

5 Наблюдаеми. Алгебричен подход към квантовата теория

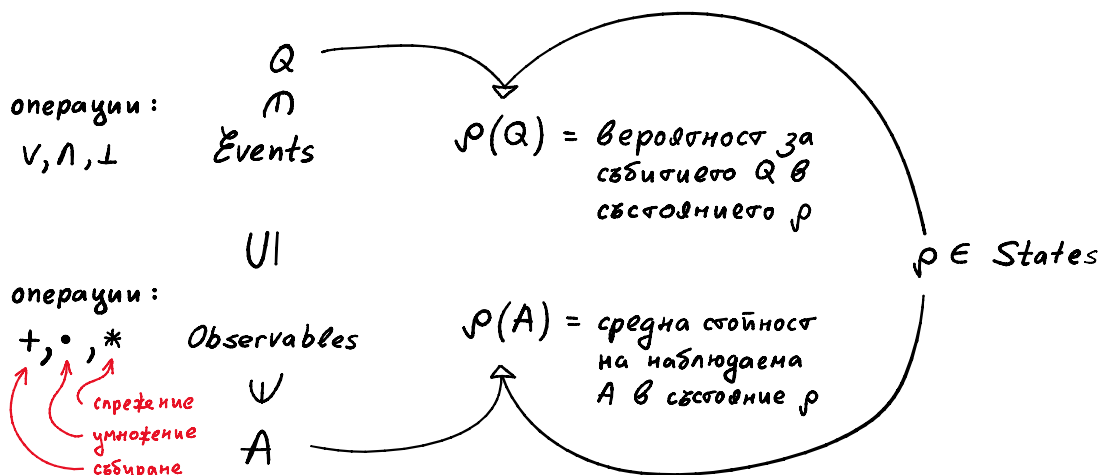
Алгебричният аксиоматичен подход, към който ще преминем сега разполага с повече първични изразни средства (или още казано, повече първични понятия), спрямо логическия подход, с който започнахме. Поради това, досегашния подход ще има интерпретация в новия. Основното предимство на алгебричния подход е, че в него по-бързо и лесно се стига до теоретични предсказания. Същевременно обаче, аксиоматичните предположения на алгебричния подход са по-силни и по-слабо свързани с интуицията ни. Въпреки това, изненадващо е, че двата аксиоматични подхода се оказват по същество еквивалентни. Ние вече въведохме редица важни понятия и принципи на квантовата теория, които ще се пренесат и в новия алгебричен подход. Това включва понятията за събития и тяхната логическа структура, експеримент, съвместна измеримост и др. В останалата част на курса обаче, ние ще продължим да изграждаме квантовата теория само в алгебричния подход. Това е от една страна, поради по-лесното изграждане на теорията, дължащо се на по-богатата изразност и от друга страна, това е и традиционния исторически път и в него е натрупан богат опит.

5.1 Съпоставка между квантово-логическия и алгебричния подход

Ще започнем с кратка съпоставка между досегашния квантово логически подход и новия алгебричен аксиоматичен подход. Схематично тази съпоставка е изобразена на долната фигура.

Наблюдатели

Обекти



фиг. 33: Съпоставка между квантово-логическия и алгебричния аксиоматични подходи.

Неотменна остава основната черта на квантовата теория, че тя не описва обектите сами по себе си, но единствено тяхното отношение спрямо нас. Така, както в квантово логическия подход така и в алгебричния аксиоматичен подход ние ще имаме две основни страни на теорията. Това са страната на наблюдателите и страната на обектите. В квантово логическия подход, страната на наблюдателите е представена от множеството на събитията **Events**. В алгебричния подход ние разширяваме множеството на събитията до по-широко множество, което ще наричаме множество на наблюдаемите и което ще означаваме с **Observables**. В множеството на събитията имаме логически операции $\vee$ (“или”), $\wedge$ (“и”), $\perp$ (“не”, т.е., “отрицание”). В алгебричния подход на тези операции ще съответстват аритметичните операции $+$ (“събиране”), $\cdot$ (“умножение”), $(\cdot)^*$ (“спрежение”), каквито, например имаме в числовата система комплексните числа.

От страната на състоянията няма да имаме промяна: множеството **States** ще остане същото заедно с неговата структура на изпъкнало множество. В квантово логическия подход състоянията се разглеждаха, като специални функции на състоянията. Тъй като в алгебричния подход множеството на наблюдаемите разширява множеството на събитията, то

състоянията ще бъдат продължени, като функции върху множеството на наблюдаемите. Стойността, която едно състояние ще съпоставя на наблюдаема ще бъде **средната ѝ стойност**, което в случая на събитие е неговата вероятност.

5.2 Понятие за наблюдаема (величина). Събитията като наблюдаеми

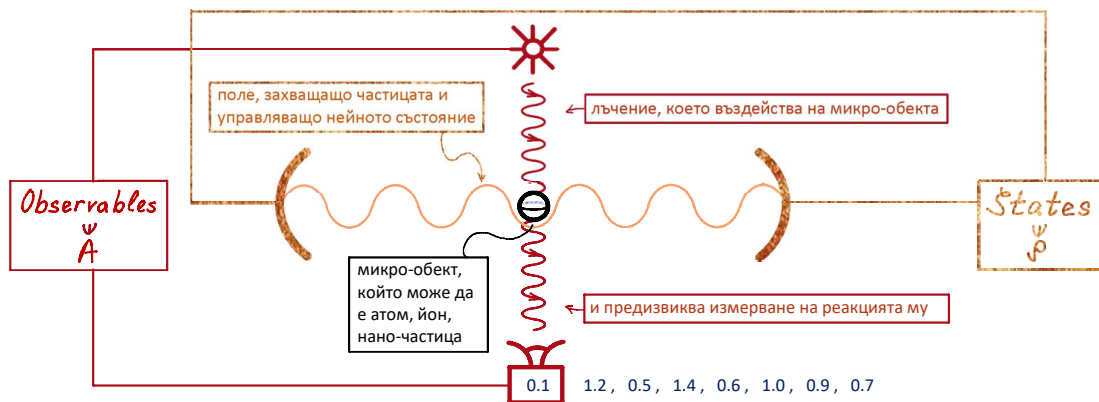
Наблюдаемите или както пълно се наричат, **наблюдаемите величини**, са първични обекти за алгебричния подход. Те могат обаче да се въведат, както на базата на квантово логическия подход, така и на базата на нашия интуитивен опит. Наблюдаемата е експеримент, с чийто елементарни алтернативи са асоциирани различни числа. Ние ще означаваме наблюдаемите с големи букви като $A, B, \dots$. Ако елементарните алтернативи на експеримента, който отговаря на измерването на наблюдаема A са събитията $Q_1, \dots, Q_m$ и на тях са съпоставени числата $\alpha_1, \dots, \alpha_m$, съответно, то казваме, че за e измерена стойността α_k , ако е измерено събитието Q_k . Множеството от числа $\{\alpha_1, \dots, \alpha_m\}$ се нарича **спектр** на наблюдаемата A и ще пишем:

