

КВАНТОВА ИНФОРМАТИКА

Николай М. Николов

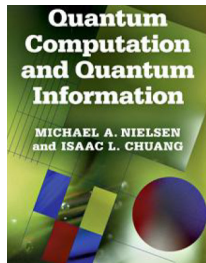
Лекция 2 / 16.10.2023, версия 1

ЧАСТ 1: АКСИОМАТИЧНИ ОСНОВИ НА КВАНТОВАТА ТЕОРИЯ

аксиоматични аксиома- тични раздели	аксиоматични подходи	квантово-логически аксиоматичен подход	алгебричен аксиоматичен подход
аксиоми на общи системи		лекции ²⁻³ <u>2-4</u>	лекции ³⁻⁵ <u>5-7</u>
аксиоми на съставни системи		_____	лекция ⁶ <u>8</u>
квантови трансформации		_____	лекция ⁷ <u>9</u>

ЧАСТ 1: АКСИОМАТИЧНИ ОСНОВИ НА КВАНТОВАТА ТЕОРИЯ

Алтернативен източник: http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/NC2010.pdf



x	Contents	
2	Introduction to quantum mechanics	60
2.1	Linear algebra	61
2.1.1	Bases and linear independence	62
2.1.2	Linear operators and matrices	63
2.1.3	The Pauli matrices	65
2.1.4	Inner products	65
2.1.5	Eigenvectors and eigenvalues	68
2.1.6	Adjoint and Hermitian operators	69
2.1.7	Tensor products	71
2.1.8	Operator functions	75
2.1.9	The commutator and anti-commutator	76
2.1.10	The polar and singular value decompositions	78
2.2	The postulates of quantum mechanics	80
2.2.1	State space	80
2.2.2	Evolution	81
2.2.3	Quantum measurement	84
2.2.4	Distinguishing quantum states	86
2.2.5	Projective measurements	87
2.2.6	POVM measurements	90
2.2.7	Phase	93
2.2.8	Composite systems	93
2.2.9	Quantum mechanics: a global view	96
2.3	Application: superdense coding	97
2.4	The density operator	98
2.4.1	Ensembles of quantum states	99
2.4.2	General properties of the density operator	101
2.4.3	The reduced density operator	105
2.5	The Schmidt decomposition and purifications	109
2.6	EPR and the Bell inequality	111
3	Introduction to computer science	120
3.1	Models for computation	122
3.1.1	Turing machines	122
3.1.2	Circuits	129
3.2	The analysis of computational problems	135
3.2.1	How to quantify computational resources	136
3.2.2	Computational complexity	138
3.2.3	Decision problems and the complexity classes P and NP	141
3.2.4	A plethora of complexity classes	150
3.2.5	Energy and computation	153
3.3	Perspectives on computer science	161
Part II	Quantum computation	171
4	Quantum circuits	171
4.1	Quantum algorithms	172
4.2	Single qubit operations	174

Quantum Computation and Quantum Information
(10th Anniversary Edition)
by *Michael A. Nielsen* and
Isaac L. Chuang

Chapt. 2
Introduction to quantum
mechanics
(стр. 60 – 119)

ЧАСТ 1: АКСИОМАТИЧНИ ОСНОВИ НА КВАНТОВАТА ТЕОРИЯ

За по-добра ориентация в изложението ще отличаваме следните два типа части:

- Илюстративни и мотивационни части.

Те няма да имат доказателствена или логическа роля при построяването на теорията, аналогично както и чертежите в геометрията нямат доказателствена стойност. Тези части ще мотивират въвежданите понятия и ще ги илюстрират как биха изглеждали в практиката.

- Формални части.

Те ще съдържат определения, аксиомите, теоремите и доказателствата в теорията, както и всички пресмятания и построения.

ЧАСТ 1: АКСИОМАТИЧНИ ОСНОВИ НА КВАНТОВАТА ТЕОРИЯ

За аксиоматичният подход:

Един от шедеврите на аксиоматичните подходи, на който ще подражаваме е книгата на Давид Хилберт “Основи на геометрията”. Тя започва така:



Мислим три различни системи от неща. Нещата от първата система наричаме *точки*; нещата от втората система наричаме *прави* и ги означаваме с $A, B, C, \dots$; нещата от третата система наричаме *равнини* и ги означаваме с $\alpha, \beta, \gamma, \dots$;

Мислим точките, правите и равнините като намиращи се в известни взаимни отношения и ние изразяваме тези отношения с думи като “*лежат*”, “*между*”, “*паралелно*”, “*конгруентно*”, “*непрекъснато*” и т.н.; точното и за математически цели описание на тези отношения се дава от аксиомите на геометрията.

Ние ще изходим от две първични съвкупности от “неща”: “множество на събитията” и “множество на състоянията”. Заедно с тях ще предположим и едно функционално отношение между тях: зададено е число $\in [0, 1]$ за всяка двойка от събитие и състояние, което наричаме “вероятност за настъпване / регистриране / измерване на събитие в състояние”.

Аксиоми на общи системи

Начална постановка: определение на статистическа система.

В началото на всеки модел на една система ние си мислим за две съвкупности:

Events – множество на събитията,

States – множество на състоянията.

