

Уводна лекция

1	Предварителни бележки	1
2	Преглед на областта	3
3	Исторически бележки	39

1 Предварителни бележки

Квантовата информатика най-общо изучава възможностите за прилагане на законите на квантовата теория за целите на обработка и пренос на информация. Квантовата теория е едно от най-големите предизвикателства към човешкия ум възниквало досега. Тя е предизвикала множество философски дискусии и в същината си е останала неразбираема и до днес. Основният проблем е, че квантовата теория не описва физическата реалност сама по себе си, а единствено в нейното отношение спрямо наблюдателя. Счита се, че всяко наблюдение (или измерване) е свързано с неотстранимо въздействие върху наблюдавания обект и това въздействие има долен, ненулев праг, който се нарича квант или още, елементарна порция на действието. От тук идва и име-

то на цялата теория - "квантова". Обръщаме внимание, че и в до-квантовата физика, която също се нарича класическа физика, също е в сила принципа, че всяко наблюдение е свързано с неотстранимото въздействие върху наблюдавания обект, но за разлика от квантовия случай, в класическата теория ние считаме, че можем неограничено да намаляваме това въздействие към нулата, т.е., няма долен, ненулев праг.

Нека уточним, че "квантовата теория" преди всичко е "квантовата физика" и още по-точно "квантовата механика". За да не плашим обаче читателите, които нямат специални познания по физика в тези лекции сме предпочели "итер-дисциплинарния" израз "квантова теория". Това обаче не е продиктувано от някакво желание за "дистанциране" от физиката (авторът на лекционните записки е физик и в никакъв случай не желае да се дистанцира от физиката!). В тези лекции ние се опитваме наистина да покажем как идеите на квантовата физика отиват далеч над самата физика: в чисто математически и информационни направления.

2 Преглед на областта

Този увод, който не се предполага, като задължителна част от изложението на лекциите, цели да представи някои от най-впечатляващите страни на квантовия свят, които указват, че квантовите явления дават нови и неподозирани възможности за пренос и обработка на информацията.

Ще представим някои ключови физични експерименти, които са придружени от кратки сведения за използваните в тях физични феномени. По нататък обаче тези физични явления няма да бъдат явно използвани и заедно с това няма нито да се предполагат, нито да се въвеждат никакви понятия и знания от физиката, собствено за излагането на квантовата информатика.

Необходимата начална подготовка включва единствено базисни знания от линейната алгебра (и аналитична геометрия). В изложението се използва и базисната теория на вероятностите, която се отнася до крайни вероятностни разпределения и е обект на изучаване още в училищното образование. За пълнота, тези базисни понятия от теория на вероятнос-

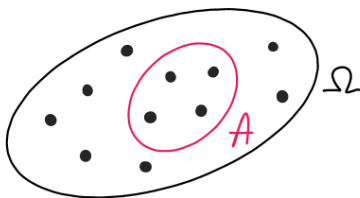
тите ще бъдат преговорени в началните лекции.

Квантови свойства, квантови събития, квантови множества

В класическата физика, т.е. във физиката до XX век, всяка една физична система се характеризира (описва) от едно множество Ω , което се нарича *множество на (елементарните) състояния на системата*. Различните свойства на системата съответстват на подмножества $A \subseteq \Omega$, т.е., свойство = (под)множество са синонимни изрази в този контекст. В теория на вероятностите множеството Ω се нарича също *множество на елементарните събития*, а подмножествата $A \subseteq \Omega$ се наричат *събития*.¹ И така, ние ще използваме като синоними “събитие” = “(под)множество” (= “свойс-

¹Фактически, в случая между “елементарните състояния” и “елементарните събития” има взаимно-однозначно съответствие: първите са елементите на Ω , а вторите са едно-елементните подмножества на Ω . В хода на построението на теорията, ще видим че това взаимно-однозначно съответствие се запазва и в най-общата ситуация на квантови системи.

тво”).



фиг. 1: Множество на елементарните събития Ω и отделяне на свойство “ A ”, като подмножество на Ω

Свойствата могат да се комбинират чрез логическите връзки “и” и “или”, които на езика на подмножествата отговарят на операциите *сечение* $\cap$ и *обединение* $\cup$.

$$A \text{ и } B \iff A \cap B,$$

$$A \text{ или } B \iff A \cup B. \quad (1)$$

Квантов феномен 1: некомутативност на наблюденията

В класическата физика и статистика, ако в едно множество Ω от състояния имаме две събития $A, B \subseteq \Omega$ (т.е. подмножества, свойства) и желаем да отделим сечението им $A \cap B \subseteq \Omega$, ние можем да направим това на две последователни стъпки по два равносилни начина:

- (1) отделяме първо състоянията, които изпълняват свойството A и после в това подмножество A отделяме състоянията изпълняващи B :

$$\Omega \rightsquigarrow A \rightsquigarrow A \text{ и } B.$$

- (2) A можем и в обратния ред

$$\Omega \rightsquigarrow B \rightsquigarrow B \text{ и } A.$$

Нека илюстрираме количествено класическата еквивалентност на двата начина на последователно отделяне на свойства. Ако означим

$$N(\Omega) := \text{брой на елементи на } \Omega$$

$$N(A) := \text{брой на елементи на } A$$

$$N(A \text{ и } B) := \text{брой на елементи на } A \text{ и } B$$

то твърдеството:

$$\underbrace{\frac{N(A \text{ и } B)}{N(\Omega)}}_{\substack{\text{относителен} \\ \text{дял на } A \text{ и } B \\ \text{в } \Omega}} = \underbrace{\frac{N(A)}{N(\Omega)}}_{\substack{\text{относителен} \\ \text{дял на } A \\ \text{в } \Omega}} \cdot \underbrace{\frac{N(A \text{ и } B)}{N(A)}}_{\substack{\text{относителен} \\ \text{дял на } B \\ \text{в } A}}$$

