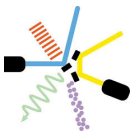
Гроверов алгоритам и блокови који броје π

Наставне белешке (радна верзија)

Јован Марков



Јесењи семинар Физике 2
Истраживачка станица Петница
4. новембар 2026.

Садржај

Предговор **4**

Како користити ове белешке **5**
Како је текст организован . . . 5
Боје и ознаке . . . 5
Шта треба знати унапред . . . 5

Увод **6**

1. **Блокови који броје π** **7**
1.1 Проблем . . . 7
1.2 Како почети . . . 7
1.3 Закони одржања и једначине судара . . . 8
1.4 Неколико судара . . . 9
1.5 Раван брзина: елипса . . . 11
1.6 Од елипсе до кружнице . . . 11
1.7 Права сталног импулса . . . 12
1.8 Када судари престају . . . 13
1.9 Од судара до геометријског проблема . . . 14
1.10 Једнаки лукови . . . 15
1.11 Колико лукова стаје на кружницу . . . 16
1.12 Цифре броја π . . . 19
1.13 Задаци . . . 23

2. **Основе квантне механике и квантног рачунарства** **25**
2.1 Квантно стање као вектор . . . 25
2.2 Суперпозиција и амплитуде . . . 26
2.3 Мерење и вероватноће . . . 26
2.4 Више кубита . . . 28
2.5 Оператори и унитарност . . . 28
2.6 Квантна кола и капије X и H . . . 29
2.7 Адамарове капије на више кубита . . . 30
2.8 Контролисане квантне капије: CNOT и CZ . . . 31
2.9 Скаларни производ, бра и пројектори . . . 32
2.10 Задаци . . . 35

3. **Гроверов алгоритам** **38**
3.1 Шта је квантна претрага? . . . 38
3.2 Колико је провера потребно? . . . 38
3.3 Сложеност алгоритама . . . 39
3.4 Формулација проблема претраге . . . 40
3.5 Шта зна оракл? . . . 40
3.6 Зашто оракл мења знак . . . 41
3.7 Зашто сам оракл није довољан . . . 42
3.8 Дејство оракла на почетно стање . . . 46
3.9 Оракл као огледање . . . 47
3.10 Дифузија: огледање у односу на осу $|s\rangle$ . . . 49
3.11 Два огледања дају ротацију . . . 51
3.12 Зашто су довољне две димензије? . . . 53
3.13 Колико је Гроверових корака потребно? . . . 54
3.14 Појачавање амплитуде . . . 55
3.15 Гроверова и класична претрага без структуре . . . 56
3.16 Квантно коло Гроверовог алгоритма . . . 57
3.17 Два кубита, корак по корак . . . 59

3.18 Задаци 61

4. **Два проблема, иста геометрија** **64**
4.1 Поставка: од много кугли до два блока 64
4.2 Заједничка раван стања 64
4.3 Судари као огледања 65
4.4 Поређење механичког система и Гроверовог алгоритма 66
4.5 Одакле разлика у броју корака? 66
4.6 Пример: погодак из прве 67
4.7 Задаци 69

Додатак А. **Бројање судара помоћу зрака светлости** **71**

Додатак Б. **Радијани, мали углови и периферијски угао** **73**

Појмовник **75**

Ознаке **78**

За даље читање и гледање **80**

Литература **80**

Коначни одговори на задатке **81**

Предговор

Ове белешке припремљене су као пратећи материјал за предавање о Гроверовом алгоритму, одржано на јесењем семинару Физике 2 у Истраживачкој станици Петница, 4. новембра 2026. године. Намењене су пре свега средњошколцима који желе да се упознају са основним идејама квантног рачунарства, а написане су тако да могу послужити и за самостално учење.

Полазна идеја предавања јесте да се један квантни алгоритам може разумети помоћу математике коју срећемо у класичној механици и геометрији. Постепено ћемо изградити геометријски опис Гроверовог алгоритма и показати како се он повезује са наизглед сасвим другачијим проблемом еластичних судара два блока.

Приступ се ослања на математичку везу коју је показао Адам Браун, као и на раније радове о геометрији судара и квантној претрази. Циљ бележака је да, поред коначних формула, објасне и како се до њих долази. Зато нове појмове уводимо постепено, а сваки корак у математичким извођењима посебно објашњавамо.

Како користити ове белешке

Како је текст организован

У првом поглављу решићемо загонетку два блока. Полазећи од закона одржања енергије и импулса, показаћемо зашто број судара открива цифре броја π.

У другом поглављу увешћемо потребне појмове квантне механике и квантног рачунарства: квантна стања, суперпозицију, мерење, кубите, операторе и квантна кола. Нове идеје објаснићемо помоћу вектора и геометрије.

У трећем поглављу упознаћемо Гроверов алгоритам. Формулисаћемо проблем претраге, објаснити како делују оракл и дифузија, извести број потребних корака и приказати одговарајуће квантно коло.

У четвртом поглављу повезаћемо претходна три: показаћемо како се судари блокова и Гроверов алгоритам описују истом геометријом огледања и ротација, ослањајући се на Браунов рад.

На крају сваког поглавља налазе се задаци за самосталан рад, од једноставнијих до сложенијих. Уз поједине задатке дата су и кратка упутства за решавање. Поједине доказе остављамо за самосталан рад и на одговарајућим местима упућујемо на задатак, на пример „в. задатак 63“. **Коначни одговори на све задатке**, без поступака решавања, налазе се на крају рукописа, у одељку Коначни одговори на задатке, како бисте могли самостално да проверите своје резултате.

После поглавља следе два додатка са допунским извођењима, појмовник, списак ознака, препоруке за даље читање и гледање и литература.

Боје и ознаке

Да бисмо лакше пратили везу између механике и квантног рачунарства, кроз цео текст користићемо исте боје за исте појмове, како на сликама тако и у формулама.

- **Наранџаста** означава мали блок (m, v, y), а у Гроверовом алгоритму тражени елемент w.
- **Плава** означава велики блок (M, V, x) и елементе који нису означени.
- **Црвена** представља одбијање од зида, односно дејство оракла.
- **Зелена** представља судар два блока, односно операцију дифузије.
- **Љубичаста** означава угао $\bar{\theta}$ и одговарајуће лукове $2\bar{\theta}$.
- **Сива** се користи за помоћне линије и област у којој судари престају.
- **Златна** означава резултат Гроверовог алгоритма.

Шта треба знати унапред

За праћење предавања довољно је основно познавање вектора у равни, тригонометрије правоуглог троугла, вероватноће и механике, пре свега појмова кинетичке енергије и импулса. Претходно познавање квантне механике није потребно: нове појмове увешћемо успут.

Увод

Ово предавање повезује две наизглед сасвим различите приче.

Прва прича говори о два блока која клизе по подлози без трења. Мали блок мирује између зида и великог блока који му се приближава. Сви судари су савршено еластични, укључујући и одбијање малог блока од зида. Ако је маса великог блока 100 пута већа од масе малог, догодиће се 31 судар. Ако је 10 000 пута већа, биће 314 судара, а ако је милион пута већа, чак 3141 судар. Ови бројеви нису случајни — у њима се крију почетне цифре броја π. Ову необичну загонетку популаризовао је канал *3Blue1Brown* 2019. године, а 2025. посветио јој је још један видео [1].

Друга прича води нас у свет квантних рачунара. Замислимо да међу N елемената тражимо један који испуњава задати услов. Можемо да проверимо сваки елемент, али немамо податке који би нам помогли да унапред издвојимо оне које вреди прво испробати. Класичан рачунар тада проверава елементе један по један и у просеку му је потребно око $N/2$ провера. **Гроверов алгоритам** омогућава квантном рачунару да тражени елемент пронађе са великом вероватноћом, уз број упита који расте као $\sqrt{N}$.

Адам Браун је 2020. године показао нешто изненађујуће: **иза ове две наизглед потпуно различите приче крије се иста математика** [2]. Испоставља се да се судари блокова и Гроверов алгоритам могу описати истим геометријским поступком, помоћу огледања и ротација. **Циљ овог предавања је да разумемо како и зашто је то могуће.**

1. Блокови који броје π

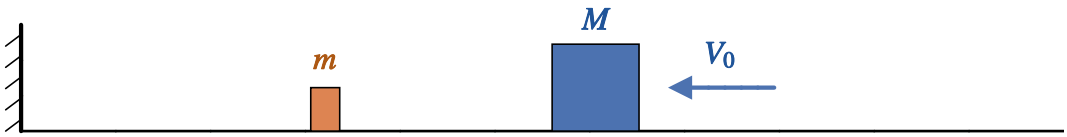
Пре него што пређемо на Гроверов алгоритам, решићемо једну загонетку из класичне механике.

1.1 Проблем

Поставка проблема

Два блока налазе се на хоризонталној подлози без трења, а лево од њих је зид. Мали блок, масе m, мирује. Велики блок, масе M, креће се ка малом блоку и зиду. Износ његове почетне брзине је $V_0 > 0$. Број судара не зависи од износа почетне брзине, већ само од односа маса блокова; то ћемо видети у §1.9. Однос маса M/m је задат и није мањи од 1. Сви судари су савршено еластични: и када се блокови сударе, и када мали блок удари у зид (Слика 1.1).

Питање: колико има судара укупно, рачунајући и сударе блокова и одбијања малог блока од зида?



Слика 1.1. Почетак: мали блок мирује, а велики блок иде ка зиду брзином чији је износ V_0. Величине блокова нису сразмерне масама.

Ево одговора за седам односа маса, почев од блокова једнаких маса, $M/m = 1$:

однос маса M/m	број судара
1	3
100	31
10^4	314
10^6	3141
10^8	31415
10^{10}	314159
10^{12}	3141592

Табела 1.1. Број судара за седам односа маса.

Бројеви судара у сваком реду дају почетне цифре броја $\pi = 3{,}14159265\ldots$, без децималног зареза. Откуд број π у проблему судара два блока?

1.2 Како почети

Како бисте приступили овом проблему? Пре него што наставите са читањем, покушајте да сами размислите о могућем решењу. У томе вам могу помоћи следећи савети, које наводи и канал *3Blue1Brown* у свом видеу [1]:

- Почните од једноставнијег случаја.

- Размислите које физичке величине остају очуване.
- Запишите једначине које описују систем.
- Потражите симетрију која би могла да поједностави проблем.
- Израчунајте неколико конкретних примера и покушајте да уочите правилност.
- Ако можете, направите једноставну рачунарску симулацију.
- Нацртајте слику.

1.3 Закони одржања и једначине судара

За позитиван смер изабраћемо смер удесно, од зида. Брзину малог блока означаваћемо са v, а великог са V. Према томе, брзина блока је позитивна када се креће удесно, а негативна када се креће улево. Пошто мали блок на почетку мирује, а велики се креће ка зиду, почетне брзине су $v = 0$ и $V = -V_0$, где је $V_0 > 0$.

Пошто нема трења и сви судари су савршено еластични, укупна **кинетичка енергија** E блокова остаје непромењена. При међусобном судару блокова чува се и њихов укупан **импулс** p, јер током судара у хоризонталном правцу делују само међусобне силе блокова. Укупна кинетичка енергија и импулс система дати су изразима

$$E = \frac{mv^2}{2} + \frac{MV^2}{2}, \qquad p = mv + MV \tag{1.1}$$

При савршено еластичном одбијању од непокретног зида мења се само смер брзине малог блока, док њен износ остаје исти: $v \to -v$. Брзина великог блока се при томе не мења. За разлику од међусобног судара блокова, при одбијању од зида њихов укупан импулс није очуван, јер зид делује спољашњом силом на посматрани систем. Ово ћемо детаљније објаснити на крају одељка.

Помоћу закона одржања енергије и импулса можемо одредити брзине блокова после њиховог међусобног судара. Означимо их са v' и V'. Закон одржања импулса препишимо у облику

$$m(v - v') = M(V' - V).$$

Закон одржања енергије, после растављања разлике квадрата, даје

$$m(v - v')(v + v') = M(V' - V)(V' + V).$$

При судару се брзина малог блока промени, па је $v' \neq v$ и другу једначину можемо поделити првом:

$$v + v' = V + V', \qquad \text{тј.} \qquad v' - V' = -(v - V).$$

Дакле, при савршено еластичном судару релативна брзина блокова мења знак, док њен износ остаје непромењен. Овај резултат и закон одржања импулса дају две линеарне једначине за непознате брзине v' и V'. Њиховим решавањем добијамо

$$v' = \frac{(m - M)\,v + 2MV}{m + M}, \qquad V' = \frac{(M - m)\,V + 2mv}{m + M} \tag{1.2}$$

Формула (1.2) објашњава и одбијање од зида. Замислимо зид као блок масе $M_з$ који на почетку мирује, $V_з = 0$ („з“ као зид). Ставимо га у (1.2) на место великог блока и погледајмо шта се дешава када његова маса расте без границе, $M_з \to \infty$.

После судара брзине малог блока и зида су

$$v' = \frac{m - M_з}{m + M_з}\, v \longrightarrow -v, \qquad V_з' = \frac{2mv}{m + M_з} \longrightarrow 0.$$

У овој граници мали блок се одбије истим износом брзине, а брзина зида тежи нули. Шта је са импулсом? Иако му је брзина све мања, зид прима импулс који не тежи нули:

$$M_з V_з' = \frac{2M_з mv}{m + M_з} \longrightarrow 2mv.$$

Кинетичка енергија зида, напротив, тежи нули:

$$\frac{M_з V_з'^2}{2} = \frac{(M_з V_з')^2}{2M_з} \longrightarrow 0.$$

Тако у граници бесконачне масе зид прими коначан импулс, а његова брзина и кинетичка енергија теже нули. Зато се при одбијању енергија два блока чува, а њихов укупан импулс мења. Пре удара мали блок иде ка зиду, $v < 0$, па је промена импулса блокова $-2mv = 2m|v|$, у смеру од зида.

1.4 Неколико судара

Размотримо најпре случај када су масе блокова једнаке, $M = m$. Тада из једначина (1.2) следи $v' = V$ и $V' = v$, што значи да блокови при судару размењују брзине. Пошто мали блок на почетку мирује, а велики се креће ка зиду, почетне брзине су $v = 0$ и $V = -V_0$. Пар брзина (v, V) мења се овако:

$$(0, -V_0) \xrightarrow{\text{блокови}} (-V_0, 0) \xrightarrow{\text{зид}} (V_0, 0) \xrightarrow{\text{блокови}} (0, V_0).$$

После првог судара велики блок се зауставља, а мали наставља да се креће ка зиду. Након одбијања од зида, мали блок се враћа и поново судара са великим. При том судару мали блок се зауставља, док велики наставља да се креће удесно, од зида. Пошто се блокови више не приближавају, нових судара неће бити. **Укупно су се догодила три судара.**

Размотримо сада случај када је велики блок 100 пута масивнији од малог, односно $M/m = 100$. Ради једноставнијег рачуна изабраћемо јединице тако да је $m = 1$, $M = 100$ и $V_0 = 1$. За ове масе формуле (1.2) гласе

$$v' = \frac{-99\, v + 200\, V}{101}, \qquad V' = \frac{99\, V + 2\, v}{101},$$

а енергија и импулс (1.1) гласе

$$E = \frac{v^2}{2} + 50\, V^2, \qquad p = v + 100\, V.$$

На почетку је $v = 0$ и $V = -1$, па је $E = 50$ и $p = -100$.

Први судар је судар блокова. Уврстимо $v = 0$ и $V = -1$:

$$v' = \frac{-99 \cdot 0 + 200 \cdot (-1)}{101} = -\frac{200}{101} \approx -1{,}98,$$
$$V' = \frac{99 \cdot (-1) + 2 \cdot 0}{101} = -\frac{99}{101} \approx -0{,}98.$$

Оба блока иду ка зиду, али се мали креће брже и зато први стиже до њега.

Други судар је одбијање од зида. Мали блок промени знак брзине, а велики задржи своју:

$$v' = -\left(-\frac{200}{101}\right) = \frac{200}{101} \approx 1{,}98,$$
$$V' = V = -\frac{99}{101} \approx -0{,}98.$$

Мали блок сада иде удесно, а велики улево, па се поново приближавају.

Трећи судар је опет судар блокова. Уврстимо брзине после другог судара:

$$v' = \frac{-99 \cdot \frac{200}{101} + 200 \cdot \left(-\frac{99}{101}\right)}{101} = -\frac{39600}{10201} \approx -3{,}88,$$
$$V' = \frac{99 \cdot \left(-\frac{99}{101}\right) + 2 \cdot \frac{200}{101}}{101} = -\frac{9401}{10201} \approx -0{,}92.$$

Оба блока поново иду ка зиду; мали је бржи, па ће следећи ударити у зид.

Сада проверимо законе одржања. Табела 1.2 за свако стање даје енергију и импулс, са бројевима увршћеним у (1.1):

стање	**врста судара**	v	V	$E = v^2/2 + 50\,V^2$	$p = v + 100\,V$
почетак		0	−1	0 + 50 = 50	0 − 100 = −100
после 1. судара	блокови	−1,98	−0,98	1,96 + 48,04 = 50	−1,98 − 98,02 = −100
после 2. судара	зид	1,98	−0,98	1,96 + 48,04 = 50	1,98 − 98,02 = −96,04
после 3. судара	блокови	−3,88	−0,92	7,53 + 42,47 = 50	−3,88 − 92,16 = −96,04

Табела 1.2. Прва три судара за $M/m = 100$, са $m = 1$, $M = 100$ и $V_0 = 1$. У колонама E и p први сабирак припада малом блоку, а други великом. Бројеви су заокружени на две децимале, а рачунати су из тачних разломака.

Иако се брзине блокова мењају при сваком судару, њихова укупна кинетичка енергија остаје иста, $E = 50$. Мења се само начин на који је та енергија расподељена између блокова. На пример, после трећег судара кинетичка енергија малог блока износи приближно 7,53, а великог 42,47.

Укупан импулс блокова чува се при њиховим међусобним сударима. Пре и после првог судара он износи −100, а пре и после трећег приближно −96,04. Међутим, при одбијању малог блока од зида импулс система се мења. У другом судару брзина малог блока мења знак, па се укупан импулс повећава за приближно 3,96.

После два међусобна судара износ брзине великог блока смањио се за свега око 8 %. Ако бисмо наставили да рачунамо на исти начин, до 31 судара стигли бисмо тек после дуготрајног рачуна, а до 314 још теже. Рачунар би могао лако да симулира све те сударе, али сама симулација не објашњава зашто се у њиховом броју појављују баш цифре броја π. **Можемо ли проблем представити геометријски и тако доћи до једноставнијег решења?**

1.5 Раван брзина: елипса

Сваком пару брзина блокова, V и v, можемо придружити једну тачку у равни. На хоризонталној оси приказиваћемо брзину великог блока V, а на вертикалној брзину малог блока v. Тако добијамо **раван брзина**, у којој свака тачка представља један могући пар брзина блокова.

Према закону одржања кинетичке енергије,

$$MV^2 + mv^2 = 2E \tag{1.3}$$

Ово је једначина **елипсе** (Слика 1.2а). Пошто се укупна кинетичка енергија блокова чува, тачка (V, v) увек мора да лежи на тој елипси. Између судара брзине блокова се не мењају, па тачка мирује у равни брзина. При сваком судару брзине се мењају, а тачка прелази на друго место на истој елипси.

Полуосе елипсе одређујемо из њених пресека са координатним осама. За $v = 0$ добијамо $V = \pm\sqrt{2E/M}$, док за $V = 0$ добијамо $v = \pm\sqrt{2E/m}$. Према томе, однос вертикалне и хоризонталне полуосе износи $\sqrt{M/m}$. Пошто је $M \geq m$, елипса је издужена у вертикалном правцу, а за једнаке масе постаје кружница.

Са порастом енергије обе полуосе расту сразмерно $\sqrt{E}$, док њихов однос, а самим тим и облик елипсе, остаје непромењен.

1.6 Од елипсе до кружнице

У броју судара појавио се број π, који најчешће срећемо у геометрији круга. Покушајмо зато да елипсу претворимо у кружницу. За разлику од елипсе са неједнаким полуосама, кружница се не мења при ротацији око свог центра, без обзира на угао ротације. Управо ту симетрију желимо да искористимо, у складу са саветом из §1.2.

Елипсу можемо претворити у кружницу тако што ћемо променити размеру координатних оса. Брзину сваког блока помножићемо квадратним кореном његове масе и тако увести нове координате:

$$x = \sqrt{M}\,V, \qquad y = \sqrt{m}\,v \tag{1.4}$$

Тада закон одржања енергије гласи

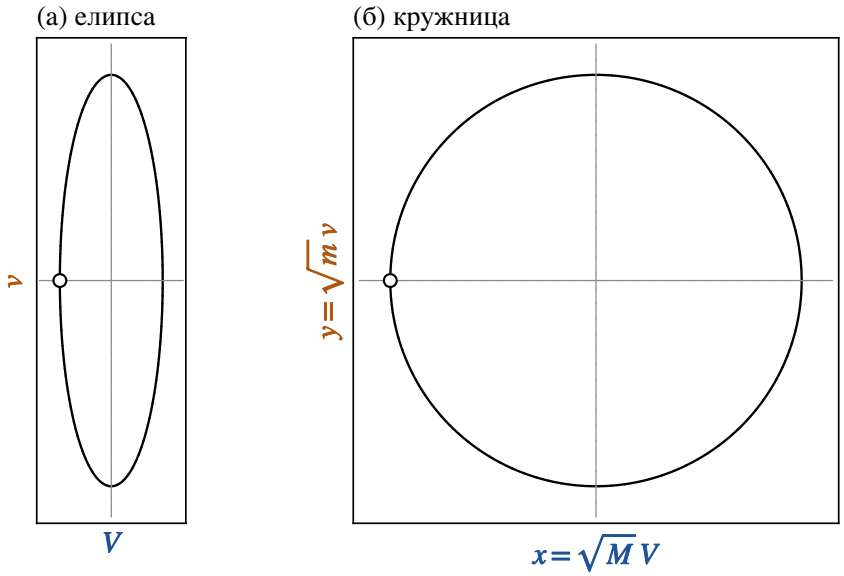
$$x^2 + y^2 = MV^2 + mv^2 = 2E \tag{1.5}$$

па тачка (x, y) лежи на кружници полупречника $R = \sqrt{2E}$ (Слика 1.2б). За разлику од претходне равни (V, v), сада користимо **раван скалираних брзина**, са координатама (x, y). У наставку ћемо сударе представљати у тој равни.

На почетку је $v = 0$ и $V = -V_0$, па је $E = MV_0^2/2$ и полупречник кружнице

$$R = \sqrt{2E} = \sqrt{M}\,V_0.$$

Кружница, дакле, не мора бити јединична. Ради једноставнијег цртања можемо обе координате поделити са R и добити кружницу полупречника 1. Таква промена размере не мења углове ни геометријску конструкцију; у једначинама и даље користимо првобитне координате x и y.



Слика 1.2. $M/m = 16$. (а) У равни (V, v) једначина одржања енергије $MV^2 + mv^2 = 2E$ описује елипсу чија је вертикална полуоса четири пута већа од хоризонталне. (б) Са $x = \sqrt{M}\,V$ и $y = \sqrt{m}\,v$ иста једначина описује кружницу $x^2 + y^2 = 2E$. Бели кружић је почетак: мали блок мирује, а велики блок иде ка зиду.

1.7 Права сталног импулса

Погледајмо како у новим координатама изгледа закон одржања импулса. Импулс је

$$MV + mv = \sqrt{M}\,(\sqrt{M}\,V) + \sqrt{m}\,(\sqrt{m}\,v) = \sqrt{M}\,x + \sqrt{m}\,y,$$

па закон одржања импулса гласи

$$\sqrt{M}\,x + \sqrt{m}\,y = p \tag{1.6}$$

За задату вредност импулса p, ова једначина описује праву у равни (x, y). Њен нагиб износи $-\sqrt{M/m}$, а називаћемо је **правом сталног импулса**, или краће правом импулса.

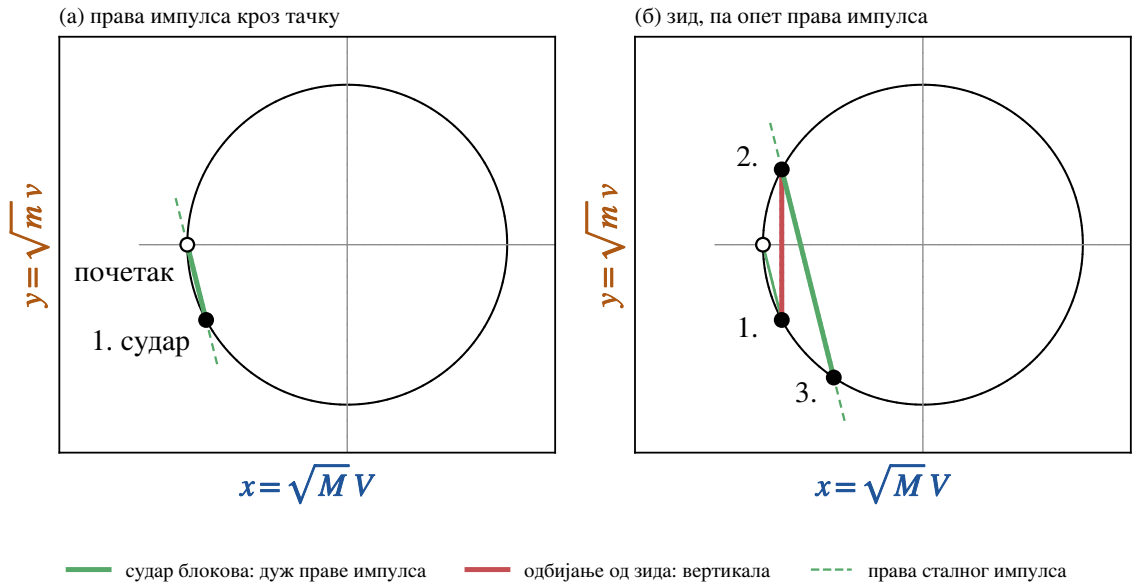
При међусобном судару блокова чувају се и кинетичка енергија и укупан импулс. Зато тачке које представљају брзине пре и после судара морају лежати на истој кружници и на истој правој сталног импулса. При судару у коме се брзине мењају, права сече кружницу у две различите тачке: једна представља брзине пре судара, а друга после њега. **Да бисмо одредили брзине после судара, довољно је да пронађемо други пресек праве сталног импулса са кружницом.**

Пошто мали блок на почетку мирује, $y = 0$, а велики се креће ка зиду, $x < 0$, почетне брзине представљене су крајњом левом тачком кружнице. Кроз њу повучемо праву сталног импулса. Њен други пресек са кружницом представља брзине после првог судара блокова (Слика 1.3а).

Следећи судар је одбијање малог блока од зида. Пошто је судар савршено еластичан, брзина малог блока мења знак, $v \to -v$, док се брзина великог блока не мења. У новим координатама то значи да x остаје исто, а y мења знак. Зато су брзине пре и после одбијања представљене двема тачкама кружнице које леже на истој вертикали (Слика 1.3б). У геометријском приказу повезаћемо их вертикалном дужи.

Поступак се затим понавља: међусобни судар блокова представљамо дужи на правој сталног импулса, а одбијање од зида вертикалном дужи. Све праве сталног импулса имају исти нагиб, $-\sqrt{M/m}$, јер он зависи само од односа маса. Различите вредности импулса одређују различите, међусобно паралелне праве.

Видећемо да овај нагиб одређује геометрију поступка, а самим тим и укупан број судара. У четвртом поглављу исти однос маса повезаћемо са Гроверовим алгоритмом.



Слика 1.3. $M/m = 16$, кружница полупречника 1. (а) Судар блокова: тачке пре и после судара повезане су дужи на правој сталног импулса, нагиба -4. (б) Одбијање од зида мења само y: одговарајуће тачке повезане су вертикалном дужи. Затим следи нова права сталног импулса. Бројеви су редни бројеви судара.

1.8 Када судари престају

Пошто се мали блок налази лево од великог, брзина промене растојања између њих износи $V-v$. Блокови се приближавају када је $V < v$, а удаљавају када је $V > v$. Ако је $V = v$, растојање између њих остаје непромењено. Судар са зидом могућ је само ако се мали блок креће ка зиду, $v < 0$.

После одбијања од зида мали блок се креће удесно, па не може поново да удари у зид пре него што се судари са великим блоком. С друге стране, при међусобном еластичном судару релативна брзина блокова мења знак (§1.3), тако да се блокови непосредно након судара удаљавају. Зато се, док судари трају, међусобни судари блокова и одбијања од зида наизменично смењују.

Да више не би дошло ни до судара са зидом ни до међусобног судара блокова, потребно је да се мали блок више не креће ка зиду и да велики блок не буде спорији од малог. Оба услова можемо записати једном неједнакошћу:

$$0 \le v \le V \tag{1.7}$$

У таквом стању мали блок мирује или се креће од зида, док велики блок има брзину удесно бар једнаку брзини малог. Зато више не може доћи ни до једне врсте судара. Скуп свих таквих

стања назваћемо **завршном облашћу**. У следећем одељку показаћемо како она изгледа у равни скалираних брзина.

1.9 Од судара до геометријског проблема

У претходном одељку показали смо да судари престају када је испуњен услов (1.7), $0 \le v \le V$. Погледајмо како овај услов изгледа у равни скалираних брзина (x, y) (Слика 1.4).

Први захтев је да мали блок више не иде ка зиду, односно $v \ge 0$. Пошто је $y = \sqrt{m}\, v$, то значи да је $y \ge 0$. Из $V \ge v \ge 0$ следи и $x \ge 0$. Завршна област зато лежи у горњем десном квадранту (Слика 1.4а).

Други захтев је да велики блок не буде спорији од малог, $V \ge v$. На граници $V = v$ блокови се крећу истом брзином, па се растојање између њих не мења. У равни обичних брзина (V, v) то је права нагиба 1, која са хоризонталном осом заклапа угао од 45° (Слика 1.4б).

У равни скалираних брзина свака брзина је помножена квадратним кореном одговарајуће масе. Зато права једнаких брзина постаје:

$$V = v \qquad \Longleftrightarrow \qquad y = \sqrt{\frac{m}{M}}\, x.$$

То је **права једнаких брзина** (Слика 1.4в). Пошто координату тежег блока множимо већим кореном, права се приближава x-оси: за $M/m = 16$ њен нагиб је 1/4, а за $M/m = 100$ само 1/10.

Оба услова заједно одређују **завршну област**: клин између позитивног дела хоризонталне осе и праве једнаких брзина,

$$x \ge 0, \qquad 0 \le y \le \sqrt{\frac{m}{M}}\, x.$$

Када тачка која представља брзине блокова уђе у овај клин, ниједан нови судар више није могућ. Ван завршне области мали блок се креће ка зиду или се растојање између блокова смањује, па ће доћи до још најмање једног судара. Што је однос маса већи, клин је ужи.

Сада имамо све што је потребно да физички проблем претворимо у геометријски. Сваки судар можемо представити дужи која повезује тачке на кружници непосредно пре и после судара. Међусобном судару блокова одговара дуж на правој сталног импулса, док одбијању од зида одговара вертикална дуж. Сваки судар тако представљамо једном дужи, па се питање о укупном броју судара своди на бројање дужи.

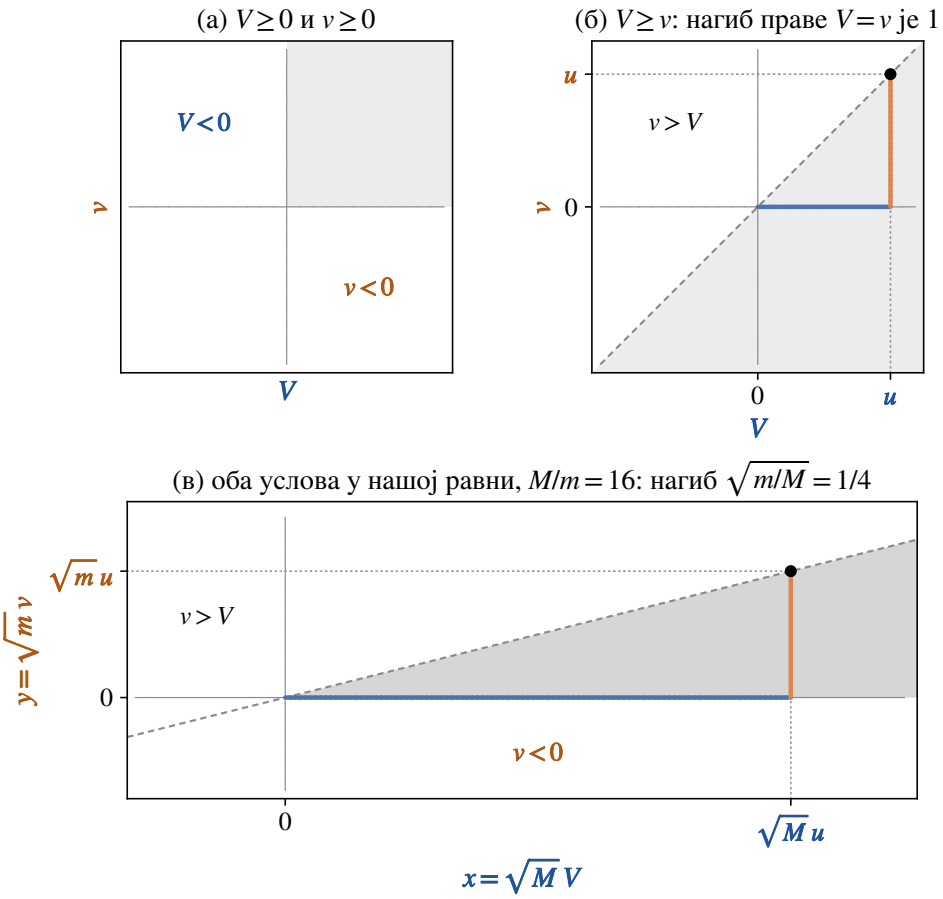
Геометријска поставка

Почните у крајњој левој тачки кружнице. Кроз њу повуците праву сталног импулса, нагиба $-\sqrt{M/m}$, и спојте почетну тачку са другим пресеком те праве и кружнице.

Из нове тачке повуците вертикалну дуж до другог пресека са кружницом. Затим наизменично понављајте ова два корака, све док не стигнете до завршне области.

Питање: колико дужи можемо нацртати пре него што стигнемо до завршне области? Тај број једнак је укупном броју судара.

За $M/m = 100$ ова конструкција даје 31 дуж, односно 31 судар (Слика 1.5б). Нагиб праве сталног импулса зависи само од односа маса, док почетна брзина V_0 одређује полупречник кру-



Слика 1.4. Где је завршна област. (а) Ниједна брзина није негативна у горњем десном квадранту (светлосиво); испод осе мали блок иде ка зиду, а лево од осе велики. (б) Велики блок није спорији од малог, $V \geq v$, испод праве $V = v$. До тачке у којој оба блока имају брзину u стижемо кораком u удесно (плаво) и u нагоре (наранџасто), па је нагиб те праве 1. (в) У нашој равни иста тачка је $(\sqrt{M}\,u, \sqrt{m}\,u)$, па права једнаких брзина има нагиб $\sqrt{m/M}$, за $M/m = 16$ баш 1/4. Оба услова заједно дају уски сиви клин, завршна област са Слике 1.5.