Заедно с това ще ни бъде определена и функция:

$$\begin{aligned} \text{Prob} : \text{Events} \times \text{States} &\rightarrow [0, 1] \\ (Q, \rho) &\mapsto \text{Prob}_\rho(Q) \ (\equiv \text{Prob}_\rho(Q)), \end{aligned}$$

което се нарича **вероятност за настъпване (регистриране) на събитието Q в състояние ρ .**

Накратко казваме: “зададена статистическа система от данни:

$$(\text{Events}, \text{States}, \text{Prob} : \text{Events} \times \text{States} \rightarrow [0, 1]).$$

Определение на статистическа система:

$$(\mathcal{E}vents, \mathcal{S}tates, Prob).$$

Множествата $\mathcal{E}vents$ и $\mathcal{S}tates$, заедно с функцията $Prob$ ще бъдат структурно-определящите данни.

Заедно с това, понятията “събитие” и “състояние” ще са всичките първични понятия.

По-нататък ще определим, като вторични понятия:

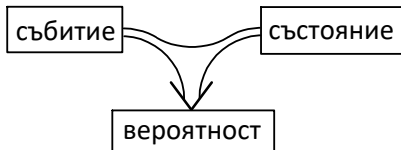
“логическата наредба и операции над събитията”, “елементарни събития”, “чисти / смесени състояния”, “експеримент”, “подсистема / надсистема”, “съвместна измеримост” и др.

Аксиоми на общи системи – начална постановка

Определение на статистическа система:

$(Events, States, Prob)$.

Илюстративна схема:

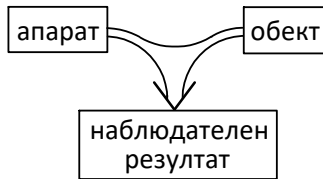


Аксиоми на общи системи – начална постановка

Определение на статистическа система:

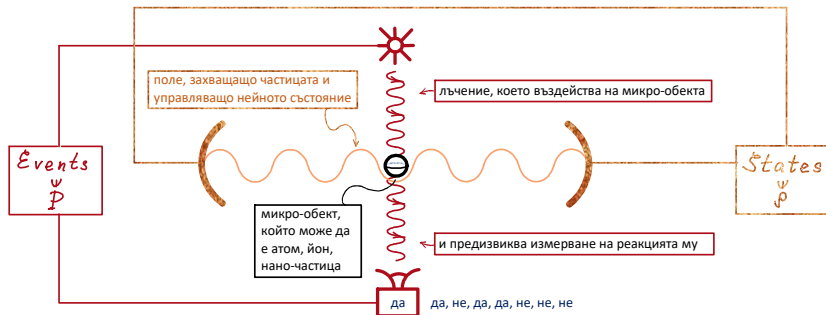
$(\mathcal{E}vents, \mathcal{S}tates, Prob)$.

Илюстративна схема:



Обръщаме внимание: квантовата теория описва взаимоотношението между “субект” (напр., апарат за наблюдение или цяла експериментална установка) И “обект” (напр., изследвания / наблюдавания обект), без да отстранява “субекта”.

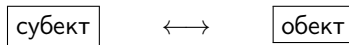
Аксиоми на общи системи – илюстрация на началната постановка



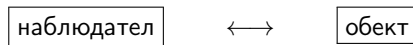
$$\text{Prob}_P = \lim_{N \rightarrow \infty} \frac{\text{брой "да" в } N \text{ последователни опита}}{N}$$

Аксиоми на общи системи – илюстрация на началната постановка

Квантовата теория описва отношението

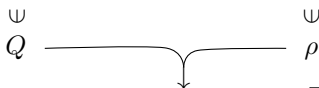


или, по-конкретно,



представено от:

Events *States*



$Prob_{\rho}(Q) =:$ вероятност за регистриране
на събитието Q в съст. ρ

$=: \rho(Q)$

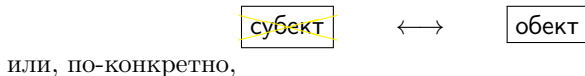
Регистрирането на събитие или още казано, установяване на свойство на обект, е “активен процес”.

То е нещо като “обичане на дреха върху обекта”, като резултата е “става” / “не става”.

При следваща регистрация на събитие, се “облича нова дреха”, което може да заличи старата.

Аксиоми на общи системи – илюстрация на началната постановка

Квантовата теория описва отношението



без да отстранява субекта / наблюдателя

и да описва обектите “сами по себе си”,
както се прави при класическото описание на природата.

Проблемът: може ли да опишем квантовия свят по класически път е т.нар. “проблем за скритите параметри (hidden variables)”.

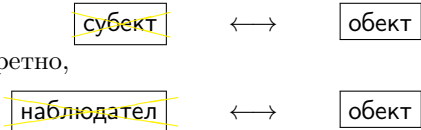
Еквивалентно: може ли да симулираме квантовите феномени на класически компютър.

Отговор: да – това е една от целите на квантовата теория.

Аксиоми на общи системи – илюстрация на началната постановка

Квантовата теория описва отношението

или, по-конкретно,



субект ↔ обект

наблюдател ↔ обект

без да отстранява субекта / наблюдателя

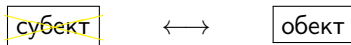
и да описва обектите “сами по себе си”,

както се прави при класическото описание на природата.

Това, което по принцип не може да се постигне, е при една такава симулация да е в сила, че на отделните части на света (напр., на отделни хора) *винаги* ще отговарят отделни части от паметта на класическия компютър, който извършва симулацията.

Аксиоми на общи системи – илюстрация на началната постановка

Квантовата теория описва отношението



или, по-конкретно,



без да отстранява субекта / наблюдателя

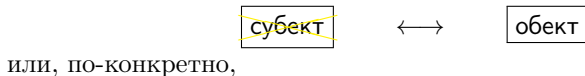
и да описва обектите “сами по себе си”,
както се прави при класическото описание на природата.

