МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2023
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2023
Proceedings of the Fifty Second Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 10–14, 2023

КВАНТОВИ ИЗЧИСЛЕНИЯ ОТВЪД ПРИЛОЖНАТА ЛИНЕЙНА АЛГЕБРА*

Николай Митов Николов

Квантовата информатика е област, изучаваща новите възможности, които предлага квантовата теория за целите на обработка и пренос на информация. В това число са и квантовите изчисления. В настоящата лекция е даден най-напред сбит увод в квантова теория. Изложението следва едно по-абстрактно и по-високо математическо равнище в съответствие с идеите, идващи от Биркхоф и фон Нойман в тяхната изключителна работа върху „логиката на квантовата механика“ (*Annals of Mathematics, Second Series*, **37**, No. 4 (1936), 823–843). Следва кратко въведение в проблематиката на квантовите изчисления от гледна точка на компютърните науки и математиката.

1. Увод и исторически бележки. Квантовите изчисления без съмнение са един от хитовете на започналия век с претенциите си да издигнат производителността на нашите изчислителни възможности на качествено ново ниво. В същото време, дори и най-беглият поглед върху литературата показва, че квантовите алгоритми се отнасят главно до подходящо избрани произведения на матрици. При това, крайни произведения на крайни матрици. С други думи, това са построения свързани с начална линейна алгебра, каквато се намира във всяка учебна програма по математика във висшите учебни заведения.[1] Същевременно, принизяването на областта на квантовите изчисления само до „приложна линейна алгебра“ би било не само некоректно, но и неуважително, при това спрямо едни от най-изтъкнатите математици на всички времена, между които например е Джон фон Нойман (John von Neumann, 1903–1957). Макар физиците обичайно да сочат Файнман (Richard Feynman, 1918–1988), като първият, въвел идеята за квантовите компютри в [7],[2] фон Нойман в съвместна статия с Биркхоф (Garrett Birkhoff, 1911–1996) въвежда концепцията за „квантова логика“ още през 1936 ([3]).[3]

С това, „бащата на съвременния (класически) компютър“, фон Нойман, ясно показва, че квантовата теория отива далеч над физичните си приложения и засяга

*Авторът благодари на Фонд Научни Изследвания за частично финансиране по договор No. КП-06-Н68/3.

2020 Mathematics Subject Classification: 03G12, 81P10, 68Q12, 81P68.

Ключови думи: квантова логика (quantum logic), квантови изчисления (quantum computations), квантови алгоритми (quantum algorithms).

[1] Авторът препоръчва началните глави в повечето учебници по квантови изчисления като един много добър и мотивиран увод в линейната алгебра за нематематици.

[2] макар, че има подобно предложение и в предходните (десетина) години

[3] На снимките от ляво и дясно са съответно Биркхоф и фон Нойман през 20те години.

THE LOGIC OF QUANTUM MECHANICS

By Garrett Birkhoff and John von Neumann

(Received April 4, 1936)

Annals of Mathematics
Vol. 37, No. 4, October, 1936

дори такива аспекти, като логиката. От тук до самата теория на алгоритмите има само една крачка.

Нека обаче на това място да вметнем кратка историческа справка. Преди всичко, квантовата теория се оформя някъде между 1900 и 1930 година. Първата от тези години, 1900, е годината, в която е открита знаменитата константа на Планк, наречена *квант*[4] *на действието*. От тук идва и името „квантова“ на цялата последвала теория. Втората година, 1930, е годината в която е отпечатана първата завършена монография по квантова механика. Това е книгата на Дирак (Paul Dirac, 1902 – 1984) [5], която и до днес не е загубила значението си дори и на учебник, редом с най-съвременните учебни пособия в областта. Новата квантова механика незабавно привлича вниманието на математиците. Тя отправя сериозни математически предизвикателства. Само след две години, през 1932 излиза първото математически строго изложение на квантовата механика. То идва от фон Нойман [15]. Подобно на книгата на Дирак, и тази на фон Нойман остава до днес с непреходно значение. Освен с математическите си предизвикателства, квантовата механика за първи път може би в науката изхожда от аксиоми, които са твърде далеч от очевидното.[5] Фон Нойман веднага се насочва към въпроса за намирането на максимално „естествени“ аксиоми на квантовата теория, както и към обсъждането на възможността за по-общи модели. В съавторство с други видни математици и физици, фон Нойман последователно достига до две по-общи и по-естествени аксиоматизации [10, 3]. Втората от тях е споменатата по-горе съвместна работа с Биркхоф.

Тук е добре да вметнем, че в същата тази година, 1936, Тюринг предлага и знаменития си модел на изчислимост – машината на Тюринг. Така, паралелно с процеса на уточняване на аксиоматичните основи на квантовата теория, тече и процесът на уточняване на математическото понятие за алгоритъм, заедно и с раждането на самата теория на алгоритмите. Фон Нойман живее още 20 години след този период, през което време той оставя забележителна следа в много раздели на математиката.

Следващите четири точки (2–5) съдържат сбито изложение на аксиомите на квантовата теория, изхождащо от квантово логическия подход на Биркхоф и фон Нойман. В точка 6 сме разгледали едни от най-атрактивните резултати на квантовата теория (в това число е и Нобеловата награда по физика за 2022). В последните три точки е даден кратък увод към квантовите изчисления в светлината на предходното математическо въведение. Почти всичко в тази статия е известно и се намира в литературата. На автора обаче не е известен единен източник, където тези факти да

[4]Квант / quantum = елементарна порция. В известен смисъл, квантовата физика издига идеите на атомизма до ново равнище – „атомизъм на действието“ (вж. още забележка 9 по-долу).

[5]Може би за това и по-често се наричат постулати.

се съдържат заедно и да са асамблирани по този начин. Доста от изложените твърдения са прости за доказване и присъстват в една или друга форма в цитираната литература. Най-нетривиалните резултати са указани с точни цитати. Някои забележки, които имат характер на допълнителен материал, са изведени като по-дълги бележки под линия (стоящи на втори, заден план в изложението).

Може да направи впечатление известна несвързаност между квантовата логика, изложена в следващата точка 2, и представения модел на квантови изчисления в точки 8 и 9. Разбира се, това е само един от моделите (макар и най-разпространеният): моделът на квантовите вериги. Има и други модели, сред които е и т. нар. „квантова машина на Тюринг“. Тя, подобно на класическата машина на Тюринг, се среща в различни модификации. Въпросът за тяхната еквивалентност, както и въобще за еквивалентността на различните модели на квантови изчисления, остава до голяма степен открит. С други думи, открит остава въпросът за квантовия аналог на *тезиса на Чърч*. Всъщност, не е напълно ясно дали квантовите изчисления не са по-скоро само симулация на изчисления, посредством физически процеси (подобно на „аналогови компютри“, каквито например са сметачните линийки или изчислителните дъски за геометрични пресмятания в равнината). С настоящата статия целим да привлечем интереса на специалисти от компютърните науки, математическата логика и от други раздели на математиката. Приносът на тези области към квантовите изчисления предстои да се задълбочи и да продължи положеното начало от Биркхоф и фон Нойман.

2. От квантова логика към хилбертови пространства. Квантовата логика е логиката на събитията в микросвета. От своя страна, събитията в микросвета отговарят на свойствата на микрообектите, които установяваме в „да–не“ експериментите (т.е., в експериментите с два изхода). Биркхоф и фон Нойман предлагат в [3] квантовите събития да се описват от една *орто-решетка*, която ще означим[6] с $\mathscr{E}vents$ и ще я наречем **(орто-)решетка на събитията**. По-подробно, понятието за решетка включва частично наредено множество, в което всеки краен брой елементи имат *инфимум* и *супремум*. Релацията на частична наредба ще означим с $\preccurlyeq$ и нейната интерпретация в решетката на събитията е, че $P \preccurlyeq Q$, ако винаги когато е установено събитието P, се установява и събитието Q. Инфимумите и супремумите на двойки елементи в решетка се означават като операции с „$\wedge$“ и „$\vee$“, съответно. Те са квантово-логическите операции на конюнкция и дизюнкция, съответно. В орторешетките имаме допълнително най-малък и най-голям елемент, наречени нула и единица и означени съответно $\mathbf{0}$ и $\mathbf{1}$ (предполага се, че $\mathbf{0} \neq \mathbf{1}$), както и операция на допълнение, която изпълнява законите на де Морган (формула (2.9) по-долу). Последната спомената операция се нарича също **орто-допълнение** и се бележи със знака за ортогонално допълнение $\perp$. За квантовите събития P това е операцията „отрицание“, $P \mapsto P^{\perp}$, което отговаря на размяна на отговорите в „да–не“ експериментите. Сумарно, законите на квантовата логика, които изброихме до тук са:

