КВАНТОВА ИНФОРМАТИКА

Николай М. Николов

Лекция 3 / 23.10.2023, версия 2

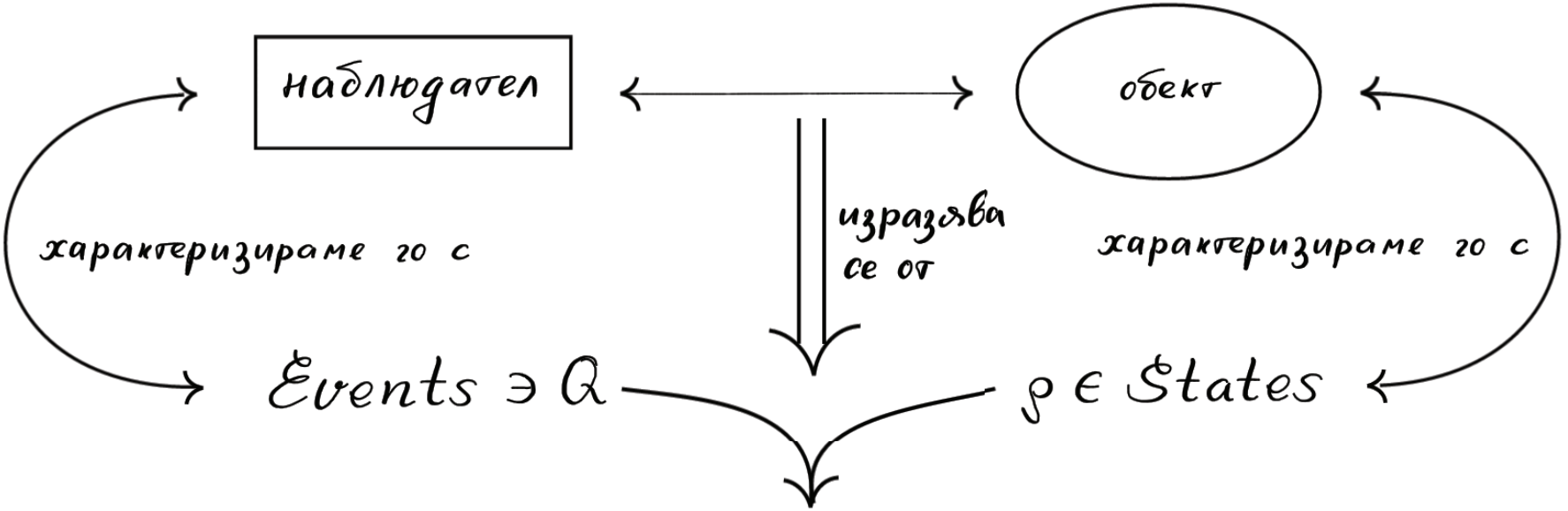
Обзорна част

ЧАСТ 1: АКСИОМАТИЧНИ ОСНОВИ НА КВАНТОВАТА ТЕОРИЯ

аксиоматични подходи / аксиоматични раздели	квантово-логически аксиоматичен подход	алгебричен аксиоматичен подход
аксиоми на общи системи	лекции 2-4	лекции 5-7
аксиоми на съставни системи	———	лекция 8
квантови трансформации	———	лекция 9

Най-важното до тук

В квантовата теория се изучава връзката



$$Prob_\rho(Q) =: \rho(Q) = \text{вероятност за } Q \text{ в } \rho$$

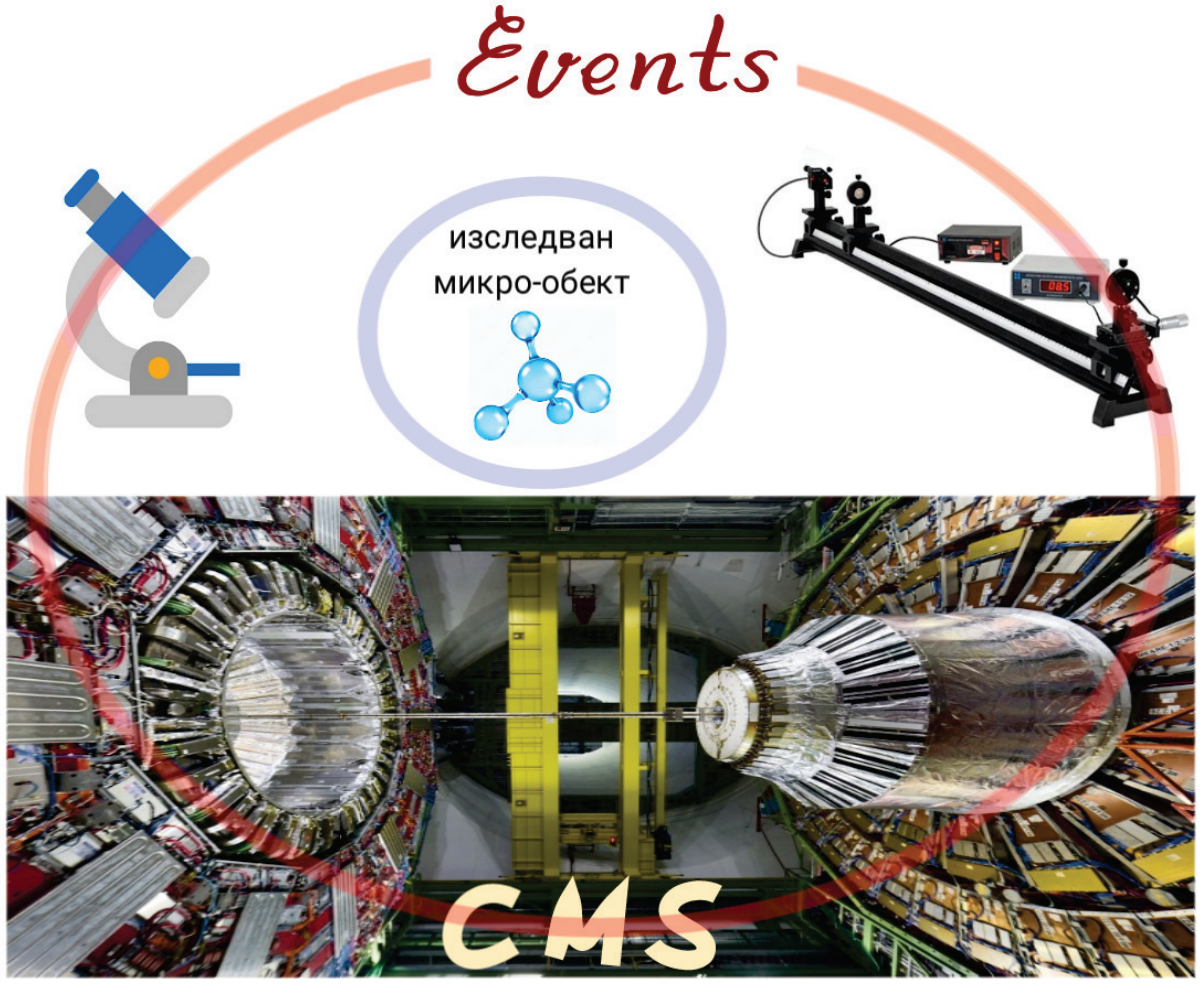
При разглеждането на сдвояването

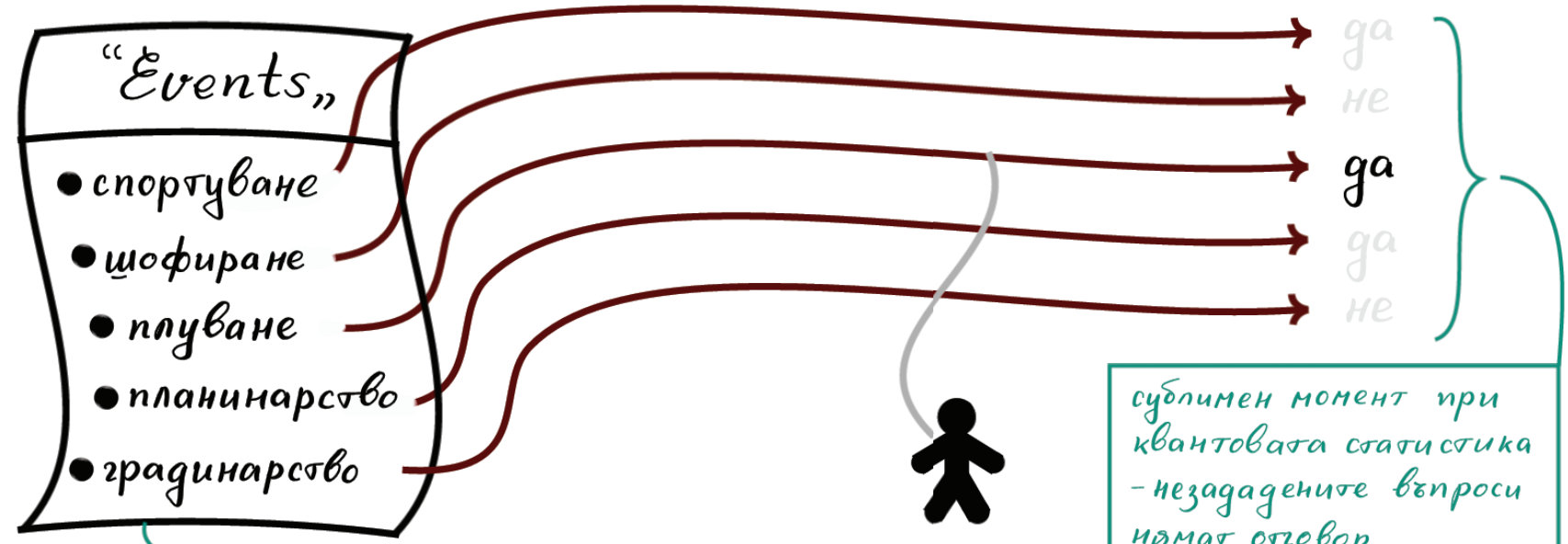
наблюдател - обект

ние фиксираме изследвания вид обект, но не фиксираме изследващия го експеимент (апарат).

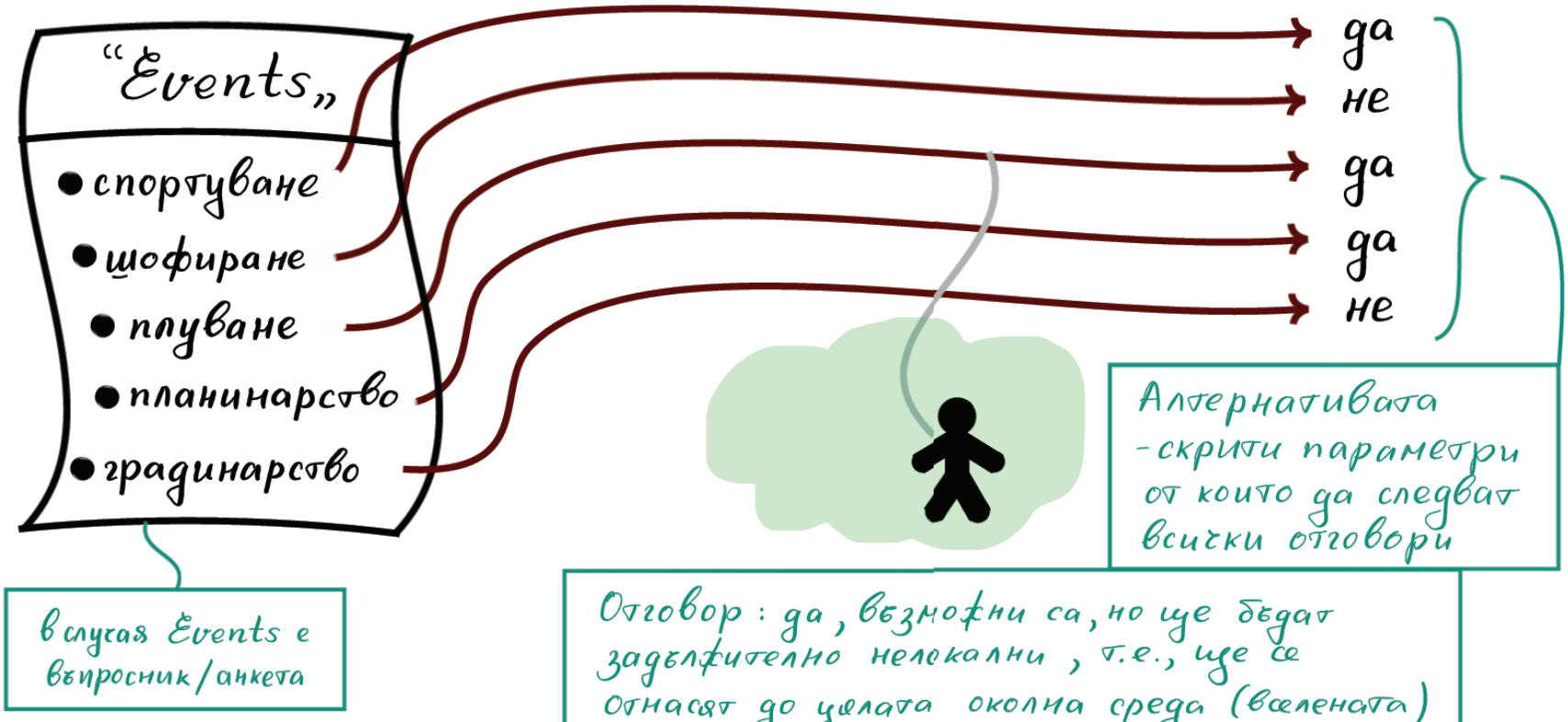
Разглеждаме "всички възможни по принцип, изследващи експерименти".