съответства на вероятностния закон:

$$\underbrace{p(A \text{ и } B)}_{\text{вероятност за } A \text{ и } B} = \underbrace{p(A)}_{\text{вероятност за } A} \cdot \underbrace{p(B|A)}_{\substack{\text{условна} \\ \text{вероятност} \\ \text{за } B \text{ при} \\ \text{условие } A}},$$

което на свой ред е всъщност определението на условна вероятност:

$$p(B|A) = \frac{p(A \text{ и } B)}{p(A)} \quad (2)$$

Тогава, равенството

$$N(A \text{ и } B) = N(B \text{ и } A)$$

се изразява във вероятностния закон

$$p(A) \cdot p(B|A) = p(B) \cdot p(A|B),$$

който се нарича *закон на Бейс*.²

В квантовата физика (и статистика) обаче този закон се нарушава. За да се случи това ф-ла (2) трябва да престане да бъде валидна и условната вероятност тогава се въвежда, като първичен обект. Илюстрация на това нарушение дава така неречения:

²Bayes' law / theorem

Експеримент с *кръстосани поляризатори*³

Той се извършва с *фотони* - частици “пренасящи” светлината. Състоянието на един фотон се описва от една наредена тройка

(посока на движение, енергия, вътрешно
състояние)

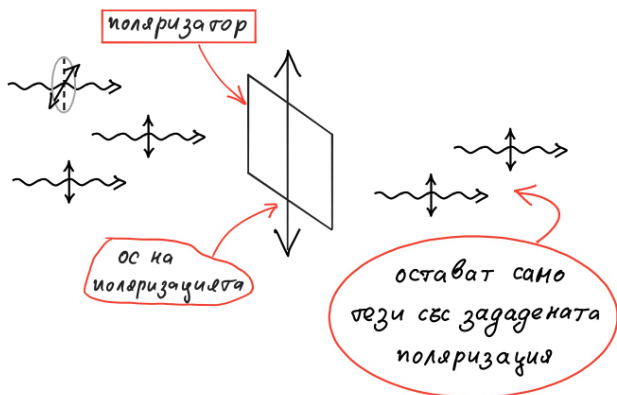
Вътрешното състояние на един фотон отговаря на така наречената *поляризация* на фотона и като квантова система се описва със системата известна като “*квантов бит*”. В описания експеримент се използват само фотони със специален вид вътрешни състояния, наречени *линейни поляризации*. Една *линейна поляризация* се характеризира от ос, която е перпендикулярна на посоката на движение на фотона.

³crossed polarizer



фиг. 2: Линеино поляризираната електромагнитна вълна е класическия “предобраз” на линеино поляризирания фотон.

Така, ако група фотони се движи в една и съща посока, то измежду тях може да се отдели подмножество от фотони, които имат еднаква линейна поляризация. Отделянето на фотони с фиксирана линейна поляризация става посредством филтри, наречени *поляризатори*.



фиг. 3: Селекция на фотони с фиксирана поляризация

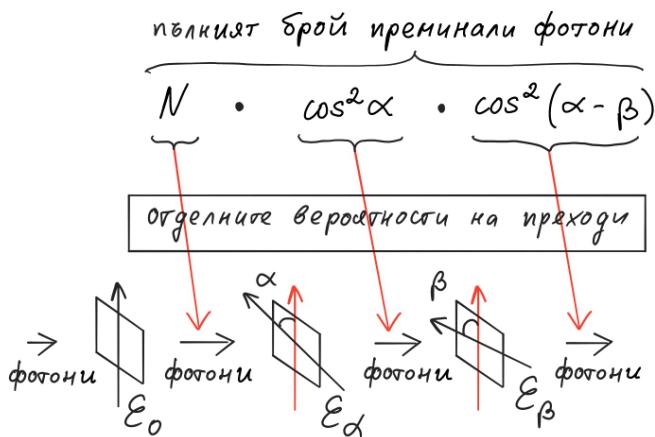
Ако сега след първия поляризатор поставим втори идентичен, то всички фотони преминали през първия ще преминат и през втория. Фотони ще продължават да преминават дори и ако завъртим оста на поляризация на втория поляризатор на ъгъл α спрямо първия. Преминава обаче само част $\cos^2 \alpha$ ($\in [0, 1]$) от фотоните.

резултат от теорията и експеримента



ФИГ. 4: Статистика на преминалите фотони през поляризатор след първоначална селекция

Нека сега допълним опита и с трети поляризатор:



ФИГ. 5: Статистика на преминалите фотони през два последователни поляризатора след първоначалната селекция

Ако сравним резултатите при размяната $\alpha \leftrightarrow \beta$, то ще получим:

$$N \cdot \cos^2 \alpha \cdot \cos^2 (\alpha - \beta) \stackrel{?}{=} N \cdot \cos^2 \beta \cdot \cos^2 (\beta - \alpha).$$

Следователно, възможна е разлика, например при $\alpha = 45^\circ$ и $\beta = 90^\circ$:

$$\underbrace{N("A \text{ и } B")}_{N \cdot \frac{1}{2} \cdot \frac{1}{2}} \neq \underbrace{N("B \text{ и } A")}_{N \cdot 0 \cdot \frac{1}{2}}. \quad (3)$$

В разгледания експеримент, свойството (събитието) A отговаря на поляризация под ъгъл α

$(\mathcal{E}_\alpha)$, а B на поляризация под ъгъл β . В частност виждаме, че поляризацията под ъгъл 0° и 90° отговарят на взаимно изключващи се събития (свойства), но ако между тях стои поляризатор $\mathcal{E}_{45^\circ}$ под ъгъл 45° , то прехода между $\mathcal{E}_{0^\circ}$ и $\mathcal{E}_{90^\circ}$ става възможен! Нека обърнем внимание, че във ф-ла (3) сме поставили в кавички “ A и B ”, понеже броя нито в лявата страна, нито в дясната има смисъл на брой на обектите със свойство A и B . В квантовата логика, която ще споменем след малко, се оказва, че логическите операции остават комутативни (виж. ф-ла (4)) и в горния експеримент събитието A и B се оказва нулевото събитие (т.е., празното или още, невъзможното събитие).