[6] $\mathscr{E}vents$:= множеството на всички квантови събития

$$P \wedge Q = P \quad \Leftrightarrow \quad P \preccurlyeq Q\,,$$

(2.1) $$P \vee Q = Q \quad \Leftrightarrow \quad P \preccurlyeq Q\,,$$

(2.2) $$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R\,, \quad P \vee (Q \vee R) = (P \vee Q) \vee R\,,$$

(2.3) $$P \wedge Q = Q \wedge P\,, \quad P \vee Q = Q \vee P\,,$$

(2.4) $$P \vee (P \wedge Q) = P\,, \quad P \wedge (P \vee Q) = P\,,$$

(2.5) $$P \wedge P = P = P \vee P\,,$$

(2.6) $$P \wedge \mathbf{0} = \mathbf{0}\,, \quad P \vee \mathbf{0} = P\,, \quad P \wedge \mathbf{1} = P\,, \quad P \vee \mathbf{1} = \mathbf{1}\,,$$

(2.7) $$\left(P^{\perp}\right)^{\perp} = P\,,$$

(2.8) $$P \vee P^{\perp} = \mathbf{1}\,, \quad P \wedge P^{\perp} = \mathbf{0}\,, \quad \mathbf{1}^{\perp} = \mathbf{0}\,,$$

(2.9) $$\left(P \wedge Q\right)^{\perp} = P^{\perp} \vee Q^{\perp}\,, \quad \left(P \vee Q\right)^{\perp} = P^{\perp} \wedge Q^{\perp}$$

(за всеки $P, Q, R \in \mathscr{E}vents$). В горните формули: (2.1) свързва релацията на частична наредба $\preccurlyeq$ с операциите $\wedge$ или $\vee$; (2.2), (2.3), (2.4) и (2.5) са съответно законите за асоциативност, комутативност, поглъщане (absorption law) и идемпотентност;[7] (2.6) задават допълнително решетки с нула и единица; (2.7), (2.8) и (2.9) завършват задаването на орто-решетките. Допълнителни сведения от теория на решетките могат да се намерят в монографиите [1, 9].

Горните закони (2.2)–(2.9) са всъщност законите на класическото съждително смятане с изключение на един, законът за **дистрибутувност**:

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)\,, \quad P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)\,.$$

Дистрибутивните орто-решетки – това са булевите алгебри. За обща орто-решетка, **булева подалгебра** наричаме под-орто-решетка, която е дистрибутивна. Булевите подалгебри на решетката на събитията $\mathscr{E}vents$ се интерпретират, като общите *експерименти* на описваната квантова система. С последното достигаме до най-фундаменталното отличие на квантовата теория спрямо класическото описание на света. Ако $\mathscr{E}vents$ не е булева алгебра, то има квантови събития, които не могат да се установят при никакъв общ експеримент. Такива събития се наричат **несъвместими** или още, **некомутиращи**.[8,9]

Законите на орто-решетки се оказват недостатъчно силни за нуждите на физи-

[7] Тези закони задават решетките като самостоятелни алгебрични структури и това задаване е равносилно на определението, изхождащо от частично наредени множества (посредством връзката (2.1)).

[8] Формално: събитията P и Q комутират по определение тогава и само тогава, когато се съдържат в обща булева подалгебра на $\mathscr{E}vents$.

[9] Физическото обяснение на наличието на съвместно непроверяеми събития е, че всяко наблюдение и измерване в природата е активен процес. Това означава, че при всяко наблюдение ние сме принудени да смущаваме изследваната система. Например, за да видим обект, първо трябва да го осветим със светлина и след това да наблюдаваме отразената светлина: 

В класическата физика, където наблюдаваме макро-системи, смущенията, внесени от нашите наблюдения, също са неизбежни. Там обаче се счита, че смущенията винаги могат да бъдат намалени под нашия праг на чувствителност и следователно могат да бъдат пренебрегнати. Оказва се обаче, че в квантовата физика, т.е., в микро-света, нашите въздействия винаги имат *неотстраним долен* (*минимален*) *праг*, който е свързан със споменатата константа на Планк.

ката. Едно кратко допълнение към тях се оказва достатъчно обаче. Това е т.нар. „закон за **орто-модуларност**“, който гласи:

$$\textit{Ако}\ \ P \preccurlyeq Q\ \ \textit{тогава}\ \ P \vee (Q \wedge P^{\perp}) = Q\,, \tag{2.10}$$

за всеки $P, Q \in \mathscr{Events}$.[10] Законът за орто-модуларност следва от дистрибутивните закони и по такъв начин може да се разглежда като тяхна „отслабена квантова версия“. В теоретичен аспект има следното важно следствие от закона за орто-модуларност. Релацията за комутируемост по-горе може естествено да се въведе не само за двойки събития, но и за произволни крайни подмножества от събития – това е „комутируемост в съвкупност“. *В орто-модуларни решетки елементите на едно крайно подмножество комутират в съвкупност тогава и само тогава, когато комутират по двойки.*

Остават само две заключителни аксиоми за квантовите събития. Първата е специфична за информационните приложения и изразява крайността на системите, които използваме в информатиката.[11] Аксиомата гласи:

$$\textit{Решетката на събитията}\ \mathscr{Events}\ \textit{е от крайно ниво.} \tag{2.11}$$

За да поясним това, първо въвеждаме следното понятие за *ниво на събитие* (или по-общо, ниво на елемент в решетка с нула). По определение, нулевото събитие и само то има ниво нула. За едно *ненулево* събитие P казваме, че има крайно ниво, ако всяка верига $0 = P_0 \preccurlyeq P_1 \preccurlyeq P_2 \preccurlyeq \cdots \preccurlyeq P_r = P$, $P_0 \neq P_1 \neq P_2 \neq \cdots \neq P_r$, е крайна и в множеството на тези вериги има такива с *най-голяма дължина* r. Числото $r \geqslant 1$ се нарича **ниво на ненулевото събитие** P. Една **решетка е от крайно ниво**, ако има единица и тази единица е от крайно ниво. Забележете, че една булева алгебра от крайно ниво е винаги изоморфна на степенното множество на едно крайно множество, чиято кардиналност е равна точно на нивото. Така, нивото на решетката на събитията отговаря на максималния брой алтернативни изхода, които могат да се случат в експеримент.

Последната аксиома за квантовите събития в системата, която тук привеждаме, се нарича **закон за покриването** (covering law) и е въведена от Пирон ([12]). Тя гласи следното:

$$\begin{aligned}&\textit{Ако}\ P\ \textit{е елементарно събитие, а}\ Q\ \textit{е събитие, такова че}\ P \wedge Q = \mathbf{0},\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{тогава}\ P \vee Q\ \textit{покрива}\ Q.\end{aligned} \tag{2.12}$$

Тук сме използвали следната терминология: събитието R **покрива** събитието Q, ако $Q \preccurlyeq R$ и от $Q \preccurlyeq S \preccurlyeq R$ следва, че $Q = S$ или $S = R$ за всяко събитие S; **елементарно събитие** е събитие, което покрива $\mathbf{0}$.[12] В контекста на общата теория на решетките (или дори на частично наредените множества), „елементарните събития“ се наричат **атоми** на решетката.

Условията (2.2)–(2.12) са аксиомите за квантовите събития за крайни квантови системи. Изказани кратко: решетката на квантовите събития е орто-модуларна ре-

[10] Орто-решетки, в които се изпълнява тъждеството (2.10), се наричат орто-модуларни решетки.

[11] Тук следва да се уточни, че фактическата крайност на информационните системи не изключва *потенциалната безкрайност*, която математически може да се свърже с определена индуктивна система от орто-решетки от крайни нива.

[12] Така: ако R покрива Q, то нивото на $R = 1 +$ нивото на Q; елементарните събития са тези и само тези от ниво 1.

шетка от крайно ниво, в която е изпълнен закона за покриването. Тези аксиоми се отнасят обаче за *прости* системи, т.е., без допълнителна структура, като „съставност“, която ще дискутираме по-късно.