жнице:

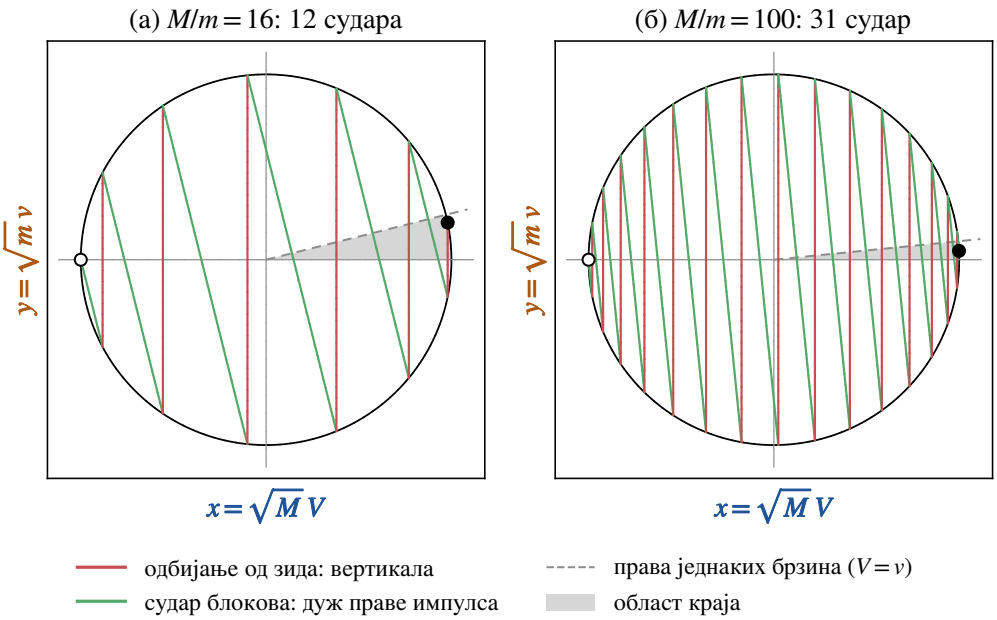
$$R = \sqrt{2E} = \sqrt{M}\,V_0.$$

Ако променимо почетну брзину, кружница ће постати већа или мања, али ће сви углови остати исти. Зато се не мења ни број дужи које можемо нацртати, односно број судара. **Укупан број судара зависи само од односа маса M/m, а не од почетне брзине.**

1.10 Једнаки лукови

Сада треба да пребројимо дужи које представљају сударе. Уместо њих, бројаћемо лукове кружнице између тачака добијених конструкцијом. Показаћемо да сваком од лукова које бројимо одговара исти централни угао $2\bar{\theta}$. Пошто сви леже на истој кружници, једнаки централни углови значе и једнаке дужине лукова; преостали лук који затвара кружницу може бити краћи (Слика 1.6).

Лук коме одговара централни угао $\Delta\varphi$, изражен у радијанима, на кружници полупречника R има дужину $R\Delta\varphi$. Зато је дужина лука са углом $2\bar{\theta}$ једнака $2R\bar{\theta}$. У наставку ћемо лукове означавати њиховим централним угловима; на јединичној кружници ти бројеви су једнаки



Слика 1.5. Све дужи у равни скалираних брзина. Зелене су судари блокова (дуж правих импулса), а црвене одбијања од зида (вертикале). (а) $M/m = 16$, нагиб -4: 12 дужи. (б) $M/m = 100$, нагиб -10: 31 дуж. Бели кружић је почетак, а црни крај. Сиво је завршна област, $0 \le v \le V$, а испрекидана сива права је њена горња ивица, права једнаких брзина (Слика 1.4).

и дужинама лукова.

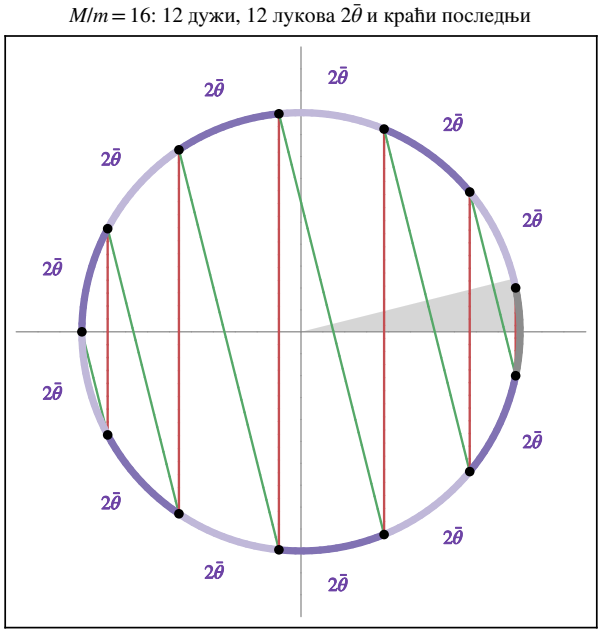
Зашто су углови исти? Свака коса дуж лежи на правој нагиба $-\sqrt{M/m}$, а свака друга дуж је вертикална. Зато свака коса и свака вертикална дуж које се сустичу у истој тачки заклапају **исти угао**; зовемо га $\bar{\theta}$. Тај угао зависи само од нагиба, тј. од односа маса; колики је, израчунаћемо у §1.12.

Узмимо три узастопне тачке, P_1, P_2 и P_3 (Слика 1.7). У средњој, P_2, сустичу се једна вертикална и једна коса дуж. Обе иду из P_2 на исту страну, обе нагоре или обе надоле, па је угао међу њима оштар, баш $\bar{\theta}$. Тај угао има теме на кружници, па је **периферијски угао** над луком P_1P_3 који не садржи P_2. Из школе знамо **теорему о централном и периферијском углу**: периферијски угао једнак је половини централног угла над истим луком (доказ је у Додатку Б). Зато је лук P_1P_3 једнак $2\bar{\theta}$, и то за сваке три узастопне тачке: свака тачка лежи $2\bar{\theta}$ даље од почетка него тачка два судара пре ње. Сви лукови су, дакле, по $2\bar{\theta}$, осим лука између последње две тачке.

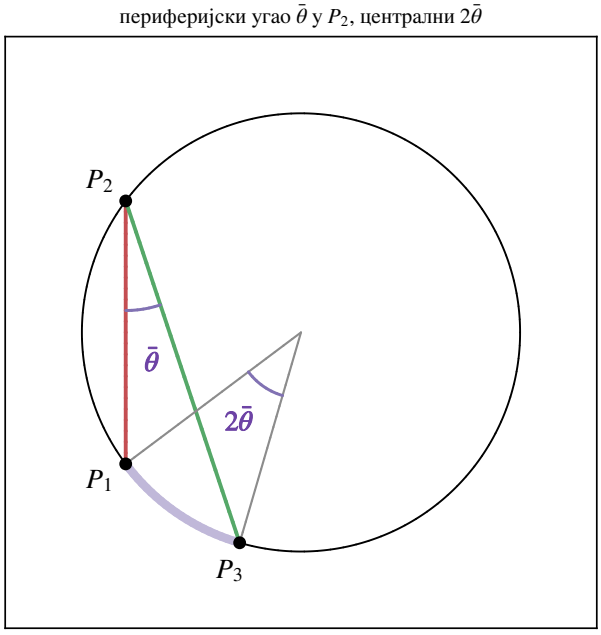
Исто важи за сваки лук (Слика 1.8). Тачке нумеришемо редом судара; почетак је тачка 0. Свака тачка осим почетне и последње је теме једног периферијског угла $\bar{\theta}$, између вертикалне и косе дужи које се у њој сустичу. Тај угао гледа на лук између претходне и следеће тачке, па је сваки такав лук $2\bar{\theta}$. Само први лук, од тачке 0 до тачке 1, нема свој угао, али и он је $2\bar{\theta}$: тачке 1 и 2 леже на истој вертикали, симетрично у односу на x-осу, а почетак лежи на x-оси, па су лукови од почетка до тачке 1 и до тачке 2 једнаки.

1.11 Колико лукова стаје на кружницу

Лукови са централним углом $2\bar{\theta}$ нижу се око кружнице на обе стране од почетка, док не стигну до завршне области. За сваки судар добијамо један такав лук, а уз завршну област остаје још један, који затвара кружницу. Судари престају чим тачка стигне у завршну област, укључујући и њену границу, па преостали лук не бројимо као судар. Зато бројање не укључује лук



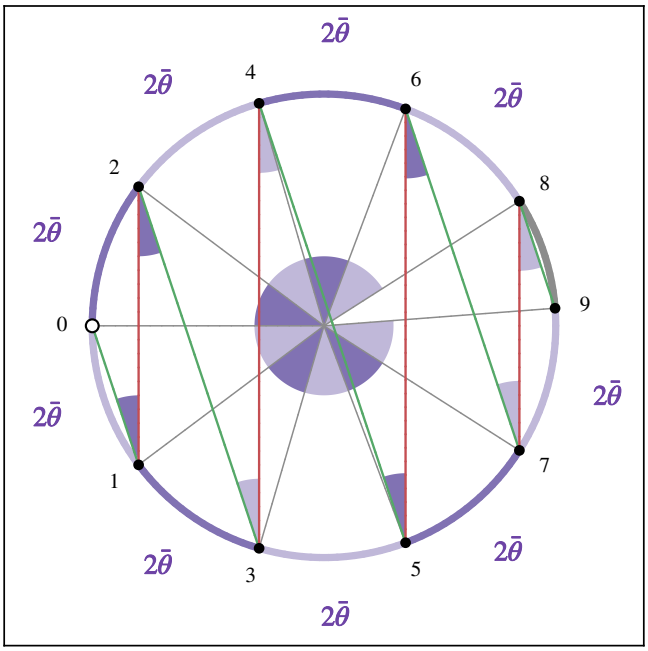
Слика 1.6. $M/m = 16$, нагиб -4: свих 12 дужи и њихових 13 тачака на кружници. Тачке деле кружницу на 12 једнаких лукова $2\bar{\theta}$, у две нијансе љубичасте, и крађи последњи лук, сив, уз завршну област.



Слика 1.7. Зашто су лукови једнаки. P_1 је тачка пре одбијања од зида, P_2 после њега, а P_3 после следећег судара блокова. Периферијски угао у P_2 је $\bar{\theta}$, па је централни угао над луком P_1P_3 (светлољубичасто) $2\bar{\theta}$. Нацртано за $M/m = 9$, где је $\bar{\theta} = 18{,}4°$, да би се углови јасно видели.

који би затворио круг. Ова строга граница следи и из конструкције у Додатку А: тамо судари одговарају само правцима $j\bar{\theta}$ строго између 0 и π; правац π зрак не пресеца.

Ако је полупречник кружнице R, дужина сваког лука који бројимо је $2R\bar{\theta}$, а обим кружнице $2\pi R$. Број судара је највећи број таквих лукова који стају пре затварања круга. Зато за број



Слика 1.8. Конструкција из Слике 1.7 примењена на све лукове, за $M/m = 9$. Тачке су нумерисане редом судара, а 0 је почетак. У свакој тачки од 1 до 8 мали клин је периферијски угао $\bar{\theta}$ између вертикалне и косе дужи; он гледа на лук између претходне и следеће тачке, обојен истом нијансом љубичасте. Исту нијансу има централни угао тог лука, у средишту, између два сива полупречника: $2\bar{\theta}$. Први лук, од 0 до 1, једнак је луку од 0 до 2 по симетрији, а преостали, сив, може бити краћи.

судара N важи

$$N \cdot 2R\bar{\theta} < 2\pi R, \qquad \text{тј.} \qquad N\bar{\theta} < \pi.$$

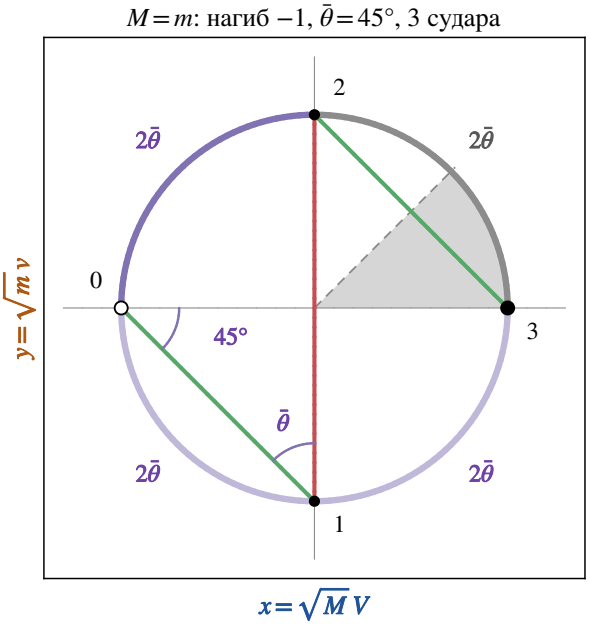
Пошто је $R > 0$, полупречник се скраћује: резултат не зависи од величине кружнице. Углове меримо у радијанима, па је цео круг 2π, а π радијана је 180° (Додатак Б). Број судара је **највећи цео број N за који је** $N\bar{\theta} < \pi$. Неједнакост је строга. За $M = m$ нагиб је -1, па коса дуж са вертикалом заклапа угао од 45°: $\bar{\theta} = \pi/4$ и $4\bar{\theta} = \pi$ тачно, а судара има 3, не 4. Ако са $\lceil q \rceil$ означимо најмањи цео број који није мањи од q (заокруживање навише), онда целих бројева $N \geq 1$ са $N < q$ има $\lceil q \rceil - 1$, јер је $\lceil q \rceil - 1 < q \leq \lceil q \rceil$. Са $q = \pi/\bar{\theta}$:

$$\text{број судара} = \left\lceil \frac{\pi}{\bar{\theta}} \right\rceil - 1 \tag{1.8}$$

За $M = m$ је $\pi/\bar{\theta} = 4$, па судара има $\lceil 4 \rceil - 1 = 3$.

Погледајмо цео цртеж за $M = m$ (Слика 1.9). Ради једноставности користимо јединичну кружницу. Права импулса тада има нагиб -1, па са обема осама заклапа угао од 45°. Зато је и угао између косе дужи и вертикале $\bar{\theta} = 45°$, а лук $2\bar{\theta}$ је четвртина круга. Тачка креће из $(-1, 0)$: велики блок иде ка зиду, а мали мирује. Први судар блокова представља коса дуж до тачке $(0, -1)$: блокови једнаких маса размене брзине, па велики стане, а мали крене ка зиду. Одбијање од зида представља вертикала до тачке $(0, 1)$: мали се враћа истом брзином. Други судар блокова представља коса дуж до тачке $(1, 0)$: мали стане, а велики оде од зида. Тачка $(1, 0)$ лежи на доњој ивици завршне области, јер мали мирује, па цртање ту стаје. **Три дужи, три судара.**

Исто се види и бројањем лукова. Четири тачке, 0, 1, 2 и 3, деле кружницу на четири четвртине. Три су положене од почетка, по једна за сваки судар, а четврта би затворила цео круг. Да бисмо имали четири судара, требало би да буде $4\bar{\theta} < \pi$, а овде је $4\bar{\theta} = \pi$ тачно: неједнакост је строга, па судара има 3, а не 4.



Слика 1.9. $M = m$. Права импулса има нагиб -1, па коса дуж са x-осом заклапа угао од 45° (у тачки 0), а са вертикалом угао $\bar{\theta} = 45°$ (у тачки 1). Тачка иде из 0 у 1 (судар блокова), из 1 у 2 (одбијање од зида) и из 2 у 3 (опет судар блокова), где је завршна област. Тачке деле кружницу на четири лука $2\bar{\theta} = 90°$: три су положена од почетка (у две нијансе љубичасте), а четврти, сиви, затворио би круг. Зато судара има 3.

1.12 Цифре броја π

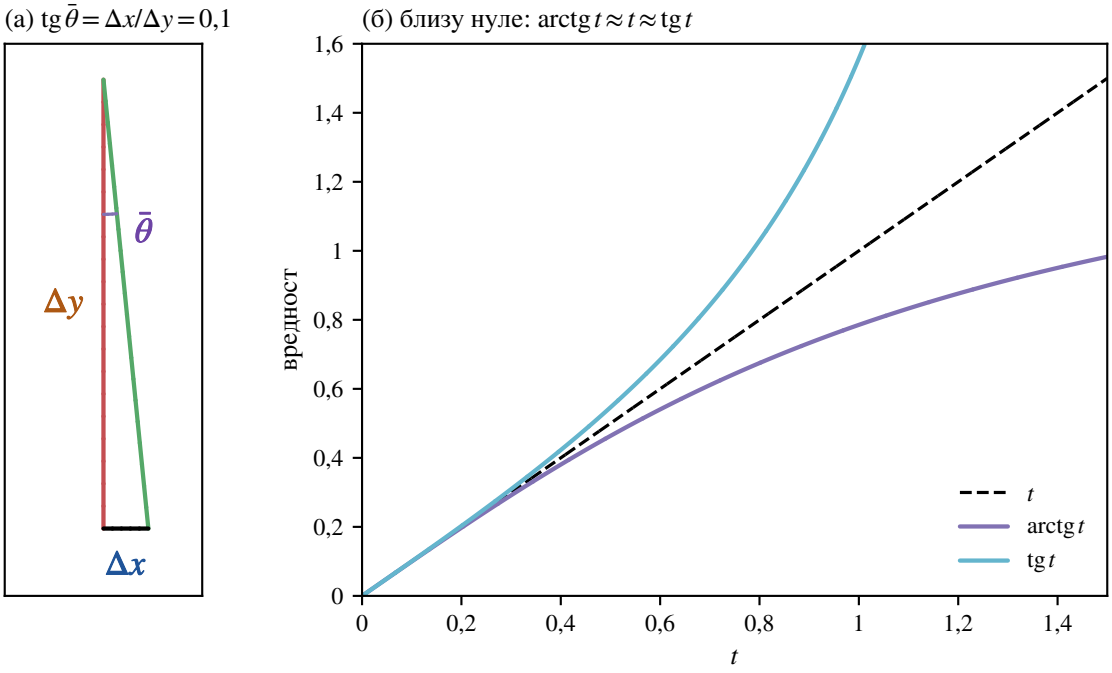
Сада имамо све делове. По (1.8) број судара зависи само од угла $\bar{\theta}$: колико пута лук $2\bar{\theta}$ стане у круг. Остаје да $\bar{\theta}$ израчунамо из маса и да видимо зашто се у одговору појављују цифре броја π. Идемо корак по корак.

Угао из нагиба. Посматрајмо правоугли троугао који коса дуж образује са вертикалним и хоризонталним правцем (Слика 1.10а). Његове катете имају дужине Δy и Δx. Нагиб косе дужи је $-\Delta y/\Delta x = -\sqrt{M/m}$. Пошто се угао $\bar{\theta}$ налази између косе дужи и вертикале, његов тангенс је количник $\Delta x/\Delta y$:

$$\operatorname{tg}\bar{\theta} = \frac{\Delta x}{\Delta y} = \sqrt{\frac{m}{M}} \tag{1.9}$$

Узмимо два примера са цртежа. За $M = m$ је $\operatorname{tg}\bar{\theta} = 1$, па је $\bar{\theta} = 45° = \pi/4$, а судара има 3 (Слика 1.9). За $M/m = 16$ је $\operatorname{tg}\bar{\theta} = 1/4$, па је $\bar{\theta} \approx 0{,}2450$, око 14,04°. Тада је $\pi/\bar{\theta} \approx 12{,}82$, и по (1.8) судара има 12 (Слика 1.5а).

Мисаони оглед: угао је степен броја 10. Замислимо на тренутак да је $\bar{\theta}$ тачно 0,1. Број судара



Слика 1.10. (а) За $M/m = 100$ је $\operatorname{tg}\bar\theta = \Delta x/\Delta y = 0{,}1$: уски троугао између вертикалне дужи (зид) и косе (судар блокова). (б) Близу нуле се $\operatorname{arctg} t$, t и $\operatorname{tg} t$ скоро поклапају, па је $\bar\theta = \operatorname{arctg} 0{,}1 \approx 0{,}1$.

је највећи цео број N за који је $N\bar\theta < \pi$, тј. највећи цео број мањи од $\pi/\bar\theta$:

$$\frac{\pi}{0{,}1} = 31{,}4159\ldots \qquad \Longrightarrow \qquad N = 31.$$

Дељење са 0,1 само помера децималну запету за једно место удесно. Дељење са 0,01 помера је за два места, а са 0,001 за три:

$$\frac{\pi}{0{,}01} = 314{,}159\ldots \implies N = 314, \qquad \frac{\pi}{0{,}001} = 3141{,}59\ldots \implies N = 3141.$$

Ако је $\bar\theta$ степен броја 10, број судара је, дакле, π без децималне запете, одсечен после онолико децимала колико цифара има $\bar\theta$ иза запете: то су **цифре броја** π. Остају два питања. Који однос маса даје такав угао? И да ли је угао тада заиста тачно степен броја 10?

Који однос маса. По (1.9) масе одређују тангенс угла, $\operatorname{tg}\bar\theta = \sqrt{m/M}$. Да би тангенс био 0,1, мора бити $m/M = 0{,}01$, тј. $M/m = 100$. Да би био 0,01, мора бити $M/m = 10\,000 = 100^2$. Уопште, за цео број $D \geq 0$ (колико цифара броја π после запете желимо да добијемо) због корена важи

$$\operatorname{tg}\bar\theta = 0{,}1^D \qquad \Longleftrightarrow \qquad \frac{M}{m} = 100^D.$$

Однос маса мора бити степен броја 100, а не 10: корен преполови изложилац. За $M/m = 1000$ је $\operatorname{tg}\bar\theta = 10^{-1{,}5} \approx 0{,}0316$, а судара има 99; за $M/m = 10^5$ има их 993. То нису цифре броја π, него броја $\pi\sqrt{10} = 9{,}93\ldots$

Тангенс није угао. До сада смо посматрали случај у коме је угао тачно 10^{-D}. Међутим, однос маса одређује тангенс угла, а не сам угао. За $M/m = 100$ тачно је $\operatorname{tg}\bar\theta = 0{,}1$, а не $\bar\theta = 0{,}1$. Сам угао је мало мањи: $\bar\theta = \operatorname{arctg} 0{,}1 = 0{,}09967\ldots$ Ту помаже **апроксимација малог угла**

(Слика 1.10б; више у Додатку Б). За мали угао t (у радијанима, на пример $t = 0{,}001$) је

$$\operatorname{arctg} t \approx t \approx \operatorname{tg} t \tag{1.10}$$

Колико је угао мањи од тангенса, и да ли то мења број судара? Табела 1.3 даје бројеве судара и заокружене вредности угла и количника. За $D \geq 1$ угао је мало мањи од тангенса, па је $\pi/\bar{\theta}$ мало већи од $\pi \cdot 10^D$: 31,52 уместо 31,42; 314,170 уместо 314,159. Вишак је око 0,10 за $D = 1$, 0,010 за $D = 2$ и 0,0010 за $D = 3$. У овим примерима количник не стиже до следећег целог броја, па број судара остаје 31, 314 и 3141. Сама апроксимација, међутим, не гарантује такво поклапање за свако D.

M/m	$\operatorname{tg}\bar{\theta}$	$\bar{\theta}$	$\pi/\bar{\theta}$	**број судара**
1	1	0,785398	4	3
100	0,1	0,0996687	31,5204	31
10^4	0,01	0,00999967	314,1697	314
10^6	0,001	0,000999999667	3141,5937	3141

Табела 1.3. Тангенс, угао и број судара за степене броја 100. Бројеви судара су тачни, а вредности угла и количника су, где је потребно, заокружене. У приказаним примерима са $D \geq 1$ угао је мало мањи од тангенса, па је $\pi/\bar{\theta}$ мало већи од $\pi \cdot 10^D$, али се цео део не мења. За $D = 0$, тј. $M = m$, угао је знатно мањи и $\pi/\bar{\theta} = 4$, а судара има 3 због строге неједнакости из §1.11.

Цела слика. Скупимо све. Из (1.8) и (1.9) тачан број судара је

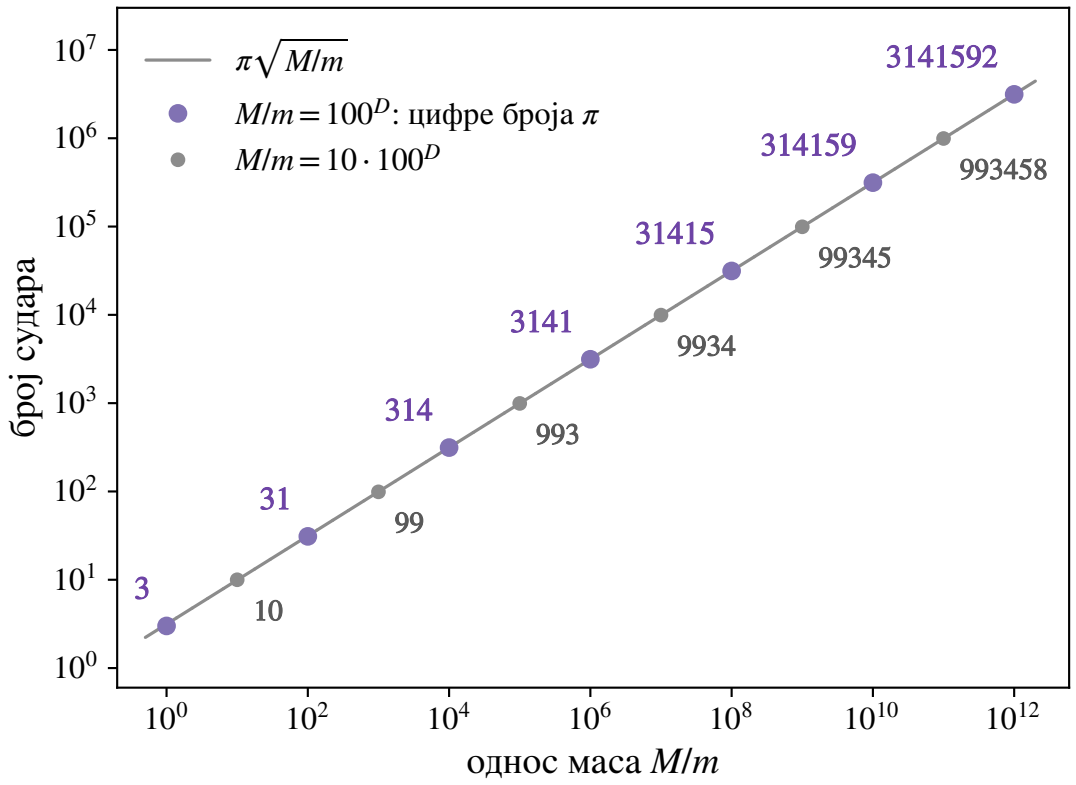
$$N = \left\lfloor \frac{\pi}{\operatorname{arctg}\sqrt{m/M}} \right\rfloor - 1.$$

За велик однос маса угао је приближно једнак свом тангенсу, $\sqrt{m/M}$, па је

$$\text{број судара} \approx \pi\sqrt{\frac{M}{m}} \tag{1.11}$$

За $M/m = 100^D$ то је $\pi \cdot 10^D$: блок 100 пута тежи даје 31 судар, 10 000 пута тежи 314, а милион пута тежи 3141 (Слика 1.11). Што је однос маса већи, лукови од $2\bar{\theta}$ су ситнији, а у круг их стане све више. **Лукови исписују π, а судари их броје.**

Када се цифре не поклапају. Разлика између $\pi/\operatorname{arctg}(10^{-D})$ и $\pi \cdot 10^D$ све је мања, али то само по себи не доказује да су им цели делови увек једнаки: први број ипак може прећи следећи цео број ако му је други довољно близу. Галперин у свом раду [4] поставља хипотезу да за природне $D \geq 1$ важи $\lfloor \pi/\operatorname{arctg}(10^{-D}) \rfloor = \lfloor \pi \cdot 10^D \rfloor$. Он разматра и повезан услов о низу деветки после D-те децимале. Та тврдња остаје хипотеза; малена разлика није сама по себи доказ поклапања свих цифара.



Слика 1.11. Број судара за $M/m = 10^k$, $k = 0, 1, \ldots, 12$, из симулације, и права $\pi\sqrt{M/m}$ из (1.11); обе осе су логаритамске. Љубичасте тачке, $M/m = 100^D$, дају цифре броја π: 3, 31, 314, ... Сиве, $M/m = 10 \cdot 100^D$, дају од $M/m = 1000$ цифре броја $\pi\sqrt{10} = 9{,}93\ldots$: 99, 993, 9934, ...

Најважније из поглавља

1. Закони одржања. Кинетичка енергија два блока чува се при свим сударима. Укупан импулс чува се при међусобном судару, али не и при одбијању од зида, који делује спољашњом силом:

$$E = \frac{mv^2}{2} + \frac{MV^2}{2}, \qquad p = mv + MV.$$

2. Од елипсе до кружнице. Пар брзина (V, v) представљамо тачком на елипси $MV^2 + mv^2 = 2E$. Са $x = \sqrt{M}\,V$ и $y = \sqrt{m}\,v$ добијамо кружницу $x^2 + y^2 = 2E$. Њен полупречник је $R = \sqrt{2E} = \sqrt{M}\,V_0$; кружница не мора бити јединична.

3. Приказ судара. Међусобни судар представљамо дужи на правој сталног импулса $\sqrt{M}\,x + \sqrt{m}\,y = p$, нагиба $-\sqrt{M/m}$. Одбијање од зида представљамо вертикалном дужи: мења се знак y. Дужи повезују тачке пре и после судара, а не приказују путање блокова.

4. Завршна област. Судари престају када је $0 \le v \le V$: мали блок не иде ка зиду, а велики му се не приближава. У равни скалираних брзина то је клин $x \ge 0$, $0 \le y \le \sqrt{m/M}\,x$.

5. Једнаки лукови. Сваком судару одговара један од лукова са централним углом $2\bar{\theta}$, где је $\operatorname{tg}\bar{\theta} = \sqrt{m/M}$. На кружници полупречника R дужина таквог лука је $2R\bar{\theta}$.

6. Тачан број судара. Број судара N највећи је цео број за који је $N\bar{\theta} < \pi$, па је

$$N = \left\lceil \frac{\pi}{\bar{\theta}} \right\rceil - 1.$$

Полупречник се скраћује при поређењу лукова са обимом, па број судара не зависи од почетне брзине. За једнаке масе је $\bar{\theta} = \pi/4$, а судара има три, јер је неједнакост строга.

7. Цифре броја π. За велики однос маса је $\bar{\theta} = \operatorname{arctg}\sqrt{m/M} \approx \sqrt{m/M}$, па је $N \approx \pi\sqrt{M/m}$. За $M/m = 100^D$ приближно добијамо $\pi 10^D$. Поклапање свих очекиваних цифара за произвољно D није доказано самом апроксимацијом; Галперинову хипотезу описали смо у §1.12.

Кључна идеја: Закони одржања омогућавају да сударе представимо геометријски и пребројимо помоћу једнаких лукова. Иза те геометрије стоје огледања која ћемо касније повезати са Гроверовим алгоритмом.

1.13 Задаци

Задаци за самосталан рад

Задаци у овом поглављу намењени су увежбавању закона одржања, рачунања брзина после еластичних судара и њиховог геометријског приказа. Почећемо од једноставнијих примера са неколико судара, а затим прећи на раван брзина, геометрију кружнице и одређивање укупног броја судара. Последњи задаци посвећени су вези са бројем π и проширењима проблема.

Закони одржања и еластични судари (§1.1–§1.4)

Задатак 1. Избројте сударе за $M = m$ без формуле, а затим проверите одговор формулом (1.8). *Упутство: у еластичном судару једнаке масе размене брзине.*

Задатак 2. Избројте сударе за $M = 3m$, ако мали блок на почетку мирује, а велики иде ка зиду са износом почетне брзине $V_0 = 1$. *Упутство: рачунајте брзине после сваког судара по (1.2).*

Задатак 3. Покажите да се формуле (1.2) могу написати као $v' = 2v_{\mathrm{cm}} - v$ и $V' = 2v_{\mathrm{cm}} - V$, где је $v_{\mathrm{cm}} = (mv + MV)/(m + M)$ брзина центра масе. *Упутство: сведите $2v_{\mathrm{cm}} - v$ на заједнички именилац.*

Задатак 4. Мали блок масе $m = 1$ мирује, а велики блок масе $M = 3$ креће се ка њему брзином $V = -4$. Израчунајте брзине после међусобног еластичног судара и проверите укупну кинетичку енергију и импулс пре и после судара. *Упутство: користите (1.2).*

Задатак 5. Мали блок масе $m = 2$ удара у непокретан зид брзином $v = -3$ и савршено еластично се одбија. Одредите његову брзину после удара, промену импулса и кинетичку енергију пре и после удара.

Задатак 6. Мали блок је између зида и великог блока. За сваки пар брзина $(v,V) = (-2,1)$, $(2,-1)$ и $(1,2)$ одредите да ли је следећи судар са зидом, између блокова, или даљих судара нема.

Раван брзина и геометријски приказ (§1.5–§1.9)

Задатак 7. Нека су $m = 1$, $M = 4$ и укупна кинетичка енергија $E = 8$. Запишите једначину елипсе у равни (V,v), одредите њене полуосе и полупречник кружнице у равни (x,y). Која тачка на кружници одговара брзинама $(V,v) = (-2,0)$?

Задатак 8. За $M/m = 16$ одредите нагиб праве сталног импулса и нагиб праве једнаких брзина

у равни (x,y). Проверите да су те праве нормалне једна на другу.

Задатак 9. За $m = 1$, $M = 4$ и брзине $(V,v) = (-1,-2)$ израчунајте E, координате (x,y) и полупречник кружнице. Која тачка представља брзине после одбијања малог блока од зида?

Задатак 10. За парове брзина $(v,V) = (0,2)$, $(2,1)$, $(-1,3)$ и $(1,1)$ одредите који припадају завршној области. За остале наведите да ли мали блок иде ка зиду или се блокови приближавају. *Упутство: користите (1.7).*

Задатак 11. Уз непромењене масе удвостручимо износ почетне брзине великог блока. Како се мењају почетна енергија, полупречник кружнице и број судара? Објасните шта се дешава са угловима геометријске конструкције.

Углови, лукови и број судара (§1.10–§1.12)

Задатак 12. Колико целих бројева $j \geq 1$ испуњава услов $0{,}3\,j < 1$, а колико услов $0{,}25\,j < 1$? Проверите оба одговора правилом бројања из §1.11.

Задатак 13. Периферијски угао над једним луком износи $15°$. Одредите одговарајући централни угао и дужину лука ако је полупречник кружнице $R = 3$. *Упутство: угао за рачунање дужине лука изразите у радијанима.*

Задатак 14. Примените тачну формулу (1.8) за $\bar{\theta} = \pi/4$, $\pi/6$ и 0,2 радијана. Објасните зашто у прва два случаја број судара није једнак количнику $\pi/\bar{\theta}$.

Задатак 15. Колико судара има за $M/m = 16$, а колико за $M/m = 10^6$? *Упутство:* $\operatorname{tg}\bar{\theta}$ *је* $1/4$, *односно* 10^{-3}*; угао рачунајте у радијанима.*

Задатак 16. За $M/m = 100$ упоредите тачан број судара са приближном вредношћу $\pi\sqrt{M/m}$. Колика је њихова разлика?

Цифре броја π и додатни изазови

Задатак 17. За односе маса $M/m = 100^D$ добијамо бројеве судара 3, 31, 314, 3141, …, који садрже почетне цифре броја π у декадном запису (§1.12).

Нађите број a такав да однос маса $M/m = a^D$ на сличан начин даје почетне цифре броја π у бинарном запису, $\pi = (11{,}001001000011\ldots)_2$. Израчунајте број судара за $D = 0,1,2,3$, запишите га бинарно и упоредите са записом броја π. Који однос маса даје цифре у систему са основом 3?

Упутство: по (1.11) судара има приближно $\pi\sqrt{M/m}$*; множење са* 10^D *помера децималну запету за* D *места, а множење са* 2^D *бинарну запету.*

Задатак 18. За бројевни систем са основом $b \geq 2$ одредите однос маса облика $M/m = a^D$ који би по приближној формули померио запис броја π за D места. Објасните зашто ова апроксимација сама по себи не гарантује поклапање цифара за свако D.

Задатак 19. За $t = 0{,}1$ израчунајте $\operatorname{arctg} t$, π/t и $\pi/\operatorname{arctg} t$. Заокружите резултате на четири децимале и упоредите целе делове последња два броја.

Задатак 20. *Додатни изазов.* Бројеви 2,999 и 3,001 разликују се за само 0,002. Одредите њихове целе делове и објасните зашто мала разлика између $\pi \cdot 10^D$ и $\pi/\operatorname{arctg}(10^{-D})$ сама по себи не доказује да су им цели делови једнаки.

2. Основе квантне механике и квантног рачунарства

Да бисмо разумели како ради Гроверов алгоритам, најпре морамо да упознамо начин на који квантна механика описује стања и њихове промене. За почетак ће нам бити довољни вектори, основна правила рачунања с њима и појам вероватноће. Рад квантног рачунара представљаћемо низом операција над векторима стања. Када усвојимо овај језик, у следећем поглављу применићемо га на претрагу.

У овом поглављу бавићемо се **чистим квантним стањима**, која представљамо векторима. Ради једноставнијег геометријског приказа ограничићемо се на реалне амплитуде. То је довољно за Гроверов алгоритам у облику који разматрамо, иако су у општој квантној механици амплитуде комплексни бројеви, а постоје и мешовита стања.

2.1 Квантно стање као вектор

Чисто квантно стање представљамо вектором. За векторе ћемо користити запис који је увео Пол Дирак [3]. У овом запису можемо представити и квантна стања и векторе из механичког проблема, што ће нам касније помоћи да уочимо њихову заједничку математичку структуру.

