

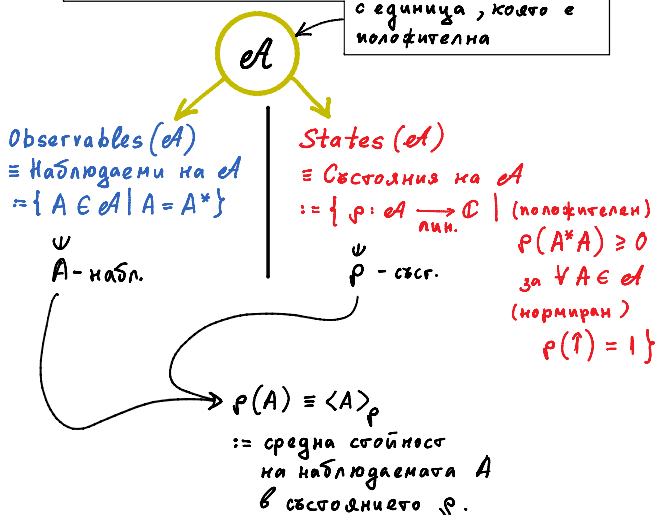
6 Теория на алгебричния подход

Нека си припомним, че съгласно аксиомите на алгебричния подход, алгебрата на наблюдаемите определя всичко в теорията: самите наблюдаеми и състоянията. Тя стои е “слънце” за теорията и ѝ дава всичко. Това схематично сме изобразили на долната фигура:

Схематично: в основата на всичко е

алгебра на наблюдаемите

- това е асоциативна, комплексна $\ast$ -алгебра, с единица, която е положителна



фиг. 40: Схема на алгебричния подход.

6.1 Положителността и нейните разновидности в курса

Положителността е аналога на логическата наредба в алгебричния подход и затова има фундаментално значение в теорията. В нашия курс имаме три различни понятия за положителност, които обаче са тясно свързани. Нека специално да ги споменем

в началото на развитието на теорията на алгебричния подход.

(а) Най-напред въведохме (точка 5.9) понятието за “положителност на цяла $*$ -алгебра $\mathcal{A}$ ”. Да припомним, че това означаваше, че за всеки $A_1, \dots, A_m \in \mathcal{A}$ от $A_1^* A_1 + \dots + A_m^* A_m = \widehat{0}$ следва, че $A_1 = \dots = A_m = \widehat{0}$.

(б) Второто понятие е за **неотрицателни елементи в $*$ -алгебра $\mathcal{A}$** : това са елементите на $\mathcal{A}$ от вида $A_1^* A_1 + \dots + A_m^* A_m$ за произволни $A_1, \dots, A_m \in \mathcal{A}$. В частност, *неотрицателните елементи са винаги самоспрегнати*, понеже $(A^* A)^* = A^* A^{**} = A^* A$. Така, неотрицателните елементи играят роля в условието за положителност на $*$ -алгебра, което може да се изкаже също и така: *във всяка $*$ -алгебра $\mathcal{A}$ нулата е неотрицателен елемент (понеже $\widehat{0}^* \widehat{0} = \widehat{0}$) и алгебрата $\mathcal{A}$ е положителна, ако сума на неотрицателни елементи е равна на нула, тогава и само тогава, когато всеки от тях е равен на нула*. И така, във всяка $*$ -алгебра има неотрицателни елементи (напр., нулата), но ако алгебрата не е положителна може да се окаже, че заедно с всеки неотрицателен елемент A , $-A$ е също неотри-

цателен! Изисква се известно усилие за да се намери $*$ -алгебра, която не е положителна, но такива все пак има.

Упражнение. (i) Покажете, че в положителна $*$ -алгебра, ако за неотрицателен елемент A противоположния елемент $-A$ е също неотрицателен, то $A = \hat{0}$.

(ii) Нека $\mathcal{A}$ е $*$ -алгебра, в която е изпълнено равенството $A^*A = -\hat{1}$, за някой елемент $A \in \mathcal{A}$. Покажете, че $\mathcal{A}$ не е положителна $*$ -алгебра. Покажете, че в този случай за всеки неотрицателен елемент A противоположния елемент $-A$ е също неотрицателен.⁶⁶

(iii) Постройте пример на $*$ -алгебра, която изпълнява предната подточка (ii) на упражнението. Например, разгледайте $Mat_2(\mathbb{C})$ само като асоциативна алгебра и я снабдете със звезда операция, различна от ермитовото спрягане, така че $Mat_2(\mathbb{C})$ да стане търсения пример.

(в) Третото понятие за положителност е понятието положителен линеен функционал над $*$ -алгебра $\mathcal{A}$ от точка 5.10. В светлината

⁶⁶ *Указание:* Използвайте, че ако $-\hat{1} = A^*A$ и $X = B^*B$, то $-X = (AB)^*(AB)$.