Орто-модуларните решетки от крайно ниво допускат разлагане до прости градивни елементи. Това е т.нар. *централно разлагане*, което се строи както следва. Нека за конкретност да разгледаме $\mathscr{E}vents$, но това може да е и произволна орто-модуларна решетка от крайно ниво. Центърът на орто-решетката $\mathscr{E}vents$ се определя като $\mathscr{Z}(\mathscr{E}vents) := \{P \in \mathscr{E}vents \,|\, P \text{ комутира с всяко } Q \in \mathscr{E}vents\}$. В следствие на определението и аксиомите, $\mathscr{Z}(\mathscr{E}vents)$ е булева подалгебра от крайно ниво. Следователно, $\mathscr{Z}(\mathscr{E}vents)$ се поражда от краен брой събития $C_1, \ldots, C_m \in \mathscr{Z}(\mathscr{E}vents)$, които са елементарни в $\mathscr{Z}(\mathscr{E}vents)$. Тогава се доказва, че съответствието $P \mapsto (P \wedge C_1, \ldots, P \wedge C_m)$, където P пробягва $\mathscr{E}vents$, задава изоморфизъм на орто-решетки между $\mathscr{E}vents$ и *пряко произведение*,

$$\mathscr{E}vents \cong \mathscr{L}_1 \times \cdots \times \mathscr{L}_m \,. \tag{2.13}$$

В горната формула $\mathscr{L}_j = \{P \,|\, \mathbf{0} \preccurlyeq P \preccurlyeq C_j\}$ за всяко $j = 1, \ldots, m$ и това се оказват орто-решетки с *тривиален* център.[13,14]

И така, класификацията на моделите на приведените аксиоми се свежда до класифициране на моделите с решетки на събитията, които имат тривиален център. Ще ги наречем (крайни) **неприводими квантови системи**.[15] Пример за това е орто-решетката $\mathscr{G}(\mathscr{H})$ на всички линейни подпространства на едно крайно-мерно комплексно хилбертово пространство $\mathscr{H}$.[16] Всъщност този пример е изходен постулат при традиционния подход към квантовата теория. Хилбертовото пространство $\mathscr{H}$ се нарича **пространство на състоянията** и в следващата точка ще го свържем по-конкретно с понятието за състояние. Пътят до хилбертовите пространства в квантовата теория, който са изминали физиците, е изключително интересен и изпълнен с много догадки. Заслугата на Биркхоф и фон Нойман е в осъзнаването, че логическата структура на събитията има силата да породи $\mathscr{H}$. Всъщност, има пълна класификация на крайните неприводими квантови системи. Тя обобщава по красив начин горния модел $\mathscr{G}(\mathscr{H})$ за хилбертови пространства $\mathscr{H}$. Поради ограничения обем на това представяне ние отпращаме интересуващите се читатели към монографията [12], където могат да намерят допълнителни сведения по резултатите от тази точка.[17]

---

[13] Центърът е тривиален, ако се състои само от два елемента.

[14] Ако $\mathscr{E}vents$ е булева алгебра, то представянето (2.13) придобива вида $\mathscr{E}vents \cong \{0,1\}^{\times m}$, което съответства на представянето на булева алгебра като степенно множество.

[15] или също, крайни чисто квантови системи

[16] Нивото на $\mathscr{G}(\mathscr{H})$ е равно на размерността на $\mathscr{H}$.

[17] Ето някои допълнителни детайли от класификацията на крайните неприводими квантови системи. Всяка такава система се определя от едно *тяло* (пръстен с делене/division ring) $\mathbb{K}$, негов *десен* модул $\mathscr{H}$, *анти*-инволюция на $\mathbb{K}$ и скаларно произведение в $\mathscr{H}$, което е *ермитово* спрямо анти-инволюцията и е *анизотропно* (т.е., няма ненулеви изотропни вектори) (виж. [12], Definitions (3.20), (3.21)). До това води следната връзка с *проективната* геометрия. Ако обявим за „точки на геометрия“ елементите на $\mathscr{E}vents$ от ниво 1 (т.е., елементарните събития, атомите), за „прави на геометрията“: елементите на $\mathscr{E}vents$ от ниво 2 и за релация на инцидентност („точка лежи на права“): релацията на наредба $\preccurlyeq$, то се изпълняват аксиомите на Уайтхед (Whitehead's axioms of projective geometry, виж. [12], Definition (3.4)). Това на свой ред води до *координатизация на геометрията*, която си има своя „числова система“ – тялото $\mathbb{K}$. Алтернативно изложение на тези геометрични построения може да се намери в [13, 14]. Особено интересен е случая на ниво 3 на

По-нататък в това изложение ще се съсредоточим основно върху моделите, произтичащи от комплексни хилбертови пространства. Най-общият модел, който ще разглеждаме, ще се задава от крайно-мерно комплексно хилбертово пространство $\mathscr{H}$, което е разбито във фиксирана оотогонална пряка сума на линейни подпространства, $\mathscr{H} = \mathscr{H}_1 \oplus \cdots \oplus \mathscr{H}_m$, по която определяме следната орто-решетка:

$$\begin{aligned} \mathscr{G}\big(\mathscr{H}_1 \oplus \cdots \oplus \mathscr{H}_m\big) \;=\;& \{V \,|\, V \text{ е линейно подпространство на } \mathscr{H}_1 \oplus \cdots \oplus \mathscr{H}_m \text{ такова,} \\ & \qquad \text{че } V \cap (\mathscr{H}_1 \oplus \cdots \oplus \mathscr{H}_m) \;=\; (V \cap \mathscr{H}_1) \oplus \cdots \oplus (V \cap \mathscr{H}_m)\} \\ \cong\;& \mathscr{G}(\mathscr{H}_1) \times \cdots \times \mathscr{G}(\mathscr{H}_m)\,. \end{aligned} \tag{2.14}$$

Тоест, това е пряко произведение на решетките на събития на крайни неприводими квантови систмеми. Забележете, че в граничния случай

$$\mathscr{G}\big(\mathbb{C} \oplus \cdots \oplus \mathbb{C}\big)\,(= \mathscr{G}\big(\mathbb{C}^{\oplus\, m}\big)\,) \;\cong\; \{0,1\}^{\times\, m} \tag{2.15}$$

получаваме крайна булева алгебра и можем да я определим като решетката на събитията на една **крайна класическа система**. По такъв начин, моделите с решетки на събитията (2.14) са хибридни между класически и квантови системи.

3. Състояния и амплитуди на вероятността. Квантовите събития се определят от това, което може да се измерва в една система. Състоянието на системата се определя от отклика, който системата дава при измерванията. Допускаме най-общо, че този отклик може да е вероятностен. Така, състояние на една квантова система е задаването на вероятност за всяко събитие. С други думи, това е функция $\rho : \mathscr{E}\mathit{vents} \to [0,1]$.

Следната аксиома обобщава адитивното свойство на класическите вероятности.[18]

(3.1) *Състоянията са функциите* $\rho : \mathscr{E}\mathit{vents} \to [0,1]$, *за които са в сила условията*

(адитивност) *ако* $P \preccurlyeq Q$ *тогава* $\rho(Q) \;=\; \rho(P) + \rho(Q \wedge P^{\perp})\,,$

(нормировка) $\rho(\mathbf{1}) \;=\; 1\,.$

Числото $\rho(P)$ *се нарича* вероятност *за установяване на събитието* P *в състояние* ρ.

В частност, $\rho(\mathbf{0}) \;=\; 0$. Множеството на състоянията ще бележим с $\mathscr{S}\mathit{tates}$. То е *изпъкнало* подмножество на реалното линейно пространство на всички функции $\mathscr{E}\mathit{vents} \to \mathbb{R}$. Изпъкналите комбинации $q_1\rho_1 + q_2\rho_2$ на състояния ρ_1 и ρ_2 с тегла $q_1, q_2 \in [0,1]$, $q_1 + q_2 \;=\; 1$ се интерпретират като квантовия аналог на понятието *вероятностна смес* от теория на вероятностите. Състоянието $q_1\rho_1 + q_2\rho_2$ се нарича **смес** на състоянията ρ_1 и ρ_2 с тегла q_1, q_2. Смесването на състояния отговаря на непрецизността при приготвянето на системата и в класическата физика това е основният източник на нетривиални вероятности в измерванията ни. **Чисто състояние** е състояние, което не може да се представи като *нетривиална* смес (т.е., смес с тегла $\neq 0, 1$). Геометрично, това са *екстремалните* точки на $\mathscr{S}\mathit{tates}$ като

решетката, когато има примери на проективни геометрии с *неасоциативни числови системи* $\mathbb{K}$ (това са т.нар., недезаргови геометрии). В алгебричния подход на [10] този пример е свързан с т.нар. *изключителна Йорданова алгебра* (27–мерна), която в последните години привлече силно вниманието на теоретичните физици с евентуалното си приложение за описване на състоянията на *кварките* в елементарните частици (виж., напр., [6]).