Вектор у равни је стрелица из координатног почетка. Описујемо га двама бројевима, **компонентама**, на пример $(3, 4)$. Векторе сабирамо по компонентама, $(a, b) + (c, d) = (a + c, b + d)$, и множимо бројем, $\lambda(a, b) = (\lambda a, \lambda b)$. Дужина вектора (a, b) је, по Питагориној теореми, $\sqrt{a^2 + b^2}$; вектор $(3, 4)$ има дужину 5. Вектор дужине 1 зовемо **јединичним**. Ништа од овога не зависи од тога да вектор има баш две компоненте. Вектор у простору има три, а требаће нам и вектори са N компоненти, где N може бити и милион. Такав вектор не можемо нацртати, али са њим рачунамо исто као у равни: сабирамо га по компонентама, множимо бројем, а дужина му је корен збира квадрата свих компоненти.

Дирак вектор пише као $|\psi\rangle$; такав запис зове се **кет**, а читамо га „кет пси“. Између усправне црте и изломљене заграде стоји име вектора, а име може бити слово, број или цела реч. Запис $|\psi\rangle$ означава вектор, баш као што у школској математици вектор можемо означити са $\vec{\psi}$. Разлика је у начину записивања, а не у правилима сабирања и множења бројем.

Најважнији вектори у равни су два јединична вектора дуж оса, нормална један на други. Зовемо их $|0\rangle$ и $|1\rangle$:

$$|0\rangle = (1, 0), \qquad |1\rangle = (0, 1).$$

Пажња: $|0\rangle$ није нула-вектор. То је јединични вектор дуж прве осе, коме је име „0“. Нула-вектор пишемо просто 0.

Сваки вектор у равни састављен је од ова два:

$$|\psi\rangle = (a, b) = a\,|0\rangle + b\,|1\rangle \tag{2.1}$$

Зато кажемо да $|0\rangle$ и $|1\rangle$ чине **базу** равни. Вектор са N компоненти има базу од N јединичних вектора, по један дуж сваке осе. Осе ћемо обележавати словом i, базне векторе писати $|i\rangle$, а компоненту вектора $|\psi\rangle$ дуж осе i писати a_i.

Погледајмо шта овај математички опис значи у квантној механици. Изаберимо мерење са N могућих **исхода**. Сваком исходу i придружићемо један базни вектор $|i\rangle$; различитим исходима одговарају различити базни вектори, нормални један на други. У тој изабраној бази представљаћемо стања и рачунати вероватноће исхода. Најједноставнији пример је **кубит**: за мерење у бази $|0\rangle$, $|1\rangle$ могући исходи су 0 и 1.

2.2 Суперпозиција и амплитуде

Стање система не мора да буде један базни вектор. Може бити збир базних вектора, сваки помножен својим бројем:

$$|\psi\rangle = \sum_i a_i |i\rangle \tag{2.2}$$

где $\sum_i$ значи збир по свим исходима, њих N. За стање које је збир више базних вектора кажемо да је у **суперпозицији** тих вектора: у изабраној бази има више од једне ненулте амплитуде. На пример, $(|0\rangle + |1\rangle)/\sqrt{2}$ је суперпозиција вектора $|0\rangle$ и $|1\rangle$.

Правило 1: чисто квантно стање представљамо јединичним вектором. У нашем реалном моделу то значи $|\psi\rangle = \sum_i a_i|i\rangle$ са $\sum_i a_i^2 = 1$. Компоненте a_i, бројеви испред базних вектора, зову се **амплитуде**. Зашто баш јединични вектор, видећемо у §2.3.

Стање кубита је $a|0\rangle + b|1\rangle$ са $a^2 + b^2 = 1$: јединични вектор у равни, стрелица од координатног почетка до јединичне кружнице (Слика 2.1а).

Амплитуде нису вероватноће. Вероватноћа је број између 0 и 1, а амплитуда може бити и **негативна**. У општем случају амплитуде су комплексни бројеви. У нашем приказу све су реалне. Видећемо да су разлике у знаковима амплитуда и њихова интерференција кључне за рад Гроверовог алгоритма.

2.3 Мерење и вероватноће

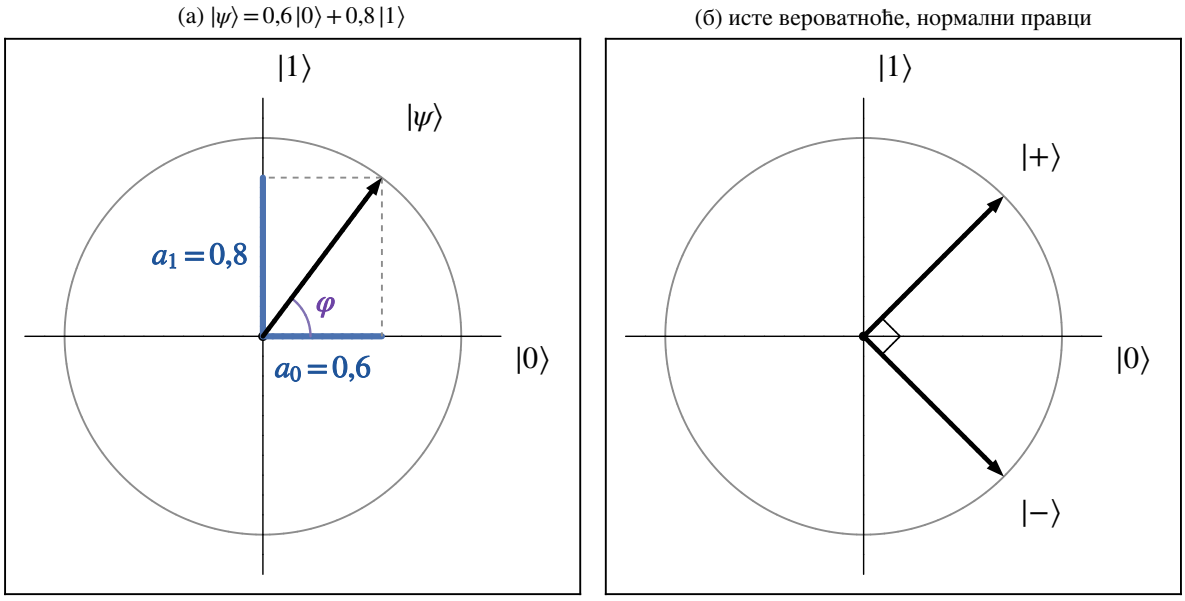
Мерење је најважнији, и најнеобичнији, део приче. Квантно стање може бити суперпозиција више базних стања, али једно мерење у изабраној бази даје само **један** исход. Не добијамо непосредан списак свих амплитуда, већ један резултат мерења.

Правило 2: вероватноће исхода мерења одређене су квадратима амплитуда. Мерење стања $|\psi\rangle$ даје исход i са вероватноћом

$$P(i) = a_i^2 \tag{2.3}$$

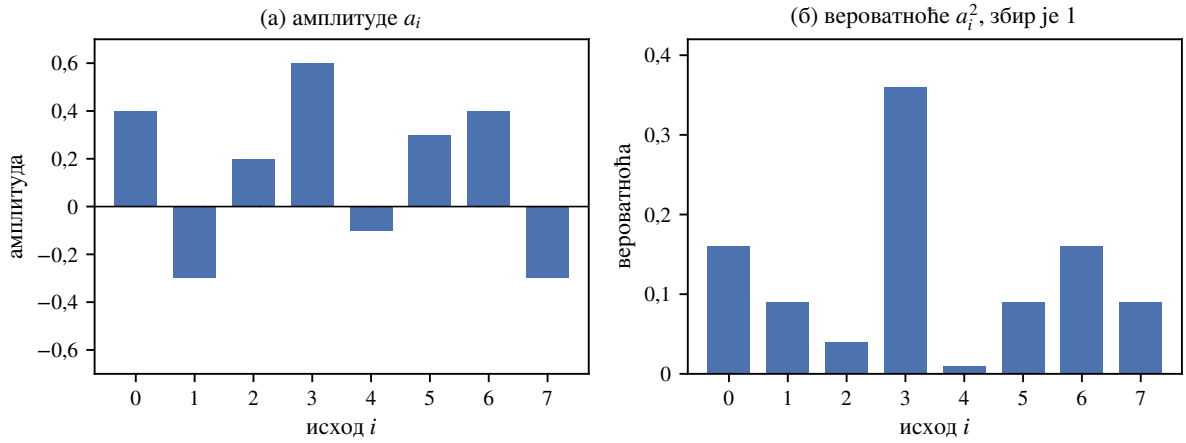
Овај облик правила важи за реалне амплитуде; у општем случају је $P(i) = |a_i|^2$. Ако много пута припремимо исто стање и поновимо исто мерење, удео огледа у којима добијемо исход i приближава се његовој вероватноћи $P(i)$. Збир свих вероватноћа мора бити 1, па је $\sum_i a_i^2 = 1$: по Питагориној теореми то значи да је стање јединични вектор. Зато правило 1 тражи јединичне векторе.

На пример, мерење кубита у стању $0{,}6\,|0\rangle + 0{,}8\,|1\rangle$ даје 0 са вероватноћом 0,36, а 1 са вероватноћом 0,64; збир је 1. Ако стрелицу стања кубита опишемо углом φ који заклапа са $|0\rangle$, онда је $|\psi\rangle = \cos\varphi\,|0\rangle + \sin\varphi\,|1\rangle$, па је $P(0) = \cos^2\varphi$ и $P(1) = \sin^2\varphi$: што је стрелица ближа оси $|1\rangle$, исход 1 је вероватнији (Слика 2.1а). Ову слику ћемо поново срести код Гровера, где ће вероватноћа успеха бити квадрат синуса угла једне стрелице.



Слика 2.1. (а) Стање кубита као стрелица. Његове амплитуде су сенке стрелице на осе, $a_0 = 0{,}6$ и $a_1 = 0{,}8$, па мерење даје 0 са вероватноћом 0,36, а 1 са вероватноћом 0,64. (б) Стања $|+\rangle$ и $|-\rangle$ из §2.6 дају исте вероватноће, 1/2 и 1/2, а ипак су нормална једно на друго.

Колапс. Ако при идеалном мерењу у изабраној бази добијемо исход i, стање система после мерења постаје $|i\rangle$: кажемо да се стање **урушило** у тај базни вектор. Ако одмах поновимо исто мерење, без додатне операције, поново добијамо исход i. Амплитуде не можемо прочитати једним мерењем: оно даје само један исход. Да бисмо проценили a_i^2, морали бисмо исто стање да припремимо много пута и да га меримо изнова. Слика 2.2 приказује једно стање са осам исхода.



Слика 2.2. Једно стање са осам исхода. (а) Амплитуде могу бити и негативне. (б) Вероватноће су квадрати амплитуда, а збир им је 1.

Глобални и релативни знак. Вектори $|\psi\rangle$ и $-|\psi\rangle$ представљају исто физичко стање: промена знака свих амплитуда не утиче на исходе ниједног мерења. Ако, међутим, променимо знак само једне амплитуде, можемо добити физички различито стање. Таква промена не мења вероватноће мерења у истој бази, али може утицати на резултат после одговарајуће квантне операције. Пример ћемо видети у §2.6. У општој квантној механици говори се о глобалној и релативној фази.

2.4 Више кубита

Када сваки од n кубита меримо у бази $|0\rangle$, $|1\rangle$, исход је низ од n битова; таквих исхода има 2^n. За два кубита исходи су 00, 01, 10 и 11. Низ битова можемо читати и као број записан бинарно: $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ су $|0\rangle$, $|1\rangle$, $|2\rangle$ и $|3\rangle$. Стање два кубита је зато вектор са четири амплитуде:

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

Како се кубити састављају? Ако су два кубита независно припремљена, први у стању $a|0\rangle+b|1\rangle$, а други у стању $c|0\rangle + d|1\rangle$, њихово заједничко стање је **тензорски производ** тих стања, који пишемо знаком $\otimes$. Рачунамо га као производ две заграде: сваки сабирак множимо сваким, а кетове спајамо, $|0\rangle \otimes |1\rangle = |01\rangle$:

$$\big(a|0\rangle + b|1\rangle\big) \otimes \big(c|0\rangle + d|1\rangle\big) = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \tag{2.4}$$

Ред је важан: први кет даје први бит. Производ два јединична вектора је јединични вектор, јер је $(ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 = (a^2 + b^2)(c^2 + d^2) = 1$.

Спрегнутост. Не може се свако стање два кубита написати као производ стања појединачних кубита. На пример, $(|00\rangle + |11\rangle)/\sqrt{2}$ није такав производ: да би у (2.4) и ac и bd били различити од нуле, и a, b, c и d морали би бити различити од нуле, па ни ad и bc не би могли бити нула. Таква стања зовемо **квантно спрегнутим стањима**. У §2.8 видећемо како настају помоћу капија.

Број исхода расте веома брзо. Двадесет кубита има $2^{20} = 1\,048\,576$ исхода, више од милион. Три стотине кубита има $2^{300} \approx 2 \cdot 10^{90}$ исхода, више него што у видљивом свемиру има атома, којих је око 10^{80}. Стање n кубита је вектор од $N = 2^n$ амплитуда. Ипак, једно мерење не открива све те бројеве: оно даје само један исход. Квантне операције могу да промене амплитуде и тако повећају вероватноћу жељеног резултата.

2.5 Оператори и унитарност

Квантни рачунар мења стање корак по корак. Капију можемо описати **оператором**: правилом U које сваком вектору $|\psi\rangle$ придружује нови вектор, $U|\psi\rangle$. Вектор $U|\psi\rangle$ зовемо **сликом** вектора $|\psi\rangle$. Оператори којима описујемо ове капије су **линеарни**: слика збира вектора је збир њихових слика, а слика вектора помноженог бројем је његова слика помножена истим бројем. Зато је довољно знати шта оператор ради са базним векторима:

$$U\Big(\sum_i a_i|i\rangle\Big) = \sum_i a_i\, U|i\rangle.$$

Слике базних вектора уписујемо у таблицу бројева, **матрицу**: колона i матрице садржи компоненте вектора $U|i\rangle$. Оператор делује на вектор тако што се матрица помножи колоном компоненти вектора: компонента j слике је збир производа бројева из врсте j матрице и одговарајућих компоненти вектора. Пример је у §2.6.

Правило 3: квантне капије које разматрамо описују се унитарним операторима. Они су линеарни и чувају дужину сваког вектора. Зато јединично стање преводе у друго јединично стање, а збир вероватноћа остаје 1. У нашем реалном моделу то су ортогоналне трансформације: у равни **ротације** и **огледања**, а у више димензија њихова уопштења. У §2.9 видећемо да чувају и углове.

Мерење је другачији процес: промену стања после мерења не описујемо једном унитарном капијом.

Унитаран корак никада не спаја два различита вектора у један. Када би било $U|\varphi\rangle = U|\psi\rangle$, онда би $U\big(|\varphi\rangle - |\psi\rangle\big)$ био нула-вектор, дужине 0. Корак не мења дужине, па би и $|\varphi\rangle - |\psi\rangle$ имао дужину 0, тј. било би $|\varphi\rangle = |\psi\rangle$. Зато сваки унитаран корак има инверзну операцију која враћа почетно стање: **унитарне капије су реверзибилне**. То ће нам бити важно у §3.6. Због линеарности се $|\psi\rangle$ и $-|\psi\rangle$ ни после низа унитарних корака не разликују ничим осим глобалним знаком.

2.6 Квантна кола и капије X и H

Унитарне кораке квантног рачунара зовемо **квантним капијама**, а низ капија **квантним колом**. Коло цртамо овако (Слика 2.3):

- свака хоризонтална линија је један кубит;
- време тече слева надесно: лево пише стање које улази, а десно стање које излази;
- квадрат са словом на линији је капија која делује на тај кубит.

Капија X је квантна верзија логичког НЕ: $|0\rangle$ пребацује у $|1\rangle$, а $|1\rangle$ у $|0\rangle$. Ево њене матрице и њеног деловања на стање $a|0\rangle + b|1\rangle$:

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0\cdot a + 1\cdot b \\ 1\cdot a + 0\cdot b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}.$$

Две амплитуде замене места.

Адамарова капија H преводи базна стања $|0\rangle$ и $|1\rangle$ у њихове равномерне суперпозиције:

$$\mathrm{H}|0\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad \mathrm{H}|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \qquad \mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.5}$$

Чинилац $1/\sqrt{2}$ чува дужину: оба стања су јединична, и мерење сваког од њих даје 0 и 1 са вероватноћом $(1/\sqrt{2})^2 = 1/2$. Стања $|+\rangle$ и $|-\rangle$ дају, дакле, исте вероватноће. Разликују се само у знаку једне амплитуде, амплитуде исхода 1.

Капија H двапут. Шта ако на $|+\rangle$ још једном применимо H? Капија је линеарна, па делује на сваки сабирак посебно:

$$\mathrm{H}|+\rangle = \frac{\mathrm{H}|0\rangle + \mathrm{H}|1\rangle}{\sqrt{2}} = \frac{1}{2}\big(|0\rangle + |1\rangle\big) + \frac{1}{2}\big(|0\rangle - |1\rangle\big) = |0\rangle.$$

Доприноси амплитуди исхода 0 сабрали су се, $1/2 + 1/2 = 1$, а доприноси амплитуди исхода 1 поништили су се, $1/2 - 1/2 = 0$. Када доприноси истој амплитуди имају исти знак, сабирају се; са супротним знацима могу се делимично или потпуно поништити. То је **интерференција**; слично се понашају таласи на води. Код $|-\rangle$ је обрнуто: доприноси амплитуди исхода 0 пониште се, а исхода 1 саберу:

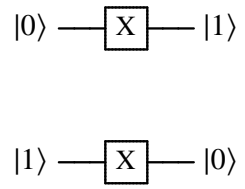
$$\mathrm{H}|-\rangle = \frac{\mathrm{H}|0\rangle - \mathrm{H}|1\rangle}{\sqrt{2}} = \frac{1}{2}\big(|0\rangle + |1\rangle\big) - \frac{1}{2}\big(|0\rangle - |1\rangle\big) = |1\rangle.$$

Дакле:

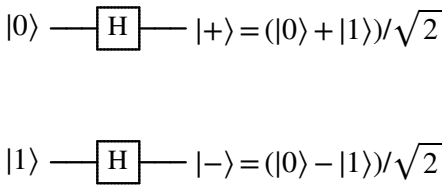
$$|0\rangle \xrightarrow{\text{H}} |+\rangle \xrightarrow{\text{H}} |0\rangle, \qquad |1\rangle \xrightarrow{\text{H}} |-\rangle \xrightarrow{\text{H}} |1\rangle \tag{2.6}$$

Капија H двапут враћа почетно стање (Слика 2.3в). Погледајмо шта се десило. Мерење у бази $|0\rangle, |1\rangle$ не разликује стања $|+\rangle$ и $|-\rangle$: оба дају 0 и 1 са по пола вероватноће. После капије H прво сигурно даје 0, а друго сигурно 1. **Релативни знак амплитуда може утицати на вероватноће мерења након одговарајуће квантне операције.** Овде капија H претвара разлику у знаку у разлику између два сигурна исхода.

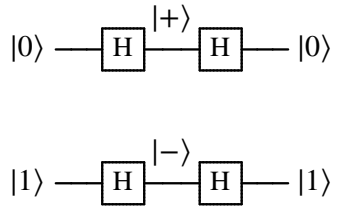
(а) капија X



(б) капија H



(в) капија H двапут



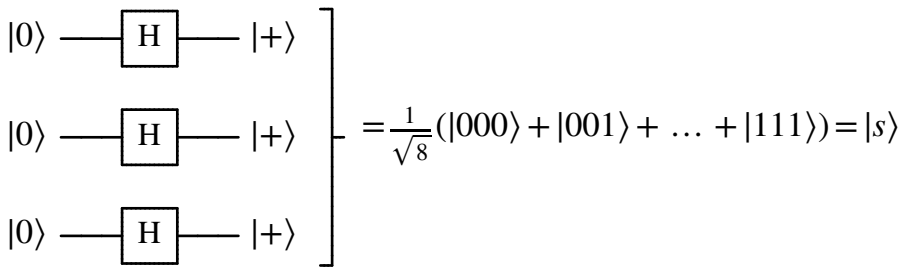
Слика 2.3. Кола на једном кубиту: линија је кубит, време тече слева надесно, лево је стање које улази, а десно стање које излази. (а) Капија X замењује $|0\rangle$ и $|1\rangle$. (б) Капија H прави $|+\rangle$ од $|0\rangle$, а $|-\rangle$ од $|1\rangle$. (в) Друга капија H враћа почетно стање.

2.7 Адамарове капије на више кубита

Узмимо три кубита, сваки у стању $|0\rangle$, и ставимо по једну капију H на сваки (Слика 2.4). Капије које стоје једна изнад друге делују у истом кораку; зовемо их **слојем**. Сваки кубит изађе у стању $|+\rangle$, а стање сва три кубита је тензорски производ, као у (2.4):

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{8}}\big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\big).$$

Из сваке заграде узимамо по један сабирак, на свих $2 \cdot 2 \cdot 2 = 8$ начина, и сваки производ има чинилац $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Бинарни низови су бројеви од 0 до 7, па је резултат $\big(|0\rangle + |1\rangle + \cdots + |7\rangle\big)/\sqrt{8}$: **све амплитуде су једнаке**.



Слика 2.4. Слој капија H на три кубита. Сваки кубит изађе у стању $|+\rangle$, а сва три заједно у стању $|s\rangle$, у коме свих осам исхода имају исту амплитуду, $1/\sqrt{8}$.

Исто важи за свако n. Слој од n капија H преводи $|0 \ldots 0\rangle$ у стање

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} (1, 1, \ldots, 1), \qquad N = 2^n \tag{2.7}$$

у коме свих N исхода имају исту амплитуду, $1/\sqrt{N}$. Оно је јединично, јер је збир квадрата амплитуда $N \cdot (1/N) = 1$. Слово s долази од енглеског *superposition*: $|s\rangle$ је **равномерна суперпозиција** свих исхода. За његову припрему потребно је n Адамарових капија, по једна на сваком кубиту. Пошто делују на различите кубите, могу бити примењене у једном слоју.

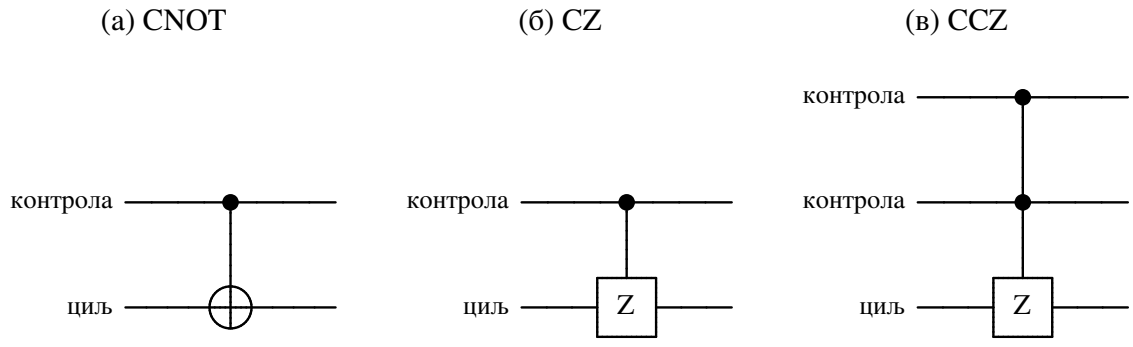
Ако бисмо одмах измерили стање $|s\rangle$, добили бисмо сваки од N исхода са истом вероватноћом $1/N$. Такво мерење не помаже да издвојимо тражени елемент: резултат је једнако случајан као при насумичном избору.

2.8 **Контролисане квантне капије:** CNOT **и** CZ

Капија на једном кубиту не повезује кубите. За рачунање су нам потребне и **капије са контролом** које делују на два или више кубита. Њихово деловање најлакше описујемо на базним стањима: ако је контролни кубит $|0\rangle$, циљна операција се не примењује, а ако је $|1\rangle$, примењује се на циљни кубит.

Важно је да се контролни кубит при томе **не мери**. Ако је у суперпозицији, капија делује линеарно на све компоненте заједничког стања.

Најпознатија таква капија је CNOT, контролисано НЕ. Цртамо је тачком на **контролном** кубиту и знаком $\oplus$ на **циљном** кубиту, спојеним усправном линијом (Слика 2.5а). Ако је контролни бит 0, капија не ради ништа; ако је 1, примени X на циљни кубит. Капија Z на једном кубиту оставља $|0\rangle$, а $|1\rangle$ мења у $-|1\rangle$. Капија CZ, контролисано Z, мења зато знак само амплитуди исхода 11; цртамо је тачком на контролном кубиту и квадратом Z на циљном (Слика 2.5б). Шта обе капије раде са базним векторима, показује **таблица истинитости**, Табела 2.1. На суперпозицију делују сабирак по сабирак, јер су линеарне. Обе само премештају амплитуде или им мењају знак, па чувају дужине: то су дозвољени кораци.



Слика 2.5. Капије са контролом; тачка означава контролни кубит. (а) CNOT: ако је контролни бит 1, циљни бит се обрне. (б) CZ: ако су оба бита 1, амплитуда мења знак. (в) CCZ: знак се мења само ако су сва три бита 1.

улаз	CNOT	CZ
$\|00\rangle$	$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$	$\|10\rangle$
$\|11\rangle$	$\|10\rangle$	$-\|11\rangle$

Табела 2.1. Капије CNOT и CZ на четири базна вектора два кубита; контролни кубит је први. CNOT обрне други бит ако је први 1, а CZ мења знак ако су оба бита 1.

Почнимо, на пример, од стања $|00\rangle$. Применимо капију H на први кубит, а затим CNOT, са првим кубитом као контролним:

$$|00\rangle \xrightarrow{\mathrm{H}\otimes\mathbb{1}} \frac{|00\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{\mathrm{CNOT}} \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Добили смо спрегнуто стање из §2.4, иако су кубити на почетку били независно припремљени.

Контрола може да стоји и на више кубита. За базна стања циљна капија се тада примењује само ако су **сви** контролни битови 1. Тако се од капија прави провера облика „ако је први бит 1 **и** други бит 1 **и** ...“. На пример, капија CCZ има два контролна и један циљни кубит и мења знак само амплитуди базног стања $|111\rangle$ (Слика 2.5в). Такве капије ће нам требати у Гроверовом алгоритму.

2.9 Скаларни производ, бра и пројектори

Остао нам је још последњи део алата. Можда сте у школи већ срели скаларни производ; ево га од почетка. У нашем моделу, у коме су компоненте реалне, **скаларни производ** вектора $|\varphi\rangle = \sum_i b_i|i\rangle$ и $|\psi\rangle = \sum_i a_i|i\rangle$ добијамо када помножимо одговарајуће компоненте и саберемо производе. Дирак га пише као $\langle\varphi|\psi\rangle$, а читамо га „бра фи, кет пси“:

$$\langle\varphi|\psi\rangle = \sum_i b_i\, a_i.$$

У општем комплексном случају компоненте првог вектора комплексно се конјугују: $\langle\varphi|\psi\rangle = \sum_i b_i^* a_i$.

Лева половина, $\langle\varphi|$, зове се **бра**. Бра и кет заједно чине заграду, на енглеском *bracket*, одакле и оба имена. У нашем реалном моделу кет можемо замислити као колону компоненти, а одговарајући бра као врсту истих компоненти; скаларни производ је тада врста помножена колоном. Дужину вектора $|\psi\rangle$ пишемо $\|\psi\|$, са две усправне црте са сваке стране. У школи сте интензитет вектора $\vec{a}$ писали са једном цртом, $|\vec{a}|$; овде пишемо две, јер једна усправна црта већ стоји у самом кету. По Питагориној теореми је $\|\psi\|^2 = \sum_i a_i^2 = \langle\psi|\psi\rangle$.

Скаларни производ има и геометријско значење, које ће нам требати на сваком кораку. Ако два ненулта вектора $|\varphi\rangle$ и $|\psi\rangle$ нису паралелна, они **разапињу** раван: то су сви вектори облика $\lambda|\varphi\rangle + \mu|\psi\rangle$. У тој равни важи обична геометрија.

Посматрајмо троугао чија су темена координатни почетак и врхови два вектора. Његове странице су $\|\varphi\|$, $\|\psi\|$ и $\|\varphi - \psi\|$, а угао између прве две зовемо γ. Спустимо нормалу из врха вектора $|\psi\rangle$ на праву кроз $|\varphi\rangle$: потписана координата њеног подножја је $\|\psi\|\cos\gamma$, а њена дужина је $\|\psi\|\sin\gamma$ (ако је угао туп, подножје је са друге стране почетка, $\cos\gamma$ је негативан, а рачун остаје исти). По Питагориној теореми је

$$\|\varphi - \psi\|^2 = \big(\|\varphi\| - \|\psi\|\cos\gamma\big)^2 + \big(\|\psi\|\sin\gamma\big)^2 = \|\varphi\|^2 + \|\psi\|^2 - 2\,\|\varphi\|\,\|\psi\|\cos\gamma,$$

јер је $\cos^2\gamma + \sin^2\gamma = 1$. То је косинусна теорема, коју знате из школе. С друге стране, по компонентама је

$$\|\varphi - \psi\|^2 = \sum_i (b_i - a_i)^2 = \sum_i b_i^2 + \sum_i a_i^2 - 2\sum_i b_i a_i.$$

Поређење две формуле даје

$$\langle\varphi|\psi\rangle = \sum_i b_i\, a_i = \|\varphi\|\,\|\psi\|\cos\gamma \tag{2.8}$$

тј. скаларни производ је производ дужина два вектора и косинуса угла између њих. За паралелне ненулте векторе исто важи са углом 0° или 180°; ако је један вектор нула, обе стране су нула, а угао није потребно одређивати. У равни је то школски скаларни производ.

Три особине скаларног производа користићемо стално.

Дужина. Скаларни производ вектора са самим собом је квадрат његове дужине, $\langle\psi|\psi\rangle = \|\psi\|^2$, па је вектор јединични ако је $\langle\psi|\psi\rangle = 1$.

Компоненте. Базни вектори су јединични и нормални један на други: $\langle i|i\rangle = 1$, а за два различита **базна** вектора $|i\rangle$ и $|i'\rangle$ је $\langle i|i'\rangle = 0$. Пазите: то важи за базне векторе, а не за свака два различита стања. На пример, $\langle 0|+\rangle = 1/\sqrt{2}$, а $\langle +|-\rangle = \big(1\cdot 1 + 1\cdot(-1)\big)/2 = 0$: стања $|+\rangle$ и $|-\rangle$ дају исте вероватноће, а нормална су једно на друго (Слика 2.1б). Скаларни производ са базним вектором издваја једну компоненту:

$$\langle i|\psi\rangle = a_i \tag{2.9}$$

па правило 2 гласи и $P(i) = \langle i|\psi\rangle^2$.

Рачунска правила. У нашем реалном моделу скаларни производ је симетричан, $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle$, и може се рачунати сабирак по сабирак: $\langle\varphi|\big(\lambda|\psi\rangle + \mu|\chi\rangle\big) = \lambda\langle\varphi|\psi\rangle + \mu\langle\varphi|\chi\rangle$. У комплексном случају важи $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$.

Значење скаларног производа најлакше се види када је један од вектора јединични. Ако је $|u\rangle$ јединични, по (2.8) је $\langle u|\psi\rangle = \|\psi\|\cos\gamma$. То је дужина сенке коју вектор $|\psi\rangle$ баца на праву кроз $|u\rangle$, са знаком минус ако сенка пада на супротну страну од $|u\rangle$. Компонента $a_i = \langle i|\psi\rangle$ је баш таква сенка, на осу i (Слика 2.1а).

Унитарни кораци чувају и углове. У нашем реалном моделу скаларни производ може се изразити преко дужина:

$$\langle\varphi|\psi\rangle = \frac{\|\varphi+\psi\|^2 - \|\varphi-\psi\|^2}{4}.$$

Ова формула следи из $\|\varphi \pm \psi\|^2 = \|\varphi\|^2 \pm 2\langle\varphi|\psi\rangle + \|\psi\|^2$, што се добија рачунањем сабирак по сабирак. Линеаран корак који чува дужине (§2.5) зато чува и скаларне производе, а тиме и углове.

Пројектор. Кет и бра можемо написати и обрнутим редом, $|u\rangle\langle u|$. То више није број, него оператор: он чека вектор са десне стране. Када делује на вектор $|r\rangle$, десни пар постаје скаларни производ:

$$\big(|u\rangle\langle u|\big)\,|r\rangle = |u\rangle\,\langle u|r\rangle = \langle u|r\rangle\,|u\rangle \tag{2.10}$$

Нека је $|u\rangle$ јединични. Тада је $\langle u|r\rangle$ потписана дужина сенке вектора $|r\rangle$ на правој кроз $|u\rangle$, па је $\langle u|r\rangle\,|u\rangle$ вектор на тој правој. Зовемо га **пројекцијом** вектора $|r\rangle$ на праву кроз $|u\rangle$, а оператор $|u\rangle\langle u|$ зовемо **пројектором**. Пројектор сам $|u\rangle$ оставља какав јесте, јер је $\langle u|u\rangle = 1$, а сваки вектор нормалан на $|u\rangle$ претвара у нулу. Зато пројектор у општем случају не чува дужину и није унитарна капија; овде га користимо као математички алат. Пројектори имају улогу и у опису мерења.

Остатак, $|r\rangle - \langle u|r\rangle\,|u\rangle$, нормалан је на праву: његов скаларни производ са $|u\rangle$ је $\langle u|r\rangle - \langle u|r\rangle\langle u|u\rangle = 0$. Сваки вектор се тако растављa на два дела, један дуж праве и један нормалан на њу:

$$|r\rangle = \underbrace{\langle u|r\rangle\,|u\rangle}_{\text{дуж праве}} + \underbrace{\big(|r\rangle - \langle u|r\rangle\,|u\rangle\big)}_{\text{нормално на праву}}.$$

Загревање. Ево колико се са пројектором лако рачуна. Нека је $\mathbb{1}$ **јединични оператор**, који ништа не мења, $\mathbb{1}|r\rangle = |r\rangle$, и посматрајмо оператор $\mathbb{1} - 2|u\rangle\langle u|$. Вектор нормалан на $|u\rangle$ пројектор претвара у нулу, па тај вектор остаје какав јесте. Сам $|u\rangle$ пројектор оставља, па је

$$\big(\mathbb{1} - 2|u\rangle\langle u|\big)\,|u\rangle = |u\rangle - 2|u\rangle = -|u\rangle.$$

Овај оператор мења знак компоненти дуж правца $|u\rangle$, а све што је нормално на њега оставља. У равни је то огледање у односу на праву нормалну на $|u\rangle$. Ако је $|u\rangle$ базни вектор, на пример $|2\rangle$, оператор мења знак само амплитуди a_2. Ову формулу запамтите: ускоро ћемо је поново срести.

Најважније из поглавља

1. Квантна стања и суперпозиција. Чисто квантно стање представљамо јединичним вектором

$$|\psi\rangle = \sum_i a_i|i\rangle, \qquad \sum_i a_i^2 = 1.$$

Бројеве a_i називамо **амплитудама**. У нашем моделу оне су реалне и могу бити позитивне или негативне. Стање које у изабраној бази има више ненултих амплитуда називамо суперпозицијом базних стања.

2. Мерење и вероватноће. При мерењу у изабраној бази добијамо један исход i, са вероватноћом

$$P(i) = a_i^2.$$

После идеалног мерења стање постаје $|i\rangle$. Промена знака свих амплитуда не мења физичко стање, али **релативни знакови амплитуда** могу утицати на исходе каснијих мерења.

3. Системи од више кубита. Стање n кубита описујемо помоћу $N = 2^n$ амплитуда. Независно припремљена стања комбинујемо **тензорским производом**, али постоје и **спрегнута стања**, која не можемо написати као производ стања појединачних кубита.

4. Квантне капије. Капије описујемо **унитарним операторима**: они су линеарни, чувају дужине и углове између вектора и имају инверзну операцију. Мерење не описујемо једном унитарном капијом.

5. Адамарова капија и интерференција. Адамарова капија H преводи базна стања у суперпозиције:

$$\mathrm{H}|0\rangle = |+\rangle, \qquad \mathrm{H}|1\rangle = |-\rangle, \qquad \mathrm{H}^2 = \mathbb{1}.$$

При узастопним квантним операцијама доприноси амплитудама могу да се сабирају или поништавају. Ову појаву називамо **интерференцијом**. Применом Адамарове капије на сваки од n кубита припремљених у стању $|0\rangle$ добијамо **равномерну суперпозицију**

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle.$$

6. Контролисане капије. Капије CNOT, CZ и CCZ делују на више кубита. Њихово деловање зависи од вредности контролних битова у базним стањима, али се **контролни кубити при томе не мере**. Ове капије омогућавају условне операције, укључујући промену знака изабраних амплитуда.

