретање. Тако се идеални гас од N честица дефинише скупом вектора положаја тих честица, $\left\{\hat{\vec{r}}_i, i = 1,2,\ldots N\right\}$. Уопштење инверзних канонских трансформација (13а') уводи једнакост $\hat{\vec{r}}_j = \hat{\vec{R}}_{CM} - \sum_m \alpha_{jm}\hat{\vec{\rho}}_m$. Непосредном сменом ове једнакости у израз за спољашње поље једне, нпр., i-те честице гаса, даје:

$$\hat{V} = V\left(\hat{\vec{r}}_j\right) = V\left(\hat{\vec{R}}_{CM} - \sum_m \alpha_{jm}\hat{\vec{\rho}}_m\right) \equiv \hat{H}_{CM+R}. \tag{13е}$$

Ознака на д.с. (13е) има за сврху да истакне да се ради о *интеракционом Хамилтонијану* за декомпозицију гаса као $CM + R$. Непосредан доказ успостављања слетености (за интерагујуће системе) захтева упознавање са неким детаљима квантне механике отворених система и читаоца само упућујемо на литературу, нпр., *Дугић 2004.*

ДОДАЦИ

Додатак 1.1 *Размена сигнала брже од светлости*

„Детерминистички“ сигнали су, по дефиницији, *непрекидни*. Њихова детерминистичност се огледа у физичкој *каузалности* која их одликује: познајући сигнал у једном тренутку могуће је, једнозначно, одредити тај сигнал (по свим његовим карактеристикама) и у било ком каснијем тренутку, и то са вероватноћом 1.

Посебан пример непрекидних сигнала су *пулсни сигнали* (нпр., код „пулсних ласера“). Под „пулсом“ се подразумева нагло, и *врло краткотрајно*, појачање (увећање интензитета) сигнала. Ако се то увећање може предвидети за сваки пулс у низу, унапред, онда се ради о детерминистичком сигналу. Како показују *Brunner et al 2004*, такви сигнали (са, или без, пулсева) се ***могу размењивати и брже од светлости у вакууму***!

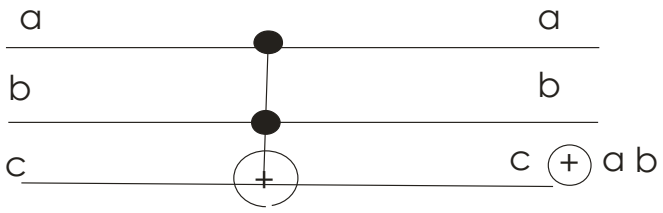
Ако се модулација пулсева обавља тако да се могу остварити „логичко 0“, и „логичко 1“, тада се и они могу размењивати брже од светлости! Али поента је у следећем: ***размена информација***, по дефиницији, ***захтева*** детерминистички ***и*** стохастички, ***независне пулсеве***. Такав низ нула и јединица (тј., пулсева) – који међусобно нису (детерминистички и стохастички) корелисани и/или условљени (а који *једини могу преносити информацију*) – се ***не могу пренети (разменити) брже од светлости***! Другим речима: све док је „групну брзину“ пулса могуће разменити брже од светлости, „брзину информације“ није могуће учинити већом од светлости у вакууму.

Додатак 1.2 *Сводивост класичног реверзибилног рачунања на класично иреверзибилно рачунање*

Такозвана Тофолијева (*Toffoli*) капија, *сама за себе*[1], остварује *универзално* (класично) *реверзибилно* рачунање. На Сл. Д1.2.1 представљена је ова капија и дефинисано њено деловање. Ту се види да је Тофолијева капија реверзибилна. Занемаривањем неких битова, непосредно се остварују реверзибилне капије које оперишу на мањем броју битова од 3. Занимљиво, такве капије немају особину универзалности. Тј., најмањи број битова за универзално реверзибилно рачунање је 3.

Манипулацијом улазима на Тофолијевој капији могуће је остварити све операције из скупова елементарних операција универзалног *иреверзибилног* класичног рачунања. Отуда се овом, једном једином, реверзибилном капијом, могу репродуковати све иреверзибилне капије из модела-кола универзалног иреверзибилног рачунања. Ова операција се може лако физички остварити – в. списак литературе на крају првог поглавља.

[1] Исто важи и за Фредкинову капију – она сама представља „скуп“ (једночлани скуп) елементарних капија универзалног класичног (реверзибилног) рачунања – видети Задатке 1.10 и 1.11, Поглавље I.



Сл. Д1.2.1 Тофолијева капија. Симбол „$\oplus$“ означава операцију ИЛИ; подразумева се обично множење, ab. Уочити једнак број улазних и излазних битова – а ова капија је *сама себи инверзна*[2]*, те је и реверзибилна*.

За фиксиран трећи бит једнак 1, ова капија функционише као операција И („НЕ-И“ – стандардна иреверзибилна капија) за прва два бита. За фиксиране први и трећи бит једнаке 1 и 0, редом, ова капија функционише као операција *FANOUT* – трећи бит постаје једнак другом. Сада, како операције И и *FANOUT* остварују један скуп *елементарних операција универзалног иреверзибилног* рачунања, сама Тофолијева капија се може користити, иако је реверзибилна операција, као универзална капија иреверзибилног класичног рачунања.

Тако је Тофолијева капија основа универзалног, и реверзибилног, и иреверзибилног класичног рачунања. Обезбеђивањем *стохастичности улаза* у Тофолијеву капију остварује се класично *стохастичко* рачунање.

Отуда је Тофојијева капија једночлани скуп елементарних капија универзалног класичног рачунања, било оно реверзибилно, или не, било оно стохастичко, или детерминистичко.

Додатак 2.1 *Операције са матрицама и детерминантама*

Матрица облика $\begin{pmatrix} a \\ b \\ c \\ \dots \end{pmatrix}$ се назива матрицом колоном, а матрица која има једнак број врста (водоравно) и колона (усправно), типа $\begin{pmatrix} \alpha & \beta & \gamma \\ \varepsilon & \phi & \mu \\ \nu & \kappa & \lambda \end{pmatrix}$, се назива квадратном.

Бројеви у матрици су *матрични елементи*. Тако, матрични елемент a_{ij} означава елемент i-те врсте (бројано одозго) и j-те колоне (бројано с лева). Зато се матрице некада и означавају кратко са $\left(a_{ij}\right)$, подразумевајући:

---

[2] Доказ (графички доказ је предмет задатка 1.7): *две примене* ове капије (памтећи да се *прва два бита не мењају*) за *трећи бит* дају резултат $\left(c \oplus ab\right) \oplus ab = c \oplus \left(ab \oplus ab\right) = c \oplus 0 = c$. Тј., $\{a,b,c\} \xrightarrow{\text{две Тофолијеве капије}} \{a,b,c\}$ – што је услов реверзибилности операције.

$$A=\left(a_{ij}\right)=\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}. \qquad \text{(Д2.1.1)}$$

Матрица транспонована матрици (Д2.1.1), у ознаци A^T, добија се заменом елемената, $a_{ij} \leftrightarrow a_{ji}$, што у запису (Д2.1.1) даје матрицу:

$$A^T=\begin{pmatrix} a_{11} & a_{21} & \dots \\ a_{12} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}. \qquad \text{(Д2.1.2)}$$

Адјунгована матрица, A^+, се дефинише као коњугована (у смислу коњуговања комплексних бројева) транспонована матрица, $\left(A^T\right)^*$:

$$A^+=\begin{pmatrix} a_{11}^{\ *} & a_{21}^{\ *} & \dots \\ a_{12}^{\ *} & a_{22}^{\ *} & \dots \\ \dots & \dots & \dots \end{pmatrix}. \qquad \text{(Д2.1.3)}$$

Множење матрица скаларом:

$$\text{(1)}\ \alpha\begin{pmatrix} a \\ b \\ c \\ \dots \end{pmatrix}=\begin{pmatrix} \alpha a \\ \alpha b \\ \alpha c \\ \dots \end{pmatrix} \qquad \text{(Д2.1.4а)}$$

$$\text{(2)}\ \alpha\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}=\begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \dots \\ \alpha a_{21} & \alpha a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}. \qquad \text{(Д2.1.4б)}$$

Сабирање матрица:

$$\text{(1)}\ \begin{pmatrix} a \\ b \\ c \\ \dots \end{pmatrix}+\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \dots \end{pmatrix}=\begin{pmatrix} a+\alpha \\ b+\beta \\ c+\gamma \\ \dots \end{pmatrix} \qquad \text{(Д2.1.5а)}$$

$$\text{(2)}\ \begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}+\begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}=\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix}. \qquad \text{(Д2.1.5б)}$$

Множење матрица:

$$C = AB = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} & \dots \\ b_{21} & b_{22} & b_{23} & \dots \\ b_{31} & b_{32} & b_{33} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} + \dots & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} + \dots & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} + \dots & \dots \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} + \dots & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} + \dots & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} + \dots & \dots \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} + \dots & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} + \dots & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} + \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \quad \text{(Д2.1.6)}$$

$$\equiv \begin{pmatrix} c_{11} & c_{12} & c_{13} & \dots \\ c_{21} & c_{22} & c_{21} & \dots \\ c_{31} & c_{32} & c_{33} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

тј. матрични елементи матрице $C = AB$, c_{ij}, задовољавају једнакост: $c_{ij} = \sum_k a_{ik} b_{kj}$.

Множење матрица-колона (врста) *није дефинисано*, док јесте дефинисано множење матрице-врсте матрицом-колоном:

$$\begin{pmatrix} a & b & \dots \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \dots \end{pmatrix} = a\alpha + b\beta + \dots, \quad \text{(Д2.1.7а)}$$

што је обичан број, није матрица, баш као за елементе матрице C у изразу (Д2.1.6). Са друге стране, множење обрнутим следом даје матрицу:

$$\begin{pmatrix} \alpha \\ \beta \\ \dots \end{pmatrix} \begin{pmatrix} a & b & \dots \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} a & b & \dots \end{pmatrix} \\ \beta \begin{pmatrix} a & b & \dots \end{pmatrix} \\ \dots \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b & \dots \\ \beta a & \beta b & \dots \\ \dots & \dots & \dots \end{pmatrix} \quad \text{(Д2.1.7б)}$$

што у случају једнакости свих елемената, $a = \alpha, b = \beta, \dots$, постаје тзв. *пројектор* (*Додатак 2.2*).

Ако за матрицу важи: $A = A^+$, за њу се каже да је *ермитска* матрица. Ако за њене елементе важи једнакост $\sum_k a^*_{ik} a_{kj} = \delta_{ij}$, тада се за њу каже да је *унутарна*, и тада важи једнакост: $A^+ A = AA^+ = I \Leftrightarrow A^{-1} = A^+$, где се појављује јединична матрица, I:

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots \end{pmatrix}, \quad \text{(Д2.1.9)}$$

и инверзна матрица $\hat{A}^{-1}$, дефинисана изразом: $AA^{-1} = A^{-1}A = I$.

Множење матрица је средишња техника рачунања са матрицама. Зато је упутно ту технику једноставније представити.

$$\begin{pmatrix} \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & a_{i3} & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}\begin{pmatrix} \dots & \dots & b_{1j} & \dots \\ \dots & .. & b_{2j} & \dots \\ \dots & \dots & b_{3j} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}=\begin{pmatrix} \dots & \dots & \dots & \dots \\ \dots & c_{ij} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}, \qquad (Д2.1.8)$$

то јест, множењем i-те врсте матрице A са j-том колоном матрице B, даје c_{ij}-ти елемент матрице $C(=AB)$, $c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+a_{i3}b_{3j}+\dots$, баш као и у (Д2.1.7).