на определението от подточка (б) по-горе можем да кажем, че един линеен функционал $\rho : \mathcal{A} \rightarrow \mathbb{C}$ е положителен, ако изпраща неотрицателни елементи на алгебрата в неотрицателни числа. В частност, нулевия линеен функционал е положителен според това определение. Би било по-естествено, така определените положителни линейни функционали да се наричат *неотрицателни*. В литературата обаче има известна утвърденост на термина “положителен линеен функционал”, така както беше определен. По-нататък ще срещнем и едно усиляване на понятието за положителен линеен функционал: линейния функционал $\rho : \mathcal{A} \rightarrow \mathbb{C}$ се нарича **строго положителен**, ако от $\rho(A^*A) = 0$ следва, че и $A = \hat{0}$ за всяко $A \in \mathcal{A}$.

Забележете, че в примера от упражнението по-горе (подточки (ii) и (ii)) следва, че за такава неположителна $*$ -алгебра единствения положителен линеен функционал е нулевия (докажете го за упражнение). Ако това би била алгебра на наблюдаемите, то тя не би допускала никакви състояния (понеже нулевия функционал не е нормиран). Това обяс-

нява изключителното значение на условието за положителност на алгебрата на наблюдаемите в аксиомите на алгебричния подход.

6.2 Подалгебри, морфизми и изоморфизми на различните типове алгебри

6.2.1 Основните определения

Определение. Нека $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$ – полето на реалните или комплексните числа. Нека $\mathcal{A}$ е линейно пространство над $\mathbb{K}$, а $\mathcal{B} \subseteq \mathcal{A}$ е линейно подпространство.

- Ако $\mathcal{A}$ е алгебра, то $\mathcal{B}$ се нарича **подалгебра** на $\mathcal{A}$, ако $\mathcal{B}$ е затворено спрямо операцията произведение, т.е., ако заедно с всеки два свои елемента $A, B \in \mathcal{B}$, там се съдържа и произведението им: $AB \in \mathcal{B}$. В частност, $\mathcal{B}$ само по себе си е алгебра спрямо наследеното произведение.
- Ако $\mathcal{A}$ е алгебра с единица, то $\mathcal{B}$ се нарича **подалгебра с единица** на $\mathcal{A}$, ако в допълнение на горното условие $\hat{1} \in \mathcal{B}$.
- Ако $\mathcal{A}$ е $*$ -алгебра, то $\mathcal{B}$ се нарича $*$ -

подалгебра на $\mathcal{A}$, ако в допълнение на първото условие по-горе, от $A \in \mathcal{B}$ следва, че $A^* \in \mathcal{B}$ (т.е., $\mathcal{B}$ е затворено спрямо $*$ -операцията).

- За другите типове алгебри, като “асоциативни”, “комутативни”, “положителни” не са нужни повече условия: тези свойства преминават към подалгебрите, което се доказва непосредствено.
- При съчетаване на няколко типа алгебри, понятието за подалгебра на съчетания тип алгебра включва условията за всеки един от съчетаните типове.

И така, понятието за подалгебра, като вид “подструктура”, зависи от типа на алгебрите, които разглеждаме. По-късно, за типа структура ще въведем и термина “категория на (типа на) структурата”.

Следващото понятие, понятието за **морфизъм** при различните типове алгебри, е тясно свързано с предното (и всъщност, го обобщава).

Определение. Нека отново $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$ и нека $\mathcal{A}, \mathcal{B}$ са линейни пространства над $\mathbb{K}$, а

$f : \mathcal{A} \rightarrow \mathcal{B}$ е линейно изображение.

- Ако $\mathcal{A}$ и $\mathcal{B}$ са алгебри, то f се нарича **морфизъм на алгебри**, ако f запазва операцията произведение, т.е., ако за всеки два елемента $A, B \in \mathcal{A}$ имаме $f(AB) = f(A)f(B)$.
- Ако $\mathcal{A}$ и $\mathcal{B}$ са алгебри с единица, то f се нарича **морфизъм на алгебри с единица**, ако f в допълнение на горното условие запазва и единиците: $f(\hat{1}_{\mathcal{A}}) = \hat{1}_{\mathcal{B}}$, където $\hat{1}_{\mathcal{A}}$ и $\hat{1}_{\mathcal{B}}$ са единиците в $\mathcal{A}$ и $\mathcal{B}$, съответно (ние обаче не винаги ще слагаме отличителни знаци на единиците в различни алгебри за да не утежняваме означенията).
- Ако $\mathcal{A}$ и $\mathcal{B}$ са $*$ -алгебри, то f се нарича **морфизъм на $*$ -алгебри**, ако f в допълнение на първото условие запазва и $*$ -операциите: $f(A^*) = f(A)^*$.
- Отново, за другите типове алгебри, като “асоциативни”, “комутативни”, “положителни” не са нужни повече условия.
- При съчетаване на няколко типа алгебри, понятието за морфизъм на съчетания тип

алгебра включва условията за всеки един от съчетаните типове.