[18] Да не забравяме, че тук разглеждаме само крайни системи и затова имаме нужда само от крайна адитивност.

изпъкнало множество.

Ако наречем *крайна класическа система* такава в която решетката на събитията е булева алгебра от крайно ниво,[19] то за такава система $\mathcal{S}tates$ е $(n-1)$–мерен затворен симплекс, където n е нивото. Екстремалните точки на $\mathcal{S}tates$ (т.е., чистите състояния) в този случай са върхове на този симплекс. Вероятностите за събитията в чистите състояния са 0 или 1 – т.е. това са **детерминистични състояния**.

В крайните неприводими квантови системи от ниво > 1 обаче чистите състояния не са детерминистични състояния и всъщност, няма детерминистични състояния. Следната теорема на Глийсон ни разкрива вида на чистистите състояния за случая на крайни неприводими квантови системи, в които решетката на събитията е $\mathcal{G}(\mathscr{H})$ (= решетката на линейните подпространства) за крайно-мерно комплексно хилбертово пространство $\mathscr{H}$ ([12], §4–2).

Теорема. *Нека $dim\mathscr{H}$ е крайна и $\geqslant 3$, и нека $P \in \mathcal{E}vents := \mathcal{G}(\mathscr{H})$ е елементарно събитие, което отговаря на едномерно линейно подпространство в $\mathscr{H}$, породено от единичен вектор Ψ. Тогава съществува единствено състояние ρ, за което $\rho(P) = 1$. То изпълнява формулата $\rho(Q) = \langle \Psi \,|\, \widehat{Q}\Psi \rangle$, за всяко събитие Q, където $\langle \Psi \,|\, \Phi \rangle$ е скаларното произведение в $\mathscr{H}$, а $\widehat{Q}$ е ортогоналният проектор върху линейното подпространство, представляващо Q.*

Тази теорема има следните важни следствия.

(*а*) *Състоянията, построени в горната теорема, са чисти и това са всички чисти състояния за тази система.*

(*б*) *Съществува* 1-1 *съответствие $P \leftrightarrow \rho$ между елементарни събития P и чисти състояния ρ, което е определено по кое да е от следните две еквивалентни условия*:

- *за дадено елементарно събитие P съществува единствено чисто състояние ρ, такова че $\rho(P) = 1$.*
- *За дадено чисто състояние ρ съществува единствено елементарно събитие P, такова че $\rho(P) = 1$.*

(*в*) Горната теорема съпоставя на всяко чисто състояние ρ и единичен вектор Ψ в хилбертовото пространство $\mathscr{H}$. Този вектор се нарича **вектор на състоянието** (затова и $\mathscr{H}$ нарекохме хилбертово пространство на състоянията). Векторът Ψ обаче *не е еднозначно определен*: $\Psi' := z\Psi$ ще бъде вектор на същото състояние за всяко комплексно число z с модул $|z| = 1$. Показва се, че *това е целият произвол при определянето на вектор на състояние.*

(*г*) Следващо важно следствие е, че *всяко състояние ρ еднозначно определя линеен функционал $\widehat{\rho}$ върху алгебрата на всички линейни оператори над хилбертовото пространство $\mathscr{H}$, така че $\widehat{\rho}(\widehat{Q}) = \rho(Q)$ за всяко събитие $Q \in \mathcal{G}(\mathscr{H})$ и съответния му ортогонален проектор $\widehat{Q}$. Полученият линеен функционал е* положителен ($\widehat{\rho}(A^*A) \geqslant 0$) *и* нормиран ($\widehat{\rho}(\widehat{\mathbf{1}}) = 1$). *Вярно е и обратното: всеки положителен, нормиран, линеен функционал η върху $*$–алгебрата на всички линейни оператори над $\mathscr{H}$ е еднозначно свързан със състояние ρ по горното съответствие (т.е. $\eta = \widehat{\rho}$).*

(*д*) Горната теорема с всички изброени следствия след нея се обобщава непосредствено за хибридните модели с решетки на събитията (2.14).

[19] Тогава и цялата булева алгебра е крайно множество.

(*е*) Нека P и Q са елементарни събития, на които съответстват (по горното съответствие от (*б*)) чистите състояния ρ и σ, съответно. Тогава е в сила равенството на вероятностите $\rho(Q) = \sigma(P)$. Това се нарича **вероятност за преход** между (чистите) състояния ρ и σ. Нещо повече, в сила е формулата

$$\rho(Q) \,=\, \sigma(P) \,=\, \big|\langle\Psi\,|\,\Phi\rangle\big|^2 \,(=\, \langle\Psi\,|\,\Phi\rangle\langle\Phi\,|\,\Psi\rangle\,)\,, \tag{3.2}$$

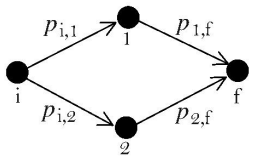
където Ψ и Φ са векторите на състоянията ρ и σ, съответно. Комплексното число $\langle\Psi\,|\,\Phi\rangle$ се нарича **амплитуда на прехода**.

Формула (3.2) има една невероятна интерпретация, когато се комбинира със следната формула от комплексната линейна алгебра

$$\langle\Psi\,|\,\Phi\rangle \,=\, \langle\Psi\,|\,\Theta_1\rangle\langle\Theta_1\,|\,\Phi\rangle + \cdots + \langle\Psi\,|\,\Theta_n\rangle\langle\Theta_n\,|\,\Phi\rangle\,, \tag{3.3}$$

където $\Theta_1, \ldots, \Theta_n$ е произволен *орто-нормиран* базис в хилбертовото пространство на състоянията $\mathscr{H}$. Съгласно изложените дотук аксиоматика и интерпретация на квантовата теория, всеки орто-нормиран базис задава максимален експеримент в една неприводима квантова система. По такъв начин (3.3) модифицира класическия вероятностен модел за преход между две състояния през няколко междинни алтернативни състояния. За простота, нека разгледаме случая на $n = 2$ междинни алтернативни състояния.

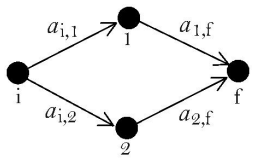
При класическия вероятностен модел вероятността за преход между две състояния, означени с „i“ и „f“, през две междинни алтернативни състояния, означени с „1“ и „2“, се дава по формулата $p_{\mathrm{i,f}} = p_{\mathrm{i},1}\, p_{1,\mathrm{f}} + p_{\mathrm{i},2}\, p_{2,\mathrm{f}}$.



При квантовия модел подобна формула се изпълнява не за вероятностите за преход, а за амплитудите:

$$a_{\mathrm{i,f}} = a_{\mathrm{i},1}\, a_{1,\mathrm{f}} + a_{\mathrm{i},2}\, a_{2,\mathrm{f}},$$

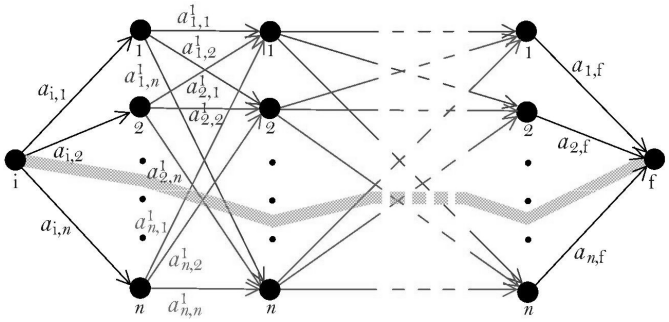
а самите вероятности за преход са: $p_{\mathrm{i,f}} = \big|a_{\mathrm{i,f}}\big|^2$, $p_{\mathrm{i},1} = \big|a_{\mathrm{i},1}\big|^2$, $p_{\mathrm{i},2} = \big|a_{\mathrm{i},2}\big|^2$, $p_{1,\mathrm{f}} = \big|a_{1,\mathrm{f}}\big|^2$, $p_{2,\mathrm{f}} = \big|a_{2,\mathrm{f}}\big|^2$.



Невероятното следствие от квантовия модел на преход през междинни алтернативи е, че е възможно вероятността за общия преход $p_{\mathrm{i,f}} = \big|a_{\mathrm{i,f}}\big|^2$ *да бъде равна на нула или единица* при междинни вероятности $0 < p_{\mathrm{i},1}, p_{\mathrm{i},2}, p_{1,\mathrm{f}}, p_{2,\mathrm{f}} < 1$.