$$Spec A = \{\alpha_1, \dots, \alpha_m\}. \quad (5.1)$$

Събитията $Q_1, \dots, Q_m$ се наричат **спектрални събития** на наблюдаемата. Един от централните математически резултати на който се основава алгебричния подход е така наречената **спектрална теорема**, с която ще се запознаем в следващата лекция.

Всяко събитие ще разглеждаме, като наблюдаема. За целта въвеждаме уговорката, че събитието е наблюдаема, която приема само две стойности – “0” и “1” – като стойността “1” съответства на настъпването на събитието и “0” съответства на настъпването на неговото отрицание.

Има съответно обобщение на илюстративната схема от фиг. 21 при квантово логическия подход:



фиг. 34: Примерна схема на измерване на наблюдаема в квантова система

Нека си припомним, че в случая на тестване на събитие в резултат от многократното повторение на опита получаваме редица от потвърждения (“*да*”) и отхвърляния (“*не*”) на събитието. В случая на измерване на наблюдаема, резултата от многократното повторение на опита е редицата от измерени стойности, които са елементи на спектъра на наблюдаемата:

$$a_1, a_2, \dots, a_N, \dots \in \{\alpha_1, \dots, \alpha_m\}. \quad (5.2)$$

Така, в случая на измерването на събитие, разглеждано като наблюдаема, тази редицата от “*да*” и “*не*” преминава в редица от “1” и “0”, съответно.

Редиците (5.2) са случайни, както и преди, в случая на тестване на събитие. Единствената значима информация, която тези редици съдържат е статистическата. За всяка наблюдаема A ние ще извлечем само една статистическа характеристика от редицата (5.2). Това е нейната **средна стойност**, чието емпирично определение е

$$\lim_{N \rightarrow \infty} \frac{a_1 + \dots + a_N}{N}, \quad (5.3)$$

което е обобщение на закона за големите числа (2.6). В следващата лекция ние ще се спрем по-подробно на връзката между ф-ли (5.4) и (2.6). Тук ще споменем само, че когато наблюдаемата A е събитие Q , то съгласно нашето съглашение по-горе, редицата (5.2) преминава в редица от нули и единици и

тогава ф-ла (5.4) преминава в (2.6):

$$\lim_{N \rightarrow \infty} \frac{\overbrace{a_1 + a_2 + \dots + a_N}^{\text{брой потвърждения "да" на } Q}}{N} \quad (5.4)$$

(за $a_1, a_2, \dots = 0, 1$). С други думи, средната стойност на събитие, разглеждано като наблюдаема е точно неговата вероятност.

Това ни доведе до интерпретацията на състоянията, като функции на наблюдаемите в алгебричния аксиоматичен подход. Както и в квантово-логическия подход, така и в алгебричния подход, статистическата информация, която получаваме в експериментите е това, което характеризира състоянието на системата. Вероятностите на всички събитията са напълно достатъчна статистическа информация, която да характеризира състоянието, съгласно резултатите на квантово-логическия подход. Към тези вероятности ние добавяме сега и средните стойности на останалите наблюдаеми. Така, състоянията стават функции върху множеството на наблюдаемите, които разширяват досегашните функции на състоянията, които бяха определени само върху множеството на събитията. Това е означено на следната фигура:

$$\begin{array}{ccc} \rho: \text{Events} & \longrightarrow & [0, 1] \\ \cap \downarrow & & \cap \downarrow \\ \text{Observables} & \longrightarrow & \mathbb{R} \end{array}$$

фиг. 35: Състоянията, като функции на наблюдаемите в алгебричния подход са продължение на функционалната им зависимост от събитията в квантово-логическия подход.

Ние ще означаваме средната стойност на наблюдаема A в състояние ρ , като

$$\langle A \rangle_\rho \equiv \rho(A), \quad (5.5)$$

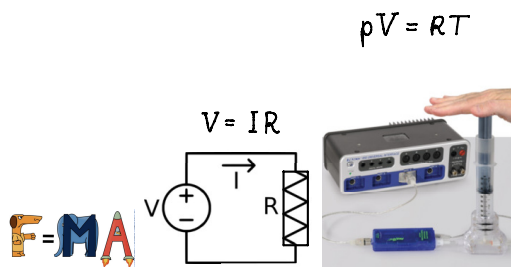
където означението в лявата страна следва традициите от теория на вероятностите и физиката, докато означението в дясната страна отразява възприемането ни за състоянията, като функции на наблюдаемите. В случая

на събитие Q и състояние ρ имаме следните съвпадащи означения:

$$\langle Q \rangle_\rho = \rho(Q) = \text{Prob}_\rho(Q) . \quad (5.6)$$

5.3 Исторически бележки

Възниква естествен въпрос, защо е било нужно да се въвеждат наблюдаемите. Ако квантовата теория беше открита от математици или информатици вероятно те нямаше да бъдат въведени: събитията и тяхната логическа структура са напълно достатъчни, а и привични за информационните приложения. Само, че квантовата теория е била открита от физиците, които традиционно описват света с помощта на физичните величини. Физична величина е алтернативно име на наблюдаема величина. Нещо повече, физичните закони се изразяват с алгебрични съотношения между наблюдаемите величини. Така стигаме до двете ключови думи на алгебричния аксиоматичен подход: **алгебра** и **наблюдаеми**. На фигурата по-долу сме дали примери на едни от най-емблематичните физични закони, които разбира се няма да имат никакво отношение към квантовата информатика.