- В горните случаи, ако $f : \mathcal{A} \rightarrow \mathcal{B}$ е биекция, то казваме, че f е **изоморфизъм** на съответния тип алгебри. Това означаваме, като $f : \mathcal{A} \cong \mathcal{B}$ и казваме също, че $\mathcal{A}$ и $\mathcal{B}$ са **изоморфни** алгебри в съответния тип. По такъв начин, при изоморфни алгебри $\mathcal{A}$ и $\mathcal{B}$ имаме 1–1 съответствие, при което структурите на $\mathcal{A}$ и $\mathcal{B}$ се пренасят една в друга. В такъв смисъл, изоморфните алгебри са идентични (в рамките на дадения тип) и въобще, изоморфните обекти в математиката са идентични (неразличими, еднакви) от гледна точка на самата област, която ги изследва.
- В случая, когато $\mathcal{B} \subseteq \mathcal{A}$, а $f : \mathcal{B} \hookrightarrow \mathcal{A}$ е изображението на **влагане**, то получаваме съответствие с понятията за подалгебри от първото определение по-горе: $\mathcal{B}$ е подалгебра на $\mathcal{A}$, тогава и само тогава, когато **влагането** на $\mathcal{B}$ в $\mathcal{A}$ е морфизъм в съответния тип на алгебри.

Нека сега разгледаме примери на горните

ПОНЯТИЯ.

6.2.2 Основният пример: алгебрата на блочно-диагоналните матрици

Преди всичко ще въведем основния ни пример за подалгебра: (под)алгебрата на блочно-диагоналните матрици на матричната алгебра. Това ще бъде пример на $*$ -подалгебра с единица. В следващата точка (точка 6.3) ще видим значението на този пример на $*$ -алгебри с единица.

По определение, **блочно-диагонална матрица за наредено разбиване** $n = k_1 + \dots + k_m$ на числото n в сума на естествени числа е квадратна матрица от размер $n \times n$, в която редовете и стълбовете са последователно разбити на групи от по $k_1, \dots, k_m$ реда и стълба; в полученото блочно разбиване всички недиагонални блокове са нулеви, а диагоналните блокове са квадратни матрици $A_1, \dots, A_m$ от размери $k_1 \times k_1, \dots, k_m \times k_m$, съответно (т.е., $A_j \in \text{Mat}_{k_j}(\mathbb{C})$ за $j = 1, \dots, m$). Получената матрица означаваме с $\text{diag}(A_1, \dots, A_m)$ и сме я изобразили на долната фигура:

$$=: \text{diag}(A_1, \dots, A_m)$$

фиг. 41: Блочно-диагонална матрица от размер $(k_1, \dots, k_m)$: блоковете са квадратни матрици $A_j \in \text{Mat}_{k_j}(\mathbb{C})$ за $j = 1, \dots, m$.

Множеството на всички блочно-диагонални матрици за фиксирано наредено разбиване $n = k_1 + \dots + k_m$ ще бележим с:

$$\begin{aligned} & \text{Mat}_{k_1, \dots, k_m}(\mathbb{C}) \\ & := \left\{ \text{diag}(A_1, \dots, A_m) \mid A_j \in \text{Mat}_{k_j} \right. \\ & \quad \left. \text{за } j = 1, \dots, m \right\}. \end{aligned} \tag{6.1}$$

Ще казваме също, че **размера на блочното разбиване** (още, “**блочен размер**”) на матриците от $\text{Mat}_{k_1, \dots, k_m}(\mathbb{C})$ е:

$$(k_1, \dots, k_m) \times (k_1, \dots, k_m). \tag{6.2}$$

В по-обща ситуация двата набора в (6.2) могат да са различни, но за да имаме блочно-диагонални матрици е необходимо да са еднакви.

Нека се убедим, че полученото подмножество $Mat_{k_1, \dots, k_m}(\mathbb{C})$ на $Mat_n(\mathbb{C})$ е $*$ -подалгебра с единица.

Да започнем с единичната матрица: тя се явява блочно-диагонална матрица при всяко разбиване на блокове от горния вид. Фактически имаме,

$$\hat{1}_n = \text{diag}(\hat{1}_{k_1}, \dots, \hat{1}_{k_m}), \quad (6.3)$$

където $\hat{1}_k$ означава квадратната матрица с размер $k \times k$.

