

Spis treści

1	Abstrakcyjna teoria kwantów	1
1.1	Elementy teorii przestrzeni Hilberta	1
1.2	Elementy teorii operatorów liniowych	5
1.3	Postulaty teorii kwantów	9
1.4	Kwantowe układy dwupoziomowe	13
1.4.1	Macierze Pauliego	13
1.4.2	Sfera Blocha	14
1.4.3	Ewolucja układu dwupoziomowego	16
1.4.4	Obroty na sferze Blocha	17
1.4.5	Przykład – magnetyczny rezonans jądrowy	18
1.5	Korelacje kwantowe	20
1.5.1	Stany dwubitowe	20
1.5.2	Operator gęstości	21
2	Obliczenia kwantowe	22
3	Informacja kwantowa	23
3.1	Bazy dopełniające	23

1 Abstrakcyjna teoria kwantów

1.1 Elementy teorii przestrzeni Hilberta

Przez $\mathbb{V} := (V, \mathbb{C}, +, \cdot)$ będziemy oznaczać przestrzeń wektorową nad ciałem liczb zespolonych.

Def 1.1. Odwzorowanie $d : V \times V \mapsto \mathbb{R}$ będziemy nazywać *metryką* w zbiorze $V \neq \emptyset$ iff

- $\forall u, v \in V : d(u, v) \geq 0$, przy czym równość zachodzi iff $u = v$ (*nieujemność*)
- $\forall u, v \in V : d(u, v) = d(v, u)$ (*symetria*)
- $\forall u, v, w \in V : d(u, v) + d(v, w) \geq d(u, w)$ (*nierówność trójkąta*)

Parę $(V, d(\cdot, \cdot))$ będziemy nazywać *przestrzenią metryczną*.

Def 1.2. Niech (V, d) będzie przestrzenią metryczną. Mówimy, iż dany ciąg (u_n) elementów zbioru V jest zbieżny do $g \in V$ tj. $u_n \rightarrow g$ przy $n \rightarrow \infty$ iff $d(u_n, g) \rightarrow 0$ przy $n \rightarrow \infty$.

Def 1.3. Ciąg (u_n) elementów $u_n \in V$ będziemy nazywać *ciągą Cauchy'ego* w przestrzeni metrycznej $(V, d(\cdot, \cdot))$ iff spełnia on kryterium Cauchy'ego tj.

$$\forall \epsilon > 0 : \exists N : \forall n, m > N : d(u_n, u_m) < \epsilon.$$

Tw 1.1. Każdy ciąg zbieżny w przestrzeni metrycznej (V, d) jest ciągiem Cauchy'ego w tej przestrzeni.

Def 1.4. Przestrzeń metryczną $(V, d(\cdot, \cdot))$ nazwiemy *zupelną* iff każdy ciąg Cauchy'ego (u_n) elementów $u_n \in V$ jest zbieżny do granicy $g \in V$.

Def 1.5. Niech \mathbb{V} będzie przestrzenią wektorową. Odwzorowanie $\langle \cdot | \cdot \rangle : V \times V \mapsto \mathbb{C}$ nazwiemy *iloczynem wewnętrznym* wektorów iff

- $\forall u, v \in V : \langle u | v \rangle^* = \langle v | u \rangle$
- $\forall u, v_1, v_2 \in V : \forall \alpha, \beta \in \mathbb{C} : \langle u | \alpha v_1 + \beta v_2 \rangle = \alpha \langle u | v_1 \rangle + \beta \langle u | v_2 \rangle$
- $\forall u \in V : \langle u | u \rangle \geq 0$, przy czym równość zachodzi iff $u = 0$. Zauważmy tutaj, iż z pierwszego aksjomatu $\langle u | u \rangle \in \mathbb{R}$, gdyż $\langle u | u \rangle = \langle u | u \rangle^* \implies \text{Im}\{\langle u | u \rangle\} = 0$.

Parę $(\mathbb{V}, \langle \cdot | \cdot \rangle)$ będziemy nazywać *przestrzenią unitarną*.

Tw 1.2. Każda przestrzeń unitarna jest metryczna z metryką indukowaną przez iloczyn wewnętrzny $d(u, v) := \|u - v\| = \sqrt{\langle u - v | u - v \rangle}$.

Tw 1.3 (*Nierówność Cauchy'ego-Schwarza*). Niech $(\mathbb{V}, \langle \cdot | \cdot \rangle)$ – przestrzeń unitarna. Wówczas

$$\forall u, v \in V : |\langle u | v \rangle|^2 \leq \langle u | u \rangle \langle v | v \rangle .$$

Def 1.6. Przeliczalny zbiór wektorów $\{v_1, \dots, v_n\}$ nazwiemy *ortogonalnym* iff

$$\forall i \neq j ; i, j \in \{1, \dots, n\} : \langle v_i | v_j \rangle = 0 .$$

Ten sam zbiór wektorów nazwiemy *ortonormalnym* iff

$$\forall i, j \in \{1, \dots, n\} : \langle v_i | v_j \rangle = \delta_{ij} ,$$

gdzie δ_{ij} jest deltą Kroneckera.

Tw 1.4. Każda przestrzeń unitarna $(\mathbb{V}, \langle \cdot | \cdot \rangle)$ posiada bazę ortonormalną, tj. bazę, której wektory bazowe tworzą zbiór ortonormalny.

Def 1.7. *Przestrzeń Hilberta* $\mathcal{H} = (\mathbb{V}, \langle \cdot | \cdot \rangle)$ nazwiemy *zupelną* przestrzeń unitarną.

Def 1.8. Niech $\mathcal{H} = (\mathbb{V}, \langle \cdot | \cdot \rangle)$ będzie przestrzenią Hilberta. Odwzorowanie liniowe $F : V \mapsto \mathbb{C}$ nazwiemy *funkcjonałem liniowym* w przestrzeni \mathcal{H} .

Tw 1.5. Niech V^* oznacza zbiór wszystkich funkcjonałów liniowych $F : V \mapsto \mathbb{C}$. Wówczas $\mathbb{V}^* := (V^*, \mathbb{C}, +, \cdot)$, gdzie

- $\forall F_1, F_2 \in V^* : \forall v \in V : (F_1 + F_2)(v) = F_1(v) + F_2(v)$
- $\forall F \in V^* : \forall \alpha \in \mathbb{C} : \forall v \in V : (\alpha \cdot F)(v) = \alpha F(v)$

jest przestrzenią wektorową, którą nazywamy *przestrzenią dualną*.

Tw 1.6 (Riesza). Niech $\mathcal{H} = (\mathbb{V}, \langle \cdot | \cdot \rangle)$ będzie przestrzenią Hilberta, a \mathbb{V}^* jej przestrzenią dualną. Wówczas istnieje wzajemnie jednoznaczne odwzorowanie wektorów $v \in V$ na funkcjonały liniowe $F \in V^*$. Dodatkowo dla każdego funkcjonału F istnieje dokładnie jeden wektor $u \in V$ taki, że

$$\forall v \in V : F(v) = \langle u | v \rangle .$$

Def 1.9. *Iloczynem Kroneckera* macierzy $\mathbf{A} = [a_{ij}]_{n \times m}$ i $\mathbf{B} = [b_{ij}]_{n' \times m'}$ nazywamy macierz wymiaru $nn' \times mm'$ postaci

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & \cdots & b_{1m'} \\ \vdots & \ddots & \vdots \\ b_{n'1} & \cdots & b_{n'm'} \end{bmatrix} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1m}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & \cdots & a_{nm}\mathbf{B} \end{bmatrix}$$

Iloczyn Kroneckera dowolnych macierzy $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$ spełnia

- Jeśli istnieją iloczyny \mathbf{AC}, \mathbf{BD} to $(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD})$.
- Jeśli macierze \mathbf{A}, \mathbf{B} są odwracalne to $(\mathbf{A} \otimes \mathbf{B})^{-1} = \mathbf{A}^{-1} \otimes \mathbf{B}^{-1}$
- $(\mathbf{A} \otimes \mathbf{B})^\dagger = \mathbf{A}^\dagger \otimes \mathbf{B}^\dagger$
- $\mathbf{A} \otimes (\mathbf{B} + \mathbf{C}) = \mathbf{A} \otimes \mathbf{B} + \mathbf{A} \otimes \mathbf{C}$
- $(\mathbf{A} + \mathbf{B}) \otimes \mathbf{C} = \mathbf{A} \otimes \mathbf{C} + \mathbf{B} \otimes \mathbf{C}$

Def 1.10. *Iloczynem tensorowym* przestrzeni Hilberta \mathcal{H}_1 i \mathcal{H}_2 o bazach ortonormalnych odpowiednio $\{\phi_i^{(1)}\}$ i $\{\phi_j^{(2)}\}$ nazywamy przestrzeń Hilberta $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ taką, że:

- Jej bazą ortonormalną jest zbiór $\{\phi_i^{(1)} \otimes \phi_j^{(2)}\}$.
- Iloczyn wewnętrzny wektorów bazowych w przestrzeni $\mathcal{H}_1 \otimes \mathcal{H}_2$ jest zdefiniowany jako

$$\left\langle \phi_i^{(1)} \otimes \phi_j^{(2)} \middle| \phi_k^{(1)} \otimes \phi_l^{(2)} \right\rangle := \left\langle \phi_i^{(1)} \middle| \phi_k^{(1)} \right\rangle_1 \cdot \left\langle \phi_j^{(2)} \middle| \phi_l^{(2)} \right\rangle_2 = \delta_{ik} \delta_{jl} ,$$

gdzie $\langle \cdot | \cdot \rangle_i$ to iloczyn wewnętrzny w \mathcal{H}_i .

Notacja Diraca

Niech \mathcal{H} będzie przestrzenią Hilberta. Wprowadzimy teraz kompaktową notację wektorów i funkcjonałów liniowych wymyśloną przez P.A.M. Diraca. Aby uprościć zapis, będziemy mówili o wektorach należących do przestrzeni \mathcal{H} (używając nawet symbolu należenia $\in \mathcal{H}$), mając oczywiście formalnie na myśli wektory należące do zbioru V .

Wektory należące do \mathcal{H} będziemy oznaczać jako

$$|\psi\rangle, |\phi\rangle, \dots,$$

przy czym $|\cdot\rangle$ to tzw. *ket* i formalnie jest to odwzorowanie $|\cdot\rangle : S \mapsto V$, gdzie S jest zbiorem znaków, których używamy do oznaczenia konkretnych wektorów ze zbioru V . Nie będziemy jednak przestrzegać tego formalnego znaczenia, utożsamiając dla wygody również sam symbol z wektorem.