По определение, две квантови събития A и B , за които винаги е изпълнен закона на Бейс (2) се наричат *взаимно комутиращи* или също *съвместно проверяеми* (*съвместно измерими*). По такъв начин, квантовата теория допуска, че има събития които **не могат** съвместно да се проверяват (измерват) – това именно наблюдаваме в представения по-горе квантов феномен 1.

Физическото обяснение на квантовия феномен 1 е, че всяко наблюдение и измерване в природата е активен процес. Това означава, че при всяко наблюдение ние сме принудени да смутим изследваната система. Например, за да видим един обект, ние трябва преди това да го осветим със светлина и да наблюдаваме отразената светлина.



фиг. 6: Наблюдението представено схематично: то винаги е съпроводено със смущение (въздействие) върху наблюдавания обект.

В класическата физика, където наблюдаваме макро-системи, смущенията които внасят нашите наблюдения, са също неизбежни. Там обаче се счита че смущенията винаги могат да се сведат под прага на нашата чувствителност и затова могат да се пренебрегнат. Оказва се обаче, че в квантовата физика, т.е., в микро-света нашите въздействия винаги имат *неотстраним долен (минимален) праг*. Има конкретна физична величина, коя-

то се въвежда в механиката и която отговаря за “въздействието”: тя се нарича “*действие*”.⁴ Минимална порция на действието, която се нарича още *квант на действието* е една от фундаменталните физични константи. Това е така наречената *константа на Планк*⁵ и тя е с изключително малка стойност ($< 10^{-33}$) спрямо стандартната единица за действие в макро-света. Затова и във физиката на макро-света смущенията внасяни при нашите наблюдения винаги могат да се пренебрегнат. По такъв начин, откриването на кванта на действието е довело до квантовата механика и физика, и на него се дължи и името “квантова”.

И така, *съвместно проверяемите събития са тези събития, които не си влияят едно на друго при наблюдения*. Един от най-фундаменталните принципи на квантовата механика, *принципа за неопределеност на Хайзенберг*⁶ гласи най-общо, че има определени двойки физични величини, за които не е възможно точното определяне на стойностите и на двете

⁴action⁵Planck's constant⁶Heisenberg's uncertainty principle

в един общ експеримент. По такъв начин, събитията отговарящи на приемането на определени стойности на такива две величини не могат да се проверят заедно (не са съвместно измерими).

Квантово-логическите операции и тяхната недистрибутивност

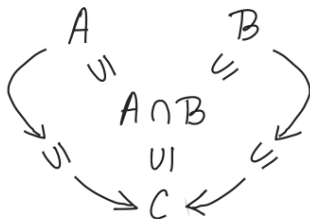
Квантовите свойства, както и класическите свойства се намират в отношение (релация) на *мажориране*: това изразяваме с изрази “свойство A влече свойство B . На езика на множествата:

$$A \subseteq B$$

(A е подмножество /включва се/ в B)

Така, съвкупността на всички събития (свойства) на една квантова система образува *частично наредено множество* – математическа структура, която ще припомним подробно в следващите лекции. Тук ще отбележим само, че във всяко частично наредено множество има конструкция, която може (евентуално) да породи операции подобни на сечение и обединение. Например, сечението, $A \cap B$ на две

събития (свойства) A , B може да се определи, като най-голямото измежду събитията C , които се мажорират както от A , така и от B (когато съществува).



фиг. 7: Сечение в частично наредено множество

По такъв начин логическите операции “и” и “или” върху събитията се пораждат от частичната наредба на мажориране в множеството на всички събития, съгласно интерпретацията от ф-ла (1). Както ще видим по-нататък, това се случва и при класическите, и при квантовите системи. Логическите операции при тази конструкция остават винаги комутативни:

$$A \text{ и } B = B \text{ и } A, \quad A \text{ или } B = B \text{ или } A. \quad (4)$$

При квантовите системи обаче условната вероятност не изпълнява закона:

$$p(B|A) = \frac{p(A \text{ и } B)}{p(A)},$$

тъй като в противен случай, както видяхме, няма да се нарушава закона на Бейс.

Тогава защо: $p(B | A) \neq \frac{p(A \text{ и } B)}{p(A)}$?

За да отговорим, нека припомним, че основно свойство на вероятността е нейната *адитивност*

$$p(A \text{ или } B) = p(A) + p(B),$$

ако $A \text{ и } B = \emptyset$ – празното (невъзможното) събитие.