По-нататък, очевидно е това, че сума на блочно-диагонални матрици от един и същи блочен размер е отново блочно-диагонална от същия блочен размер. Всъщност имаме:

$$\begin{aligned} & \text{diag}(A_1, \dots, A_m) + \text{diag}(B_1, \dots, B_m) \\ &= \text{diag}(A_1 + B_1, \dots, A_m + B_m) \end{aligned} \quad (6.4)$$

и аналогично:

$$\lambda \text{diag}(A_1, \dots, A_m) = \text{diag}(\lambda A_1, \dots, \lambda A_m) \quad (6.5)$$

$(\lambda \in \mathbb{C})$. Последните две формули показват, че $Mat_{k_1, \dots, k_m}(\mathbb{C})$ е линейно подпространство на $Mat_n(\mathbb{C})$. По-малко очевидно е, че и произведението на блочно-диагонални матрици от един и същи блочен размер е отново блочно-диагонална от същия блочен размер. Това обаче може да бъде онагледено на следната фигура:

$$\begin{array}{c}
 \begin{array}{|c|c|c|c|} \hline A_1 & 0 & \dots & 0 \\ \hline 0 & A_2 & \dots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \dots & A_m \\ \hline \end{array} \cdot \begin{array}{|c|c|c|c|} \hline B_1 & 0 & \dots & 0 \\ \hline 0 & B_2 & \dots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \dots & B_m \\ \hline \end{array} \\
 \\
 = \begin{array}{|c|c|c|c|} \hline C_1 & 0 & \dots & 0 \\ \hline 0 & C_2 & \dots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \dots & C_m \\ \hline \end{array}
 \end{array}$$

фиг. 42: Произведение на блокочно-диагонални матрици: в

три цвята са изобразени три реда и три стълба, като в един цвят са начертани

тези, които са от една и съща група на разбиването $n = k_1 + \dots + k_m$.

Така, когато умножим ред по стълб от една и съща група на разбиването,

например, първата то ще получим ненулево засичане само на тези елементите,

които са от първите диагонални блокове и това ще възпроизведе матричното

умножение на тези блокове, $A_1 B_1 = C_1$. Аналогично, $A_j B_j = C_j$ за

всяко $j = 1, \dots, m$. Ако умножим обаче ред по стълб от различни групи на

разбиването, например “синия” ред по “зеления” стълб, тогава ще се получим

разминаване на евентуалните ненулеви компоненти и крайния резултат ще е нула.

Затова всички компонентите на произведението извън диагоналните блокове ще са

нула.

Съгласно обяснението към горната фигура имаме:

$$\begin{aligned} \text{diag}(A_1, \dots, A_m) \text{diag}(B_1, \dots, B_m) & \quad (6.6) \\ = \text{diag}(A_1 B_1, \dots, A_m B_m). \end{aligned}$$

И така, $\text{Mat}_{k_1, \dots, k_m}(\mathbb{C})$ е подалгебра с единица на $\text{Mat}_n(\mathbb{C})$. Остава да проверим, че $\text{Mat}_{k_1, \dots, k_m}(\mathbb{C})$ е $*$ -подалгебра на $\text{Mat}_n(\mathbb{C})$. Но ако погледнем вида на $*$ -операцията в $\text{Mat}_n(\mathbb{C})$, която е ермитовото спрягане (фиг. 39) и вида от фиг. 41 на блочно-диагонална матрица, то получаваме непосредствено, че

$$\text{diag}(A_1, \dots, A_m)^* = \text{diag}(A_1^*, \dots, A_m^*). \quad (6.7)$$

И така, наистина $\text{Mat}_{k_1, \dots, k_m}(\mathbb{C})$ е $*$ -подалгебра с единица на $\text{Mat}_n(\mathbb{C})$.

Ще завършим този пример с една допълнителна бележка, която не е задължителна за проследяването на този курс, но е добре за общата математическа култура на читателите с по-малък опит в областта на алгебрата. Както се вижда от фиг. 41, задаването на блочно-диагонална матрица е равносилно на задаване на набор квадратни матрици от предварител-

но зададен размер. Като множества имаме:

$$\text{Mat}_{k_1, \dots, k_m}(\mathbb{C}) \cong \text{Mat}_{k_1}(\mathbb{C}) \times \dots \times \text{Mat}_{k_m}(\mathbb{C}), \quad (6.8)$$

изоморфно представяне на $\text{Mat}_{k_1, \dots, k_m}(\mathbb{C})$ с декартово произведение. По нататък, формули (6.3)–(6.7) определят в декартовото произведение $\text{Mat}_{k_1}(\mathbb{C}) \times \dots \times \text{Mat}_{k_m}(\mathbb{C})$ структура на $*$ -алгебра с единица, като просто изтрием навсякъде в тях символите “*diag*”. Получената конструкция е известна в алгебрата, като **пряко произведение на алгебри** Също така, декартовите проекции

$$(A_1, \dots, A_m) \mapsto A_j \quad (6.9)$$

задават морфизми на $*$ -алгебри с единица

$$\text{Mat}_{k_1}(\mathbb{C}) \oplus \dots \oplus \text{Mat}_{k_m}(\mathbb{C}) \rightarrow \text{Mat}_{k_j}(\mathbb{C}) \quad (6.10)$$

за всяко $j = 1, \dots, m$ и се наричат **структурни проекции**. Всъщност, от гледна точка на теория на категориите, с която ще се запознаем по-късно, именно структурните проекции определят категорното (пряко) произведение. Понякога обаче така определеното понятие за пряко произведение на алгебри се нарича “**пряка сума на алгебри**”, а не произведение

и се бележи с

$$“Mat_{k_1}(\mathbb{C}) \oplus \cdots \oplus Mat_{k_m}(\mathbb{C})”. \quad (6.11)$$

Това е доста неуместно от гледна точка на теория на категориите, където категорната (пряка) сума се явява в известен смисъл дуално понятие на категорното произведение. Ние ще видим по-нататък, че в категорията на асоциативните $*$ -алгебри с единица няма в общия случай категорна пряка сума.