Горният модел се обобщава непосредствено и за преход през няколко междинни алтернативи по формулата $a_{\mathrm{i,f}} = \sum\limits_{j_1,\ldots,j_k\,=\,1}^{n} a_{\mathrm{i},j_1}\, a^1_{j_1,j_2} \cdots a^k_{j_k,j_k}\, a_{j_k,\mathrm{f}}$. Това може да се онагледи с долната фигура, на която е изобразен такъв преход „$\mathrm{i} \to \mathrm{f}$“:

В определени условия, наречени във физиката „класическа граница“, амплитудите на повечето пътища се погасяват взаимно и остава един доминиращ път – указан на долната фигурата с удебелена линия – това е „класическата траектория“ на системата.



4. Измерване, колапс, квантов паралелелизъм и събиране на вектори Квантовата теория е характерна с това, че въвежда на първично, фундаментално ниво понятието за „наблюдател“. Той определя решетката на събитията $\mathscr{E}vents$, а наблюдаваният обект се представя от множеството на състоянията $\mathscr{S}tates$. Фактически, квантовата теория описва взаимовръзката наблюдател – обект, а не обекта „сам по себе си“. Това поражда и до днес дискусии и неудовлетворения, които на кратко ще засегнем по-долу.

Преди това обаче ще приведем заключителната аксиома на квантовата теория: това е въпросът какво се случва след измерване. То е обект на нов постулат, известен като **проекционен постулат на фон Нойман**. Той е формулиран за моделите на неприводими квантови системи с решетки на събитията $\mathscr{G}(\mathscr{H})$ или дори по-общо, за хибридните модели (2.14).

(4.1) *Нека при измерване е установено събитие P, когато системата се е намирала в състояние ρ. Тогава след измерване системата преминава* със скок *в ново състояние ρ', което се определя по формулата* $\rho'(Q) = \dfrac{\widehat{\rho}\big(\widehat{P}\widehat{Q}\widehat{P}\big)}{\rho(P)}$.

В горната формулировка сме използвали конвенциите от точка 3 (*г*) и (*д*). Следват коментари и следствия:

(*а*) Тъй като $\rho'(Q)$ е фактически вероятността за събитието Q *при условие*, че преди това е установено събитието P, то проекционният постулат по същество въвежда **квантовата условна вероятност**.

(*б*) В допълнение на (*а*), за класическите системи (които са тези с булеви решетки на събитията (2.15)) формулата за $\rho'(Q)$ преминава във *формулата на Бейс*: $\rho'(Q) = \rho(P \wedge Q)/\rho(P)$. Последната формула обаче не би могла да определи условна вероятност в общи орто-решетки поради липсата на дистрибутивност.

(*в*) За квантовите модели над хилбертови пространства (с решетки на събитията (2.14)) е в сила, че две събития P и Q комутират в смисъла на орто-решетки (забележка 8 в точка 2) тогава и само тогава, когато съответните им ортогонални проектори комутират, като оператори: $\widehat{P}\widehat{Q} = \widehat{Q}\widehat{P}$. При това, в този случай също $\widehat{P \wedge Q} = \widehat{P}\widehat{Q}$. Така, само единствено за комутиращи събития се изпълнява *законът на Бейс*:

$$Prob_\rho(Q \,|\, P)\, Prob_\rho(P) \;=\; Prob_\rho(P \,|\, Q)\, Prob_\rho(Q)\,, \tag{4.2}$$

където сме въвели означенията $Prob_\rho(P) := \rho(P)$ и $Prob_\rho(Q \mid P) := \rho'(Q)$ от (4.1). По такъв начин, некомутируемостта на събития придобива и допълнителна, „операционна“ интерпретация: за такива събития е важен редът на измерване.

(*г*) Когато измерването е направено в чисто състояние ρ с вектор на състояние Ψ (вж. точка 3 (в)), то и полученото състояние ρ' е чисто и има вектор на състояние, пропорционален на ортогоналната проекция $\widehat{P}\Psi$ (P е установеното събитие).

(*д*) Във формулировката на проекционния постулат употребихме израза *скок*. Това са знаменитите квантови скокове (quantum jumps), които се случват при измерване. Те са въведени от Бор (Niels Bohr, 1885 – 1962). В квантовата физика за тях се говори и като *колапс* на състоянието. Всъщност, „колапс“ има и при класическия закон на Бейс: ако условието, което е настъпило, е елементарно събитие (за класическите системи това са синглетоните[20], т.е., едно-елементните подмножества), тогава крайното вероятностно разпределение „колапсира“ към разпределение, съсредоточено в точка. В класическия случай обаче, това е „колапс“ на нашето незнание (неувереност, непрецизност). Оставяме без дискусия философския въпрос къде всъщност е квантовия колапс: в нас или извън нас. Нека обаче да подчертаем тук едно нещо – това с което започнахме в началото на тази точка: квантовата теория описва взаимовръзката „наблюдател“ – „обект“, без да отстранява „наблюдателя“, както това става в класическата физика. Следователно и колапсът, и скоковете се отнасят преди всичко до тази взаимовръзка.

(*е*) Продължаваме накратко вече в дискусионни въпроси, които обичайно избиват във философски спекулации. Всеки максимален експеримент отговаря на максимална булева алгебра в орто-решетката на събитията, а тя на свой ред поражда ортонормиран базис $\{e_1, \ldots, e_n\}$ в хилбертовото пространство на състоянията $\mathscr{H}$. Всеки вектор на състояние Ψ се разлага в този ортонормиран базис: $\Psi = \psi_1 e_1 + \cdots + \psi_n e_n$, като координатите ψ_j са всъщност амплитудите на преход $\langle e_j \mid \Psi \rangle$ и определят вероятностите $|\psi_j|^2$ за получаване на j-тия изход в този експеримент. След експеримента при получаване на j-тия изход състоянието се изменя със скок към състояние с вектор e_j. Тези факти често получават интерпретацията, че преди измерването състоянието на системата е било „паралелно“ във всички състояния e_j – „квантов паралелелизъм“. Всъщност обаче системата не се е намирала в нито едно от състоянията $e_1, \ldots, e_n$ преди измерването, а в състоянието с вектор Ψ, който се изразява като векторна сума (по-точно, линейна комбинация) с векторите $e_1, \ldots, e_n$. Сумите на вектори във физиката се наричат също „суперпозиции“ и от там идва и изразът, че „състоянието Ψ е суперпозиция на състоянията $e_1, \ldots, e_n$“. Но както вече споменахме в точка 3 (*в*), векторът на състояние не е определен еднозначно от състоянието и по тази причина линейните комбинации на вектори на състояние не задават операции върху състоянията. Независимо от това, идеята за суперпозицията е изиграла ключова роля при откриването на законите на квантовата механика и остава до днес неотменна част от учебниците по квантова физика.

5. Мистерията на квантуването и теория на категориите. Известният математик и физик Едуард Нелсън (Edward Nelson, 1932–2014) казва, че квантуването е мистерия и добавя, че „вторичното квантуване е функтор“. Вторичното квантуване е свързано с квантовата теория на полето и излиза извън тематиката на

[20] бел. ред. (на англ. singletons)

настоящото изложение. Връзката с функтори и теория на категориите представлява обаче интерес.[21] Преди всичко, квантуването е преход (макар и „мистериозен“), при който една класическа система се заменя с квантова. При това, замяната е „плавна“, подобна на деформация и дори математически се описва с „вариране“ на константата на Планк h, като в границата $h \to 0$ е изходната класическа система, която се квантува.[22] В частност, предполага се, че езикът на квантовата теория трябва да включва в себе си и описанието на класическите системи. Това е постигнато вече в хибридния модел на решетки на събитията (2.14). Както отбелязахме, класическите системи са граничният случай на булеви решетки на събитията.

Тук ще добавим едно тривиално наблюдение, което обаче има известно принципно значение. Категорията на крайните булеви алгебри е *дуално* еквивалентна на категорията на крайните множества. Функторът, който задава тази еквивалентност е ***контра-вариантният*** **функтор на степенното множество**: $\Omega \mapsto \mathscr{P}(\Omega)$, $(\Omega_1 \xrightarrow{f} \Omega_2) \mapsto (\mathscr{P}(\Omega_2) \xrightarrow{f^*} \mathscr{P}(\Omega_1))$. В частност, важни теоретико-множествени конструкции, като пряката сума и произведение, се превеждат в категорията на булевите алгебри *дуално*: съответно – като пряко произведение и пряка сума на булеви алгебри (категорни!).