7. Скаларни производ, пројектори и огледања. Скаларни производ $\langle\varphi|\psi\rangle$ описује геометријски однос два вектора, док оператор $P_u = |u\rangle\langle u|$ представља пројектор на правац јединичног вектора $|u\rangle$. Помоћу њега можемо конструисати унитарни оператор

$$R_u = \mathbb{1} - 2|u\rangle\langle u|,$$

који **мења знак компоненте дуж** $|u\rangle$, а све компоненте нормалне на тај правац оставља непромењеним.

Кључна идеја: Квантни алгоритми користе унитарне операције да мењају амплитуде и омогуће њихову интерференцију. У Гроверовом алгоритму комбинација два геометријска огледања постепено ће повећавати вероватноћу добијања траженог исхода.

2.10 Задаци

Задаци за самосталан рад

Задаци у овом поглављу намењени су увежбавању основних појмова квантне механике и квантног рачунарства. Почећемо од једноставнијих рачуна са квантним стањима, амплитудама и вероватноћама мерења, а затим прећи на системе од више кубита, квантне капије и кола. Последњи задаци посвећени су скаларном производу, пројекторима и геометријским трансформацијама које ће нам бити потребне за разумевање Гроверовог алгоритма.

Осим ако није другачије назначено, у задацима користимо реалне амплитуде, а мерења вршимо у рачунској бази.

Стања, нормализација и мерење (§2.1–§2.3)

Задатак 21. Нађите позитиван број λ такав да је $\lambda\,(|0\rangle + 2|1\rangle)$ јединични вектор. Колике су тада вероватноће исхода 0 и 1? *Упутство: услов је* $\langle\psi|\psi\rangle = 1$.

Задатак 22. Вектор са четири компоненте задат је са $|r\rangle = (0, -2, 0, 1)$. Нормализујте га и запишите добијено стање у кет-нотацији помоћу $|0\rangle$,$|1\rangle$,$|2\rangle$,$|3\rangle$. Одредите вероватноће сва четири исхода.

Задатак 23. Запишите стање $|\psi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ као пар компоненти. Проверите да је нормализовано, одредите вероватноће исхода 0 и 1 и препознајте о ком стању из §2.6 је реч.

Задатак 24. Кубит је припремљен у стању $|\psi\rangle = (\sqrt{3}\,|0\rangle - |1\rangle)/2$. Колике су вероватноће исхода 0 и 1? Ако је прво идеално мерење дало исход 1, које је стање непосредно после мерења и шта ће показати поновљено мерење у истој бази?

Задатак 25. Упоредите стања $|\psi\rangle = (\sqrt{3}\,|0\rangle + |1\rangle)/2$, $-|\psi\rangle$ и $\mathrm{Z}|\psi\rangle$. Која два вектора описују исто физичко стање? Колике су вероватноће мерења у бази $\{|0\rangle,|1\rangle\}$ за сва три вектора? *Упутство:* $\mathrm{Z}|0\rangle = |0\rangle$, $\mathrm{Z}|1\rangle = -|1\rangle$.

Задатак 26. Покажите да стања $|+\rangle$ и $|-\rangle$ из (2.5) дају исте вероватноће и да је $\langle +|-\rangle = 0$. Затим оба ротирајте за 45° у позитивном математичком смеру и покажите да их мерење у бази $\{|0\rangle,|1\rangle\}$ после тога разликује са сигурношћу. *Упутство: $|+\rangle$ лежи под углом* 45°, *а $|-\rangle$ под углом* $-45°$.

Задатак 27. Исти кубит припремљен је у стању $|0\rangle$. Колика је вероватноћа исхода 0 ако га меримо у бази $\{|0\rangle,|1\rangle\}$? А колике су вероватноће исхода + и − ако га меримо у бази $\{|+\rangle,|-\rangle\}$? *Упутство: изразите $|0\rangle$ преко $|+\rangle$ и $|-\rangle$.*

Задатак 28. Стање система са три могућа исхода има амплитуде $(1, -2, 2)/3$. Проверите нормализацију. Колике су вероватноће исхода 0, 1 и 2? Колика је вероватноћа да добијемо исход 1 **или** исход 2?

Задатак 29. Кубит у сваком огледу припремамо изнова, у стању које даје исход 1 са вероватноћом $1/4$. Три пута независно поновимо припрему и мерење. Колика је вероватноћа да исход 1 добијемо бар једном? *Упутство: лакше је прво израчунати вероватноћу да га не добијемо ниједном.*

Више кубита и тензорски производ (§2.4)

Задатак 30. Развијте тензорски производ $|+\rangle \otimes |-\rangle$ у бази $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ и запишите сва четири коефицијента као уређену четворку.

Задатак 31. Два кубита су у производном стању $\big(\sqrt{3}\,|0\rangle + |1\rangle\big)/2 \otimes \big(|0\rangle - |1\rangle\big)/\sqrt{2}$. Колике су вероватноће исхода 00 и 11? Колика је вероватноћа да је **први** измерени бит једнак 1?

Задатак 32. Размотрите стање $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Који исходи мерења су могући и са којим вероватноћама? Да ли се ово стање може написати као тензорски производ стања два појединачна кубита?

Задатак 33. Колико рачунских базних стања има систем од три кубита? За равномерну суперпозицију сва три кубита израчунајте вероватноћу исхода 101 и вероватноћу да је први бит једнак 1.

Оператори и квантне капије (§2.5–§2.8)

Задатак 34. Израчунајте $\mathrm{X}(a|0\rangle + b|1\rangle)$ и $\mathrm{X}|-\rangle$. Да ли се резултат у другом случају физички разликује од почетног стања?

Задатак 35. Оператор R има матрицу $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Одредите $R|0\rangle$ и $R|1\rangle$, па проверите да је $R^{T}R = \mathbb{I}$, где R^{T} означава транспоновану матрицу (замењене врсте и колоне). Коју геометријску трансформацију представља R?

Задатак 36. Покажите да капија H вектор $(a,b) = a|0\rangle + b|1\rangle$ преводи у $\big((a+b)/\sqrt{2},(a-b)/\sqrt{2}\big)$ и да двапут примењена враћа сваки вектор (a,b) на почетак. *Упутство: користите (2.5) и то да је капија линеарна.*

Задатак 37. На један кубит најпре применимо H, затим X, па поново H. Одредите резултат за улазна стања $|0\rangle$ и $|1\rangle$. Којој познатој капији одговара цео низ?

Задатак 38. Примените H на стање $(\sqrt{3}\,|0\rangle + |1\rangle)/2$. Одредите две излазне амплитуде и вероватноће исхода 0 и 1 после мерења.

Задатак 39. На стање $|000\rangle$ примените по једну капију H на сваки кубит. Запишите резултат помоћу збира рачунских базних стања. Колика је вероватноћа исхода 101, а колика вероватноћа да је први бит једнак 1? Колико капија и колико слојева је потребно?

Задатак 40. Почните од $|00\rangle$, примените H на први кубит, а затим CNOT са првим кубитом као контролом и другим као циљем. Које је крајње стање и које исходе мерења можете добити?

Задатак 41. На стање $(|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$ примените CZ. Запишите ново стање и вероватноће сва четири исхода мерења у рачунској бази.

Задатак 42. Примените CNOT са првим кубитом као контролом на стање $(|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$. Запишите све четири излазне амплитуде у редоследу 00,01,10,11.

Задатак 43. На равномерну суперпозицију осам базних стања три кубита примените CCZ. Која амплитуда мења знак? Запишите излазно стање и вероватноћу исхода 111.

Скаларни производ, пројектори и огледања (§2.9)

Задатак 44. Нека је $|s\rangle = (1,1,1,1)/2$ и $|\psi\rangle = (1,1,1,-1)/2$. Израчунајте $\langle s|\psi\rangle$ и угао између ова два вектора. *Упутство: користите (2.8); оба вектора су јединична.*

Задатак 45. Израчунајте $\langle +|-\rangle$, $\langle 0|+\rangle$ и $\langle 1|-\rangle$. Која два од наведених вектора су међусобно ортогонална?

Задатак 46. За $|\psi\rangle = (3|0\rangle + 4|1\rangle)/5$ и $P_0 = |0\rangle\langle 0|$ израчунајте $P_0|\psi\rangle$ и део $|\psi\rangle - P_0|\psi\rangle$. Колики је квадрат дужине пројекције?

Задатак 47. Нека је $P_+ = |+\rangle\langle +|$. Израчунајте $P_+|0\rangle$ у бази $\{|0\rangle,|1\rangle\}$ и квадрат дужине добијеног вектора. *Упутство: прво одредите $\langle +|0\rangle$.*

Задатак 48. Нека је $F = \mathbb{I} - 2|+\rangle\langle +|$. Израчунајте $F|+\rangle$, $F|-\rangle$ и $F|0\rangle$. Којој унитарној капији одговара оператор F, уз могући глобални знак?

Задатак 49. У четвородимензионалном простору нека је $|s\rangle = (1,1,1,1)/2$ и $|r\rangle = (1,1,1,-1)/2$. Израчунајте $D|r\rangle$ за $D = 2|s\rangle\langle s| - \mathbb{I}$. Који резултат мерења добијамо са сигурношћу? *Овај оператор ћемо поново срести у трећем поглављу.*

За радознале — први корак ка комплексним амплитудама

Задатак 50. У општем случају амплитуде могу бити комплексне. Нека је $i^2 = -1$ и нека за комплексну амплитуду важи $P = |a|^2$, при чему је $|1+i|^2 = |1-i|^2 = 2$. Упоредите мерење стања $|\psi\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ и $|+\rangle$ у бази $\{|0\rangle,|1\rangle\}$. Затим примените H на оба стања и поново израчунајте вероватноће мерења. *Овај задатак је необавезан; не захтева се за наставак рукописа.*

3. Гроверов алгоритам

Сада када познајемо основни језик квантних стања и капија, можемо да се посветимо претрази. Прво ћемо упоредити класичан и квантни поступак, а затим поставити проблем математички прецизно. Видећемо зашто оракл сам по себи није довољан, како дифузија појачава амплитуду траженог стања и зашто се цео алгоритам своди на низ ротација у једној равни.

3.1 Шта је квантна претрага?

Гроверов алгоритам је **квантни алгоритам претраге** [5]. Његов циљ је да међу многим могућностима пронађе ону која испуњава задати услов, користећи правила квантне механике.

Размотримо једноставан пример. Замислимо бројеве од 0 до 99, од којих је само један решење неког проблема [6]. Не знамо који. Знамо само да проверимо: за сваки број можемо да питамо „да ли си ти решење?“ и да добијемо одговор „да“ или „не“. Тај један број треба наћи. Зваћемо га **тражени (означени) елемент** и писати w. У овом примеру претпостављамо да постоји тачно једно решење. Касније ћемо могућности представити базним стањима квантног регистра: за n кубита има их $N = 2^n$, док је пример са 100 бројева само уводна илустрација.

3.2 Колико је провера потребно?

Како бисмо тражили без квантног рачунара? Ако о могућностима не знамо ништа, ако нису поређане и нема наговештаја „топлије, хладније“, не преостаје ништа боље него да их проверавамо једну по једну. Таква претрага зове се **претрага без структуре**. Пример из живота је катанац са шифром од четири цифре: могућих шифри има $N = 10\,000$, а једина провера је да шифру пробамо и видимо да ли се катанац отвара.

Понекад погодимо из прве, понекад тек на крају. Свако место у низу подједнако је вероватно, па ако проверавамо редом, без понављања, у просеку је потребно $(1+2+\cdots+N)/N = (N+1)/2$ провера, отприлике половина:

$$\text{класично: у просеку } \frac{N+1}{2} \text{ провера} \tag{3.1}$$

Ако се број могућности удвостручи, удвостручи се и посао.

Гроверов алгоритам налази w са великом вероватноћом уз много мање упита квантној провери:

$$\text{Гроверов алгоритам: број провера сразмеран са } \sqrt{N} \tag{3.2}$$

Ако се број могућности учетворостручи, провера треба само двапут више. За $N = 10\,000$ то је реда величине 100 провера уместо око 5000, а за милион могућности реда величине хиљаду уместо пола милиона. Тачан број, са сталним чиниоцем испред корена, израчунаћемо у §3.13. Број упита није исто што и време извршавања: стварно време зависи и од сложености сваке провере, осталих капија и уређаја на коме се коло изводи.

Корен није нов. У поглављу 1 број судара растао је као $\sqrt{M/m}$, по (1.11). Да то није случајност, видећемо у четвртом поглављу.

3.3 Сложеност алгоритама

Управо смо, а да то нисмо рекли, почели да говоримо о **сложености алгоритама**. При поређењу сложености алгоритама не полазимо од времена извршавања у секундама, јер оно зависи од рачунара. Питамо нешто друго: **како број корака расте када расте величина проблема** N? Одговор пишемо великим словом O. Запис $O(N)$ означава асимптотску горњу границу: за довољно велико N број корака није већи од неког сталног вишекратника броја N. Ако желимо да истакнемо да расте управо тим редом, и одозго и одоздо, пишемо $\Theta(N)$. Сталне чиниоце не пишемо: класична претрага, око $N/2$ провера, има сложеност $O(N)$, а Гроверов алгоритам $O(\sqrt{N})$. Неколико примера даје Табела 3.1.

сложеност	**пример**	**за** $N = 10^6$
$O(1)$, сталан	Да ли је број од N цифара паран? Уз непосредан приступ последњој цифри довољно је погледати само њу.	1 корак
$O(\log N)$, логаритамски	Погађање замишљеног броја од 1 до N уз одговоре „више“ и „мање“: свако питање преполови могућности. Тако тражимо и реч у речнику.	око 20 питања
$O(\sqrt{N})$, корен	Гроверов алгоритам.	реда 1000 провера
$O(N)$, линеаран	Провера N могућности једне по једне, као код катанца.	око 500 000 провера
$O(N^2)$, квадратни	Сваки од N ученика рукује се са сваким: $N(N-1)/2$ руковања.	око 500 милијарди
$O(2^N)$, експоненцијални	Испробавање свих положаја N прекидача: сваки нови прекидач удвостручи број могућности.	број од преко 300 000 цифара

Табела 3.1. Сложеност неких поступака. У сваком реду N је величина задатка: број цифара, бројева, могућности, ученика или прекидача.

Пазимо на једну разлику. Сложеност у Табели 3.1 је особина **алгоритма**. Исти проблем може да има више алгоритама различите сложености: за претрагу без структуре провера редом има сложеност $O(N)$, а Гроверов алгоритам $O(\sqrt{N})$. **Класе сложености**, о којима се такође много говори, групишу **проблеме** по томе шта се са њима може брзо урадити на одређеној врсти рачунара: решити их или бар проверити њихово решење. Најпознатије две зову се P и NP. У P су одлучивачки проблеми које обичан рачунар брзо **решава**, а у NP одлучивачки проблеми за које се сваки потврдан одговор може брзо **проверити** помоћу одговарајуће потврде. Примери су одлучивачке верзије уопштеног судокуа и бојења мапе са три боје: питамо да ли за дати задатак постоји исправно решење. Ако нам се решење покаже, можемо га проверити у полиномском броју корака [10]. Да ли је сваки проблем из NP уједно и у P, највеће је отворено питање рачунарства.

Овде реч „брзо“ има прецизно значење: број корака расте највише као неки степен **дужине записа** задатка, на пример као n^2 или n^3, где је n број цифара. Ту се крије замка. Ако је кандидат за решење низ од n битова, могућности има $N = 2^n$. Провера редом тада кошта $O(N) = O(2^n)$ корака: то је линеарно у N, а експоненцијално у n, као у последњем реду Табеле 3.1, где је N био број прекидача. Гроверов алгоритам то спушта на $O(\sqrt{N}) = O(2^{n/2})$. Уштеда је огромна, али је и то експоненцијално у n. Зато квадратна уштеда у броју упита са-

ма по себи не претвара експоненцијалан раст у полиномски. Није сваки проблем претрага без структуре, а стварни трошак зависи и од извођења провере.

Куда идемо. На располагању нам је провера која за сваку од N могућности каже да ли је тражена. У претходном поглављу упознали смо квантна стања, амплитуде, мерење и капије. Сада можемо прецизно да формулишемо претрагу и покажемо како квантни рачунар користи два огледања да би до решења стигао после реда $\sqrt{N}$ упита.

3.4 Формулација проблема претраге

Сада проблем можемо тачно да поставимо, језиком квантне механике.

- **Могућности.** Рачунар има n кубита, дакле $N = 2^n$ базних стања, $|0\rangle, |1\rangle, \ldots, |N-1\rangle$, са бројевима записаним бинарно. Свако базно стање је једна могућност.
- **Решење.** Једно од њих, $|w\rangle$, је решење. Не знамо које.
- **Провера.** На располагању нам је провера f која за сваку могућност i каже да ли је решење: $f(i) = 1$ ако је $i = w$, а $f(i) = 0$ иначе. Функција f је класично правило провере. Њено одговарајуће унитарно квантно коло зовемо **оракл**, а сваку примену тог кола **упит**.
- **Циљ.** Почињемо од стања $|0 \ldots 0\rangle$ и смемо да користимо капије. Желимо да на крају мерење покаже w са вероватноћом блиском 1, и то после што мање упита: око $\sqrt{N}$, а не око $N/2$. Капије које не питају оракл, на пример слој H, не бројимо; бројимо само упите.

3.5 Шта зна оракл?

Како можемо да направимо поступак који препознаје решење ако само решење не знамо? Кључ је у томе што **провера решења не захтева нужно да га унапред познајемо**.

Замислимо задати судоку и предложену попуну целе табле. Можемо да проверимо да ли су сачувани унапред уписани бројеви и да ли се у сваком реду, колони и квадрату 3×3 бројеви од 1 до 9 појављују без понављања. За ту проверу потребни су нам задата табла и правила, а не већ пронађена исправна попуна. Од такве провере начелно можемо саставити реверзибилно квантно коло. У конкретној примени морамо рачунати и цену капија и помоћних кубита потребних за проверу.

Други пример је хеш-функција: за задати улаз израчунамо његов отисак и упоредимо га са задатим, без претходног познавања улаза који даје тај отисак. Може постојати више од једног таквог улаза или ниједан; у главном извођењу, међутим, претпостављамо тачно једно означено решење.

У теоријској анализи често користимо **модел црне кутије**: алгоритам може да примењује оракл, али не користи његову унутрашњу конструкцију. У том моделу поредимо број упита. Ако је конструкција позната, она може открити додатну структуру проблема коју и класичан алгоритам може да искористи; уштеда у броју упита сама по себи не гарантује убрзање у стварном времену.

У једноставним наставним примерима понекад намерно правимо проверу за унапред познат одговор. У §3.17 конструисаћемо коло које означава 11: пошто смо тај одговор сами изабрали, пример не проналази непознато решење, већ показује како алгоритам ради. Опис таквог кола открива шта је означено, док код провере судокуа познавање правила не значи да већ знамо решену таблу.

Дакле, оракл описујемо по томе **шта ради са понуђеним кандидатом**. Можемо га конструисати из услова који решење мора да испуни, без претходног проналажења решења; у демонстрацији можемо и намерно уградити познат одговор.

3.6 Зашто оракл мења знак

Класична провера је функција: могућности i придружује бит $f(i)$, 0 или 1. Може ли квантни рачунар да уради исто, да стање $|i\rangle$ претвори у стање $|f(i)\rangle$ једног кубита, тј. у $|0\rangle$ или $|1\rangle$? Не може, чим је $N \geq 3$. Тај корак би свих $N-1$ погрешних могућности, $N-1$ различитих базних вектора, спојио у исти вектор $|0\rangle$. По §2.5 унитаран корак никада не спаја различита стања: из $|0\rangle$ се више не би видело од које је могућности дошао, и корак се не би могао поништити.

Квантни оракл зато не замењује могућност одговором. Дозвољена су два начина, и у оба могућност остаје на месту: одговор се може уписати у један додатни кубит, или у **знак**. Гроверов алгоритам користи знак: сваки базни вектор остаје на месту, а одговор се упише у његов знак:

$$U_w|i\rangle = (-1)^{f(i)}\,|i\rangle \tag{3.3}$$

тј. $U_w|w\rangle = -|w\rangle$, а $U_w|i\rangle = |i\rangle$ за $i \neq w$. Записано по амплитудама, то гласи:

$$a_w \longmapsto -a_w, \qquad a_i \longmapsto a_i \quad \text{за } i \neq w.$$

Ово је дозвољен корак. Оператор је линеаран, а промена знака једне амплитуде чува збир квадрата свих амплитуда и тиме дужину стања; ниједна два стања се не спајају; двапут примењен оракл враћа све на почетак. У запису из §2.9 то је оператор огледања који смо упознали у претходном поглављу, са $|u\rangle = |w\rangle$:

$$U_w = \mathbb{1} - 2|w\rangle\langle w| \tag{3.4}$$

У (3.4) слово w означава јединог кандидата који пролази проверу; тај запис описује **дејство** оракла, а не захтева да унапред знамо вредност w или да коло направимо поређењем са њом. Ако провера судокуа има једно решење, њен фазни оракл има баш овакав математички облик, чак и када нам је решење непознато.

Проверимо рачуном да (3.4) ради исто што и (3.3). Применимо U_w на означени базни вектор $|w\rangle$:

$$U_w|w\rangle = |w\rangle - 2|w\rangle\langle w|w\rangle = |w\rangle - 2|w\rangle = -|w\rangle,$$

јер је $\langle w|w\rangle = 1$. Применимо га на било који други базни вектор $|i\rangle$, $i \neq w$:

$$U_w|i\rangle = |i\rangle - 2|w\rangle\langle w|i\rangle = |i\rangle - 0 = |i\rangle,$$

јер су различити базни вектори нормални један на други, $\langle w|i\rangle = 0$. Означени вектор добија знак минус, а сваки други се множи са 1. На произвољно стање $|\psi\rangle$ оператор делује исто: по (2.9) је $\langle w|\psi\rangle = a_w$, па је

$$U_w|\psi\rangle = |\psi\rangle - 2a_w|w\rangle.$$

Компоненту $a_w|w\rangle$ одузели смо двапут, па од ње остаје $-a_w|w\rangle$, а остале компоненте се не мењају.

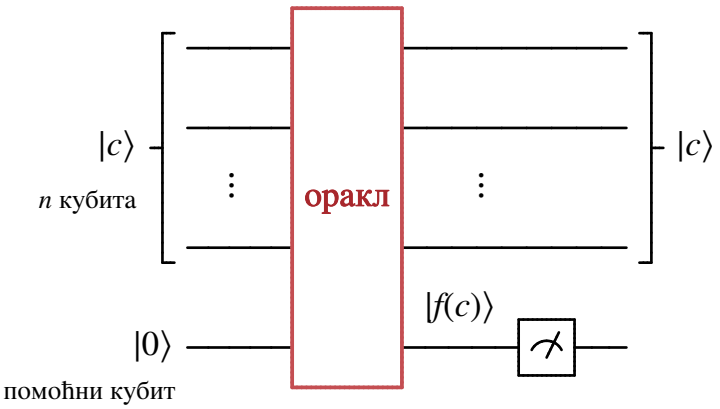
Геометријски, оракл је огледало: мења смер једном правцу, $|w\rangle$, а све што је нормално на њега оставља. Једна примена оракла је један упит. Други дозвољени начин, упис одговора у додатни кубит, делује на $n+1$ кубит: на n кубита кандидата и на тај додатни. Оба начина упоредићемо у §3.7: видећемо да су то два лица истог кола, и зашто Гровер бира знак.

3.7 Зашто сам оракл није довољан

Хајде сада да оракл употребимо, и то прво онако како бисмо то урадили и на обичном рачунару, проверавајући једног по једног кандидата. Оракл је направљен од провере (§3.5), а провера која ништа не брише свој одговор уписује у један додатни кубит, који зовемо **помоћни кубит**. Кандидата, једну од N могућности из §3.4, записујемо у n кубита, као базно стање $|c\rangle$, а помоћни кубит постављамо у стање $|0\rangle$ (Слика 3.1). Заједничко стање пишемо $|c\rangle|0\rangle$, што је кратак запис за $|c\rangle \otimes |0\rangle$ из §2.4. Оракл је сада коло на $n+1$ кубиту: кандидата оставља какав јесте, а у помоћни кубит уписује одговор:

$$|c\rangle|0\rangle \longmapsto |c\rangle\,|f(c)\rangle.$$

Када измеримо помоћни кубит, добијамо $f(c)$: јединицу ако је c тражени елемент, а нулу ако није. Један упит тако провери тачно једног кандидата, баш као обична провера. Зато нам треба исто колико и обичном рачунару, у просеку око $N/2$ упита (§3.2). Када кандидате проверавамо појединачно, квантни рачунар не доноси убрзање у броју упита.



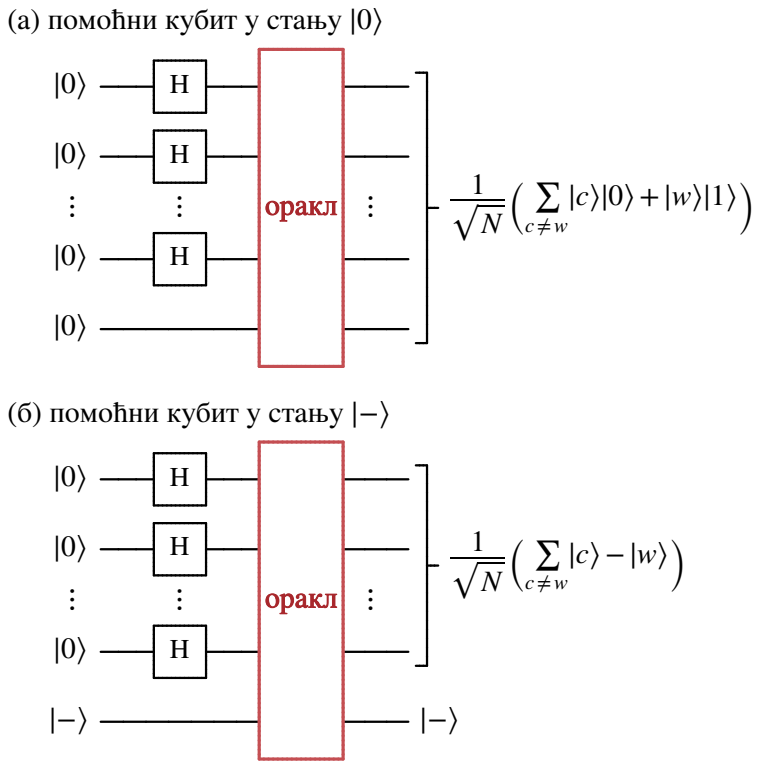
Слика 3.1. Класична употреба оракла. Горњих n кубита носи кандидата, базно стање $|c\rangle$, а доњи, помоћни кубит почиње у стању $|0\rangle$. Оракл кандидата не мења, а у помоћни кубит упише одговор $f(c)$. Мерење помоћног кубита покаже 1 ако је c тражени елемент, а 0 ако није. Мали бројчаник са казаљком на крају линије означава мерење.

Можда је снага квантног рачунара у суперпозицији? Пробајмо да оракл провери све кандидате одједном. Слојем капија H прво направимо стање $|s\rangle$, у коме сви кандидати имају исту амплитуду $1/\sqrt{N}$, а помоћни кубит, као малопре, поставимо у стање $|0\rangle$ (Слика 3.2а). Оракл делује на сваки сабирак посебно, па после једног упита стање гласи

$$\frac{1}{\sqrt{N}} \sum_{c \neq w} |c\rangle|0\rangle + \frac{1}{\sqrt{N}} |w\rangle|1\rangle.$$

Изгледа као да је оракл једним упитом проверио све кандидате: уз тражени елемент помоћни кубит сада показује 1, а уз све остале 0. Али шта показује мерење? Мерење покаже само једног кандидата c и уз њега бит $f(c)$, и то сваки такав пар са вероватноћом $(1/\sqrt{N})^2 = 1/N$. Помоћни

кубит показаће 1, а уз њега и тражени елемент, само са вероватноћом $1/N$, исто као када насумично изаберемо једног кандидата и проверимо га. Ако нешто успева са вероватноћом $1/N$, у просеку треба око N покушаја, као што за шестицу на коцкици у просеку треба шест бацања. То је чак горе од провере редом, којој треба око $N/2$ упита. Оракл је, дакле, заиста деловао на све кандидате одједном, али од тога нема користи: мерење покаже само један, насумичан исход.



Слика 3.2. Исти оракл на стању $|s\rangle$, које прави слој капија H. (а) Са помоћним кубитом у стању $|0\rangle$ оракл уз сваког кандидата упише одговор: уз w јединицу, а уз све остале нулу. (б) Са помоћним кубитом у стању $|-\rangle$ оракл само промени знак амплитуди w, а помоћни кубит остаје $|-\rangle$. Мерење у оба случаја покаже тражени елемент тек са вероватноћом $1/N$.

Гроверов алгоритам помоћни кубит не поставља у стање $|0\rangle$, него у стање $|-\rangle$ (Слика 3.2б). Тада оракл не уписује одговор, него мења знак, као у (3.3), а сам помоћни кубит остаје непромењен. Како стање $|-\rangle$ то постиже? Погледајмо оракл изблиза, у три корака.

Први корак: условно обртање помоћног кубита. Подсетимо се шта ради капија CNOT (§2.8). Она има контролни и циљни кубит: циљни обрне ако је контролни 1, а иначе не ради ништа. Записано за базна стања, $|a\rangle|b\rangle \mapsto |a\rangle|b\oplus a\rangle$, где је $\oplus$ збир по модулу 2: $0\oplus 0 = 1\oplus 1 = 0$ и $0\oplus 1 = 1\oplus 0 = 1$. Оракл ради исто, са кандидатом и помоћним кубитом: помоћни кубит обрне ако кандидат пролази проверу, а иначе не ради ништа; ако је h бит помоћног кубита,

$$|c\rangle|h\rangle \;\longmapsto\; |c\rangle\,|h\oplus f(c)\rangle.$$

Облик је исти као код CNOT, само уместо контролног бита a стоји одговор провере, $f(c)$. Најлакше се то види на најмањем примеру, $N=2$. Кандидат је тада један кубит; нека је тражени елемент $w=1$. Провера каже „да“ тачно када је кандидат 1, тј. $f(c)=c$, па правило гласи $|c\rangle|h\rangle \mapsto |c\rangle|h\oplus c\rangle$. То је дословно CNOT: кандидат је контролни кубит, а помоћни кубит циљни. За $w=0$ провера каже „да“ када је кандидат 0; зато пре и после капије CNOT на кандидата

ставимо капију X, па контрола реагује на 0 уместо на 1. За два кубита кандидата и $w = 11$ помоћни кубит треба обрнути само када су оба кубита кандидата 1: то је CNOT са две контроле, Тофолијева капија из §3.17. Исто важи за сваку проверу која се може направити од капија: коло израчуна $f(c)$ не бришући кандидата, тај резултат управља капијом X на помоћном кубиту, а онда коло свој помоћни рачун поништи, па од целе провере остане само промена на помоћном кубиту. **У општем случају оракл је коло које условно обрће помоћни кубит; једна капија** CNOT **довољна је само за посебне провере.**

Други корак: шта капија X **ради помоћном кубиту.** Капија X замени две амплитуде кубита: амплитуду уз $|0\rangle$ и амплитуду уз $|1\rangle$. Шта та замена значи, зависи од стања помоћног кубита (Слика 3.3а–в). Стање $|0\rangle$ има амплитуде 1 и 0, а после замене 0 и 1: то је друго стање, $|1\rangle$. Одговор је тада уписан у помоћни кубит, као у класичној провери. Стање $|+\rangle$ има две једнаке амплитуде, $1/\sqrt{2}$, па замена не мења ништа: $\mathrm{X}|+\rangle = |+\rangle$. **Са помоћним кубитом у стању** $|+\rangle$ **оракл не ради ништа:** нити упише одговор, нити промени знак, па упит ништа не открије. Стање $|-\rangle$ има амплитуде $1/\sqrt{2}$ и $-1/\sqrt{2}$, а после замене $-1/\sqrt{2}$ и $1/\sqrt{2}$. То је исто стање, само помножено са -1:

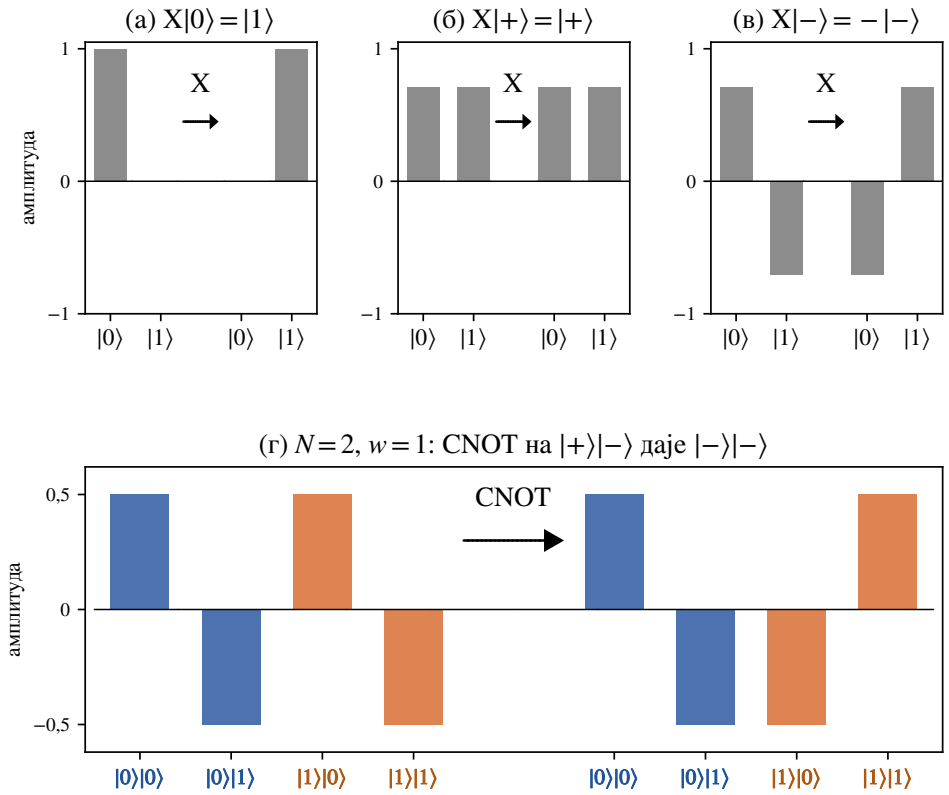
$$\mathrm{X}|-\rangle = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle.$$

Капија X, дакле, стање $|-\rangle$ не претвара у неко друго стање: само га помножи са -1.

Трећи корак: минус прелази на кандидата. Ставимо помоћни кубит у стање $|-\rangle$. За тражени елемент оракл обрне помоћни кубит, па $|w\rangle|-\rangle$ постаје $|w\rangle(-|-\rangle) = -|w\rangle|-\rangle$. За сваког другог кандидата c стање $|c\rangle|-\rangle$ остаје какво јесте. Укратко,

$$|c\rangle|-\rangle \longmapsto (-1)^{f(c)}\,|c\rangle|-\rangle.$$

Минус који стоји испред производа можемо да припишемо кандидату: тражени кандидат добија минус, а остали не. Ако на улазу стоји суперпозиција кандидата, исто се деси у сваком сабирку посебно, а помоћни кубит у сваком сабирку остаје $|-\rangle$. На кандидатима зато остаје баш оракл (3.3). Слика 3.3г то показује на најмањем примеру, $N = 2$ и $w = 1$, где је оракл сам CNOT. Стање $|+\rangle|-\rangle$ има четири амплитуде, $1/2, -1/2, 1/2$ и $-1/2$. CNOT замени две амплитуде помоћног кубита само уз кандидата 1. Тај пар је $1/2$ и $-1/2$, па замена даје $-1/2$ и $1/2$: исто што и минус на целом пару. Излаз је $|-\rangle|-\rangle$: кандидат је добио минус уз w, а помоћни кубит је остао $|-\rangle$. Знак је „одскочио“ са помоћног кубита на кандидата; на енглеском се ова појава зове *phase kickback*.



Слика 3.3. Како помоћни кубит у стању $|-\rangle$ претвара упис у знак. Капија X замени две амплитуде кубита (сиво, пре и после стрелице). (а) Стање $|0\rangle$ постаје друго стање, $|1\rangle$: одговор се упише. (б) Стање $|+\rangle$ остаје исто: оракл не ради ништа. (в) Стање $|-\rangle$ остаје исто, само са знаком минус. (г) $N = 2$ и $w = 1$, где је оракл баш CNOT: од четири амплитуде стања $|+\rangle|-\rangle$ замене се само две, уз кандидата 1 (наранџасто), а то је исто што и минус на том пару. Излаз је $|-\rangle|-\rangle$: кандидат је добио минус, а помоћни кубит је остао $|-\rangle$.