6.2.2 Допълнителни примери и контрапримери

Тази точка ще завършим с допълнителни примери за подалгебри, някои от които са “патологични” от гледна точка на нашия курс макар, че от гледна точка на други дисциплини те се явяват интересни. Ние няма да дадем всички детайли около следващите примери, като оставим на читателите да запълнят липсващите аргументи в качеството на упражнение.

– Подпространството $\{\text{diag}(A, A) \mid A \in Mat_k(A)\}$ е $*$ -подалгебра с единица на

- $Mat_{2k}(A)$, която като самостоятелна $*$ -алгебра с единица е *изоморфна* на $Mat_k(A)$.
- Подпространството $\{\text{diag}(\hat{0}_k, A) \mid A \in Mat_k(A)\}$, където $\hat{0}_k \in Mat_k(A)$ е нулата, е $*$ -подалгебра на $Mat_{2k}(A)$, но не е подалгебра с единица. Същевременно, като самостоятелна $*$ -алгебра $\{\text{diag}(\hat{0}_k, A) \mid A \in Mat_k(A)\}$ има единица и това е $\text{diag}(\hat{0}_k, \hat{1}_k)$, но това не е единицата на $Mat_{2k}(A)$ (която е $\hat{1}_{2k} = \text{diag}(\hat{1}_k, \hat{1}_k)$). Всъщност, $\{\text{diag}(\hat{0}_k, A) \mid A \in Mat_k(A)\} \cong Mat_k(A)$, като $*$ -алгебра с единица.
 - Подпространството на **горно триъгълните** матрици

$$\left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix} \right\}$$

- е подалгебра с единица на $Mat_n(A)$, но не е $*$ -подалгебра.
- Подпространството на **строго горно триъгълните** матрици

$$\left\{ \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right\}$$

е подалгебра на $Mat_n(A)$, но не е $*$ -подалгебра с единица, като въобще в нея няма единица.

6.3 Основна структурна теорема

Достигаме до главния резултат, който води до разplitане на теорията на алгебричния подход.

Теорема. *Всяка крайно-мерна, положителна, комплексна, асоциативна $*$ -алгебра с единица е изоморфна на $Mat_{k_1, \dots, k_m}(\mathbb{C})$ за единствен набор от естествени числа $k_1 \leq k_2 \leq \dots \leq k_m$. Следователно, без ограничение на общността, алгебрите на наблюдаемите на крайните квантови системи могат да се считат от вида $Mat_{k_1, \dots, k_m}(\mathbb{C})$.*

Доказателството на тази теорема сме привели за пълнота, като допълнение към тази лекция. То обаче не е от съществено значение

за този курс, а единствено твърдението в теоремата. Забележете, че ние не твърдим, че всяка $*$ -подалгебра с единица на $Mat_n(\mathbb{C})$ е от вида $Mat_{k_1, \dots, k_m}(\mathbb{C})$ или, че дори може да се преобразува в такава, например, чрез смяна на базиса. Така например в първия от допълнителните примери по-горе имахме $*$ -подалгебра с единица на $Mat_{2k}(\mathbb{C})$, която не е от вида на $Mat_{k_1, \dots, k_m}(\mathbb{C})$ подалгебра, но същевременно, като самостоятелна $*$ -алгебра с единица тя беше изоморфна на $Mat_k(\mathbb{C})$, което и се очаква според теоремата.

Още една допълнителна любопитна забележка. В условието на теоремата по-горе не е нужно да се изисква предварително съществуването на единица: заключението е вярно и без това предположение, от където пък следва, че съществува единица (в $Mat_{k_1, \dots, k_m}(\mathbb{C})$ има единица).

И така, вече знаем какви могат да са алгебрите на наблюдаемите на квантовата информатика в алгебричния подход (с точност до изоморфизъм). Информацията за тях се кодира в една крайна монотонна редица от естествени числа, която е един вид “регистра-

ционен номер” на квантовата система, както схематично сме изобразили на долната фигура.

$$\circ \ k_1 \leq k_2 \leq \dots \leq k_m \ \circ$$

фиг. 43: “Регистрационен номер” на крайна квантова система: крайна монотонно ненамаляваща редица от естествени числа.