Някои от тях ще могат да се провеждат съвместно, други - не.



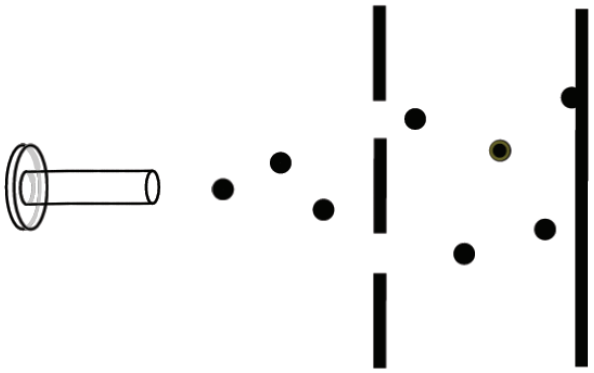


Пример от социологията

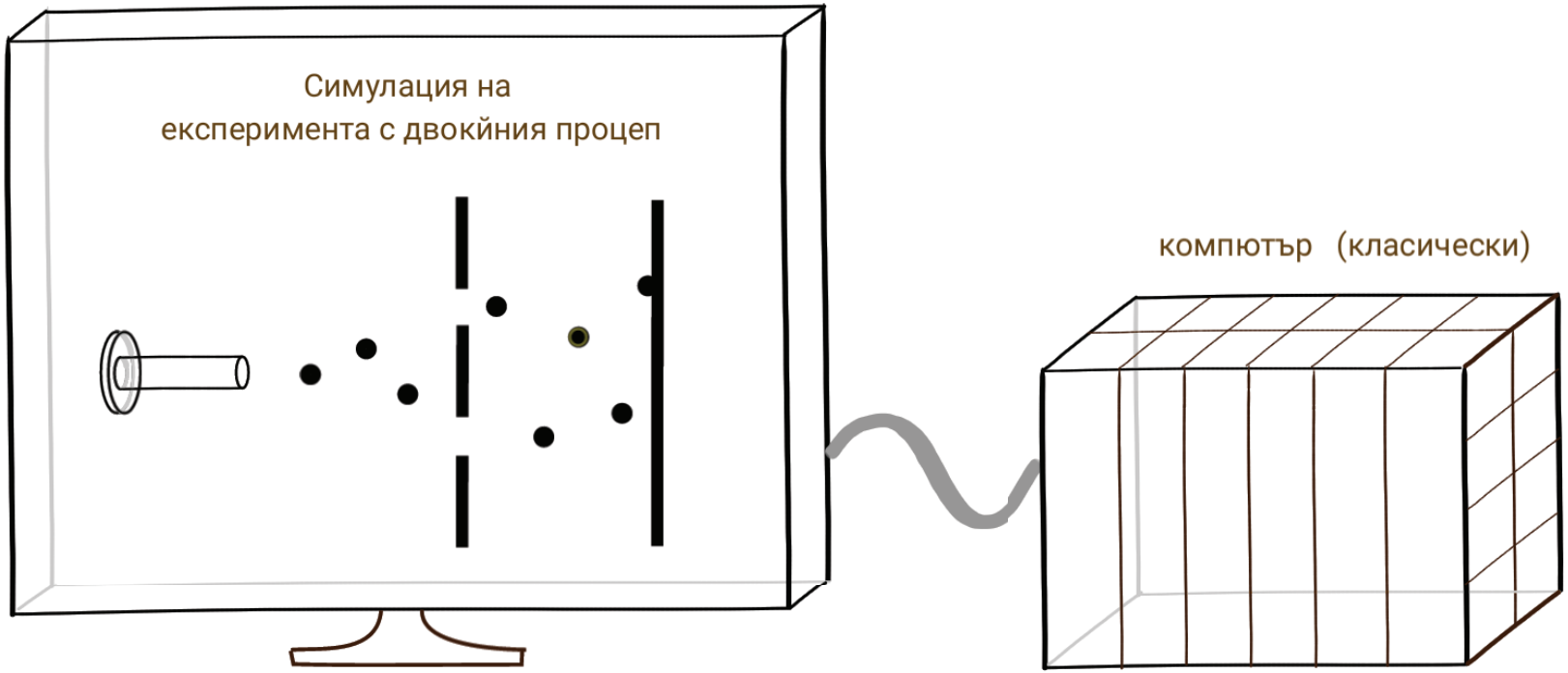


Пример от социологията

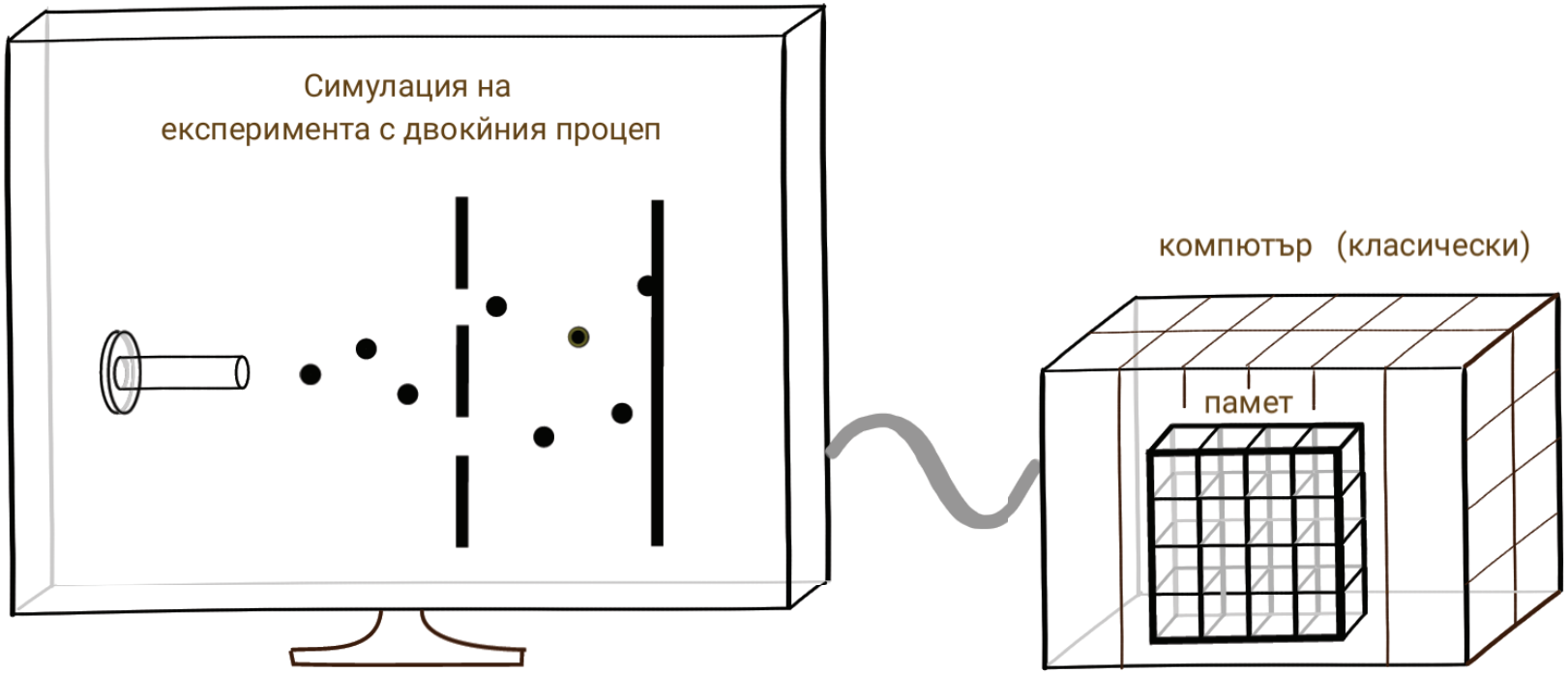
Скрити параметри и нелокалност



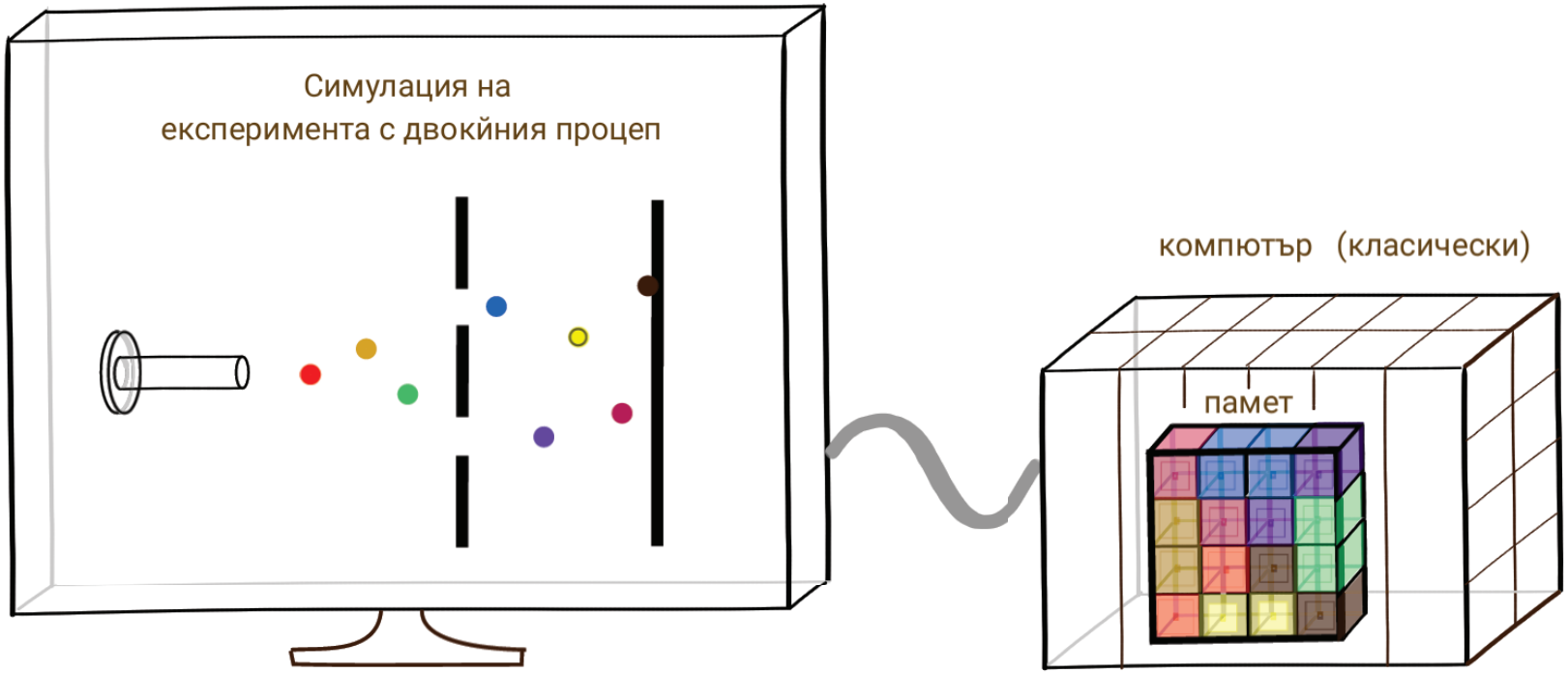
Скрити параметри и нелокалност



Скрити параметри и нелокалност

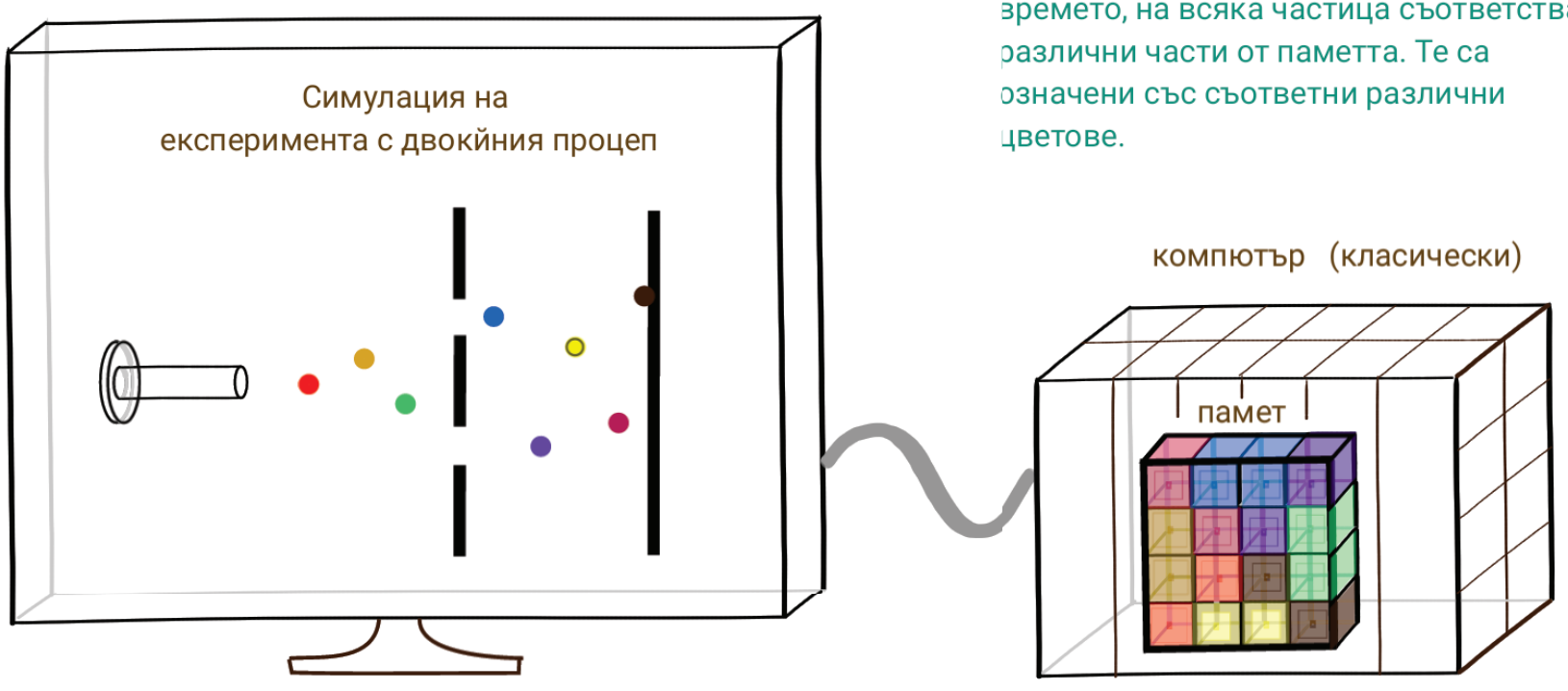


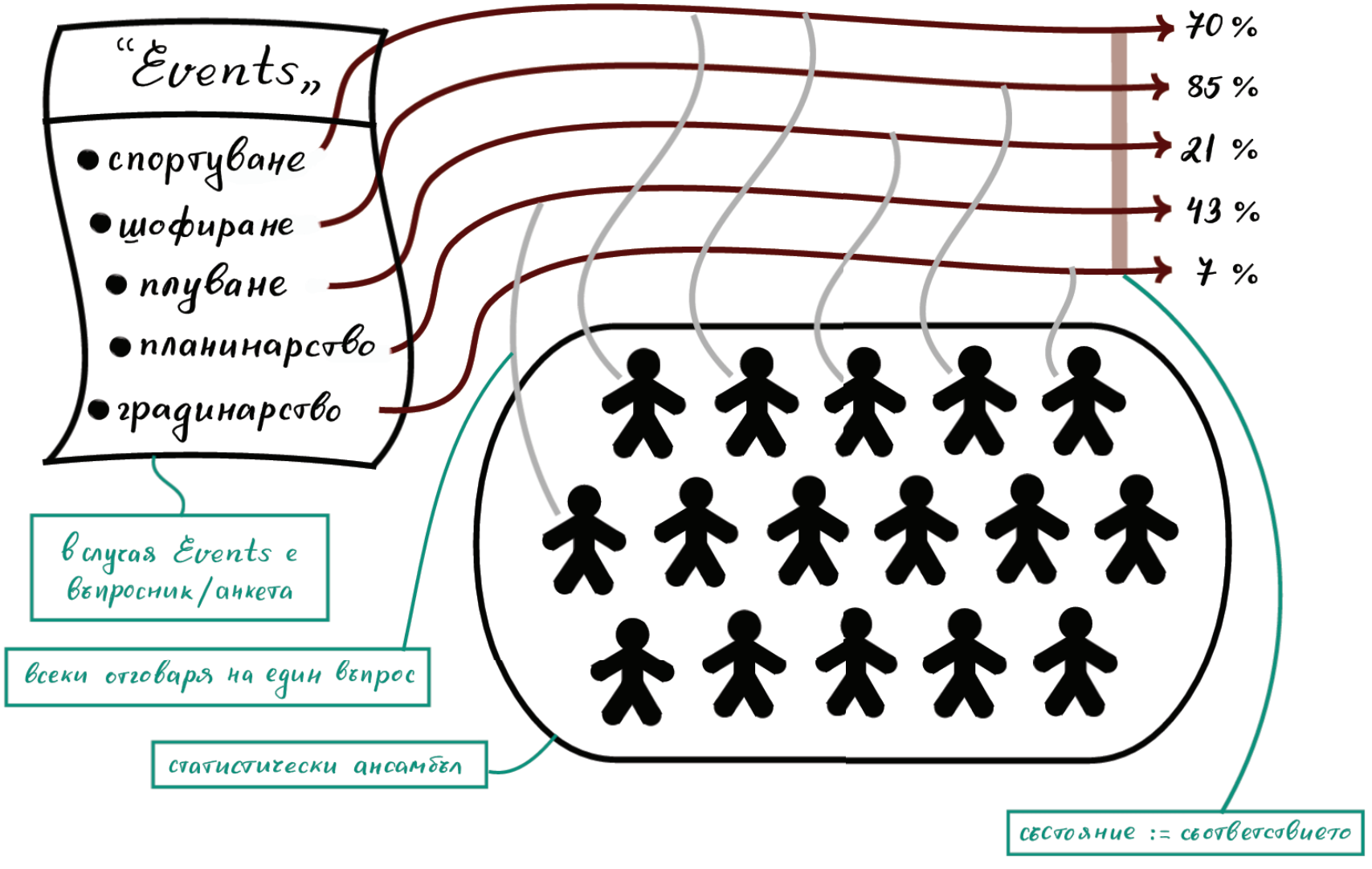