„Двонивоске“ матрице

Израчунавање детерминанте

Детерминанта другог реда (две врсте и две колоне) се дефинише, тј. израчунава по пропису:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}=a_{11}a_{22}-a_{12}a_{21}. \qquad (Д2.1.10)$$

Детерминанта 3. реда израчунава се по обрасцу:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}=\sum_{k=1}^{3}(-1)^{i+k}\,a_{ik}A^{(i)}{}_{k}\,, \qquad (Д2.1.11а)$$

У изразу (Д2.1.11) се не подразумева сабирање по индексу i (који се овде тиче i-те врсте, који се *произвољно бира*, и који је *фиксиран*), док $A^{(i)}{}_{k}$ представљају *поддетерминанте* полазне матрице када се из ње избришу i-та врста и k-та колона, чиме ове поддетерминанте постају другог реда. Уопштење (Д2.1.11) је непосредно: поддетерминанте су увек, за један, нижег реда од полазне детерминанте, и тиме се прорачун своди на коначно израчунавање детерминанте 2. реда. Еквивалентно (Д2.1.11а), вредност детерминанте се може задати преко произвољне колоне:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}=\sum_{k=1}^{3}(-1)^{i+k}\,a_{ki}A^{(i)}{}_{k}\,. \qquad (Д2.1.11б)$$

Тако десна страна (Д2.1.11б) постаје[3], нпр.:

$$-a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{22}\begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} - a_{32}\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}. \qquad (Д2.1.12)$$

Множење детерминанте скаларом

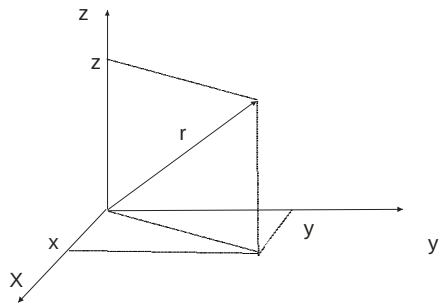
$$\alpha\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} \alpha a_{11} & a_{12} & a_{13} \\ \alpha a_{21} & a_{22} & a_{23} \\ \alpha a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \alpha a_{31} & \alpha a_{32} & \alpha a_{33} \end{vmatrix}, \qquad (Д2.1.13)$$

тј. множење се састоји у множењу свих елемената једне врсте, или једне колоне детерминанте. Детерминанта је једнака нули ако су (видети (Д2.1.11а,б)): елементи једне врсте (или једне колоне) сви једнаки нули, или ако су две врсте (или две колоне) међусобно једнаке.

Додатак 2.2 *Хилбертов простор и оператори на њему*

Под Хилбертовим простором се подразумева, у општем случају бесконачнодимензионални, линеарни, унитарни векторски простор који је сепарабилан, компактан[4] и комплетан, на коме је дефинисана метрика задавањем скаларног производа.

ИДЕЈА: О *векторским просторима* се може мислити по аналогији са обичним, еуклидским тродимензионалним простором обичних вектора, као на Сл. Д2.2.1.



Сл. Д2.2.1 Вектор $\vec{r} = (x, y, z) \equiv (r_x, r_y, r_z)$.

Овај простор чине, нпр., вектори положаја материјалне тачке, којих има непребројиво много (колико и тачака у простору). Линеарни збир два вектора, $a\vec{r} + b\vec{q}$ (где су скалари a, b реални бројеви) је такође вектор у простору – *линеарност* векторског простора.

[3] Овде је детерминанта израчуната преко елемената друге колоне ($i = 2$).

[4] Особине компактности и комплетности су од важности за бесконачнодимензионалне просторе.

Сваки вектор $\vec{r}$ се једнозначно може развити по ортонормираном базису (ОНБ), $\left(\vec{i},\vec{j},\vec{k}\right)$:

$$\vec{r}=r_x\vec{i}+r_y\vec{j}+r_z\vec{k}, \qquad (Д2.2.1)$$

где су координате $r_i, i=x,y,z$, реални бројеви, уз важење *ортонормираности базиса*:

$$\vec{i}\cdot\vec{i}=\vec{j}\cdot\vec{j}=\vec{k}\cdot\vec{k}=1$$
$$\vec{i}\cdot\vec{j}=\vec{i}\cdot\vec{k}=\vec{k}\cdot\vec{j}=0 \qquad (Д2.2.2)$$

где се појављује *скаларни производ*,

$$\left(\vec{r},\vec{q}\right)\equiv\vec{r}\cdot\vec{q}=|\vec{r}|\cdot|\vec{q}|\cdot\cos\angle(\vec{r},\vec{q}) \qquad (Д2.2.3)$$

Други запис десне стране (Д2.3) је: $r_xq_x+r_yq_y+r_zq_z$. Постојање *пребројивог базиса* у простору је особина *сепарабилности* простора. Број вектора (јединичне норме - ортова) у ОНБ је *димензионалност простора*.

Увођење скаларног производа омогућује увођење мере на векторском простору, тј., дужине вектора: $|\vec{r}|=\sqrt{\vec{r}\cdot\vec{r}}=\sqrt{r_x^{\,2}+r_y^{\,2}+r_z^{\,2}}$ - *метрички простор*.

Хилбертов простор H', за који важи: сваки елемент H' је истовремено и елемент H, и постоје елементи простора H који нису елементи H', је *подпростор* простора H, што се пише $H'\subset H$. Два подпростора, H' и H'', такви да важи ортогоналност за све векторе ових подпростора, $\langle x|y\rangle=0,\forall|x\rangle\in H',\forall|y\rangle\in H''$, су међусобно *ортогонални подпростори*.

Елемент x Хилбертовог простора, H, се означава са $|x\rangle$ - *Диракова нотација* (ознаке). Особина *линеарности простора* је представљена изразом:

$$\alpha|x\rangle+\beta|y\rangle\in H,\forall|x\rangle,|y\rangle\in H, \qquad (Д2.2.4)$$

где су константе α,β у општем случају *комплексни бројеви* – особина *унитарности* Хилбертовог простора.

За свака два елемента простора, $|x\rangle,|y\rangle$, уводи се *скаларни производ,* $(x,y)\equiv\langle x|y\rangle$, тако да важи[5]:

(а) $\langle x|y\rangle=\langle y|x\rangle^*$,

(б) $\langle x|x\rangle=\|\|x\rangle\|^2\geq 0$,

(в) $\langle x|x\rangle=0$, акко $|x\rangle=|0\rangle$; нулти вектор се дефинише: $|x\rangle+\alpha|0\rangle=|x\rangle,\forall|x\rangle\in H$ и нулте је норме, $\langle 0|0\rangle=0$; ознака $\|\|x\rangle\|$ представља норму („дужину“) вектора.

[5] У општем случају, скаларни производ је комплексни број; симбол «*» означава комплексно коњуговање.

Ортонормирани базис (ОНБ) представља максимални скуп линеарно независних[6] вектора, $\{|v_i\rangle\}$, где за свака два вектора из овог скупа важи услов ортонормираности:

$$\langle v_i | v_j \rangle = \delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}. \qquad (Д2.2.5)$$

Постојање пребројивог ОНБ је особина *сепарабилности* простора.

Сваки елемент простора се *једнозначно* разлаже по датом ОНБ[7]:

$$|x\rangle = \sum_i \xi_i |v_i\rangle, \xi_i = \langle v_i | x \rangle, \qquad (Д2.2.6а)$$

уз дефинисање *норме вектора*[8]:

$$\| |x\rangle \| = \sqrt{\langle x | x \rangle} = \sqrt{\sum_i |\xi_i|^2}. \qquad (Д2.2.6б)$$

Имајући у виду (Д2.2.6а), скаларни производ два вектора има облик:

$$\langle x | y \rangle = \sum_i \xi_i^* \eta_i, \qquad (Д2.2.7)$$

уз важење разлагања по базису: $|y\rangle = \sum_i \eta_i |v_i\rangle$, уз дефиницију:

$$\langle y | = |y\rangle^+ = \left(\sum_i \mu_i |v_i\rangle \right)^+ = \sum_i \mu^*_i \langle v_i |.$$

Избор једног ОНБ води *репрезентацији* вектора Хилбертовог простора, тј., изоморфизму овог простора са простором матрица-колона:

$$|x\rangle \leftrightarrow \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \dots \end{pmatrix} = \begin{pmatrix} \langle v_1 | x \rangle \\ \langle v_2 | x \rangle \\ \langle v_3 | x \rangle \\ \dots \end{pmatrix} \qquad (Д2.2.8)$$

---

[6] Линеарна независност скупа је дефинисана изразом: $\sum_i \alpha_i |v_i\rangle = 0 \Rightarrow \alpha_i = 0, \forall i$.

«*Максималност*» линеарно независног скупа значи следећи услов: додавање новог елемента (вектора) скупу уводи линеарну зависност тог, новог, скупа.

[7] Тада се каже да ОНБ «развија» простор, и означава се: $H = L\left(\{|v_i\rangle\}, i = 1,2,...,N\right)$, $\dim L = N$.

[8] Доказ да је $\xi_i = \langle v_i | \psi \rangle$: скаларно множење

$$\langle v_j | \psi \rangle = \langle v_i | \left(\sum_i \xi_i | v_j \rangle \right) = \sum_i \xi_i \langle v_j | v_i \rangle = \sum_i \xi_i \delta_{ji} = \xi_1 \delta_{j1} + \xi_2 \delta_{j2} + \xi_3 \delta_{j3} + ... \xi_j \delta_{jj} + ...$$

$$= \xi_1 \cdot 0 + \xi_i \cdot 0 + \xi_i \cdot 0 + ... + \xi_i \cdot 1 + ... = \xi_j$$

Вектор $\langle x| = |x\rangle^+$ се репрезентује матрицом-врстом, која је елемент простора дуалног Хилбертовом простору:

$$\langle x| = \begin{pmatrix} \xi_1^* & \xi_2^* & \xi_3^* & \dots \end{pmatrix}, \tag{Д2.2.9}$$

па се скаларни производ репрезентује производом матрица:

$$\langle x|y\rangle = \begin{pmatrix} \xi_1^* & \xi_2^* & \xi_3^* & \dots \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \dots \end{pmatrix} = \sum_i \xi_i^* \eta_i . \tag{Д2.2.10}$$

Број елемената у ОНБ је *димензионалност простора*, $\dim H$. А ми ћемо надаље имати у виду, пре свега, коначнодимензионалне просторе. Изоморфизам Хилбертовог простора и простора матрица-колона се састоји у једнозначном пресликавању (памтећи одабрани ОНБ репрезентације):

$$\alpha|x\rangle \leftrightarrow \alpha \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \dots \end{pmatrix} = \begin{pmatrix} \alpha\xi_1 \\ \varepsilon\xi_2 \\ \alpha\xi_3 \\ \dots \end{pmatrix} \tag{Д2.2.11а}$$

$$\alpha|x\rangle + \beta|y\rangle \leftrightarrow \alpha \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \dots \end{pmatrix} + \beta \begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \dots \end{pmatrix} = \begin{pmatrix} \alpha\xi_1 + \beta\eta_1 \\ \alpha\xi_2 + \beta\eta_2 \\ \alpha\xi_3 + \beta\eta_3 \\ \dots \end{pmatrix}, \tag{Д2.2.11б}$$

где су примењени прописи множења скаларом, и сабирања матрица, изрази (Д2.1.4а,б).