Зашто онда помоћни кубит припремамо у стању $|-\rangle$, а не у стању $|0\rangle$? Са помоћним кубитом у стању $|0\rangle$ оракл уписује одговор $f(c)$, као што смо видели (Слика 3.2а). Ако је регистар кандидата у суперпозицији, после упита он може бити спрегнут са помоћним кубитом. То можемо разумети и ако напишемо $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$: део са $|+\rangle$ остаје непромењен, док део са $|-\rangle$ добија знак који зависи од $f(c)$. Оба дела заједно дају упис одговора у помоћни кубит. Када је он од почетка у стању $|-\rangle$, после упита се може издвојити из заједничког стања, а оракл је променио знак амплитуде означеног кандидата. Зато у следећем кораку можемо да пратимо само регистар кандидата.

Шта је, дакле, оракл? Разматрали смо два повезана начина да представимо проверу. Први је реверзибилно коло које на регистру кандидата и помоћном кубиту делује као

$$U_f|c\rangle|h\rangle = |c\rangle|h \oplus f(c)\rangle.$$

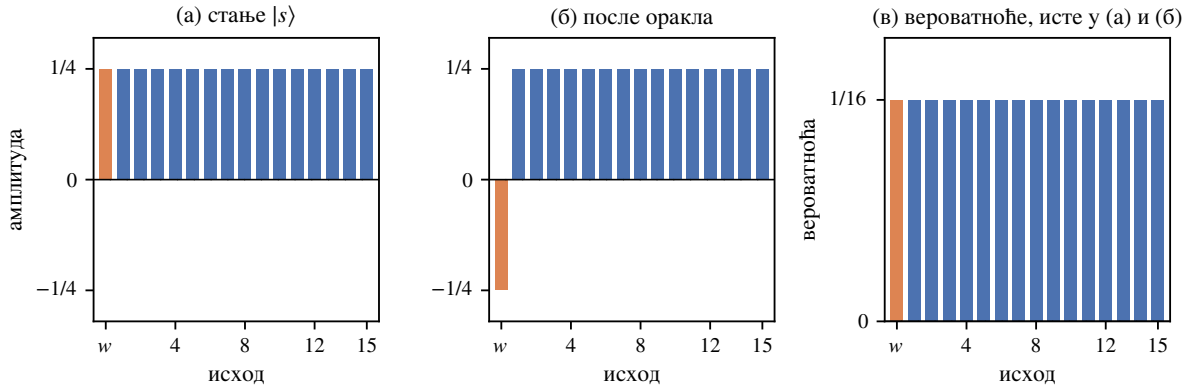
Када је помоћни кубит у стању $|0\rangle$, у њега се уписује резултат провере. Ако га припремимо у стању $|-\rangle$, исти оператор мења знак амплитуде сваког кандидата за који је $f(c) = 1$, док помоћни кубит остаје у стању $|-\rangle$. Тако на регистру кандидата добијамо дејство фазног оракла, $|c\rangle \mapsto (-1)^{f(c)}|c\rangle$. За једно означено стање то је оператор U_w из (3.3).

Ово је један начин да остваримо фазни оракл, али не и једини. У једноставним примерима можемо га извести и непосредно, без помоћног кубита, као што ћемо видети у §3.16. За сложеније провере могу бити потребни и додатни радни кубити. Ако их користимо за привремено

рачунање, морамо их вратити у почетно стање да не би остали спрегнути са регистром кандидата.

У наставку дејство оракла описујемо фазним оператором U_w на простору кандидата. Његова дефиниција казује шта оператор ради, али не прописује једини начин на који се он може остварити.

После једног упита оракл је променио знак амплитуди w, и само њој (Слика 3.4а, б). Једним упитом означили смо решење! Али ни сада мерење не помаже. Вероватноћа је $(1/\sqrt{N})^2 = 1/N$ за сваку неозначену могућност и $(-1/\sqrt{N})^2 = 1/N$ за означену, исто као пре упита (Слика 3.4в). Мерење је и даље насумично погађање, а ни понављање огледа не помаже: ако оглед поновимо много пута, свих N исхода видећемо подједнако често. Знак минус стоји баш на месту w, али мерење знак не види.



Слика 3.4. Шеснаест амплитуда, $N = 16$; амплитуда означеног елемента w је наранџаста, остале су плаве. (а) Стање $|s\rangle$: све амплитуде су 1/4. (б) После једног упита оракл је амплитуди w променио знак. (в) Вероватноће су у оба случаја исте, 1/16: мерење не види знак.

Сам оракл, дакле, није довољан. Потребан нам је још један корак, који више не пита оракл, него искористи знак који је оракл оставио: амплитуду означене могућности повећа, а амплитуде свих осталих смањи. Тада расте и вероватноћа да мерење покаже баш w. Видели смо да тако нешто може да се уради.

Кључна идеја

Стања $|+\rangle$ и $|-\rangle$ разликују се само у знаку једне амплитуде, па их мерење не разликује. Али после још једне капије H она постају $|0\rangle$ и $|1\rangle$, а њих мерење разликује сигурно (§2.6):

$$|+\rangle \xrightarrow{\text{H}} |0\rangle, \qquad |-\rangle \xrightarrow{\text{H}} |1\rangle.$$

Други корак, после оракла, ради исто то, али са свих N амплитуда.

Да бисмо разумели и оракл и тај нови корак, погледаћемо их геометријски: показаће се да су оба корака огледања.

3.8 Дејство оракла на почетно стање

Сада прелазимо на геометрију. Гроверов алгоритам [5] користи два огледања, и сва геометрија коју смо видели код блокова поновиће се овде.

Вратимо се ораклу какав је у (3.4):

$$U_w = \mathbb{1} - 2|w\rangle\langle w|.$$

Он мења знак само делу стања дуж $|w\rangle$, а све што је нормално на $|w\rangle$ оставља какво јесте. Погледајмо шта то значи за стање на које га примењујемо.

Оракл примењујемо на почетно стање Гроверовог алгоритма, $|s\rangle$ из (2.7). Њега слој капија H направи од $|0\ldots0\rangle$ (§2.7), и у њему сви елементи имају исту амплитуду, $1/\sqrt{N}$. Раставимо $|s\rangle$ на два дела, нормална један на други.

Први део је дуж $|w\rangle$. По (2.9) компонента стања $|s\rangle$ дуж $|w\rangle$ је $\langle w|s\rangle = 1/\sqrt{N}$, па је тај део $|w\rangle/\sqrt{N}$.

Други део је остатак: збир свих осталих базних вектора, сваки са амплитудом $1/\sqrt{N}$. Квадрат његове дужине је збир квадрата $N-1$ таквих амплитуда, $(N-1)/N$. Када остатак поделимо његовом дужином, $\sqrt{(N-1)/N}$, добијамо јединични вектор

$$|\bar{s}\rangle = \frac{1}{\sqrt{N-1}} \sum_{i\neq w} |i\rangle,$$

у коме сви неозначени елементи имају исту амплитуду, а означени елемент нулу. Црта изнад s подсећа да у њему нема означеног елемента. Вектори $|w\rangle$ и $|\bar{s}\rangle$ су међусобно нормални, $\langle w|\bar{s}\rangle = 0$, јер немају ниједну заједничку компоненту различиту од нуле. Почетно стање је збир та два дела:

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|\bar{s}\rangle = \sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle, \qquad \sin\bar{\theta} = \frac{1}{\sqrt{N}} \tag{3.5}$$

Нацртајмо раван коју разапињу $|\bar{s}\rangle$ и $|w\rangle$, са $|\bar{s}\rangle$ водоравно и $|w\rangle$ усправно (Слика 3.5а). Праву кроз $|\bar{s}\rangle$ зваћемо **осом** $|\bar{s}\rangle$, а праву кроз $|w\rangle$ осом $|w\rangle$. Стање $|s\rangle$ је у овој равни јединична стрелица под углом $\bar{\theta}$ изнад осе $|\bar{s}\rangle$. Њена пројекција на осу $|\bar{s}\rangle$ је $\cos\bar{\theta}$, а на осу $|w\rangle$ износи $\sin\bar{\theta}$. За велико N угао $\bar{\theta}$ је мали: почетно стање је скоро нормално на одговор $|w\rangle$. Угао смо намерно обележили истим словом као угао код блокова (§1.10): у §4.2 видећемо да је то исти угао.

Применимо сада оракл на $|s\rangle$. По (3.5) је $\langle w|s\rangle = \sin\bar{\theta}$, па је

$$U_w|s\rangle = |s\rangle - 2\langle w|s\rangle\,|w\rangle = \big(\sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle\big) - 2\sin\bar{\theta}\,|w\rangle = -\sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle.$$

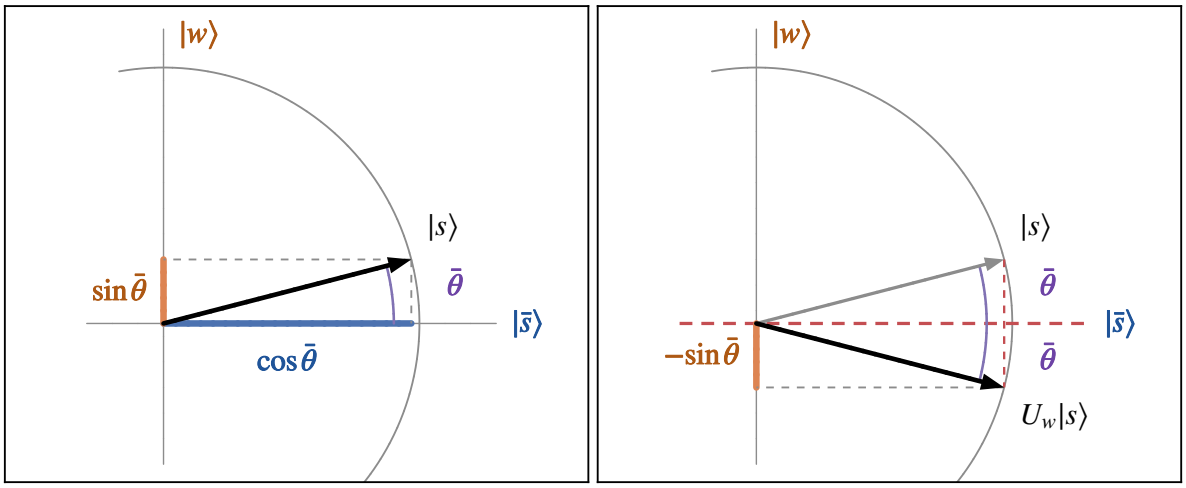
Део дуж осе $|\bar{s}\rangle$ остао је исти, а део дуж $|w\rangle$ променио је знак. Стрелица је била за угао $\bar{\theta}$ изнад осе $|\bar{s}\rangle$, а сада је за исти угао испод ње (Слика 3.5б). Стање $U_w|s\rangle$ је, дакле, слика стања $|s\rangle$ у огледалу постављеном дуж осе $|\bar{s}\rangle$: **оракл је, у равни вектора $|\bar{s}\rangle$ и $|w\rangle$, огледање у односу на осу $|\bar{s}\rangle$.**

3.9 Оракл као огледање

У §3.8 видели смо шта оракл ради са једним стањем, $|s\rangle$. Сада ћемо рачуном показати да исто ради са сваким стањем ове равни, тј. да је оракл заиста огледање у односу на осу $|\bar{s}\rangle$.

Прво кажимо тачно шта значи огледање у односу на осу. У школи се то зове осна симетрија: свака тачка прелази у тачку са друге стране осе, на истом растојању од ње. За стрелицу то

(а) два дела стања $|s\rangle$ (б) оракл: огледање у односу на осу $|\bar{s}\rangle$



Слика 3.5. Раван коју разапињу $|\bar{s}\rangle$ и $|w\rangle$, за $N = 16$. (а) Почетно стање $|s\rangle$ и његова два дела: дуж осе $|\bar{s}\rangle$ (плаво, $\cos\bar{\theta}$) и дуж осе $|w\rangle$ (наранџасто, $\sin\bar{\theta}$). (б) Оракл мења знак делу дуж $|w\rangle$, а део дуж осе $|\bar{s}\rangle$ оставља: $U_w|s\rangle$ је слика стања $|s\rangle$ у огледалу на оси $|\bar{s}\rangle$ (црвено), за угао $\bar{\theta}$ испод ње.

значи следеће. Раставимо стање $|\psi\rangle$ на део дуж осе, $|\psi_\parallel\rangle$, и део нормалан на осу, $|\psi_\perp\rangle$ (знак $\parallel$ читамо „паралелно“, а знак $\perp$ „нормално“):

$$|\psi\rangle = |\psi_\parallel\rangle + |\psi_\perp\rangle.$$

Огледање задржава део дуж осе, а делу нормалном на осу мења знак:

$$|\psi_\parallel\rangle + |\psi_\perp\rangle \longmapsto |\psi_\parallel\rangle - |\psi_\perp\rangle \tag{3.6}$$

Из ове дефиниције одмах следе два својства. Двапут примењено, огледање враћа свако стање на почетак, јер део нормалан на осу двапут промени знак. И огледање не мења дужину стања. Делови $|\psi_\parallel\rangle$ и $|\psi_\perp\rangle$ су међусобно нормални, па је по Питагориној теореми квадрат дужине стања збир квадрата њихових дужина, и пре и после огледања (в. задатак 56). Огледање је, дакле, дозвољен корак (правило 3).

Пређимо сада на оракл. Свако стање у равни коју разапињу $|\bar{s}\rangle$ и $|w\rangle$ можемо да напишемо као

$$|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle,$$

где су x и y бројеви: координате врха стрелице, x дуж осе $|\bar{s}\rangle$, а y дуж осе $|w\rangle$. Почетно стање, на пример, има $x = \cos\bar{\theta}$ и $y = \sin\bar{\theta}$, по (3.5). Оса $|w\rangle$ је нормална на осу $|\bar{s}\rangle$, па је део стања дуж осе $|\bar{s}\rangle$ једнак $|\psi_\parallel\rangle = x\,|\bar{s}\rangle$, а део нормалан на ту осу $|\psi_\perp\rangle = y\,|w\rangle$ (Слика 3.6а).

Применимо оракл на $|\psi\rangle$, корак по корак. Прво помножимо заграде:

$$U_w|\psi\rangle = \big(\mathbb{1} - 2|w\rangle\langle w|\big)\big(x\,|\bar{s}\rangle + y\,|w\rangle\big) = x\,|\bar{s}\rangle + y\,|w\rangle - 2|w\rangle\big(x\,\langle w|\bar{s}\rangle + y\,\langle w|w\rangle\big).$$

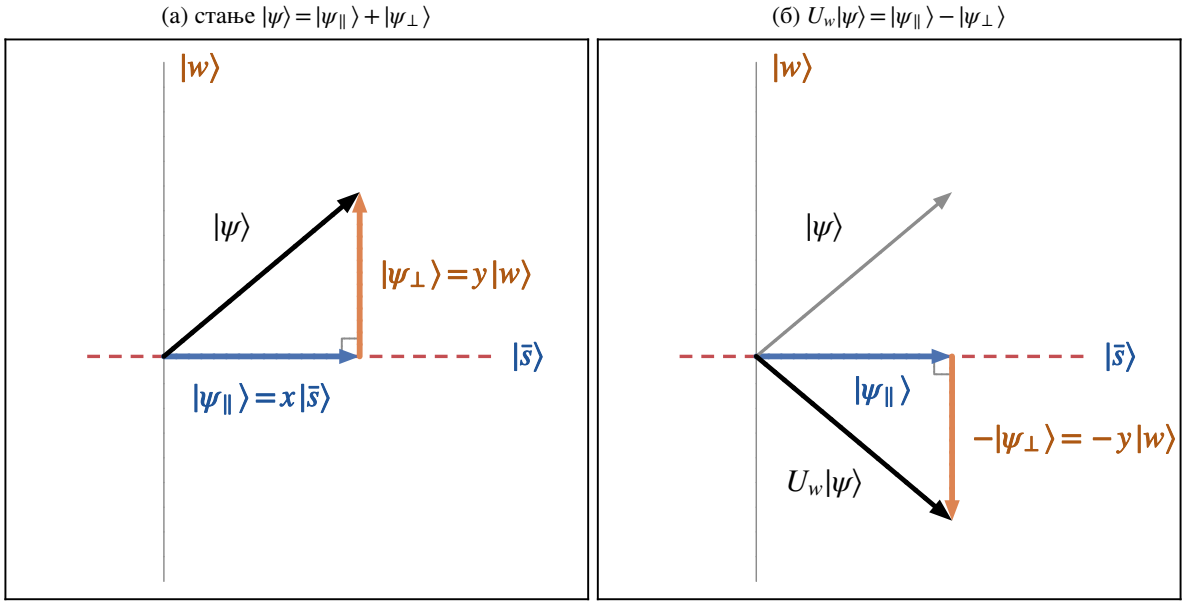
У последњој загради су два скаларна производа: $\langle w|\bar{s}\rangle = 0$, јер су $|w\rangle$ и $|\bar{s}\rangle$ међусобно нормални, и $\langle w|w\rangle = 1$, јер је $|w\rangle$ јединични. Заграда је зато једнака y, па је

$$U_w|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle - 2y\,|w\rangle = x\,|\bar{s}\rangle - y\,|w\rangle.$$

Дакле:

$$U_w\big(x\,|\bar{s}\rangle + y\,|w\rangle\big) = x\,|\bar{s}\rangle - y\,|w\rangle, \qquad \text{тј.} \qquad (x,y) \longmapsto (x,-y) \tag{3.7}$$

Део дуж осе $|\bar{s}\rangle$ остао је исти, а део нормалан на ту осу променио је знак: то је тачно огледање (3.6), са осом $|\bar{s}\rangle$ (Слика 3.6б). У координатама, $(x,y) \mapsto (x,-y)$ је осна симетрија у односу на x-осу, исто што и одбијање од зида код блокова (§1.7). Нигде нисмо користили да је стање баш $|s\rangle$, па оракл огледа у односу на осу $|\bar{s}\rangle$ свако стање ове равни. Ван те равни, међутим, U_w и огледање у односу на осу $|\bar{s}\rangle$ нису исто. Огледање у односу на осу $|\bar{s}\rangle$ мења знак свему што је нормално на ту осу, а у N димензија таквих праваца има $N-1$. U_w мења знак само једном од њих, правцу $|w\rangle$. У равни је то исто, јер је тамо $|w\rangle$ једини правац нормалан на $|\bar{s}\rangle$. Ево примера са само три правца, без кубита: за $N=3$ и $w=0$ вектор $(|1\rangle - |2\rangle)/\sqrt{2}$ нормалан је и на $|w\rangle$ и на $|\bar{s}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$. U_w га оставља какав јесте, а огледање у односу на осу $|\bar{s}\rangle$ променило би му знак. Гроверов алгоритам, међутим, раван никад не напусти (§3.12), па нам је довољно оно што важи у равни.



Слика 3.6. Оракл на произвољном стању $|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle$. (а) Део дуж осе $|\bar{s}\rangle$, $|\psi_\parallel\rangle = x\,|\bar{s}\rangle$ (плаво), и део нормалан на ту осу, $|\psi_\perp\rangle = y\,|w\rangle$ (наранџасто). (б) Оракл задржава $|\psi_\parallel\rangle$, а делу $|\psi_\perp\rangle$ мења знак: $U_w|\psi\rangle = |\psi_\parallel\rangle - |\psi_\perp\rangle$ је слика стања $|\psi\rangle$ у огледалу на оси $|\bar{s}\rangle$ (црвено).

3.10 Дифузија: огледање у односу на осу $|s\rangle$

Сам оракл није довољан (§3.7): после њега мерење и даље не види знак. Треба нам други оператор, онај који недостаје. И он је огледање, овога пута у односу на осу кроз само почетно стање, **осу** $|s\rangle$:

$$U_s = 2|s\rangle\langle s| - \mathbb{1} \tag{3.8}$$

Овај оператор се зове **дифузија**; зашто баш тако, видећемо на крају одељка.

Покажимо рачуном, истим путем као за оракл, да је U_s огледање у односу на осу $|s\rangle$. Раставимо произвољно стање $|\psi\rangle$ на део дуж осе $|s\rangle$ и део нормалан на њу. Део дуж осе је пројекција стања

$|\psi\rangle$ на $|s\rangle$ (§2.9):

$$|\psi_{\parallel}\rangle = \langle s|\psi\rangle\,|s\rangle.$$

Део нормалан на осу је остатак:

$$|\psi_{\perp}\rangle = |\psi\rangle - \langle s|\psi\rangle\,|s\rangle.$$

Остатак је заиста нормалан на осу. Његов скаларни производ са $|s\rangle$ је нула, јер је $\langle s|s\rangle = 1$:

$$\langle s|\psi_{\perp}\rangle = \langle s|\psi\rangle - \langle s|\psi\rangle\langle s|s\rangle = \langle s|\psi\rangle - \langle s|\psi\rangle = 0.$$

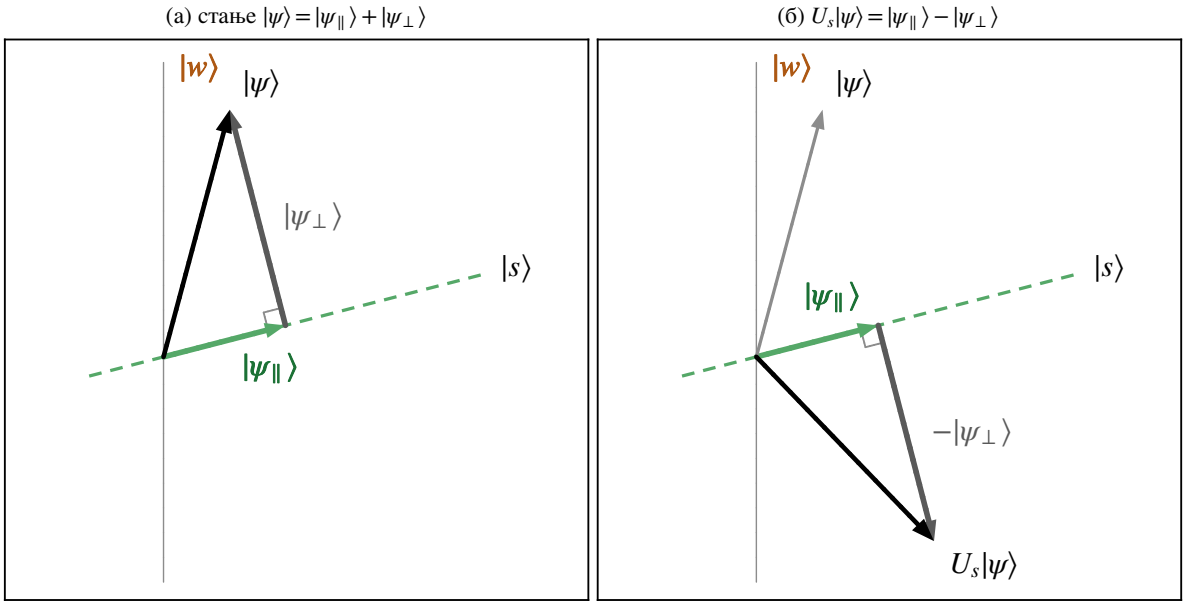
Применимо сада U_s на $|\psi\rangle$, корак по корак. Прво помножимо:

$$U_s|\psi\rangle = \big(2|s\rangle\langle s| - \mathbb{1}\big)|\psi\rangle = 2\langle s|\psi\rangle\,|s\rangle - |\psi\rangle.$$

Први сабирак је двапут део дуж осе, $2|\psi_{\parallel}\rangle$, а други је цело стање, $|\psi\rangle = |\psi_{\parallel}\rangle + |\psi_{\perp}\rangle$. Зато је

$$U_s|\psi\rangle = 2|\psi_{\parallel}\rangle - |\psi_{\parallel}\rangle - |\psi_{\perp}\rangle = |\psi_{\parallel}\rangle - |\psi_{\perp}\rangle.$$

Део дуж осе $|s\rangle$ остао је исти, а део нормалан на њу променио је знак: то је огледање (3.6), са осом $|s\rangle$ (Слика 3.7). Посебно, стање на оси остаје исто, $U_s|s\rangle = |s\rangle$, а стању нормалном на осу мења се знак.



Слика 3.7. Дифузија на произвољном стању $|\psi\rangle$. (а) Део дуж осе $|s\rangle$, $|\psi_{\parallel}\rangle = \langle s|\psi\rangle\,|s\rangle$ (зелено), и остатак, $|\psi_{\perp}\rangle$, нормалан на осу (сиво). (б) U_s задржава $|\psi_{\parallel}\rangle$, а делу $|\psi_{\perp}\rangle$ мења знак: $U_s|\psi\rangle = |\psi_{\parallel}\rangle - |\psi_{\perp}\rangle$ је слика стања $|\psi\rangle$ у огледалу на оси $|s\rangle$ (зелена испрекидана права).

Рачун нигде није користио да је $|s\rangle$ баш почетно стање, него само да је јединични вектор. Зато исто важи за осу кроз било који јединични вектор $|u\rangle$: огледање у односу на осу $|u\rangle$ је

$$\big(2|u\rangle\langle u| - \mathbb{1}\big)|\psi\rangle = 2\langle u|\psi\rangle\,|u\rangle - |\psi\rangle \tag{3.9}$$

Срешћемо га још једном, код блокова (четврто поглавље).

При мерењу у рачунској бази добијамо један исход i, са вероватноћом a_i^2. Погледајмо зато како огледање мења амплитуде, а тиме и вероватноће могућих исхода. Правило ће бити врло једноставно, а у §3.14 ћемо помоћу њега видети како амплитуда означеног елемента расте. Нека је $|\psi\rangle = \sum_i a_i|i\rangle$. По (2.8) скаларни производ са $|s\rangle$ је

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_i a_i = \sqrt{N}\,\bar{a},$$

где је $\bar{a}$ аритметичка средина амплитуда, њихов збир подељен са N. Део дуж осе $|s\rangle$ је зато

$$|\psi_{\|}\rangle = \langle s|\psi\rangle\,|s\rangle = \sqrt{N}\,\bar{a} \cdot \frac{1}{\sqrt{N}}\,(1, 1, \ldots, 1) = \bar{a}\,(1, 1, \ldots, 1),$$

вектор чија је свака компонента једнака средини. Компонента i стања $U_s|\psi\rangle = 2|\psi_{\|}\rangle - |\psi\rangle$ је, дакле, $2\bar{a} - a_i$:

$$a_i \longmapsto 2\bar{a} - a_i \tag{3.10}$$

Свака амплитуда прелази на другу страну средине, на исто растојање од ње: ако је била за 3 изнад средине, сада је за 3 испод. Средина се при томе не мења (в. задатак 57). Ово зовемо **одраз у односу на аритметичку средину**; код блокова средина ће бити брзина центра масе (§4.3).

Остаје још да објаснимо име. Гровер овај корак зове „трансформација дифузије“ и показује да је то одраз у односу на средину [5], али име не објашњава. По (3.10) свака нова амплитуда зависи од свих старих, преко њихове средине. Ако је на почетку, рецимо, сва амплитуда на једном елементу, $a_j = 1$, средина је $1/N$, па после дифузије сваки други елемент добије амплитуду $2/N$. Мали део амплитуде разлије се тако подједнако по свим елементима, као кап мастила у води. Тако је име касније објаснио и сам Гровер: његов корак личи на дифузију, у којој из сваког стања у свако друго прелази по мало [9]. Код Гровера се ти мали делови, захваљујући знаку који је дао оракл, саберу баш на означеном елементу.

3.11 Два огледања дају ротацију

Један **Гроверов корак** је оракл, па дифузија: $U_s U_w$ (оператор који делује први пише се десно). То су два огледања, у односу на осе $|\bar{s}\rangle$ и $|s\rangle$, које заклапају угао $\bar{\theta}$. Покажимо да два огледања заједно окрећу стрелицу, и то за двоструки угао између оса.

Углове меримо од осе $|\bar{s}\rangle$, у позитивном смеру, супротно од кретања казаљке на сату. Стање под углом φ је $|\psi\rangle = \cos\varphi\,|\bar{s}\rangle + \sin\varphi\,|w\rangle$; почетно стање има $\varphi = \bar{\theta}$, по (3.5).

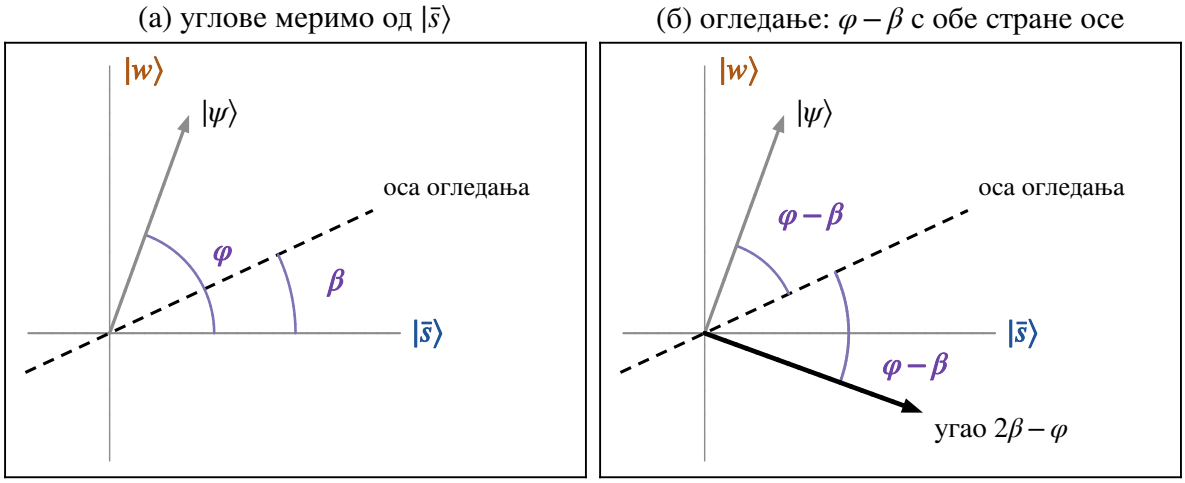
Шта огледање ради са углом? Узмимо било коју осу огледања у овој равни, праву кроз координатни почетак, и означимо са β угао који **та оса** заклапа са осом $|\bar{s}\rangle$ (Слика 3.8а). Пазите: β је угао саме осе, а не неког стања, и не мења се од корака до корака. За оракл оса је баш $|\bar{s}\rangle$, па је $\beta = 0$; за дифузију оса је $|s\rangle$, па је $\beta = \bar{\theta}$. Стрелица је под углом φ од осе $|\bar{s}\rangle$, па је од осе огледања удаљена за угао $\varphi - \beta$: део дуж осе је $\cos(\varphi - \beta)$, а део нормалан на осу $\sin(\varphi - \beta)$. Огледање (3.6) мења знак само другом делу, па стрелица прелази на исто растојање са друге стране осе, на угао $-(\varphi - \beta)$ мерен од осе (Слика 3.8б). Мерено од осе $|\bar{s}\rangle$, то је угао $\beta - (\varphi - \beta)$:

$$\varphi \longmapsto 2\beta - \varphi. \tag{3.11}$$

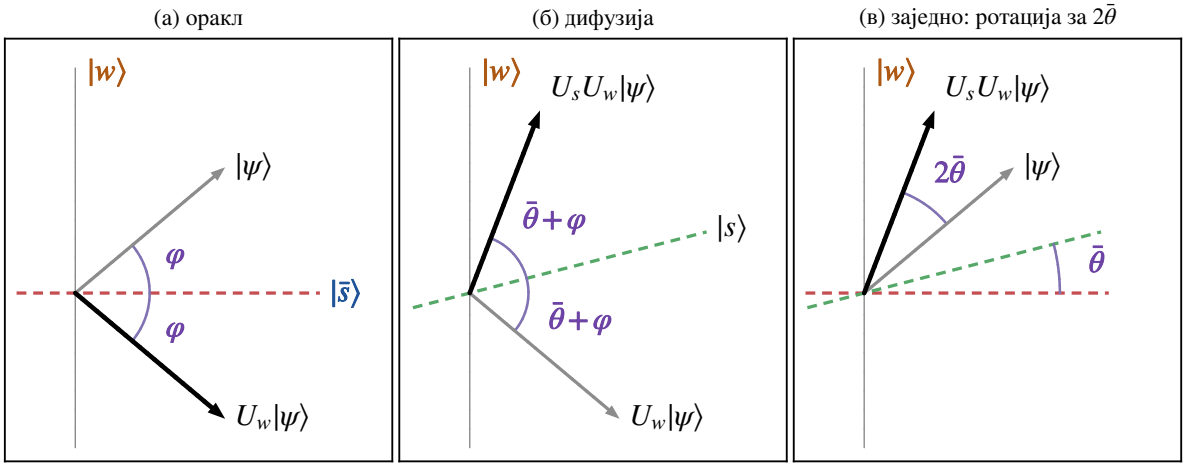
Оса $|\bar{s}\rangle$ има угао $\beta = 0$, па оракл шаље φ у $-\varphi$; то је $(x, y) \mapsto (x, -y)$ из (3.7). Оса $|s\rangle$ има угао $\beta = \bar{\theta}$, па дифузија шаље φ у $2\bar{\theta} - \varphi$. Један Гроверов корак, оракл па дифузија, даје зато

$$\varphi \xrightarrow{U_w} -\varphi \xrightarrow{U_s} 2\bar{\theta} - (-\varphi) = \varphi + 2\bar{\theta}.$$

Свака стрелица се окренула за исти угао, $2\bar{\theta}$, без обзира на свој почетни угао φ: то је ротација (Слика 3.9).



Слика 3.8. Шта је β. (а) Углове меримо од осе $|\bar{s}\rangle$: стрелица $|\psi\rangle$ је под углом φ, а оса огледања, права кроз координатни почетак, под углом β. Угао β припада оси, а не стању: за оракл је $\beta = 0$, а за дифузију $\beta = \bar{\theta}$. (б) Стрелица је од осе удаљена за угао $\varphi - \beta$; огледање је пребаци на исто растојање са друге стране осе, на угао $2\beta - \varphi$ мерен од осе $|\bar{s}\rangle$.



Слика 3.9. Два огледања дају ротацију, $N = 16$. (а) Оракл, огледање у односу на осу $|\bar{s}\rangle$ (црвено), шаље стање под углом φ на угао $-\varphi$. (б) Дифузија, огледање у односу на осу $|s\rangle$ (зелено), под углом $\bar{\theta}$, пребацује га на другу страну те осе, на исто растојање, $\bar{\theta} + \varphi$. (в) Заједно: стање се окренуло за $2\bar{\theta}$, двоструки угао између оса.

Исти рачун важи за било које две осе. Ако прва има угао β_1, а друга β_2, огледање у односу на прву, па у односу на другу, даје

$$\varphi \longmapsto 2\beta_1 - \varphi \longmapsto 2\beta_2 - (2\beta_1 - \varphi) = \varphi + 2(\beta_2 - \beta_1).$$

Ако осе заклапају угао $\alpha = \beta_2 - \beta_1$:

$$\text{огледање у односу на прву осу, па у односу на другу} \;=\; \text{ротација за } 2\alpha \tag{3.12}$$

Ротација је двоструко већа од угла између оса. Редослед је важан: обрнут редослед даје ротацију за -2α, на другу страну (в. задатак 63). Ако су осе скоро поклопљене, ротација је мала, и треба много корака да се стрелица окрене далеко. Тај мали угао је извор корена у обе приче.

Код Гровера осе заклапају угао $\bar{\theta}$:

$$\text{Гроверов корак} = U_s U_w = \text{ротација за } 2\bar{\theta} \tag{3.13}$$

Осе се не померају: у сваком кораку примењујемо исти оракл и исту дифузију. Зато се угао стања не удвостручује, него му се у сваком кораку дода $2\bar{\theta}$. Почетни угао $\bar{\theta}$ прелази у $3\bar{\theta}$, па у $5\bar{\theta}$, $7\bar{\theta}$, и тако даље: стрелица се мало по мало окреће ка $|w\rangle$.

Кључна идеја

Осе два огледања су почетно стање $|s\rangle$ и вектор $|\bar{s}\rangle$, који је у Гроверовој равни нормалан на означени вектор $|w\rangle$. Оракл мења знак амплитуде означеног стања према правилу провере. Оса $|\bar{s}\rangle$ математички зависи од w, али алгоритам не мора да зна w нити да ту осу посебно конструише: довољно је да примени оракл. Дифузија, с друге стране, зависи од познатог почетног стања $|s\rangle$, а не од тога који је елемент означен.