Скрити параметри и нелокалност

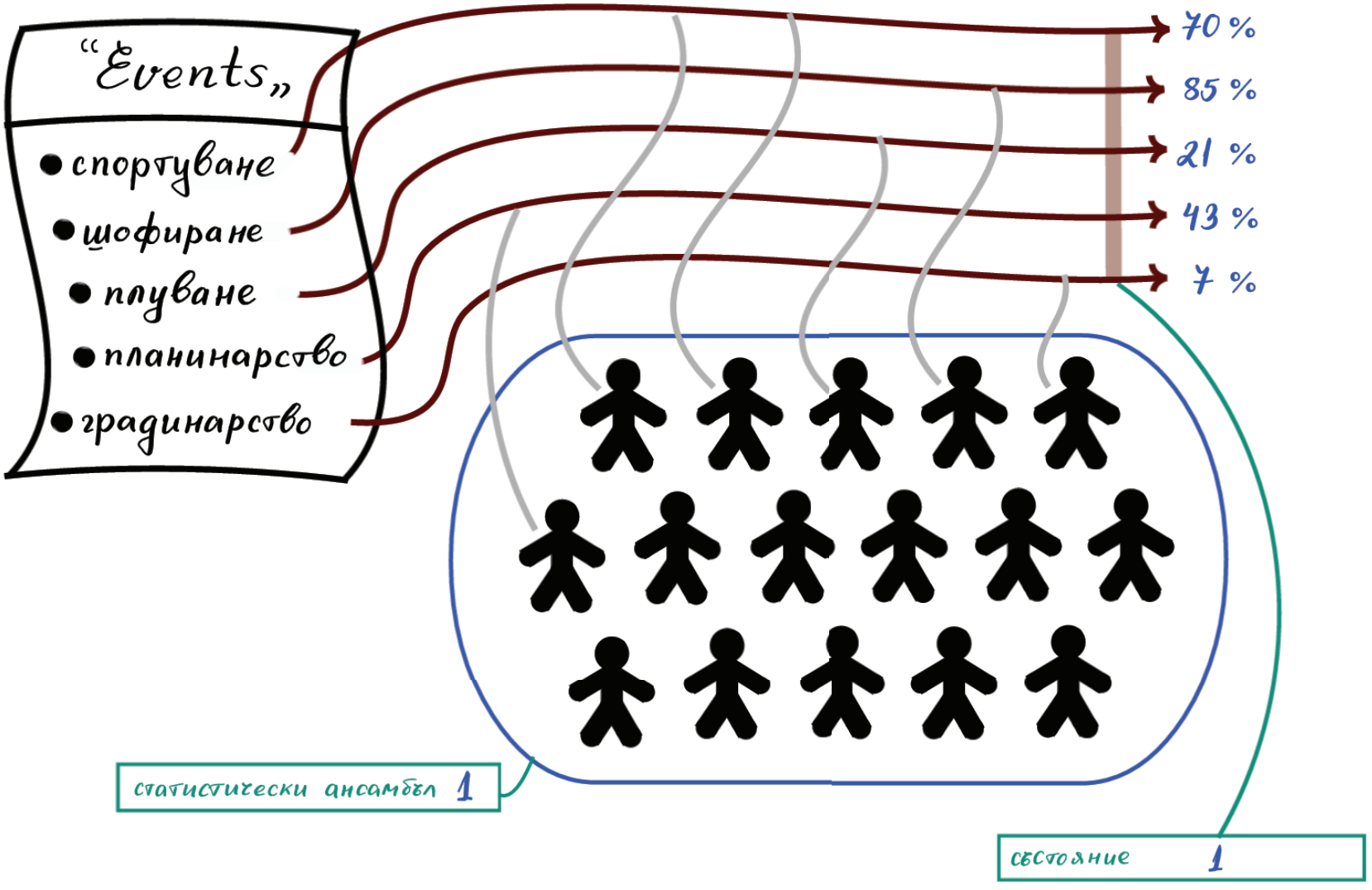


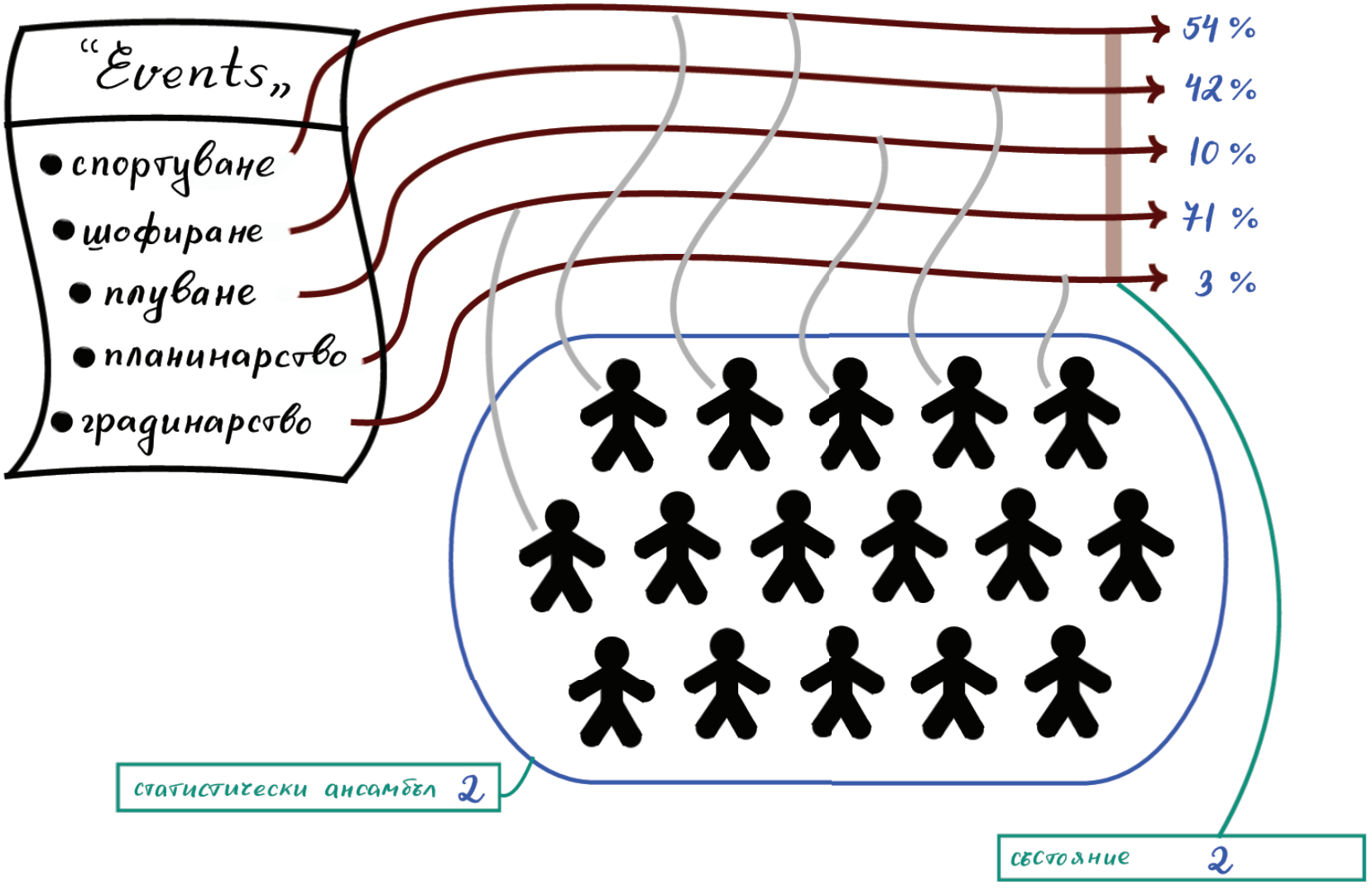
Скрити параметри и нелокалност

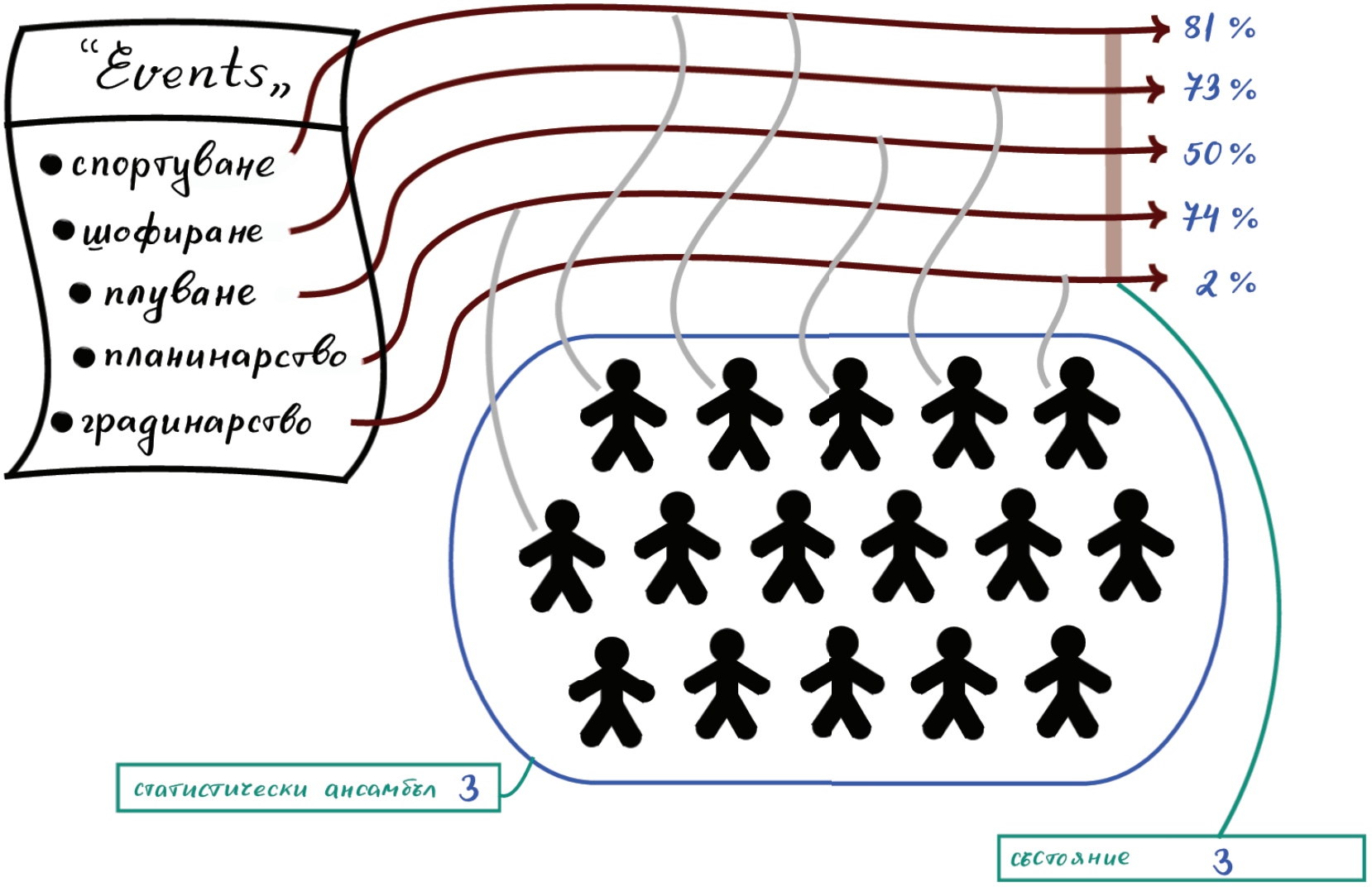
При локалност на симулацията (локални скрити параметри) във всеки момент от времето, на всяка частица съответстват различни части от паметта. Те са означени със съответни различни цветове.

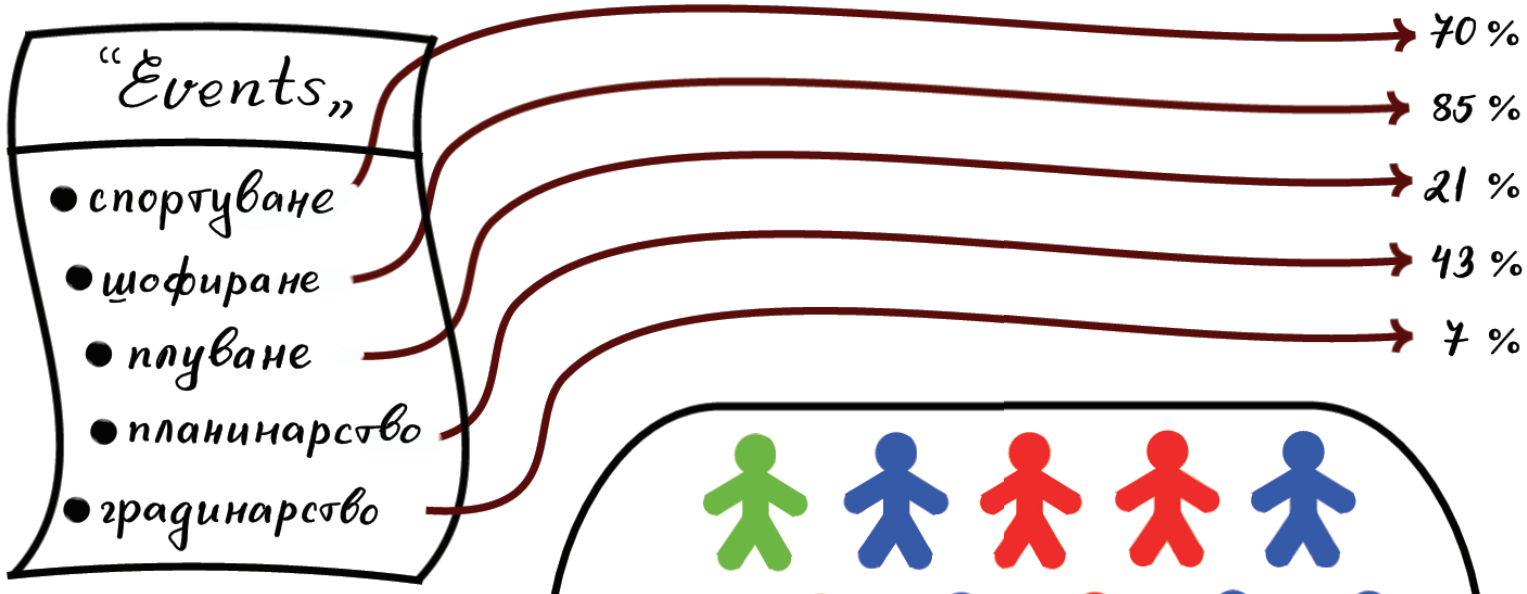



"Events"
спортуване
шофиране
плуване