Оператори на Хилбертовом простору су пресликавања вектора простора, што у ознакама изгледа:

$$\hat{A} : |x\rangle \to |y\rangle, \tag{Д2.2.12}$$

тј.

$$\hat{A}|x\rangle = |y\rangle, \tag{Д2.2.13}$$

За нас су од интереса само *ермитски,* и *унитарни* оператори, за које важи $|x\rangle, |y\rangle \in H$; за $|x\rangle$ се каже да је у *домену оператора* $\hat{A}$ ($|x\rangle \in D(\hat{A})$).

Помоћу скаларног производа се уводи *адјунговани оператор*, $\hat{A}^+$:

$$\left(x, \hat{A}y\right) = \left(\hat{A}^+ x, y\right), \tag{Д2.2.14а}$$

као и

$$\left(x,\hat{A}y\right)^{*}=\left(\hat{A}^{+}y,x\right).\qquad\text{(Д2.2.14б)}$$

У ознакама Диракове нотације, израз (Д2.2.14б) постаје:

$$\langle x|\hat{A}|y\rangle^{*}=\langle y|\hat{A}^{+}|x\rangle.\qquad\text{(Д2.2.15)}$$

Адјунговање збира оператора је по дефиницији операције адјунговања: $\left(\alpha\hat{A}+\beta\hat{B}\right)^{+}=\alpha^{*}\hat{A}^{+}+\beta^{*}\hat{B}^{+}$.

Сада, ако важи:

$$\hat{A}=\hat{A}^{+},\qquad\text{(Д2.2.16)}$$

оператор се назива *ермитским*.

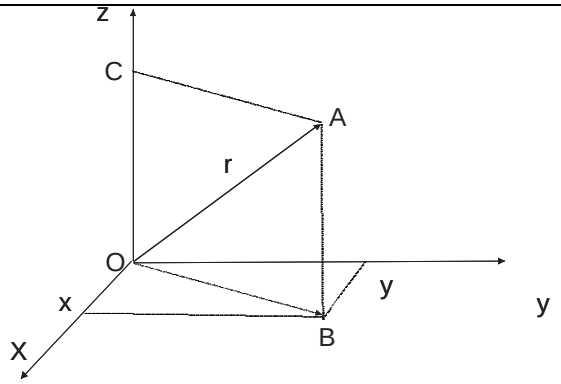
Сваки ермитски оператор задовољава *својствену једнакост*:

$$\hat{A}|a_i\rangle=a_i|a_i\rangle,\qquad\text{(Д2.2.17)}$$

где *реални бројеви* a_i представљају *својствене вредности*, а $|a_i\rangle$ *својствене векторе* оператора $\hat{A}$; скуп својствених вредности, $\{a_i\}$, се назива (дискретним, пребројивим) спектром оператора $\hat{A}$. Ако једној својственој вредности a_n одговара само један својствени вектор, $|a_n\rangle$ ($a_n\leftrightarrow|a_n\rangle$), тада се каже да је a_n *недегенерисана* својствена вредност. У супротном, $a_n\leftrightarrow\left\{|x^{(n)}{}_1\rangle,|x^{(n)}{}_2\rangle,|x^{(n)}{}_3\rangle,...,|x^{(n)}{}_{g_n}\rangle\right\}$, где се број својствених вектора који одговарају својственој вредности a_n, g_n, назива дегенерација својствене вредности a_n.

Посебна врста ермитских оператора су, тзв., *пројектори*, $\hat{P}$. Они пројектују сваки вектор простора у *исти* подпростор; наравно, два пута пројектовано даје исто што и једном пројектован вектор.

ИДЕЈА: На Сл. Д2.2.2 је представљено придруживање вектора $\vec{r}$ и његових *пројекција*, како у XOY-раван, тако и на Z-осу. XOY-раван је један дводимензионални, док је оса Z један једнодимензионални подпростор еуклидовог простора. Ова два подпростора су међусобно ортогонална, а у ортогоналном збиру дају цео еуклидов простор.



Сл. Д2.2.2 Вектор OB је пројекција вектора $\vec{r}$ у XOY раван; вектор OC је пројекција на Z -осу. Ова два вектора су мање дужине од дужине вектора $\vec{r}$, а међусобно су ортогонални – припадају ортогоналним подпросторима, XOY -равни, и Z -оси, редом.

Дуж (вектор) OB је пројекција у равни, а дуж OC је пројекција дуж Z -осе вектора $\vec{r}$. У операторском облику, ово пројектовање одговара операторима, пројекторима: $OB = \hat{P}_{XOY}\vec{r}$, и $OC = \hat{P}_Z\vec{r}$. Наравно, пројектовање OB у XOY раван не мења овај вектор: $\hat{P}_{XOY}OB = OB$, тј. $\hat{P}^2_{XOY} = \hat{P}_{XOY}$; и аналогно за други (сваки) пројектор. У терминима пројектовања, ортогоналност XOY и Z значи: $\hat{P}_{XOY}\vec{\rho} = 0, \forall\vec{\rho} \in Z$, и $\hat{P}_Z\vec{\sigma} = 0, \forall\vec{\sigma} \in XOY$; у терминима пројектора, ортогоналност гласи: $\hat{P}_{XOY}\hat{P}_Z = 0$.

Пројектори имају особину *идемпотентности*, $\hat{P} = \hat{P}^2$, а ако пројектују на ортогоналне подпросторе Хилбертовог простора, тада задовољавају и особину ортогоналности: $\hat{P}_m\hat{P}_n = \delta_{mn}\hat{P}_m$. За *ортогоналне* пројекторе важи и то да је њихов збир, $\hat{P}_m + \hat{P}_n$, такође пројектор (тј. да и за збир пројектора важи особина идемпоитентности[9]). Једнозначно придруживање ортогоналних пројектора и ортогоналних подпростора (на које они пројектују), H_n, дефинише једно ортогонално разлагање Хилбертовог простора, H:

$$H = \oplus_n H_n. \qquad (Д2.2.19)$$

Специјалан ермитски оператор, који је истовремено и пројектор, и унитарни оператор, је тзв. јединични оператор, $\hat{I}$, који не мења ниједан вектор: $\hat{I}|x\rangle = |x\rangle, \forall|x\rangle \in H$. Зато се уз скаларе (тј. обичне бројеве) подразумева идентични оператор, који се обично и не пише: $c \equiv c\hat{I}$.

Сваки ермитски оператор се може једнозначно представити својом спектралном формом, еквивалентном својственој једнакости (Д.2.2.17):

---

[9] $\left(\hat{P}_m + \hat{P}_n\right)^+ = \hat{P}^+_m + \hat{P}^+_n = \hat{P}_m + \hat{P}_n; \left(\hat{P}_m + \hat{P}_n\right)^2 = \hat{P}^2_m + \hat{P}_m\hat{P}_n + \hat{P}_n\hat{P}_m + \hat{P}^2_m = \hat{P}_m + \hat{P}_n$, ако $\hat{P}_m\hat{P}_n = 0$.

$$\hat{A} = \sum_i a_i \hat{P}_i, \qquad \text{(Д2.2.20)}$$

где важи узајамно једнозначно придруживање својствених вредности и својствених пројектора оператора $\hat{A}$: $a_n \leftrightarrow \hat{P}_n$; тада увек важи ортогоналност $\hat{P}_m \hat{P}_n = \delta_{mn} \hat{P}_m$, као и услов „разлагања јединице“:

$$\sum_n \hat{P}_n = \hat{I}\,. \qquad \text{(Д2.2.21)}$$

Ако је a_n недегенерисана својствена вредност, тада њој одговарајући својствени пројектор има облик „дијаде“:

$$\hat{P}_n = |a_n\rangle\langle a_n|, \qquad \text{(Д2.2.22)}$$

а ако се ради о дегенерисаној својственој вредности, тада има облик збира дијада[10]:

$$\hat{P}_n = \sum_{i=1}^{g_n} |x^{(n)}{}_i\rangle\langle x^{(n)}{}_i|\,. \qquad \text{(Д2.2.23)}$$

Из (Д2.2.21) је јасно да јединични оператор, $\hat{I}$, представља пројектор на цео простор H. Отуда, имајући у виду опсервабле чије су све својствене вредности недегенерисане, као и изразе (Д2.2.21) и (Д2.2.22), важи „разлагање јединице“ по својственом базису те опсервабле:

$$\hat{I} = \sum_n |a_n\rangle\langle a_n|\,. \qquad \text{(Д2.2.24)}$$

Сваки оператор се задаје *деловањем на неки ОНБ*:

$$\hat{A}|v_i\rangle = |u_i\rangle = \sum_i a_{ji} |v_j\rangle, \qquad \text{(Д2.2.25)}$$

где матрични елементи, $a_{ji} = \langle v_j | \hat{A} | v_i \rangle$, дају матричну репрезентацију оператора, у датом ОНБ:

$$\hat{A} \leftrightarrow A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{21} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}; \qquad \text{(Д2.2.26)}$$

Уочити да се у *репрезентационој матрици* налазе елементи по распореду *транспонованом* у односу на распоред у изразу (суми) (Д2.2.25). Дакле,

---

[10] Дијада, као пројектор, делује на неки вектор по дефиницији: $\big(|a_n\rangle\langle a_n|\big)|\psi\rangle = |a_n\rangle\big(\langle a_n|\psi\rangle\big) = \langle a_n|\psi\rangle |a_n\rangle$.

репрезентовање оператора у неком ОНБ подразумева транспоновање[11] *„матрице развијања“*, $\left(a_{ji}\right)$, чији се елементи налазе у (Д2.2.25).

Ермитски оператори се репрезентују ермитским матрицама, за које важи: $a_{ij}=a_{ji}^{*}$, док су дијагонални елементи, a_{ii}, реални бројеви.

Збир дијагоналних елемената оператора не зависи од избора репрезентације, тј. ОНБа у којем се оператор репрезентује, и назива се *„трагом“ оператора*, а означава са:

$$tr\hat{A}=\sum_i a_{ii}=\sum_i \langle v_i|\hat{A}|v_i\rangle . \qquad (Д2.2.27)$$

Особине операције трага су:

(а) $tr\left(\lambda\hat{A}\right)=\lambda tr\hat{A}$,

(б) $tr\left(\hat{A}\hat{B}\right)=tr\left(\hat{B}\hat{A}\right)$,

где $\hat{A}\hat{B}$ означава узастопно деловање („множење“) оператора, дефинисано изразом $\hat{A}\hat{B}|x\rangle=\hat{A}\left(\hat{B}|x\rangle\right)$, који указује на редослед деловања оператора. Адјунговање производа оператора дефинисано је изразом: $\left(\hat{A}\hat{B}\right)^{+}=\hat{B}^{+}\hat{A}^{+}$.

Оператор $\hat{A}$ у репрезентацији свог *својственог базиса*, постаје дијагонална матрица:

$$\hat{A}\leftrightarrow\begin{pmatrix} a_1 & 0 & 0 & 0\\ 0 & a_2 & 0 & 0\\ 0 & 0 & a_3 & 0\\ 0 & 0 & 0 & ... \end{pmatrix} \qquad (Д.2.2.28)$$

где се на дијагонали појављују својствене вредности[12] оператора $\hat{A}$. Тако се за јединични оператор, на дијагонали налазе само јединице – јединична матрица. Сада, на основи (Д2.2.27) и (Д2.2.28), може се писати:

$$tr\hat{A}=\sum_i a_i , \qquad (Д2.2.29)$$

што одмах даје и једнакост: $tr\hat{I}=\dim H$.

Згодно је увести скраћено писање:

---

[11] Нека је дато деловање: $\begin{aligned}\hat{A}|1\rangle&=a|1\rangle+b|2\rangle\\ \hat{A}|2\rangle&=c|1\rangle+d|2\rangle\end{aligned}$, Матрица развијања је $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$, а *репрезентациона матрица* оператора је њој транспонована: $\begin{pmatrix} a & c\\ b & d\end{pmatrix}$.