Условните вероятности за класически системи са също адитивни:

$$p((A \text{ или } B) | C) = p(A | C) + p(B | C),$$

ако $A \text{ и } B = \emptyset$. Действително:

$$\begin{aligned} p((A \text{ или } B) | C) &= \frac{p((A \text{ или } B) \text{ и } C)}{p(C)} \\ &= \frac{p((A \text{ и } C) \text{ или } (B \text{ и } C))}{p(C)} \\ &= \frac{p(A \text{ и } C)}{p(C)} + \frac{p(B \text{ и } C)}{p(C)}, \end{aligned}$$

където сме използвали двата логически закона:

- *дистрибутивност:*

$$(A \text{ или } B) \text{ и } C = (A \text{ и } C) \text{ или } (B \text{ и } C) ; \quad (5)$$

- *асоциативност:*

$$(A \text{ и } C) \text{ и } (B \text{ и } C) = \underbrace{(A \text{ и } B)}_{\emptyset} \text{ и } \underbrace{(C \text{ и } C)}_C = \emptyset . \quad (6)$$

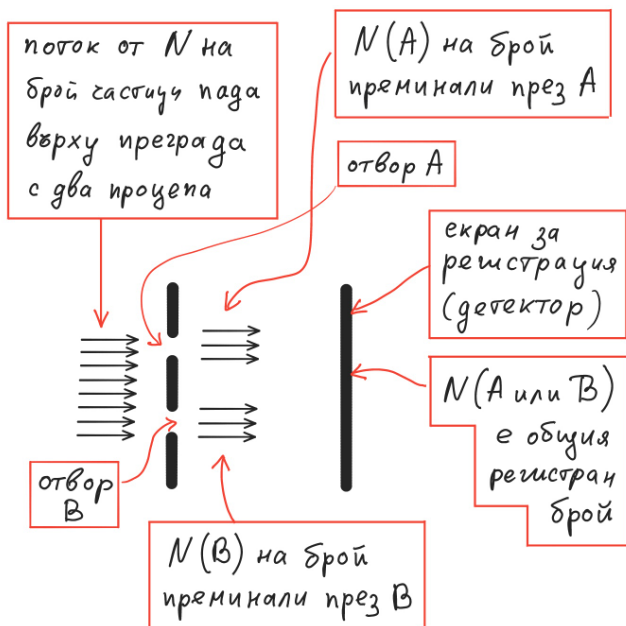
И така, докато закона (6) остава валиден и в квантовата логика, то дистрибутивността (5) престава да е в сила в микро-света. Това се илюстрира от следното експериментално наблюдение.

Квантов феномен 2: интерференция на вероятността. Той се базира на един реален опит, наречен *експеримент с двоен проце*⁷, който ще представим тук в опростена схема. В опита, поток от частици се пропуска през преграда с два процепа и преминалите частици се регистрират върху екран с фотоплака поставен след преградата с процепите. Опитът се провежда в няколко варианта.

– Случай (1): в този случай се изследва

⁷double-slit experiment

общото количество на преминалите частици. На фиг. 8 по-долу е представена схемата.



фиг. 8: Опит с общо преброяване на преминалите частици

Общият брой $N(A \text{ или } B)$ регистрирани частици по целия екран е сума на броевете $N(A)$ и $N(B)$ на частите преминали през отвор A и отвор B , съответно:

$$N(A \text{ или } B) = N(A) + N(B) < N$$

всяка преминала частица се регистрира

но не всяка частица преминава

За да се определят експериментално числата $N(A)$, $N(B)$ и $N(A \text{ или } B)$, поотделно се изследват следните три случая, съответно

(1_A) отворен е само процеп A , при което определяме $N(A)$;

(1_B) отворен е само процеп B , при което определяме $N(B)$;

(1_{A или B}) отворени са A и B , т.е. всяка частица преминава през A или B и следователно, така определяме $N(A \text{ или } B)$.

За да са сравними получените числа $N(A)$, $N(B)$ и $N(A \text{ или } B)$, в трите подслучая погоре е необходимо да осигурим еднакъв начален брой N на частиците падащи върху процесите (или равносилно, еднакви начални потоци на частиците). Изводът от този случай е, че ако поставим достатъчно широк екран (детектор), ние улавяме всички частици, които

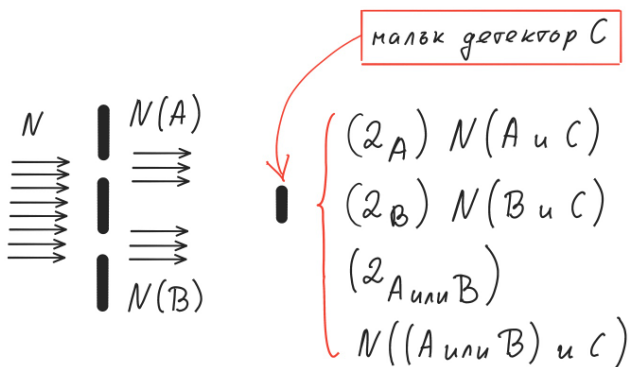
преминават през двата отвора. Така, тук няма никаква разлика с между класическата и квантовата теория.

– Случай (2): зад процепите е поставен малък екран (детектор) C и тогава ние регистрираме само малка част от преминалите частици – тези, които попадат в C . Отново проследяваме 3 под случая:

(2_A) отворен е само процеп A . Тогава в C се регистрират $N(A \text{ и } C)$ на брой частици.

(2_B) отворен е само процеп B . Тогава в C се регистрират $N(B \text{ и } C)$ на брой частици.

($2_{A \text{ или } B}$) отворени са A и B . Тогава в C се регистрират $N((A \text{ или } B) \text{ и } C)$ на брой частици.



