

1 Увод

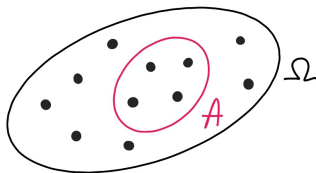
Този увод не е необходима логическа част от изложението на този курс от лекции. По-нататък, ние ще въведем систематично понятията, споменати тук. В това въведение имаме за цел да представи някои от най-впечатляващите аспекти на квантовия свят, които показват, че квантовите явления предоставят нови и неподозирани възможности за предаване и обработка на информация. Ще представим някои ключови физически експерименти, които са придружени от кратки сведения за използваните в тях физически явления. По нататък обаче тези физични явления няма да бъдат явно използвани. Заедно с това няма 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 началната теория на вероятностите, която се отнася до крайни вероятностни разпределения и е предмет на изучаване още в училищното образование.

Квантови свойства, квантови събития, квантови множества

В класическата физика, т.е. във физиката до XX век, всяка физична система се характеризира (описва) с множество, наречено *множество на (елементарните) състояния на системата*. Нека означим с Ω това множество. Различните свойства на системата съответстват на подмножества $A \subseteq \Omega$: всяко свойство определя на подмножеството от състоянията, в които описваната система го притежава и обратно, всяко подмножество от състояния може да се разглежда като определено свойство на системата. Така, свойство = (под)множество и те са синонимни изрази в този контекст.

В контекста на 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” (= “свойство”).



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* $\cup$.

$$\begin{aligned} A \text{ и } B &\longleftrightarrow A \cap B, \\ A \text{ или } B &\longleftrightarrow A \cup B. \end{aligned} \tag{1.1}$$

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 искаме да отделим сечението им $A \cap B \subseteq \Omega$, ние можем да направим това в две последователни стъпки по два равносилни начина:

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

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

- (2) А можем и в обратния ред

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

¹Всъщност, тук имаме взаимно-еднозначно съответствие между “елементарните състояния” и “елементарните събития”: първите са елементите на Ω , а вторите са едно-елементните подмножества на Ω . В хода на изграждането на теорията ще видим, че това едно към едно съответствие се запазва дори в най-общата ситуация на квантовите системи.

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 тъждеството:

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

съответства на вероятностния закон:

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

което от своя страна всъщност е определението за условна вероятност:

$$p(B|A) = \frac{p(A \text{ и } B)}{p(A)} \quad (1.2)$$

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 статистиката) обаче този закон е нарушен. За да се случи това ф-ла (1.2) 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

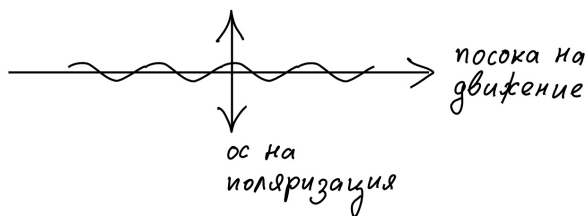
Експеримент с *кръстосани поляризатори*

Той³ 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 фотона съответства на така наречената *поляризация* на фотона.

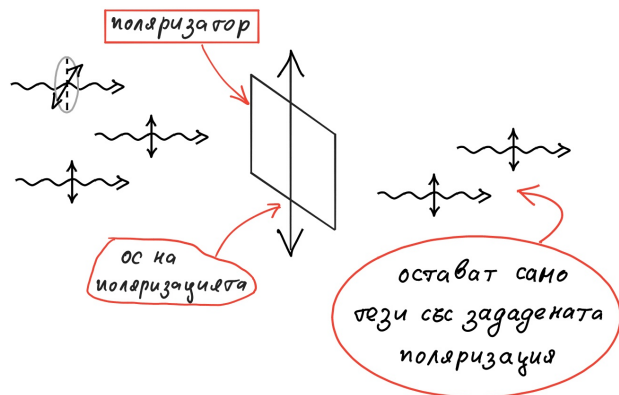
Поляризационните състояния са същите, като състоянията на най-простата квантова система наречена “*квантов бит*”. В описания експеримент се използват само фотони със специален тип вътрешни състояния: те се наричат *линейни поляризации*. Състояние на *линейна поляризация* се характеризира с *ос*, която е перпендикулярна на посоката на движение на фотона.



фиг. 2: Линейно поляризираната електромагнитна вълна е класическия “предобраз” на линейно поляризирания фотон.