Funkcjonały liniowe należące do przestrzeni dualnej będziemy oznaczać jako

$$\langle\psi|, \langle\phi|, \dots,$$

przy czym $\langle\cdot|$ to tzw. *bra* i formalnie jest to odwzorowanie $\langle\cdot| : S^* \mapsto V^*$, gdzie S^* jest zbiorem znaków, których używamy do oznaczenia konkretnych funkcjonałów ze zbioru V^* . Ponieważ z tw. Riesz istnieje wzajemnie jednoznaczne odwzorowanie funkcjonałów liniowych na wektory, więc możemy utożsamiać $S^* = S$.

Skończenie wymiarowa przestrzeń Hilberta nad \mathbb{C}

Rozważymy teraz konstrukcję skończenie wymiarowej przestrzeni Hilberta złożonej ze skończenie wymiarowej przestrzeni wektorowej $\mathbb{V} = (\mathbb{C}^n, \mathbb{C}, +, \cdot)$, które elementy będziemy w danej bazie *ortonormalnej* $\{\phi_1, \dots, \phi_n\}$ zapisywać jako

$$\mathbb{V} \ni |\psi\rangle = \sum_{i=1}^n a_i |\phi_i\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix},$$

gdzie $a_i = \langle\phi_i|\psi\rangle \in \mathbb{C}$ oraz iloczynu wewnętrznego zdefiniowanego jako

$$\langle\psi|\phi\rangle := \sum_{i=1}^n a_i^* b_i$$

dla

$$\psi = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \quad \phi = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Powstała w ten sposób skończenie wymiarowa przestrzeń unitarna jest trywialnie zupełna, a zatem skonstruowaliśmy skończenie wymiarową przestrzeń Hilberta. Wektor w tej przestrzeni możemy utożsamiać (poprzez iloczyn wewnętrzny) z macierzą kolumnową jego współrzędnych w danej bazie ortonormalnej. Jasne jest również czym jest funkcjonał liniowy stowarzyszony z danym wektorem

$$\langle\psi| = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}^\dagger = [a_1^* \quad \dots \quad a_n^*],$$

gdzie \dagger oznacza *sprzężenie hermitowskie* macierzy, tj. sprzężoną macierz transponowaną. W dalszej części skupimy się głównie na skończeniu wymiarowych przestrzeniach Hilberta $((\mathbb{C}^n, \mathbb{C}, +, \cdot), \langle\cdot|\cdot\rangle)$, gdyż stanowią one podstawę opisu teorii obliczeń kwantowych i kwantowej teorii informacji. Należy zdawać sobie

jednak sprawę, iż stanowi to duże uproszczenie w stosunku do wymagań pełnoprawnych teorii fizycznych (mechanika falowa, kwantowa teoria pola), w których niezbędna jest teoria nieskończenie wymiarowych przestrzeni Hilberta.

1.2 Elementy teorii operatorów liniowych

Def 1.11. Operatorem liniowym \mathbf{A} w przestrzeni $\mathcal{H} = (\mathbb{V}, \langle \cdot | \cdot \rangle)$ nazywamy odwzorowanie liniowe

$$\mathbf{A} : D(\mathbf{A}) \mapsto D(\mathbf{A}) ,$$

gdzie $D(\mathbf{A})$ jest pewną podprzestrzenią wektorową przestrzeni \mathbb{V} . Dodatkowo zakładamy, iż dziedziny operatorów są gęste, to znaczy ich domknięcia są równe \mathcal{H} .

Zgodnie z wcześniejszymi komentarzami nie będziemy wnikali w subtelne problemy wynikające z faktu, iż w nieskończenie wymiarowej przestrzeni Hilberta pojęcie operatora liniowego jest nieodłącznie związane z pojęciem dziedziny tego operatora, który w ogólności nie jest określony na całej przestrzeni Hilberta, a tylko na pewnym jej podzbiorze. Komplikacje te nie występują w skończenie wymiarowych przestrzeniach Hilberta wymiaru n , w których operatory liniowe możemy utożsamiać z *endomorfizmami* tej przestrzeni

$$\mathbf{A} : V \mapsto V .$$

Jak wiadomo z elementarnej algebry w przypadku n -wymiarowej przestrzeni wektorowej każdemu endomorfizmowi \mathbf{A} możemy przyporządkować macierz wymiaru $n \times n$, której elementy w danej bazie ortonormalnej $\{\phi_1, \dots, \phi_n\}$ są dane przez wartości \mathbf{A} na wektorach bazowych

$$\begin{aligned} \mathbf{A} |\phi_1\rangle &= A_{11} |\phi_1\rangle + A_{21} |\phi_2\rangle + \dots + A_{n1} |\phi_n\rangle \\ &\vdots \\ \mathbf{A} |\phi_n\rangle &= A_{1n} |\phi_1\rangle + A_{2n} |\phi_2\rangle + \dots + A_{nn} |\phi_n\rangle \end{aligned} ,$$

skąd element A_{ij} macierzy \mathbf{A} w bazie ortonormalnej $\{\phi_i\}$ jest dany przez

$$A_{ij} = \langle \phi_i | \mathbf{A} | \phi_j \rangle .$$

Def 1.12. *Sprzężeniem* operatora \mathbf{A} nazywamy operator \mathbf{A}^\dagger zdefiniowany (pomijając wszelkie problemy związane z określeniem dziedzin operatorów) przez równanie

$$\forall \psi, \phi \in \mathcal{H} : \langle \psi | \mathbf{A}^\dagger | \phi \rangle = \langle \phi | \mathbf{A} | \psi \rangle^* .$$

Podstawiając w miejsce wektorów ψ, ϕ wektory bazy otrzymujemy (w przypadku skończenie wymiarowych przestrzeni Hilberta) zależność między macierzą \mathbf{A} i jej sprzężeniem hermitowskim \mathbf{A}^\dagger

$$A_{ij}^\dagger = A_{ji}^* .$$

Def 1.13. *Komutatorem* operatorów \mathbf{A}, \mathbf{B} operator $[\mathbf{A}, \mathbf{B}]$ zdefiniowany jako

$$\forall \psi \in D : [\mathbf{A}, \mathbf{B}]\psi = \mathbf{A}\mathbf{B}\psi - \mathbf{B}\mathbf{A}\psi.$$

Jeśli $[\mathbf{A}, \mathbf{B}] = \mathbf{0}$ (gdzie $\mathbf{0}$ oznacza operator zerowy $\mathbf{0}\psi = 0$), to mówimy, że operatory \mathbf{A}, \mathbf{B} *komutują*.

Def 1.14. *Antykomutatorem* operatorów \mathbf{A}, \mathbf{B} nazywamy operator $\{\mathbf{A}, \mathbf{B}\}$ zdefiniowany jako

$$\{\mathbf{A}, \mathbf{B}\}\psi := \mathbf{A}\mathbf{B}\psi + \mathbf{B}\mathbf{A}\psi.$$

Tw 1.7. Dla dowolnych operatorów $\mathbf{A}, \mathbf{B}, \mathbf{C}$ zakładając odpowiednie dziedziny, zachodzi:

- $[\mathbf{A} + \mathbf{B}, \mathbf{C}] = [\mathbf{A}, \mathbf{C}] + [\mathbf{B}, \mathbf{C}]$;
- $[\mathbf{A}\mathbf{B}, \mathbf{C}] = \mathbf{A}[\mathbf{B}, \mathbf{C}] + [\mathbf{A}, \mathbf{C}]\mathbf{B}$.
- $[[\mathbf{A}, \mathbf{B}], \mathbf{C}] + [[\mathbf{B}, \mathbf{C}], \mathbf{A}] + [[\mathbf{C}, \mathbf{A}], \mathbf{B}] = \mathbf{0}$ (*tożsamość Jacobiego*)

Def 1.15. *Ślad operatora* \mathbf{A} definiujemy jako liczbę $\text{Tr } \mathbf{A} \in \mathbb{C}$ równą

$$\text{Tr } \mathbf{A} := \sum_i \langle \phi_i | \mathbf{A} | \phi_i \rangle ,$$

gdzie $\{\phi_i\}$ jest dowolną ortonormalną bazą przestrzeni \mathcal{H} .

Tw 1.8. Ślad operatora nie zależy od wyboru ortonormalnej bazy przestrzeni Hilberta.

Tw 1.9. Podstawowe własności śladu.

- $\text{Tr}(\alpha \mathbf{A} + \beta \mathbf{B}) = \alpha \text{Tr}(\mathbf{A}) + \beta \text{Tr}(\mathbf{B})$
- $\text{Tr } \mathbf{ABC} = \text{Tr } \mathbf{BCA} = \text{Tr } \mathbf{CAB}$
- $\text{Tr } \mathbf{A} = \left(\text{Tr } \mathbf{A}^\dagger \right)^*$
- $\det\{e^{\mathbf{A}}\} = e^{\text{Tr } \mathbf{A}}$

Def 1.16 (*Funkcja operatora*). Niech $f(x) : \mathbb{R} \mapsto \mathbb{R}$ będzie funkcją zmiennej rzeczywistej taką, że istnieje szereg potęgowy

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n ,$$

który jest zbieżny jednostajnie na \mathbb{R} do f . Wówczas funkcję operatora $f(\mathbf{A})$ definiujemy jako

$$f(\mathbf{A}) := \sum_{n=0}^{\infty} \frac{a_n}{n!} \mathbf{A}^n ,$$

gdzie przyjmujemy $\mathbf{A}^0 := \mathbf{1}$. W szczególności mamy

- $\exp(\mathbf{A}) := \sum_{n=0}^{\infty} \frac{1}{n!} \mathbf{A}^n$
- $\sin(\mathbf{A}) := \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} \mathbf{A}^{2n+1}$
- $\cos(\mathbf{A}) := \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} \mathbf{A}^{2n}$

W teorii kwantowej główną rolę odgrywają trzy rodziny operatorów: operatory samosprężone, rzutowe i unitarne.

Def 1.17. *Operatorem samosprężonym* (pomijając wszelkie problemy związane z określeniem dziedzin operatorów) nazywamy operator \mathbf{A} , dla którego $\mathbf{A} = \mathbf{A}^\dagger$.