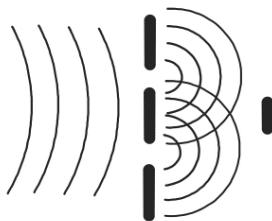
фиг. 9: Опит с локално преброяване на преминалите частици

Резултатът сега е, че:

$$N(A \text{ и } C) + N(B \text{ и } C) \neq N((A \text{ или } B) \text{ и } C). \quad (7)$$

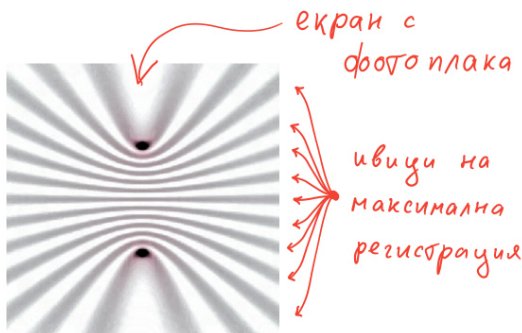
Първи опит за интерпретация: имаме си работа не с частици, а с вълни, и наблюдаваме явлениято *интерференция*.⁸

⁸wave interference



фиг. 10: Общата картина на локалното разпределение на преминалите частици изглежда като картина на интерференция на вълни. Да напомним, че при интерференцията имаме наред с усилващото събиране на вълните също и взаимно погасяване в определени точки.

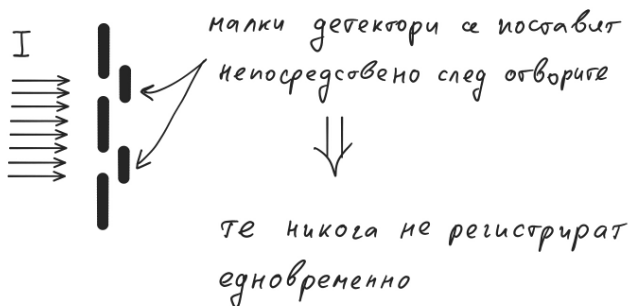
И наистина, при по-детайлен вариант на случай (2), при който се поставя голяма фотоплака (т.е. множество малки детектори), се наблюдава типична интерференчна картина, когато и двата процепа са отворени. Сякаш тогава частиците преминават и през двата процепа едновременно, подобно на вълните и в определени точки става “погасяване” на въздействието им върху екрана.



фиг. 11: Наблюдаваната интерференчна картина върху екрана (фото-плаката)

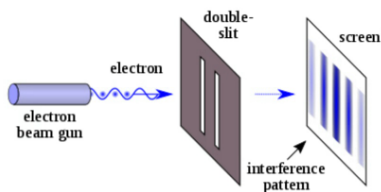
Предложеното обяснение обаче противоречи на следния трети вариант на опита:

– Случай (3): в този случай, посредством малки детектори, които се поставят непосредствено зад процепите ние се убеждаваме, че частиците винаги преминават само през единия процеп. За целта ние пускаме слаб поток от частици, при което те практически се излъчват една по една. В резултат, двата детектора никога не регистрират заедно частица.



фиг. 12: Опит с индивидуална регистрация пред всеки процеп: показва, че всяка частица преминава през точно един от процепите.

Нещо повече, оказва се, че ако повторим по този начин и случай (2), т.е., пускаме частиците една по една, то те ще оставят последователно точкови следи върху фото-плаката, които след достатъчно дълго натрупване ще оформят интерференчна картина. Следователно, оказва се, че вълни са не частиците, а вероятността за тяхната регистрация!



фиг. 13: Опитната постановка в реалистичен вид

И така, констатирахме че (виж. фиг. 14):
една за частица

да премине през A и да попадне в C

или да премине през B и да попадне в C

не е същото, като

да премине без проследяване през A или B

и да попадне в C .



фиг. 14: Нарушение на дистрибутивността

С това констатираме нарушение на дистрибутивността при квантовите събития:

$$\begin{aligned} (A \cap C) \cup (B \cap C) &\neq (A \cap B) \cup C, \\ (A \cup C) \cap (B \cup C) &\neq (A \cup B) \cap C. \end{aligned} \quad (8)$$

спрямо логическите операции произтичащи от логическата им подредба (мажорирането).

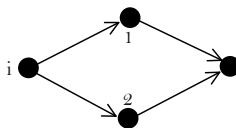
Недистрибутивността също се явява пряко свързана със съвместната неизмеримост на две събития. В крайна сметка, логическата структура на събитията, които се наблюдават (измерват) в общ експеримент трябва да е класическа и в частност, дистрибутивна. Следователно, отклонението от дистрибутивността при някои събития означава и невъзможност за съвместно им наблюдение. В следващите лекции ние специално ще въведем и изучим релацията на съвместност между събитията, а по-късно, при въвеждането на т.нар. *проекционен постулат*⁹ окончателно ще свържем това понятие с понятието за комутируемост между събитията, за което споменахме по-горе.

Амплитуди вместо вероятности на преход

В малко по-абстрактен вариант експериментът по-горе може да се разглежда, като преход на система между две състояния, начално

⁹постулат (postulate) = аксиома

“i” (initial) и крайно “f” (final), през две алтернативни междинни състояния: “1” и “2”. Имаме два канала за преход $i \rightarrow 1 \rightarrow f$ и $i \rightarrow 2 \rightarrow f$:



В класическата статистика, ако вероятностите за преходи $i \rightarrow 1$, $i \rightarrow 2$, $1 \rightarrow f$ и $2 \rightarrow f$ са $p_{i,1}$, $p_{i,2}$, $p_{1,f}$ и $p_{2,f}$, съответно, то прехода $i \rightarrow f$ се извършва с вероятност

$$p_{i,f} = p_{i,1} p_{1,f} + p_{i,2} p_{2,f}. \quad (9)$$

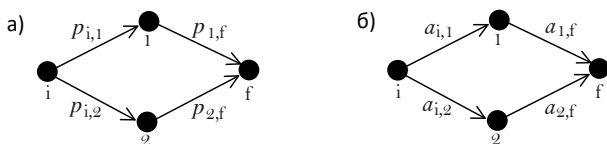
В този случай обаче не се наблюдава “интерференцията” (т.е., погасяването) на вероятността от експеримента по-горе. Оказва се, както ще видим в този курс, че в квантовия случай заедно с вероятностите $p_{i,1}$, $p_{i,2}$, $p_{1,f}$ и $p_{2,f}$ са определени и *комплексни числа* $a_{i,1}$, $a_{i,2}$, $a_{1,f}$ и $a_{2,f}$, наречени *амплитуди на вероятността*, които са свързани с отношенията

$$\begin{aligned} p_{i,1} &= |a_{i,1}|^2, & p_{i,2} &= |a_{i,2}|^2, \\ p_{1,f} &= |a_{1,f}|^2, & p_{2,f} &= |a_{2,f}|^2. \end{aligned} \quad (10)$$

Заедно с това, вероятността за прехода $i \rightarrow f$ се определя от т.нар., *амплитуда на прехода* $a_{i,f}$, която на свой ред се изчислява по формулата

$$a_{i,f} = a_{i,1} a_{1,f} + a_{i,2} a_{2,f}, \quad p_{i,f} = |a_{i,f}|^2. \quad (11)$$

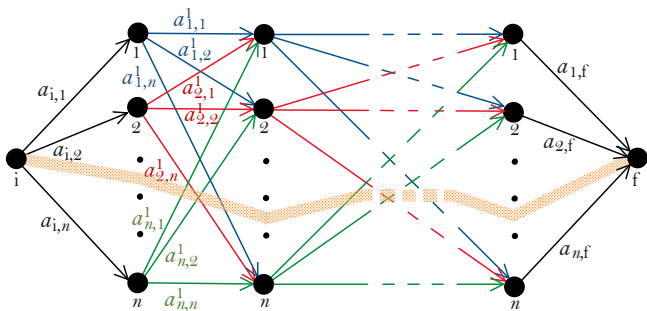
С други думи, класическия вероятностен закон (9) се заменя с квантов аналог при който, грубо казано, вероятностите се “коренуват”, допускайки с това не само обикновената реална нееднозначност ± 1 , но и произволен комплексен множител равен по модул на 1. Схематично това е дадено на фиг. 15.



фиг. 15: Преход между две състояния $i \rightarrow f$ през две алтернативни състояния 1 и 2 - а) класически; и б) квантов

В този курс ние ще видим, че има дълбоки и много общи причини, които водят до замяната на закона (9) с (11).

В по-обща ситуация, прехода $i \rightarrow f$ може се извърши през n алтернативни междинни състояния на k брой стъпки, както е дадено на фиг. 16.



фиг. 16: Преход между състояния $i \rightarrow f$ на няколко стъпки през алтернативни междинни състояния. В определени условия, наречени във физиката “класическа граница” амплитудите на повечето пътища се погасяват взаимно и остава един доминиращ път – оцветения с плътна оранжева линия – това е “класическата траектория” на системата.

Тогава пълната амплитуда на прехода се дава по закона

$$a_{i,f} = \sum_{j_1, \dots, j_k = 1}^n a_{i,j_1} a_{j_1,j_2}^1 \cdots a_{j_k,j_k}^k a_{j_k,f},$$

$$p_{i,f} = |a_{i,f}|^2. \quad (12)$$

Горната формула е довела до подхода на така наречения *интеграл на Файнман по пътищата*,¹⁰ тъй като при прехода към “непрекъснатия” физически свят сумата преминава в “ин-

¹⁰Feynman path integral

теграл”. Формулировката на квантовата механика с файнмановия интеграл по пътищата обаче си остава до днес математически незавършена (всъщност, математически необоснована). За щастие, това не е историческият път по който е построена квантовата теория и тя има солидни математически основи. Въпреки това, формулировката на Файнман си остава до днес един много силен евристичен инструмент. Например, тя дава просто обяснение, защо макро-света не е квантов. Оказва се, че в условия на макро-системи в горната сума (12) всички членове по различните пътища се унищожават взаимно с изключение на един член (или по-точно, на няколко члена близки) на един определен път. Последният е именно и “класическата траектория” на системата.

Квантови изчисления

Този момент от нашия увод ни открива възможността да се доближим до темата за квантовите изчисления. Във втората част на нашия курс ние ще разгледаме систематично тази тема започвайки от нейния класически ас-

пект. Тук ще илюстрираме накратко новите възможностите, които предлага квантовата теория. За целта, нека се върнем на схемата от фиг. 16 и да си представим, че става дума за изчислителна процедура, при която на определен брой стъпки компютър преминава от някакво начално състояние “ i ” към желаното крайно състояние “ f ”. При всяка от междинните стъпки, компютърът се намира в едно измежду няколко алтернативни състояния $1, \dots, n$. В класическите детерминистични алгоритми прехода при всяка стъпка е точно фиксиран – това е програмата, която компютърът следва. Съществуват изчислителни подходи обаче, при които в междинните състояния няма единствено указана следваща стъпка. Това са така наречените *недетерминистични алгоритми*. Ползата при недетерминистичните изчислителни процедури е, че до отговора може да се достигне за по-кратък брой стъпки. За сметка на това обаче са нужни повече проби докато се “налучка” правилния път. Когато този недетерминистичен изчислителен процес се симулира с класическо вероятно “блуждаене по пътища” имаме

единствено събиране на положителни вероятности. Това силно разпростира опитването до всички възможни пътища. В квантовия случай обаче се сумират амплитуди и има интерференция (погасяване) на вероятността. Това дава възможност при сполучливо конструирани междинни преходи квантовия компютър с голяма вероятност да последва “правилния” изчислителен път (този път може да си го мислим, като оранжевата линия на фиг. 16).