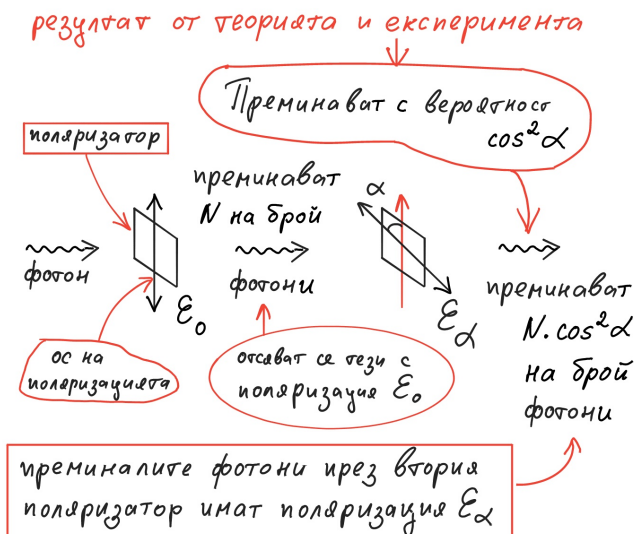
По този начин, ако група фотони се разпространяват в една и съща посока, тогава от тях може да бъде отделено подмножество от фотони, които имат еднаква линейна поляризация. Отделянето на фотони с фиксирана линейна поляризация се извършва чрез филтри, наречени *поляризатори*.

³crossed polarizer experiment



фиг. 3: Селекция на фотони с фиксирана поляризация

Ако сега поставим втори поляризатор след първия, който е идентичен, тогава всички фотони, които са 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. Препминава обаче само част $\cos^2 \alpha$ ($\in [0, 1]$) от фотоните.

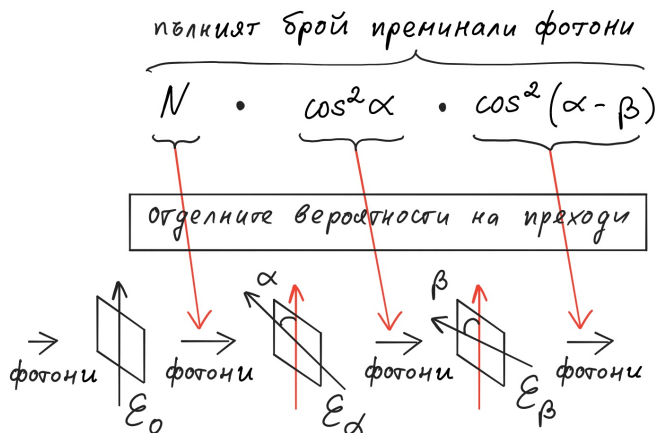


фиг. 4: Статистика на преминалите фотони през поляризатор след първоначална селекция

Важно е да се отбележи, че ние може да пускаме фотоните един по един и в този случай един фотон преминава или напълно не преминава през всеки

поляризатор. Числото $\cos^2 \alpha$ в този случай представлява *вероятността* за преминаване на фотон през втория поляризатор след, като е бил пропуснат от първия.

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

$$\underbrace{N("A \text{ и } B")}_{N \cdot \frac{1}{2} \cdot \frac{1}{2}} \neq \underbrace{N("B \text{ и } A")}_{N \cdot 0 \cdot \frac{1}{2}}. \quad (1.3)$$

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 (1.3) сме поставили в кавички " $A \text{ и } B$ ", понеже броя нито в лявата страна, нито в дясната има смисъл на брой на обектите със свойство $A \text{ и } B$. В квантовата логика, която ще споменем след малко, се оказва, че логическите операции остават комутативни (виж. ф-ла (1.4)) 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 (1.2) 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 смущаваме изследваната система. Например, за да видим обект, първо трябва да го осветим със светлина и след това да наблюдаваме отразената светлина.



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

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*. Има конкретна физична величина, която се въвежда в механиката и която отговаря за “въздействието”: тя се нарича “*действие*”.⁴ Минимална порция на действието, наричана още *квант на действието*, е една от фундаменталните физични константи. Това е така наречената *константа на Планк*⁵ и тя има изключително малка стойност ($< 10^{-33}$) в сравнение със стандартната единица за действие в

⁴action

⁵Planck's constant

макро света. Това е причината, поради която във физиката на макро-света смущенията внасяни при нашите наблюдения винаги могат да бъдат пренебрегнати. Така откриването на кванта на действието е довело до квантовата механика и физика и на нея се дължи 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 да се определят точно стойностите на двете в общ експеримент. По такъв начин, събитията отговарящи на приемането на определени точни стойности на такива две величини не могат да бъдат проверени заедно (не са съвместно измерими).