Това следва от т.нар. теорема на Бел, която може да се изказва така: “ако има скрити параметри, то те не са локални”.

Тази теорема е част от раздела по съставни системи.

Аксиоми на общи системи – илюстрация на началната постановка

Квантовата теория описва отношението



без да отстранява субекта / наблюдателя

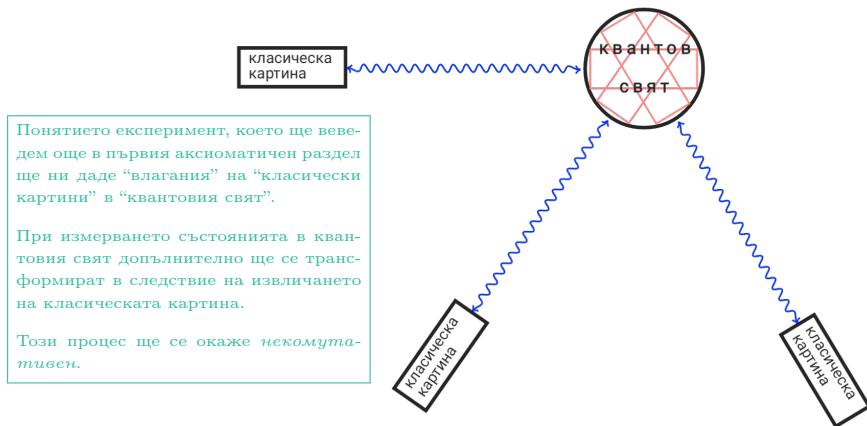
и да описва обектите “сами по себе си”,
както се прави при класическото описание на природата.

От друга страна, квантовото описание допуска локалност. Тя обаче идва преди всичко от наблюдателната страна.

Локалността е особено важна за т.нар. квантова теория на полето (Quantum Field Theory), която поради това също бива наричана “локална квантова физика” (Local Quantum Physics).

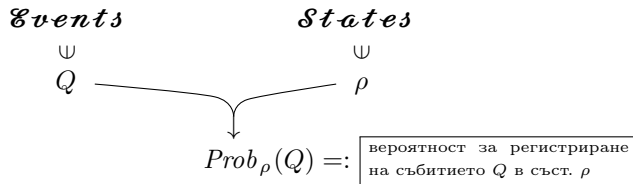
Аксиоми на общи системи – илюстрация на началната постановка

Допълнителни сведения за взаимоотношението между “наблюдателя” и “обекта” ще ни даде постулата за измерване от третия аксиоматичен раздел за “квантовите трансформации”.



Аксиоми на общи системи

Аксиомите до тук:



- Квантова система се задава от: $(\mathcal{Events}, \mathcal{States}, Prob)$.

Аксиоми на общи системи

Еднаквост (еквивалентност / изоморфност) на статистически системи:

$$\left(\mathcal{E}vents_1, \mathcal{S}tates_1, Prob_1 : \mathcal{E}vents_1 \times \mathcal{S}tates_1 \rightarrow [0, 1] \right), \\ \left(\mathcal{E}vents_2, \mathcal{S}tates_2, Prob_2 : \mathcal{E}vents_2 \times \mathcal{S}tates_2 \rightarrow [0, 1] \right).$$

Наричат се **еквивалентни** (изоморфни), ако са зададени биекции

$$F : \mathcal{E}vents_1 \cong \mathcal{E}vents_2, \\ G : \mathcal{S}tates_1 \cong \mathcal{S}tates_2,$$

такива че

$$Prob_{G(\rho)}(F(Q)) = Prob_{\rho}(Q),$$

за всеки $Q \in \mathcal{E}vents_1$ и $\rho \in \mathcal{S}tates_1$.

Аксиоми на общи системи – еднаквост на статистически системи

Значение на аксиомата за еднаквост на статистически системи:
пълното описание на системата трябва да следва единствено от информацията, съдържаща се в задаването на тройката

$$(\mathcal{E}vents, \mathcal{S}tates, Prob : \mathcal{E}vents \times \mathcal{S}tates \rightarrow [0, 1]) .$$

Аксиоми на общи системи

Аксиоми за отделимост. Нека е зададена статистическа система

$$(\mathcal{Events}, \mathcal{States}, Prob : \mathcal{Events} \times \mathcal{States} \rightarrow [0, 1]).$$

- За всеки две състояния $\rho, \sigma \in \mathcal{States}$,
ако $Prob_{\rho}(Q) = Prob_{\sigma}(Q)$ при всяко събитие $Q \in \mathcal{Events}$,
то $\rho = \sigma$.
- За всеки две събития $P, Q \in \mathcal{Events}$,
ако $Prob_{\rho}(P) = Prob_{\rho}(Q)$ при всяко състояние $\rho \in \mathcal{States}$,
то $P = Q$.

Съгласно първата от горните аксиоми ние отъждествяваме две състояния, ако при всеки експеримент те водят до еднакви наблюдателни резултати. Втората аксиома привежда същия принцип спрямо събитията.

Аксиоми на общи системи

Първо следствие: състоянията като функции на събитията

От първата от аксиомите за отделимост следва, че ние може да третираме състоянията, като *функции върху множеството на събитията $\mathcal{Events}$* .