планинарство
градинарство
70 %
85 %
21 %
43 %
7 %
в случая Events е въпросник/анкета
всеки отговаря на един въпрос
статистически ансамбъл
състояние := съответствието


"Events"
спортуване
шофиране
плуване
планинарство
градинарство
70 %
85 %
21 %
43 %
7 %
статистически ансамбъл 1
състояние 1

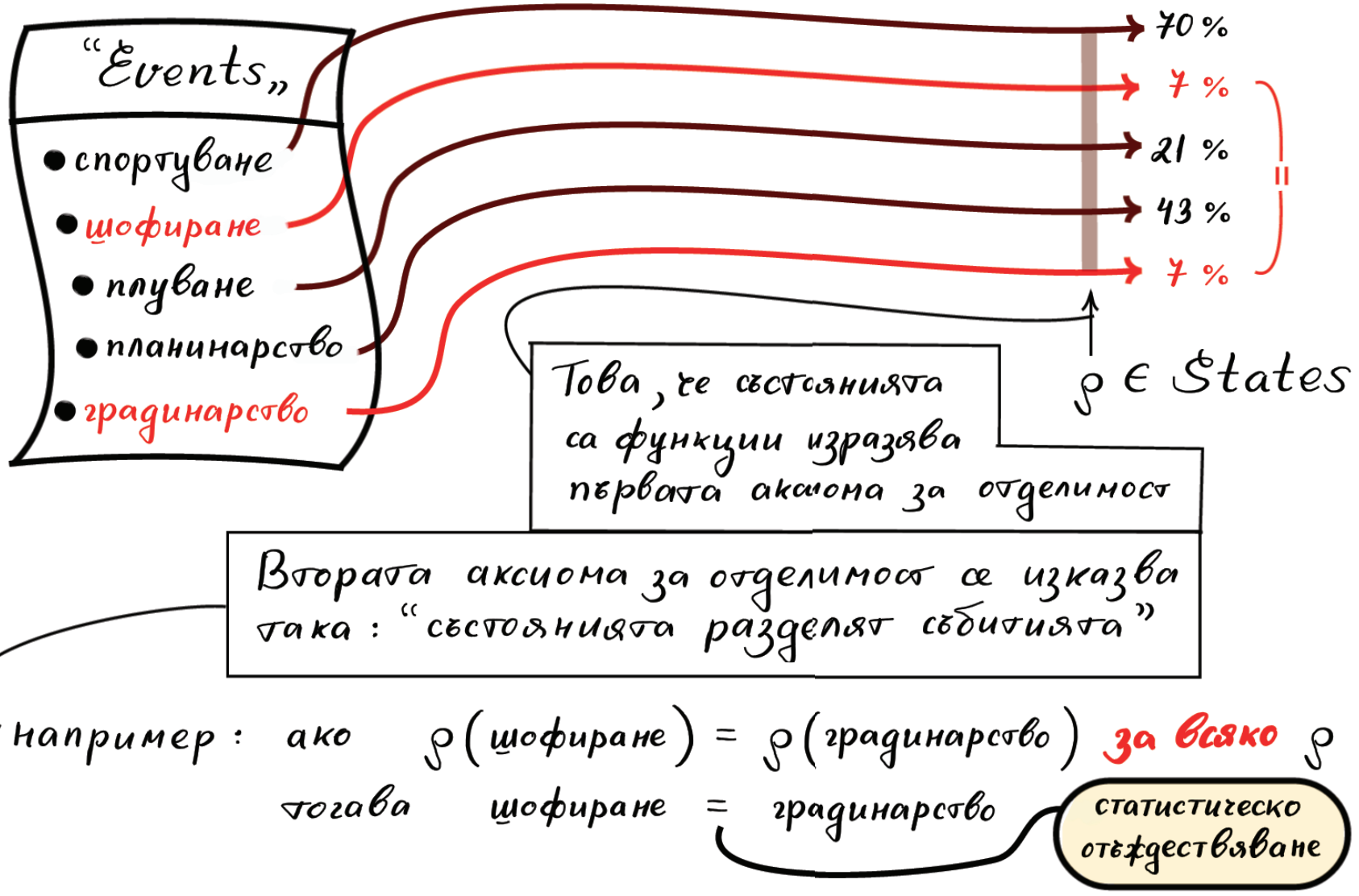

"Events"
спортуване
шофиране
плуване
планинарство
градинарство
54 %
42 %
10 %
71 %
3 %
статистически ансамбъл 2
състояние 2