[12] Доказ је једноставан: на основи (Д2.2.17), $a_{ji}=\left\langle a_j\middle|\hat{A}\middle|a_i\right\rangle=\left\langle a_j\middle|a_i\middle|a_i\right\rangle=a_i\left\langle a_j\middle|a_i\right\rangle=a_i\delta_{ij}$, где се *не подразумева* сабирање по индексу i, иако се два пута појављује у производу.

(а) комутатор: $\hat{A}\hat{B}-\hat{B}\hat{A}\equiv\left[\hat{A},\hat{B}\right]$, (Д2.2.30)

(б) антикомутатор: $\hat{A}\hat{B}+\hat{B}\hat{A}\equiv\left\{\hat{A},\hat{B}\right\}$. (Д2.2.31)

На основи (Д2.2.30) јасно је да важи: $\left[\hat{A},\hat{B}\right]=-\left[\hat{B},\hat{A}\right]$. А на основи овога, као и израза (Д2.2.30) и (Д2.2.31), лако је доказати: $\langle x|\left[\hat{A},\hat{B}\right]|x\rangle$ је чисто имагинарни број, док је $\langle x|\left\{\hat{A},\hat{B}\right\}|x\rangle$ реални број.

На основи (Д2.2.26), јасно је да се производ оператора, који је и сам оператор, $\hat{C}=\hat{A}\hat{B}$, репрезентује као производ њихових репрезентационих матрица, $C=AB$; наравно, множење оператора значи множење марица, по правилу (Д2.1.6), тј., у репрезентационој матрици оператора $\hat{C}$ се налазе матрични елементи, c_{ij}, који су облика: $c_{ij}=\sum_k a_{ik}b_{kj}$.

За оператор $\hat{C}$ се лако доказује[13] да је и он ермитски оператор *акко* ермитски оператори $\hat{A}$ и $\hat{B}$ комутирају: $\left[\hat{A},\hat{B}\right]=0$.

Унитарни оператор, $\hat{U}$, дефинисан је изразом:

$$\hat{U}^+=\hat{U}^{-1}\Leftrightarrow\hat{U}\hat{U}^+=\hat{U}^+\hat{U}=\hat{I}, \quad (Д2.2.32)$$

где $\hat{U}^{-1}$ представља оператор инверзан у односу на оператор $\hat{U}$.

Сваки унитарни оператор се може представити у облику:

$$\hat{U}=\exp\left(i\alpha\hat{A}\right), \quad (Д2.2.33)$$

где је α реалан број, а оператор $\hat{A}$ ермитски. Важење спектралног облика (Д2.2.20) повлачи спектралну форму унитарног оператора, за који важи (Д2.2.33):

$$\hat{U}=\sum_n \exp\left(i\alpha a_n\right)\hat{P}_n, \quad (Д2.2.34)$$

што говори да скуп својствених вредности унитарног оператора, $\left\{\exp\left(i\alpha a_n\right)\right\}$, пада на јединичну кружницу у комплексној равни. Из (Д2.2.34) лако се доказује[14]: $\hat{U}^{-1}=\hat{U}^+=\sum_n \exp\left(-i\alpha a_n\right)\hat{P}_n$.

---

[13] Ако ермитски оператори $\hat{A},\hat{B}$ комутирају, тада $\hat{C}^+=\hat{B}^+\hat{A}^+=\hat{B}\hat{A}=\hat{A}\hat{B}=\hat{C}$. Обрнуто, ако је $\hat{C}$ ермитски оператор, тј. $\hat{C}=\hat{C}^+$, тада, како $\hat{C}^+=\hat{B}\hat{A}$, па важи комутативност: $\hat{C}=\hat{A}\hat{B}=\hat{B}\hat{A}=\hat{C}^+$.

[14] $\hat{U}^+=\left(\sum_n \exp\left(i\alpha a_n\right)\hat{P}_n\right)^+=\sum_n \exp\left(-i\alpha a_n\right)\hat{P}_n^+=\sum_n \exp\left(-i\alpha a_n\right)\hat{P}_n$. Сада,

$$\hat{U}\hat{U}^+=\left(\sum_m \exp\left(i\alpha a_m\right)\hat{P}_m\right)\left(\sum_n \exp\left(-i\alpha a_n\right)\hat{P}_n\right)=$$

$$\sum_{m,n}\exp\left(-i\alpha(a_n-a_m)\right)\hat{P}_n\hat{P}_m=\sum_{m,n}\exp\left(-i\alpha(a_n-a_m)\right)\delta_{mn}\hat{P}_n=\sum_n\hat{P}_n=\hat{I}$$

Репрезентациона матрица унитарног оператора је унитарна матрица, $U=(u_{ij})$, чији матрични елементи задовољавају услов ортогоналности:

$$\sum_k u^*_{ik}u_{kj}=\delta_{ij}. \qquad \text{(Д2.2.35)}$$

Израз (Д2.2.35) заправо значи ортогоналност врста (као и ортогоналност колона) унитарне матрице, када се врсте (тј. колоне) третирају као вектори, попут матрица-колона, израз (Д2.2.11а).

Унитарни оператор *сачувава норму* вектора: $|x'\rangle=\hat{U}'|x\rangle$ па $\langle x'|=\langle x|\hat{U}^+$, те $\||x'\rangle\|^2=\langle x'|x'\rangle=\langle x|\hat{U}^+\hat{U}|x\rangle=\langle x|x\rangle=\||x\rangle\|^2$. Штавише, унитарни оператор преводи један ОНБ у други ОНБ: нека $|u_i\rangle=\hat{U}|v_i\rangle,\langle v_i|v_j\rangle\delta_{ij}$; тада важи $\langle u_i|u_j\rangle=\langle v_i|\hat{U}^+\hat{U}|v_j\rangle=\langle v_i|v_j\rangle=\delta_{ij}$. Отуда унитарни оператори представљају везу између различитих (међусобно изоморфних) репрезентација вектора и оператора – *операција сличности* на Хилбертовом простору.

Норма оператора $\hat{A}$, означава се са $\|\hat{A}\|$, дефинише се као супремум: $\|\hat{A}\|=\sup\{\langle\psi|\hat{A}|\psi\rangle,|\psi\rangle\in H\}$. Ако супремум не постоји, такав оператор се назива неограниченим. Сви пројектори су ограничени оператори, а норма унитарног оператора је једнака 1.

Тензорски (директни) производ векторских простора, H_1 и H_2, означава се са $H=H_1\otimes H_2\equiv\otimes_i H_i$, и сам представља Хилбертов простор, ако су простори H_1 и H_2 (који се називају *фактор просторима*) Хилбертови простори.

Један ОНБ у H се може добити тензорским производом елемената базиса из H_1 и H_2, $\{|\varphi_i\rangle_1\},\{|\chi_j\rangle_2\}$, редом:

$$\{|\varphi_i\rangle_1\otimes|\chi_j\rangle_2,\forall i,j\}. \qquad \text{(Д2.2.36а)}$$

Скаларни производ се дефинише на следећи начин:

$$\left({}_1\langle\varphi|\,{}_2\langle\chi|\right)\left(|\psi\rangle_1|\phi\rangle_2\right)={}_1\langle\varphi|\psi\rangle_1\;\;{}_2\langle\chi|\phi\rangle_2. \qquad \text{(Д2.2.36б)}$$

Дакле, сваки елемент простора H, $|\Psi\rangle$, може се једнозначно развити по овом базису:

$$|\Psi\rangle=\sum_{i,j}C_{ij}|\varphi_i\rangle_1|\chi_j\rangle_2,C_{ij}=\left({}_1\langle\varphi_i|\,{}_2\langle\chi_j|\right)|\Psi\rangle, \qquad \text{(Д2.2.37)}$$

где услов нормирања, $\langle\Psi|\Psi\rangle=1$, повлачи услов:

$$\sum_{i,j}|C_{ij}|^2=1. \qquad \text{(Д2.2.38)}$$

Сада се деловање сваког оператора, $\hat{A}$, који делује само на фактор простору H_1, на укупном простору H записује у облику („једночестични оператор“):

$$\hat{A}_1 \otimes \hat{I}_2 , \qquad \text{(Д2.2.39а)}$$

где јединични оператор сугерише немењање вектора у другом фактор простору стања, H_2. Аналогно, „једночестични“ оператор, $\hat{B}$, на другом фактор простору стања, се записује у облику:

$$\hat{I}_1 \otimes \hat{B}_2 . \qquad \text{(Д2.2.39б)}$$

У општем случају, оператори на укупном простору стања су облика:

$$\hat{A}_1 \otimes \hat{B}_2 ; \ \hat{I} = \hat{I}_1 \otimes \hat{I}_2 , \qquad \text{(Д2.2.40)}$$

где $\hat{I}_i$ представља јединични оператор на *i*-ти фактор простор. Деловање оператора на укупном простору се задаје изразом:

$$\hat{A}_1 \otimes \hat{B}_2 |\eta\rangle_1 \otimes |\lambda\rangle_2 = \left(\hat{A}_1 |\eta\rangle_1\right) \otimes \left(\hat{B}_2 |\lambda\rangle_2\right). \qquad \text{(Д2.2.41)}$$

Парцијални траг је операција која значи узимање трага само у једном фактор простору, и означава се са „tr_i“, где индекс i означава о ком фактор простору се ради. Тако, нпр., парцијални траг по фактор простору H_2 неког оператора $\hat{A}$ се дефинише изразом:

$$tr_2 \hat{A} = \sum_i {}_2\langle \chi_i | \hat{A} | \chi_i \rangle_2 , \qquad \text{(Д2.2.42а)}$$

где је $\{|\chi_i\rangle_2\}$ један ОНБ у H_2. Памтећи (Д2.2.40), јасно је да је $tr_2 \hat{A}$ „једночестични оператор“ на фактор простору H_1. Наравно, траг по целом простору се тиче базиса у целом простору H:

$$tr\hat{A} = \sum_{i,j} {}_1\langle \varphi_i | \otimes {}_2\langle \chi_j | \hat{A} | \varphi_i \rangle_1 \otimes |\chi_j\rangle_2 , \qquad \text{(Д2.2.42б)}$$

што је број једнак збиру својствених вредности оператора $\hat{A}$.

Парцијални скаларни производ представља операцију скаларног производа елемента простора H са неким елементом фактор простора, нпр фактор простора H_1:

$${}_1\langle \xi | \Psi \rangle = \sum_{i,j} C_{ij} \, {}_1\langle \xi | \varphi_i \rangle_1 \cdot |\chi_j\rangle_2 , \qquad \text{(Д2.2.43)}$$

што је елемент фактор простора H_2 : $\sum_j \alpha_j |\chi_j\rangle_2$, где $\alpha_j \equiv \sum_i C_{ij} \, {}_1\langle \xi | \varphi_i \rangle_1$.

У матричној репрезентацији вектора и оператора, тензорски производ се уводи на следећи начин:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \dots \end{pmatrix} \otimes \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ \dots \end{pmatrix} = \begin{pmatrix} c_1 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ \dots \end{pmatrix} \\ c_2 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ \dots \end{pmatrix} \\ c_3 \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ \dots \end{pmatrix} \\ \dots \end{pmatrix} \qquad \text{(Д2.2.44)}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \\ \dots & \dots & \dots \end{pmatrix} = \begin{pmatrix} a_{11} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \\ \dots & \dots & \dots \end{pmatrix} & a_{12} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \\ \dots & \dots & \dots \end{pmatrix} & \dots \\ a_{21} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \\ \dots & \dots & \dots \end{pmatrix} & a_{22} \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & b_{22} & \\ \dots & \dots & \dots \end{pmatrix} & \dots \\ \dots & \dots & \dots \\ & & \end{pmatrix} \qquad \text{(Д2.2.45)}$$

где се са десне стране подразумева множење матрице константом, изрази (Д2.1.4а,б).