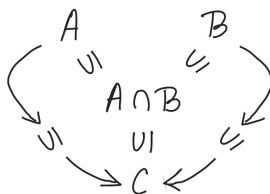
Квантово-логическите операции и тяхната недистрибутивност

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:

$$A \subseteq B \text{ (} A \text{ е подмножество/включва се/ в } B \text{)}.$$

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 (евентуално) може да породи операции подобни на сечение и обединение. Например, сечението, $A \cap B$ на две събития (свойства) A , B може да бъде определено, като най-голямото от събитията C , които се мажорират както от A , така и от B (когато то съществува).

⁶Heisenberg’s uncertainty principle



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, според интерпретацията от ф-ла (1.1). Както ще видим по-нататък, това се случва както в класическите, така и в квантовите системи. Логическите операции при тази конструкция остават винаги комутативни:

$$A \text{ и } B = B \text{ и } A, \quad A \text{ или } B = B \text{ или } A. \quad (1.4)$$

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.

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

За да отговорим, нека си 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 също са 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*:

$$(A \text{ или } B) \text{ и } C = (A \text{ и } C) \text{ или } (B \text{ и } C) ; \quad (1.5)$$

- *асоциативност*:

$$(A \text{ и } C) \text{ и } (B \text{ и } C) = \underbrace{(A \text{ и } B)}_{\emptyset} \text{ и } \underbrace{(C \text{ и } C)}_C = \emptyset. \quad (1.6)$$

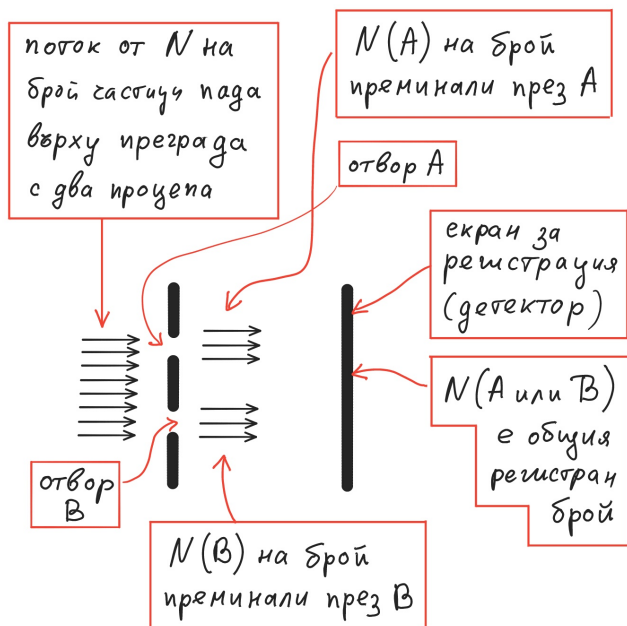
И така, докато закона (1.6) остава валиден и в квантовата логика, то дистрибутивността (1.5) престава да е в сила в микро-света. Това се илюстрира от следното експериментално наблюдение.

Квантов феномен 2: интерференция на вероятността.

Той се основава на един реален опит, наречен *експеримент с двоен проце́п*,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 фото-плака поставен след преградата с процепите. Опитът се провежда в няколко варианта.

– Случай (1): в този случай се изследва общото количество на преминалите частици. На фиг. 8 по-долу е представена схемата.

⁷double-slit experiment



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 частиците преминали през отвор A и отвор B , съответно:

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

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 $N(B)$;

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

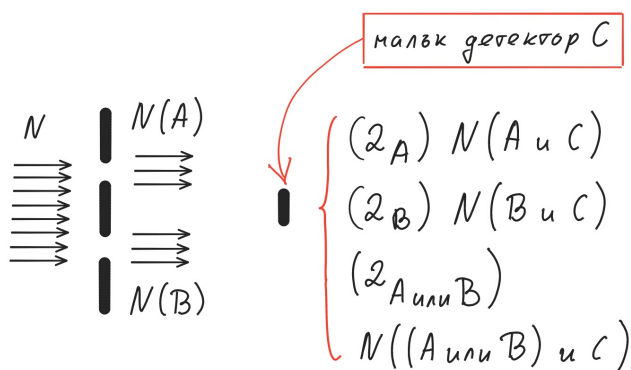
За да са сравними получените числа $N(A)$, $N(B)$ и $N(A \text{ или } B)$, в трите подслучая по-горе е необходимо да осигурим еднакъв начален брой N на частиците падащи върху процепите (или равносилно, еднакви начални потоци на частиците). Изводът от този случай е, че ако поставим достатъчно широк екран (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.