W przypadku skończone wymiarowych przestrzeni Hilberta definicja ta jest pełna, a operatory samosprężone możemy utożsamiać z macierzami hermitowskimi tj. macierzami, których elementy spełniają związek

$$A_{ij} = A_{ji}^*.$$

W przypadku nieskończone wymiarowych przestrzeni Hilberta definicja ta jest niepełna gdyż trzeba mieć świadomość, iż równość operatorów oznacza z definicji równość ich dziedzin, co wymaga wprowadzenia rozróżnienia między operatorami jedynie *symetrycznymi* (tj. spełniającymi równość $\langle \psi | \mathbf{A} | \phi \rangle = \langle \phi | \mathbf{A} | \psi \rangle^*$ dla dowolnych $\psi, \phi \in D(\mathbf{A})$), a operatorami samosprężonymi.

Operatory samosprężone odgrywają wyróżnioną rolę w teorii kwantowej ze względu na trzy twierdzenia, które są dla nich spełnione.

Tw 1.10. Wartości własne operatora samosprężonego są liczbami rzeczywistymi.

Tw 1.11. Zbiór wektorów własnych operatora samosprężonego rozpiną przestrzeń \mathcal{H} .

Tw 1.12. Jeśli widmo operatora samosprężonego nie jest zdegenerowane, to wektory własne tworzą zbiór ortogonalny.

Def 1.18. *Operatorem rzutowym* nazywamy operator \mathbf{P} taki, że $\mathbf{P} = \mathbf{P}^\dagger$ (samosprężoność) i $\mathbf{P}^2 = \mathbf{P}$ (idempotentność).

Ważnym przykładem operatora rzutowego jest operator rzutowania na jednowymiarową podprzestrzeń rozpiętą na unormowanym wektorze $|\phi\rangle$ (rzutowanie na kierunek wektora ϕ), który w notacji Diraca możemy zapisać jako $\mathbf{P} = |\phi\rangle \langle \phi|$ tj. $\forall \psi : \mathbf{P}(\psi) = \langle \phi | \psi \rangle \phi$. Jest to oczywiście operator liniowy, gdyż dla dowolnych wektorów $|\psi_1\rangle, |\psi_2\rangle$ i skalarów α, β mamy

$$\begin{aligned} |\phi\rangle \langle \phi| (\alpha |\psi_1\rangle + \beta |\psi_2\rangle) &= |\phi\rangle \langle \phi | \alpha \psi_1 + \beta \psi_2 \rangle \\ &= \alpha |\phi\rangle \langle \phi | \psi_1 \rangle + \beta |\phi\rangle \langle \phi | \psi_2 \rangle. \end{aligned}$$

Jest również idempotentny, gdyż

$$|\phi\rangle \langle\phi| (|\phi\rangle \langle\phi|\psi\rangle) = |\phi\rangle \langle\phi|\psi\rangle$$

z założenia $\langle\phi|\phi\rangle = 1$ oraz samosprzężony

$$(\langle\psi_1|\phi\rangle \langle\phi|\psi_2\rangle)^* = \langle\psi_1|\phi\rangle^* \langle\phi|\psi_2\rangle^* = \langle\phi|\psi_1\rangle \langle\psi_2|\phi\rangle = \langle\psi_2|\phi\rangle \langle\phi|\psi_1\rangle .$$

Łatwo pokazać również, iż jeśli $\{\phi_i\}$ jest ortonormalnym zbiorem wektorów, to

$$\mathbf{P} = \sum_i |\phi_i\rangle \langle\phi_i|$$

jest operatorem rzutowym. W szczególności, jeśli $\{\phi_i\}$ jest ortonormalną bazą przestrzeni \mathcal{H} , to

$$\sum_i |\phi_i\rangle \langle\phi_i| = \mathbf{1} .$$

Def 1.19. *Operatorem unitarnym* nazywamy operator \mathbf{U} taki, że

$$\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{1} .$$

Przekształcenia unitarne reprezentowane przez operatory unitarne mają użyteczną własność polegającą na zachowywaniu wartości iloczynu wewnętrznego dwóch wektorów, a zatem w szczególności normy wektora

$$\langle\mathbf{U}\psi|\mathbf{U}\phi\rangle = \langle\mathbf{U}^\dagger\mathbf{U}\psi|\phi\rangle = \langle\psi|\phi\rangle .$$

Tw 1.13 (*spektralne*). Niech \mathcal{H} będzie przestrzenią Hilberta. Dla każdego samosprzężonego operatora liniowego \mathbf{A} w \mathcal{H} istnieje unikalna rodzina operatorów rzutowych $\mathbf{P}(\lambda)$ indeksowanych ciąglym parametrem $\lambda \in \mathbb{R}$ taka, że

- $\mathbf{P}(\lambda_1)\mathbf{P}(\lambda_2) = \mathbf{P}(\min(\lambda_1, \lambda_2))$
- $\forall \lambda : \lim_{\epsilon \rightarrow 0^+} \mathbf{P}(\lambda + \epsilon) = \mathbf{P}(\lambda)$
- $\lim_{\lambda \rightarrow -\infty} \mathbf{P}(\lambda) = \mathbf{0}$
- $\lim_{\lambda \rightarrow +\infty} \mathbf{P}(\lambda) = \mathbf{1}$
- $\mathbf{A} = \int_{-\infty}^{+\infty} \lambda d\mathbf{P}(\lambda)$

gdzie ostatnia całka to tzw. *całka Riemanna–Stieltjesa* względem miary operatorowej zdefiniowana jako

$$\int_a^b f(x) d\sigma(x) := \lim_{n \rightarrow \infty} \sum_{k=1}^n f(x_k) [\sigma(x_k) - \sigma(x_{k-1})] ,$$

dla

$$f : \mathbb{R} \mapsto \mathbb{R}, \quad \sigma : \mathbb{R} \mapsto X,$$

gdzie $[a; b] = \bigcup_{k=1}^n [x_{k-1}; x_k]$ jest podziałem normalnym odcinka $[a; b]$. Dodatkowo dla dowolnej funkcji operatora f zachodzi

$$f(\mathbf{A}) = \int_{-\infty}^{+\infty} f(\lambda) d\mathbf{P}(\lambda).$$

W szczególnym przypadku, gdy operator samosprężony \mathbf{A} ma niezdegenerowane widmo $\{\lambda_i\}$ będące zbiorem przeliczalnym, wiemy, że zbiór unormowanych wektorów własnych $\{\phi_i\}$ jest bazą ortonormalną przestrzeni \mathcal{H} , czyli dla dowolnego wektora $\psi \in \mathcal{H}$ możemy zapisać

$$|\psi\rangle = \sum_i c_i |\phi_i\rangle = \sum_i \langle \phi_i | \psi \rangle |\phi_i\rangle,$$

gdzie $c_i = \langle \phi_i | \psi \rangle \in \mathbb{C}$ to współrzędne wektora w zadanej bazie. Działając operatorem \mathbf{A} na wektor ψ mamy

$$\mathbf{A} |\psi\rangle = \sum_i \langle \phi_i | \psi \rangle \mathbf{A} |\phi_i\rangle = \sum_i \langle \phi_i | \psi \rangle \lambda_i |\phi_i\rangle = \left(\sum_i \lambda_i |\phi_i\rangle \langle \phi_i| \right) |\psi\rangle.$$

Całka Stieltjesa z twierdzenia spektralnego przechodzi więc w tym przypadku w sumę (być może nieskończoną) operatorów rzutowych rzutujących na jednowymiarowe podprzestrzenie rozpięte na kolejnych wektorach własnych operatora

$$\mathbf{A} = \sum_i \lambda_i |\phi_i\rangle \langle \phi_i|.$$

1.3 Postulaty teorii kwantów

Poniżej przedstawiono postulaty ogólnej, abstrakcyjnej teorii kwantów. Postulaty te obowiązują we wszystkich realizacjach teorii kwantów np. mechanice falowej, czy kwantowej teorii pola, jednak ze względu na swój ogólny charakter same w sobie nie dostarczają narzędzi do rozwiązywania żadnych konkretnych problemów fizycznych. Nie należy ich również traktować jako podstaw do aksjomatyzacji teorii kwantowej. Stanowią one raczej sposób uporządkowania w spójną strukturę wiedzy dotyczącej konkretnych realizacji teorii kwantów

- I. **O modelu matematycznym.** Modelem matematycznym teorii kwantów jest teoria przestrzeni Hilberta nad ciałem liczb zespolonych i teoria operatorów liniowych działających w tej przestrzeni.
- II. **O pytaniach elementarnych.** Pytaniem elementarnym nazwiemy pytanie, na które odpowiedź może brzmieć jedynie „TAK” lub „NIE”. Pytanie elementarne nazwiemy rozstrzygalnym w obrębie danej teorii kwantowej

iff istnieje wzajemnie jednoznaczne przyporządkowanie tego pytania do pewnego operatora rzutowego \mathbf{P} . Będziemy wówczas mówili, iż dane pytanie elementarne jest reprezentowane przez \mathbf{P} . Każde pytanie elementarne reprezentowane przez \mathbf{P} można zanegować otrzymując pytanie reprezentowane przez $\mathbf{1} - \mathbf{P}$, natomiast dwa pytania elementarne reprezentowane przez \mathbf{P}_1 i \mathbf{P}_2 można połączyć spójnikiem

- „I”; otrzymując pytanie reprezentowane przez $\mathbf{P}_1\mathbf{P}_2$, przy czym musi zachodzić $[\mathbf{P}_1, \mathbf{P}_2] = \mathbf{0}$.
- „LUB”; otrzymując pytanie reprezentowane przez $\mathbf{P}_1 + \mathbf{P}_2$, przy czym musi zachodzić $\mathbf{P}_1\mathbf{P}_2 = \mathbf{0}$.

III. **O stanach układu.** Stan układu fizycznego jest reprezentowany przez unormowany wektor $|\Psi\rangle$ w pewnej przestrzeni Hilberta \mathcal{H} , przy czym utożsamiamy ze sobą wektory różniące się jedynie globalnym czynnikiem fazowym tj. $|\Psi\rangle \sim e^{i\alpha} |\Psi\rangle$, $\alpha \in \mathbb{R}$.

IV. **O prawdopodobieństwach.** Teoria kwantowa dostarcza jedynie probabilistycznych odpowiedzi na rozstrzygalne pytania elementarne. Prawdopodobieństwo p , iż odpowiedź na pytanie elementarne reprezentowane przez \mathbf{P} jest twierdząca, dla układu reprezentowanego przez Ψ wynosi

$$p = \langle \Psi | \mathbf{P} | \Psi \rangle .$$

Zauważmy, że z samosprężoności operatora \mathbf{P} mamy $p = p^*$, więc $p \in \mathbb{R}$, natomiast z nierówności Cauchy’ego–Schwarza mamy

$$\langle \Psi | \Psi \rangle \langle \mathbf{P} \Psi | \mathbf{P} \Psi \rangle = 1 \cdot \langle \Psi | \mathbf{P} | \Psi \rangle = p \geq |\langle \Psi | \mathbf{P} | \Psi \rangle|^2 = p^2 ,$$

skąd $p(p - 1) \leq 0$, co implikuje $p \in [0; 1]$ zgodnie z aksjomatami prawdopodobieństwa.