За едно състояние $\rho \in \mathcal{States}$ ще пишем

$$\rho(Q) := \text{Prob}_\rho(Q)$$

Така, ρ става функция

$$\rho : \mathcal{Events} \rightarrow [0, 1] : Q \mapsto \rho(Q)$$

Нека подчертаем обаче, че далеч не всяка функция $\mathcal{Events} \rightarrow [0, 1]$ идва от състояние.

Аксиоми на общи системи – смесване на състояния

Аксиома за смесване на състояния. За една статистическа система

$$(\mathcal{E}vents, \mathcal{S}tates, Prob)$$

и произволни нейни състояния $\rho_1, \rho_2 \in \mathcal{S}tates$ и числа

$$q_1, q_2 \in [0, 1], \quad q_1 + q_2 = 1,$$

съществува състояние $\rho \in \mathcal{S}tates$, такова че

$$Prob_{\rho}(P) = q_1 Prob_{\rho_1}(P) + q_2 Prob_{\rho_2}(P),$$

за всяко събитие $P \in \mathcal{E}vents$.

От първата аксиома за отделимост следва, че горното ρ е единствено.

Състоянието ρ се нарича **смес на ρ_1 и ρ_2 с тегла q_1 и q_2** .

Еквивалентно условие: $\rho(P) = q_1 \rho_1(P) + q_2 \rho_2(P)$.

Аксиоми на общи системи – смесване на състояния

Аксиома за смесване на състояния – след итерация:

За една статистическа система $(\mathcal{E}vents, \mathcal{S}tates, Prob)$

и произволни нейни състояния $\rho_1, \dots, \rho_n \in \mathcal{S}tates$ и числа

$$q_1, \dots, q_n \in [0, 1], \quad q_1 + \dots + q_n = 1,$$

съществува състояние $\rho \in \mathcal{S}tates$, такова че

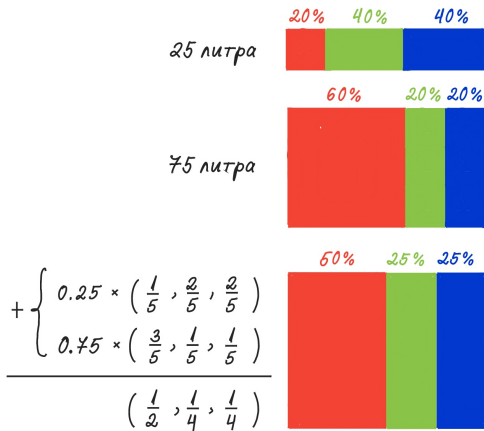
$$\rho(P) = q_1 \rho_1(P) + \dots + q_n \rho_n(P),$$

за всяко събитие $P \in \mathcal{E}vents$.

Състоянието ρ се нарича **смес на** $\rho_1, \dots, \rho_n$ **с тегла** $q_1, \dots, q_n$.

Аксиоми на общи системи – смесване на състояния

Илюстрация: смес на бои



Аксиоми на общи системи – смесване на състояния

Чисти и смесени състояния:

Чисто състояние е състояние, което не може да се представи като *нетривиална смес*.

Подробно, състоянието ρ е чисто

$\Leftrightarrow$ за всяко представяне на ρ в смес $\rho = q_1\rho_1 + q_2\rho_2$ е в сила, че
или $q_1 = 1$ ($\Leftrightarrow q_2 = 0 \Leftrightarrow \rho = \rho_1$), или $q_2 = 1$ ($\Leftrightarrow q_1 = 0 \Leftrightarrow \rho = \rho_2$)

(последните именно казваме, че отговарят на тривиални смеси).

Смесено състояние = не чисто състояние.

И така, чистите състояния съответстват на най-прецизно приготвените състояния. Логично е да се очаква, че при тях вероятностите на всички събития биха били 1 или 0. Оказва се обаче, че това е така само за т.нар. “класически системи”. За обща квантова система се оказва, че дори и в чисто състояние определени събития могат да настъпват с вероятност отлична от 1 или 0. Това е именно точния израз на неотстранимия индетерминизъм на квантовата теория, за който споменахме в увода.

Аксиоми на общи системи – смесване на състояния

Чисти и смесени състояния

Терминология от квантовата физика:

Когато една система е в чисто състояние се казва, че имаме “**кохерентност**” (“**coherence**”).

Когато системата премине по някаква причина от чисто в смесено състояние се казва, че губим “**кохерентността**”. Този процес се нарича “**декохерентност**” (“**decoherence**” = “загуба на чистота”).

Една от стандартните причини за загуба на чистотата (декохерентността) е сплитането с околната среда. Това ще изучим като едно приложение на втория аксиомитичен раздел за съставни системи. Борбата за кохерентост се състои в добрата изолация от околната среда.

Аксиоми на общи системи

Преговор от теория на вероятностите

Крайно вероятностно пространство – включва:

- $\Omega = \{\omega_1, \dots, \omega_n\}$ = множество на елементарните състояния
 $\equiv$ множество на елементарните “събития”.

- Зададени са вероятности:

$$\begin{array}{ccc} \Omega = \{\omega_1, & \dots, & \omega_n\} \\ \downarrow & & \downarrow \\ p_1, & \dots, & p_n \\ & & = p_1(\omega_1), \dots, p_n(\omega_n). \end{array}$$

Тоест, $p_j \in [0, 1]$, $\sum_{j=1}^n p_j \left(\equiv \sum_{\omega \in \Omega} p(\omega) \right) = 1$

– $(p_1, \dots, p_n)$ е вероятностно разпределение.

