Postuláty kvantové mechaniky

Postulát 1. Izolovaný kvantový systém, je popsán unitárním prostorem. Stav systému je plně popsán stavovým vektorem, což je jednotkový vektor stavového prostoru.

Vektory, které se liší pouze o násobek jednotkovým komplexním číslem, tedy $e^{i\varphi}$ jsou experimentálně nerozlišitelné. Ve fyzice se o tomto násobku mluví jako o *globální fázi*. V jistém smyslu je tedy stavem jednodimenzionální podprostor stavového systému.

Přirozeným základem kvantové informatiky je kvantový systém se dvěma bázovými stavy, které jsou analogií 0 a 1 používaných v klasické teorii informace. Takový systém se proto nazývá *kubit* a jeho bázové stavy se značí $|0\rangle$ a $|1\rangle$. Vezmeme-li v úvahu projektivní ekvivalenci danou globální fází, je tedy kubit *komplexní projektivní přímka* $\mathbb{P}^1(\mathbb{C})$. Budeme ho ale obvykle značit jako $\mathbb{H}_2$ (čímž ignorujeme fázovou ekvivalenci stavů).

Postulát 2. Časový vývoj kvantového systému $|u(t)\rangle$ je dán diferenciální rovností

$$i\hbar \frac{\partial}{\partial t} |u(t)\rangle = H|u(t)\rangle,$$

kde $\hbar \in \mathbb{R}$ je tzv. redukovaná Planckova konstanta a H je hermitovský operátor, označovaný jako *hamiltonián* systému.

Uvedená rovnost se nazývá *Schrödingerova rovnice*. Fyzikální význam Planckovy konstanty je poměr mezi energií a frekvencí fotonu. Protože se jedná o reálné číslo, je možné ho z rovnice vypustit (a uvažovat hamiltonián vydělený touto konstantou). Protože je hamiltonián hermitovský, má pro jeho vlastní vektory Schrödingerova rovnice jednoduchou podobu (vynecháváme Planckovu konstantu)

$$\frac{\partial}{\partial t} |u(t)\rangle = -ir|u(t)\rangle,$$

kde $r \in \mathbb{R}$ je vlastní číslo operátoru H. Pokud předpokládáme, že se hamiltonián v průběhu času nemění, je snadné najít pro vlastní vektor $|u(t)\rangle$ řešení

$$|u(t)\rangle = e^{-irt}|u(t_0)\rangle.$$

S použitím dohody o operátorových funkcích dostáváme pro obecný vektor $|v\rangle$ zápis

$$|v(t)\rangle = e^{-iHt}|v(t_0)\rangle.$$

Je vidět, že operátor e^{-iHt} má vlastní čísla velikosti jedna (konkrétně e^{-irt}), a je tedy unitární.

Protože v kvantových počítačích chceme na vstupu (na vstupních kubitech) provádět přesně definované diskrétní operace, můžeme druhý postulát přeformulovat v diskrétní podobě takto:

Postulát 2'. Kvantový stav $|\varphi\rangle$ se za časovou jednotku Δt změní na stav $U|\varphi\rangle$, kde U je unitární operátor.

Postulát 3. Měření je dáno hermitovským operátorem M, nazývaným *pozorovatelná veličina*. Nechť

$$M = \sum_i m_i P_i$$

je spektrální rozklad M (tj. m_i jsou vlastní čísla M a P_i projekce na vlastní podprostor příslušný vlastnímu číslu m_i).

- Výsledkem měření je jedno z čísel m_i (které je reálné, protože operátor je hermitovský).
- Pravděpodobnost, že výsledek měření stavu $|\varphi\rangle$ bude m_i je rovna $\langle\varphi|P_i|\varphi\rangle$.
- Je-li výsledek měření stavu $|\varphi\rangle$ roven m_i, je systém bezprostředně po měření ve stavu
$$\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$$
(říkáme, že systém do tohoto stavu *zkolabuje*).

Uvedený postulát popisuje tzv. *projektivní měření* a nevystihuje fenomén kvantového měření v plné obecnosti. Pro naše účely to však bude stačit, navíc platí, že každé měření lze jistými úpravami na projektivní měření převést. V tzv. *nedegenerovaném* případě je počet různých vlastních čísel roven dimenzi systému (neexistují násobná vlastní čísla) a všechny zmiňované podprostory jsou jednodimenzionální. Degenerované měření se tedy vyznačuje tím, že je počet možných výsledků menší než je dimenze systému, tedy menší než u měření jiných veličin (připomeňme, že jsme dimenzi systému popsali jako počet možných výsledků měření).

Všimněme si, že měření je dáno sadou projekčních operátorů P_i a to, který bude použit, je náhodný jev určující výsledek měření. Pravděpodobnost, že bude použit právě operátor P_i, je dána druhou mocninou velikostí výsledku projekce, tedy druhou mocninou normy vektoru $P_i|\varphi\rangle$. Ta je rovna $\langle\varphi|P_i^\dagger P_i|\varphi\rangle$, což je rovno $\langle\varphi|P_i|\varphi\rangle$ vzhledem k tomu, že projekce je hermitovská a idempotentní. Protože platí $|\varphi\rangle = \sum_i P_i|\varphi\rangle$, je pro jednotkový vektor součet všech pravděpodobností roven jedné.

Výsledek projekce je ve výše uvedeném předpisu znormován, a to odmocninou z pravděpodobnosti výsledku. Uvědomme si, že normační faktor, závislý na vektoru $|\varphi\rangle$, činí z měření nelineární zobrazení.

Každé měření vystihuje nějakou vlastnost systému. Hamiltonián, který se vyskytuje ve Schrödingerově rovnici, např. odpovídá tzv. totální energii systému (časový vývoj systému je tedy určen touto veličinou).

Protože je veličina hermitovská, má ortonormální bázi vlastních vektorů $|\mathbf{b}_i\rangle$. Projekce na podprostor P_i je potom rovna
$$P_i = \sum_j |\mathbf{b}_j\rangle\langle\mathbf{b}_j|,$$
kde sčítáme přes všechny bázové vektory s vlastním číslem m_i.

Zápis veličiny jako jednoho operátoru (tedy nikoli např. jako souboru projekcí) umožňuje mimo jiné úsporný výpočet střední hodnoty veličiny M na konkrétním stavu $|\varphi\rangle$ jako
$$\mathbf{E}(M) = \sum_i m_i p(m_i) = \sum_i m_i\langle\varphi|\mathbf{b}_i\rangle\langle\mathbf{b}_i|\varphi\rangle = \langle\varphi|(\sum_i m_i|\mathbf{b}_i\rangle\langle\mathbf{b}_i|)|\varphi\rangle = \langle\varphi|M|\varphi\rangle.$$

Postulát 4. Nechť U a V jsou kvantové systémy. Pak systém složený z U a V je popsán tenzorovým součinem $U \otimes V$. Je-li systém U ve stavu $|u\rangle$ a systém V ve stavu $|v\rangle$, je stav složeného systému roven $|u\rangle \otimes |v\rangle$.