фиг. 36: Някои от най-емблематичните закони на физиката. Ние няма тук да ги поясняваме (като например, че съвпадащите букви, като V и R във втората и третата фигура не са едни и същи величини). Дори няма и да назовем тези закони (читателите вероятно ги помнят още от училище), тъй като не бихме искали някой да остане с впечатлението, че те ще играят някаква роля в настоящия курс. Единствено обръщаме внимание на ролята на аритметичните операции във формулировката на физичните закони.

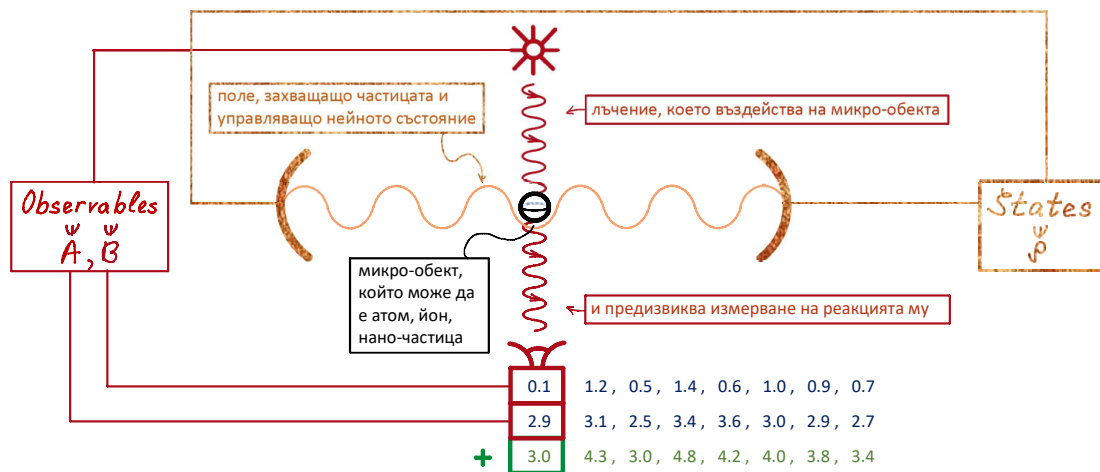
Физичните закони илюстрирани в горната фигура включват само операцията умножение, но разбира се в други закони срещаме не само

останалите аритметични операции, но и по-сложни математически функции. В квантовата теория обаче специална роля е отредена на умножението, което след известни догадки е предложено да стане **некомутативно**. Ние ще видим по-нататък, как некомутативността на умножението се оказва свързана с некомутативността на измерванията в квантовата теория.

5.4 Съвместно измерими наблюдаеми и функции от тях

Както вече сме отбелязвали в квантовата теория срещаме принципно нова релация между събитията: **съвместната измеримост**. Тази релация се пренася и върху наблюдаемите: две наблюдаеми са съвместно измерими, ако спектралните им събития са две по две съвместно измерими. По-просто казано, *две наблюдаеми са съвместно измерими, ако могат да се измерят в общ експеримент*. На този етап ще приемем тази релация на интуитивно ниво, до колкото ще ни е нужно за да мотивираме аксиомите на алгебричния подход.

Важна операция, която може да се извършва със съвместно измеримите наблюдаеми е да образуваме функция от тях. Например, ако A и B са съвместно измерими наблюдаеми, то можем да вземем тяхната сума $A + B$, както е илюстрирано на долната фигура (обобщаваща ситуацията от фиг. 34):



Най-общо, ако $A, B, \dots, C$ са краен брой съвместно измерими наблюдаеми и $F(a, b, \dots, c)$ функция на същия брой променливи, то можем да определим функцията $F(A, B, \dots, C)$ така, че ако

$$\begin{array}{lll} a_1, & a_2, & \dots, \\ b_1, & b_2, & \dots, \\ \vdots & \vdots & \dots \\ c_1, & c_2, & \dots, \end{array} \quad (5.7)$$

$$f_1, \quad f_2, \quad \dots, \quad (5.8)$$
$$f_k := F(a_k, b_k, \dots, c_k), \quad k = 1, 2, \dots. \quad (5.9)$$

В общия случай на функция, както ще видим след малко е изключително важно, че наблюдаемите са съвместно измерими. Преди всичко това е така,

защото ние образуваме редицата (5.8), като синхронно пресмятаме функцията върху отделните стойности в реда в който са дошли от общия експеримент. Ако експеримента не беше общ, то взаимните разположения в редиците (5.7) стават напълно случайни и следователно, ф-ла (5.9) престава да има смисъл на действителна функционална зависимост.

Специалният случай на функция от една наблюдаема не изисква допълнителното изискване на съвместна измеримост: всяка наблюдаема е “съвместна със себе си”. Така например, може да вземем степените на една наблюдаема A : $A^2, A^3, \dots$, както е дадено на долните таблици на редиците от измервания:

$$\begin{aligned} \text{ако за } A \text{ е: } & a_1, \quad a_2, \quad \dots, \\ \text{то за } A^2 \text{ е: } & a_1^2, \quad a_2^2, \quad \dots, \\ & \vdots \quad \vdots \quad \vdots \quad \dots \\ \text{за } A^n \text{ е: } & a_1^n, \quad a_2^n, \quad \dots. \end{aligned} \quad (5.10)$$

И така, виждаме че множеството на наблюдаемите има доста богата “семантична” структура. Ние обаче няма да аксиоматизираме горната обща схема на съвместно измерими наблюдаеми и образуване на функции от тях. Ние ще аксиоматизираме доста по-малка част от горните понятия, но това ще се окаже достатъчно да получим интерпретация и на останалите.