Аксиоми на общи системи – преговор от теория на вероятностите

В крайно вероятно пространство Ω :

- за подмножествата $S \subseteq \Omega$: $p(S) := \sum_{\omega \in S} p(\omega) \in [0, 1]$
– вероятност за събитието S
- Вероятностите $p(S)$ имат свойствата:
 - (p_1) адитивност $S = S_1 \dot{\cup} S_2 \Rightarrow p(S) = p(S_1) + p(S_2)$,
където $S = S_1 \dot{\cup} S_2 \Leftrightarrow S = S_1 \cup S_2$ и $\emptyset = S_1 \cap S_2$
и се нарича *дизюнктивно обединение*;
 - (p_2) монотонност $S_1 \subseteq S \Rightarrow p(S_1) \leq p(S)$;
 - (p_3) нормировка $p(\emptyset) = 0$, $p(\Omega) = 1$.

Аксиоми на общи системи – преговор от теория на вероятностите

В крайно вероятностно пространство Ω :

- **Условната вероятност:** $p(S \mid Q) := \frac{p(S \cap Q)}{p(Q)}$ (ф-ла на Бейс)

элементарни
состояния

ω_1 ω_2 ω_3 ω_4 ω_5 ω_6



вероятности

$\frac{1}{12}$ $\frac{1}{6}$ $\frac{1}{6}$ $\frac{1}{6}$ $\frac{1}{6}$ $\frac{1}{4}$

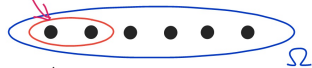
условие
 A

$(1 : 2 : 2 : 2 : 2 : 3)$

редукция
след условието

элементарни
состояния

ω_1 ω_2 ω_3 ω_4 ω_5 ω_6



вероятности

$\frac{1}{3}$ $\frac{2}{3}$ 0 0 0 0

$(1 : 2)$

элиминировани
от условието

като пропорциите в A се запазват

Аксиоми на общи системи – преговор от теория на вероятностите

В крайно вероятностно пространство Ω :

- **Условната вероятност:** $p(S | Q) := \frac{p(S \cap Q)}{p(Q)}$ (ф-ла на *Бейс*)
- Забележете: $p'(\omega_k) := p(\omega_k | Q)$ ($k = 1, \dots, n$) отново е вероятностно разпределение. Действително:

$$\begin{aligned} \sum_{k=1}^n p(\omega_k | Q) &= \sum_{k=1}^n \frac{p(\{\omega_k\} \cap Q)}{p(Q)} = \frac{1}{p(Q)} \sum_{k=1}^n p(\{\omega_k\} \cap Q) \\ &= \frac{1}{p(Q)} p\left(\bigcup_{k=1}^n (\{\omega_k\} \cap Q)\right) = \frac{1}{p(Q)} p\left(\underbrace{\left(\bigcup_{k=1}^n \{\omega_k\}\right) \cap Q}_{\Omega}\right) = 1. \end{aligned}$$

Аксиоми на общи системи – преговор от теория на вероятностите

В крайно вероятностно пространство Ω :

- **Условната вероятност:** $p(S | Q) := \frac{p(S \cap Q)}{p(Q)}$ (ф-ла на Бейс)
- Събитията $S, Q \subseteq \Omega$ се наричат **независими събития**, ако $p(S | Q) = p(S)$. Така, S и Q са независими

$$\iff p(Q | S) = p(Q)$$

$$\iff p(S \cap Q) = p(S)p(Q)$$

и в частност, релацията независимост е симетрична.

(но не и рефлексивна или транзитивна)

Аксиоми на общи системи – смесване на състояния

Вероятностна смес: пример

$$\begin{array}{l}
 75 \text{ зарсета} \\
 \text{от вид 1:}
 \end{array}
 \begin{array}{cccccc}
 \omega_1 & \omega_2 & \omega_3 & \omega_4 & \omega_5 & \omega_6 \\
 \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
 \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6}
 \end{array}$$

$$\begin{array}{l}
 25 \text{ зарсета} \\
 \text{от вид 2:}
 \end{array}
 \begin{array}{cccccc}
 \omega_1 & \omega_2 & \omega_3 & \omega_4 & \omega_5 & \omega_6 \\
 \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
 \frac{1}{12} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{4}
 \end{array}$$

$$\begin{array}{cccccc}
 \omega_1 & \omega_2 & \omega_3 & \omega_4 & \omega_5 & \omega_6 \\
 \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
 + \left\{ \begin{array}{l} 0.75 \times \left(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6} \right) \\ 0.25 \times \left(\frac{1}{12}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{4} \right) \end{array} \right. \\
 \hline
 \left(\frac{7}{48}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{3}{16} \right)
 \end{array}$$

Аксиоми на общи системи – смесване на състояния

Вероятностна смес: обща постановка

Допускаме, че експеримент с елементарни събития $\tilde{\omega}_k := \{\omega_k\}$, за $k = 1, \dots, n$, има по-fino описание, при което всяко $\tilde{\omega}_k$ престава да бъде елементарно и се реализира при две взаимно допълнителни се ситуации A_1, A_2 :

$$A_1 \cap A_2 = \emptyset \text{ (невъзможно събитие),}$$

$$A_1 \cup A_2 = \text{винаги изпълненото събитие.}$$

Тогава: $\tilde{\omega}_k = (A_1 \cup A_2) \cap \tilde{\omega}_k = (A_1 \cap \tilde{\omega}_k) \cup (A_2 \cap \tilde{\omega}_k)$, като

$$(A_1 \cap \tilde{\omega}_k) \cap (A_2 \cap \tilde{\omega}_k) = \emptyset.$$

Аксиоми на общи системи – смесване на състояния

Вероятностна смес: обща постановка

Допускаме: $\tilde{\omega}_k = (A_1 \cup A_2) \cap \tilde{\omega}_k = (A_1 \cap \tilde{\omega}_k) \cup (A_2 \cap \tilde{\omega}_k)$, като

$$(A_1 \cap \tilde{\omega}_k) \cap (A_2 \cap \tilde{\omega}_k) = \emptyset.$$

Следователно,

$$p(\omega_k) = p(A_1 \cap \tilde{\omega}_k) + p(A_2 \cap \tilde{\omega}_k) = p(A_1) p(\omega_k | A_1) + p(A_2) p(\omega_k | A_2).$$