За съжаление обаче категорията на орто-решетките не е толкова „услужлива“, колкото подкатегорията ѝ на булевите алгебри. В категорията на орто-решетките има преки произведения – тях вече ги срещнахме в (2.13) и (2.14). Това дава категорен модел на „квантовата пряка сума на множества“: прякото произведение на орто-решетките. Такъв късмет липсва обаче по отношение на „квантуването“ на декартовото произведение. А именно с декартово произведение се описват *съставните системи* в класическата физиката.

В квантова теория съставните системи се въвеждат посредством тензорното произведение на хилбертовите пространства на състоянията. Нека погледнем от категорна гледна точка тази конструкция. Нека имаме две крайни неприводими квантови системи, именувани A и B, които се описват с решетки на събитията $\mathscr{G}(\mathscr{H}_A)$ и $\mathscr{G}(\mathscr{H}_B)$, съответно. Постулира се, че комбинираната система съставена от A и B има хилбертово пространство на състоянията $\mathscr{H}_A \otimes \mathscr{H}_B$ и следователно, нейната решетка на събитията е $\mathscr{G}(\mathscr{H}_A \otimes \mathscr{H}_B)$. Налице са естествени изображения на влагане на орто-решетки:

$$\begin{array}{ccccc} \mathscr{G}(\mathscr{H}_A) & \hookrightarrow & \mathscr{G}(\mathscr{H}_A \otimes \mathscr{H}_B) & \hookleftarrow & \mathscr{G}(\mathscr{H}_B) \\ V & \mapsto & V \otimes \mathscr{H}_B & & \\ & & \mathscr{H}_A \otimes W & \mapsfrom & W\,. \end{array} \tag{5.1}$$

Лесно се вижда обаче, че горната диаграма няма универсалното свойство на категорна пряка сума и всъщност, такава няма в категорията на орто-решетките.

Ние ще се върнем отново в точка 9 към теория на категориите и търсенето на подходящи категории за квантовата теория. Засега изглежда, че категорията на

[21] Поради ограничения обем на това изложение не сме включили никакъв увод към теория на категориите. Препоръчваме като такъв монографията [8]. Осовните понятия, които използваме тук, са понятията за категорни пряко произведение и пряка сума, както и за функтор.

[22] Разбира се, от физическа гледна точка константата на Планк е константа (и то фундаментална) и не е открита още „командната зала“, от която тя се регулира. Коректната постановка е, че има физически условия, откъдето следват някои приближения, които математически са еквивалентни на клонене към нула на константата на Планк.

орто-решетките не е съвсем подходяща.

6. Квантово сплитане, скрити параметри, нелокалност и декохерентност. Тези теми, макар и на пръв поглед несвързани, имат всичките отношение към „квантовото сплитане“ и то играе ключова роля за тяхното „разплитане“.

Квантовото сплитане (quantum entanglement) е феномен, отнасящ се до състоянията съставните системи. Ние вече въведохме накратко постулата за комбиниране на системи и го изразихме в диаграмата (5.1). Нека да препишем (5.1), като означим по-абстрактно $\mathscr{E}vents_A := \mathscr{G}(\mathscr{H}_A), \mathscr{E}vents_B := \mathscr{G}(\mathscr{H}_B), \mathscr{E}vents_{A\times B} := \mathscr{G}(\mathscr{H}_A \otimes \mathscr{H}_B)$:[23]

$$\mathscr{E}vents_A \overset{\iota_A}{\hookrightarrow} \mathscr{E}vents_{A\times B} \overset{\iota_B}{\hookleftarrow} \mathscr{E}vents_B\,. \tag{6.2}$$

Диаграмата (6.2) поражда *дуална* диаграма:

$$\mathscr{S}tates_A \overset{\iota_A^*}{\leftarrow} \mathscr{S}tates_{A\times B} \overset{\iota_B^*}{\rightarrow} \mathscr{S}tates_B\,, \tag{6.3}$$

където сме означили със $\mathscr{S}tates_A$, $\mathscr{S}tates_B$ и $\mathscr{S}tates_{A\times B}$, съответно (изпъкналите) множества на състоянията на системите A, B и съставната система $A\times B$ (съгласно аксиома (3.1)). Нека въведем и означения за подмножествата на *чистите* състояния на тези три системи: $\mathscr{P}ure\mathscr{S}tates_A$, $\mathscr{P}ure\mathscr{S}tates_B$ и $\mathscr{P}ure\mathscr{S}tates_{A\times B}$, съответно. Вече сме готови за дискусията по темите на настоящата точка, които сме оформили отново като коментари, определения и следствия.

(*а*) Ако някой очаква, че диаграмата (6.3) задава разбиване на $\mathscr{S}tates_{A\times B}$ в декартово произведение на $\mathscr{S}tates_A$ и $\mathscr{S}tates_B$, то следва да предупредим, че това не се случва дори и за класически системи. Това, което е налице за класическите системи[24] е, че подмножествата на чистите състояния са свързани с декартово произведение посредством ограничението на диаграмата (6.3) до тях:

$$\mathscr{P}ure\mathscr{S}tates_{A\times B} = \mathscr{P}ure\mathscr{S}tates_A \times \mathscr{P}ure\mathscr{S}tates_B$$

(по-коректно, това е изоморфизъм, който ние ще приемем за отъждествяване). За квантови системи обаче, макар че имаме естествено влагане

$$\mathscr{P}ure\mathscr{S}tates_A \times \mathscr{P}ure\mathscr{S}tates_B \hookrightarrow \mathscr{P}ure\mathscr{S}tates_{A\times B},$$

съвпадение няма. Чистите състояния в допълнението

$$\mathscr{P}ure\mathscr{S}tates_{A\times B} \backslash (\mathscr{P}ure\mathscr{S}tates_A \times \mathscr{P}ure\mathscr{S}tates_B)$$

се наричат **сплетени състояния** (**entangled states**). И така, това е пълното математическо определение на квантовото сплитане.

(*б*) За квантови системи изображенията ι_A^* и ι_B^* *не могат* да се ограничат до чистите състояния. Тоест, за образите на ι_A^* и ι_B^* имаме $\iota_A^*(\mathscr{P}ure\mathscr{S}tates_{A\times B}) \nsubseteq \mathscr{P}ure\mathscr{S}tates_A$ и $\iota_B^*(\mathscr{P}ure\mathscr{S}tates_{A\times B}) \nsubseteq \mathscr{P}ure\mathscr{S}tates_B$. Изказано само с думи, има чисти състояния на съставните системи, които, когато се ограничат върху отделните съставляващи подсистеми, престават да бъдат чисти състояния (всъщност, това са само сплетените състояния). Загубата на чистота при ограничаване до подсистема се нарича **декохерентност** (decoherence, „загуба на кохерентност“).[25]

[23] Тук полезна забележка е, че макар и диаграмата (5.1) да не е универсална, в смисъл на категорна пряка сума, тя е универсална сред диаграмите, в които образите на ι_A и ι_B комутират взаимно.

[24] Да припомним, че за класически системи множествата $\mathscr{S}tates$ са затворени симплекси с върхове $\mathscr{P}ure\mathscr{S}tates$ – виж. точка 3.

[25] Декохерентността е основния враг на квантовите компютри (а и на всяка квантова установка).