5.5 Статистическа сума на произволни (дори и на несъвместими) наблюдаеми

Един от основните проблеми при аксиоматизацията на понятието за функция на съвместно измерими наблюдаеми е, че операцията на вземане на функция трудно се свързва със състоянията. Ние вече поискахме едно състояние ρ да се определя, като функция от наблюдаемите, която съпоставя на всяка наблюдаема A нейната средна стойност $\langle A \rangle_\rho$. Да вземем например n -тата степен A^n и да видим какво може да кажем за $\langle A^n \rangle_\rho$:

A	a_1	a_2	a_3	a_4	$\cdot \cdot \cdot$	$\langle A \rangle_\rho = \lim_{N \rightarrow \infty} \frac{a_1 + a_2 + \dots + a_N}{N}$
A^n	a_1^n	a_2^n	a_3^n	a_4^n	$\cdot \cdot \cdot$	$\langle A^n \rangle_\rho = \lim_{N \rightarrow \infty} \frac{a_1^n + a_2^n + \dots + a_N^n}{N}$

(5.11)

– всъщност нищо не може да кажем в общия случай, съгласно горната таблица.

Ако вземем обаче по-простите случаи на умножаване по-число или на сума се оказва, че имаме изключителен “късмет”:

A	a_1	a_2	a_3	a_4	$\cdot \cdot \cdot$	$\langle A \rangle_{\mathcal{F}} = \lim_{N \rightarrow \infty} \frac{a_1 + a_2 + \dots + a_N}{N}$
B	b_1	b_2	b_3	b_4	$\cdot \cdot \cdot$	$\langle B \rangle_{\mathcal{F}} = \lim_{N \rightarrow \infty} \frac{b_1 + b_2 + \dots + b_N}{N}$
λA	λa_1	λa_2	λa_3	λa_4	$\cdot \cdot \cdot$	$\langle \lambda A \rangle_{\mathcal{F}} = \lim_{N \rightarrow \infty} \frac{(\lambda a_1) + \dots + (\lambda a_N)}{N} = \lambda \langle A \rangle_{\mathcal{F}}$
$A+B$	a_1+b_1	a_2+b_2	a_3+b_3	a_4+b_4	$\cdot \cdot \cdot$	$\begin{aligned} \langle A+B \rangle_{\mathcal{F}} &= \lim_{N \rightarrow \infty} \frac{(a_1+b_1) + \dots + (a_N+b_N)}{N} \\ &= \lim_{N \rightarrow \infty} \frac{(a_1 + \dots + a_N) + (b_1 + \dots + b_N)}{N} \\ &= \lim_{N \rightarrow \infty} \frac{a_1 + \dots + a_N}{N} + \lim_{N \rightarrow \infty} \frac{b_1 + \dots + b_N}{N} \\ &= \langle A \rangle_{\mathcal{F}} + \langle B \rangle_{\mathcal{F}} \end{aligned}$

(5.12)

В частност, накрая на горната таблица стои добре известния извод от теория на вероятностите на факта, че средната стойност на сума на случайни величини е равна на сумата средните им стойности. Последно се оказва от фундаментално значение, понеже за да пресметнем $\langle A+B \rangle_{\rho}$ не се изисква наблюдаемите A и B да са съвместно измерими. Достатъчно е да измерим средните им стойности $\langle A \rangle_{\rho}$ и $\langle B \rangle_{\rho}$ в отделни експерименти и да ги съберем!

Все пак, за да “узаконим” горната процедура е необходима аксиома. Това е първата съществена аксиома на алгебричния подход:

Аксиома за съществуване на статистическа сума:

За всеки две наблюдаеми A и B съществува (единствена) наблюдаема C , такава че за всяко състояние ρ имаме $\langle C \rangle_{\rho} = \langle A \rangle_{\rho} + \langle B \rangle_{\rho}$. Наблюдаемата C се нарича **статистическа сума** (или просто, **сума**) на наблюдаемите A и B .

Нека добавим към горната аксиома и операцията на умножаване на наблюдаема A по число λ , $A \mapsto \lambda A$, с изискването $\langle \lambda A \rangle_{\rho} = \lambda \langle A \rangle_{\rho}$. Така горната аксиома придобива далеч по-компактната (но и по-скупната) форма:

Аксиома за линейността:

Множеството от наблюдаеми **Observables** е линейно пространство, а състоянията са линейни функционали върху него.

(Напомняме, че линеен функционал върху линейно пространство е линейна функция, чийто стойности са числа.)

До тук ние избягвахме въпроса, какъв вид числа са стойностите на наблюдаемите. В следващите точки на тази лекция ние ще видим, че е естествено да приемем, че стойностите на наблюдаемите са **реални числа**. По такъв начин, множеството на наблюдаемите **Observables** ще стане **реално линейно пространство**.

Както във всяко линейно пространство, така и в **Observables** има нула, която ще означаваме с $\hat{0}$. Това е **нулевата наблюдаема**, която при всяко измерване дава един и същи резултат: числото нула. По-късно ще включим в разглежданията и останалите константни наблюдаеми и по-специално **единичната наблюдаема** $\hat{1}$. Така, ако α е число, то наблюдаемата $\alpha\hat{1}$ дава при всяко измерване един и същи резултат: числото α .

5.6 Проблемът с произведението. Квантово произведение

След големия успех в сумирането на наблюдаемите един бърз поглед показва, че с произведението нещата не стоят толкова просто:

A	a_1	a_2	a_3	a_4	$\cdot \cdot \cdot$	$\langle A \rangle = \lim_{N \rightarrow \infty} \frac{a_1 + a_2 + \dots + a_N}{N} =: \rho(A)$
B	b_1	b_2	b_3	b_4	$\cdot \cdot \cdot$	$\langle B \rangle = \lim_{N \rightarrow \infty} \frac{b_1 + b_2 + \dots + b_N}{N} =: \rho(B)$
$A \cdot B$	$a_1 \cdot b_1$	$a_2 \cdot b_2$	$a_3 \cdot b_3$	$a_4 \cdot b_4$	$\cdot \cdot \cdot$	$\rho(A \cdot B) = \lim_{N \rightarrow \infty} \frac{(a_1 \cdot b_1) + \dots + (a_N \cdot b_N)}{N}$ $\neq \rho(A) \cdot \rho(B)$

(5.13)

Наистина, добре известно е от теория на вероятностите, че в общия случай на средната стойност произведението на случайни величини не може да се изрази чрез отделните им средни стойности.