НАПОМЕНЕ:

- два вектора, $|x\rangle, |y\rangle$, за које важи $\langle x|y\rangle \neq 0$, се називају *неортогоналним*.
- два пројектора, $\hat{P}_m, \hat{P}_n$, за која $\hat{P}_m \hat{P}_n \neq \delta_{mn} \hat{P}_m$, називају се *неортогоналним*, и пројектују на *неортогоналне подпросторе*.
- вектор $|x\rangle$ који није нормиран, *нормира* се по рецепту: $\frac{1}{\||x\rangle\|}|x\rangle$.
- *репрезентовање* стања и оператора обично подразумева узимање *својственог базиса неког ермитског оператора* као базиса репрезентације. Отуда и репрезентација носи назив, нпр., $\hat{A}$-репрезентација.

Додатак 2.3 *Релације неодређености: коментари*

Само у случају да је комутатор две опсервабле умножак јединичног оператора, $\left[\hat{A},\hat{B}\right]=c\hat{I}$, стоји често, иначе некритички, коришћен став: „што је прецизније позната вредност једне опсервабле, нпр., опсервабле $\hat{A}$, утолико је мање позната вредност друге опсервабле, $\hat{B}$ (тј., веће је $\Delta\hat{B}$)“. У општем случају, вредност комутатора *зависи од стања*, баш као и стандардна одступања опсервабли – тј., није константа.

Ради провере конзистентности релација неодређености, овде су дати следећи специјални случајеви.

(1) $\left[\hat{A},\hat{B}\right]\neq 0$, али постоји заједничко својствено стање ових опсервабли. Проверимо ваљаност релације неодређености за овај случај. Прво, стандардна одступања обеју опсервабли у заједничком својственом стању је тачно нула, $\Delta\hat{A}=0=\Delta\hat{B}$. Међутим, на десној страни израза (2.9) се налази: $\langle\varphi|\left[\hat{A},\hat{B}\right]|\varphi\rangle=\langle\varphi|\left(\hat{A}\hat{B}-\hat{B}\hat{A}\right)|\varphi\rangle=\langle\varphi|\left(\hat{A}b-\hat{B}a\right)|\varphi\rangle=\langle\varphi|(ab-ba)|\varphi\rangle=0$, па је задовољена једнакост у изразу (2.9).

(2) $\left[\hat{A},\hat{B}\right]\neq 0$, али је ансамбл у својственом стању, нпр., опсервабле $\hat{A}$. Тада је $\Delta\hat{A}=0$, док $\Delta\hat{B}\neq 0$. Дакле, лева страна (2.9) је опет једнака нули. Сада, $\langle\varphi|\left(\hat{A}\hat{B}-\hat{B}\hat{A}\right)|\varphi\rangle=\langle\varphi|\left(a\hat{B}-\hat{B}a\right)|\varphi\rangle=0$, јер из $\hat{A}|\varphi\rangle=a|\varphi\rangle$ следи $\langle\varphi|\hat{A}=\langle\varphi|a$. И све аналогно за обрнути случај: стање је својствено за $\hat{B}$, али није својствено за опсерваблу $\hat{A}$.

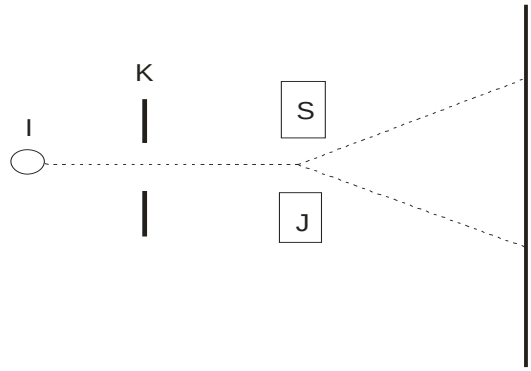
(3) $\left[\hat{A},\hat{B}\right]=0$, али стање није својствено за макар једну од ових двеју опсервабли; нпр. стање је $|\psi\rangle=\alpha|\varphi\rangle+\beta|\chi\rangle$ и својствено је за $\hat{A}$, али важи $\hat{B}|\varphi\rangle=b|\varphi\rangle$, док $\hat{B}|\chi\rangle=b'|\varphi\rangle$, за $b\neq b'$ – тј. стања $|\varphi\rangle,|\chi\rangle$ не припадају заједничком својственом базису ових опсервабли. Важење једнакости у (2.9) се доказује у пуној аналогији са горњим случајем (2).

Додатак 2.4 *Штерн-Герлахов експеримент*

Експериментална ситуација: сноп атома (нпр. сребра) се пропушта кроз врло јако и врло нехомогено магнетно поље. На екрану иза магнета (гледано у односу на извор атома) хватају се атоми и уочавају се два оштра, међусобно непресецајућа трага упада атома. У духу класичне физике, закључак[15] се сам намеће: услед дејства магнетног поља, упадни (колимисани) сноп атома се цепа на два снопа, тако да сваки атом има приближно добро дефинисану путању, као на

[15] Физички нетачан закључак! Испоставља се (*Dugić, Arsenijević, Jeknić-Dugić 2009*) да појединачни атоми немају путању. Појављивање трагова на застору је последица *утицаја застора на атоме* – што овде неће бити од важности, те неће ни бити наглашено у тексту.

Сл. Д2.2.1. Наравно, нужно, тада сваки појединачни атом представља неки магнетни дипол, $\vec{\mu}$, који „осећа“ спољашње магнетно поље индукције $\vec{B}$.



Сл. Д2.4.1 Илустрација Штерн-Герлаховог експеримента. *I*-означава извор, *K*-колиматор снопа атома, *S,J*-северни и јужни пол (сталног, јаког, нехомогеног) магнета, а са десне стране је екран који захвата упадне атоме – испрекидане цртице одговарају замишљеним путањама атома до јасних (непресецајућих) трагова на екрану.

У потрази за физичким пореклом $\vec{\mu}$, природно је поћи од класичне слике: валентни (једини у задњој „љусци“ атома) електрон има одређену орбиту којој се може придружити момент импулса $\vec{l}$. Како је електрон наелектрисан (наелектрисања e, m – маса електрона, а c – брзина светлости у вакууму), то *ово орбитирање представља магнетни дипол,* $\vec{\mu} = g\mu_B \hat{l} \equiv g\frac{e}{mc}\hat{l}$; g је константа која се феноменолошки одређује.

Класична слика овог модела, међутим, казује: интеракција овог дипола са спољашњим магнетним пољем даје *онолико путања електрона* иза магнета, а отуда и онолико трагова на екрану, *колико има вредности за момент импулса,* $|\vec{l}|$. Тако, *чисто класично*, путања иза магнета би било непребројиво много, а отуда и *непребројиво много трагова на застору* – уместо само два оштра, просторно раздвојена трага.

Са друге стране, *квантна теорија* момента импулса (Хербут 1984) уводи *непаран* број вредности импулса иза магнета, па би отуда и *број трагова на екрану морао нити непаран*.

Тако се мора закључити: *коришћење само степени слободе* x, y, z, који дефинишу момент импулса ($\vec{l} = \vec{r} \times \vec{p} = \sum_{i,j,k} \varepsilon_{ijk}\, \vec{e}_i\, x_j\, p_k$), није довољно за објашњење и опис ефекта, тј., добијање *само два трага на екрану*.

Додатак 8.1 *Модели кубита*

ДЕФ. 8.1 уводи ***модел кубита***. То значи да кубит не треба буквално схватити као простор стања спина-1/2. Физички, по својој природи, кубит може бити било који квантни систем чији дводимензионални (ефективни) простор стања

се може довољно добро контролисати тако да ***у току операција на том простору стање система никада не излази изван тог дводимензионалног простора***.

У формализму, ако је базис израчунавања, $\{|0\rangle,|1\rangle\}$, дефинисан, тада је кубит заправо (под)простор (или ефективни простор) стања који се развија над овим базисом[16]:

$$\text{kubit}=L(|0\rangle,|1\rangle) \qquad \text{(Д8.1.1)}$$

то јест,

$$\forall|\psi\rangle\in\text{kubit}:|\psi\rangle=a|0\rangle+b|1\rangle,\langle\psi|\psi\rangle=1. \qquad \text{(Д8.1.2)}$$

Сада се, уз помоћ овог базиса (у Поглављу 10 названог базисом израчунавања за један кубит) могу *изградити опсервабле (10.4)*:

$$\begin{aligned}\hat{\sigma}_z&=|0\rangle\langle 0|-|1\rangle\langle 1|\\ \hat{\sigma}_x&=|0\rangle\langle 1|+|1\rangle\langle 0|\\ \hat{\sigma}_y&=i|1\rangle\langle 0|-i|0\rangle\langle 1|\end{aligned}\quad , \qquad \text{(Д8.1.3)}$$

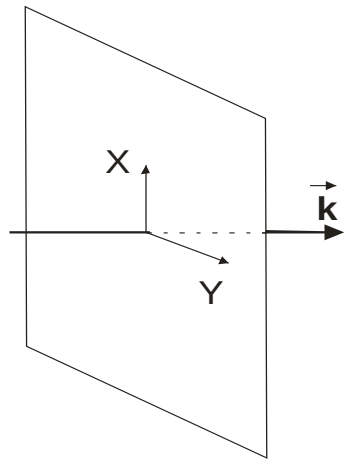
тј., формално Паулијеви сигма-оператори. ***Наравно***, то опет не значи да се буквално ради о операторима спина-1/2. Ако су још и дефинисани поступци мерења ових опсервабли, кажемо да ***имамо модел кубита***.

НЕКИ ПРИМЕРИ:

(1) *Ефективни спин фотона*

У електродинамици је познато да *спин фотона*, који се тиче векторског потенцијала ЕМ поља, има *само две линеарно независне компоненте*, као на Сл. Д8.1.1. Ово је последица Кулоновог калибрационог услова, $div\vec{A}=0$, која у Фуријеовом трансформу има облик $\vec{k}\cdot\vec{A}=0$. Отуда се спин (тј. *поларизација*) фотона као вектор налази у равни управној на вектор $\vec{k}$ - правац овог вектора одговара правцу простирања ЕМ таласа.

[16] Ознака $L(|0\rangle,|1\rangle)$ је објашњена у ***Додатку 2.2***, у вези са изразом (Д2.2.5).



Сл. Д8.1.1 Правац вектора $\mathbf{k}$ - таласни вектор – је правац простирања ЕМ таласа (квантно: фотона). Раван управна на овај вектор је раван поларизације светлости (фотона). А раван је дводимензионална – само два вектора у равни (нпр., дуж оса X и Y) могу бити линеарно независни; наравно то су међусобно ортогонални вектори.

Квантномеханички, ова ситуација се мора поштовати. Али, тада се може дефинисати кубит који се физички тиче *поларизације* фотона. Наиме, како су пројекције A_x и A_y међусобно ортогоналне, ове *физичке поларизације* (стања ЕМ поља) се *квантномеханички могу моделовати* у складу са прескрипцијом:

$$A_x \leftrightarrow |0\rangle, A_y \leftrightarrow |1\rangle, \qquad (Д8.1.4)$$

чиме је дефинисан базис израчунавања. Сада је јасно: све линеарне суперпозиције стања (Д8.1.4) леже (физички) у равни на Сл. Д8.1 и представљају (одређују) поларизацију фотона (ЕМ поље у квантном третману). Међутим, оне истовремено представљају модел кубита у складу са горе реченим, (Д8.1.1)-(Д8.1.3).