Минус који оракл дода амплитуди w је, геометријски, огледање; два огледања окрећу стање, корак по корак, ка решењу.

3.12 Зашто су довољне две димензије?

Простор стања има N димензија, а ми цртамо раван. Да ли је то само згодна слика? Није: стање Гроверовог алгоритма никад не изађе из равни коју разапињу $|\bar{s}\rangle$ и $|w\rangle$, и слика је тачна, без икакве апроксимације.

Оба оператора направљена су само од вектора $|w\rangle$ и $|s\rangle$ и јединичног оператора. Примењени на стање $|\psi\rangle$, они дају то исто стање, можда са промењеним знаком, плус умножак једног од та два вектора:

$$U_w|\psi\rangle = |\psi\rangle - 2\langle w|\psi\rangle\,|w\rangle, \qquad U_s|\psi\rangle = 2\langle s|\psi\rangle\,|s\rangle - |\psi\rangle.$$

Ако је $|\psi\rangle$ збир вектора $|w\rangle$ и $|s\rangle$ помножених неким бројевима, такав је и резултат. Алгоритам почиње од самог $|s\rangle$, па је после сваког корака стање такав збир: лежи у равни коју разапињу $|w\rangle$ и $|s\rangle$. То је иста раван коју разапињу $|w\rangle$ и $|\bar{s}\rangle$, јер када од $|s\rangle$ одузмемо његов део дуж $|w\rangle$, остаје вектор дуж $|\bar{s}\rangle$:

$$|s\rangle - \frac{1}{\sqrt{N}}\,|w\rangle = \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle = \sqrt{\frac{N-1}{N}}\,|\bar{s}\rangle.$$

После сваког корака стање је, дакле, облика $x\,|\bar{s}\rangle + y\,|w\rangle$, као у §3.9.

Исто се види и из амплитуда. Ни $|s\rangle$, ни оракл, ни дифузија не разликују два неозначена елемента: на почетку сви имају исту амплитуду, оракл им ништа не мења, а дифузија сваку одражава у односу на исту средину. Зато у сваком кораку сви неозначени елементи имају

исту амплитуду и крећу се заједно, као један. Правци у којима би се неозначене амплитуде међусобно разликовале, њих $N-2$, имају амплитуду нула од почетка до краја.

> **За радознале: раван у соби.** Нека је $N = 3$, само као три правца, без кубита, и нека је $|w\rangle$ усправна оса собе. Два неозначена елемента су две осе пода, а $|\bar{s}\rangle$ је дијагонала пода, на пола пута између њих. Усправна оса и та дијагонала разапињу један раван лист; он је усправан и дијагонално пресеца собу. Преостали правац, друга дијагонала пода, нормалан је на тај лист, и Гроверов алгоритам га никад не дотакне: стање се све време окреће у листу.

3.13 Колико је Гроверових корака потребно?

Гроверов алгоритам [5] гласи: почиње се од стања $|s\rangle$; затим се k пута понови Гроверов корак, оракл па дифузија; на крају се стање измери. Колико корака треба?

Повежимо угао са бројем корака. Почетни угао одређује (3.5): $\sin\bar{\theta} = 1/\sqrt{N}$. За велико N угао је мали, а мали угао је скоро једнак свом синусу, по (Б.1): $\bar{\theta} \approx 1/\sqrt{N}$. Сваки корак окрене стрелицу за $2\bar{\theta}$, па после k корака стрелица стоји на углу $(2k+1)\bar{\theta}$:

$$|\psi_k\rangle = \sin\big((2k+1)\bar{\theta}\big)\,|w\rangle + \cos\big((2k+1)\bar{\theta}\big)\,|\bar{s}\rangle, \qquad P(w) = \sin^2\big((2k+1)\bar{\theta}\big) \tag{3.14}$$

Вероватноћа је квадрат амплитуде (§2.3), а амплитуда стања $|w\rangle$ је синус угла стрелице. Док се стрелица окреће ка $|w\rangle$, амплитуда означеног елемента расте, а амплитуде свих осталих опадају (Слика 3.10).

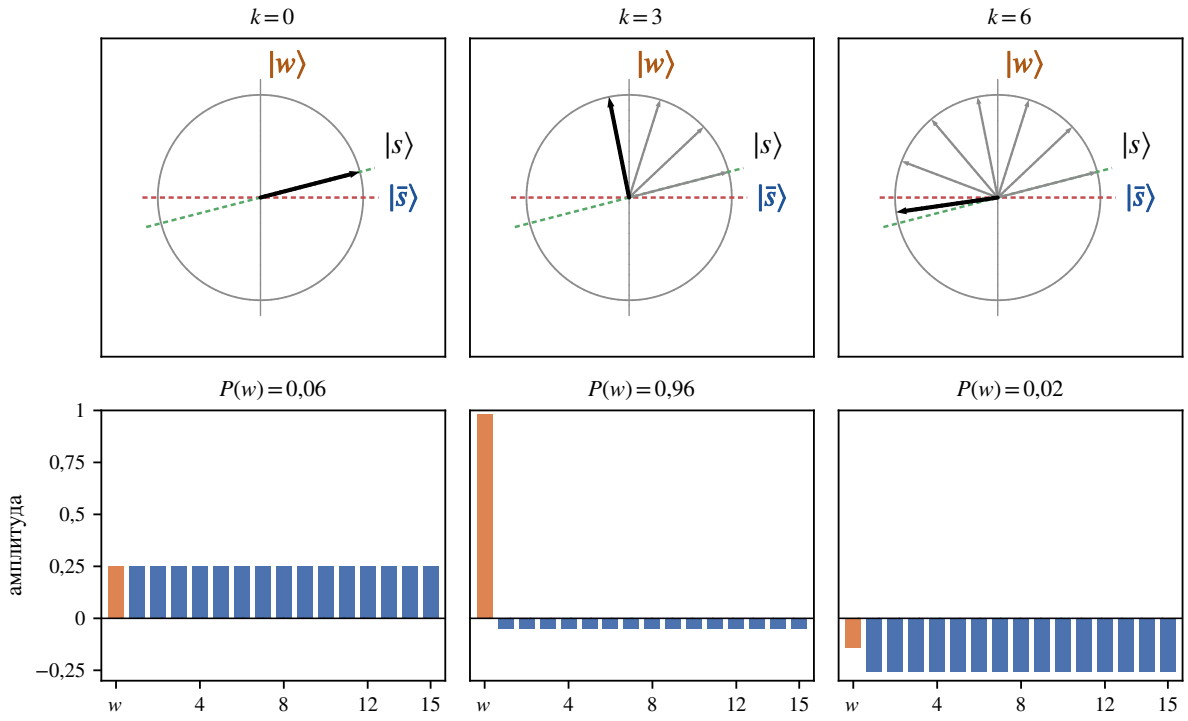
Колико корака треба да стрелица стигне до $|w\rangle$? Она креће са угла $\bar{\theta}$, а $|w\rangle$ је под правим углом, $\pi/2$. Треба, дакле, да је $(2k+1)\bar{\theta} = \pi/2$, тј. $k = q - 1/2$, где је $q = \pi/(4\bar{\theta})$. Број корака мора бити цео, а цео број најближи броју $q-1/2$ је $\lfloor q \rceil$, највећи цео број који није већи од q (заокруживање наниже). Наиме, $\lfloor q \rfloor \le q < \lfloor q \rfloor + 1$, па $q - 1/2$ лежи између $\lfloor q \rfloor - 1/2$ и $\lfloor q \rfloor + 1/2$. Један избор броја корака после кога је стрелица први пут најближа $|w\rangle$ је зато

$$k^* = \left\lfloor \frac{\pi}{4\bar{\theta}} \right\rceil \approx \frac{\pi}{4}\sqrt{N} \tag{3.15}$$

Ако је q цео број, и $q-1$ и q су подједнако близу првом максимуму; формула бира q. На пример, за $N = 2$ већ је почетна вероватноћа $1/2$, а један корак је не повећава. Касније се могу појавити други максимуми, па овај избор не мора бити јединствен међу свим бројевима корака. Приближна вредност следи из $\bar{\theta} \approx 1/\sqrt{N}$. После k^* корака стрелица је од $|w\rangle$ удаљена највише за угао $\bar{\theta}$, па је вероватноћа успеха најмање $1 - 1/N$; то је доња граница, а не нужно тачна вредност: $P(w) \ge \cos^2\bar{\theta} = 1 - 1/N$ (в. задатак 64).

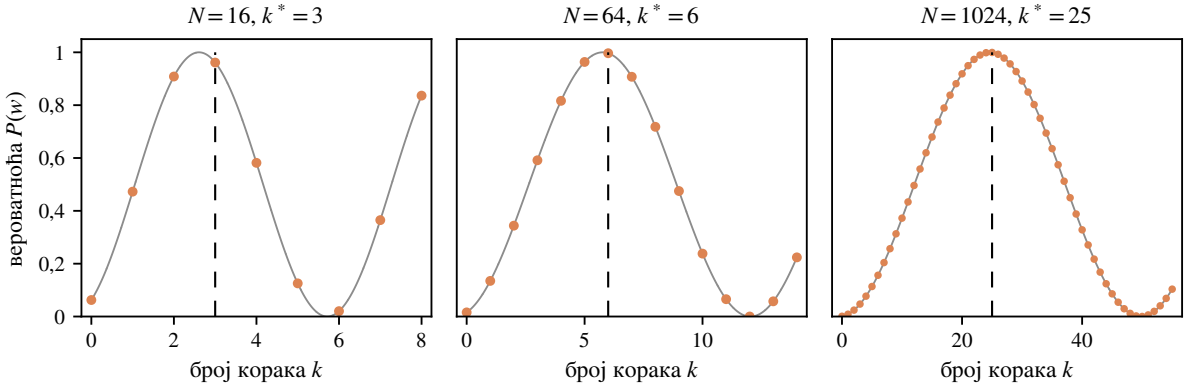
Што је N веће, то је мањи део $|w\rangle$ у почетном стању, $1/\sqrt{N}$, то је мањи угао $\bar{\theta}$, и то треба више корака, сразмерно са $\sqrt{N}$. Ево неколико бројева: за $N = 4$ је $\bar{\theta} = 30°$, па један корак доводи стрелицу тачно на $|w\rangle$, јер је $3\bar{\theta} = 90°$, и $P(w) = 1$ (то ћемо видети и у колу, §3.17); за $N = 8$ је $k^* = 2$ и $P(w) = 121/128 \approx 0{,}945$ (в. задатак 66); за $N = 16$ је $\bar{\theta} = 14{,}5°$, $k^* = 3$ и $P(w) = 0{,}96$; за $N = 2^{20} = 1\,048\,576$ стања је $k^* = 804$.

Више корака одмах после k^* није боље. Ротација не стаје сама: ако наставимо после k^*, стрелица прође поред $|w\rangle$, вероватноћа почне да опада, а амплитуда се враћа неозначеним елементима (Слика 3.11). У основној верзији коју разматрамо број корака бирамо пре мерења,



Слика 3.10. $N = 16$, после $k = 0$, 3 и 6 корака. Горе: стрелица стања у равни $|\bar{s}\rangle$, $|w\rangle$ (сиве стрелице су претходни кораци). Доле: шеснаест амплитуда, означена наранџаста, неозначене плаве. После $k^* = 3$ корака стрелица је најближа $|w\rangle$ и $P(w) = 0{,}96$; после шест корака прошла је поред њега, и $P(w)$ је опет мала.

користећи познат број означених елемената. Када тај број није познат, потребан је другачији поступак избора броја корака [11]. После још пола круга стрелица опет прође близу правца $|w\rangle$, сада са друге стране, понекад и ближе него после k^* корака; али за то треба око три пута више упита.



Слика 3.11. Вероватноћа $P(w)$ после k корака, за $N = 16$, 64 и 1024. Тачке су цели бројеви корака, а сива крива је $\sin^2((2k+1)\bar{\theta})$ за непрекидно k. Испрекидана линија означава k^*: што је N веће, то је даље.

3.14 Појачавање амплитуде

Стрелица у равни показала нам је да Гроверов корак окреће стање и колико корака треба. Мерење, међутим, даје исходе чије вероватноће одређују амплитуде, па погледајмо исти корак

на амплитудама, стубић по стубић. Треба нам правило из §3.10: дифузија сваку амплитуду одрази у односу на њихову аритметичку средину $\bar{a}$. По (3.10) је $a_i \mapsto 2\bar{a} - a_i$. Стубић испод средине пребаци се изнад ње, исто толико далеко, а стубић изнад средине спусти се исто толико испод ње.

Почнимо од стања $|s\rangle$, у коме су све амплитуде $1/\sqrt{N}$. Оракл амплитуди w промени знак, па она постане $-1/\sqrt{N}$. Тиме се и средина спусти. Средина је збир амплитуда подељен са N, а сада је $N-1$ амплитуда једнако $1/\sqrt{N}$ и једна $-1/\sqrt{N}$, па је

$$\bar{a} = \frac{1}{N}\Big[(N-1)\cdot\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}}\Big] = \frac{N-2}{N\sqrt{N}},$$

што је за велико N мало испод $1/\sqrt{N}$ (Слика 3.12а). Сада дифузија одрази сваку амплитуду у односу на ту средину. Амплитуда w лежи далеко испод средине, за $\bar{a} + 1/\sqrt{N}$, па се пребаци исто толико изнад ње:

$$a_w \longmapsto 2\bar{a} + \frac{1}{\sqrt{N}} = \frac{3N-4}{N\sqrt{N}} \approx \frac{3}{\sqrt{N}}.$$

Остале амплитуде се после дифузије мењају овако: $a_i \mapsto 2\bar{a} - 1/\sqrt{N} = (N-4)/(N\sqrt{N})$. За велико N оне остају близу $1/\sqrt{N}$, а амплитуда w је приближно три пута већа него на почетку. Вероватноћа успеха је тада приближно девет пута већа, односно око $9/N$. За мала N треба користити тачну формулу.

Погледајмо мали пример, $N = 4$. Средина после оракла је $1/4$, па амплитуда w скочи на $2\cdot 1/4 + 1/2 = 1$, а остале падну на $2\cdot 1/4 - 1/2 = 0$: један корак налази w сигурно, као у §3.13. За $N = 16$ амплитуда w порасте са $1/4$ на $11/16$, а остале падну са $1/4$ на $3/16$ (Слика 3.12б). Вероватноћа да мерење покаже w порасте са $1/16$ на $121/256$, скоро на половину.

Корак затим понављамо. Лако је видети шта цео корак ради амплитуди w. Нека је она пре корака a_w. Оракл је пребаци у $-a_w$, а средину после оракла означимо са $\bar{a}$. Дифузија затим од $-a_w$ направи $2\bar{a} - (-a_w)$, па је

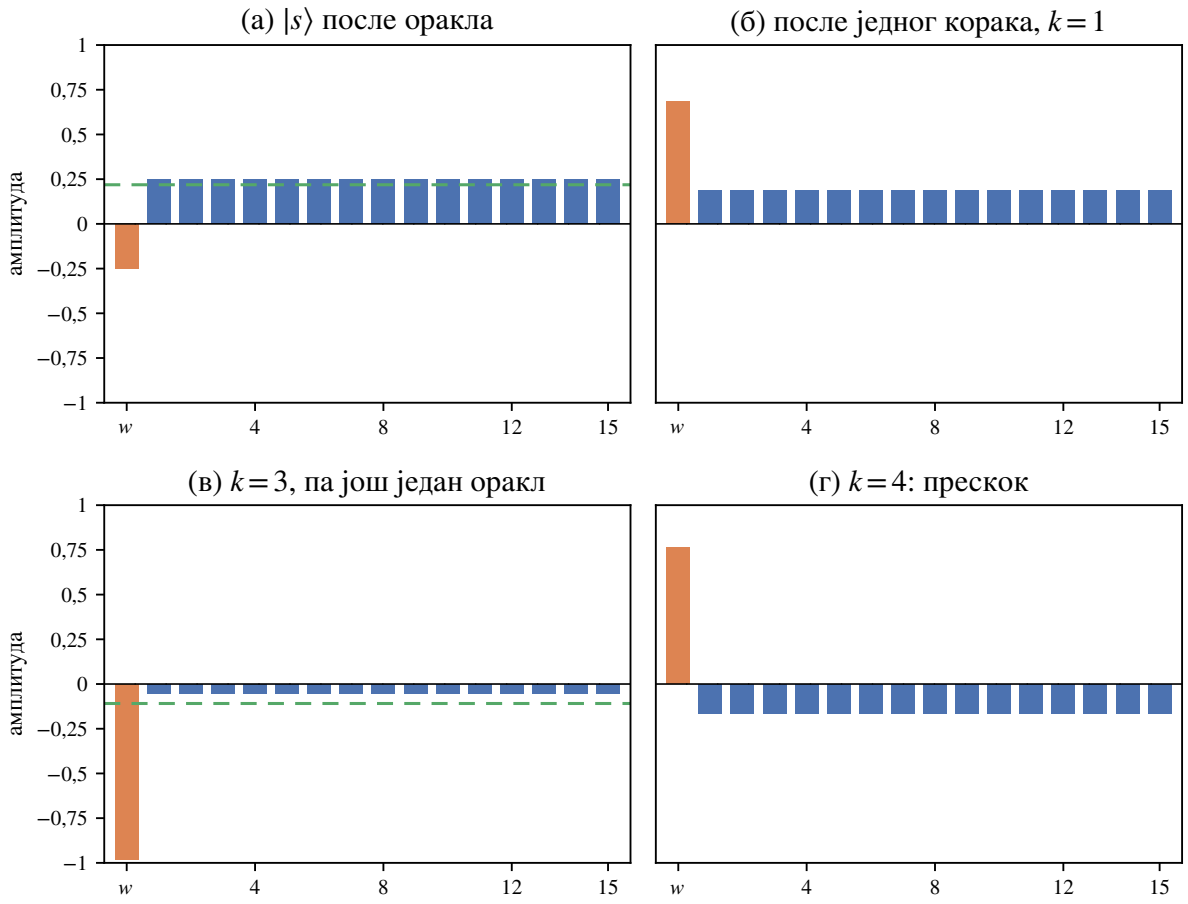
$$a_w \longmapsto a_w + 2\bar{a}.$$

Цео корак амплитуди w, дакле, дода двоструку средину, израчунату после оракла. Док је та средина позитивна, амплитуда w расте, корак по корак, а остале амплитуде се сваки пут смање: то је **појачавање амплитуде**. Стубићи и стрелица показују исто: амплитуда w је синус угла стрелице, $\sin((2k+1)\bar{\theta})$, по (3.14). То се види и на Слици 3.10, где су испод сваке црне стрелице нацртане њене амплитуде.

Појачавање, ипак, не траје довека. За довољно велико N, после k^* корака остале амплитуде су скоро нула, а амплитуда w скоро 1. Следећи оракл је пребаци близу -1, па средина постане негативна (Слика 3.12в). Корак амплитуди w и тада дода двоструку средину, али је та средина сада негативна, па је амплитуда w после корака мања него пре њега. За $N = 16$ амплитуда w после три корака износи 0,98. Четврти оракл је пребаци на $-0{,}98$, а дифузија је одатле подигне само до 0,76, ниже него што је била пре оракла (Слика 3.12г). То је прескок из §3.13, виђен на стубићима.

3.15 Гроверова и класична претрага без структуре

Класичној претрази треба око $N/2$ упита, а Гроверовом алгоритму око $(\pi/4)\sqrt{N}$ (Слика 3.13). Може ли боље? Не: доказано је да ниједан квантни алгоритам не може да нађе означени



Слика 3.12. Појачавање амплитуде, $N = 16$; амплитуда w је наранџаста, остале су плаве, а испрекидана зелена линија је средина $\bar{a}$. (а) Стање $|s\rangle$ после оракла: w је испод нуле, а средина мало испод 1/4. (б) После једног корака: w је скочила на 11/16, а остале су пале на 3/16. (в) После три корака и још једног оракла: средина је негативна. (г) Четврти корак: одраз у односу на негативну средину подигне w само до 0,76, ниже него пре четвртог оракла (0,98); то је прескок.

елемент са сталном вероватноћом успеха уз асимптотски мање од $\sqrt{N}$ упита [7]. Гроверов алгоритам је зато најбољи могућ по томе како број упита расте са N. Бољи алгоритам могао би број упита да смањи највише сталан број пута, ма колико N било велико.

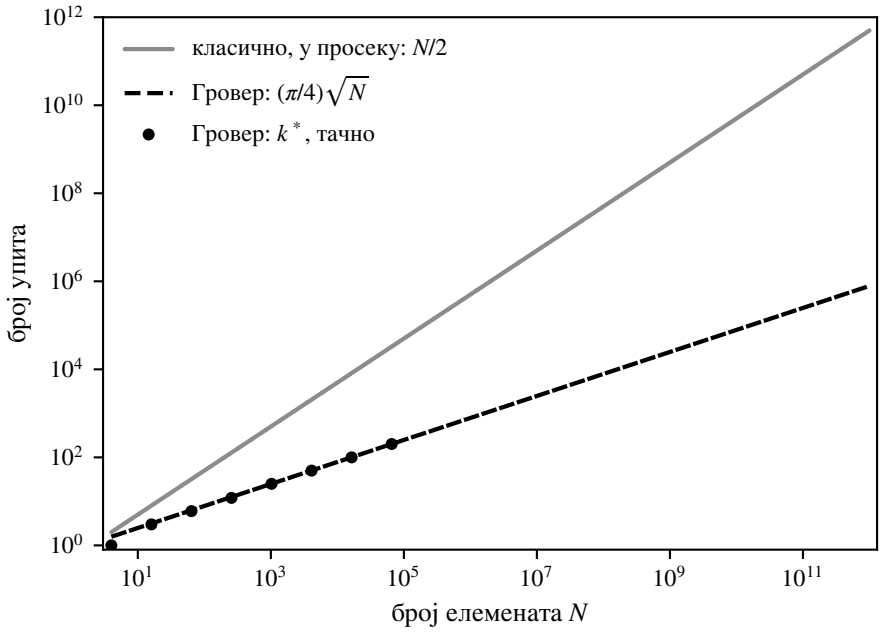
Убрзање треба оценити трезвено. Оно је **квадратно**, а не експоненцијално: $\sqrt{N}$ уместо N, а не, рецимо, $\log N$ уместо N. И важи за претрагу без икаквог реда. Ако проблем има структуру, на пример азбучни ред, и класични алгоритми раде много брже од $N/2$.

3.16 Квантно коло Гроверовог алгоритма

Сада имамо све делове и можемо да нацртамо цело коло (Слика 3.14). Рачунар има n кубита за кандидате и један помоћни кубит, као у §3.7. Коло има три дела.

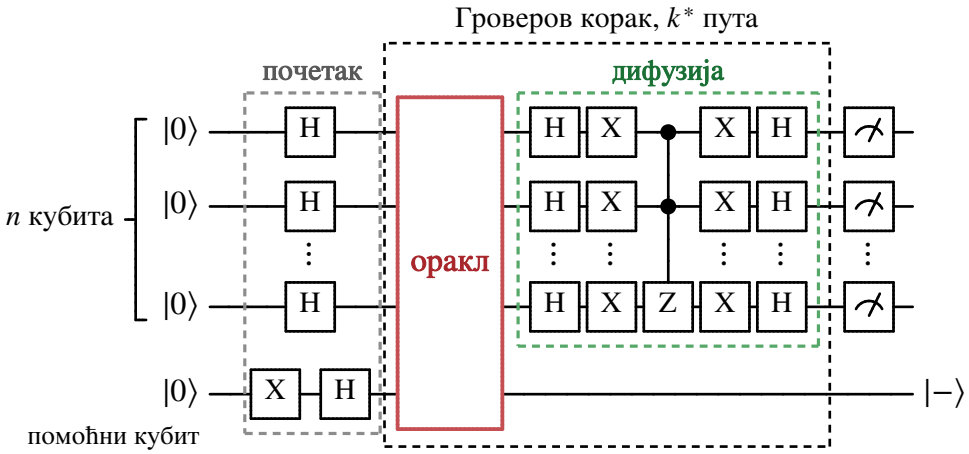
1. **Почетак.** Слој капија H преводи $|0\ldots0\rangle$ у $|s\rangle$ (§2.7). Помоћни кубит почиње у стању $|0\rangle$; капија X га пребаци у $|1\rangle$, а капија H у $|-\rangle$, по (2.5).

2. **Гроверов корак, поновљен k^* пута.** Прво иде оракл: провера која уз помоћни кубит у стању $|-\rangle$ мења знак само амплитуди w, а помоћни кубит оставља у стању $|-\rangle$ (§3.7). Затим иде дифузија: слој H, слој X, капија која мења знак само амплитуди $|1\ldots1\rangle$, па опет слој X и слој H.



Слика 3.13. Број упита у зависности од броја елемената N: класично у просеку $N/2$, Гроверов алгоритам $(\pi/4)\sqrt{N}$. Тачке су тачне вредности k^*.

3. **Мерење.** Мерење кубита кандидата даје w са вероватноћом $\sin^2\big((2k^*+1)\bar{\theta}\big)$, по (3.14).



Слика 3.14. Гроверово коло за n кубита кандидата (тачке замењују кубите између другог и последњег) и помоћни кубит. Испрекидани оквири означавају почетак, дифузију и цео Гроверов корак, оракл па дифузију, који се понавља k^* пута. Капија са тачкама на свим кубитима кандидата осим последњег и квадратом Z на последњем мења знак само амплитуди $|1\ldots1\rangle$.

Зашто дифузија изгледа баш тако? Слој капија H преводи $|0\ldots0\rangle$ у $|s\rangle$ (§2.7), а двапут примењен не мења ништа: то важи за сваку капију H (§2.6), а капије на различитим кубитима не сметају једна другој. Зато слој H преводи и $|s\rangle$ назад у $|0\ldots0\rangle$. Он чува дужине, па и углове (§2.9), па вектор нормалан на $|s\rangle$ преводи у вектор нормалан на $|0\ldots0\rangle$. Погледајмо сада три корака: слој H, огледање у односу на осу $|0\ldots0\rangle$, тј. оператор $2|0\ldots0\rangle\langle0\ldots0| - \mathbb{1}$ из (3.9), и опет слој H. Вектор $|s\rangle$ први слој преведе у $|0\ldots0\rangle$, огледање га не мења, а други слој га врати у $|s\rangle$. Вектор нормалан на $|s\rangle$ први слој преведе у вектор нормалан на $|0\ldots0\rangle$, огледање му промени знак, а други слој га врати на место одакле је кренуо, са промењеним знаком. Та три корака,

дакле, остављају $|s\rangle$, а свему што је нормално на $|s\rangle$ мењају знак. То је огледање у односу на осу $|s\rangle$, оператор U_s из (3.8):

$$U_s = 2|s\rangle\langle s| - \mathbb{1} = \mathrm{H}\big(2|0\ldots0\rangle\langle 0\ldots0| - \mathbb{1}\big)\,\mathrm{H} \tag{3.16}$$

где H овде означава цео слој, $\mathrm{H}^{\otimes n}$. Огледање у односу на осу $|s\rangle$ је, дакле, огледање у односу на осу $|0\ldots0\rangle$, обухваћено са два слоја H.

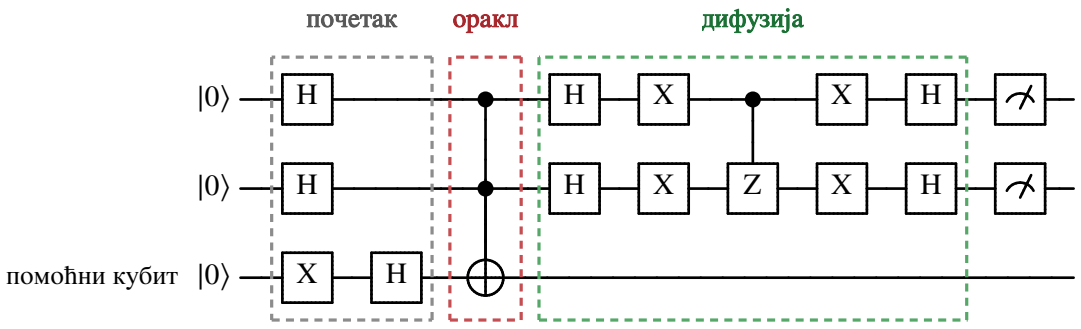
Средишње огледање оставља само $|0\ldots0\rangle$, а свим осталим базним векторима мења знак. Коло ради обрнуто. Слој X обрне све битове у свакој ознаци, па амплитуда исхода $0\ldots0$ дође на место $1\ldots1$. Капија Z на последњем кубиту, са контролом на свим осталим, промени знак само амплитуди $|1\ldots1\rangle$; за $n = 2$ то је CZ, а за $n = 3$ CCZ (§2.8). Други слој X врати све амплитуде на своја места. Тако коло мења знак само амплитуди $|0\ldots0\rangle$, а остале оставља: то је оператор $\mathbb{1} - 2|0\ldots0\rangle\langle 0\ldots0|$, тј. потребно огледање помножено са -1, јер је $\mathbb{1} - 2|0\ldots0\rangle\langle 0\ldots0| = -\big(2|0\ldots0\rangle\langle 0\ldots0| - \mathbb{1}\big)$. Приказано коло зато даје $-U_s$: у овом алгоритму то је физички еквивалентно примени U_s, јер се резултујућа стања разликују само у глобалном знаку (§2.3).

Коло дифузије исто је за сваки проблем претраге. Од проблема зависи само оракл.

У приказаном колу помоћни кубит служи да реверзибилну проверу претворимо у фазни оракл (§3.7). Ако за неки проблем знамо како да знак амплитуде w променимо директно, такав помоћни кубит није потребан. За $n = 2$ и $w = 11$ то ради сама капија CZ, и тако се то коло често црта у уџбеницима.

3.17 Два кубита, корак по корак

Пратимо сада коло за $n = 2$ и $w = 11$, колону по колону (Слика 3.15). Провера „да ли је кандидат 11?“ пита да ли су оба бита 1. Оракл је зато капија X на помоћном кубиту, са контролом на оба кубита кандидата, тј. CNOT са две контроле; зове се **Тофолијева капија**. Помоћни кубит је у стању $|-\rangle$, па она, као у §3.7, мења знак само амплитуди $|11\rangle$. Означени низ 11 смо у овом наставном примеру унапред изабрали, па коло не служи да откријемо непознат одговор, већ да пратимо дејство капија. У другим проблемима оракл можемо градити од правила провере, без претходног познавања решења, као у примеру судокуа (§3.5).



Слика 3.15. Гроверово коло за $n = 2$ и $w = 11$, са помоћним кубитом, један корак. Оракл је Тофолијева капија: обрне помоћни кубит ако су оба бита кандидата 1. Испрекидани оквири означавају почетак, оракл и дифузију.

Коло се чита као у §2.6, а кубит 1 је горе. Капије које стоје једна изнад друге чине једну колону кола. Последњи симбол на линијама кандидата, мали бројчаник са казаљком, означава мерење; помоћни кубит се не мери.

Да бисмо израчунали стање после сваке колоне, треба нам правило по коме капија на једном кубиту делује на стање више кубита. То је **правило парова**: капија дели амплитуде у парове чије се ознаке разликују само у биту тог кубита, и на сваки пар делује исто, као на вектор у равни. За $n = 2$ капија на кубиту 1 делује на парове (a_{00}, a_{10}) и (a_{01}, a_{11}), а капија на кубиту 2 на парове (a_{00}, a_{01}) и (a_{10}, a_{11}). Капија X у пару замени амплитуде, а капија H пар (a, b) преводи у $\big((a+b)/\sqrt{2}, (a-b)/\sqrt{2}\big)$, по (2.5) (в. задатак 36). Капија са контролом делује само на оне парове у чијим су ознакама контролни битови 1; зато CZ мења знак само амплитуди a_{11}.

За $N = 4$ је $\bar{\theta} = 30°$, па је $k^* = \lfloor \pi/(4\bar{\theta}) \rfloor = \lfloor 1{,}5 \rfloor = 1$: довољан је један корак. Табела 3.2 даје амплитуде кандидата, $(a_{00}, a_{01}, a_{10}, a_{11})$, после сваке колоне кола. Помоћни кубит после почетка све време остаје у стању $|-\rangle$, па га у табели не пишемо.

после	**амплитуде кандидата**
улаз	$(1, 0, 0, 0)$
H H (почетак)	$(1, 1, 1, 1)/2$
Тофолијева капија (оракл)	$(1, 1, 1, -1)/2$
H H	$(1, 1, 1, -1)/2$
X X	$(-1, 1, 1, 1)/2$
CZ	$(-1, 1, 1, -1)/2$
X X	$(-1, 1, 1, -1)/2$
H H	$(0, 0, 0, -1)$

Табела 3.2. Амплитуде кандидата после сваке колоне кола са Слике 3.15. Последњих пет колона су дифузија.

Мерење даје 11 са вероватноћом $(-1)^2 = 1$: погодак из прве, као у §3.13. Крајњи знак минус је знак целог вектора из §3.16, који се не види.

Најважније из поглавља

1. Претрага без структуре. За једно означено решење међу N могућности класична провера редом захтева у просеку $(N+1)/2$ провера. Гроверов алгоритам користи реда $\sqrt{N}$ упита оракулу, уз велику вероватноћу успеха. Време извршавања зависи и од цене сваког упита.

2. Оракл. Функција $f(i)$ проверава да ли је i решење. Фазни оракл мења знак означеној амплитуди:

$U_w|i\rangle = (-1)^{f(i)}|i\rangle$, односно $U_w = \mathbb{I} - 2|w\rangle\langle w|$.

3. Зашто оракл није довољан. Самом променом знака вероватноће мерења у рачунској бази не мењају се. Потребна је и интерференција која ће прерасподелити амплитуде.

4. Дифузија. Оператор $U_s = 2|s\rangle\langle s| - \mathbb{I}$ огледа стање у односу на правац $|s\rangle$. Сваку амплитуду одражава у односу на средину: $a_i \mapsto 2\bar{a} - a_i$.

5. Раван алгоритма. Почетно стање и сва наредна стања остају у равни коју разапињу $|w\rangle$ и равномерна суперпозиција неозначених стања $|\bar{s}\rangle$. У тој равни оракл је огледање у односу на осу $|\bar{s}\rangle$.

6. Два огледања. Један Гроверов корак је оракл, па дифузија. У равни алгоритма он ротира стање за $2\bar{\theta}$, где је $\sin\bar{\theta} = 1/\sqrt{N}$.

7. Број корака и успех. После k корака вероватноћа да мерење да тражени исход износи $P_k(w) = \sin^2((2k+1)\bar{\theta})$. За први максимум бирамо $k^* = \lfloor \pi/(4\bar{\theta}) \rfloor \approx (\pi/4)\sqrt{N}$; тада је $P_{k^*}(w) \geq 1 - 1/N$. Превише корака може поново смањити вероватноћу.

Ова геометрија два огледања омогућиће нам да у следећем поглављу упоредимо алгоритам са сударима блокова.

3.18 Задаци

Задаци за самосталан рад

Задаци су намењени увежбавању математичког описа Гроверовог алгоритма: од провере и оракла, преко дифузије и ротације, до броја корака и квантних кола. Последња група доноси додатне изазове. Не морате их решавати све одједном; бирајте их према ономе што желите да увежбате.

Претрага, провере и оракл

Задатак 51. За $N = 100$ могућности, ако је положај јединог решења подједнако вероватан и проверавамо без понављања, колико провера у просеку треба? Шта се мења ако је могућности 100 пута више?

Задатак 52. Нека је $N = 4$ и означено стање $|10\rangle$. Напишите функцију $f(i)$ и матрицу фазног оракла у бази $|00\rangle$,$|01\rangle$,$|10\rangle$,$|11\rangle$. Примените оракл на $|s\rangle$ и упоредите вероватноће свих исхода пре и после њега.

Задатак 53. Реверзибилна провера делује као $|c\rangle|h\rangle \mapsto |c\rangle|h \oplus f(c)\rangle$. За $f(c) = 1$ одредите излаз када је помоћни кубит редом у стањима $|0\rangle$, $|+\rangle$ и $|-\rangle$. Како изгледају излази за $f(c) = 0$?

Задатак 54. За $N = 8$ и $w = 101$ запишите $|\bar{s}\rangle$, одредите угао између $|s\rangle$ и $|\bar{s}\rangle$, па примените фазни оракл на $|s\rangle$.

Задатак 55. Ако се број могућности увећа 100 пута, како се за велико N приближно мења број класичних провера, а како број Гроверових корака? Да ли се у истом односу мора променити и стварно време рада?