(*в*) Както отбелязахме в (*а*) по-горе, дори за класически системи имаме

$$\mathcal{S}tates_A \times \mathcal{S}tates_B \nsubseteq \mathcal{S}tates_{A\times B}.$$

В този случай обаче изпъкналата обвивка,

$$\mathit{ConvexHull}(\mathcal{S}tates_A \times \mathcal{S}tates_B)$$

съвпада с $\mathcal{S}tates_{A\times B}$. Това се нарушава за квантовите системи:

$$\mathit{ConvexHull}(\mathcal{S}tates_A \times \mathcal{S}tates_B) \subsetneqq \mathcal{S}tates_{A\times B}\,. \tag{6.4}$$

Горното неравенство се изразява в нарушаване на определени неравенства между вероятности, $(\cdots) \leqslant (\cdots)$, които са общият вид на т. нар. **неравенства на Бел**.[26]

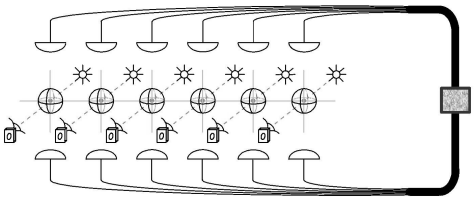
(*г*) Последната подточка има ключово значение за т.нар. проблем за *скритите параметри*. Идеята е, че може би странностите в квантовата теория са в следствие на това, че ние се държим в микро-света като „слон в стъкларски магазин“, но въпреки това, поведението на микро-обектите е напълно детерминирано и е следствие от някакво по-пълно описание, което включва някакви скрити, напълно класически, параметри. Понеже не знаем точното значение на тези параметри, ние усредняваме по тях и от там идва вероятностният характер на квантовата теория. Всъщност, класически скрити параметри действително има: това донякъде е тривиалното наблюдение, че всяка симулация на квантова система на класически компютър е именно описание със скрити класически параметри: класическите параметри – това е класическата памет на компютъра. В следствие на неравенствата на Бел обаче, ако симулираната квантова система е съставна, например това е движението на електрона около протона във водородния атом, то в никой момент не можем да разделим паметта на компютъра на две части, така че състоянието на едната подсистема да зависи от едната част на паметта, а състоянието на другата подсистема – от другата част на паметта. Този феномен се нарича *нелокалност на скритите параметри*.

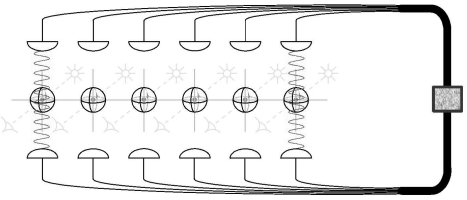
7. Първо сглобяване на квантов компютър. Ще дадем едно начално, силно опростено и схематично от физична гледна точка, описание на квантов компютър и неговата работа. Следваме един от най-утвърдените модели на квантови изчисления – модела на квантовите вериги, който ще определим по-пълно в следващата точка. В този модел на квантови изчисления имаме три главни стъпки, които са дадени на долните схеми. На фигурите, в малките сфери са разположени микро-обекти. Това са отделните *квантови битове* или още наричани *кубити*. Те се удържат в малки области от електромагнитни полета, изобразени във вертикална посока. Тези полета също се използват за промяна на състоянието на кубитите в хода на изчислението. В хоризонтална посока са разположени други източници за въздействие върху кубитите, резултата от които се регистрира от детектори.

Тя идва от това, че изследваната система (напр., системата от квантовите битове на компютъра) влиза в сплетено чисто състояние с околната среда и затова, когато състоянието се ограничи върху нея, то става смесено (губи чистотата си). Сплитането с околната среда е в следствие на взаимодействието с нея. Спасението е в изолацията.

[26] John Bell, 1928 – 1990. За експерименталното потвърждение на нарушаването на неравенствата на Бел беше дадена Нобеловата награда по физика за 2022.

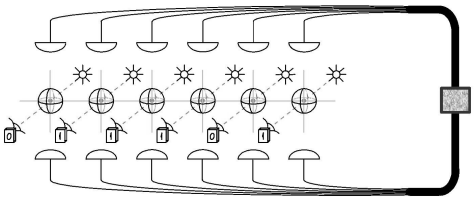
1) *Инициализация.* Квантовите битове се привеждат всеки в начално състояние. Общото състояние е несплетено. За тази инициализация може да се използва измерване (проекционният постулат). Измерванията, които извършваме, считаме, че съответстват на един фиксиран ортонормиран базис на хилбертовото пространство на състоянията на кубитите. Този базис се нарича **изчислителен базис**.



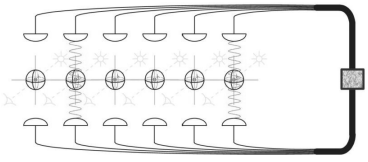


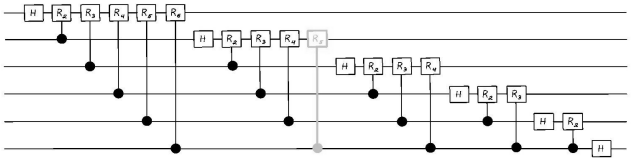
2) *Изпълнение на квантовото изчисление.* Тук се изпълняват т.нар. *квантови трансформации* или още, *квантови гейтове* (quantum gates). За тях ще спомена повече в следващата точка. Тези операции променят последователно състоянието на кубитите и те се сплитат. Промените на състоянията се извършват под въздействие на вертикалните полета, които се командват от някакъв общ команден център – сивата кутия в дясно.

3) *Прочитане на резултата.* Отново, както и в стъпка 1), извършваме измерване на състоянието на всеки кубит. Ако след стъпка 2) общото състояние е на кубитите остава сплетено, то резултатът ще е вероятностен. При подходящо подбрана последователност на квантовите операции обаче, може да се окаже, че макар на междинните стъпки системата да е преминала през сплетени състояния, в края тя е в несплетено състояние и ние с вероятност 1 (или, по-общо, близка до 1) прочитаме търсения резултат.



8. Моделът на квантовите вериги за квантови изчисления. Съществената част от работата на квантовия компютър, която се отнася до самото квантово изчисление и алгоритъм, е стъпка 2) в предходната точка. Тя се състои от последователно изпълняване на квантови операции върху един или няколко квантови бита. Тази последователност се онагледява с т.нар. **квантова верига** (quantum circuit), изобразена на долната фигура:





В дясната част на горната фигурата, в по-блед сив цвят е указана една от квантовите операции в последователността, която се изпълнява върху втория и последния бит, както е илюстрирано на схемата отляво на фигурата.

Квантвата верига обобщава т.нар. *булеви вериги*, или още, булеви *схеми*, които са един класически модел на изчисление, особено популярен в курсовете по цифрова електроника (digital electronics). В класическия случай, горната верига би означавала определена *булева* функция $\{0,1\}^{\times n} \to \{0,1\}^{\times n}$ (на фигурата, $n = 6$). Тя съставлява композиция от отделни изображения от тип $\{0,1\} \to \{0,1\}$ (на фигурата: на първо, седмо, дванайсто, шестнайсто и последно място, от ляво на дясно) и от тип $\{0,1\}^{\times 2} \to \{0,1\}^{\times 2}$. В допълнение, тези изображения, $\{0,1\} \to \{0,1\}$ или $\{0,1\}^{\times 2} \to \{0,1\}^{\times 2}$, са „вмъкнати“ на определени позиции в декартовото произведение $\{0,1\}^{\times n}$, като върху другите декартови множители се изпълнява идентитетът. При квантовите вериги, отново имаме композиция, но тя е линейно изображение $(\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ и композицията се формира по правилата на *полилинейната алгебра*.

Пространството $\mathbb{C}^2$ е хилбертовото пространство на състоянията на кубит. Така, квантовият бит е неприводима квантова система от ниво 2 (всеки експеримент има максимум 2 алтернативи, виж. точка 2). Изпъкналото множество на състоянията на кубита е единичното затворено кълбо в $\mathbb{R}^3$, на чиято граница, единичната сфера, са чистите състояния: това е **сферата на Блох** (Bloch sphere, Felix Bloch, 1905 – 1983).

Вече споменахме, че квантовите операции, или още, квантовите трансформации, са линейни изображения. Те се оказват всъщност *унитарни автоморфизми* на хилбертовото пространство на състоянията $\mathscr{H}$. Най-общо, те идват от т.нар. теорема на Вигнер (Eugene Wigner, 1902 – 1995), която дава най-общия вид на *автоморфизмите* на орто-решетките $\mathscr{G}(\mathscr{H})$ ([12], Theorem (3.28)). Така, **квантовите трансформации са винаги обратими** (или поне засега, само за такива можем говорим и такива можем да извършваме). Това е едно важно ограничение при квантовите изчисления, каквото отсъства при класическите. Впрочем, постигането на обратимост при класическите изчислителни вериги отдавна е привлякло вниманието и е известно като областта *обратими изчисления* (reversible computing, виж., напр., [2]). Това е свързано с постигането на по-ниско отделяне на топлина при работата на компютрите (low power computation).

Квантовите трансформации на квантовия бит формират унитарната група $\mathrm{SU}(2)$, която е двукратно накритие над групата на тримерните евклидови ротации $\mathrm{SO}(3)$ (не случайно състоянията на кубит се представят в кълбо в $\mathbb{R}^3$). Това е един от изключителните математически феномени и благодарение на него има връзка между логическите квантови автоморфизми на най-простата квантова система и геометричните симетрии на пространството, в което живеем.