Това е един доста силен резултат, понеже нашите аксиоми бяха първоначално доста абстрактни, а ние ги изпълваме сега със съвсем конкретно съдържание.

6.4 Комутативния случай

Основната структурна теорема от предната точка ни позволява напълно да разрешим специалния случай, когато алгебрата на наблюдаемите е комутативна.

Следствие. *Алгебрата на наблюдаемите $\mathcal{A}$ на една крайна квантова система е комутативна, тогава и само тогава, когато е изоморфна на $\text{Mat}_{1,\dots,1}(\mathbb{C})$ (т.е., когато $k_1 = \dots = k_m = 1$ и $m = n$ в условието на*

теоремата). В този случай, алгебрата на наблюдаемите $\mathcal{A}$ е също изоморфна на $*$ -алгебрата с единица на всички комплексни функции над едно крайно множество Ω .

Доказателство. Да започнем с въпроса кога $Mat_{k_1, \dots, k_m}(\mathbb{C})$ е комутативна. Отговора идва от ф-ла (6.6), от която виждаме, че произведението е комутативно само, ако произведенията във всеки блок са комутативни. Последното на свой ред се случва само, ако всички блокове са 1×1 , т.е., са числа. Така $\mathcal{A}$ е комутативна, тогава и само тогава, когато $k_1 = \dots = k_m = 1$.

Към втория проблем: как тогава $\mathcal{A}$ е изоморфна на алгебрата от комплексните функции на едно крайно множество Ω . Всъщност, това крайно множество трябва да се избере n елементно: $\Omega = \{\omega_1, \dots, \omega_n\}$. Изоморфизмът е изобразен на долната фигура:

$$\begin{array}{ccc} \Omega = \{\omega_1, \dots, \omega_n\} & & \\ A \downarrow & \Downarrow & \Downarrow \\ \mathbb{C} & \in & a_1, \dots, a_n \end{array}$$

$$\longleftrightarrow \begin{pmatrix} a_1 & \dots & 0 \\ 0 & \dots & a_n \end{pmatrix}$$

*понеже имат еднакви закони за
събиране, умножение и спрягане*

фиг. 44: Изоморфизъм на комутативните $*$ -алгебри с алгебри от функции.

Нека разпишем по-подробно горния изоморфизъм. Нека означим алгебрата на комплексните функции над множеството Ω с:

$$Func_{\mathbb{C}}(\Omega) := \{A | A : \Omega \rightarrow \mathbb{C}\}, \quad (6.12)$$

операциите в която са **потоково** определени, т.е.,

$$(A + B)(\omega) := A(\omega) + B(\omega), \quad (6.13)$$

$$(\lambda A)(\omega) := \lambda A(\omega), \quad (6.14)$$

$$(AB)(\omega) := A(\omega)B(\omega), \quad (6.15)$$

$$(A^*)(\omega) := \overline{A(\omega)}, \quad (6.16)$$

за всеки $A, B \in \text{Func}_{\mathbb{C}}(\Omega)$, $\lambda \in \mathbb{C}$ и $\omega \in \Omega$. Тогава, изоморфизма от фиг. 44 съпоставя на функцията със стойности $A(\omega_1) = a_1, \dots, A(\omega_n) = a_n$ диагоналната матрица $\text{diag}(a_1, \dots, a_n)$. Изказано само с думи: всяка диагонална матрица представя таблицата от стойностите на функция, която е изписана по диагонала на матрицата. Операциите от ф-ли (6.13)–(6.16) се пренасят в операциите от ф-ли (6.4)–(6.7) в случая на блокове 1×1 . $\square$

6.5 Класическите системи в алгебричния подход

Достигаме до формулировката на класическите системи в алгебричния подход. От предната лекция знаем, че в класическите системи наблюдаемите трябва да комутират. Също отбелязахме, че квантовото произведение на наблюдаеми е наблюдаема тогава и само тогава, когато двете наблюдаеми комутират. И така, ясно е, че алгебрата на наблюдаемите на една класическа система трябва да е комутативна. Но ние вече изчерпателно разгледахме случая на комутативни алгебри на наблюда-

еми в предната точка и имаме основания да заявим и обратното.

Всъщност, ние ще положим всичко това, като определение: **крайна класическа система** това е крайна квантова система с комутативна алгебра на наблюдаемите. В този случай, алгебрата на наблюдаемите е изоморфна на алгебра от функции, като самите наблюдаеми по начало са реално-значните функции, макар че вече и комплексно-значните функции могат да се разглеждат, като двойка съвместно измерими реални наблюдаеми, както отбелязахме в точка ??1. И също така, само в този случай наблюдаемите образуват реална алгебра (и тя е комутативна).

$$\begin{array}{ccc}
 \Omega = \{\omega_1, \dots, \omega_n\} & & \\
 A = A^* & \downarrow & \downarrow \quad \downarrow \\
 \textcolor{red}{\mathbb{R}} & \in & a_1, \dots, a_n
 \end{array}$$

фиг. 45: Класическите наблюдаеми са функции.