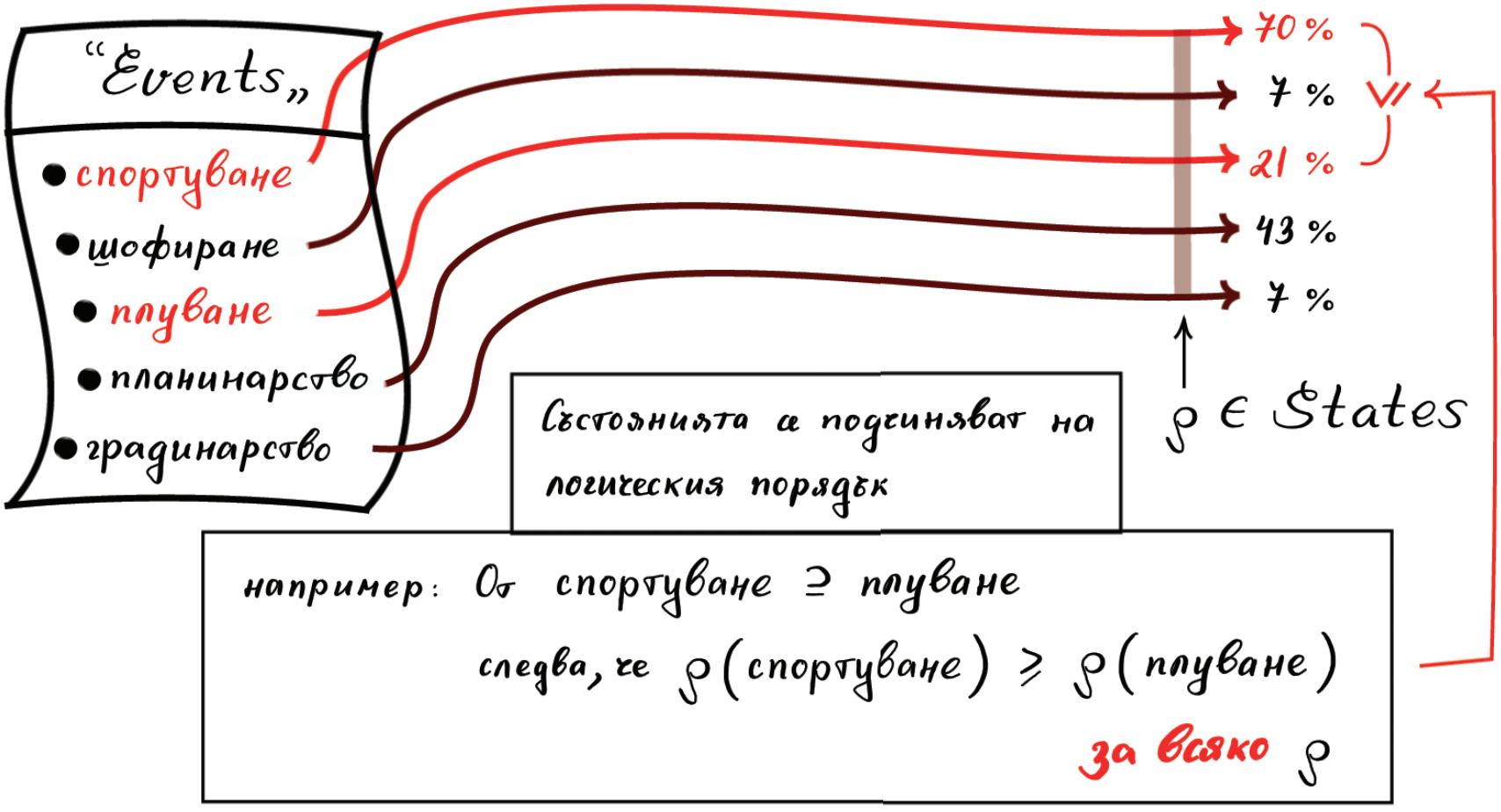

"Events"
спортуване
шофиране
плуване
планинарство
градинарство
81 %
73 %
50 %
74 %
2 %
статистически ансамбъл 3
състояние 3



Смесване : $1 = \frac{2}{16} + \frac{8}{16} + \frac{6}{16}$

$$\begin{pmatrix} 70\,\% \\ 85\,\% \\ 21\,\% \\ 43\,\% \\ 7\,\% \end{pmatrix} = \frac{2}{16}\begin{pmatrix} 96\,\% \\ 0\,\% \\ 88\,\% \\ 40\,\% \\ 0\,\% \end{pmatrix} + \frac{8}{16}\begin{pmatrix} 74\,\% \\ 98\,\% \\ 14\,\% \\ 46\,\% \\ 2\,\% \end{pmatrix} + \frac{6}{16}\begin{pmatrix} 56\,\% \\ 96\,\% \\ 8\,\% \\ 40\,\% \\ 16\,\% \end{pmatrix}$$


"Events"
спортуване
шофиране
плуване
планинарство
градинарство
70 %
7 %
21 %
43 %
7 %
ρ ∈ States
Това, че състоянията са функции изразява първата аксиома за отделимост
Втората аксиома за отделимост се изказва така: "състоянията разделят събитията"
например: ако ρ(шофиране) = ρ(градинарство) за всяко ρ
тогава шофиране = градинарство
статистическо отъждествяване



Забележка: От аксиомите ще следва твърдението и в обратната посока.

Някои общи водещи принципи в изграждането на теорията

Водеща роля в теоретичния модел ще играе множеството на събитията Events

То ще изразява нашата "сетивност" (способностите на наблюдателя за измерване).

По такъв начин Events ще трябва еднозначно да определи States: състоянията на изследваните обекти не са им "вътрешно присъщи", а изразяват отклика на обектите на нашите измервания.

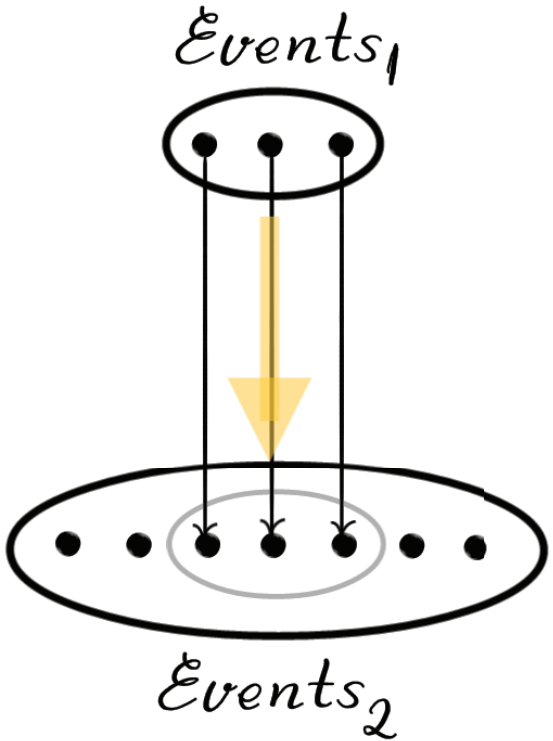
Формално-аксиоматично, ние ще определим States като всевъзможните "вероятностни разпределения" върху Events. От тук ще следва, че States е изпъкнало подмножество на линейното пространство от функции върху Events. Така, аксиомата за смесването ще бъде автоматично изпълнена.

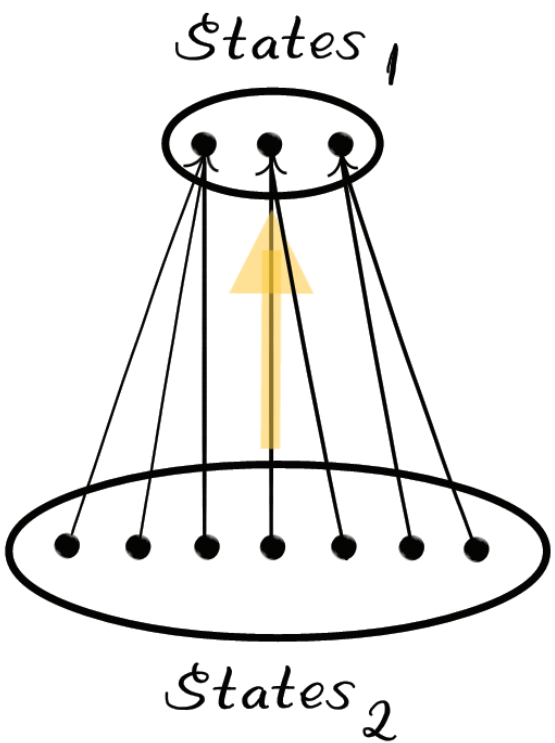
Някои общи водещи принципи в изграждането на теорията

повече подробности – аксиоми III

Възможно е разширение на Events.

Това ще наричаме "надсистема", а в обратната посока: "подсистема".





Някои общи водещи принципи в изграждането на теорията

В Events ще имаме логическа структура – квантовата логика на Биркхоф и фон Нойман

Ще имаме:

Установяването на събитие "P и Q" = Установяването на събитие "Q и P"

$\not\Vert$ $\not\Vert$

1. Установяване на P
2. Установяване на Q

$\neq$

1. Установяване на Q
2. Установяване на P

Някои общи водещи принципи в изграждането на теорията

В Events ще имаме логическа структура – квантовата логика на Биркхоф и фон Нойман

Ще имаме:

плуване и риболов ?	=	риболов и плуване ?
⫫		⫫
1. плуване ? 2. риболов ?	≠	1. риболов ? 2. плуване ?

Пример от социологията

Квантова { социология / психология / икономика ?

Защо не , но ...

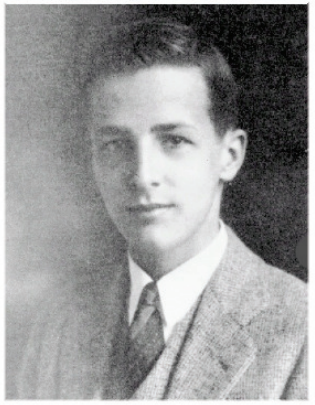
нужна е сериозна експериментална обосновка

и ... линейна алгебра ...

Бърз преглед на квантово-логическия подход до края

а) Квантовата логика на Биркхоф и фон Нойман

http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/BVN1936.pdf



(1911 – 1996)

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

(1903 – 1957)

1. **Introduction.** One of the aspects of quantum theory which has attracted the most general attention, is the novelty of the logical notions which it presupposes. It asserts that even a complete mathematical description of a physi-

Основен обект за математическо моделиране са "експерименталните твърдения / сведения" ("experimental propositions"), за които можем да си мислим като за експериментални тестове, чийто резултати са "да" ("1") или "не" ("0").

Наричаме ги също (експериментални) "събития" и ще ги бележим с $P, Q, R \ldots$
Казваме: "събитието P е (респ., не е) установено" и пишем "$P = 1$" (респ., "$P = 0$").

Събитията формират множеството Events

Изходната математическа структура върху множеството на всички събития е на частична наредба. Тя изразява елементарното логическо следствие между събития

$$P \preccurlyeq Q \quad \Leftrightarrow \quad \begin{cases} \text{"}P = 1\text{"} & \Rightarrow \text{ "}Q = 1\text{"} \\ \text{"}Q = 0\text{"} & \Rightarrow \text{ "}P = 0\text{"} \end{cases}$$

The experimental propositions concerning any system in classical mechanics, correspond to a "field" of subsets of its phase-space. More precisely: To the "quotient" of such a field by an ideal in it. At any rate they form a "Boolean Algebra."[9]

p.826

DEFINITION: A partially ordered system L will be called a "lattice" if and only if to any pair x and y of its elements there correspond

S5: A "meet" or "greatest lower bound" $x \cap y$ such that (5a) $x \cap y \subset x$, (5b) $x \cap y \subset y$, (5c) $z \subset x$ and $z \subset y$ imply $z \subset x \cap y$.