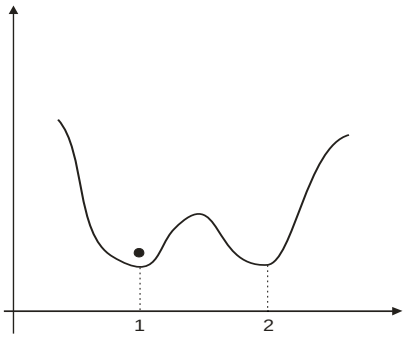
(2) *Ридбергова стања атома*

Посебна стања атома (нпр., рубидијума, или цезијума), основно стање $|g\rangle$ и посебно одабрано побуђено стање $|e\rangle$, имају следећу особину: постоје услови (спољашње ЕМ поље, нпр., ласера) под којима стање атома (тј., електрона у атому) увек може (са занемарљивом грешком) бити представљено као суперпозиција ових стања, типа (Д8.1.2). Дакле, вештим манипулацијама над појединачним атомима, стање је увек у (ефективном) дводимензионалном простору (Д8.1.1), што је модел кубита.

(3) *Квантне тачке*

У чврстој, кристалној структури (нпр., силицијума) могуће је просторно конфинирање квантних честица, нпр., електрона. Посебна врста конфинирања представљена је Сл. Д8.2, на којој локални минимуми, *1* и *2*, одговарају добро

дефинисаним *просторним положајима* (стањима) електрона у чврстој структури. Ова два положаја су међусобно различива (у смислу Одељка 4.4), а спољашњим манипулацијама (нпр., електричним пољем) се честица може пребацивати из једног у други положај, као и остварити интерференција (линеарна суперпозиција) ових положаја – тада је положај квантно неодређен. При томе, поља се тако модулирају да квантна честица никада не напусти дати део кристала – између (приближно) два положаја *1* и *2*, као на Сл. Д8.1.2. Ово се у физици чврстог стања зове *квантном тачком*.



Сл. Д8.1.2 Уочити два локална минимума потенцијала $V(x)$, исте дубине. Облик потенцијала јасно говори да квантна честица (представљена, семикласично, црном тачком) не може сама да напусти област приближно одређену положајима 1 (лево) и 2 (десно) – честица је просторно конфинирана – осим путем тунеловања, или спољашњим утицајем.

Различивост положаја сада оправдава *квантномеханички модел* квантне тачке:

$$1 \leftrightarrow |0\rangle,\ 2 \leftrightarrow |1\rangle, \qquad \text{(Д8.1.5)}$$

док интерференција ових положаја одговара линеарним суперпозицијама стања. Контролабилност стања (Д8.1.5) оправдава овај модел као модел кубита.

(4) *Стања ЕМ шупљине*

Посебно дизајнирано ЕМ поље се назива „електромагнетном шупљином“ (енглеска скраћеница: *QEC*). Ово поље има сасвим посебну одлику: може се контролисати *број фотона у пољу*, тако да он буде 0, или 1, или суперпозиција ових стања поља – у којем случају број фотона је квантно неодређен. Различивост стања броја фотона омогућује увођење квантних стања $|0\rangle, |1\rangle$, као и произвољне суперпозиције ових стања. При томе, ова стања *нису елементи Хилбертовог простора стања*, већ се тичу формализма, тзв., *друге квантизације* (Хербут 1984). Свеједно, могућност контроле ових стања оправдава њихов квантномеханички третман као кубитова – формално, као елемената дводимензионалног Хилбертовог простора стања.

Додатак 9.1 *Статистички нееквивалентни кубитови*

У разматраном протоколу сви (међусобно неинтерагујући) кубитови су ***идентично третирани*** – отуда се они могу сматрати и ***ансамблом*** (на којем се сада могу вршити и усредњавања физичких величина). ***Супротан пример*** (илустрација у овом смислу) је дат ниже.

Пре мерења, Ева *одлучује да ли, и шта да мери*, на сваком појединачном кубиту. За 1. кубит она баца новчић да одлучи *да ли уопште да врши мерење*, а онда бацањем новчића одлучи коју опсерваблу да мери. На 2. кубиту она *баца коцку*, у складу са следећим прописом: ако бацањем коцке добије резултат већи од 2, онда врши мерење. Тада, независно од начина одлучивања *шта* да мери, ова два кубита *нису статистички еквивалентни*. У првом случају вероватноћа (било којег) мерења (на 1. кубиту) износи 1/2, а у другом случају (2. кубит) вероватноћа да ишта мери износи 2/3. У овом случају (за ова два разматрана кубита), величина λ из израза (9.14) је *средња вредност вероватноће* да Ева врши мерење на једном кубиту, која износи:

$$\lambda = p_{bacanjeNovcica}\frac{1}{2} + p_{bacanjaKocke}\frac{2}{3}; p_{bacanjeNovcica} + p_{bacanjaKocke} = 1. \qquad (Д9.1.1)$$

Додатак 9.2 *BB84 протокол са шумом*

Форма протокола у присуству спољашњег шума је иста, у основи, као и протокола без шума. Да би се „елиминисао“ утицај шума, у протокол се, на самом крају, убацују кораци[17], тзв., „усаглашавања информација“ и „приватне амплификације“. Формално, други поступак је сличан другом кораку у другој фази протокола (Одељак 9.3.3) – случајном избору битова и провери на тим битовима, те коначном избору мањег стринга битова који преостају после провере. Успешност овог корака има претпоставку о могућој, највећој, информацији коју може имати Ева. Доказ успешности овог поступка, заједно са претходним, далеко превазилази ниво основног курса квантне информатике. Напоменимо на крају да је први поступак, „усаглашавање информација“, заправо поступак корекције грешака, који је истакнут у Одељку 10.10.

Додатак 10.1 *О реверзибилном рачунању: дисипација енергије*

Иреверзибилно рачунање има двоструки узрок дисипације енергије (тј., грејања процесора): услед иреверзибилности операција (Сл. 10.1), и услед брисања информација (Ландауеров принцип):

[17] Енгл.: *information reconciliation*, *privacy amplification*, редом.

$$\Delta E^{(disipirano)} = \Delta E_{operacije}^{(disipirano)} + \Delta E_{brisanje\ informacije}^{(disipirano)}, \qquad (Д10.1.1)$$

с тим што је, типично, $\Delta E_{operacije}^{(disipirano)} >> \Delta E_{brisanje\ informacije}^{(disipirano)}$.

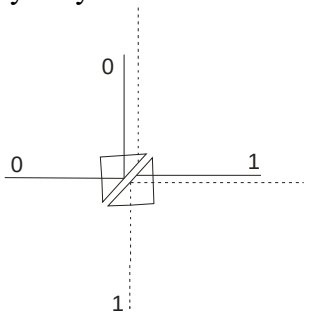
Код реверзибилног рачунања нема првог сабирка у (Д10.1.1).

Отуда и важно уочавање: густина дисипиране енергије код реверзибилног рачунања је *знатно мања* него код иреверзибилног. Отуда: ниво дисипације иреверзибилних рачунара се код реверзибилних може досегнути *смањењем димензија (минијатуризацијом) процесора* – што даје физичку основу *даље минијатуризације* процесора *преласком на реверзибилно (класично) рачунање.*

Додатак 10.2 *Изградња операције „корен из НЕ“*

Нека је, као у класичној оптици, задата призма која функционише у складу са прописима датим на Слици Д10.4.1.

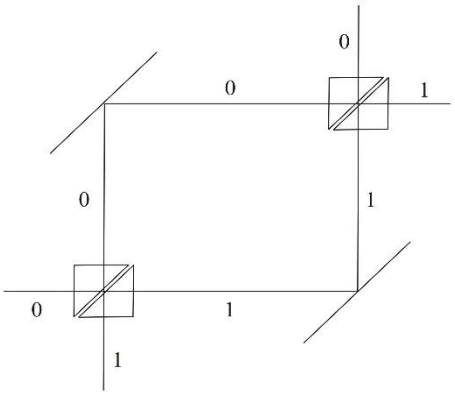
Дакле, улазак једног фотона путањом $|1\rangle$, *деловањем призме*, $\hat{V}$, даје суперпозицију могућих „путања“: $|1\rangle \to C_{10}|0\rangle + C_{11}|1\rangle$, и аналогно за другу путању, $|0\rangle \to C_{01}|0\rangle + C_{01}|1\rangle$. Ако се константе одаберу, $C_{00} = C_{11} = i/\sqrt{2}, C_{01} = C_{10} = 1/\sqrt{2}$, детектори на овим путањама иза призме дају *стохастички одговор*, са вероватноћама $1/2$, за сваку путању[18].



Сл. Д10.4.1 Ако је фотон ишао путањом 0, тада је иза призме добијена интерференција двеју путања, $C_{01}|0\rangle + C_{01}|1\rangle$, а ако је ишао путањом 1, тада се иза призме добија интерференција путања: $C_{10}|0\rangle + C_{11}|1\rangle$.

Међутим, ако се ставе две овакве призме, као на Слици Д104.2, детектори на излазу из друге призме дају излаз са ***вероватноћом 1***: ако је улаз $|1\rangle$, тада је излаз $|0\rangle$, и обрнуто – што је на овом скупу (базису израчунавања у овом случају) класична једнобитна операција НЕ. Али, тада, наравно, за одабране константе C_{ij}, једна призма функционише као „*корен из НЕ*“, јер, $\hat{V}^2$=НЕ!

[18] Наравно, детектори раде у *антикоинциденцији*: детекција једног фотона на једној путањи у потпуности искључује детекцију (истог) фотона на другој путањи.



Сл. Д10.4.2 Постављена су два потпуно одбијајућа огледала. Она преусмеравају интерферирајуће „путање“ од једне, ка другој призми. Може се показати да за дати избор константи, ако је улаз 0, излаз је увек (са вероватноћом једнаком јединици) 1, и обрнуто.

Доказ ове тврдње је једноставан: улаз у другу призму је суперпозиција путања једног фотона (фотон интерферира са самим собом дуж обе путање), што за одабране вредности константи лако даје[19], или $|0\rangle$, или $|1\rangle$, ако је улаз у прву призму или $|1\rangle$, или $|0\rangle$, редом.

Физички, укупни систем на Сл. Д10.4.2 функционише тако да, ако је фотон ушао путањом $|1\rangle$, он ће на крају изаћи путањом $|0\rangle$, и обратно. Тиме је физички остварена операција НЕ, али на основи две примене „апарата“ (овде: призме), који отуда делује као „корен из НЕ“, $\sqrt{\text{НЕ}}$.

Додатак 10.3 *О Шоровом алгоритму за факторисање великих бројева*

Шоров алгоритам представља уопштење Сајмоновог алгоритма (Одељак 10.9.4). Шор (*Shor 1997*) је заправо уопштио Сајмонов алгоритам, у смислу да Адамарова трансформација (и њихови тензорски производи) представља Фуријеов трансформ на једној факторизацији стања система кубитова, док ДКФТ, представљен у Одељку 10.9.5, заправо представља уопштење Адамарове трансформације. Тако се може уочити и известан прогрес у дизајну квантних алгоритама: почев од Дојчовог до Шоровог алгоритма, у употреби су све општији облици Фуријеовог трансформа.