Определението съответства на нашата интуиция и мотивация, която изложихме в предната лекция. В класическата физика така се моделират всички физични величини:

като функции върху множества, наречени “множества на състоянията” на системата. Разбира се, за повечето физични системи, тези множества на състоянията могат да бъдат много сложни и с голяма мощност (по-голяма от мощност на континуум). Но за нуждите на информатиката, класическите системи ще се задават с крайни множества.

Предстои да изучим и структурата на състоянията на крайните класически системи в алгебричния подход. Тогава ще се убедим, че в крайна сметка получаваме напълно еквивалентно понятие с това, което имахме и в квантово-логическия подход от точка 2.11.

6.6 Вторият граничен случай на квантови системи: неприводимите или също, чисто квантовите системи

До тук се запознахме основно с първия граничен случай на алгебрите $Mat_{k_1, \dots, k_m}(\mathbb{C})$ от основната структурна теорема (точка 6.3). Това беше случая когато $k_1 = \dots = k_m = 1$ и имаме максимално число $m = n$ блока.

В този случай, алгебрата на наблюдаемите беше комутативна и това бяха класическите системи.

Другият граничен случай на алгебрите $Mat_{k_1, \dots, k_m}(\mathbb{C})$ е когато имаме само един блок, $m = 1$ и това е пълната матрична алгебра $Mat_n(\mathbb{C})$. Този пример вече въведохме в точка 5.11 и го нарекохме (крайна) чисто квантова система. Тези системи ги нарекохме още неприводими понеже те имат следното свойство:

*В матричната алгебра $Mat_n(\mathbb{C})$ единствените матрици $C \in Mat_n(\mathbb{C})$, които комутират с всички останали матрици $A \in Mat_n(\mathbb{C})$ (т.е., $AC = CA$) са пропорционални на единичната матрица (т.е., $C = \lambda \hat{1} \equiv \text{diag}(\lambda, \dots, \lambda)$) – тези матрици се наричат също **скаларни матрици**).*

Това е стандартно твърдение от линейната алгебра и ние го оставяме без доказателство (макар, че то става и за упражнение). По-късно, ние ще разгледаме по-общо понятията за приводимост и неприводимост.

6.7 Подсистеми, надсистеми, експерименти, съвместна (едновременно) измеримост

- **Подсистема** се определя от $\ast$ -подалгебра с единица на алгебрата на наблюдаемите. Смисъл: подсистемата отделя подмножество от наблюдаеми, отнасящи се до измерванията върху нея. Това е аналогично на квантово-логическия подход и както там, така и тук искаме основните операции, които в случая са алгебричните, да се наследяват в подсистемата.

- При размяна на местата във включването

$$\text{подсистема} \subseteq \text{система},$$

получаваме

$$\text{система} \subseteq \text{надсистема}.$$

Както и при квантово-логическия подход, една възможна ситуация при преход към надсистема е процеса на уточняване (“изфинване”) на измерванията. В квантовата информатика, прехода към надсистема се използва при надграждане на изчисленията, например.

- **Експеримент:** това е подсистема, която сама по себе си е класическа. Следователно, това е комутативна $*$ -подалгебра с единица на алгебрата на наблюдаемите.
- Ако $A \in \mathcal{A}$ е наблюдаема (т.е., $A^* = A$), то подмножеството

$$\begin{aligned}\mathbb{C}[A] &:= \text{множеството на всички} \\ &\quad \text{полиноми от } A \\ &\equiv \{a_0\hat{1} + a_1A^1 + \dots + a_nA^n \mid \\ &\quad \text{за } \forall n \in \mathbb{N} \text{ и } a_0, \dots, a_n \in \mathbb{C}\} \\ &= \text{Span}_{\mathbb{C}} \{\hat{1}, A, A^2, \dots, A^n, \dots\}\end{aligned}$$

е най-малката комутативна $*$ -подалгебра с единица на $\mathcal{A}$, която съдържа A . Следователно, това е минималния експеримент, при който се измерва наблюдаемата A .

- Две наблюдаеми $A, B \in \mathcal{A}$ се наричат **съвместни** (още, “едновременно” / **съвместно измерими**), ако могат да се измерят в общ експеримент. Следователно, и B са съвместни тогава и само тогава, когато те се съдържат в обща комутативна, $*$ -подалгебра с единица на $\mathcal{A}$.

Теорема. Две наблюдаеми $A, B \in \mathcal{A}$ са

съвместни тогава и само тогава, когато комутират, т.е., $AB = BA$.

6.8 Събитията в алгебричния подход

Първоначално определихме събитие, като наблюдаема Q , която приема стойности 0 или 1. Това се изразява от алгебричното съотношение $Q^2 = Q$, понеже $\{0, 1\}$ е множеството от корени на уравнението $x^2 - x = 0$. Добавяйки и условието за наблюдаема $Q = Q^*$ достигаме до следите определения.