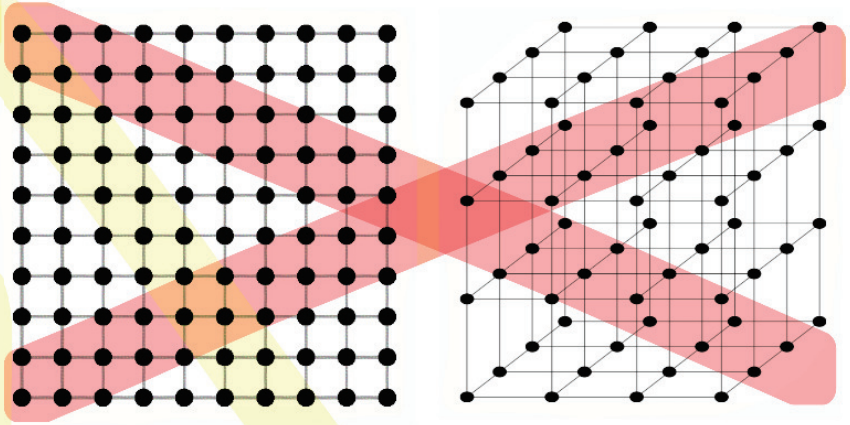
S6: A "join" or "least upper bound" $x \cap^{\vee} y$ satisfying (6a) $x \cup y \supset x$, (6b) $x \cup y \supset y$, (6c) $w \supset x$ and $w \supset y$ imply $w \supset x \cup y$.

p.829

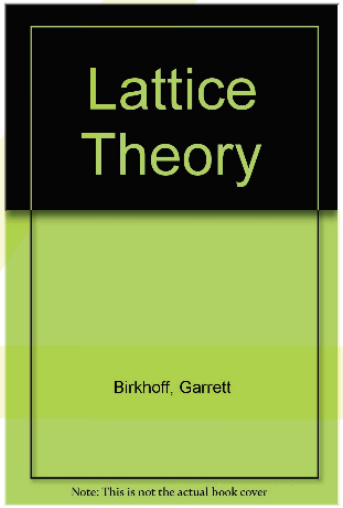
В решетка: $P \wedge Q = P \Leftrightarrow P \preccurlyeq Q$ (пишем: $\wedge$ вместо $\cap$),

$P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$ (пишем: $\vee$ вместо $\cup$).

Внимание: тук термина "решетка" / "lattice" няма нищо общо с решетките в геометрията



Допълнителна литература:



. . .

http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/B_LT.pdf

Закони на квантовата логика

$P \wedge Q = P \Leftrightarrow P \preccurlyeq Q$,
$P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$,
} задават връзките $\wedge \leftrightarrow \preccurlyeq \leftrightarrow \vee$

$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$, $P \vee (Q \vee R) = (P \vee Q) \vee R$,
$P \wedge Q = Q \wedge P$, $P \vee Q = Q \vee P$,
$P \vee (P \wedge Q) = P$, $P \wedge (P \vee Q) = P$,
$P \wedge P = P$, $P \vee P = P$,
} аксиоми на решетка

$P \wedge 0 = 0$, $P \vee 0 = P$, $P \wedge 1 = P$, $P \vee 1 = 1$,
} единица 1 и нула 0

$(P^{\perp})^{\perp} = P$,
$P \vee P^{\perp} = 1$, $P \wedge P^{\perp} = 0$,
$(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$, $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$,
} аксиоми на отрицанието $\perp$

} орторешетка

Закони на класическата логика

$P \wedge Q = P \Leftrightarrow P \preccurlyeq Q$,
$P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$,
} задават връзките $\wedge \leftrightarrow \preccurlyeq \leftrightarrow \vee$

$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$, $P \vee (Q \vee R) = (P \vee Q) \vee R$,
$P \wedge Q = Q \wedge P$, $P \vee Q = Q \vee P$,
$P \vee (P \wedge Q) = P$, $P \wedge (P \vee Q) = P$,
$P \wedge P = P$, $P \vee P = P$,
} аксиоми на решетка

$P \wedge 0 = 0$, $P \vee 0 = P$, $P \wedge 1 = P$, $P \vee 1 = 1$,
} единица 1 и нула 0

$(P^{\perp})^{\perp} = P$,
$P \vee P^{\perp} = 1$, $P \wedge P^{\perp} = 0$,
$(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$, $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$,
} аксиоми на отрицанието $\perp$

} орторешетка

$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$, $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$, } дистрибутивност

Закони на класическата логика

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

$P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$,

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

$P \wedge Q = Q \wedge P$, $P \vee Q = Q \vee P$,

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

$P \wedge P = P$, $P \vee P = P$,

$P \wedge 0 = 0$, $P \vee 0 = P$, $P \wedge 1 = P$, $P \vee 1 = 1$,

$(P^{\perp})^{\perp} = P$,

$P \vee P^{\perp} = 1$, $P \wedge P^{\perp} = 0$,

$(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$, $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$,

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

задават връзките $\wedge \leftrightarrow \preccurlyeq \leftrightarrow \vee$

аксиоми на решетка

единица 1 и нула 0

аксиоми на отрицанието $\perp$

орторешетка

дистрибутивност

БУЛЕВА АЛГЕБРА

Закони на квантовата логика

$P \wedge Q = P \Leftrightarrow P \preccurlyeq Q$,
$P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$,
} задават връзките $\wedge \leftrightarrow \preccurlyeq \leftrightarrow \vee$

$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$, $P \vee (Q \vee R) = (P \vee Q) \vee R$,
$P \wedge Q = Q \wedge P$, $P \vee Q = Q \vee P$,
$P \vee (P \wedge Q) = P$, $P \wedge (P \vee Q) = P$,
$P \wedge P = P$, $P \vee P = P$,
} аксиоми на решетка

$P \wedge 0 = 0$, $P \vee 0 = P$, $P \wedge 1 = P$, $P \vee 1 = 1$,
} единица 1 и нула 0

$(P^{\perp})^{\perp} = P$,
$P \vee P^{\perp} = 1$, $P \wedge P^{\perp} = 0$,
$(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$, $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$,
} аксиоми на отрицанието $\perp$

} орторешетка

~~$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$, $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$,~~ } дистрибутивност

Закони на квантовата логика

$P \wedge Q = P \Leftrightarrow P \preccurlyeq Q$, $P \vee Q = Q \Leftrightarrow P \preccurlyeq Q$ } задават връзките $\wedge \leftrightarrow \preccurlyeq \leftrightarrow \vee$

НАКРАТКО:

Законите на квантовата логика включват тези на класическата логика, с изключение на законите на дистрибутивност

$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$, $P \vee (Q \vee R) = (P \vee Q) \vee R$, } аксиоми на решетка

$P \vee (P \wedge Q) = P$, $P \wedge (P \vee Q) = P$, } аксиоми на решетка

$P \wedge 0 = 0$, $P \vee 0 = P$, $P \wedge 1 = P$, $P \vee 1 = 1$, } единица 1 и нула 0

$P \vee P^{\perp} = 1$, $P \wedge P^{\perp} = 0$, } аксиоми на отрицанието $\perp$

$(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$, $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$, } ортомодулна решетка

~~$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$, $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$,~~ } дистрибутивност

б) Геометрия на квантовата логика

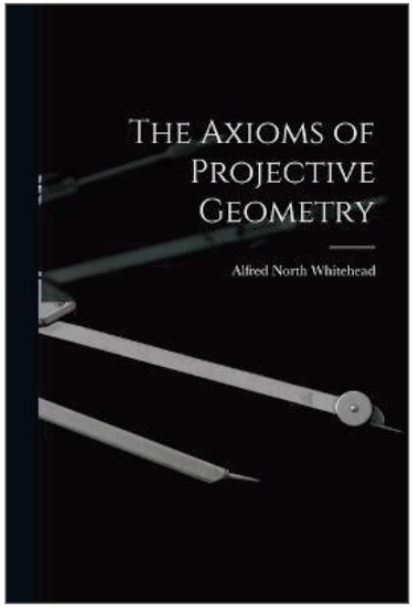
Определения ■ $P \lessdot Q \underset{\text{опр.}}{\iff} P \overset{\neq}{\preccurlyeq} Q$ и от $P \preccurlyeq R \preccurlyeq Q$ следва, че $P = R$ или $R = Q$.

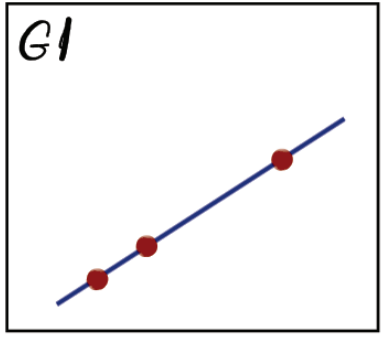
"Q покрива P"

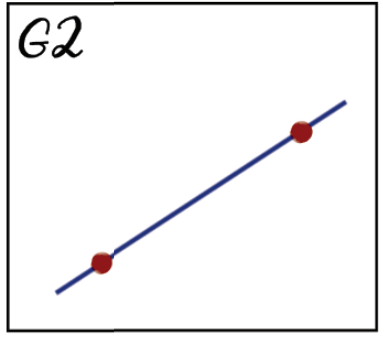
■ P е елементарно събитие $\underset{\text{опр.}}{\iff} 0 \lessdot P$

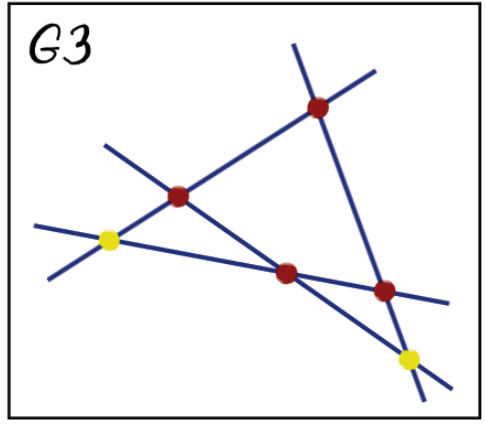
■ Обявяваме елементарните събития P за "точки на геометрия", а събитията L, които покриват елементарни събития обявяваме за "прави на геометрия" и казваме, че: "P лежи на L" $\underset{\text{опр.}}{\iff} P \preccurlyeq L$.

Тогава, при определени допълнителни аксиоматични предположения за орторешетката на събитията следва, че полученото геометрично пространство ще изпълнява т. нар. аксиоми на Уайтхед (Whitehead) на проективната геометрия