Нека положим: $p'(\omega_k) := p(\omega_k | A_1)$, $q_1 := p(A_1)$,
 $p''(\omega_k) := p(\omega_k | A_2)$, $q_2 := p(A_2)$ ($k = 1, \dots, n$).

Тогава полученият резултат се записва като:

$$p(\omega_k) = q_1 \cdot p'(\omega_k) + q_2 \cdot p''(\omega_k) \quad (k = 1, \dots, n),$$

където $(p'(\omega_1), \dots, p'(\omega_n))$, $(p''(\omega_1), \dots, p''(\omega_n))$ и (q_1, q_1)

са вероятностни разпределения.

Аксиоми на общи системи – смесване на състояния

Вероятностна смес: обща постановка

Полученото вероятностно разпределение $(p(\omega_1), \dots, p(\omega_n))$ се нарича **смес** на $(p'(\omega_1), \dots, p'(\omega_n))$ и $(p''(\omega_1), \dots, p''(\omega_n))$ с тегла q_1 и q_2 .

То се дава по формулата

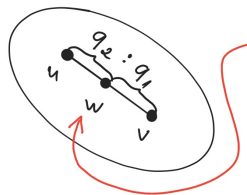
$$(p(\omega_1), \dots, p(\omega_n)) = q_1 \cdot (p'(\omega_1), \dots, p'(\omega_n)) + q_2 \cdot (p''(\omega_1), \dots, p''(\omega_n)).$$

Упражнение. За всяко събитие $S \subseteq \Omega$ е в сила равенството:

$$p(S) = q_1 p'(S) + q_2 p''(S).$$

Аксиоми на общи системи – смесване на състояния

Геометрия на множеството на състоянията

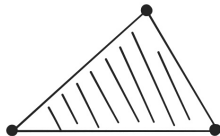


w се нарича
изпъкнала комбинация
на u и v с тегла q_1, q_2

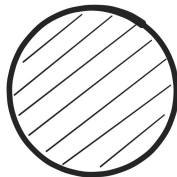
- Следователно:
- ***States*** е изпъкнало множество в линейното пространство $\{f \mid f : \mathcal{Events} \rightarrow \mathbb{R}\}$.
 - Смес $\Leftrightarrow$ изпъкнала комбинация
 - Чисто състояние $\Leftrightarrow$ екстремална точка

Аксиоми на общи системи – смесване на състояния

Геометрия на множеството на състоянията



Всеки затворен триъгълник е изпъкнало множество.
Екстремалните му точки са само върховете му, без останалата част от границата му.



Всеки затворен диск е изпъкнало множество.
Екстремалните му точки са цялата граница.

Геометрия на множеството на състоянията

Симплексът:

$$\Delta_{n-1} := \left\{ (p_1, \dots, p_n) \in \mathbb{R}^n \mid 0 \leq p_j \leq 1, \text{ за } j = 1, \dots, n; \right. \\ \left. p_1 + \dots + p_n = 1 \right\}.$$

Това е изпъкнало подмножество на $\mathbb{R}^n$, в което изпъкналата комбинация, както видяхме в предната точка, има смисъл на *вероятностна смес*.

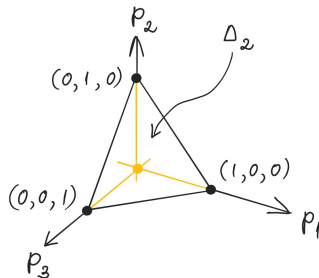
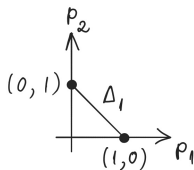
Екстремалните точки на Δ_{n-1} са разпределенията от вида $(0, \dots, 0, 1, 0, \dots, 0)$.

Аксиоми на общи системи – смесване на състояния

Геометрия на множеството на състоянията

Симплексът:

$$\Delta_{n-1} := \{ (p_1, \dots, p_n) \in \mathbb{R}^n \mid 0 \leq p_j \leq 1, \text{ за } j = 1, \dots, n; \\ p_1 + \dots + p_n = 1 \}.$$

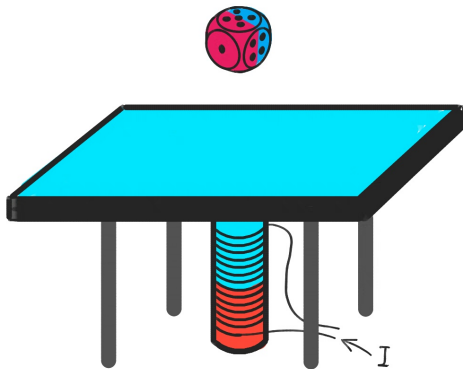


Аксиоми на общи системи

Класически системи

Класическа крайна система се определя от едно крайно множество Ω , по което задаваме:

- $\mathcal{Events} := \mathcal{P}(\Omega)$ - това е **степенното множество** (power set) на Ω
(т.е., това е множеството на всички подмножества на Ω);
- $\mathcal{States} := \text{Prob.Func.}(\Omega)$ – това е множеството на всички вероятностни разпределения над Ω – то е симплекс.