Тази точка ще завършим с точното фиксиране на модела на квантовите вериги за квантови изчисления. Една верига изчислява крайна функция $\{0,1\}^{\times n} \to \{0,1\}^{\times n}$. За да говорим за алгоритъм, ни трябва цяла *фамилия* от вериги за $n = 1, 2, \ldots$. Това са **равномерни фамилии от вериги** (uniform circuit families), което е понятие, включващо в себе си две условия. Първо, съгласуваност при нарастване на n (старите изчислителни резултати не трябва да се променят). Второ, фамилията трябва да е алгоритмично породена от *класически алгоритъм* (т.е., трябва да има

класическа закономерност при строенето на веригата, каквато ясно се вижда на фигурата по-горе). Така, това понятие за квантов алгоритъм не е автономно и изисква предварително понятие за класически алгоритъм.

През изминалите две десетилетия на новия век са излезли редица монографии по квантови изчисления. Тук ще спомена две. Една от първите и най-разпространени е книгата на Ниелсен и Чуанг [11], чието първо издание е от 2000, а през 2010 излиза 10-ото юбилейно издание. Една от монографиите излезли през второто десетилетие на нашия век, е книгата на Мингшенг Инг [16], в която може да се открие и връзка с квантовата логика на Биркхоф и фон Нойман.

9. Квантови алгоритми и квантово програмиране: дискусия. Програмните езици са практическият израз на алгоритмите. Програмните езици, които описват разгледания в предната точка модел на квантов алгоритъм, трябва първо да изразяват в себе си набора базисни гейтове (т.е., да съдържат символи за определени унитарни оператори $(\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes k}$ за $k = 1, 2$ и евентуално и повече кубита). След това, езикът просто описва реда на композициите на базисните гейтове, като се указват и номерата на кубитите, върху които те се извършват. Ние няма да се спираме на конкретните примери за такива езици, доколкото в тях няма да открием нищо повече, което да е от фундаментално и принципно значение. Фактически, при този модел на квантови алгоритми, ние строим определени произведения на унитарни матрици[27] $W_n := U_1 U_2 \cdots U_{t(n)} : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$, за всяко $n = 1, 2, \ldots$ (това беше в концепцията за *равномерна* фамилия). Целта е получената матрица W_n да има коефициенти, които в иделания случай да са само 0 или 1.[28] От значение е ръстът на $t(n)$ – това е *изчислителното време* – в зависимост от броя n на кубитите, които се обработват. Всъщност, при класическия модел на алгоритъм с булеви вериги, когато веригата допълнително е обратима, тя може да се представи също и с произведение на унитарни матрици, $M_1 M_2 \cdots M_{t_{classical}}$, всяка от които сега се състои само от 0 или 1. Квантовият авантаж идва от това, че квантовото изчислително време $t(n)$ може да е $\ll$ от класическото $t_{classical}(n)$ при $n \to \infty$. Това се дължи на феномена на „погасяване на амплитудите“, който срещнахме в края на точка 3. В това именно се корени очакването за превъзходството на квантовите компютри над класическите.

От по-принципна и концептуална гледна точка обаче, моделът на квантовите вериги и свързаните с него програмни езици изглеждат като „програмиране на ниско ниво“. Ние директно описваме инструкциите за обработка на квантовите регистри. Засега обаче не е толкова добре изградена концепцията за квантово програмиране от по-високо ниво. В класическите програмни парадигми има декларативен, функционален подход, при който алгоритми могат да оперират върху алгоритми (при подходяща формализация на това). В класическата теория на алгоритмите, това е може би най-добре изразено в т.нар. ламбда–смятане (типово или безтипово).[29] Съществуват развити аналози за това и в квантовия свят, макар засега да не е ясна

[27] По-коретно е да се обърне редът на произведението, както при композиция на функции, но не сме го направили за по-добра „операционна“ нагледност.

[28] Или, поне да са по модул $< \varepsilon$ или $> 1 - \varepsilon$, за всяко отнапред зададено $\varepsilon > 0$. В този случай, в произведението $U_1 U_2 \cdots U_t$ зависи и от желаната точност ε.

[29] На това място отново може да започне да играе роля теорията на категориите, тъй като е добре известна връзката ѝ с класическото ламбда–смятане, която е оказала голямо влияние.

пълната им взаимовръзка с императивния подход на веригите. Основният концептуален проблем е въпроса с измерването, което в класическия случай е постоянно и поради това не се отчита изобщо. В този ред на концептуални проблеми ще отбележим и липсата на ясен квантов аналог на проблема за спиране (halting problem). В известните квантови алгоритми, като този за търсене (на Гровер /Grover) или за факторизация (на Шор/Shor), ние не само знаем кога ще спрат алгоритмите, ние отнапред знаем времето, по което *трябва* да ги спрем. Алгоритъмът за търсене е направо цикличен и ако не бъде спрян в точния момент, той ще ни върне обратно в изходното състояние.

Всъщност, добрата новина е, че има много и интересни отворени проблеми, работата по които може да намери допълнителен тласък, ако се постигне по-голяма приемственост между класическата теория на алгоритмите във всичките ѝ аспекти и квантовата.

Благодарности. Авторът е благодарен на проф. Божко Бакалов, Станислав Велков, доц. Димитър Гелев, д-р Петко Николов, проф. Иван Пенков, д-р Тодор Тодоров, и д-р Валдемар Цанов за корекциите, бележките, отзивите и подкрепата им при подготовката на настоящия доклад. В точки 2–8 са използвани фигури от [17].

ЛИТЕРАТУРА

[1] G. Birkhoff. Lattice Theory. American Mathematical Society, Providence, Rhode Island, 1st edition 1940, 3d edition 1973.
[2] A. De Vos. Reversible Computing: Fundamentals, Quantum Computing, and Applications. Wiley, 2010
[3] G. Birkhoff, J. Von Neumann. The Logic of Quantum Mechanics. *Annals of Mathematics*, Second Series, **37**, No. 4 (1936), 823–843.
[4] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. 1985
[5] P. A. M. Dirac. The Principles of Quantum Mechanics. Oxford University Press, 1st edition 1930, 4th edition 1967.
[6] M. Dubois-Violette. Exceptional quantum geometry and particle physics. *Nucl. Phys.* **B 912** (2016), 426–444; arXiv:1604.01247
[7] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, **21**, Nos. 6/7 (1982), 467-488.
[8] R. Goldblatt. Topoi: The Categorial Analysis of Logic. Revised Edition, Elsevier, New Yoyk, 1984.
[9] G. Grätzer. Lattice Theory: Foundation. Basel, Birkhauser, 2011.
[10] P. Jordan, J. Von Neumann, E. Wigner. On an Algebraic Generalization of the Quantum Mechanical Formalism. *Annals of Mathematics*, Second Series, **35**, No. 1 (1934), 29–64.
[11] M. A. Nielsen, I. L. Chuang. Quantum Computation and Quantum Information. 10th Anniversary Edition, Cambridge University Press, 2010.
[12] C. Piron. Foundations of Quantum Physics. London, W.A. Benjamin, Inc., 1976.
[13] V. S. Varadarajan. Geometry of Quantum Theory, Volume 1. New York, Springer, 1968.
[14] V. S. Varadarajan. Geometry of Quantum Theory, Second Edition. New York, Springer, 1968.
[15] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*, Springer, 1st edition 1932; english translation by Princeton University Press 1955, 2018

[16] M. Ying. Foundations of Quantum Programming. Elsevier, 2016.
[17] Н. М. Николов. Квантова информатика, учебно пособие, 2022.

Николай Митов Николов
Институт за ядрени изследвания и ядрена енергетика
Българската академия на науките
бул. Цариградско шосе 72
1784 София, България

Факултет по математика и информатика
Софийски университет „Св. Климент Охридски“
бул. Джеймс Баучър 5
1164 София, България
e-mail: nikolov.qft@gmail.com

QUANTUM COMPUTING BEYOND APPLIED LINEAR ALGEBRA

Nikolay M. Nikolov

Quantum Informatics is a field studying the new possibilities that quantum theory offers for the purposes of information processing and transfer. This involves Quantum Computing. In this lecture we first give a brief introduction to quantum theory. The content follows a more abstract and higher mathematical level in line with the ideas coming from Birkhoff and von Neumann in their outstanding work on the "logic of quantum mechanics" (*Annals of Mathematics*, Second Series, **37**, No. 4 (1936), 823–843). This is followed by a brief introduction to the problems of Quantum Computing from the perspective of Computer Science and Mathematics.