Определение. а) **Самоспрегнат идемпотент** Q в $*$ -алгебра $\mathcal{A}$, това е елемент $Q \in \mathcal{A}$ такъв, че

$$Q^* = Q = Q^2. \quad (6.17)$$

б) **Събитие** в квантова система това е самоспрегнат идемпотент на алгебрата на наблюдаемите.

Пример. Събитие в класическа система: нека тя се определя от крайно множество $\Omega = \{\omega_1, \dots, \omega_n\}$, така че алгебрата на наблюдаемите

е $\mathcal{A} := \text{Func}_{\mathbb{C}}(\Omega)$; тогава условието една функция Q да бъде наблюдаема ни дава:

$$Q^* = Q = Q^2$$

$$\Leftrightarrow \overline{Q(\omega)} = Q(\omega) = Q(\omega)^2 \quad (\forall \omega \in \Omega)$$

$$\Leftrightarrow Q(\omega) \in \{0, 1\}$$

$\Leftrightarrow Q = \chi_S$, т.е., Q е характеристична функция на подмножество $S \subseteq \Omega$.

Напомняме, че характеристична функция на подмножество $S \subseteq \Omega$ се определя, като

$$\chi_S := \begin{cases} 1 & \text{ако } \omega \in S, \\ 0 & \text{ако } \omega \notin S \end{cases} \quad (6.18)$$

и тогава

$$S = \{\omega \in \Omega \mid Q(\omega) = 1\}. \quad (6.19)$$

6.9 Логика и аритметика

В класическите системи логическите операции имат алгебричен израз. За $S_1, S_2 \subseteq \Omega$ имаме:

$$\chi_{S_1 \cap S_2} = \chi_{S_1} \chi_{S_2} \quad (6.20)$$

$$\chi_{S_1 \cup S_2} = \chi_{S_1} + \chi_{S_2} - \chi_{S_1} \chi_{S_2}. \quad (6.21)$$

В частност,

$$\Omega = S_1 \dot{\cup} \cdots \dot{\cup} S_m \quad (\text{дизюнктивно разбиване})$$

$$\iff \begin{cases} \hat{1} \equiv \chi_\Omega = \chi_{S_1} + \cdots + \chi_{S_m} \\ \hat{0} \equiv \chi_\emptyset = \chi_{S_j} \chi_{S_k} \text{ за } \forall j \neq k. \end{cases} \quad (6.22)$$

6.10 Спектрална теорема. Спектър и спектрално разлагане на наблюдаема

Спектрална теорема. Нека $\mathcal{A}$ е крайномерна, комплексна, положителна $*$ -алгебра с единица и нека $A \in \mathcal{A}$ е самоспрегнат елемент ($A = A^*$). Тогава съществуват двойки

$$(Q_1, \alpha_1), \dots, (Q_m, \alpha_m), \quad (6.23)$$

които са единствени с точност до пренапреждане и са такива, че

- $\alpha_1, \dots, \alpha_m$ са две по две различни числа.
- $Q_1, \dots, Q_m$ са ненулеви самоспрегнати идемпотенти.
- $A = \alpha_1 Q_1 + \cdots + \alpha_m Q_m$ - това наричаме **спектрално разлагане на A** .
- $\hat{1} = Q_1 + \cdots + Q_m$,

$\hat{0} = Q_j Q_k$ ако $j \neq k$, $j, k = 1, \dots, m$

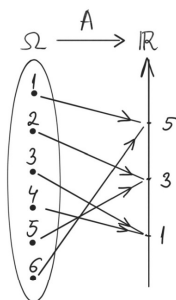
– в случая на последните две условия казваме, че $Q_1, \dots, Q_m$ задават разбиване на единицата в $*$ -алгебрата A .

Множеството $\{\alpha_1, \dots, \alpha_m\}$ се нарича **спектър** на A , а $Q_1, \dots, Q_m$ – **спектрални идемпотенти** на A .

Нека разгледаме като пример спектралното разлагане в комутативни $*$ -алгебри, които са алгебри от функции. Ето един конкретен случай:

Пример:

$$\begin{aligned} A &= \\ &= 1. \chi_{\{3,4\}} \\ &+ 3. \chi_{\{2,5\}} \\ &+ 5. \chi_{\{1,6\}} \end{aligned}$$



$$\begin{aligned} \{3, 4\} &= A^{-1}(1), \\ \{2, 5\} &= A^{-1}(3), \\ \{1, 6\} &= A^{-1}(5). \end{aligned}$$

$$A = \underbrace{1. \chi_{\{3,4\}}}_{\alpha_1 Q_1} + \underbrace{3. \chi_{\{2,5\}}}_{\alpha_2 Q_2} + \underbrace{5. \chi_{\{1,6\}}}_{\alpha_3 Q_3}$$