Operator jednostkowy $\mathbf{1}$ reprezentuje pytanie, na które odpowiedź jest zawsze pozytywna. Jest to więc w istocie pytaniem o istnienie układu.

V. **O wielkościach fizycznych.** Każda wielkość fizyczna A występująca w danej teorii kwantowej jest reprezentowana przez samosprężony operator liniowy \mathbf{A} i stowarzyszoną z nim na mocy twierdzenia spektralnego rodzinę operatorów rzutowych $\mathbf{P}_A(\lambda)$. Operator rzutowy $\mathbf{P}_A(\lambda)$ reprezentuje pytanie:

czy wielkość fizyczna A ma wartość nie większą od λ ?

Na mocy postulatu drugiego możemy skonstruować pytanie:

czy wielkość fizyczna A ma wartość z przedziału $(\lambda_1; \lambda_2]$?

reprezentowane przez operator

$$\mathbf{P}_A(\lambda_1; \lambda_2) = [\mathbf{1} - \mathbf{P}_A(\lambda_1)] \mathbf{P}_A(\lambda_2) = \mathbf{P}_A(\lambda_2) - \mathbf{P}_A(\lambda_1) .$$

Wartość oczekiwaną funkcji f wielkości A dla zespołu statystycznego układów przygotowanych w stanie Ψ obliczamy jako

$$\begin{aligned}\langle f(A) \rangle &= \int_{-\infty}^{+\infty} f(\lambda) \frac{dp(\lambda)}{d\lambda} d\lambda = \int_{-\infty}^{+\infty} f(\lambda) \frac{d \langle \Psi | \mathbf{P}_A(\lambda) | \Psi \rangle}{d\lambda} d\lambda \\ &= \langle \Psi | \left[\int_{-\infty}^{+\infty} f(\lambda) d\mathbf{P}_A(\lambda) \right] | \Psi \rangle = \langle \Psi | f(\mathbf{A}) | \Psi \rangle .\end{aligned}$$

VI. **O ewolucji układu w czasie.** Stan układu $|\Psi\rangle$ ewoluuje zgodnie z *równaniem Schrödingera*

$$\mathbf{H} |\Psi\rangle = i\hbar \partial_t |\Psi\rangle ,$$

gdzie \mathbf{H} jest specjalnym operatorem samosprzężonym reprezentującym hamiltonian układu, tworzonym wedle określonych reguł w danej realizacji teorii kwantów. Równoważnie możemy powiedzieć, iż istnieje operator unitarny $\mathbf{U}(t; t_0)$ taki, że

$$|\Psi(t)\rangle = \mathbf{U}(t; t_0) |\Psi(t_0)\rangle .$$

Istotnie pokażemy, iż ewolucja zgodna z równaniem Schrödingera jest unitarna

$$\frac{d \langle \Psi | \Psi \rangle}{dt} = \langle \dot{\Psi} | \Psi \rangle + \langle \Psi | \dot{\Psi} \rangle = -\frac{1}{i\hbar} \langle \mathbf{H} \Psi | \Psi \rangle + \frac{1}{i\hbar} \langle \Psi | \mathbf{H} \Psi \rangle = 0 ,$$

gdzie w ostatniej linijce skorzystaliśmy z samosprzężoności \mathbf{H} . Powyższy wynik nazywa się również zasadą zachowania prawdopodobieństwa.

VII. **O kolapsie.** Po pomiarze wielkości A układu w stanie $|\Psi\rangle$, który zwrócił wartość z przedziału $(\lambda_1; \lambda_2]$ stan układu zostaje natychmiastowo zredukowany do

$$|\Psi\rangle \rightarrow \frac{\mathbf{P}_A(\lambda_1; \lambda_2) |\Psi\rangle}{\sqrt{\langle \Psi | \mathbf{P}_A(\lambda_1; \lambda_2) | \Psi \rangle}} .$$

VIII. **O układach złożonych.** Przestrzeń Hilberta \mathcal{H} układu złożonego ma strukturę iloczynu tensorowego przestrzeni Hilberta układów prostych wchodzących w jego skład $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$.

Zasady nieoznaczoności

Niech A będzie pewną wielkością fizyczną reprezentowaną przez operator \mathbf{A} . Zdefiniujmy odchylenie standardowe σ_A wielkości A dla układu w stanie Ψ jako

$$\sigma_A := \sqrt{\langle (A - \langle A \rangle)^2 \rangle} = \sqrt{\langle \Psi | \mathbf{A}^2 | \Psi \rangle} ,$$

gdzie $\mathcal{A} := \mathbf{A} - \langle A \rangle$. Dla dowolnych dwóch wielkość fizycznych A i B w układzie reprezentowanym przez Ψ mamy z nierówności Cauchy'ego–Schwarza

$$\sigma_A^2 \sigma_B^2 \geq |\langle \mathcal{A}\Psi | \mathcal{B}\Psi \rangle|^2.$$

Jednocześnie dla dowolnego $z = x + iy \in \mathbb{C}$ mamy

$$|z|^2 = x^2 + y^2 = \left(\frac{z + z^*}{2} \right)^2 + \left(\frac{z - z^*}{2i} \right)^2.$$

Z powyższego mamy więc

$$\sigma_A^2 \sigma_B^2 \geq \left[\frac{1}{2i} (\langle \mathcal{A}\Psi | \mathcal{B}\Psi \rangle - \langle \mathcal{B}\Psi | \mathcal{A}\Psi \rangle) \right]^2 + \left[\frac{1}{2} (\langle \mathcal{A}\Psi | \mathcal{B}\Psi \rangle + \langle \mathcal{B}\Psi | \mathcal{A}\Psi \rangle) \right]^2,$$

skąd po prostych przekształceniach otrzymujemy

$$\sigma_A^2 \sigma_B^2 \geq \left(\frac{1}{2i} \langle \Psi | [\mathbf{A}, \mathbf{B}] | \Psi \rangle \right)^2 + \left(\frac{1}{2} \langle \Psi | \{\mathbf{A}, \mathbf{B}\} | \Psi \rangle - \langle A \rangle \langle B \rangle \right)^2.$$

Powyższą nierówność nazywamy *zasadą nieoznaczoności Schrödingera*. W szczególności z powyższego wynika *zasada nieoznaczoności Robertsona*

$$\sigma_A^2 \sigma_B^2 \geq \left(\frac{1}{2i} \langle \Psi | [\mathbf{A}, \mathbf{B}] | \Psi \rangle \right)^2,$$

która dla operatorów spełniających *kanoniczną relację komutacyjną* $[\mathbf{A}, \mathbf{B}] = i\hbar \mathbf{1}$ przyjmuje postać *zasady nieoznaczoności Heisenberga*

$$\sigma_A \sigma_B \geq \frac{\hbar}{2}.$$

Zauważmy jednakże, iż w rozważanych przez nas n -wymiarowych przestrzeniach Hilberta nie istnieją operatory spełniające kanoniczną relację komutacyjną. Istotnie biorąc ślad z powyższego wyrażenia mamy

$$0 = \text{Tr } \mathbf{AB} - \text{Tr } \mathbf{BA} = i\hbar \neq 0.$$

Twierdzenie Ehrenfesta

Niech A będzie pewną wielkością fizyczną reprezentowaną przez operator \mathbf{A} , wówczas

$$\frac{d\langle A \rangle}{dt} = \frac{d}{dt} \langle \Psi | \mathbf{A} \Psi \rangle = \left\langle \frac{\partial \Psi}{\partial t} | \mathbf{A} \Psi \right\rangle + \left\langle \Psi | \mathbf{A} \frac{\partial \Psi}{\partial t} \right\rangle + \left\langle \Psi | \frac{\partial \mathbf{A}}{\partial t} \Psi \right\rangle.$$

Jednocześnie z równania Schrödingera mamy $\mathbf{H}\Psi = i\hbar \partial_t \Psi$, skąd

$$\frac{d\langle A \rangle}{dt} = \frac{i}{\hbar} \langle \mathbf{H}\Psi | \mathbf{A} \Psi \rangle - \frac{i}{\hbar} \langle \Psi | \mathbf{A} \mathbf{H} \Psi \rangle + \langle \Psi | \frac{\partial \mathbf{A}}{\partial t} | \Psi \rangle,$$

ale ze względu na fakt, iż \mathbf{H} jest operatorem samosprzężonym mamy

$$\frac{d\langle A \rangle}{dt} = \langle \Psi | \frac{\partial \mathbf{A}}{\partial t} | \Psi \rangle + \frac{i}{\hbar} \langle \Psi | [\mathbf{H}, \mathbf{A}] | \Psi \rangle.$$

Powyższe równanie nazywamy *twierdzeniem Ehrenfesta*.

Zasada nieoznaczoności energii–czasu

Z twierdzenia Ehrenfesta dla operatora \mathbf{A} niezależnego od czasu mamy

$$\frac{d\langle A \rangle}{dt} = \frac{i}{\hbar} \langle \Psi | [\mathbf{H}, \mathbf{A}] | \Psi \rangle .$$

Jednocześnie z zasady nieoznaczoności Robertsona mamy

$$\sigma_H^2 \sigma_A^2 \geq \left(\frac{1}{2i} \langle \Psi | [\mathbf{H}, \mathbf{A}] | \Psi \rangle \right)^2 .$$

Podstawiając wyrażenie na wartość oczekiwaną komutatora otrzymujemy z powyższego

$$\sigma_H \sigma_A \geq \frac{\hbar}{2} \left| \frac{d\langle A \rangle}{dt} \right| .$$

Jeśli wartość oczekiwana nie zmienia się w czasie to powyższa nierówność nie mówi nic odkrywczego. Jeśli jednak rozważymy pewien proces, podczas którego wartość oczekiwana zmienia się w czasie Δt o ΔA to możemy dokonać przybliżenia

$$\frac{\sigma_A}{\left| \frac{d\langle A \rangle}{dt} \right|} \approx \frac{|\Delta A|}{|\Delta A|/\Delta t} = \Delta t ,$$

a wówczas z powyższej nierówności otrzymujemy zależność

$$\sigma_H \Delta t \gtrsim \frac{\hbar}{2} ,$$

którą nazywamy *zasadą nieoznaczoności energii–czasu*.