Квантова логика и квантови категории

Нека се върнем към недистрибутивността на квантово-логическите операции. Това ни води до едно специално направление, наречено *квантова логика*.¹¹ В него се изследват възможностите за въвеждане на нов вид *сложително смятане* (*propositional calculus*), за чиято *семантика* да служат съвкупностите от квантови събития. В нашия курс ще започнем именно с това направление.

Заедно с новия вид логическа структура на квантовите събития, възниква и нов вид

¹¹quantum logic

категорна структура, която също ще разгледаме в този курс. За целта, ще включим и съвсем кратък увод за понятието *категория*. Въпросът за категорната структура при квантовите системи възниква във темата за *квантови трансформации*. Важен въпрос свързан с тези трансформации е дали те могат да бъдат необратими или по необходимост винаги са обратими. Ще въведем две картини за трансформациите:

- *картина на състоянията* (*картина на Шрьодингер*,¹² при която освен квантови биекции възможни са и квантови инекции.
- *картина на наблюденията* (*картина на Хайзенберг*.¹³ Тази картина в известен смисъл е дулана на предходната и позволява да се въведат освен биекции също и сюрективни квантови трансформации.

¹²Schrödinger's picture

¹³Heisenberg's picture

Неотстраним индетерминизъм на наблюденията върху квантовите системи

Квантовите феномени 1 и 2, които описахме на кратко по-горе, имат едно фундаментално следствие. Както ще покажем още в първите лекции, некомутативността при последователните наблюдения, както и недистрибутивността в логическата структура на квантовите събития, водят до това, че *резултатите от нашите наблюдения винаги носят вероятностен характер*.

За да се убедим в това, ние ще въведем единно аксиоматично описание, както на класическите, така и на квантовите системи. Ще въведем понятие за състояние на система, в което от една страна ще бъде допусната възможност за вероятностен характер на наблюденията, но заедно с това ще бъде заложен и начин, по който можем да “изчистваме” състоянията от недетерминираност (непредсказуемост) на наблюденията. Граничният резултат на това “изчистване” ще бъдат така наречените “*чисти състояния*”, които за класическите системи ще бъдат напълно лишени от неопре-

деленост и случайност, т.е. всяко едно събитие ще се случва с вероятност нула или единица.

При квантовите системи обаче, макар че отново ще има чисти състояния, те няма да бъдат напълно лишени от неопределеност и случайност. По-точно, ще покажем, че за всяка съвкупност $\mathcal{S}$ от взаимно комутиращи събития винаги съществува състояние ρ , в което събитията от $\mathcal{S}$ се случват с вероятност 0 и 1, но заедно с това, за всяко едно от тези “изчистени” състояния ρ винаги може да се намери събитие A , което не комутира с някое от събитията в $\mathcal{S}$ и A се случва в състоянието ρ с вероятност различна от 0 или 1. Това показва, че квантовите системи са винаги статистически.

Квантово сплитане и неговите приложения

*Квантовото сплитане*¹⁴ е феномен, който произтича от постулата (аксиомата) за *съставни* / *многокомпонентни* системи.¹⁵

Такава система е например системата от два класически бита, чието множество на

¹⁴quantum entanglement

¹⁵composite / compound systems

елементарни състояния е

$$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Оказва се, че в квантовия случай съществуват чисти състояния, които съдържат корелации между отделните компоненти на системата (например, между отделните битове) и тези корелации са по-силни дори от най-силните корелации допустими в класически статистически съставни системи. По такъв начин, в една многокомпонентна квантова система, отделните компоненти се оказват взаимно свързани (корелирани) по-силно отколкото при класически системи. Това от своя страна е в основата на много приложения:

- Квантовата криптография използва този феномен за да предложи нови протоколи за защитен пренос на информация, при които защитата е гарантирана от самите принципи на квантовата физика.
- В квантовата теория на информацията се изследва възможността, както за по-висока степен на архивиране на информацията, така и за по-висока ефектив-

ност при пренос на информацията (по-голям капацитет, по-ниски загуби).

- Не на последно място, квантовото сплитане играе важна роля и в споменатите вече квантови изчисления и алгоритми. А именно, сплитането между отделните квантови битове предлага нови възможности за по-ефективни, по-бързи алгоритми.

Тези три приложни аспекта ще бъдат разгледани в курса.

3 Исторически бележки

Квантовата механика и физика възниква в началото на XX век. Тя се оформя в продължение на почти три десетилетия. В началото стои т.нар. “криза на класическата физика” от края на XIX век и откритието на константата на Планк.¹⁶

¹⁶Max Planck



Max Planck (1858 – 1947)

$$h = 6.62607015 \times 10^{-34} \text{ J}\cdot\text{s}$$

фиг. 17: Макс Планк и неговата константа

Без да претендираме за изчерпателност в изброяването учените допринесли в изграждането на теорията тук ще споменем още Вернер Хайзенберг,¹⁷ формулирал т.нар. *свотношения / принцип за неопределеност*.¹⁸ Тези съотношения, освен че въвеждат фундаменталното понятие за отсъствие на съвместна измеримост на някои величини, са довели и до т.нар. *канонични комутационни свотношения*,¹⁹ които на свой ред дават началото на *алгебричния подход* към квантовата механика.