За щастие важен частен случай на умножение е вдигането на квадрат и то е функция само на една наблюдаема, поради което за него не стои

ограничението на съвместната измеримост. В допълнение на това идва и елементарния трик на “поляризация”, който в случая на числа a и b ни изразява тяхното произведение само чрез вземане на суми (заедно с разлики) и квадрати:

$$ab = \frac{1}{2}((a+b)^2 - a^2 - b^2). \quad (5.14)$$

Въз основа на това нека определим т.нар. **йорданово произведение**⁶² на наблюдаеми A и B :

$$A \bullet B := \frac{1}{2}((A+B)^2 - A^2 - B^2), \quad (5.15)$$

което разчита единствено на операциите на събиране, изваждане и вдигане на квадрат за наблюдаеми.

Йордановото произведение $A \bullet B$ е по определение комутативно, $A \bullet B = B \bullet A$. Едва ли обаче може да очакваме от него да има и останалите хубави свойства на произведението, като например асоциативността:

$$(A \bullet B) \bullet C \stackrel{?}{=} A \bullet (B \bullet C). \quad (5.16)$$

Същевременно обаче ние ще приемем за изпълнено друго основно свойство на произведението – **дистрибутивността** (“разкриването на скоби”):

$$(A_1 + A_2) \bullet (B_1 + B_2) = A_1 \bullet B_1 + A_1 \bullet B_2 + A_2 \bullet B_1 + A_2 \bullet B_2. \quad (5.17)$$

В крайна сметка тогава се налага да се откажем от асоциативността (5.16), тъй като в противен случай попадаме в досегашната класическа теория. Тук обаче идва една от най-силните и в същото време неинтуитивни аксиоми на алгебричния подход:

Аксиома за квантовото произведение:

Съществува дистрибутивно, асоциативно, но евентуално некомутативно произведение на наблюдаеми

$$(A, B) \mapsto A \cdot B \equiv AB, \quad (5.18)$$

$$(AB)C = A(BC), \quad (5.19)$$

⁶²наречено на името на Йордан

$A, B, C \in \mathbf{Observables}$, което възпроизвежда функцията “вдигане на квадрат”:

$$A \cdot A \equiv f(A) \quad \text{за} \quad f(a) = a^2. \quad (5.20)$$

Като пряко следствие получаваме следния израз за йордановото произведение:

$$A \bullet B = \frac{1}{2}(AB + BA), \quad (5.21)$$

понеже $(A + B)^2 - A^2 - B^2 = (A + B)(A + B) - AA - BB = AA + AB + BA + BB - AA - BB = AB + BA$. За асоциативността на йордановото произведение обаче получаваме

$$(A \bullet B) \bullet C - A \bullet (B \bullet C) = \frac{1}{4} [B, [A, C]], \quad (5.22)$$

където $[A, B]$ е знаменития **комутатор**:

$$[A, B] := AB - BA. \quad (5.23)$$

Комутаторът играе фундаментална роля в квантовата механика, но в нашия курс по квантова информатика той всъщност няма да се среща изобщо. Все пак, виждаме, че ако $AC \neq CA$ и $B[A, C] \neq [A, C]B$, то дясната страна на (5.22) е различна от нула, т.е., имаме нарушение на асоциативността на йордановото произведение при отсъствие на комутативност.

В горната аксиома за квантовото произведение пропуснахме една важна подробност. Квантовото произведение на две наблюдаеми не винаги ще е наблюдаема. Ние ще отложим тази дискусия, като преди това ще въведем важни някои математически понятия.

Тази точка ще завършим с няколко допълнителни **коментари**:

(а) Дирак е първия, който забелязва че ако въведем означението

$$\{A, B\} := \frac{1}{i\hbar} [A, B] \quad \Longleftrightarrow \quad [A, B] = i\hbar \{A, B\}, \quad (5.24)$$

където $\hbar$ е т.нар. “редуцирана константа на Планк”, то получаваме наблюдаема, която е квантовия аналог на т.нар. **скобка на Поасон** от класическата механика и която измерва ефекта от въздействието на A върху B при нейното измерване. По тази причина, въведената скобка

във ф-ла (5.24) се нарича още **скобка на Дирак** и тя играе роля в тази част от аксиомите на квантовата теория, които се отнасят до непрекъснатата динамика на квантовите системи, т.е., до **непрекъснатите квантови трансформации**. При нас обаче, в курса по квантова информатика ще разглеждаме само **стъпкови** квантови трансформации, които задават елементарните стъпки в един квантов алгоритъм. Това е точната причина, поради която комутаторите и заедно с това, скобката на Дирак няма да играят роля в настоящия курс.

(б) От горните полагания непосредствено следва, че

$$\underbrace{AB}_{\text{квантово произведение}} = \underbrace{A \bullet B}_{\text{йорданово произведение}} + \underbrace{\frac{i\hbar}{2} \{A, B\}}_{\text{квантова корекция}}. \quad (5.25)$$

Тоест, квантовото произведение е равно на комутативното йорданово произведение плюс квантова корекция, която е имагинерна и клони към нула, когато $\hbar$ е пренебрежима.

(в) Дирак нарича квантовите наблюдаеми q -числа (“ q ” от “quantum”), а класическите наблюдаеми c -числа (“ c ” от “classical” или още от “commuting”). Така, Дирак е първия, който въвежда “ q -терминологията”, към която по-късно се добавя и “ q -бита”.

(г) Между комутатора (5.23) и йордановото произведение (5.21) има известна алгебрична аналогия. Прието е в алгебрата израза $AB + BA$ да се нарича **антикомутатор**.