Сам алгоритам је сложен. Ефективно, користи подалгоритам, тзв., *„налажење реда“* (“*order finding*”), чијом анализом се може утврдити ефикасност Шоровог алгоритма, тј., ефикасно факторисање великих бројева. У корену и једног и другог је, тзв., алгоритам за процену (квантне) „фазе“ (“*phase estimation*”) што је

---

[19] Нпр., нека је улаз $|1\rangle$. Тада је улаз у другу призму: $C_{10}|0\rangle + C_{11}|1\rangle$. А излаз из друге призме је $C_{10}\left(C_{00}|0\rangle + C_{01}|1\rangle\right) + C_{11}\left(C_{10}|0\rangle + C_{11}|1\rangle\right) = |0\rangle$. *Нема стохастичности* излаза из друге призме!

једна од најважнијих примена КДФТ. Како је за потребе представљања свих ових алгоритама (процена фазе, те на основи тога „налажење реда“ и њему заснованог квантног алгоритма за факторисање бројева) неопходно много детаља, нових дефиниција и доказа, читаоца упућујемо на књигу *Nielsen and Chuang 2000*.

Ове опште напомене завршимо једном важном опаском: поред процене фазе, одређивања реда, факторисања великих бројева, још један квантни алгоритам се може ефикасно засновати на КДФТ – израчунавање, тзв., дискретних логаритама (*discrete logarithms*). Са чисто математичког становишта, ово није изненађење. Наиме, *сви поменути проблеми* су само различити видови једног општијег математичког задатка – тзв., „проблема скривене подгрупе“ (*the hidden subgroup problem – Kitaev et al 2002*). Отуда се може рећи да су сви, овде наведени, корисни алгоритми заправо „само један“ (општи) математички задатак. Упркос немалом труду истраживача, до данас није направљен значајнији продор у смислу дизајнирања алгоритама за задатке који нису овог типа.

Додатак 10.4 *О Гроверовом алгоритму претраге базе података*

Вероватно најкориснија рачунарска операција је претрага података. Да би се претрага могла ваљано обавити, подразумева се да су подаци некако уређени (одабрани и поређани по неком критеријуму). У пракси, то увек значи претрагу неке базе података.

Гроверов алгоритам (*Grover 1997*) је пионирски рад у овом смислу. У међувремену, овај алгоритам вишеструко је проанализиран, проширен (редефинисаног задатка) и уопштен. Отуда се не може говорити о само једном алгоритму претраге података. Свеједно, оригинални Гроверов алгоритам је, и историјски први, и парадигматичан (па и оптималан у својој класи претрага базе података) за све постојеће разраде и уопштења. Вреди истаћи да овај алгоритам не даје „експоненцијално“, већ само полиномско убрзање у односу на најбоље одговарајуће класичне алгоритме претраге. Прецизније: ако је класичној претрази потребан број претрага реда-величине броја N, онда је Гроверовој претрази довољно $\sqrt{N}$ операција. Иако, и формално, и појмовно знатно једноставнији од Шоровог алгоритма, Гроверов алгоритам претраге такође захтева засебно и обимно представљање, те заинтересованог читаоца упућујемо на књигу *Nielsen and Chuang 2000*.

Додатак 10.5 *Стратегије борбе против декохеренције. Појам корекције грешака*

Грубо, стратегије борбе против декохеренције се могу поделити у три групе. *Прву*, и најстарију групу чине протоколи корекције грешака (*Error Correction Codes - ECC*), кратко представљене у Одељку 10.10, чија је основа следећа одлука: декохеренција се не може избећи, те се морају кориговати грешке услед декохеренције. *Другу* групу чине протоколи за избегавање декохеренције (*Error Avoiding Codes - EAC*). Наиме, група симетрије интеракције кубитова са окружењем може дефинисати (хардверски зависно) подпросторе на чија стања

дата интеракција не делује, тј., чија стања (у тим подпросторима) су инваријантна на интеракцију. Прављење сплетености од стања у тим подпросторима омогућује основу за избегавање декохеренције. *Треће*, постоји метод за суспрезање декохеренције, који је својеврсна „инжењерија“ декохеренције. Метод (*Decoherence-Induced Suppression of Decoherence - DISD, Dugić 2000*) полази од могућности декохеренцији-сличног утицаја на окружење („купатило“) кубитова. Довољно јак такав утицај може промену стања услед утицаја купатила на кубитове учинити мало вероватним ефектом чак и у макроскопски дугим временским интервалима. Овај трећи метод је истовремено и метод дефинисања информатичке независности физичког система од окружења (Одељак 13.3.2) – такав систем у времену еволуира приближно Шредингеровски.

Најразрађенији, и од највећег интереса су кодови за корекцију грешака (*ECC*). Уместо једног физичког кубита, користи се *скуп* физичких кубитова; један логички кубит се имплементира физичким скупом кубитова, и у складу са тим се редефинишу и жељене логичке операције. Полаз ових кодова (протокола) јесте претпоставка да се „грешке“ (нежељене промене стања кубитова) могу међусобно разликовати (у смислу Одељка 4.4). Ово, наравно, за произвољни квантни систем не мора бити испуњено. Али, у формализму кубитова се испоставља да алгебра (математичка структура над операторима) кубитова омогућује *дискретизацију грешака*. Наиме, свака (операторски представљена) промена стања једног кубита се може представити као нека линеарна сума четири основне операције на кубиту (које чине, тзв., Хајзенбергову групу), изрази (10.4), плус идентични оператор; уопштење на скуп кубитова је непосредно. На овој основи формулисан је метод, тзв., стабилизујућих кодова (*stabilizer codes*[20]), па на основи тога формулисани и протоколи за корекцију грешака. Идеја је да се на скупу кубитова обави посебно дизајнирано квантно мерење које ће дати одговор *који кубит* (у регистру) је, и *како* (врста грешке), измењен. На основи тога се доноси одлука о поправци грешке – *утврђене* (уочене) грешке на *датом* кубиту.

Физички, квантно рачунање се сада своди, углавном, на кориговање грешака и у значајно мањем проценту на примену логичких капија, а све то на регистрима у којима је сваки логички кубит[21] остварен скупом физичких кубитова. Такав модел – *fault tolerant model* [22] – рачунања је могућ и, упркос техничкој сложености, и даље је у предности у односу на класично реверзибилно рачунање.

---

[20] *Gottesman 1998.*

[21] Када не би било шума, један логички кубит био би остварен једним физичким кубитом.

[22] Изузетно детаљан приказ овога може се наћи у Прескиловој презентацији, *Preskill 1998.*

ЛИТЕРАТУРА

Aliferis P. and Leung D., 2004, Phys. Rev. A **70**, 062314

Araki H. and Yanase M. M., 1960, Phys. Rev. **120**, 622

Aspect A., Dalibard J., and Roger R., 1982, Phys. Rev. Lett. **49**, 1804

Atkins P. and Friedman R., 2005, *Molecular Quantum Mechanics* (fourth edition), Oxford University Press, Oxford, UK&NI

Barenco et al, 1995, Phys. Rev. A **52**, 3457

Bell J. S., 1964, Physics **1**, 195

Bell J. S., 1987, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, UK&NI

Bennett C. H., 1982, Int. J. Theoret. Phys. **21**, 905

Bennett C.H. et al, 1993, Phys. Rev. Lett. **70**, 1895

Bennett C. H. and Wiesner S. J., 1992, Phys. Rev. Lett. **69**, 2881

Bennett C. H. and Brassard G., 1984, Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, IEEE, New York, Bangalor, India, pp 175-179

Benioff P., 1980, J. Stat. Phys. **22**, 563

Blum K., 1981, *Density Matrix, Theory and Applications*, Springer, Berlin

Brillouin L., 1962, *Science and Information Theory*, Academic Press, New York (Dover, 299)

Brunner N. et al, 2004, Phys. Rev. Lett. **93**, 203902

Clauser J. F. et al, 1969, Phys. Rev. Lett. **49**, 1804

Childs A. M. and Farhi E., 2001, Phys. Rev. **65**, 012322

Csiszar I. and Korner J., 1982, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York

Cvjetković V. i Dugić M., 2004 "Predlog softverske simulacije kvantnog protokola za razmenu tajnog kljuca",YUINFO'04, Kopaonik 8-12 Mart, SCG

d'Espagnat B., 1971, *Conceptual Foundations of Quantum Mechanics*, Benjamin, Reading, MA

Deutsch D., 1985, Proc. R. Soc. London A **425**, 73

Deutsch D. and Josza A.,1992, Proc. R. Soc. London **439**, 553

DiVincenzo D. P., 2001, Quantum Information and Computation, Special Issue **1**, 1

Dugić M., 2000, Quantum Computers & Computing **1**, 102

Dugić M., 2002a, "Quantum Technologies: Quantum Mechanics as Applied Physics", in *Proc. Applied Physics in Serbia-APS*, S. Koički, N. Konjević, Z. Lj. Petrović and Đ. Bek-Uzarov (Eds.), 27-29 May Beograd

Dugić M., 2002b, Open Systems and Information Dynamics **9**, 115

Dugić M., 2002c, Europhys. Lett. **60**, 7

Дугић М., 2004, *Декохеренција у класичном лимиту квантне механике, СФИН,* XVII (2), Институт за физику, Београд

Dugić M., Arsenijević M., and Jeknić-Dugić J., 2009, eprint arXiv, quant-ph/0812. 1677v

Dugić M. and Raković D., 2000, Europ. Phys. J. B **13**, 781

Dugić M. and Ćirković M. M., 2002a, Phys. Lett. A **302**, 291

Dugić M. and Ćirković M. M., 2002b, Int. J. Theor. Phys. **41**, 1641

Dugić M., Jeknić-Dugić J., 2006, Int. J. Theor. Physics **45**, 2215

Dugić M., Jeknić-Dugić J., 2008, Int. J. Theor. Physics **47**, 805

Dugić M., Jeknić-Dugić J., 2009, Chin. Phys. Lett. **26**, 090306

Farhi E. et al, 2001, Science **292**, 472

Feynman R. P., 1982, Int. J. Theor. Physics **21**, 467

Forcer T. M. et al, 2002, Quantum Information and Computation **2**, 97

Giulini D., Joos E., Kiefer C., Kupsch J., Stamatescu I.-O. and Zeh H. D., 1996, *Decoherence and the Appearance of a Clasical World in Quantum Theory*, Springer, Berlin

Gribov L. A. and Mushtakova S. P., 1999, *Kvantovaya himiya*, Gardaraki, Moskva

Greenberger D., Horn M. A., and Zeilinger A., 1989, in *Bell's Theorem, Quantum Theory and Concepts of the Universe*, M. Kifato (Ed.), Kluwer, Dordrecht, pp. 69-72

Gottesman D., 1998, Phys. Rev. A **57**, 127

Grover L., 1997, Phys. Rev Lett. **79**, 325

Хербут Ф., 1984, *Квантна механика*, ПМФ, Београд

Herbut F., 1969, Ann. Phys. **55**, 271

Herbut F., 1974, Int. J. Theor. Phys. **11**, 193

Horodecki M., 2001, Quantum Information and Computation **1**, 3

Jeknić-Dugić J., Dugić M., 2008, Chin. Phys. Lett. **25**, 371

Kane B. E., 1998, Nature **393**, 1331

Kraus K., 1983, *States, Effects and Operations*, Springer-Verlag, Berlin

Kitaev A. Yu., 1997, RMS: Russian Mathematical Surveys **52**, 1191

Kitaev A. Yu., Shen A. and Vyalyi M., 2002, *Classical and Quantum Computation*, American Mathematical Society