1.4 Kwantowe układy dwupoziomowe

Przedstawimy teraz ważną realizację abstrakcyjnej teorii kwantów – teorię układów dwupoziomowych, które stanowią podstawę teorii obliczeń kwantowych i kwantowej teorii informacji. Modelem matematycznym tej teorii jest skończenie wymiarowa przestrzeń Hilberta

$$\mathcal{H} = ((\mathbb{C}^2, \mathbb{C}, +, \cdot), \langle \cdot | \cdot \rangle)$$

i teoria operatorów liniowych w tej przestrzeni, które możemy utożsamiać z zespolonymi macierzami 2×2 .

1.4.1 Macierze Pauliego

Macierze Pauliego definiujemy jako zespolone macierze 2×2

$$\mathbf{X} := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{Y} := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \mathbf{Z} := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} .$$

Przydatne jest zdefiniowanie *wektora macierzy Pauliego* σ

$$\sigma = (\mathbf{X}, \mathbf{Y}, \mathbf{Z}),$$

dzięki któremu możemy łatwo zapisać sumę przeskalowanych macierzy Pauliego jako $\mathbf{c} \cdot \sigma$, gdzie $\mathbf{c} \in \mathbb{C}^3$ jest pewnym wektorem o elementach zespolonych.

$\mathbf{XY} = i\mathbf{Z} = -\mathbf{YX}$	$[\mathbf{X}, \mathbf{Y}] = 2i\mathbf{Z}$	$\{\mathbf{X}, \mathbf{Y}\} = \mathbf{0}$
$\mathbf{YZ} = i\mathbf{X} = -\mathbf{ZY}$	$[\mathbf{Y}, \mathbf{Z}] = 2i\mathbf{X}$	$\{\mathbf{Y}, \mathbf{Z}\} = \mathbf{0}$
$\mathbf{ZX} = i\mathbf{Y} = -\mathbf{XZ}$	$[\mathbf{Z}, \mathbf{X}] = 2i\mathbf{Y}$	$\{\mathbf{Z}, \mathbf{X}\} = \mathbf{0}$
$\mathbf{X}^2 = \mathbf{Y}^2 = \mathbf{Z}^2 = \mathbf{1}$	$\text{Tr } \mathbf{X} = \text{Tr } \mathbf{Y} = \text{Tr } \mathbf{Z} = 0$	$\det \mathbf{X} = \det \mathbf{Y} = \det \mathbf{Z} = -1$
$e^{i\mathbf{a} \cdot \sigma} = \mathbf{1} \cos \mathbf{a} + i\hat{\mathbf{a}} \cdot \sigma \sin \mathbf{a} $		
$(\mathbf{a} \cdot \sigma) \cdot (\mathbf{b} \cdot \sigma) = (\mathbf{a} \cdot \mathbf{b})\mathbf{1} + i(\mathbf{a} \times \mathbf{b}) \cdot \sigma$		

Tabela 1: Wybrane własności macierzy Pauliego

Zauważmy, że dowolny operator samosprężony \mathbf{A} w rozpatrywanej przestrzeni \mathcal{H} ma postać

$$\mathbf{A} = \begin{bmatrix} a_0 + a_z & a_x - ia_y \\ a_x + ia_y & a_0 - a_z \end{bmatrix} = a_0 \mathbf{1} + \mathbf{a} \cdot \sigma,$$

gdzie $a_0, a_x, a_y, a_z \in \mathbb{R}$. Jednocześnie bez straty ogólności możemy przyjąć $a_0 = 0$, gdyż stała ta przesuwaa jedynie widmo operatora \mathbf{A} o ustaloną wartość, co pozwala przedstawić dowolny operator samosprężony jako wektor \mathbf{a} w trójwymiarowej przestrzeni.

1.4.2 Sfera Blocha

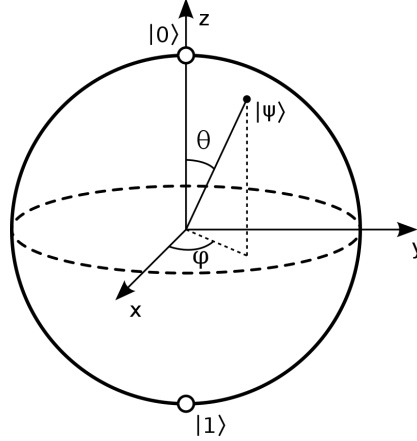
W trójwymiarowej przestrzeni możemy również przedstawić wektor stanu Ψ . Istotnie wektor stanu jest określony przez 2 zmienne zespolone

$$|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

czyli 4 zmienne rzeczywiste, ale ze względu na warunek unormowania $|\alpha|^2 + |\beta|^2 = 1$ mamy tylko 3 zmienne niezależne. Dodatkowo pamiętając, iż globalna faza wektora stanu nie ma znaczenia możemy wyeliminować jeszcze jedną zmienną i zapisać wektor Ψ jako

$$|\Psi\rangle = \cos \frac{\theta}{2} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + e^{i\phi} \sin \frac{\theta}{2} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$$

dla pewnych parametrów $\phi, \theta \in \mathbb{R}$. Powyżej wektory bazy ortonormalnej oznaczyliśmy jako $\{|0\rangle, |1\rangle\}$ zgodnie z oznaczeniami stosowanymi w teorii obliczeń kwantowych (w szczególności $|0\rangle$ *nie oznacza* w powyższej notacji wektora zerowego 0). Zmienne ϕ, θ możemy interpretować odpowiednio jako kąt azymutalny i kąt zenitalny punktu na sferze jednostkowej, którą nazywamy *sferą Blocha*. Zauważmy, iż przy wybranej parametryzacji bieguny sfery określają odpowiednio stany $|0\rangle$ i $|1\rangle$.



Rysunek 1: Sfera Blocha

Możemy połączyć oba przedstawienia tj. przedstawienia operatora i wektora stanu jeśli tylko zamiast wektora stanu użyjemy operatora rzutowania na stan Ψ . Możemy rozłożyć go wówczas (jak każdy operator samosprężony) na macierze Pauliego

$$|\Psi\rangle\langle\Psi| = s_0\mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma},$$

przy czym parametry s_0, s_x, s_y, s_z muszą spełniać

$$|\Psi\rangle\langle\Psi||\Psi\rangle\langle\Psi| = |\Psi\rangle\langle\Psi|,$$

czyli

$$s_0\mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma} = (s_0^2 + |\mathbf{s}|^2)\mathbf{1} + 2s_0\mathbf{s} \cdot \boldsymbol{\sigma},$$

skąd $s_0 = |\mathbf{s}| = 1/2$. Operator rzutowania $|\Psi\rangle\langle\Psi|$ możemy zatem w ogólności rozłożyć na macierze Pauliego w następujący sposób

$$|\Psi\rangle\langle\Psi| = \frac{1}{2}(\mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma}),$$

gdzie przeskalowaliśmy zmienne s_x, s_y, s_z tak, że teraz $|\mathbf{s}| = 1$.

Widzimy więc, iż stan Ψ możemy reprezentować jako wektor \mathbf{s} określający punkt na sferze jednostkowej w trójwymiarowej przestrzeni, a operator samosprężony jako dowolny wektor \mathbf{a} w tej przestrzeni. Przejście od rzeczywistego

wektora \mathbf{s} do abstrakcyjnego wektora stanu $|\Psi\rangle$ odbywa się poprzez określenie współrzędnych sferycznych (θ, ϕ) wektora \mathbf{s} i zmapowanie ich zgodnie z przepisem

$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle .$$

1.4.3 Ewolucja układu dwupoziomowego

Dla układów dwupoziomowych ogólne równania ewolucji amplitud prawdopodobieństwa wektora stanu

$$|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

dla hamiltonianu postaci

$$\mathbf{H} = \begin{bmatrix} H_{11}(t) & H_{12}(t) \\ H_{21}(t) & H_{22}(t) \end{bmatrix}$$

mają postać

$$\begin{cases} i\hbar\dot{\alpha} = H_{11}(t)\alpha + H_{12}(t)\beta \\ i\hbar\dot{\beta} = H_{21}(t)\alpha + H_{22}(t)\beta \end{cases}$$

Równanie ewolucji możemy zapisać również wykorzystując przedstawienie geometryczne wektorów stanu i operatorów na sferze Blocha. Istotnie różniczkując operator rzutowy $\rho = |\Psi\rangle\langle\Psi|$ mamy

$$\begin{aligned} \frac{\partial \rho}{\partial t} &= \left| \dot{\Psi} \right\rangle \langle \Psi | + |\Psi\rangle \left\langle \dot{\Psi} \right| = \frac{1}{i\hbar} |\mathbf{H}\Psi\rangle \langle \Psi| - \frac{1}{i\hbar} |\Psi\rangle \langle \mathbf{H}\Psi| \\ &= \frac{1}{i\hbar} (\mathbf{H}\rho - \rho\mathbf{H}) = \frac{1}{i\hbar} [\mathbf{H}, \rho] . \end{aligned}$$

Z powyższego mamy więc dla $\rho = \frac{1}{2}(\mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma})$ i $\mathbf{H} = \mathbf{H} \cdot \boldsymbol{\sigma}$

$$\frac{\hbar}{2} \dot{\mathbf{s}} = \mathbf{H} \times \mathbf{s}$$

Przedstawienie geometryczne wektora stanu na sferze Blocha nie jest jedynie obserwacją matematyczną. Pozwala ono zwizualizować semi-klasyczną ewolucję wektorowej wielkości fizycznej \mathbf{S} , której składowe S_x, S_y, S_z są w przestrzeni \mathcal{H} reprezentowane przez samosprężone operatory Pauliego $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$. Istotnie zgodnie z twierdzeniem Ehrenfesta

$$\frac{d\langle \mathbf{S} \rangle}{dt} = \frac{i}{\hbar} \langle \Psi | [\mathbf{H}, \boldsymbol{\sigma}] | \Psi \rangle = \frac{i}{\hbar} \langle \Psi | ([\mathbf{H}, \mathbf{X}], [\mathbf{H}, \mathbf{Y}], [\mathbf{H}, \mathbf{Z}]) | \Psi \rangle .$$

Jednocześnie dla $\mathbf{H} = \mathbf{H} \cdot \boldsymbol{\sigma}$

$$\begin{aligned} [\mathbf{H}, \mathbf{X}] &= -2iH_y\mathbf{Z} + 2iH_z\mathbf{Y} \\ [\mathbf{H}, \mathbf{Y}] &= -2iH_z\mathbf{X} + 2iH_x\mathbf{Z} , \\ [\mathbf{H}, \mathbf{Z}] &= -2iH_x\mathbf{Y} + 2iH_y\mathbf{X} \end{aligned}$$

skąd

$$\frac{\hbar}{2} \frac{d \langle \mathbf{S} \rangle}{dt} = \mathbf{H} \times \langle \mathbf{S} \rangle .$$

Widzimy zatem, iż ruch wektora \mathbf{s} po sferze Blocha odpowiada ewolucji wartości oczekiwanej wielkości fizycznej \mathbf{S} , którą to ewolucję możemy w przybliżeniu semi-klasycznym traktować jako faktyczną ewolucję tych wielkości.