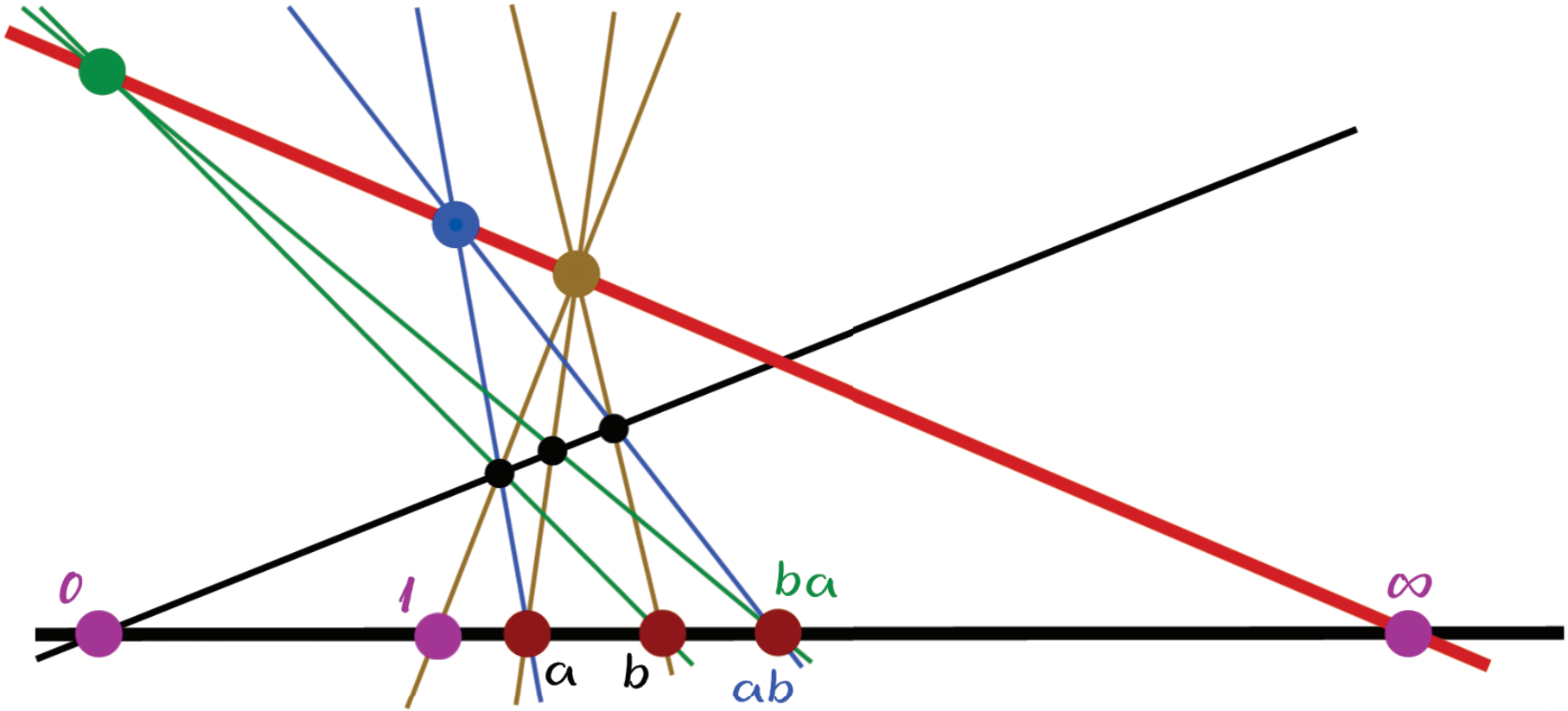






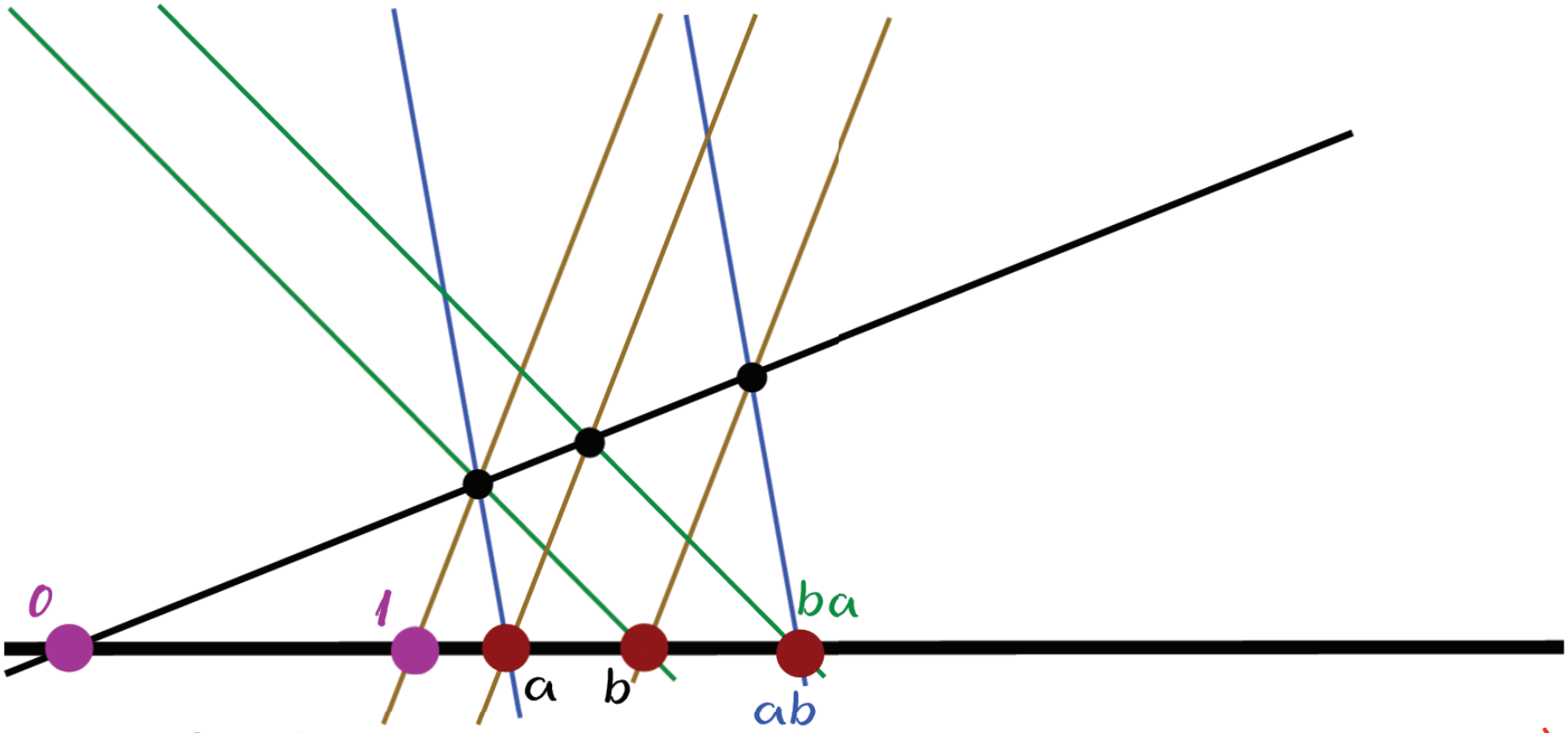


Аритметика в проективната геометрия : произведение



Всяка права с белязани три точки става тяло (поле, евентуално некомутативно)

Аритметика в проективната геометрия : произведение



Всяка права с белязани три точки става тяло (поле, евентуално некомутативно)

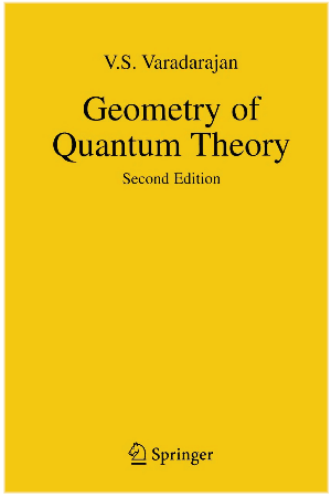
Основните модели на орторешетките "Events" на квантовите събития са от вида:

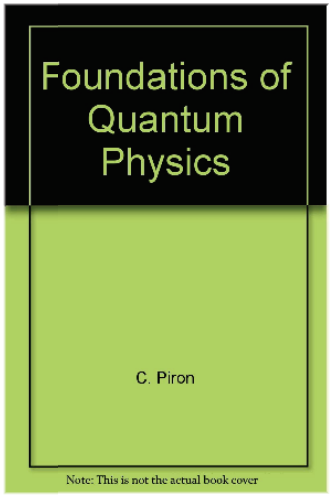
$Events := \mathcal{L}(\mathcal{H}) :=$ множеството на всички (затворени) линейни подпространства на (комплексно) хилбертово пространство $\mathcal{H}$ с частичната наредба на включване $\subseteq$ и $\perp :=$ ортогоналното допълнение

$\mathcal{L}$ — алтернативно означение

"хилбертово пространство на състоянията"

Възможни са и по-общи модели





http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/Varadarajan.pdf
http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/Piron.pdf

в) Заключителни аксиоми за квантовите събития

Аксиома за орто-модулярност : Ако $P \preccurlyeq Q$ тогава $P \vee (Q \wedge P^{\perp}) = Q$

Закон за покриването : Ако $0 \lessdot P$ и $P \wedge Q = 0$ тогава $Q \lessdot P \vee Q$

Аксиома за крайност: $\exists\, N \in \mathbb{N} : 0 \lessdot P_1 \lessdot P_2 \lessdot \cdots \lessdot P_{N-1} \lessdot 1$

Това са всички структуро-определящи аксиоми на квантовата теория.
Останалите аксиоми са по-скоро определения на допълнителни понятия
(с изключение на постулата за измерването)

Формална част

Аксиоми на квантово-логическия подход – продължение

Логическата наредба между събитията

Въвеждаме бинарна релация в множеството на събитията $\boldsymbol{\mathcal{Events}}$:
за $P, Q \in \boldsymbol{\mathcal{Events}}$ нека

$P \preccurlyeq Q$ се определя чрез условието,
че за всички състояния $\rho, \sigma \in \boldsymbol{\mathcal{States}}$,
от $Prob_\rho(P) = 1$ следва, че $Prob_\rho(Q) = 1$,
от $Prob_\sigma(Q) = 0$ следва, че $Prob_\sigma(P) = 0$.

Когато $P \preccurlyeq Q$ ще казваме, че

събитието P **се мажорира от** събитието Q.

Синоними: $Q \succcurlyeq P$, "Q *мажорира* P", "P *се съдържа в* Q",
"Q *съдържа* P", "*от* P *следва* Q", "Q *следва от* P".

Непосредствени следствия (чисто логически):

(рефлексивност) за всяко събитие P имаме: $P \preccurlyeq P$;

(транзитивност) за всеки три събития P, Q и R имаме че:
от $P \preccurlyeq Q$ и $Q \preccurlyeq R$ следва $P \preccurlyeq R$.

Като поредна *аксиома* налагаме следното свойство:

(антисиметрия) за всеки две събития P и Q имаме че:
от $P \preccurlyeq Q$ и $Q \preccurlyeq P$ следва $P = Q$.

Еквивалентно, $P = Q \Leftrightarrow \begin{cases} Prob_\rho(P) = 1 \Leftrightarrow Prob_\rho(Q) = 1 \ (\forall \rho)\,, \\ Prob_\sigma(P) = 0 \Leftrightarrow Prob_\sigma(Q) = 0 \ (\forall \sigma)\,. \end{cases}$

Изказана с думи горната аксиома гласи, че ако P, респективно, настъпва или не настъпва, тогава и само тогава, когато Q настъпва или не настъпва, то тогава P и Q са едно и също събитие. Новата аксиомата засилва втората аксиома за отделимост, както непосредствено се вижда от еквивалентната формулировка.

И така, свойствата на релацията $\preccurlyeq$ са:

(рефлексивност) за всяко събитие P имаме: $P \preccurlyeq P$;

(транзитивност) за всеки три събития P, Q и R имаме че: от $P \preccurlyeq Q$ и $Q \preccurlyeq R$ следва $P \preccurlyeq R$;

(антисиметрия) за всеки две събития P и Q имаме че: от $P \preccurlyeq Q$ и $Q \preccurlyeq P$ следва $P = Q$.

По такъв начин, множеството $\mathscr{Events}$, снабдено с релацията $\preccurlyeq$, се превръща в *частично наредено множество* (partially ordered set = poset), тъй като (нека припомним, че) горните три свойствата се явяват дефиниционни за това.

В следствие на допълнителни аксиоми ще получим усилването:

$P \preccurlyeq Q$ тогава и само тогава, когато
за всяко състояние $\rho \in \boldsymbol{States}$: $Prob_\rho(P) \leqslant Prob_\rho(Q)$

За класическите системи, когато $\boldsymbol{\mathscr{Events}} = \mathscr{P}(\Omega)$, релацията $\preccurlyeq$ е просто релацията на включване на едно подмножество в друго:

$$P \preccurlyeq Q \quad \Longleftrightarrow \quad P \subseteq Q$$

за всеки $P, Q \subseteq \Omega$ (т.е., $P, Q \in \mathscr{P}(\Omega) = \boldsymbol{\mathscr{Events}}$).

За квантовите системи, когато $\boldsymbol{\mathscr{Events}} = \mathfrak{L}(\mathbb{C}^n)$, релацията $\preccurlyeq$ е отново релацията на включване, но едно линейно подпространство в друго:

$$V \preccurlyeq W \quad \Longleftrightarrow \quad V \subseteq W$$

за всеки $V, W \underset{\text{лин.}}{\subseteq} \mathbb{C}^n$ (т.е., $V, W \in \mathfrak{L}(\mathbb{C}^n) = \boldsymbol{\mathscr{Events}}$).

Аксиома за нулата и единицата:

> в частично наредената множество на всички събития съществуват *най-голям* и *най-малък* елемент.

Последните ще означаваме с **0** (**нула**) и **1** (**единица**), съответно.
невъзможното събитие винаги изпълненото събитие

Написано с формули: за всяко събитие $P \in \boldsymbol{Events}$ имаме:

$$\mathbf{0} \preccurlyeq P \preccurlyeq \mathbf{1}\,.$$

От допълнителните аксиоми по-нататък ще следва, че:

$P = \mathbf{0}$ тогава и само тогава, когато
за всяко състояние $\rho \in \boldsymbol{States}$: $Prob_\rho(P) = 0\,.$

и също $P = \mathbf{1}$ тогава и само тогава, когато
за всяко състояние $\rho \in \boldsymbol{States}$: $Prob_\rho(P) = 1\,.$

За класическите системи (когато $\boldsymbol{\mathscr{Events}} = \mathscr{P}(\Omega)$):

$$\begin{aligned}\mathbf{0} &= \emptyset \in \mathscr{P}(\Omega)\ (= \boldsymbol{\mathscr{Events}})\,,\\ \mathbf{1} &= \Omega \in \mathscr{P}(\Omega)\ (= \boldsymbol{\mathscr{Events}})\,.\end{aligned}$$

За квантовите системи (когато $\boldsymbol{\mathscr{Events}} = \mathfrak{L}(\mathbb{C}^n)$):

$$\begin{aligned}\mathbf{0} &= \{0\} \in \mathfrak{L}(\mathbb{C}^n)\ (= \boldsymbol{\mathscr{Events}})\,,\\ \mathbf{1} &= \mathbb{C}^n \in \mathfrak{L}(\mathbb{C}^n)\ (= \boldsymbol{\mathscr{Events}})\,.\end{aligned}$$

Логическите операции "*и*" и "*или*" за събития

Всяко частично наредено множество допуска формулирането на логическите операции "*и*" и "*или*" посредством понятията за

инфимум (или още, *точна долна граница*) и
сюпремум (*точна горна граница*), съответно.