Магнитно зарче, чието вероятно разпределение на паданията може да се манипулира от тока I намагнетизиращ масата

состояние $\downarrow$	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
вероятность $p_{(I=+3)}$	$\frac{1}{54}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{5}{6}$
вероятность $p_{(I=+1)}$	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{4}$
вероятность $p_{(I=0)}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
вероятность $p_{(I=-1)}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{12}$
вероятность $p_{(I=-3)}$	$\frac{5}{6}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{1}{27}$	$\frac{1}{54}$

Примерни вероятностни разпределения за зарчето от предната фигура, в зависимост от силата на тока I

АКСИОМИТЕ ДО ТУК

Следващата аксиома може да се изкаже така:

States е изпъкнало множество в реалното линейно пространство

$$\{f \mid f : \mathcal{Events} \rightarrow \mathbb{R}\}.$$

- При това:
- напомниме, че изпъкналостта на *States* означава, че заедно с всеки два него елемента $\rho_1, \rho_2 \in \mathcal{States}$, то съдържа и всяка тяхна изпъкнала комбинация, $\rho = q_1\rho_1 + q_2\rho_2$
(на свой ред, “изпъкнала комбинация” $\Leftrightarrow q_1, q_2 \in [0, 1]$ и $q_1 + q_2 = 1$;
изпъкналите комбинации са точките от свързващата отсечка).
 - Изпъкналите комбинации на състояния наричаме смес на състояния.
Смесването на състояния се интерпретира, като на “квантова” вероятностна смес.
 - Чисто състояние = екстремална точка на *States* = такова състояние, което не може да се представи, като нетривиална смес на други състояния.
Смесено състояние = не чисто състояние.

АКСИОМИТЕ ДО ТУК

Първи пример: крайни класически системи

Крайна класическа система се строи по едно крайно множество Ω

($\Omega = \{\omega_1, \dots, \omega_n\}$). Тогава:

- $\mathcal{Events} := \mathcal{P}(\Omega) :=$ степенното множество (**power set**) на Ω
(т.е., това е множеството на всички подмножества на Ω);
- $\mathcal{States} := \mathcal{Prob.Func.}(\Omega)$
 $=$ множеството на всички вероятностни разпределения
над Ω ($= \{p : \Omega \rightarrow [0, 1] \mid \sum_{j=1}^n p(\omega_j) = 1\}$)
 $\cong \Delta_{n-1}$ ($(n-1)$ -мерния симплекс)
 $= \{(p_1, \dots, p_n) \in [0, 1]^n \mid p_1 + \dots + p_n = 1\}$.
- Чистите състояния $\longleftrightarrow (p_1, \dots, p_n) = (0, \dots, 0, 1, 0, \dots, 0)$
(в частност, чистите състояния са n на брой).

ПО-НАТАТЪК В ТАЗИ ЛЕКЦИЯ ЩЕ ВЪВЕДЕМ

Втори пример: крайни (чисто) квантови системи

Крайна квантова система се строи по $\mathbb{C}^n$ – крайно-мерно, комплексно хилбертово (= унитарно) пространство с размерност n .

- *Events* $:= \mathfrak{L}(\mathbb{C}^n) := \{V \mid V \text{ е линейно подпространство на } \mathbb{C}^n\}$
(това е вече безкрайно множеството);

- *States* $:= \text{ConvexHull} \{ \rho_\Psi \mid \Psi \in \mathbb{C}^n \text{ е единичен вектор} \},$

$$\text{където } \rho_\Psi(V) := \|\Pi_V \Psi\|^2,$$

а Π_V е ортогоналния проектор върху V

- Чистите състояния ще са тези и само тези, които са от вида ρ_Ψ
(множеството на чистите състояния е също безкрайно).

Аксиомите до тук бяха толкова общи, че допускат не само горните два класа модели, но и много други, които са “безинтересни”.

Една от целите на аксиоматиката е да се въведат такива аксиоми, които освен че са “интуитивни”, също и максимално да стесняват кръга на моделите, по възможност дори, само до тези два класа (и евентуално, “хибриди” между тях).

Преговор по алгебра

Комплексни числа: $\mathbb{C} = \{z = x + iy \mid (x, y) \in \mathbb{R}^2\}$

$$i^2 = -1$$

i – имажинерна единица

$x = \operatorname{Re} z$ – реална част на z

$y = \operatorname{Im} z$ – имажинерна част

$$(x_1 + iy_1)(x_2 + iy_2) = x_1x_2 - y_1y_2 + i(y_1x_2 + x_1y_2)$$

– асоциативно и комутативно умножение.

За $z = x + iy \in \mathbb{C}$: $\bar{z} := x - iy$ – комплексно спрягане,

$$|z| := \sqrt{z\bar{z}} = \sqrt{x^2 + y^2} \text{ – модул на } z.$$

Формула на Ойлер: $e^{i\varphi} = \cos \varphi + i \sin \varphi$

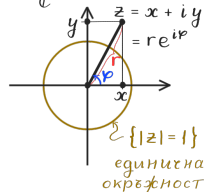
Euler

– общ вид на комплексно число по модул 1.