5.7 Математическото понятие за алгебра

Основната структура, която ще имаме в множеството на наблюдаемите ще бъде на **алгебра**. В тази точка на лекцията ще направим кратък увод в математическата теория на алгебрите, включващ основните понятия и видове алгебри.

5.7.1 Общо определение на алгебра

Нека имаме едно **числово поле** $\mathbb{K}$, т.е., множество от числа, което е затворено спрямо операциите събиране, изваждане, умножение и деление (т.е., тези

операции не ни вадят извън множеството и в частност, $\mathbb{K}$ съдържа нулата и единицата). Най-често $\mathbb{K}$ ще бъде полето на реалните $\mathbb{R}$ или на комплексните числа $\mathbb{C}$. Едно линейно пространство $\mathcal{A}$ над полето $\mathbb{K}$ се нарича **алгебра (над $\mathbb{K}$ или още, $\mathbb{K}$ -алгебра)**, ако е снабдено с бинарна операция, която наричаме умножение (или произведение) и ще бележим с малка точка, която понякога ще пропускаме:

$$(A, B) \mapsto A \cdot B \equiv AB \in \mathcal{A}, \quad A, B \in \mathcal{A} \quad (5.26)$$

$A, B \in \mathcal{A}$. Произведението в алгебра изпълнява свойствата на **хомогенност**,

$$(\lambda A) \cdot B = \lambda A \cdot B = A \cdot (\lambda B), \quad (5.27)$$

$A, B \in \mathcal{A}$, $\lambda \in \mathbb{K}$ и на **дистрибутивност**,

$$(A_1 + A_2) \cdot (B_1 + B_2) = A_1 \cdot B_1 + A_1 \cdot B_2 + A_2 \cdot B_1 + A_2 \cdot B_2, \quad (5.28)$$

$A_1 A_2, B_1, B_2 \in \mathcal{A}$. Двата закона за хомогенност и дистрибутивност заедно са еквивалентни на закона за **билинейност** (или още, “разделна линейност”):

$$(\alpha_1 A_1 + \alpha_2 A_2) \cdot (\beta_1 B_1 + \beta_2 B_2) = \alpha_1 \beta_1 A_1 \cdot B_1 + \alpha_1 \beta_2 A_1 \cdot B_2 + \alpha_2 \beta_1 A_2 \cdot B_1 + \alpha_2 \beta_2 A_2 \cdot B_2, \quad (5.29)$$

$A_1 A_2, B_1, B_2 \in \mathcal{A}$, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{K}$.

Упражнение. Докажете, че във всяка алгебра $A\hat{0} = \hat{0} = \hat{0}A$.⁶³

5.7.2 Видове алгебри

- $\mathbb{R}$ -алгебрите се наричат още **реални алгебри**, а $\mathbb{C}$ -алгебрите се наричат още **комплексни алгебри**.
- Алгебрата $\mathcal{A}$ се нарича **комутативна**, ако

$$A \cdot B = B \cdot A \quad \text{за всеки } A, B \in \mathcal{A}. \quad (5.30)$$

В противен случай алгебрата се нарича **некомутативна**.

⁶³ *Указание:* използвайте хомогенността (5.27); опитайте също и с дистрибутивността (5.28).

- Алгебрата $\mathcal{A}$ се нарича **асоциативна**, ако

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \text{за всеки } A, B, C \in \mathcal{A}. \quad (5.31)$$

- **Алгебра с единица** е такава, в която има специално посочен елемент, наречен **единица** и означаван с $\hat{1}$, за който е в сила, че:

$$A\hat{1} = A = \hat{1}A \quad \text{за всеки } A \in \mathcal{A}. \quad (5.32)$$

- Горните типове алгебри могат да се **комбинират** или още **съчетават**, например:

- асоциативни и комутативни алгебри;
- асоциативни алгебри с единица;
- комутативни и асоциативни алгебри с единица;
- отделно, изброените до тук алгебри могат да бъдат реални или комплексни.

Така, при съчетаване на няколко типа алгебри в един, ние налагаме всички условия от съчетаните типове алгебри.

Някои допълнителни типове алгебри, които играят роля в квантовата теория, но не и в този курс са:

- **Антикомутативните** алгебри, които са специален случай на некомутативни алгебри, където:

$$A \cdot B = -B \cdot A \quad \text{за всеки } A, B \in \mathcal{A}. \quad (5.33)$$

- **Алгебрите на Ли** са антикомутативни алгебри, в които операцията се означава със “скобка”

$$(A, B) \mapsto [A, B] \quad (5.34)$$

и се изпълнява т.нар. **твърждение на Якоби**:

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0. \quad (5.35)$$

В частност, алгебрите на Ли не са асоциативни. В квантовата теория, а и по-общо във физиката, алгебрите на Ли са свързани с инфинитезималните

преобразувания на симетрия. Тъй като обаче квантовите трансформации, които ще използваме в квантовата информатика не са непрекъснати, а са дискретни (стъпкови), то алгебрите на Ли няма да играят роля в курса ни.

- **Степенно–асоциативна алгебра** е такава алгебра, в която асоциативния закон (5.31) се изпълнява за всеки три **степен**и на един елемент $A := X^j$, $B := X^k$, $C := X^\ell$, където степените се дефинират рекурсивно по формулата $X^{n+1} := X \cdot X^n$ ($X^1 := X$).
- **Йорданова алгебра** (или още, алгебра на Йордан) е комутативна и степенно–асоциативна алгебра. Алгебрите на Йордан са свързани с аксималното обобщение на алгебричния подход, което ще коментираме допълнително. Тук ще споменем, че те изхождат от възможно най-първични конструкции, които имат непосредствена експериментална интерпретация, която дадохме по-горе. Същевременно обаче, йордановите алгебри са значително по-трудни за теоретична работа, а от друга страна са по същество дават по същество еквивалентен подход. Ето защо ние няма да работим с тях и ги споменаваме единствено за пълнота.