Landauer R., 1961, IBM J. Res. Dev. **5**, 183

Landauer R., 1996, Phys. Lett. A **217**, 180

Y. L. Lim et al, 2006, Phys. Rev. A **73**, 012304

Maeda H., Norum D. V. L., and Gallagher T. F., 2005, Science **307**, 1757

Mancini S. and Tombesi P., 2003, Quantum Information and Computation **2**, 106

Margolus N. and Levitin L. B., 1998, Physica D **120**, 188

Марић З., 1986, *Оглед о физичкој реалности*, Нолит, Београд

Milburn G. J., 1997, *Schrodinger Machines: Quantum Technology Reshaping Everyday Life*, Freeman, New York

Messiah A., 1976, *Quantum Mechanics*, North Holland Publ. Co., Amsterdam

Мушицки Ђ., 1984, *Теоријска физика I: теоријска механика*, ПМФ, Београд

Nielsen M. A. and Chuang I. L., 2000, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK

Nielsen M., 2001, eprint arXiv, quant-ph/0111122

Papadimitriou C. M., 1994, *Computational Complexity*, Addison-Wesley, Reading, MA

Peres A., 1993, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht

Popescu S. and Rorlich D., 1992, Phys. Lett. A **169**, 411

Preskill J., 1998, http://www.theory.caltech.edu/people/preskill/ph229

Raussendorf R. and Briegel H.-J., 2001, Phys. Rev. Lett. **86**, 910

Raussendorf R. and Briegel H.-J., 2002, Quantum Information and Computation **6**, 443

Schumacher B. and Westmoreland M. D., 2005, Quantum Information Processing **4**, 13

Simon D. R., 1997, SIAM J. Comp. **26**, 1474

Shannon C. E., 1948, The Bell System Technical Journal, **27**, 623

Shannon C. E. and Weaver W., 1963, *The Mathematical Theory of Communication*, Univ. Illinois Press

Shor P., 1995, Phys. Rev. A **52**, 2493

Shor P. W., 1997, SIAM J. Comp. **26**, 1484

Steane A. M., 1996, Phys. Rev. Lett. **77**, 793

Volovich I., 2001, private communication

von Neumann J., 1955, *Mathematical Foundations of Quantum Mechanics*, Princeton Univ. Press, Princeton

Vujičić M., 2008, *Linear Algebra Thoroughly Explained*, Springer, Berlin

Walther P. Et al, 2005, Nature **434**, 169

Wheeler J. A. and Zurek W. H., Eds., 1983, *Quantum Theory and Measurement*, Princeton Univ. Press, Princeton

Wigner E., 1952, Z. Phys. **131**, 101

Wooters W.K. and Zurek W. H., 1982, Nature **299**, 802

Yanase M. M., 1961, Phys. Rev. **123**, 666

Zeh H. D., 2007, *The Physical Basis of the Direction of Time* (fifth edition), Springer, Berlin

ИНДЕКС АУТОРА

Х. Араки (*H. Araki*)

Џон С. Бел (*John S. Bell*)

Чарлс Бенет (*Charles Bennett*)

Пол Бениоф (*Paul Benioff*)

Нилс Бор (*Niels Bohr*)

Жил Брасар (*Gilles Brassard*)

Х. Ј. Бригел (*H.-J. Briegel*)

Леон Бријуен (*Leon Brilouin*)

Часлав Брукнер

Николас Брунер (*Nicolas Brunner*)

Џон А. Вилер (*John. A. Wheeler*)

Вилијем Вутерс (*William Wooters*)

Лов Гровер (*Lov Grover*)

Дејвид Готесман (*David Gottesman*)

Бернар Деспања (*Bernard d'Espagnat*)

Дејвид П. ДиВинћенцо (*David P. DiVincenzo*)

Дејвид Дојч (*David Deutsch*)

Д. Ђулини (*D. Giulini*)

Војчех Х. Зурек (*Wojciech H. Zurek*)

Игор Ивановић

М. М. Јанас (*M. M. Yanase*)

Јасмина Јекнић-Дугић

А. Јоса (*A. Josza*)

А. Ју. Китајев (*A. Yu. Kitaev*)

Ролф Ландауер (*Rolph Landauer*)

Л. Б. Левитин (*L. B. Levitin*)

Н. Марголис (*N. Margolus*)

Џерард Џ. Милбурн (*Gerard J. Milburn*)

Мајкл А. Нилсен (*Michael A. Nielsen*)

Роџер Пенроуз (*Roger Penrose*)

Санду Попеску (*Sandu Popescu*)

Џон Прескил (*John Preskill*)

Р. Раусендорф (*R. Raussendorf*)

Д. Р. Сајмон (*D. R. Simon*)

Ендрју Стин (A*ndrew Steane*)

Алан Тјуринг (*Alan Turing*)

Милан М. Ћирковић

Ричард П. Фајнман (*Richard P. Feynman*)

Едвард Фархи (*E. Farhi*)

Јохан фон Нојман (*Johann von Neumann*)

Федор Хербут

Антон Цајлингер (*Anton Zeilinger*)

Ендрју Чилдс (*Andrew Childs*)

Исак Л. Чуанг (*Isac L. Chuang*)

Алонзо Чрч (*Alonzo Church*)

Клод И. Шенон (*Claude E. Shannon*)

Питер В. Шор (*Peter W. Shor*)

Б. Шумахер (*B. Schumacher*)

ИНДЕКС ПОЈМОВА

Адијабатско квантно рачунање (*adiabatic quantum computation*)

Алгоритам (*algorithm*)

Ансамбли (*ensembles*)
- класични
- квантни
  - просторни, временски
  - чисти, мешани

Антикомутатор (*anticommutator*)

Белова стања/базис (*Bell states/basis*)

Белова неједнакост (*Bell inequality*)

Бит (*bit*)

Блохова сфера (*Bloch sphere*)

Боров принцип комплементарности (*Bhor's complementarity principle*)

Булова логика и алгебра

Двокубитне трансформације (*two-qubit transformations*)

Декодирање (*decoding*)

Декохеренција (*decoherence*)

Диракова нотација (симболика)

Дискретни Фуријеов трансформ (*discrete Fourier transform*)

Ентропија (*entropy*):

Информатичка:
- Изолованост (локалност)
- Локалност

Једнокубитне трансформације (*one-qubit transformations*)

Једносмерно квантно рачунање (*one-way quantum computation*)
(као и : *measurement-based*, или *cluster quantum computation*)

Квантна криптографија (*quantum cryptography*)

Квантна нелокалност (*quantum nonlocality*)

Квантна неодређеност (*quantum uncertainty/indeterminism*)

Квантна несепарабилност (*quantum non-separability*)
(в. и „Квантна сплетеност“)

Квантна телепортација (*quantum teleportation*)

Квантни алгоритми:
- Гроверов (*Grover*)
- Дојчов (*Deutsch*)
- Дојч-Јозин (*Deutsch-Josza*)
- Сајмонов (*Simon*)
- Шоров (*Shor*)

Квантни (информатички) канал (*quantum channel*)

Квантни информатички лимит (*quantum information limit*)

Квантни паралелизам (*quantum parallelism*)

Квантни протоколи:
- супергусто кодирање (*superdense coding*)
- телепортација (*teleportation*)
- криптографски (*BB84*)

Квантни информатички ресурси (*quantum information resources*)

Квантни хардвер (*quantum hardware*)

Квантно мерење (*quantum measurement*):
- предиктивно (ортогонално, пројективно) мерење (*1. врсте*)
- ретроспективно мерење (*2. врсте*)
- уопштено мерење
- *POVM* мерење

Класична неодређеност

Класична реалност (*classical reality*)

Класични (информатички) канал (*classical channel*)

Клонирање стања (*state cloning*)

Кључ (*key*):
- сирови (*raw key*)
- тајни (*secret key*)

Кодирање (*coding*)

Комуникација брже од светлости

Комутатор (*commutator*)

Корекција грешака (*error correction*)

Криптографија (*cryptography*)

Кубит - квантни бит (*qubit*)

Ландауеров принцип (*Landauer principle*)

Лиувилова једначина (*Liouville equation*)

Логичке капије/операције (*logic gates/operations*)
- Адамарова (*Haddamard*)
- Булове операције (И, ИЛИ, НЕ, и друге)
- *CROSSOVER*, или *SWAP*
- *CNOT*, или *XOR* (што је искључиво ИЛИ: ИЛИ)
- Тофолијева капија (*Toffoli gate*)
- Фредкинова капија (*Fredkin gate*)
- *FANOUT*, или *COPY*
- Корен из НЕ ($\sqrt{\text{НЕ}}$)

Матрица (*matrix*)

Матрица густине (*density matrix*) – видети: *Статистички оператор*

Мексвелов демон (*Maxwell's demon*)

Методи корекције грешака ("*error correction codes (EEC)" methods*)

Мешавине друге врсте (*improper mixtures*)

Мешавине прве врсте (*proper mixtures*)

Мешана стања (*mixed states*)

Модел-кола (*circuit model*):
- класичног рачунања
- квантног рачунања

Неизрачунљивост (*noncomputability*)

Немогућност клонирања квантних стања (*No-cloning theorem*)

Неразличивост квантних стања (*quantum states indistinguishability*)

Паулијев принцип (*Pauli principle*)

Паулијеви оператори (*Pauli operators*)

Производ
- оператора
- матрица
- скаларни производ
- тензорски (директни)

Процесирање на идеалном гасу

Рачунање (*computation, computing*)

Реверзибилно рачунање (*reversible computation*)

Репрезентација (*representation*)

Спин (*spin*)

Спољашњи шум (*noise*)

Статистички оператор (*statistical operator*)

Стохастичко рачунање (*stochastic computation*)

Стохастичка Тјурингова машина (*stochastic Turing machine*)

Тезе:
- Јака Чрч-Тјурингова теза (*strong Church-Turing thesis*)
- Чрч-Тјурингова теза (*Church-Turing thesis*)

Теорија комплексности (*complexity theory*)

Тјурингова машина (*Turing machine*)

Универзално рачунање (*universal computation*)
- квантно
- класично

Условна ентропија (*conditional entropy*)

Фазни простор (*phase space*)

Хилбертов простор (*Hilbert space*)

Шенонова ентропија/информација (*Shannon entropy/information*)

Шенонови теореми (*Shannon's theorems*)

Шмитова канонска форма (*Schmidt canonical decomposition*)

Шредингерова једначина (*Schrödinger equation*)

Поговор

Квантна информатика и квантно рачунање је типична област технологије у развоју – тзв. *квантне технологије*. Успеси са развојем практично-корисних протокола квантне криптографије те успешне експерименталне имплементације и провере Гроверовог и Шоровог квантних алгоритама указују на могућу практичну па и комерцијалну корисност ове мултидисциплинарне области. У време писања ове књиге, посебно обећавајући део квантног рачунања је *кластерни* модел квантног рачунања и сасвим је могуће да ће то бити основа практичних, па можда и комерцијалних, будућих квантних рачунара. Свеједно, значај модела-кола квантног рачунања који је овде представљен задуго неће изгубити своју важност и значај.

21. век је већ препознат као век квантне технологије – инжењери 21. века биће инжењери квантне механике. На путу ка пуном развоју ове технологије се налазе поступци тзв. нанотехнологије – још једне области у развоју. У научном смислу, манипулација наносклоповима непосредно се тиче фундаменталног проблема „преласка са квантног на класично“ – који је и један аспект проблема квантног мерења (као фундаменталног проблема квантне механике). Отуда се од развоја нанотехнологије, као и квантне технологије, може очекивати и значајнији продор у поимању, а можда и развијању својеврсне интуиције везане за основе квантне механике – што је уједно и главни научни мотив аутора.