Дифузија, пројектори и огледања

Задатак 56. Покажите да огледање (3.6) не мења дужину стања. *Упутство: делови $|\psi_{\parallel}\rangle$ и $|\psi_{\perp}\rangle$ су међусобно нормални; израчунајте квадрат дужине стања $|\psi_{\parallel}\rangle \pm |\psi_{\perp}\rangle$ сабирак по сабирак.*

Задатак 57. Покажите да одраз у односу на аритметичку средину, (3.10), не мења средину, и да двапут примењен враћа почетне бројеве. *Упутство: израчунајте средину бројева $2\bar{a} - a_i$.*

Задатак 58. Примените дифузију на стање $(-1, 1, 1, 1)/2$. *Упутство: прво израчунајте средину амплитуда.*

Задатак 59. За $N = 8$ крените од $|s\rangle$ и израчунајте средину амплитуда после оракла, затим означену и неозначене амплитуде после дифузије и вероватноћу успеха.

Задатак 60. У ортонормираној бази $\{|\bar{s}\rangle,|w\rangle\}$ запишите матрице оракла и дифузије. Помножите их исправним редоследом и покажите да је Гроверов корак ротација за $2\bar{\theta}$.

Ротације и број Гроверових корака

Задатак 61. За $N = 16$ израчунајте $\bar{\theta}$, број корака до првог максимума и вероватноће успеха за $k = 0{,}1{,}2{,}3{,}4$. Нацртајте график и објасните шта се дешава после трећег корака.

Задатак 62. За $N = 2$ израчунајте вероватноћу успеха пре првог и после првог Гроверовог корака. Упоредите оба избора са формулом за k^*.

Задатак 63. Покажите да огледање у односу на другу осу, па у односу на прву, даје ротацију за -2α; осе су као у (3.12). *Упутство: пратите угао по правилу (3.11).*

Задатак 64. Покажите да је после k^* корака стрелица од $|w\rangle$ удаљена највише за угао $\bar{\theta}$, па је $P(w) \geq \cos^2\bar{\theta} = 1 - 1/N$. *Упутство: из* $k^* \leq \pi/(4\bar{\theta}) < k^* + 1$ *следи* $2k^*\bar{\theta} \leq \pi/2 < 2k^*\bar{\theta} + 2\bar{\theta}$.

Задатак 65. Колико Гроверових корака треба за $N = 2^{20}$, и колика је тада вероватноћа успеха? *Упутство: за мали угао је* $\bar{\theta} \approx \sin\bar{\theta}$.

Задатак 66. Израчунајте вероватноћу успеха за $n = 3$ после два корака, користећи само разломке. *Упутство: почните од амплитуда* $1/\sqrt{8}$ *и два пута примените оракл и одраз у односу на средину.*

Квантна кола

Задатак 67. Пратите коло са Слике 3.15 по правилу парова и упоредите резултате са Табелом 3.2.

Задатак 68. У Табели 3.2 проверите да последњих пет колона, коло дифузије, дају $-(2\bar{a} - a_i)$, тј. дифузију са промењеним знаком свих амплитуда. *Упутство: пре дифузије стање је* $(1, 1, 1, -1)/2$*; израчунајте средину.*

Задатак 69. Направите оракл за $w = 01$ по узору на §3.17, од Тофолијеве капије и капија X, са помоћним кубитом у стању $|-\rangle$. Проверите да мења знак само амплитуди $|01\rangle$. *Упутство: кандидат је 01 ако је бит кубита 1 једнак 0, а бит кубита 2 једнак 1. Капија* X *на кубиту 1 пре Тофолијеве капије претвара први услов у „бит је 1“, а иста капија после ње враћа кандидата.*

Задатак 70. Конструишите фазни оракл за $w = 01$ и примените га на равномерно почетно стање два кубита, а затим примените дифузију U_s. Које стање и исход добијате?

Задатак 71. Покажите да слојеви H, X, контролисана Z, X, H из §3.16 реализују $-U_s$. Како тај знак утиче на вероватноће мерења?

Додатни изазови

Задатак 72. Нека су међу $N = 16$ елемената означена два, w_1 и w_2, и нека оракл мења знак амплитудама оба. Покажите да прича из §3.8–§3.13 остаје иста ако $|w\rangle$ заменимо вектором $(|w_1\rangle + |w_2\rangle)/\sqrt{2}$, а $|\bar{s}\rangle$ вектором са једнаким амплитудама осталих 14 елемената, и да је тада $\sin\bar{\theta} = \sqrt{2/16}$. Колико корака треба, и са којом вероватноћом мерење тада даје један од два означена елемента? *Упутство: за стање у коме* w_1 *и* w_2 *имају једнаке амплитуде оракл мења знак само компоненти дуж нові* $|w\rangle$*; затим користите (3.14) и (3.15).*

Задатак 73. Ако је међу $N = 64$ стања означено $M = 4$, узмите $\sin\bar{\theta} = \sqrt{M/N}$. Колико корака бисте изабрали до првог максимума и колика је вероватноћа да исход буде једно од означених стања?

Задатак 74. Један Гроверов корак користи један упит ораклу од 400 капија и још 40 других капија. Колико укупно капија захтева 100 таквих корака? Да ли број упита сам по себи одређује тај трошак?

Задатак 75. За $N = 4$ упоредите вероватноћу успеха после једног корака када је означено једно стање и када су означена два стања. Шта пример говори о избору броја корака ако број означених стања није познат?

4. Два проблема, иста геометрија

У првом поглављу избројали смо сударе два блока, а у трећем смо извели Гроверов алгоритам. У оба резултата појављују се број π и квадратни корен: у броју судара приближно $\pi\sqrt{M/m}$, а у броју Гроверових упита приближно $(\pi/4)\sqrt{N}$. То није случајност. Погледајмо како се иза ова два проблема крију иста геометријска огледања.

4.1 Поставка: од много кугли до два блока

У проблему судара имали смо два блока и две брзине, а квантно стање описали смо са N амплитуда. Како повезати ова два описа? Послужићемо се конструкцијом у којој је велики блок састављен од једнаких кугли које се крећу заједно.

Замислимо N једнаких кугли, свака масе 1, на правој уз зид. Залепимо $N-1$ кугли у један велики блок, масе $M = N-1$; оне се крећу заједно, брзином V. Преостала кугла је мали блок, масе $m = 1$ и брзине v. Брзине свих N кугли чине вектор

$$|a\rangle = (v, V, V, \dots, V),$$

са по једном компонентом за сваку куглу. Ради једноставнијег записа брзину мале кугле ставили смо на прво место. Ако означеном елементу $|w\rangle$ одговара неко друго место, на њему стоји компонента v, а на осталим местима компоненте V. Квадрат његове дужине је $v^2 + (N-1)V^2 = 2E$. Нека је укупна кинетичка енергија $E = 1/2$: тада је $|a\rangle$ јединични вектор, баш као стање система са N исхода. Мала кугла одговара означеном елементу w, а кугле великог блока неозначеним елементима. Брзине су, као и раније, позитивне удесно, од зида.

Пошто су кугле великог блока спојене, независне су само две брзине, v и V. Вектор брзина можемо нормализовати и за произвољну енергију $E > 0$: делимо га са $\sqrt{2E}$. Таква промена размере не мења углове ни редослед судара. Избор $E = 1/2$ само поједностављује запис.

4.2 Заједничка раван стања

У Гроверовој равни $|w\rangle$ је означени базни вектор, а $|\bar{s}\rangle$ нормализован збир $N-1$ неозначених вектора. Свака његова ненулта компонента је $1/\sqrt{N-1}$; множилац $\sqrt{N-1}V$ зато даје компоненту V на сваком неозначеном месту.

Вектор $|a\rangle$ има компоненту v на месту w, а исту компоненту V на свих $N-1$ осталих места. По дефиницији вектора $|\bar{s}\rangle$ из §3.8, то значи

$$|a\rangle = v\,|w\rangle + \sqrt{N-1}\,V\,|\bar{s}\rangle = y\,|w\rangle + x\,|\bar{s}\rangle \tag{4.1}$$

јер је по (1.4) $x = \sqrt{M}\,V = \sqrt{N-1}\,V$ и $y = \sqrt{m}\,v = v$. Раван скалираних брзина, дакле, није само слична Гроверовој равни: тачка (x, y) представља вектор брзина блокова у равни $|\bar{s}\rangle$, $|w\rangle$. Хоризонтална оса равни скалираних брзина је $|\bar{s}\rangle$ (велики блок), а вертикална $|w\rangle$ (мали блок). И угао је исти: $\operatorname{tg}\bar{\theta} = \sqrt{m/M} = 1/\sqrt{N-1}$ значи да је $\sin\bar{\theta} = 1/\sqrt{N}$, јер правоугли троугао са катетама 1 и $\sqrt{N-1}$ има хипотенузу $\sqrt{N}$.

За нормализован вектор је $x^2 + y^2 = 1$, а за произвољну енергију $x^2 + y^2 = 2E$. Брзине нису физичке квантне амплитуде: поистовећујемо координате и математичке операције, док су физички системи различити. Два блока описују само ову дводимензионалну раван, не произвољно стање са N независних компонената.

4.3 Судари као огледања

Одбијање од зида. Само мала кугла удара у зид. Њена брзина мења знак, а брзина великог блока остаје иста: $(x, y) \mapsto (x, -y)$. То је управо дејство фазног оракла $U_w = \mathbb{I} - 2|w\rangle\langle w|$ у нашој равни, по (3.3).

Судар блокова. Посматрајмо га из система који се креће брзином центра масе:

$$v_{\mathrm{cm}} = \frac{mv + MV}{m + M}.$$

Укупни импулс се при судару чува, па је v_{cm} и пре и после судара исти. У систему центра масе укупни импулс је нула: импулси блокова једнаких су величина, а супротних смерова. Чува се и укупна кинетичка енергија. Она је једнака квадрату величине тог импулса помноженом са $1/(2m) + 1/(2M)$, па величина импулса остаје иста.

У једнодимензионалном еластичном судару блокови се после судара разилазе. Зато у систему центра масе оба импулса, а тиме и обе брзине, мењају смер. За мали блок је $v' - v_{\mathrm{cm}} = -(v - v_{\mathrm{cm}})$, а исто важи и за велики. Враћањем у систем везан за под добијамо

$$v' = 2v_{\mathrm{cm}} - v, \qquad V' = 2v_{\mathrm{cm}} - V \tag{4.2}$$

Свака брзина се огледа у односу на брзину центра масе (исто следи из (1.2), в. задатак 3). За N кугли масе 1 брзина центра масе је просто аритметичка средина брзина свих кугли:

$$v_{\mathrm{cm}} = \frac{v + (N-1)\,V}{N} = \bar{a} \tag{4.3}$$

Свака кугла добија брзину $2\bar{a} - a_i$. Дифузија $U_s = 2|s\rangle\langle s| - \mathbb{I}$ делује на амплитуде истим правилом, по (3.10). У овој равни то је исти линеарни оператор, а не само слична слика. На квантна стања изван те равни модел са два блока не даје физичку реализацију. Дакле:

$$\text{одбијање од зида} = \text{оракл}, \qquad \text{судар блокова} = \text{дифузија} \tag{4.4}$$

4.4 Поређење механичког система и Гроверовог алгоритма

Сада можемо да упоредимо одговарајуће појмове из механичког проблема и Гроверовог алгоритма (Табела 4.1).

Блокови	**Гровер**
мала кугла, маса 1	означени елемент w
велики блок, маса $N-1$	$N-1$ неозначених елемената
вектор брзина кугли	вектор реалних амплитуда, у истом математичком запису
$2E=1$ за нормализован вектор брзина	збир вероватноћа, 1
одбијање од зида	оракл
судар блокова	дифузија
оба блока иду ка зиду истом брзином	почетно стање: $-\lvert s\rangle$, исто стање као $\lvert s\rangle$
мали блок мирује, велики иде ка зиду	$-\lvert \bar{s}\rangle$
сва енергија у малом блоку	одговор, $\pm\lvert w\rangle$

Табела 4.1. Речник између блокова и Гроверовог алгоритма, по [2].

У квантном опису супротан глобални знак не мења физичко стање; код блокова промена знака свих брзина мења смер њиховог кретања.

4.5 Одакле разлика у броју корака?

Упоредимо укупан број судара C у оригиналној загонетки са бројем Гроверових упита k^*. За $m=1$ и $M=N-1$ оба проблема имају исти угао $\bar{\theta}$, али различите почетке и услове заустављања:

$$C=\left\lceil\frac{\pi}{\bar{\theta}}\right\rceil-1,\qquad k^*=\left\lfloor\frac{\pi}{4\bar{\theta}}\right\rfloor,\qquad \bar{\theta}=\operatorname{arctg}\frac{1}{\sqrt{N-1}}=\arcsin\frac{1}{\sqrt{N}}.$$

За велико N прва формула даје $C\approx\pi\sqrt{N-1}$, а друга $k^*\approx(\pi/4)\sqrt{N}$, па количник C/k^* тежи броју четири. То није тачна једнакост за сваки N: бројеви судара и корака су цели, а разликују се и почетни услови. На пример, за $N=4$ оригинална загонетка има пет судара, а Гровер један корак.

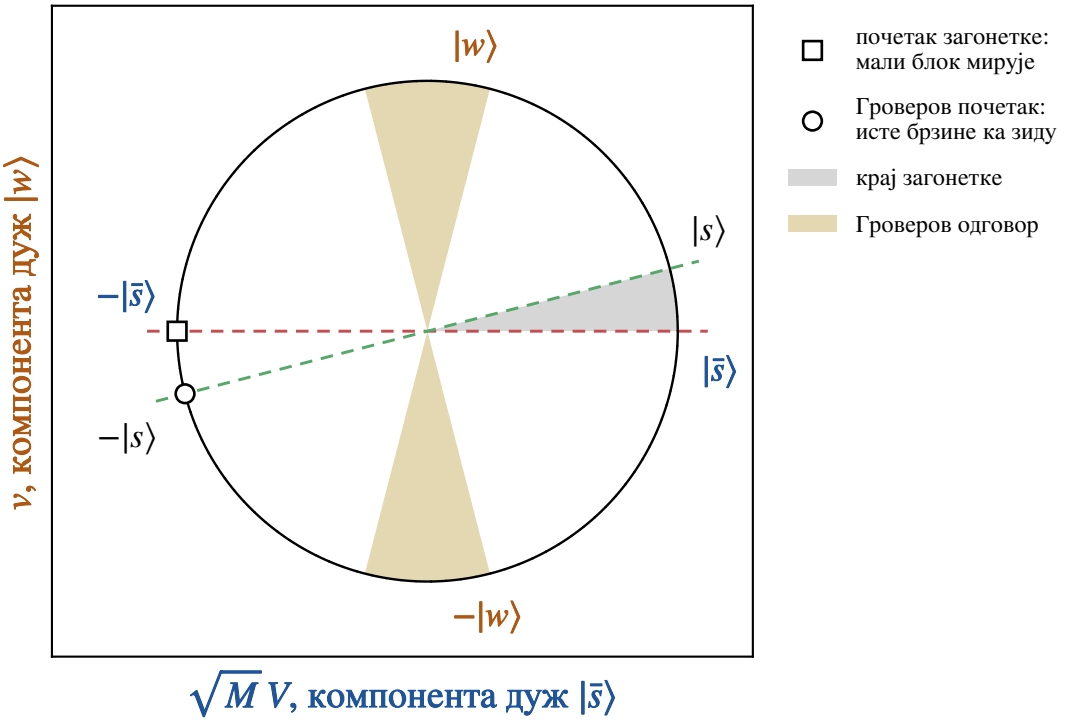
Одакле приближна четворка? Можемо је разумети као два чиниоца два:

1. **Како се броји.** Једном Гроверовом кораку одговара пар судара: одбијање од зида, па судар блокова. Гровер у броју упита рачуна само оракл, а не дифузију. Два судара зато одговарају једном упиту у механичком приказу Гроверовог корака.
2. **Када се стаје.** Гровер стаје близу означеног правца после приближно четвртине кружнице. У оригиналној загонетки судари трају док се блокови не разиђу; тачка пређе приближно пола кружнице.

Почеци нису исти (Слика 4.1). У оригиналној загонетки мали блок мирује, а велики се креће ка зиду: нормализовани вектор је $-\lvert\bar{s}\rangle$. За механички приказ Гроверовог почетка оба блока крећу ка зиду једнаком брзином: вектор је $-\lvert s\rangle$. На квантној страни $-\lvert s\rangle$ и $\lvert s\rangle$ представљају исто стање, али код блокова промена знака обе брзине обрће њихово кретање. Зато за механички приказ бирамо управо негативне брзине.

У тој другој поставци мали блок је ближи зиду и прво удари у зид; затим следи судар блокова. Тај пар има дејство U_sU_w, као један Гроверов корак, а исти поредак важи за наредне парове

док су физички судари могући (Слика 4.2). Оригинална загонетка користи иста огледања, али почиње из другог стања, па њен укупан број судара не мора бити цео број таквих парова.

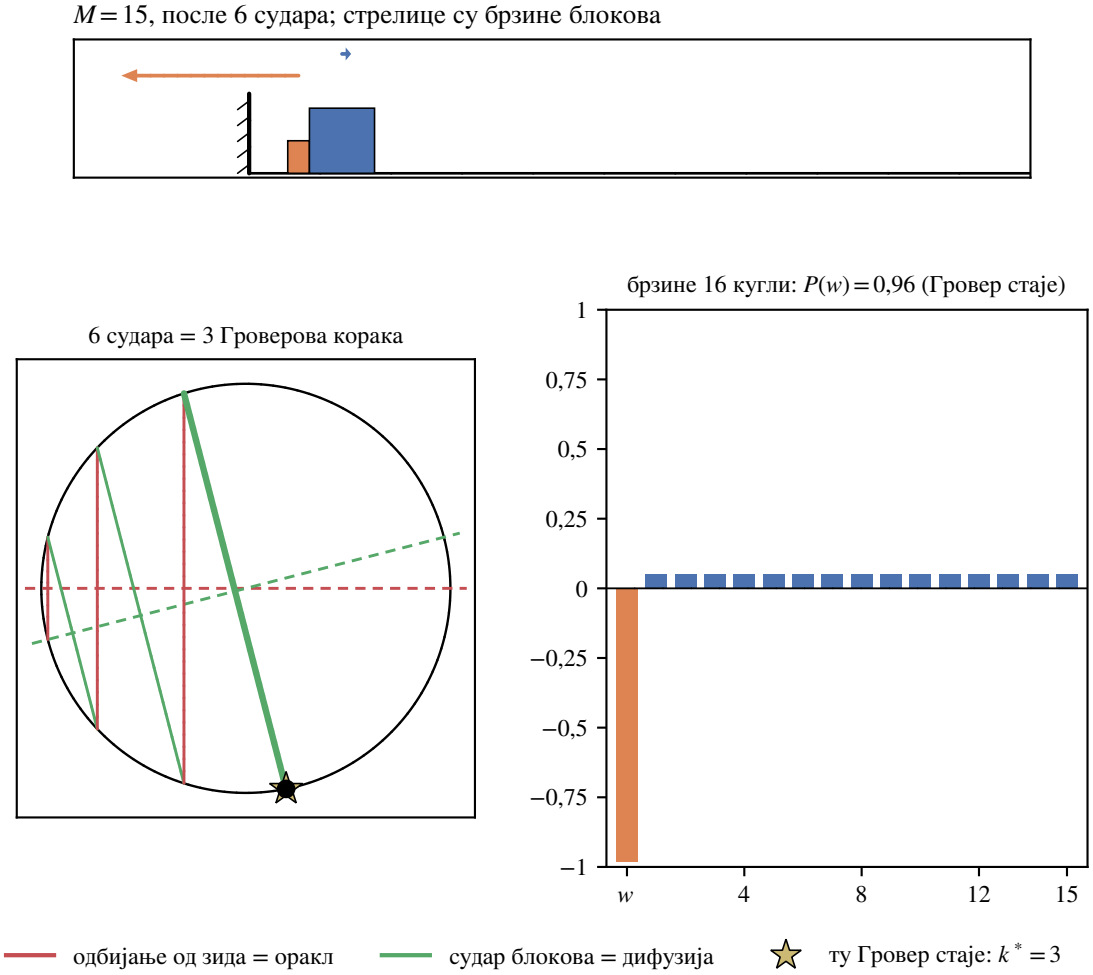


Слика 4.1. $M = 15$, $N = 16$, на истој кружници. Квадрат је почетак загонетке ($-|\bar{s}\rangle$: мали блок мирује, а велики иде ка зиду), а кружић Гроверов почетак на страни блокова ($-|s\rangle$: исте брзине ка зиду). Сива област је крај загонетке (више нема судара), између $|\bar{s}\rangle$ и $|s\rangle$, а златне су Гроверов одговор (на највише $\bar{\theta}$ од $|w\rangle$ или од $-|w\rangle$, што је исто квантно стање, али одговара супротним брзинама блокова). Црвена и зелена испрекидана права су осе два огледања, оракла и дифузије.

4.6 Пример: погодак из прве

За $N = 4$ Гроверов алгоритам налази w после једног корака (§3.13). На страни блокова то је $M = 3$. Почетне брзине четири кугле су $(-1/2, -1/2, -1/2, -1/2)$: све иду ка зиду истом брзином, а енергија је $4 \cdot (1/2)^2/2 = 1/2$. Мала кугла удари у зид: $v = 1/2$. Средина брзина је сада $(1/2 - 3\cdot 1/2)/4 = -1/4$, па судар блокова даје $v' = 2\cdot(-1/4) - 1/2 = -1$ и $V' = 2\cdot(-1/4) + 1/2 = 0$. **Велики блок стоји**, а сва енергија је у малом. То је стање $-|w\rangle$, исто као $|w\rangle$: погодак из прве, на страни блокова. Блокови би после тога наставили да се сударају, али Гровер стаје овде.

У последњем примеру знак минус уз вектор брзина показује да се мали блок креће ка зиду. На квантној страни глобални минус не мења вероватноће мерења.



Слика 4.2. Тренутак у коме Гровер стаје. Горе: блокови за $M = 15$ после 6 судара; стрелице су брзине блокова: мали блок брзо иде ка зиду, а велики се полако удаљава. Лево: њихова тачка на кружници; 6 судара чини 3 Гроверова корака, а звезда је тачка у којој Гровер стаје. Десно: брзине 16 кугли у истом тренутку, тј. Гроверове амплитуде са промењеним знаком целог вектора; $P(w) = 0{,}96$. Блокови би наставили до пола круга, а Гровер би тада промашио циљ.

Најважније из поглавља

1. Од брзина до вектора. За $m = 1$ и $M = N-1$ брзине кугли су компоненте вектора $(v, V, \ldots, V)$. Његов квадрат дужине је $2E$; дељењем са $\sqrt{2E}$ добијамо јединични вектор.

2. Иста раван. Вектор брзина има само две независне координате: $x = \sqrt{N-1}V$ и $y = v$. Оне су координате у равни $|\bar{s}\rangle$, $|w\rangle$, а заједнички угао задовољава $\sin\bar{\theta} = 1/\sqrt{N}$.

3. Зид и оракл. Одбијање од зида мења y у $-y$: у овој равни исто делује фазни оракл.

4. Судар и дифузија. Брзина центра масе је средина брзина кугли. Међусобни судар пресликава сваку брзину a_i у $2\bar{a} - a_i$, исто као дифузија.

5. Два судара и Гроверов корак. Одбијање од зида, па судар блокова, дају композицију $U_s U_w$: ротацију за $2\bar{\theta}$. То важи за одговарајући редослед судара у заједничкој равни.

6. Почетак и крај су важни. Оригинална загонетка и механички приказ Гровера почињу различито и не заустављају се у истом тренутку. За велико N укупан број судара приближно је

четири пута већи од броја Гроверових упита; за коначно N однос не мора бити тачно четири.

Исти математички оператори описују два различита физичка система. Управо нам та заједничка геометрија омогућава да закључак из једног проблема разумемо и у другом.

4.7 Задаци

Задаци за самосталан рад

Ови задаци повезују брзине блокова са квантним стањима и сударе са ораклом и дифузијом. Затим ћемо упоредити почетне услове, број судара и број Гроверових корака. Последњи задаци доносе конкретан пример и додатне изазове.

Од брзина до квантних стања

Задатак 76. За $N = 4$ одредите масе блокова и запишите вектор брзина. Разложите га у бази $\{|w\rangle,|\bar{s}\rangle\}$, прво за произвољне брзине v,V, а затим када мали блок мирује.

Задатак 77. За $N = 8$, $v = 1$ и $V = 2$ израчунајте $2E$, па нормализујте вектор брзина. Запишите добијени вектор у бази $\{|w\rangle,|\bar{s}\rangle\}$.

Задатак 78. Покажите да из $\operatorname{tg}\bar{\theta} = 1/\sqrt{N-1}$ следи $\sin\bar{\theta} = 1/\sqrt{N}$. Зашто се исти угао јавља у Гроверовој равни?

Задатак 79. Упоредите механичке почетке $-|\bar{s}\rangle$ и $-|s\rangle$: како се блокови крећу и који судар је први? Шта би за кретање блокова значила промена предзнака целог вектора?

Судари као квантни оператори

Задатак 80. Изведите формуле (1.2) из огледања (3.9). *Упутство: за* $|r\rangle = (\sqrt{M}\,V, \sqrt{m}\,v)$ *и јединични вектор* $|u\rangle = (\sqrt{M}, \sqrt{m})/\sqrt{M+m}$ *дуж праве једнаких брзина (§1.9) је* $\langle u|r\rangle = (MV + mv)/\sqrt{M+m}$*; прву компоненту слике поделите са* $\sqrt{M}$*, а другу са* $\sqrt{m}$.

Задатак 81. За $m = 1$, $M = 3$ и произвољне брзине v,V израчунајте брзине после међусобног судара помоћу формула еластичног судара и помоћу одраза у односу на средину четири брзине. Упоредите резултате.

Задатак 82. У бази $\{|\bar{s}\rangle,|w\rangle\}$ запишите матрицу одбијања од зида и матрицу судара блокова за $m = 1$, $M = N - 1$. Помножите их редоследом зид, па блокови, и одредите угао ротације.

Број судара и број Гроверових корака

Задатак 83. За $N = 4$ упоредите укупан број судара у оригиналној загонетки, број Гроверових корака и број судара у механичком приказу до Гроверовог заустављања. Да ли је однос прва два броја тачно четири?

Задатак 84. Нека је $M = 15$ и $m = 1$, тј. $N = 16$. Колико судара има ако мали блок на почетку мирује? После колико судара Гровер стаје, ако блокови крену из Гроверовог почетка? *Упутство:* $\sin\bar{\theta} = 1/4$*; користите (1.8) и (3.15).*

Примери и додатни изазови

Задатак 85. Објасните зашто за $N = 4$ један Гроверов корак налази ω са сигурношћу, и зашто за $M = 3$, када оба блока крену ка зиду истом брзином, велики блок стане после два судара. *Упутство:* $3 \cdot 30° = 90°$.

Задатак 86. За $N = 16$ крените од нормализованих једнаких брзина ка зиду. Нађите брзину малог блока и брзину великог после три пара судара, као и удео енергије у малом блоку. Упоредите га са вероватноћом Гроверовог успеха.

Задатак 87. Додатни изазов: у претрази је означено r од N елемената, при чему је $0 < r < N$. Ако кугле сваке групе спојимо у засебан блок, које су масе блокова и колики је угао $\bar{\theta}$? Посебно израчунајте угао и број Гроверових корака до првог максимума за $N = 8, r = 2$. Масе означене и неозначене групе обележите редом са m и M; не претпостављајте да је $M \geq m$.

Задатак 88. Објасните зашто математичка једнакост оператора судара и Гроверових оператора у овој равни не значи да два класична блока представљају општи квантни рачунар.

Додатак А. **Бројање судара помоћу зрака светлости**

Ово није део главне приче, него занимљивост: исти број судара види се и на други начин, цртањем положаја уместо брзина. Нека је d_1 растојање великог блока од зида, а d_2 растојање малог, и нека су блокови толико мали да их сматрамо тачкама. Уведимо

$$\xi = \sqrt{M}\, d_1, \qquad \eta = \sqrt{m}\, d_2.$$

Множење растојања коренима маса изабрано је тако да компоненте брзине тачке буду $\dot\xi = \sqrt{M}\, V$ и $\dot\eta = \sqrt{m}\, v$. Зато њихов збир квадрата даје двоструку кинетичку енергију.

Тачка (ξ, η) у **равни положаја** креће се док се блокови крећу. Мали блок не може да прође иза зида, $d_2 \geq 0$, ни иза великог блока, $d_2 \leq d_1$. Зато тачка остаје у клину између праве $\eta = 0$ и праве $\eta/\xi = \sqrt{m/M}$, а угао тог клина је по (1.9) баш $\bar\theta$.

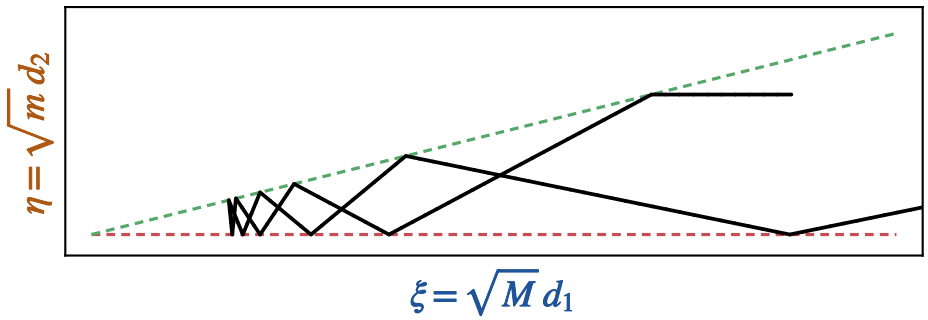
На граници $d_1 = d_2$ је $\eta/\xi = \sqrt{m/M}$, па угао клина износи $\bar\theta = \operatorname{arctg}\sqrt{m/M}$: то је исти угао као у равни скалираних брзина. Услов $0 \leq d_2 \leq d_1$ описује редослед блокова у овој тачкастој идеализацији.

Брзине су позитивне од зида, а растојања расту од зида, па је брзина тачке $(\sqrt{M}\, V, \sqrt{m}\, v) = (x, y)$: баш тачка из равни скалираних брзина. Отуда следе две ствари. Прво, квадрат брзине тачке је $x^2 + y^2 = 2E$, па је **износ брзине тачке сталан**. Њен смер се мења при судару; путању зато можемо геометријски упоредити са светлосним зраком. Друго, судари мењају вектор (x, y) тачно као у §1.7. Одбијање мења знак y, а то је огледање у односу на x-осу. Судар блокова премешта тачку на другу пресечну тачку праве импулса; права импулса је нормална на праву једнаких брзина, а пречник нормалан на тетиву полови ту тетиву, па је то огледање у односу на праву једнаких брзина. То су баш правци две странице клина. Када тачка удари у страницу, њена брзина се огледа у односу на ту страницу, као зрак светлости у огледалу: угао упада једнак је углу одбијања. **Путања тачке је као путања светлосног зрака између два огледала која заклапају угао $\bar\theta$.**

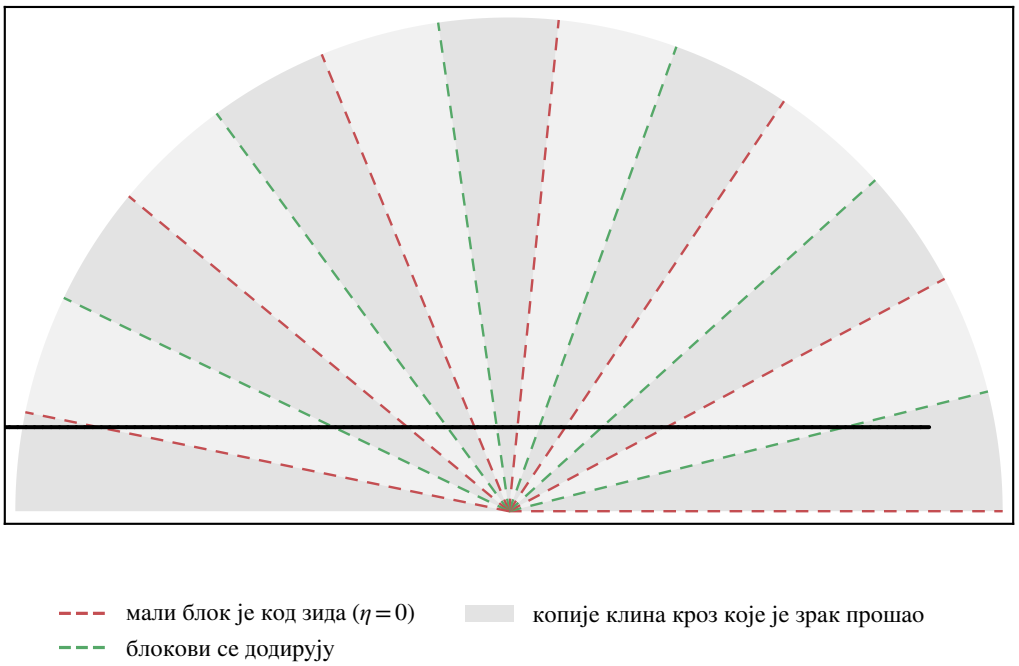
При развијању клина не мењамо механички систем: огледамо геометријску слику путање. У огледаној копији упадни и одбијени део чине једну праву, а прелаз преко заједничке странице одговара тачно једном судару.

Сада долази трик: уместо да зрак одбијемо, огледајмо цео клин преко странице у коју зрак удара, и пустимо зрак да иде право. Зрак тако пролази кроз лепезу копија клина, свака са углом $\bar\theta$, а свако одбијање постаје прелазак једне линије лепезе (Слика А.1). Линије лепезе излазе из темена под угловима $\bar\theta, 2\bar\theta, 3\bar\theta, \ldots$, мерено од странице $\eta = 0$. На почетку мали блок мирује, па се зрак креће паралелно тој страници. Гледано из темена, права паралелна страници пролази кроз све правце са угловима строго између 0 и π, па сече тачно оне линије лепезе чији је угао $j\bar\theta < \pi$. По правилу бројања из §1.11 њих има $\lceil \pi/\bar\theta \rceil - 1$: опет (1.8).

раван положаја, $M/m = 16$: зрак се одбија, број одбијања 12



развијено: зрак иде право и прелази 12 линија



Слика А.1. $M/m = 16$. Горе: зрак се одбија у клину 12 пута. Доле: исти зрак, развијен, иде право кроз лепезу копија клина и прелази 12 линија.

Додатак Б. Радијани, мали углови и периферијски угао

Радијани и дужина лука

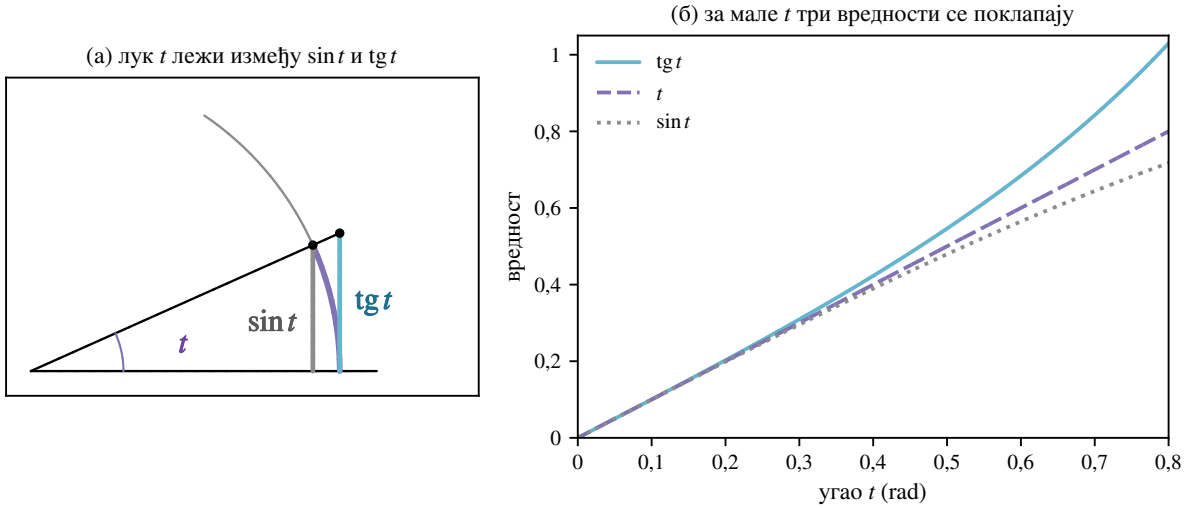
За централни угао φ у радијанима и кружницу полупречника R, дужина лука је $\ell = R\varphi$. Само за јединичну кружницу је $\ell = \varphi$: тада је број радијана једнак дужини одговарајућег лука. Цела кружница има обим 2π, па је π радијана исто што и 180°, а прав угао је $\pi/2$. У овом тексту, када уз угао не пише °, угао је у радијанима. Без радијана број π не би могао да се појави у бројању судара: у степенима би одговор гласио „180° подељено углом“; број судара би био исти, али се π у формули не би видео.