1.4.4 Obroty na sferze Blocha

Powyższe rozważania pokazują, iż w przedstawieniu geometrycznym stan Ψ reprezentowany przez jednostkowy wektor \mathbf{s} na sferze Blocha ewoluuje w taki sposób, iż efektywnie jego położenie na sferze Blocha w czasie t można przedstawić jako obrót wektora położenia w czasie t_0 o pewien kąt φ wokół ustalonej osi $\hat{\mathbf{n}}$

$$\mathbf{s}(t) = \overleftrightarrow{\mathbf{R}}_{\hat{\mathbf{n}}}(\varphi) \mathbf{s}(t_0) .$$

W ujęciu abstrakcyjnego wektora $|\Psi\rangle$ przekształcenie to odpowiada oczywiście pewnemu przekształceniu unitarnemu \mathbf{U} , tj.

$$|\Psi(t)\rangle = \mathbf{U} |\Psi(t_0)\rangle .$$

Warte zbadania wydaje się więc wyznaczenie operatora \mathbf{U} , który odpowiada obrotowi na sferze Blocha. Aby wyznaczyć jawny wzór na operator \mathbf{U} rozważmy nieskończenie mały obrót wektora \mathbf{s} wokół osi $\hat{\mathbf{n}}$ o kąt ϵ . Jak łatwo pokazać

$$\mathbf{s}' = \overleftrightarrow{\mathbf{R}}_{\hat{\mathbf{n}}}(\epsilon) \mathbf{s} = \mathbf{s} + \epsilon (\mathbf{s} \times \hat{\mathbf{n}})$$

w przybliżeniu do wyrazów liniowych względem ϵ . Wektor rzeczywisty \mathbf{s} najłatwiej powiązać z abstrakcyjnym wektorem $|\Psi\rangle$ poprzez operator rzutowy $\boldsymbol{\rho} = |\Psi\rangle \langle \Psi|$ dla którego zachodzi

$$|\mathbf{U}\Psi\rangle \langle \mathbf{U}\Psi| = \mathbf{U} \boldsymbol{\rho} \mathbf{U}^\dagger = \frac{1}{2} (\mathbf{1} + \mathbf{s}' \cdot \boldsymbol{\sigma}) ,$$

skąd

$$\mathbf{s} \cdot \mathbf{U} \boldsymbol{\sigma} \mathbf{U}^\dagger = (\mathbf{s} + \epsilon (\mathbf{s} \times \hat{\mathbf{n}})) \cdot \boldsymbol{\sigma} = \mathbf{s} \cdot (\boldsymbol{\sigma} + \epsilon (\hat{\mathbf{n}} \times \boldsymbol{\sigma})) .$$

Otrzymujemy zatem równanie

$$\mathbf{U} \boldsymbol{\sigma} \mathbf{U}^\dagger = \boldsymbol{\sigma} + \epsilon (\hat{\mathbf{n}} \times \boldsymbol{\sigma}) .$$

Poszukajmy \mathbf{U} spełniających to równanie postaci

$$\mathbf{U} = \mathbf{1} + i\epsilon \mathbf{A} , \quad \mathbf{U}^\dagger = \mathbf{1} - i\epsilon \mathbf{A}^\dagger ,$$

gdzie \mathbf{A} jest operatorem samosprężonym postaci $\mathbf{A} = \mathbf{a} \cdot \boldsymbol{\sigma}$. Zauważmy, iż tak zdefiniowany \mathbf{U} jest unitarny w przybliżeniu do wyrazów liniowych względem ϵ . Podstawiając powyższe wzory na \mathbf{U} oraz \mathbf{U}^\dagger i ograniczając się do wyrazów liniowych względem ϵ otrzymujemy

$$i\epsilon [\mathbf{A}, \boldsymbol{\sigma}] = \epsilon (\hat{\mathbf{n}} \times \boldsymbol{\sigma}) .$$

Widzimy zatem, iż taki, a nie inny strzał na postać operatora \mathbf{U} był podyktowany wyprowadzonymi wcześniej wzorami na komutatory operatora samosprężonego z operatorami Pauliego, które naśladują strukturę zwykłego trójwymiarowego iloczynu wektorowego. Z powyższego otrzymujemy zatem $\mathbf{a} = \frac{1}{2}\hat{\mathbf{n}}$, skąd

$$\mathbf{U} = \mathbf{1} + \frac{i\epsilon}{2}\hat{\mathbf{n}} \cdot \boldsymbol{\sigma}.$$

Stąd łatwo możemy już uzyskać operator unitarny $\mathbf{U}_{\hat{\mathbf{n}}}(\varphi)$ odpowiadający obrotowi o kąt φ wokół osi $\hat{\mathbf{n}}$

$$\mathbf{U}_{\hat{\mathbf{n}}}(\varphi) = \lim_{N \rightarrow \infty} \left(\mathbf{1} + \frac{i\varphi}{2N}\hat{\mathbf{n}} \cdot \boldsymbol{\sigma} \right)^N = \exp \left\{ \frac{i}{2}\varphi \hat{\mathbf{n}} \cdot \boldsymbol{\sigma} \right\} = \mathbf{1} \cos \frac{\varphi}{2} + i(\hat{\mathbf{n}} \cdot \boldsymbol{\sigma}) \sin \frac{\varphi}{2}$$

W szczególności dla obrotów wokół osi x, y, z mamy odpowiednio

$$\begin{aligned} \mathbf{U}_{\hat{\mathbf{x}}}(\varphi) &= \begin{bmatrix} \cos \frac{\varphi}{2} & i \sin \frac{\varphi}{2} \\ i \sin \frac{\varphi}{2} & \cos \frac{\varphi}{2} \end{bmatrix} \\ \mathbf{U}_{\hat{\mathbf{y}}}(\varphi) &= \begin{bmatrix} \cos \frac{\varphi}{2} & \sin \frac{\varphi}{2} \\ -\sin \frac{\varphi}{2} & \cos \frac{\varphi}{2} \end{bmatrix} \\ \mathbf{U}_{\hat{\mathbf{z}}}(\varphi) &= \begin{bmatrix} e^{+i\varphi/2} & 0 \\ 0 & e^{-i\varphi/2} \end{bmatrix} \end{aligned}.$$

1.4.5 Przykład – magnetyczny rezonans jądrowy

Rozpatrzmy cząstkę obdarzoną momentem magnetycznym μ o spinie połówkowym i nie posiadającą ładunku elektrycznego (neutron), która została umieszczona w wirującym z częstością radiową polu magnetycznym

$$\mathbf{B}(t) = B_{\text{rf}} \cos(\omega t) \hat{\mathbf{x}} - B_{\text{rf}} \sin(\omega t) \hat{\mathbf{y}} + B_0 \hat{\mathbf{z}}.$$

Cząstka ta stanowi pewien układ dwupoziomowy, którego oddziaływanie z polem magnetycznym jest opisane hamiltonianem Pauliego

$$\mathbf{H} = -\mu \mathbf{B} \cdot \boldsymbol{\sigma} = -\mu \begin{bmatrix} B_0 & B_{\text{rf}} e^{+i\omega t} \\ B_{\text{rf}} e^{-i\omega t} & -B_0 \end{bmatrix}.$$

Równania ewolucji na amplitudy prawdopodobieństwa mają więc postać

$$\begin{cases} \frac{1}{i\omega_0} \dot{\alpha} = n e^{+i\omega t} \beta + \alpha \\ \frac{1}{i\omega_0} \dot{\beta} = n e^{-i\omega t} \alpha - \beta \end{cases},$$

gdzie wprowadziliśmy parametry $\omega_0 := \mu B_0 / \hbar$ i $n := B_{\text{rf}} / B_0$. Łatwo sprawdzić, iż rozwiązaniem powyższego układu równań jest

$$\begin{cases} \alpha(t) = (c_1 e^{+i\Omega t} + c_2 e^{-i\Omega t}) n e^{+i\omega t/2} \\ \beta(t) = [c_1(\Omega - \delta) e^{+i\Omega t} - c_2(\Omega + \delta) e^{-i\Omega t}] \omega_0^{-1} e^{-i\omega t/2} \end{cases},$$

gdzie

$$\delta = \omega_0 - \frac{\omega}{2}, \quad \Omega = \sqrt{n^2 \omega_0^2 + \delta^2}.$$

Zdefiniowaną wielkość Ω nazywamy *częstością Rabiego*. Załóżmy, iż w chwili początkowej $\alpha = 0$ i $\beta = 1$, wówczas

$$\begin{aligned} \alpha(t) &= \frac{i n \omega_0}{\Omega} \sin(\Omega t) e^{+i \omega t / 2} \\ \beta(t) &= \left\{ \cos(\Omega t) + \frac{i}{\Omega} \left(\frac{1}{2} \omega - \omega_0 \right) \sin(\Omega t) \right\} e^{-i \omega t / 2} \end{aligned}$$

Z powyższego prawdopodobieństwo $p_{1 \rightarrow 0}$ znalezienia układu w stanie $|0\rangle$ wynosi

$$p_{1 \rightarrow 0}(t) = |\alpha|^2 = \left(\frac{n \omega_0}{\Omega} \right)^2 \sin^2(\Omega t) = \frac{1}{2} \left(\frac{n \omega_0}{\Omega} \right)^2 (1 - \cos(2\Omega t)).$$

Natomiast prawdopodobieństwo $p_{1 \rightarrow 1}$ znalezienia układu w stanie $|1\rangle$ wynosi

$$p_{1 \rightarrow 1}(t) = |\beta|^2 = \cos^2(\Omega t) + \left(\frac{\omega_0 - \frac{1}{2}\omega}{\Omega} \right)^2 \sin^2(\Omega t) = 1 - p_{1 \rightarrow 0}(t).$$