Полярно разлагане: $z = re^{i\varphi}$,

където $r = |z|$ е модула на z , а φ се нарича аргумент / фаза.

комплексна равнина
 $\mathbb{C}$



Крайно-мерни комплексни хилбертови пространства

(= унитарни пространства)

Определение. Крайно-мерно комплексно хилбертово пространство е крайно-мерно линейно пространство $\mathcal{H}$ над $\mathbb{C}$, снабдено с функция

$$\mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C} : \underbrace{(\Phi, \Psi)}_{\text{внимание: наредена двойка}} \longmapsto \underbrace{\langle \Phi | \Psi \rangle}_{\text{число}},$$

наречена **скалярно произведение** със свойствата:

- $\langle \alpha\Phi + \beta\Psi | \alpha'\Phi' + \beta'\Psi' \rangle = \bar{\alpha}\alpha' \langle \Phi | \Phi' \rangle + \bar{\alpha}\beta' \langle \Phi | \Psi' \rangle + \bar{\beta}\alpha' \langle \Psi | \Phi' \rangle + \bar{\beta}\beta' \langle \Psi | \Psi' \rangle,$ (антилинейност-линейност)
- $\langle \Phi | \Psi \rangle = \overline{\langle \Psi | \Phi \rangle}$ (емитова симетрия),
- $\langle \Phi | \Phi \rangle \geq 0,$ като $\langle \Phi | \Phi \rangle = 0 \Leftrightarrow \Phi = 0$ (строга положителна дефинитност),

за всеки $\Phi, \Psi, \Phi', \Psi' \in \mathcal{H}$ и $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$.

Елементарната теория на хилбертовите пространства в голяма степен прилича на теорията евклидовите пространства.

(Евклидовите пространства ги наричат също “реални евклидови пространства”).

Например, аналогично на евклидовите пространства въвеждаме понятията: • $\|\Psi\| := \sqrt{\langle \Psi | \Psi \rangle}$ се нарича **норма** (дължина) на вектор Ψ в хилбертово пространство $\mathcal{H}$.

- Ψ е **единичен вектор** $\Leftrightarrow \|\Psi\| = 1$.
- Векторите Ψ и Φ са взаимно **ортогонални** $(\Psi \perp \Phi) \Leftrightarrow \langle \Psi | \Phi \rangle = 0$.
- Базисът $e_1, \dots, e_n$ на $\mathcal{H}$ се нарича **орто-нормиран**, ако се състои от единични вектори, които са взаимно ортогонални.

$$\text{Еквивалентно: } \langle e_j | e_k \rangle = \boxed{\delta_{j,k} := \begin{cases} 1 & \text{при } j = k \\ 0 & \text{при } j \neq k \end{cases}} \leftarrow \begin{cases} \text{делта-символ} \\ \text{на Крьонекер.} \end{cases}$$

Елементарната теория на хилбертовите пространства в голяма степен прилича на теорията евклидовите пространства.

(Евклидовите пространства ги наричат също “реални евклидови пространства”).

Например, аналогично на евклидовите пространства въвеждаме понятията: • Ако $V \subseteq \mathcal{H}$ е линейно подпространство, то

$$V^\perp := \{\Phi \in \mathcal{H} \mid \Phi \perp \Psi \text{ за всяко } \Psi \in V\}$$

наричаме **ортогонално допълнение** на V .

Теорема.

Всеки вектор $\Theta \in \mathcal{H}$ се представя по единствен начин като сума:

$$\Theta = \Psi + \Phi \quad \text{за } \Psi \in V \text{ и } \Phi \in V^\perp.$$

Последното се записва също така: $\mathcal{H} = V \oplus V^\perp$.

Полагането $\Pi_V(\Theta) := \Psi$ определя линейен оператор $\Pi_V : \mathcal{H} \rightarrow \mathcal{H}$, наречен **ортогонален проектор върху V** .

Основен пример на хилбертово пространство:

Това е $\mathbb{C}^n$ снабдено със скаларното произведение:

$$\langle \Psi | \Phi \rangle = \overline{\psi}_1 \phi_1 + \cdots \overline{\psi}_n \phi_n,$$

$$\text{ако } \Psi = (\psi_1, \dots, \psi_n) \in \mathbb{C}^n \text{ и}$$

$$\Phi = (\phi_1, \dots, \phi_n) \in \mathbb{C}^n.$$

Скаларното произведение в орто-нормиран базис придобива вида на скаларното произведение в $\mathbb{C}^n$ и по такъв начин, разглеждането на хилбертовото пространство $\mathbb{C}^n$ е равносилно на задаване на n -мерно хилбертово пространство с *посочен* орто-нормиран базис.

ТАКА ДЕФИНИРАМЕ

Втори пример: крайни (чисто) квантови системи

Крайна квантова система се строи по $\mathbb{C}^n$ – крайно-мерно, комплексно хилбертово (= унитарно) пространство с размерност n .

- $\mathcal{Events} := \mathfrak{L}(\mathbb{C}^n) := \{V \mid V \text{ е линейно подпространство на } \mathbb{C}^n\}$
(това е вече безкрайно множеството);
- $\mathcal{States} := \text{ConvexHull} \{ \rho_\Psi \mid \Psi \in \mathbb{C}^n \text{ е единичен вектор} \},$
където $\rho_\Psi(V) := \|\Pi_V \Psi\|^2,$
а Π_V е ортогоналния проектор върху V
- Чистите състояния ще са тези и само тези, които са от вида ρ_Ψ
(множеството на чистите състояния е също безкрайно).