Апроксимација малог угла

За мали угао t лук дужине t лежи између две дужи на Слици Б.1а: синуса, који је мало краћи, и тангенса, који је мало дужи. То следи из поређења три површине. Троугао са теменима у центру кружнице, у тачки $(1, 0)$ и у крају лука има основицу 1 и висину $\sin t$, па површину $(\sin t)/2$. Кружни исечак тог угла је део круга површине π сразмеран углу, па има површину $t/2$. Правоугли троугао са катетама 1 и $\operatorname{tg} t$ има површину $(\operatorname{tg} t)/2$. Свака од ових фигура садржи претходну, па је за $0 < t < \pi/2$ неједнакост $\sin t < t < \operatorname{tg} t$. За мале углове су сва три броја скоро једнака:

$$\sin t \approx t \approx \operatorname{tg} t \qquad \text{за мало } t. \tag{Б.1}$$

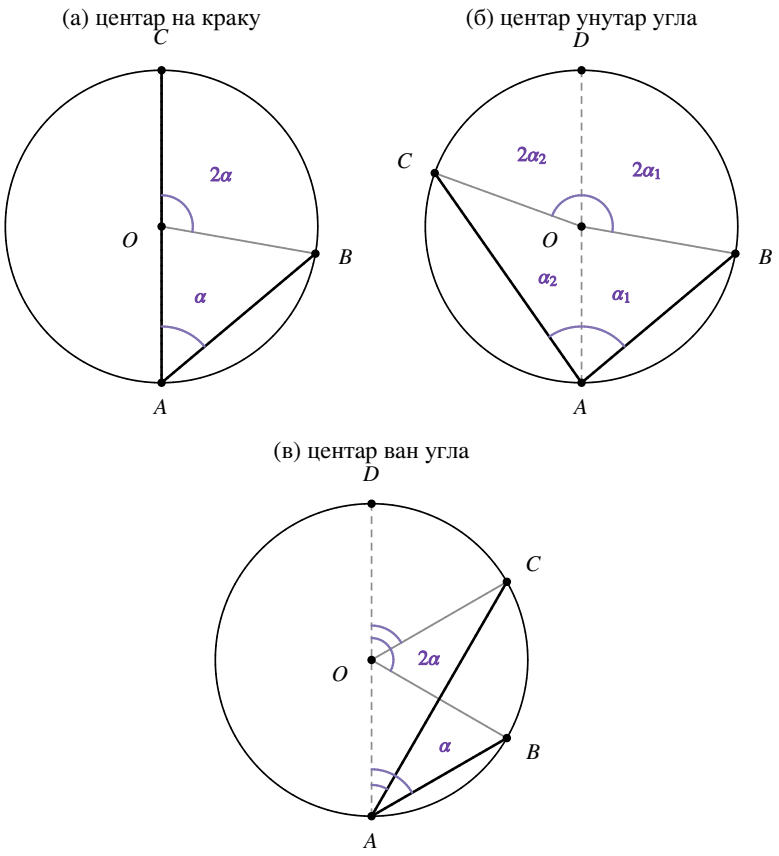
На пример, $\sin 0{,}1 = 0{,}0998$, а $\operatorname{tg} 0{,}1 = 0{,}1003$. Исто важи и обрнуто: угао чији је тангенс мали број t приближно је једнак t, тј. $\operatorname{arctg} t \approx t$, и мало је мањи од t, јер је тангенс мало већи од угла.



Слика Б.1. (а) На кружници полупречника 1 лук дужине t лежи између $\sin t$ и $\operatorname{tg} t$. (б) Три вредности у зависности од угла: за мале углове се поклапају.

Теорема о централном и периферијском углу. У §1.10 користимо да је периферијски угао једнак половини централног угла над истим луком. Ево доказа какав се учи у школи (Слика Б.2).

Нека је O центар кружнице, а A, B и C тачке на њој. Угао BAC има теме A на кружници, а краци му пролазе кроз B и C: то је **периферијски угао** над луком BC који не садржи A. Централни угао BOC над истим луком, који по потреби може бити и већи од 180°, је **централни угао**. Тврдимо да је $\angle BOC = 2\angle BAC$.



Слика Б.2. Теорема о централном и периферијском углу. (а) Центар O лежи на краку AC: троугао AOB је једнакокраки, па је централни угао BOC једнак 2α. (б) Центар унутар угла: пречник AD дели оба угла на по два дела из случаја (а), $\alpha_1 = \angle BAD$ и $\alpha_2 = \angle DAC$, па су централни делови $2\alpha_1$ и $2\alpha_2$ и сабирају се. (в) Центар ван угла: делови из случаја (а) се одузимају. Лукови у A означавају углове DAB и DAC, а лукови у O углове DOB и DOC; α и 2α су њихове разлике.

Најпре размотримо посебан случај, када центар лежи на краку AC, тј. када је AC пречник (Слика Б.2а). Дужи OA и OB су полупречници, па је троугао AOB једнакокраки, а углови на његовој основици AB су једнаки. Означимо их са α; један од њих је баш периферијски угао BAC. Збир углова у троуглу је π, па је $\angle AOB = \pi - 2\alpha$. Тачке A, O и C леже на једној правој, па је $\angle AOB + \angle BOC = \pi$. Одатле је $\angle BOC = \pi - (\pi - 2\alpha) = 2\alpha$.

Општи случај своди се на посебан. Повуцимо пречник AD. Ако центар лежи унутар угла BAC (Слика Б.2б), пречник дели оба угла на по два дела: $\angle BAC = \angle BAD + \angle DAC$ и $\angle BOC = \angle BOD + \angle DOC$. Сваки део је посебан случај, јер му је један крак пречник AD: $\angle BOD = 2\angle BAD$ и $\angle DOC = 2\angle DAC$. Сабирањем добијамо $\angle BOC = 2\angle BAC$. Ако центар лежи ван угла (Слика Б.2в), оба крака су са исте стране пречника, па се углови одузимају: $\angle BAC = \angle DAB - \angle DAC$ и $\angle BOC = \angle DOB - \angle DOC$, и опет је $\angle BOC = 2\angle BAC$.

Периферијском углу $\bar{\theta}$ у §1.10 одговара централни угао $2\bar{\theta}$. На кружници полупречника R дужина тог лука износи $2R\bar{\theta}$, а на јединичној кружници бројно је једнака $2\bar{\theta}$. Теорема је стара: то је став 20 треће књиге Еуклидових *Елемената*.

Појмовник

Адамарова капија – капија H на једном кубиту, $(a, b) \to \big((a+b)/\sqrt{2}, (a-b)/\sqrt{2}\big)$: огледање у односу на праву под углом 22,5°. Шаље $|0\rangle$ у $|+\rangle$, а $|1\rangle$ у $|-\rangle$.

амплитуда – компонента стања у изабраној бази, $a_i = \langle i|\psi\rangle$. У нашем реалном моделу је $P(i) = a_i^2$; за комплексне амплитуде важи $P(i) = |a_i|^2$.

апроксимација малог угла – за мали угао t, мерен у радијанима, је $\sin t \approx t \approx \operatorname{tg} t$ и $\operatorname{arctg} t \approx t$, (1.10) и (Б.1).

база – јединични вектори, нормални један на други, од којих се сабирањем и множењем бројевима састављају сви вектори; у равни то су $|0\rangle$ и $|1\rangle$.

бра – лева половина скаларног производа, $\langle\varphi|$; заједно са кетом $|\psi\rangle$ даје број $\langle\varphi|\psi\rangle$.

Гроверов алгоритам – квантна претрага: почетак у стању $|s\rangle$, затим $k^* \approx (\pi/4)\sqrt{N}$ Гроверових корака, па мерење.

Гроверов корак – оракл, а затим дифузија. У равни $|\bar{s}\rangle$, $|w\rangle$ то је ротација за $2\bar{\theta}$.

дифузија – Гроверово огледање које не користи оракл: огледање у односу на осу $|s\rangle$. Сваку амплитуду одражава у односу на аритметичку средину свих амплитуда, $a_i \to 2\bar{a} - a_i$.

еластичан судар – судар при коме се чува укупна кинетичка енергија тела која учествују у судару.

завршна област – скуп стања у којима више не може доћи до судара, одређен условом $0 \le v \le V$. У равни скалираних брзина то је клин између позитивне x-осе и праве једнаких брзина.

закон одржања – тврђење да се нека величина, на пример енергија или импулс, не мења током кретања.

збир по модулу 2 – операција $\oplus$ на битовима: $0 \oplus 0 = 1 \oplus 1 = 0$ и $0 \oplus 1 = 1 \oplus 0 = 1$.

импулс – производ масе и брзине. У судару два блока укупни импулс се не мења.

интерференција – сабирање и поништавање амплитуда када корак помеша амплитуде; на пример, капија H враћа $|+\rangle$ у $|0\rangle$.

исход – један од могућих резултата мерења. Сваком исходу i одговара базни вектор $|i\rangle$.

јединични вектор – вектор дужине 1.

јединични оператор – оператор $\mathbb{1}$ који сваки вектор оставља какав јесте.

капија са контролом – капија која делује само на оне парове амплитуда у чијим је ознакама бит контролног кубита једнак 1.

квантна капија – унитарни оператор који делује на један или више кубита.

квантно коло – низ квантних капија.

кет – Дираков запис вектора, $|\psi\rangle$.

класа сложености – скуп проблема одлучивања према рачунским ресурсима потребним за њихово решавање. У P одговор се налази у полиномском времену; у NP потврдан одговор може се проверити у полиномском времену уз одговарајући сертификат (§3.3).

колапс – промена стања после мерења; при идеалном мерењу у бази која се овде користи стање постаје базни вектор добијеног исхода.

кубит – квантни систем са дводимензионалним простором стања; рачунску базу чине $|0\rangle$ и $|1\rangle$.

матрица – таблица бројева која записује линеаран оператор: колона i је слика базног вектора $|i\rangle$.

мерење – поступак са могућим исходима; у нашем моделу идеално мерење у изабраној бази даје исход i са вероватноћом a_i^2.

нормалан – који заклапа прав угао. Два вектора су међусобно нормални ако им је скаларни производ нула.

огледање – пресликавање које део стања дуж осе огледања задржава, а делу нормалном на осу мења знак, (3.6); у равни је то осна симетрија из школе. Огледање у односу на осу кроз јединични вектор $|u\rangle$ је оператор $2|u\rangle\langle u| - \mathbb{1}$, (3.9).

одбијање од зида – мали блок удари у зид и промени смер, $v \to -v$. У равни скалираних брзина то је огледање у односу на x-осу, а код Гровера оракл.

одраз у односу на аритметичку средину – пресликавање $a_i \to 2\bar{a} - a_i$: свака компонента прелази на другу страну средине, на исто растојање од ње. Код Гровера се зове дифузија.

означени елемент – елемент w који тражимо.

оператор – правило које сваком вектору придружује вектор; кораци квантног рачунара су линеарни оператори.

оракл – поступак провере или одговарајући квантни оператор коме алгоритам приступа упитима. Фазни оракл мења знак амплитуда означених стања, а остале оставља непромењеним (§3.5).

периферијски угао – угао са теменом на кружници, чији краци секу кружницу; једнак је половини централног угла над истим луком (теорема о централном и периферијском углу, доказ у Додатку Б).

појачавање амплитуде – поступак у коме унитарне операције повећавају вероватноћу означених исхода. У Гроверовом алгоритму, после превише корака вероватноћа поново опада (§3.14).

помоћни кубит – додатни кубит у који провера уписује свој резултат. У стању $|-\rangle$ он пребаци знак на амплитуду кандидата, а сам се не мења.

права импулса – права сталног импулса у равни скалираних брзина, на којој леже тачке са истим укупним импулсом, (1.6); нагиб јој је $-\sqrt{M/m}$. Тачке пре и после судара блокова леже на истој правој (§1.7).

права једнаких брзина – права у равни скалираних брзина на којој је $V = v$; са x-осом заклапа угао $\bar{\theta}$ (по (1.9)) и омеђује завршну област (§1.9). Судар блокова је огледање у односу на њу (Додатак А, задатак 80).

правило парова – капија на једном кубиту делује на сваки пар амплитуда чије се ознаке разликују само у биту тог кубита, на сваки пар исто.

претрага без структуре – претрага у којој немамо корисну структуру која би издвојила кандидате; класично их проверавамо једног по једног (§3.2).

пројектор – оператор који издваја пројекцију на потпростор. За јединични $|u\rangle$, пројектор на његов правац је $|u\rangle\langle u|$.

пројекција – део вектора $|r\rangle$ дуж јединичног вектора $|u\rangle$, вектор $\langle u|r\rangle\,|u\rangle$.

раван брзина – раван са координатама (V,v), брзинама великог и малог блока; за сталну енергију могуће брзине леже на елипси (§1.5).

раван скалираних брзина – раван са координатама $(x,y) = (\sqrt{M}\,V,\sqrt{m}\,v)$; за сталну енергију могуће брзине леже на кружници (§1.6).

раван положаја – раван у којој је положај два блока једна тачка, $(\sqrt{M}\,d_1,\sqrt{m}\,d_2)$.

равномерна суперпозиција – стање у коме све могућности имају исту амплитуду, као $|s\rangle$ у (2.7).

радијан – мера угла: дужина лука који угао исеца на кружници полупречника 1. Угао од π радијана је угао од 180°.

ротација – обртање свих вектора око координатног почетка за исти угао.

скаларни производ – број $\langle\varphi|\psi\rangle$; за реалне векторе једнак је збиру производа одговарајућих компонената и производу дужина и косинуса угла.

сложеност – како број корака алгоритма расте са величином проблема N; пише се $O(\ldots)$, на пример $O(N)$ или $O(\sqrt{N})$.

слој – капије које у колу стоје једна изнад друге и делују у истом кораку (§2.7).

стање – јединични вектор $|\psi\rangle = \sum_i a_i|i\rangle$ који описује квантни систем.

судар блокова – еластичан судар малог и великог блока. У равни скалираних брзина то је огледање у односу на праву једнаких брзина, а код Гровера дифузија.

суперпозиција – линеарна комбинација базних вектора; израз обично користимо када је у изабраној бази више амплитуда различито од нуле.

таблица истинитости – табела која за сваки базни вектор на улазу капије даје излаз.

тензорски производ – операција којом комбинујемо просторе и стања система; на пример $|0\rangle\otimes|1\rangle = |01\rangle$. Спрегнута стања не могу се записати као производ стања појединачних кубита.

Тофолијева капија – капија X на једном кубиту са контролом на два друга, тј. CNOT са две контроле (§3.17).

унитаран оператор – линеаран оператор који чува скаларне производе и има инверз. Квантне капије су унитарне; мерење је другачији процес.

упит – једна употреба оракла.

хеш-функција – функција која податке пресликава у отисак фиксне дужине. Код криптографских хеш-функција циљ је да се отисак лако израчуна, а да проналажење улаза за задати отисак буде рачунски тешко.

Ознаке

Квантна стања и оператори

$|\psi\rangle$, $\langle\varphi|$, $\langle\varphi|\psi\rangle$ – кет, бра и скаларни производ (§2.1, §2.9).

$\|\psi\|$ – дужина вектора $|\psi\rangle$.

λ, μ – бројеви којима множимо векторе.

$|0\rangle$, $|1\rangle$ – базни вектори равни, придружени исходима 0 и 1 кубита.

$|i\rangle$, a_i – базни вектор исхода i и амплитуда тог исхода, $a_i = \langle i|\psi\rangle$.

$\sum_i$ – збир по свим исходима i, њих N.

γ – угао између два вектора, (2.8).

$P(i)$ – вероватноћа да мерење покаже исход i.

$O(\ldots)$ – асимптотска горња граница раста; $O(N)$ значи да је за довољно велико N број корака ограничен сталним вишекратником N (§3.3).

$\otimes$ – тензорски производ (§2.4).

$|+\rangle$, $|-\rangle$ – стања $(|0\rangle + |1\rangle)/\sqrt{2}$ и $(|0\rangle - |1\rangle)/\sqrt{2}$, (2.5).

$|r\rangle$ – произвољан вектор који растављамо на пројекцију и остатак (§2.9, задатак 80).

$|u\rangle$ – јединични вектор: пројектор $|u\rangle\langle u|$ (§2.9) и оса огледања (§3.10).

$|\psi_\parallel\rangle$, $|\psi_\perp\rangle$ – део стања дуж осе огледања и део нормалан на њу (§3.9).

φ, α – угао стања, мерен од осе $|\bar{s}\rangle$; угао између две осе огледања (§3.11).

β, β_1, β_2 – угао осе огледања, мерен од осе $|\bar{s}\rangle$; углови две осе (§3.11).

$|s\rangle$ – вектор са свим компонентама једнаким, (2.7).

$\bar{a}$ – аритметичка средина компоненти (§3.10, §3.14).

$|a\rangle$ – вектор са компонентама a_i; у четвртом поглављу вектор брзина свих кугли (§4.1).

$\lfloor q \rfloor$, $\lceil q \rceil$ – заокруживање наниже (§3.13) и навише (§1.11).

Механика и геометрија

m, M – масе малог и великог блока.

v, V – брзине малог и великог блока, позитивне када се блок креће удесно, од зида.

V_0 – почетни износ брзине великог блока: на почетку је $V = -V_0$ (§1.4).

E, p – кинетичка енергија и импулс.

x, y – координате равни скалираних брзина, $x = \sqrt{M}\,V$ и $y = \sqrt{m}\,v$; код Гровера координате стања у равни $|\bar{s}\rangle$, $|w\rangle$ (§3.9).

Δx, Δy – катете уског троугла уз косу дуж у равни скалираних брзина, (1.9).

$\bar{\theta}$ – код блокова угао између вертикалне и косе дужи у равни скалираних брзина, $\operatorname{tg}\bar{\theta} = \sqrt{m/M}$; код Гровера угао између $|\bar{s}\rangle$ и $|s\rangle$, $\sin\bar{\theta} = 1/\sqrt{N}$.

j – редни број судара или линије лепезе (Додатак А).

$M_з$, $V_з$ – маса и брзина зида, када га замислимо као блок огромне масе (§1.3).

D – цео број $D \geq 0$ у односу маса $M/m = 100^D$.

t – мали угао или мали број (§1.12, Додатак Б).

u – брзина оба блока када су им брзине једнаке (§1.9).

d_1, d_2 – растојања великог и малог блока од зида.

ξ, η – координате равни положаја, $\xi = \sqrt{M}\, d_1$ и $\eta = \sqrt{m}\, d_2$.

Претрага и квантна кола

N, w, n – у претрази број могућности, означени елемент и број кубита, $N = 2^n$; у §1.11 N означава број судара.

$|w\rangle$, $|\bar{s}\rangle$ – базни вектор означеног елемента; стање у коме сви неозначени елементи имају једнаке амплитуде, а означени нулу.

k – број Гроверових корака (§3.13).

$|\psi_k\rangle$ – стање после k корака, (3.14).

k^*, $P(w)$ – изабран број корака близу првог максимума и вероватноћа означеног исхода. У случају изједначења и суседни број корака може бити једнако добар (§3.13).

H, X, Z, CZ – капије из §2.6 и §2.8; пишу се усправним словима.

CNOT, CCZ – капије са контролом (§2.8).

$\mathbb{1}$, $|u\rangle\langle u|$ – јединични оператор и пројектор (§2.9).

U_w, U_s – оракл и дифузија као оператори, (3.3) и (3.8).

f, c, h, $\oplus$ – провера, кандидат, бит помоћног кубита и збир по модулу 2 (§3.4, §3.7).

v_{cm} – брзина центра масе, $(mv + MV)/(m + M)$, (4.2).

C – укупан број судара у оригиналној механичкој загонетки (§4.5).

r – број означених елемената у проширењу претраге са више решења (задатак 87).

ℓ, R – дужина лука и полупречник кружнице; $\ell = R\varphi$ за угао φ у радијанима (Додатак Б).

За даље читање и гледање

- Адам Браун, рад који повезује блокове и Гроверов алгоритам [2]: научни рад за читаоце који желе да упореде ова извођења са оригиналом.
- Два образовна видео-снимка 3Blue1Brown: о блоковима [1] и о Гроверовом алгоритму [6].
- Нилсен и Чуанг (Nielsen, Chuang), поглавље 6 [8]: стандардни уџбеник квантног рачунања; захтева више математичке припреме.

Литература

[1] 3Blue1Brown, „The most unexpected answer to a counting puzzle“ (2019). 3blue1brown.com/lessons/clacks · „Why colliding blocks compute pi“ (2025). youtu.be/6dTyOl1fmDo

[2] A. R. Brown, „Playing Pool with $|\psi\rangle$: from Bouncing Billiards to Quantum Search“, *Quantum* **4**, 357 (2020). doi:10.22331/q-2020-11-02-357 · arXiv:1912.02207

[3] P. A. M. Dirac, „A new notation for quantum mechanics“, *Mathematical Proceedings of the Cambridge Philosophical Society* **35**, 416–418 (1939). doi:10.1017/S0305004100021162

[4] G. Galperin, „Playing pool with π (the number π from a billiard point of view)“, *Regular and Chaotic Dynamics* **8**(4), 375–394 (2003). doi:10.1070/RD2003v008n04ABEH000252

[5] L. K. Grover, „Quantum mechanics helps in searching for a needle in a haystack“, *Phys. Rev. Lett.* **79**, 325–328 (1997). doi:10.1103/PhysRevLett.79.325

[6] 3Blue1Brown, „But what is quantum computing? (Grover’s Algorithm)“ (2025). youtu.be/RQWpF2Gb-gU

[7] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, „Strengths and weaknesses of quantum computing“, *SIAM J. Comput.* **26**, 1510–1523 (1997). doi:10.1137/S0097539796300933 · arXiv:quant-ph/9701001

[8] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, гл. 6 (Cambridge University Press, 2010). Cambridge University Press

[9] L. K. Grover, „From Schrödinger’s equation to the quantum search algorithm“, *Am. J. Phys.* **69**, 769–777 (2001). arXiv:quant-ph/0109116

[10] Massachusetts Institute of Technology, *Introduction to Algorithms*, Lecture 19: Complexity (2020). MIT OpenCourseWare

[11] M. Boyer, G. Brassard, P. Høyer, A. Tapp, „Tight bounds on quantum searching“, *Fortschritte der Physik* **46**, 493–505 (1998). arXiv:quant-ph/9605034

Коначни одговори на задатке

Овде су наведени **само коначни одговори**, без поступака решавања. Одговори су груписани по поглављима. Код задатака у којима се тражи доказ дата је тврдња коју треба добити; сам доказ није наведен. Изрази који се разликују само по глобалном знаку могу описивати исто квантно стање, али је овде, када је то важно, задржан знак који следи из наведеног редоследа капија.

Поглавље 1 — Блокови који броје π

1. 3 судара.

2. 5 судара.

3. $v' = 2v_{\mathrm{cm}} - v$; $V' = 2v_{\mathrm{cm}} - V$.

4. $v' = -6$, $V' = -2$; пре и после судара $E = 24$, $p = -12$.

5. $v' = 3$; $\Delta p = 12$; кинетичка енергија пре и после удара је 9.

6. Редом: судар са зидом; судар блокова; даљих судара нема.

7. $4V^2 + v^2 = 16$; полуосе су 2 дуж осе V и 4 дуж осе v; $R = 4$; $(x,y) = (-4,0)$.

8. Нагиб праве сталног импулса је -4, а праве једнаких брзина $1/4$; њихов производ је -1.

9. $E = 4$; $(x,y) = (-2,-2)$; $R = \sqrt{8}$; после одбијања $(x,y) = (-2,2)$.

10. Завршној области припадају (0,2) и (1,1). За (2,1) блокови се приближавају; за $(-1,3)$ мали блок иде ка зиду.

11. Енергија се учетворостручује, а полупречник удвостручује; углови и број судара остају исти.

12. 3; 3.

13. Централни угао је $30° = \pi/6$; дужина лука је $\pi/2$.

14. Редом 3, 5 и 15 судара. У прва два случаја количник $\pi/\bar{\theta}$ је цео, па се због строге неједнакости одузима 1.

15. За $M/m = 16$: 12 судара; за $M/m = 10^6$: 3141 судар.

16. Тачно 31 судар; приближна вредност је $10\pi \approx 31{,}4159$; разлика је $10\pi - 31 \approx 0{,}4159$.

17. Бинарни запис: $a = 4$; за $D = 0,1,2,3$ бројеви судара су 3,6,12,25, односно $(11)_2$, $(110)_2$, $(1100)_2$ и $(11001)_2$. За тројни запис: $a = 9$.

18. $a = b^2$, односно $M/m = b^{2D}$; приближан број судара је πb^D, али сама апроксимација не гарантује поклапање целих делова.

19. $\operatorname{arctg}(0{,}1) \approx 0{,}0997$; $\pi/0{,}1 \approx 31{,}4159$; $\pi/\operatorname{arctg}(0{,}1) \approx 31{,}5204$. Оба цела дела су 31.

20. $\lfloor 2{,}999 \rfloor = 2$, а $\lfloor 3{,}001 \rfloor = 3$; мала разлика може прећи границу између два цела броја.

Поглавље 2 — Основе квантне механике и квантног рачунарства

21. $\lambda = 1/\sqrt{5}$; $P(0) = 1/5$, $P(1) = 4/5$.

22. $|\psi\rangle = (-2|1\rangle + |3\rangle)/\sqrt{5}$; $(P_0,P_1,P_2,P_3) = (0,4/5,0,1/5)$.

23. $(1,-1)/\sqrt{2} = |-\rangle$; $\|\psi\| = 1$; $P(0) = P(1) = 1/2$.

24. $P(0) = 3/4$, $P(1) = 1/4$; после исхода 1 стање је $|1\rangle$ и поновљено мерење даје 1 са сигурношћу.

25. $|\psi\rangle$ и $-|\psi\rangle$ су исто физичко стање, док је $\mathrm{Z}|\psi\rangle$ различито; за сва три вектора $(P_0,P_1) = (3/4,1/4)$.

26. За оба стања $(P_0,P_1) = (1/2,1/2)$; $\langle +|-\rangle = 0$; ротација за $+45°$ даје $|+\rangle \mapsto |1\rangle$ и $|-\rangle \mapsto |0\rangle$.

27. У бази $\{|0\rangle,|1\rangle\}$: $P(0) = 1$; у бази $\{|+\rangle,|-\rangle\}$: $P(+) = P(-) = 1/2$.

28. $\|\psi\| = 1$; $(P_0,P_1,P_2) = (1/9,4/9,4/9)$; $P(1 \text{ или } 2) = 8/9$.

29. 37/64.

30. $|+\rangle \otimes |-\rangle = (|00\rangle - |01\rangle + |10\rangle - |11\rangle)/2$; амплитуде $(1,-1,1,-1)/2$.

31. $P(00) = 3/8$; $P(11) = 1/8$; $P(\text{први бит} = 1) = 1/4$.

32. $P(00) = P(11) = 1/2$; $P(01) = P(10) = 0$; стање није производно — спрегнуто је.

33. 8 базних стања; $P(101) = 1/8$; $P(\text{први бит} = 1) = 1/2$.

34. $\mathrm{X}(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle$; $\mathrm{X}|-\rangle = -|-\rangle$, што је исто физичко стање.

35. $R|0\rangle = |1\rangle$; $R|1\rangle = -|0\rangle$; $R^T R = \mathbb{I}$; ротација за $+90°$.

36. $\mathrm{H}(a,b) = ((a+b)/\sqrt{2},(a-b)/\sqrt{2})$; $\mathrm{H}^2 = \mathbb{I}$.

37. $|0\rangle \mapsto |0\rangle$; $|1\rangle \mapsto -|1\rangle$; $\mathrm{HXH} = \mathrm{Z}$.

38. Амплитуде: $((\sqrt{3}+1)/(2\sqrt{2}),(\sqrt{3}-1)/(2\sqrt{2}))$; вероватноће: $P(0) = (2+\sqrt{3})/4$, $P(1) = (2-\sqrt{3})/4$.

39. $|s\rangle = \frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle$; $P(101) = 1/8$; $P(\text{први бит} = 1) = 1/2$; 3 капије у једном слоју.

40. $(|00\rangle + |11\rangle)/\sqrt{2}$; исходи 00 и 11, сваки са вероватноћом 1/2.

41. $(|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$; сва четири исхода имају вероватноћу 1/4.

42. Излазне амплитуде у редоследу 00,01,10,11: $(1,1,-1,1)/2$.

43. Само амплитуда $|111\rangle$ мења знак; $\left(\sum_{i=0}^{6} |i\rangle - |111\rangle\right)/\sqrt{8}$; $P(111) = 1/8$.

44. $\langle s|\psi\rangle = 1/2$; $\gamma = 60°$.

45. $\langle +|-\rangle = 0$; $\langle 0|+\rangle = 1/\sqrt{2}$; $\langle 1|-\rangle = -1/\sqrt{2}$; ортогонални су $|+\rangle$ и $|-\rangle$.

46. $P_0|\psi\rangle = (3/5)|0\rangle$; $|\psi\rangle - P_0|\psi\rangle = (4/5)|1\rangle$; $\|P_0|\psi\rangle\|^2 = 9/25$.

47. $P_+|0\rangle = (|0\rangle + |1\rangle)/2$; $\|P_+|0\rangle\|^2 = 1/2$.

48. $F|+\rangle = -|+\rangle$; $F|-\rangle = |-\rangle$; $F|0\rangle = -|1\rangle$; $F = -\mathrm{X}$.

49. $D|r\rangle = |11\rangle = (0,0,0,1)$; мерење сигурно даје 11.

50. Пре H: за оба стања $(P_0,P_1) = (1/2,1/2)$. После H: за $|\psi\rangle$ и даље $(1/2,1/2)$, а за $|+\rangle$ вредности су $(1,0)$.

Поглавље 3 — Гроверов алгоритам

51. 50,5 провера; за $N = 10\,000$ просек је 5000,5.

52. $f(10) = 1$, за остале $f = 0$; $U_w = \mathrm{diag}(1,1,-1,1)$; после оракла $(1,1,-1,1)/2$; све вероватноће пре и после су 1/4.

53. За $f(c) = 1$: $|c\rangle|1\rangle$, $|c\rangle|+\rangle$, $-|c\rangle|-\rangle$; за $f(c) = 0$ сва три улазна стања остају непромењена.

54. $|\bar{s}\rangle = (\sum_{i\neq 101} |i\rangle)/\sqrt{7}$; $\bar{\theta} = \arcsin(1/\sqrt{8}) \approx 20{,}7°$; $U_w|s\rangle = (\sum_{i\neq 101} |i\rangle - |101\rangle)/\sqrt{8}$.

55. Класичан број провера приближно 100 пута, број Гроверових корака приближно 10 пута; време зависи и од цене упита и других операција.

56. $\|\psi_{\parallel} + \psi_{\perp}\|^2 = \|\psi_{\parallel} - \psi_{\perp}\|^2 = \|\psi_{\parallel}\|^2 + \|\psi_{\perp}\|^2$.

57. Средина остаје $\bar{a}$; две примене враћају сваки a_i.

58. Средина је 1/4; после дифузије $(1,0,0,0) = |0\rangle$.

59. Средина после оракла је $3/(4\sqrt{8})$; означена амплитуда $5/(2\sqrt{8})$, остале $1/(2\sqrt{8})$; вероватноћа 25/32.

60. У наведеном редоследу базе $U_w = \mathrm{diag}(1,-1)$ и $U_s = \begin{pmatrix} \cos 2\bar{\theta} & \sin 2\bar{\theta} \\ \sin 2\bar{\theta} & -\cos 2\bar{\theta} \end{pmatrix}$. Производ $U_s U_w$ је матрица ротације за $2\bar{\theta}$.

61. $\bar{\theta} = \arcsin(1/4) \approx 14{,}48°$, $k^* = 3$; вероватноће су редом 1/16, 121/256, 3721/4096, 63001/65536, 609961/1048576. Четвртим кораком вероватноћа опада.

62. Пре и после једног корака $P(w) = 1/2$; формула даје $k^* = 1$, али и $k = 0$ даје исти успех.

63. Ротација за -2α.

64. $|\Delta\varphi| \leq \bar{\theta}$; $P(w) \geq \cos^2\bar{\theta} = 1 - 1/N$.

65. $k^* = 804$; $P(w) \approx 0{,}999999757$.

66. После два корака $P(w) = 121/128$.

67. Крајње стање је $-|11\rangle = (0,0,0,-1)$; исход 11 добија се са вероватноћом 1.

68. Последњих пет колона реализују $-U_s$; за улаз $(1,1,1,-1)/2$ резултат је $(0,0,0,-1)$.

69. Капије X на првом кубиту пре и после Тофолијеве капије; фазно дејство на кандидатима је $\mathrm{diag}(1,-1,1,1)$.

70. После оракла $(1,-1,1,1)/2$, после U_s стање $|01\rangle$; исход 01 са вероватноћом 1.

71. Средишњи слојеви дају $\mathbb{I} - 2|0\cdots 0\rangle\langle 0\cdots 0|$; окружени слојевима H дају $\mathbb{I} - 2|s\rangle\langle s| = -U_s$. Глобални знак не мења вероватноће.

72. $\sin\bar{\theta} = 1/\sqrt{8}$; $k^* = 2$; вероватноћа означеног исхода је $121/128 \approx 0{,}9453125$.

73. $\sin\bar{\theta} = 1/4$; $k^* = 3$; $P = 63001/65536 \approx 0{,}9613$.

74. $100(400 + 40) = 44\,000$ капија; број упита не одређује цену без податка о цени оракла и других операција.

75. За једно означено стање $P = 1$; за два $P = 1/2$. Број означених стања утиче на избор корака; када је непознат, основна формула за избор корака није непосредно применљива.

Поглавље 4 — Два проблема, иста геометрија

76. $m = 1$, $M = 3$; $(v,V,V,V) = v|w\rangle + \sqrt{3}V|\bar{s}\rangle$; за $v = 0$ остаје $\sqrt{3}V|\bar{s}\rangle$.

77. $2E = 29$; нормализовано стање је $(|w\rangle + 2\sqrt{7}|\bar{s}\rangle)/\sqrt{29}$.

78. $\cos\bar{\theta} = \sqrt{N-1}/\sqrt{N}$ и $\sin\bar{\theta} = 1/\sqrt{N}$; права једнаких брзина и $|s\rangle$ имају исте координате.

79. За $-|\bar{s}\rangle$ мали блок мирује и први је међусобни судар; за $-|s\rangle$ оба иду ка зиду и прво је одбијање малог блока од зида. Супротан знак обрће обе брзине.

80. $v' = \big((m-M)v + 2MV\big)/(m+M)$; $V' = \big((M-m)V + 2mv\big)/(m+M)$.

81. $v' = (3V - v)/2$; $V' = (v+V)/2$; оба начина дају исти резултат.

82. Зид: $\mathrm{diag}(1,-1)$; судар: $\begin{pmatrix} (N-2)/N & 2\sqrt{N-1}/N \\ 2\sqrt{N-1}/N & -(N-2)/N \end{pmatrix}$; производ је ротација за $2\bar{\theta}$.

83. Редом 5 судара, 1 Гроверов корак и 2 судара; количник прва два броја је 5.

84. За $M/m = 15$ и почетно мировање малог блока: 12 судара; из Гроверовог почетка: 3 корака, односно 6 судара до заустављања алгоритма.

85. Гровер за $N = 4$: један корак, $P(w) = 1$; за једнаке почетне брзине $v = V = -u$ и $M = 3m$: после судара са зидом и међусобног судара $V' = 0$, $v' = -2u$.

86. $v = -251/256$, $V = 13/256$; удео енергије малог блока је $63001/65536 \approx 0{,}9613$, једнак вероватноћи успеха.

87. $m = r$, $M = N - r$, $\sin\bar{\theta} = \sqrt{r/N}$; за $N = 8$, $r = 2$: $\bar{\theta} = 30°$, један корак и вероватноћа успеха 1. Овде m и M означавају масе означене и неозначене групе; за $r > N/2$ је $m > M$.

88. Једнаки су математички оператори на посебној дводимензионалној равни; брзине блокова и квантна стања имају различито физичко значење, а блокови не остварују произвољне квантне операције нити квантно мерење.