5.8 Спрежение

Следващата математическа операция, която ще ние нужна е спрежението в алгебри. Защо ни е необходимо спрежение? Квантовото произведение, макар и да е асоциативно, в общия случай е некомутиративно. Оказва се тогава, че ако A и B са наблюдаеми, то AB вече не наблюдаема. Така, асоциативната алгебра $\mathcal{A}$, в която се умножават наблюдаемите е по-широко множество от множеството **Observables**:

$$\mathcal{A} \supsetneq \text{Observables}$$

и нас ни се налага да отделим подмножеството на наблюдаемите в $\mathcal{A}$. За тази цел, ние въвеждаме нова аксиома, че в $\mathcal{A}$ има допълнителна операция, **спрежение**:

$$\mathcal{A} \ni A \mapsto A^* \in \mathcal{A}, \quad (5.36)$$

която е такава, че има свойствата:

- **ИНВОЛЮТИВНОСТ:**

$$A^{**} = A \quad \text{за всяко } A \in \mathcal{A}. \quad (5.37)$$

- **Обръща произведението:**

$$(AB)^* = A^*B^* \text{ за всеки } A, B \in \mathcal{A}. \quad (5.38)$$

- **Антилинейност:**

$$(\alpha A + \beta B)^* = \bar{\alpha}A^* + \bar{\beta}B^* \quad (5.39)$$

за всеки $A, B \in \mathcal{A}$ и $\alpha, \beta \in \mathbb{C}$.

- **Аксиома за наблюдаемите:**

$$A \in \mathbf{Observables} \Leftrightarrow A = A^*. \quad (5.40)$$

Елементите, за които $A = A^*$ се наричат **самоспрегнати**, така че с думи горната аксиома се изказва така: A е наблюдаема тогава и само тогава, когато е самоспрегнат елемент на алгебрата на наблюдаемите.

По такъв начин имаме следните преки следствия:

(1) Множеството на наблюдаемите **Observables** се оказва винаги *реално линейно пространство*, в следствие на (5.39).

(2) Също така, за две наблюдаеми $A, B \in \mathbf{Observables}$, то $(AB)^* = B^*A^* = BA$ и отгук:

– йордановото произведение (5.21) на две наблюдаеми е винаги наблюдаема, понеже

$$(A \bullet B)^* = \frac{1}{2}((AB)^* + (BA)^*) = A \bullet B; \quad (5.41)$$

– комутатора на наблюдаеми няма да е самоспрегнат в общия случай:

$$[A, B]^* = ((AB)^* - (BA)^*) = -[A, B], \quad (5.42)$$

но ако го умножим по имажинерната единица ще стане. Поради това, скобката на Дирак (5.24) на две наблюдаеми е отново наблюдаема.

– Произведенето на наблюдаеми било наблюдаема, ако те комутират:

$$AB \text{ е наблюдаема} \Leftrightarrow AB = BA \quad (A \text{ и } B \text{ комутират}). \quad (5.43)$$

Както ще видим в последствие, последното е равносилно на това, че двете наблюдаеми A и B са съвместни (т.е., могат да бъдат измерени съвместно).

5.9 *-Алгебри

Така стигнахме до ново математическо понятие, което съчетава понятията за алгебра и за спрежение: това е понятието за ***-алгебри**, наричани още **инволютивни алгебри**.

По определение, *-алгебра $\mathcal{A}$ е асоциативна алгебра над реалните или комплексните числа ($\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$, съответно), която е допълнително снабдена с едноместна операция (5.36), изпълняваща законите за инволютивност (5.37), обръщане на произведението (5.38) и антилинейност (5.39). В частност, ако алгебрата е реална, то в (5.39) нямаме спрягане на числата.

Това е понятието за *-алгебра. Към него ние ще добавим едно допълнително техническо предположение, което ще наричаме свойство на **положителност на алгебрата**, което понякога се нарича също **формална реалност** или още **евклидовост**:

$$A_1^* A_1 + \dots + A_m^* A_m = \widehat{0} \implies A_1 = \dots = A_m = \widehat{0} \quad (5.44)$$

за всеки $A_1, \dots, A_m \in \mathcal{A}$.

Упражнение. Докажете, че във всяка *-алгебра $\mathcal{A}$: $\widehat{0}^* = \widehat{0}$. Ако $\mathcal{A}$ е *-алгебра с единица, то $\widehat{1}^* = \widehat{1}$.⁶⁴

5.10 Аксиоми на алгебричния подход

Ние вече приведохме заедно с основната мотивация на алгебричния подход и главните аксиоми. В тази точка ние ще дадем за пълнота цялостната аксиоматична схема на алгебричния подход за статистиката на общи квантови системи.

⁶⁴ *Указание:* спрегнете равенствата $A^* + \widehat{0} = A^*$ и $\widehat{1}^* \widehat{1} = \widehat{1}^*$.

Аксиоми на алгебричния подход за общи статистически системи

(a1) Съществува *комплексна асоциативна $*$ -алгебра $\mathcal{A}$ с единица*, която е *положителна* и се нарича **алгебра на наблюдаемите**. Самите наблюдаеми на квантовата система $A \in \mathbf{Observables}$ са тези и само тези елементи $A \in \mathcal{A}$, които са *самоспрегнати* $A = A^*$. Така, макар и $\mathcal{A}$ да се нарича “алгебра на наблюдаемите”, то не всичките ѝ елементи отговарят на наблюдаеми.

(a2) Втората аксиома е подобна на аксиомата за крайност на квантово-логическия подход и затова е специфична за квантовата информатика, като за по-общи квантови системи тя се пропуска. Приемаме, че алгебрата на наблюдаемите е *крайно-мерно* линейно пространство. (Такива алгебри се наричат **крайно-мерни**.)

(a3) Третата аксиома се отнася до структурата на множеството на състоянията. Състоянията $\rho \in \mathbf{States}$ са тези и само тези линейни функционали $\rho : \mathcal{A} \rightarrow \mathbb{C}$, за които са в сила условията:

(положителност) за всяка наблюдаема $A \in \mathbf{Observables}$:

$$\rho(A^2) \geq 0. \quad (5.45)$$

(нормираност)

$$\rho(\widehat{1}) \geq 1. \quad (5.46)$$

Накратко, *състоянията са линейните, положителни и нормирани функционали на алгебрата на наблюдаемите*. Както вече отбелязвахме, числото $\rho(A)$ за наблюдаема A се интерпретира, като *средна стойност* на наблюдаемата A в състоянието ρ и се бележи също с $\langle A \rangle_\rho$.