Нашата следваща *аксиома* е, че

> в множеството на всички събития съществуват инфимумите и сюпремумите на произволни подмножества от събития.

Припомняне: ако $(\mathscr{T}, \preccurlyeq)$ е едно частично наредено множество и $S \subseteq \mathscr{T}$, то **инфимум** на S се определя като:

$$\wedge S\,(\equiv \inf S) := a \quad \Longleftrightarrow \quad \begin{cases} \forall x \in S \,:\, a \preccurlyeq x \\ \forall y \in \mathscr{T} \,:\, (\forall x \in S \,:\, y \preccurlyeq x) \Rightarrow y \preccurlyeq a\,. \end{cases}$$

Изказано с думи, a е най-големия елемент в множеството на всички елементи y, които са по-малки от всеки елемент x на S.

Дуално понятие е **сюпремума**:

$$\vee S\,(\equiv \sup S) := a \quad \Longleftrightarrow \quad \begin{cases} \forall x \in S \,:\, x \preccurlyeq a \\ \forall y \in \mathscr{T} \,:\, (\forall x \in S \,:\, x \preccurlyeq y) \Rightarrow a \preccurlyeq y\,. \end{cases}$$

Изказано с думи, a е най-малкия елемент в множеството на всички елементи y, които са по-големи от всеки елемент x на S.
Подчертаваме, че елементите $\wedge S$ и $\vee S$ не винаги съществуват.
Доказва се обаче, че *ако съществуват* $\wedge S$ *или* $\vee S$, *то определенията по-горе ги дефинират еднозначно.*

Забележка: Нека отбележим, че ако частично наредената множество $(\mathscr{T}, \preccurlyeq)$ има нула и единица, то

- $\wedge\emptyset = \mathbf{1}, \quad \vee\emptyset = \mathbf{0}, \quad \wedge\mathscr{T} = \mathbf{0}, \quad \vee\mathscr{T} = \mathbf{1}.$
- $\vee S = \wedge\{y \in \mathscr{T} \,|\, \forall x \in S : x \preccurlyeq y\}.$
- $\wedge S = \vee\{y \in \mathscr{T} \,|\, \forall x \in S : y \preccurlyeq x\}.$

В математиката, частично наредени множества, в които произволни, непразни, крайни подмножества от елементи имат сюпремум и инфимум, се наричат *решетки* (наредбени)(**lattice**).

Ако в решетка съществуват сюпремумите и инфимумите на произволни подмножества, тогава решетката се нарича *пълна* (**complete lattice**).

По такъв начин, аксиомите формулирани до тук могат да се свият просто до формулировката, че *множеството на събитията* $\mathbb{Events}$ *е пълна решетка с нула и единица, спрямо операцията* "$\preccurlyeq$", *в качеството на частична наредба.*

Особено важен случай е, когато имаме инфимум и сюпремум на множество от два елемента. За $P, Q \in \boldsymbol{\mathscr{Events}}$ полагаме:

$$P \wedge Q \ \ (\equiv \ \ P \textit{ и } Q \ \ ) := \wedge\{P, Q\}\,,$$
$$P \vee Q \ \ (\equiv P \textit{ или } Q\,) := \vee\{P, Q\}$$

и по-нататък ние основно ще използваме означения "$\wedge$" и "$\vee$" за обозначаване на логическите операции "*и*" и "*или*" между събитията, съответно.

По-нататък, операциите "$\wedge$" и "$\vee$" ще наричаме също **решетъчни операции**.

"$\wedge$" и "$\vee$" могат да се разглеждат, като бинарни операции..

За класическите системи множеството на събитията, което е степенното множество, е пълна решетка.

В този случай решетъчните операции "$\wedge$" и "$\vee$" съвпадат с теоретико-множествените операции сечение "$\cap$" и обединение "$\cup$", съответно:

$$P \wedge Q = P \cap Q\,, \quad P \vee Q = P \cup Q$$

за всеки $P, Q \in \boldsymbol{\mathscr{Events}} = \mathscr{P}(\Omega)$ (класическа система).

Аксиома за отрицанието:

> за всяко събитие P съществува събитие Q такова, че Q се случва (наблюдава) тогава и само тогава, когато P не се случва, както и P се случва тогава и само тогава, когато Q не се случва.

Написано с формула това условие изглежда така: за всяко състояние $\rho \in \boldsymbol{States}$ имаме следните еквивалентности:

$$\begin{aligned} Prob_\rho(P) = 1 \quad &\Longleftrightarrow \quad Prob_\rho(Q) = 0\,, \\ Prob_\rho(P) = 0 \quad &\Longleftrightarrow \quad Prob_\rho(Q) = 1 \end{aligned}$$

От аксиомата за наредбата следва, че събитието Q е еднозначно определено от събитието P.

Ще казваме, че Q **е отрицание на събитието** P и ще пишем:

$$Q =: P^\perp \, (\equiv \textit{ не } P)\,.$$

Следствие: $$P_1 \preccurlyeq P_2 \quad \Longrightarrow \quad P_2^{\perp} = P_1^{\perp}\,.$$

От останалите аксиоми по-нататък ще покажем, че:

$$Prob_\rho\left(P^{\perp}\right) = 1 - Prob_\rho(P)$$

за всички $P \in \boldsymbol{\mathscr{Events}}$ и $\rho \in \boldsymbol{\mathscr{States}}$.

За класическите системи отрицанието е теоретико-множественото допълнение:

$$P^{\perp} = \Omega \setminus P$$

за всеки $P, Q \in \boldsymbol{\mathscr{Events}} = \mathscr{P}(\Omega)$ (класическа система).

Общи закони на съждителното (пропозиционалното) смятане за събития

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

тъждества за *асоциативност*;

$$P \wedge Q = Q \wedge P\,, \quad P \vee Q = Q \vee P\,,$$

тъждества за *комутативност*;

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

тъждества за "*поглъщането*";

$$P \wedge P = P = P \vee P\,,$$

тъждества за *идемпотентност*;

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

обратна характеризация на релацията на частична наредба $\preccurlyeq$ посредством операциите $\wedge$ или $\vee$;

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

идемпотентността на отрицанието;

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

закон за изключеното трето и др.;

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

законите на де Морган.

(за всеки $P, Q, R \in \boldsymbol{\mathcal{E}vents}$).

Това са законите за класическото съждително смятане, от които са изпуснати само *законите за дистрибутивност*:

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

В общия случай, това което следва вместо тъждествата за дистрибутивност, са неравенства:

$$P \wedge (Q \vee R) \succcurlyeq (P \wedge Q) \vee (P \wedge R)\,,$$
$$P \vee (Q \wedge R) \preccurlyeq (P \vee Q) \wedge (P \vee R)$$

В алгебрата, множество с бинарни операции "$\wedge$" и "$\vee$" и едномесна операция "$\perp$", в което изпълняват тъждествата от предната страница, се нарича **орто-решетка**. Така, аксиомите до тук могат на кратко да се изкажат така:
множеството $\mathscr{Events}$ *на квантовите събития е орто-решетка (спрямо релацията "*$\preccurlyeq$*" и операциите "*$\wedge$*" и "*$\vee$*").*

Аксиома за орто-модуларност

(закон за орто-модуларност)

ако $P \preccurlyeq Q$ тогава $P \vee (P^{\perp} \wedge Q) = Q$

за всеки две събития $P, Q \in \boldsymbol{\mathscr{Events}}$.

Може да се разглежда, като специален случай на дистрибутивност понеже: $P \vee (P^{\perp} \wedge Q) = (P \vee P^{\perp}) \wedge (P \wedge Q) = \mathbf{1} \wedge Q = Q\,.$

В алгебрата: ... това са **орто-модуларни решетки**.

В една класическа система:
за събития P, Q, ако $P \preccurlyeq Q$, то $Q \wedge P^{\perp}$ е допълнението на P в Q, $Q \setminus P := P^{\perp} \wedge Q$. Пренесяме това и в общи орто-модулари решетки. Така, закона за орто-модуларност приема вида:

ако $P \preccurlyeq Q$ тогава $P \vee (Q \setminus P) = Q\,.$

Състоянията като вероятности върху орто-решетката на събитията

Завършващи аксиоми за състоянията в общите системи:

> Всяко състояние $\rho \in \mathbb{States}$ изпълнява свойствата:
>
> адитивност $\rho(Q) = \rho(P) + \rho(Q \setminus P)\,,$ за всеки две събития P, $Q \in \mathbb{Events}$, за които $P \preccurlyeq Q$;
>
> нормираност $\rho(\mathbf{1}) = 1\,.$

→ Вероятност върху орто-решетка.
Множеството на на всички вероятностти върху орто-решетка е изпъкнало.

> За всяко *ненулево* събитие $P \in \mathbb{Events}$ съществува състояние $\rho \in \sigma$, в което P настъпва почти сигурно, т.е., $Prob_\rho(P) = 1$.

По-нататък ще покажем, че от аксиомите следва, че $\mathbb{States}$ съвпада с множеството на всички вероятностти върху орто-решетката $\mathbb{Events}$.
Така, структуро-определяща е именно орто-решетката на събитията $\mathbb{Events}$

Определение. Елементарно събитие е събитие $P \in \mathscr{Events}$, такова, че за всяко друго събитие $Q \in \mathscr{Events}$ следва, че:

$$Q \preccurlyeq P \quad \Longrightarrow \quad Q = \mathbf{0} \text{ или } Q = P\,.$$

В теорията на частично наредените множества с *най-малък елемент* (и в частност, решетките с $\widehat{0}$ и $\widehat{1}$) горното свойство определя понятието **атом в частично наредено множество**. Така, *елементарните събития – това са атомите на решетката на събитията.*

Аксиома за атомарност:

- всяко ненулево събитие мажорира поне едно елементарно събитие.

Определение на ниво на събитие.

Нулевото събитие и само то има **ниво нула**. За едно *ненулево* събитие P, казваме че има **крайно ниво**, ако всяка верига

$$\begin{gathered} 0 = P_0 \preccurlyeq P_1 \preccurlyeq P_2 \preccurlyeq \cdots \preccurlyeq P_r = P \\ P_0 \neq P_1 \neq P_2 \neq \cdots \neq P_r \end{gathered}$$

е *крайна* и в множеството на тези вериги има такива с *най-голяма дължина* r.

Числото $r \geqslant 1$ се нарича **ниво на ненулевото събитие** P.

Ясно е, че *елементарните събития са тези и само тези събития, които са от ниво* 1.

Системата наричаме от **система от крайно ниво** или още **крайна система**, ако *единицата* $\mathbf{1}$ *има крайно ниво.*

Тогава нивото на единицата ще наричаме **ранг на системата**.

Аксиома за крайност:

Всички системи на квантовата информатика са крайни.

Това е равносилно на твърдението, че *всички събития имат крайно ниво.*

Едни от най-фундаменталните системи на квантовата информатика са системите от ниво 2: това е **системата на един бит**.

По-нататък в този курс ще покажем, че *в следствие на аксиомите ни, има* по същество *точно две системи от ниво две*: *това са* класическия *и* квантовия *бит*.

Последния се нарича също ***q*-бит**

Определение. В едно частично наредено множество $\mathscr{T}$ и два негови елемента $a, b \in \mathscr{T}$ казваме, че

$$b \textbf{ покрива } a, \text{ ако } a \preccurlyeq b,\ a \neq b \text{ и за всеки елемент } c \in \mathscr{T},$$
$$a \preccurlyeq c \preccurlyeq b \implies a = c \text{ или } b = c\,.$$

Така, твърдението, че a е атом на частично наредено множество $\mathscr{T}$ с най-малък елемент $\mathbf{0} \in \mathscr{T}$ е равносилно на изказването, че a покрива $\mathbf{0}$.

Последната аксиома е известна също, като **закон за покриването**:

> Ако P е елементарно събитие, а Q е събитие, такова че $P \wedge Q = \mathbf{0}$, тогава $P \vee Q$ *покрива* Q.

Еквивалентно, *ако* P *е елементарно събитие, а* Q *е събитие, такова че* $P \wedge Q = \mathbf{0}$, *тогава* $(P \vee Q) \wedge P^{\perp}$ *е елементарно събитие.*

Последната еквивалентност оставяме без доказателство.