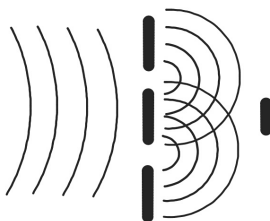


фиг. 9: Опит с локално преброяване на преминалите частици

Резултатът сега е, че:

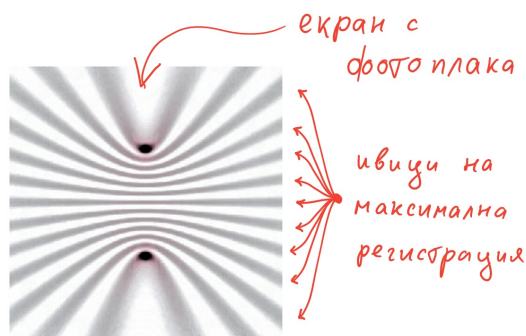
$$N(A \text{ и } C) + N(B \text{ и } C) \neq N((A \text{ или } B) \text{ и } C). \quad (1.7)$$

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



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

И наистина, при по-детайлен вариант на случай (2), при който се поставя голяма фото-плака (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.



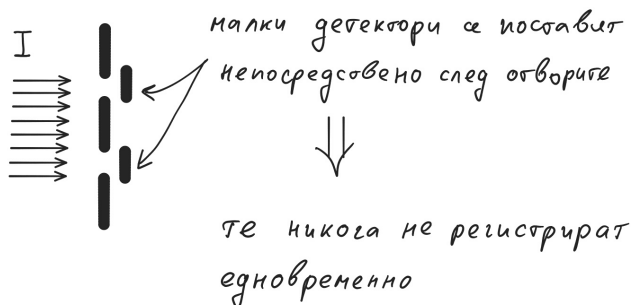
фиг. 11: Наблюдаваната интерференчна картина върху екрана (фото-плаката)

Предложеното обяснение обаче противоречи на следния трети вариант на опита:

– Случай (3): в този случай, посредством малки детектори, които се поставят

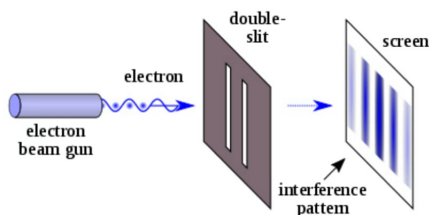
⁸wave interference

непосредствено зад процеците 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: той показва, че всяка частица преминава през точно един от процеците.

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): за една 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:

$$\begin{aligned} (A \cap C) \cup (B \cap C) &\neq (A \cap B) \cup C, \\ (A \cup C) \cap (B \cup C) &\neq (A \cup B) \cap C. \end{aligned} \quad (1.8)$$

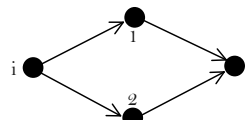
спрямо логическите операции произтичащи от логическата им подредба (мажорирането).

Недистрибутивността също е пряко свързана със съвместната неизмеримост на две събития. В крайна сметка, логическата структура на събитията, които се наблюдават (измерват) в общ експеримент, трябва да бъде класическа и в частност, дистрибутивна. Следователно, отклонението от дистрибутивността при някои събития означава и невъзможност за съвместно им наблюдение. По-нататък ние специално ще въведем и изучим релацията на съвместност между събитията, а след това, 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

В малко по-абстрактен вариант експериментът по-горе може да се разглежда, като преход на система между две състояния, начално “i” (initial) и крайно “f” (final), през две алтернативни междинни състояния: “1” и “2”. Имаме два

⁹постулат (postulate) = аксиома

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

$$p_{i,f} = p_{i,1} p_{1,f} + p_{i,2} p_{2,f}. \quad (1.9)$$

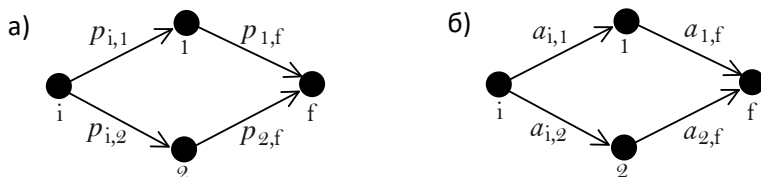
В този случай обаче не се наблюдава “интерференцията” (т.е., погасяването) на вероятността от експеримента по-горе. Оказва се, както ще видим в този курс, че в квантовия случай заедно с вероятностите $p_{i,1}$, $p_{i,2}$, $p_{1,f}$ и $p_{2,f}$ са определени и *комплексни числа* $a_{i,1}$, $a_{i,2}$,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

$$p_{i,1} = |a_{i,1}|^2, \quad p_{i,2} = |a_{i,2}|^2, \quad p_{1,f} = |a_{1,f}|^2, \quad p_{2,f} = |a_{2,f}|^2. \quad (1.10)$$