Prawdopodobieństwa oscylują w czasie z częstością równą podwojonej częstości Rabiego. Amplituda tych oscylacji wynosi

$$\frac{1}{2} \left(\frac{n \omega_0}{\Omega} \right)^2 = \frac{n^2 \omega_0^2}{2} \frac{1}{(\omega_0 - \frac{1}{2}\omega)^2 + (n \omega_0)^2}$$

i przyjmuje wartość maksymalną, gdy spełniony jest *warunek rezonansu* postaci

$$\hbar \omega = 2 \mu B_0.$$

Zauważmy, iż opisane zjawisko stanowi podstawę do manipulacji qbitami. Istotnie w stanie rezonansu wektor stanu ewoluuje zgodnie z

$$|\Psi(t)\rangle = \alpha(t) |0\rangle + \beta(t) |1\rangle = i \sin(\Omega t) e^{+i \omega_0 t} |0\rangle + \cos(\Omega t) e^{-i \omega_0 t} |1\rangle$$

Poprzez dostosowanie czasu t przez jaki układ dwupoziomowy oddziałuje z wirowym polem możemy sterować stanem Ψ w jakim się znajduje, przykładowo jeśli początkowo układ był w stanie $|1\rangle$ to włączając wirowe pole magnetyczne na czas $t = \pi/2\Omega$ (tzw. *impuls* π , gdyż na sferze Blocha odpowiada mu obrót o π) układ przechodzi do stanu $|0\rangle$ (pomijając nieistotny globalny czynnik fazowy), natomiast dla $t = \pi/4\Omega$ (tzw. *impuls* $\pi/2$) układ przechodzi do stanu

$$\frac{1}{\sqrt{2}} (i e^{+i \omega_0 t} |0\rangle + e^{-i \omega_0 t} |1\rangle),$$

w którym mamy jednakowe prawdopodobieństwa odpowiedzi twierdzących na pytania $|0\rangle\langle 0|$ i $|1\rangle\langle 1|$.

Dla atomu z dwoma poziomami energetycznymi poddanemu działaniu wiązki laserowej otrzymuje się identyczne równanie pod warunkiem przyjęcia przybliżenia tzw. *wirującej fali*, które jest prawdziwe, gdy długość fali jest znacznie większa od rozmiarów próbki. W tym przypadku $2\hbar\omega_0$ jest różnicą energii między dwoma poziomami atomowymi, ω jest częstotliwością laserową, a iloczyn μB_{rf} przechodzi na iloczyn elektrycznego momentu dipolowego atomu i amplitudy pola elektrycznego fali elektromagnetycznej pE_0 .

1.5 Korelacje kwantowe

Wydawałoby się, że przejście od układów jednoqbitowych (dwupoziomowych) to układów złożonych dwuqbitowych nie wniesie wiele nowości. Tymczasem jak się przekonamy struktura z dwoma qbitami jest wyjątkowo bogata.

1.5.1 Stany dwuqbitowe

Rozważmy dwa układy dwupoziomowe A, B , których modelem matematycznym są przestrzenie Hilberta $\mathcal{H}_A = \{|0_A\rangle, |1_A\rangle\}$, $\mathcal{H}_B = \{|0_B\rangle, |1_B\rangle\}$ (zauważmy, iż w przypadku przestrzeni skończonego wymiaru podanie wektorów bazy ortonormalnej w jakiej pracujemy w pełni charakteryzuje przestrzeń Hilberta nad \mathbb{C}). Ogólne stany układów A i B mają więc postać

$$|\Psi_A\rangle = \psi_0^{(A)} |0_A\rangle + \psi_1^{(A)} |1_A\rangle, \quad |\Psi_B\rangle = \psi_0^{(B)} |0_B\rangle + \psi_1^{(B)} |1_B\rangle,$$

gdzie oczywiście $|\psi_0^{(A)}|^2 + |\psi_1^{(A)}|^2 = 1 = |\psi_0^{(B)}|^2 + |\psi_1^{(B)}|^2$. Zgodnie z postulatem o układach złożonych układ złożony z podukładów A, B jest opisany przestrzenią Hilberta $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Ogólny stan układu złożonego ma zatem postać

$$\begin{aligned} |\Psi_{AB}\rangle &= \psi_{00} |0_A\rangle \otimes |0_B\rangle + \psi_{01} |0_A\rangle \otimes |1_B\rangle + \psi_{10} |1_A\rangle \otimes |0_B\rangle + \psi_{11} |1_A\rangle \otimes |1_B\rangle \\ &= \psi_{00} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \psi_{01} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \psi_{10} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \psi_{11} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \\ &= \psi_{00} |0_A 0_B\rangle + \psi_{01} |0_A 1_B\rangle + \psi_{10} |1_A 0_B\rangle + \psi_{11} |1_A 1_B\rangle. \end{aligned}$$

Jaką informację zawiera wektor stanu układu złożonego? Jeśli istnieje faktoryzacja $|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$ to wówczas wektor stanu układu złożonego mówi, iż A znajduje się w stanie $|\Psi_A\rangle$, a B w stanie $|\Psi_B\rangle$. Zauważmy jednak, iż w ogólności taka faktoryzacja nie musi być możliwa. Istotnie jeśli $|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$ to

$$\begin{aligned} |\Psi_{AB}\rangle &= \begin{bmatrix} \psi_0^{(A)} \\ \psi_1^{(A)} \end{bmatrix} \otimes \begin{bmatrix} \psi_0^{(B)} \\ \psi_1^{(B)} \end{bmatrix} \\ &= \psi_0^{(A)} \psi_0^{(B)} |0_A 0_B\rangle + \psi_0^{(A)} \psi_1^{(B)} |0_A 1_B\rangle + \psi_1^{(A)} \psi_0^{(B)} |1_A 0_B\rangle + \psi_1^{(A)} \psi_1^{(B)} |1_A 1_B\rangle, \end{aligned}$$

czyli współczynniki $\psi_{q_A q_B}$ muszą spełniać

$$\psi_{00} \psi_{11} = \psi_{01} \psi_{10},$$

przy czym jest to warunek konieczny i wystarczający. Stany Ψ_{AB} , dla których powyższy warunek nie zachodzi nazywamy *stanami splątanymi*. W ogólności więc współczynniki $\psi_{q_A q_B}$ są amplitudami prawdopodobieństw znalezienia układu A w stanie q_A i układu B w stanie q_B (zauważmy, iż w przypadku N qbitów potrzebujemy 2^N współczynników $\psi_{q_1 q_2 \dots q_N}$, gdyż możliwych konfiguracji, których amplitudy prawdopodobieństwa musimy określić jest właśnie 2^N).

Operatory

W ogólności operatory liniowe w przestrzeni \mathcal{H}_{AB} są zespolonymi macierzami 4×4 . Jednakże interesować nas będą głównie operatory liniowe postaci

$$\mathbf{M} = \mathbf{M}_A \otimes \mathbf{M}_B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{bmatrix},$$

gdzie $\mathbf{M}_A, \mathbf{M}_B$ są operatorami liniowymi w przestrzeniach $\mathcal{H}_A, \mathcal{H}_B$. Nietrudno zauważyć, iż jeśli $\mathbf{M}_A, \mathbf{M}_B$ są samosprężone to $\mathbf{M}_A \otimes \mathbf{M}_B$ również jest samosprężony. Dodatkowo jeśli $\mathbf{P}_A, \mathbf{P}_B$ są operatorami rzutowymi to $\mathbf{P}_A \otimes \mathbf{P}_B$ również jest operatorem rzutowym tylko że w przestrzeni \mathcal{H} . Istotnie dla dowolnych operatorów $(\mathbf{P}_A \otimes \mathbf{P}_B)^2 = \mathbf{P}_A^2 \otimes \mathbf{P}_B^2$, więc dla operatorów rzutowych mamy $(\mathbf{P}_A \otimes \mathbf{P}_B)^2 = \mathbf{P}_A \otimes \mathbf{P}_B$ i wiemy, że $\mathbf{P}_A \otimes \mathbf{P}_B$ jest samosprężony. Można również pokazać, iż jeśli $\mathbf{U}_A, \mathbf{U}_B$ są unitarne to $\mathbf{U}_A \otimes \mathbf{U}_B$ również jest unitarny. Istotnie dla dowolnych operatorów $(\mathbf{U}_A \otimes \mathbf{U}_B)^\dagger = \mathbf{U}_A^\dagger \otimes \mathbf{U}_B^\dagger$ i $(\mathbf{U}_A \otimes \mathbf{U}_B)^{-1} = \mathbf{U}_A^{-1} \otimes \mathbf{U}_B^{-1}$, więc dla operatorów unitarnych $(\mathbf{U}_A \otimes \mathbf{U}_B)^\dagger = (\mathbf{U}_A \otimes \mathbf{U}_B)^{-1}$.

Niech M będzie pewną wielkością fizyczną określającą układ A reprezentowaną w przestrzeni \mathcal{H}_A przez \mathbf{M} . W przestrzeni \mathcal{H}_{AB} ta wielkość jest reprezentowana przez $\mathbf{M} \otimes \mathbf{1}_B$. Jeśli $\mathbf{P}_M(\lambda_1; \lambda_2)$ jest operatorem rzutowym reprezentującym w przestrzeni \mathcal{H}_A pytanie o wartość wielkości M , to w przestrzeni \mathcal{H}_{AB} (tj. jeśli A jest częścią większego układu AB) pytanie to reprezentuje operator $\mathbf{P}_M(\lambda_1; \lambda_2) \otimes \mathbf{1}_B$.