¹⁷Werner Heisenberg

¹⁸uncertainty principle

¹⁹canonical commutation relations



Werner Heisenberg
(1901 – 1976)

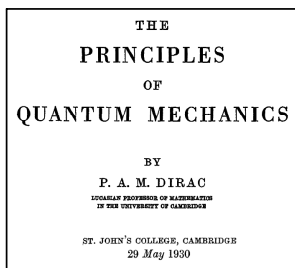


фиг. 18: Хайзенберг и Борн. Надпис от надгробната плоча на Борн с неговите канонични комутационни съотношения

Като един ясен момент, бележещ завършването на теоретичните основи на квантовата механика, може да се посочи издаването на книгата на Дирак²⁰ [?].



Paul Dirac
(1902 - 1984)



фиг. 19: Пол Дирак и първото издание на книгата му по основи на квантовата механика

²⁰Paul Dirac

В книгата на Дирак в завършен вид присъстват няколко от най-фундаменталните теоретични концепции на квантовата механика, като *асоциативната, но некомутативна алгебра на наблюдаемите величини*,²¹ която заменя комутативната алгебра на наблюдаемите в класическата физика. В *алгебрата на наблюдаемите*,²² т.нар. *комутатор*²³ заменя *скобката на Пуасон*²⁴ от класическата механика и затова често се нарича *скобка на Дирак*.

Книгата на Дирак излиза през 1930, а две години по-късно, през 1932 излиза и книгата на Джон фон Нойман²⁵ по математическите основи на квантовата механика [?].²⁶

²¹Дирак нарича елементите на тази некомутативна алгебра “*q-числа*” (*q-numbers*) в отличие от “*c-числата*” (“*c-numbers*”), които са класическите (classical), или още комутиращите (commuting) величини.

²²observable algebra / algebra of observables

²³commutator: в една асоциативна алгебра $[a, b] := ab - ba$ се нарича комутатор на елементите a и b

²⁴Poisson bracket

²⁵John von Neumann

²⁶Може да възникне недоумение за необходимостта от труда на фон Нойман върху математическите основи на квантовата механика, както и за неговото специалното значение. Затова нека си припомним, че и



John von Neumann (1903 – 1957)

фиг. 20: Джон фон Нойман и труда му по математическите основи на квантовата механика

Заедно с това, фон Нойман уточнява и математическите основи на алгебричния подход към квантовата механика. Неговото име днес носи един от основните типове алгебрични структури, които моделират алгебрата на наблюдаемите: *алгебрите на фон Нойман*.²⁷

Още две години след труда на фон Нойман излиза обобщение на алгебричния подход, съчинение номер едно на физиката за всички времена, книгата на Исак Нютон, започва в заглавието си с “математически основи” (Sir Isaac Newton, “Philosophiæ Naturalis Principia Mathematica”, latin edition from 1687 / “Mathematical Principles of Natural Philosophy”, english translation from 1728). Всъщност, може да се каже че физиката се е обособила, като наука, когато е била поставена на математически основи.

²⁷von Neumann algebras

основано на т.нар. *йорданови алгебри*.²⁸

**ON AN ALGEBRAIC GENERALIZATION OF THE QUANTUM
MECHANICAL FORMALISM**

BY P. JORDAN, J. V. NEUMANN, AND E. WIGNER

(Received November 10, 1933)

ANNALS OF MATHEMATICS
Vol. 35, No. 1, January, 1934

фиг. 21: Завършващата статия на алгебричния подход

Това е статията на Йордан,²⁹ фон Нойман и Вигнер,³⁰ от 1934 ([?]).



Pascual Jordan
(1902 – 1980)



Eugene Wigner
(1902 – 1995)



Garrett Birkhoff
(1911 – 1996)

фиг. 22: Йордан, Вигнер и Биркхоф

Продължавайки с този две годишен интервал,
през 1936 излиза и статията на Биркхоф³¹ и

²⁸Jordan algebras

²⁹Pascual Jordan

³⁰Eugene Wigner

³¹Garrett Birkhoff

фон Нойман, в която се формулира и най-общия подход за обосноваване на квантовата механика известен до днес.

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

фиг. 23: Основополагащата статия на квантово-логическия
подход

Това е подхода на *квантовата логика*.

Обръщаме внимание на бързата каскада от трудове фиксиращи основите на квантовата теория: от труда на Дирак през 1930 до Биркхоф – фон Нойман през 1936. Друг факт, който заслужава внимание е особената роля на фон Нойман, който участва във всички от изброените основополагащи работи по математическите принципи на квантовата механика. При това, още през 1936 е забелязан новият тип логическа структура – квантовата логика – която възниква в микро-света. Това е първото указание към бъдещите информационни приложения на квантовата теория. Фон

Нойман е един от учените оставили най-ярка в математиката и физиката, за сравнително краткия си живот. В това число са приносите му в математическата логика и компютърните науки. Фон Нойман взема важно участие и в проекта Манхатън по създаването на атомната бомба.

След смъртта на фон Нойман, в квантовата логика няма много съществен напредък, до възраждането на идеята за информационните приложения на квантовата физика. Една от често споменаваните статии дали силен тласък за идеята за квантови компютри е статията на Файнман³² [?].

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

фиг. 24: Статията на Файнман от 1982 – една от първите, в които се споменава за “квантов компютър”

(???) (???)

³²Richard Feynman

Proc. R. Soc. Lond. A **400**, 97–117 (1985)
Printed in Great Britain

Quantum theory, the Church–Turing principle and
the universal quantum computer

BY D. DEUTSCH

Department of Astrophysics, South Parks Road, Oxford OX1 3RQ, U.K.

(Communicated by R. Penrose, F.R.S. – Received 13 July 1984)

фиг. 25: Статията на Дойч от 1986 – една от първите, в
които се въвежда концепцията за квантови изчисления

(???) (???)