5.11 Основен пример на алгебра на наблюдаемите

И така, алгебрата на наблюдаемите $\mathcal{A}$ в алгебричния подход е централния обект определящ теорията. В тази точка ще дадем основния пример за такава алгебра, който е напълно аналогичен на аналогичния пример в квантово-логическия подход.

Нека най-напред напомним, че по допускане $\mathcal{A}$ е комплексна, асоциативна, $*$ -алгебра с единица и нека повторим сумарно, че това включва това, че $\mathcal{A}$ е комплексно линейно пространство, снабдено с бинарна операция на произведение, $\mathcal{A} \times \mathcal{A} \ni (A, B) \mapsto AB \in \mathcal{A}$, едноместна операция на спрежение, $\mathcal{A} \ni A \mapsto A^* \in \mathcal{A}$ и избран елемент $\hat{1} \in \mathcal{A}$, така че са изпълнени следните тъждества (изпълнени за всеки $A, B, C, D \in \mathcal{A}$, $\alpha, \beta, \mu, \nu \in \mathbb{C}$):

$$(\alpha A + \beta B)(\mu C + \nu D) = \alpha\mu AC + \alpha\nu AD + \beta\mu BC + \beta\nu BD, \quad (5.47)$$

$$(AB)C = A(BC), \quad (5.48)$$

$$(\alpha A + \beta B)^* = \bar{\alpha}A^* + \bar{\beta}B^*, \quad (5.49)$$

$$A^{**} = A, \quad (5.50)$$

$$(AB)^* = B^*A^*, \quad (5.51)$$

$$\hat{1}A = A = A\hat{1}. \quad (5.52)$$

Основен пример на такива алгебри са **матричните алгебри**:

$$Mat_n(\mathbb{C}) := \text{множеството на всички } n \times n \text{ матрици с комплексни коефициенти.} \quad (5.53)$$

Това е едно n^2 -мерно комплексно линейно пространство. Асоциативното умножение в $Mat_n(\mathbb{C})$ е матричното умножение, което е изобразено на долната фигура:

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jk} & \cdots & a_{jn} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1k} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{j1} & \cdots & b_{jk} & \cdots & b_{jn} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nk} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1k} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{j1} & \cdots & c_{jk} & \cdots & c_{jn} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nk} & \cdots & c_{nn} \end{pmatrix}$$

фиг. 38: Умножение на матрици:

$$\text{ако } A = (a_{j,k})_{j,k=1}^n, \quad B = (b_{j,k})_{j,k=1}^n, \quad C = AB = (c_{j,k})_{j,k=1}^n, \quad \text{то } c_{j,k} = \sum_{\ell=1}^n a_{j,\ell} b_{\ell,k}.$$

Алгебрата $Mat_n(\mathbb{C})$ има единица: единичната матрица,

$$\hat{1} := \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}. \quad (5.54)$$

(Нулата в $Mat_n(\mathbb{C})$ пък е нулевата матрица.) $Mat_n(\mathbb{C})$ се превръща в $*$ -алгебра посредством операцията на **ермитово спрягне**,⁶⁵ което е дефинирано на долната фигура:

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{a_{j1}} & \cdots & \overline{a_{jk}} & \cdots & \overline{a_{jn}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{pmatrix} = A \longmapsto A^* := \begin{pmatrix} \overline{a_{11}} & \cdots & \overline{a_{k1}} & \cdots & \overline{a_{n1}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{1j} & \cdots & a_{kj} & \cdots & a_{nj} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{a_{1n}} & \cdots & \overline{a_{kn}} & \cdots & \overline{a_{nn}} \end{pmatrix} = \overline{(A^T)} = (\overline{A})^T$$

фиг. 39: Ермитово спрягне.

За проверка, нека например да вземем (5.51):

$$(AB)^* = (\overline{AB})^T = (\overline{AB})^T = \overline{B}^T \overline{A}^T = B^* A^*. \quad (5.55)$$

Останалите свойства от (5.48)–(5.52) се изучават в базисните курсове по линейна алгебра или се проверяват съвсем непосредствено (което силно препоръчваме на читателите, които не са ги срещали до сега).

Матричната $*$ -алгебра $Mat_n(\mathbb{C})$ има също така свойството на *положителност* (5.44). За да докажем това, нека първо разгледаме случая с $m = 1$ и да пресметнем:

$$A^* A = \begin{pmatrix} \overline{a_{11}} & \cdots & \overline{a_{k1}} & \cdots & \overline{a_{n1}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{a_{1j}} & \cdots & \overline{a_{kj}} & \cdots & \overline{a_{nj}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{a_{1n}} & \cdots & \overline{a_{kn}} & \cdots & \overline{a_{nn}} \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jj} & \cdots & a_{jn} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} := X := \begin{pmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{j1} & \cdots & x_{jj} & \cdots & x_{jn} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nj} & \cdots & x_{nn} \end{pmatrix}$$

Резултата за x_{jj} е неотрицателно число:

$$x_{jj} = |a_{1j}|^2 + \cdots + |a_{nj}|^2 \geq 0, \quad (5.56)$$

⁶⁵Hermitian conjugation

което би могло да е равно на нула само ако всички събираеми модули са равни на нула, т.е., само ако $a_{k,j} = 0$ за всяко $k = 1, \dots, n$, а също и j е произволно. Така, $X = \widehat{0}$ само, ако и $A = \widehat{0}$. Ако $m > 1$ то за диагоналните матрични елементи на сумата в (5.44) получаваме, както и в (5.56) сума от модули на матричните елементи на матриците $A_1, \dots, A_m$ и така аналогично доказваме и общия случай на (5.44).

Квантовите системи, които се определят от тази алгебра на наблюдаемите ще наричаме **чисто квантови** или също **неприводими квантови системи**.