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

$$a_{i,f} = a_{i,1} a_{1,f} + a_{i,2} a_{2,f}, \quad p_{i,f} = |a_{i,f}|^2. \quad (1.11)$$

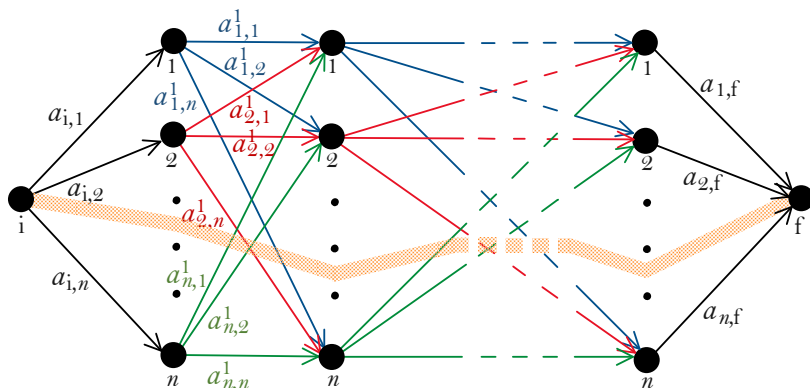
С други думи, класическия вероятностен закон (1.9) се заменя с квантов аналог при който, грубо казано, вероятностите се “коренуват”, допускайки с това не само обикновената реална нееднозначност ± 1 , но и произволен комплексен множител равен по модул на 1. Схематично това е дадено на фиг. 15.



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 (1.9) с (1.11).

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

$$a_{i,f} = \sum_{j_1, \dots, j_k=1}^n a_{i,j_1} a_{j_1,j_2}^1 \cdots a_{j_k,j_k}^k a_{j_k,f}, \quad p_{i,f} = |a_{i,f}|^2. \quad (1.12)$$

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 “интеграл”. 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 (1.12) всички членове по различните пътища се унищожават взаимно с изключение на един член (или

¹⁰Feynman path integral

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. Накрая на нашия курс ние систематично ще разгледаме тази тема, започвайки от нейния класически аспект. Тук ще илюстрираме накратко новите възможности, предлагани от квантовата теория. За целта, нека се върнем на схемата от фиг. 16 и да си представим, че става дума за изчислителна процедура, при която компютър преминава от някакво начално състояние “i” към желаното крайно състояние “f” на определен брой стъпки. При всяка от междинните стъпки, компютърът се намира в едно от няколко алтернативни състояния $1, \dots, n$. В класическите детерминистични алгоритми прехода при всяка стъпка е точно фиксиран – това е програмата, която компютърът следва. Има обаче изчислителни подходи, при които в междинните състояния не е посочена единствена следваща стъпка (преход). 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 квантовия компютър с голяма вероятност да последва “правилния” изчислителен път при сполучливо конструирани междинни преходи (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 *съждително смятане* (*propositional calculus*), за чиято *семантика* да служи съвкупността от всички квантови събития на една квантова система. В нашия курс ще започнем именно с това направление.

Заедно с новия вид логическа структура на квантовите събития, възниква и нов вид 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 са непременно са винаги 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 дуална на предходната и позволява да се въведат освен биекции също и сюрективни квантови трансформации.

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 *результатите от нашите наблюдения имат винаги вероятностен характер*.

¹¹quantum logic

¹²Schrödinger's picture

¹³Heisenberg's picture

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, при което от една страна ще се допуска възможност за вероятностен характер на наблюденията, но заедно с това ще бъде зададен и начин, по който можем да “изчистваме” състоянията от недетерминираност (непредсказуемост) на наблюденията. Крайният резултат от това “изчистване” ще бъдат така наречените “*чисти състояния*”, които за класическите системи ще бъдат напълно лишени от неопределеност и случайност, т.е. всяко едно събитие ще се случва с вероятност нула или единица.

Въпреки това, при квантовите системи, 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 или 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 и 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 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 разрешени в класически статистически съставни системи. По такъв начин, в една многокомпонентна квантова система, отделните

¹⁴quantum entanglement

¹⁵composite / compound systems

компоненти се оказват взаимно свързани (корелирани) по-силно отколкото в класически системи. Това от своя страна е в основата на много приложения:

- *Квантовата криптография* използва този феномен за да предложи нови протоколи за защитено пренасяне 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 ефективност 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.