1.5.2 Operator gęstości

Jak wspomnieliśmy ogólny stan układu złożonego Ψ_{AB} nie ma postaci $|\Psi_A\rangle \otimes |\Psi_B\rangle$ i wówczas nazywamy go stanem splątanym. Podstawową cechą układu splątanego jest fakt, iż jeśli $|\Psi_{AB}\rangle$ jest stanem splątanym to dla dowolnej wielkości fizycznej M określającej podukład A nie istnieje stan $|\Psi_A\rangle$, dla którego

$$p = \langle \Psi_{AB} | \mathbf{P} \otimes \mathbf{1}_B | \Psi_{AB} \rangle = \langle \Psi_A | \mathbf{P} | \Psi_A \rangle.$$

Istotnie zakładając $|\Psi_A\rangle = \psi_0 |0_A\rangle + \psi_1 |1_A\rangle$

$$\langle \Psi_A | \mathbf{P} | \Psi_A \rangle = \sum_{i,j} \psi_i^* \psi_j \langle i_A | \mathbf{P} | j_A \rangle = \text{Tr}(\mathbf{P} |\Psi_A\rangle \langle \Psi_A|)$$

oraz

$$\begin{aligned}
\langle \Psi_{AB} | \mathbf{P} \otimes \mathbf{1}_B | \Psi_{AB} \rangle &= \langle \Psi_{AB} | \mathbf{P} \otimes \mathbf{1}_B \sum_{k,l} \psi_{kl} |k_A l_B\rangle \\
&= \langle \Psi_{AB} | \sum_{k,l} \psi_{k,l} \mathbf{P} |k_A\rangle \otimes |l_B\rangle = \sum_{i,j} \psi_{ij}^* \langle i_A j_B | \sum_{k,l} \psi_{k,l} \mathbf{P} |k_A\rangle \otimes |l_B\rangle \\
&= \sum_{i,j,k,l} \psi_{ij}^* \psi_{kl} \langle i_A j_B | (\mathbf{P} |k_A\rangle \otimes |l_B\rangle) = \sum_{i,j,k,l} \psi_{ij}^* \psi_{kl} \langle i_A | \mathbf{P} |k_A\rangle \otimes \langle j_B | l_B\rangle \\
&= \sum_{i,j,k,l} \psi_{ij}^* \psi_{kl} \delta_{jl} \langle i_A | \mathbf{P} |k_A\rangle = \sum_{i,j,k} \psi_{ij}^* \psi_{kj} \langle i_A | \mathbf{P} |k_A\rangle .
\end{aligned}$$

Zauważmy, iż definiując $\rho_{ki} = \sum_j \psi_{kj} \psi_{ij}^*$ możemy zapisać

$$\langle \Psi_{AB} | \mathbf{P} \otimes \mathbf{1}_B | \Psi_{AB} \rangle = \sum_{i,k} \rho_{ki} \langle i_A | \mathbf{P} |k_A\rangle = \text{Tr}(\mathbf{P}\boldsymbol{\rho}) ,$$

gdzie jawnie

$$\boldsymbol{\rho} = \begin{bmatrix} |\psi_{00}|^2 + |\psi_{01}|^2 & \psi_{00}\psi_{10}^* + \psi_{01}\psi_{11}^* \\ \psi_{10}\psi_{00}^* + \psi_{11}\psi_{01}^* & |\psi_{10}|^2 + |\psi_{11}|^2 \end{bmatrix}$$

Operator $\boldsymbol{\rho}$ nazywamy *operatorem gęstości*. Zauważmy, że operator gęstości jest operatorem samosprzężonym $\boldsymbol{\rho}^\dagger = \boldsymbol{\rho}$, nieujemnie określonym (wystarczy zauważyć, że $\langle \Phi | \boldsymbol{\rho} | \Phi \rangle = |\phi_0\psi_{00} + \phi_1\psi_{10}|^2 + |\phi_0\psi_{01} + \phi_1\psi_{11}|^2 \geq 0$), o śladzie równym jedności $\text{Tr} \boldsymbol{\rho} = 1$.

Jednocześnie

$$|\Psi_A\rangle\langle\Psi_A| = \begin{bmatrix} |\psi_0|^2 & \psi_0^*\psi_1 \\ \psi_0\psi_1^* & |\psi_1|^2 \end{bmatrix} .$$

więc z operatora gęstości można wyciągnąć stan $|\Psi_A\rangle$ iff

$$(|\psi_{00}|^2 + |\psi_{01}|^2)(|\psi_{10}|^2 + |\psi_{11}|^2) = (\psi_{10}\psi_{00}^* + \psi_{11}\psi_{01}^*)(\psi_{00}\psi_{10}^* + \psi_{01}\psi_{11}^*)$$

skąd

$$|\psi_{01}\psi_{10} - \psi_{00}\psi_{11}|^2 = 0 ,$$

skąd $\psi_{01}\psi_{10} = \psi_{00}\psi_{11}$, czyli gdy stan Ψ_{AB} nie jest stanem splątany. W ogólności jednak jeśli A jest podukładem układu złożonego AB to informacja o nim (w sensie prawdopodobieństw wyników pomiarów wielkości fizycznych) nie jest opisywana przez wektor stanu tylko przez macierz gęstości $\boldsymbol{\rho}$, a prawdopodobieństwa i wartości oczekiwane są dane przez ślady

$$p = \text{Tr}(\mathbf{P}_M(\lambda_1; \lambda_2)\boldsymbol{\rho}) , \quad \langle M \rangle = \text{Tr}(\mathbf{M}\boldsymbol{\rho}) .$$

2 Obliczenia kwantowe

Algorytm RSA

Bob wybiera dwie liczby pierwsze $p, q \in \mathbb{P}$, oblicza liczbę $N = pq$ oraz wybiera liczbę $c \perp \phi(N) = (p-1)(q-1)$, gdzie ϕ to funkcja Eulera (liczbę c nazywamy

kluczem publicznym). Następnie oblicza odwrotność liczby c modulo $\phi(N)$, tj. liczbę d taką, że $cd \equiv_{\phi(N)} 1$ (liczbę d nazywamy *kluczem prywatnym*). Istnienie liczby d zapewnia twierdzenie Eulera, istotnie wynika z niego, iż d można obliczyć jako (przy czym nie jest to efektywne i zwykle używa się rozszerzonego algorytmu Euklidesa)

$$c^{\phi(\phi(N))} \equiv_{\phi(N)} c \cdot c^{\phi(\phi(N))-1} \equiv_{\phi(N)} 1 \implies d \equiv_{\phi(N)} c^{\phi(\phi(N))-1}.$$

Bob wysyła następnie Alicji niezabezpieczoną drogą liczby c i N .

Założmy, że Alicja chce wysłać do Boba zaszyfrowaną wiadomość reprezentowaną przez liczbę $a < N$. Aby to zrobić Alicja oblicza liczbę $b \equiv_N a^c$ i wysyła ją do Boba niezabezpieczoną drogą.

Bob odczytuje wiadomość obliczając

$$b^d \equiv_N a^{cd} \equiv_N a.$$

Powyższa równość wynika z Małego Twierdzenia Fermata. Istotnie zauważmy wpierw, iż jeśli $p \perp q$ to $x \equiv_p y$ i $x \equiv_q y$ implikują $x \equiv_{pq} y$. Istotnie z założeń wynika, iż $\exists k, k' \in \mathbb{Z}$ takie, że $x - y = kp = k'q$, ale ponieważ $p \perp q$ to $q|k$ (i analogicznie $p|k'$), więc istnieje $k'' \in \mathbb{Z}$ takie, że $x - y = k''pq$. Do udowodnienia powyższej równości wystarczy zatem pokazać, iż $a^{cd} \equiv_p a$ i $a^{cd} \equiv_q a$. Pokażemy dowód dla p (dowód dla q jest analogiczny). Istotnie z definicji liczb c, d mamy $cd = k(p-1)(q-1) + 1 = l(p-1) + 1$ dla pewnych $k, l \in \mathbb{Z}$. Z powyższego mamy więc

$$a^{cd} \equiv_p a(a^{p-1})^l.$$

Jeśli $a \perp p$ to z MTF mamy $a^{p-1} \equiv_p 1$, zatem $a^{cd} \equiv_p a \cdot 1^l \equiv_p a$, w przeciwnym wypadku mamy natomiast $p|a$, zatem $a^{cd} \equiv_p 0 \equiv_p a$, co kończy dowód.

Trudność w odszyfrowaniu wiadomości znając jedynie zaszyfrowaną wiadomość b , liczbę N i klucz publiczny c wynika z faktu, iż aby wyznaczyć klucz prywatny d musimy wyznaczyć funkcję Eulera $\phi(N)$ (aby obliczyć odwrotność liczby c modulo $\phi(N)$), której efektywne wyznaczenie wymaga faktoryzacji liczby N na czynniki pierwsze. Rozkład liczby na czynniki pierwsze jest z kolei powszechnie uznawany za problem bardzo trudny obliczeniowo (przynajmniej na klasycznym komputerze nie jest znany algorytm rozwiązujący ten problem w czasie wielomianowym względem liczby bitów faktoryzowanej liczby).

3 Informacja kwantowa

3.1 Bazy dopełniające

Def 3.1. Niech $\{\phi_i\}, \{\theta_i\}$ będą dwiema bazami ortonormalnymi N -wymiarowej przestrzeni Hilberta \mathcal{H} . Bazy te nazwiemy *dopełniającymi* iff

$$\forall i, j \in \{1, \dots, N\} : |\langle \phi_i | \theta_j \rangle|^2 = \frac{1}{N}.$$

Jedną z możliwości skonstruowania bazy dopełniającej bazy $\{\phi_i\}$ jest wykorzystanie dyskretnej transformacji Fouriera tj. wektory bazy dopełniającej są dane przez

$$|\theta_i\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^N e^{2\pi i j i / N} |\phi_j\rangle .$$

Nietrudno zauważyć, iż wówczas $|\langle \phi_m | \theta_n \rangle|^2 = 1/N$ dla dowolnych m, n oraz dodatkowo mamy

$$\begin{aligned} \langle \theta_m | \theta_n \rangle &= \frac{1}{N} \sum_{j=1}^N e^{2\pi i (m-n)j / N} \\ &= \begin{cases} 1, & \text{dla } m = n \\ N^{-1} e^{2\pi i (m-n)/N} \frac{e^{2\pi i (m-n)} - 1}{e^{2\pi i (m-n)/N} - 1} = 0, & \text{dla } m \neq n \end{cases} = \delta_{mn} , \end{aligned}$$

gdzie ostatnia równość wynika z faktu, iż $m - n \in \mathbb{Z}$, zatem $e^{2\pi i (m-n)} = \cos(2\pi(m-n)) + i \sin(2\pi(m-n)) = 1$, czyli $\{\theta_i\}$ tworzą bazę ortonormalną.

Założmy, że mamy zespół układów kwantowych przygotowanych w stanie $|\theta_k\rangle$, gdzie θ_k jest (określonym) jednym z wektorów bazowych ortonormalnej bazy $\{\theta_i\}$, ale nie wiemy o jaki stan chodzi. Jeśli dokonamy pomiaru używając bazy $\{\theta_i\}$ to w 100% przypadków otrzymamy wynik $|\theta_k\rangle$ – uzyskamy więc maksymalną „informację” o układzie. Jeśli natomiast pomiaru dokonamy w bazie dopełniającej $\{\phi_i\}$ to otrzymamy wszystkie możliwe wyniki $\{\phi_i\}$, każdy z prawdopodobieństwem $1/N$ – uzyskamy więc minimalną „informację” o układzie.