# Spis treści

# 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. $u_n \to g$ przy $n \to \infty$ iff $d(u_n, g) \to 0$ przy $n \to \infty$.

**Def 1.3.** Ciąg $(u_n)$ elementów $u_n \in V$ będziemy nazywać *ciągiem 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 *zupełną* 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 $u = \mathsf{0}$. Zauważmy tutaj, iż z pierwszego aksjomatu $\langle u|u\rangle \in \mathbb{R}$, gdyż $\langle u|u\rangle = \langle u|u\rangle^* \implies \mathrm{Im}\{\langle u|u\rangle\} = 0$.

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 $\{v_1, ..., v_n\}$ nazwiemy *ortogonalnym* iff

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

Ten sam zbiór wektorów nazwiemy *ortonormalnym* iff

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

gdzie $\delta_{ij}$ 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.** *Przestrzenią Hilberta* $\mathscr{H} = (\mathbb{V}, \langle\cdot|\cdot\rangle)$ nazwiemy zupełną przestrzeń unitarną.

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

**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 $\mathscr{H} = (\mathbb{V}, \langle\cdot|\cdot\rangle)$ 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 $\mathscr{H}_1$ i $\mathscr{H}_2$ o bazach ortonoromalnych odpowiednio $\{\phi_i^{(1)}\}$ i $\{\phi_i^{(2)}\}$ nazywamy przestrzeń Hilberta $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$ taką, że:

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

### Notacja Diraca

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

Wektory należące do $\mathscr{H}$ będziemy oznaczać jako

$$|\psi\rangle\,,\ |\phi\rangle\,,\ \ldots\,,$$

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

Funkcjonały liniowe należące do przestrzeni dualnej będziemy oznaczać jako

$$\langle\psi|\,,\ \langle\phi|\,,\ \ldots\,,$$

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

**Skończenie wymiarowa przestrzeń Hilberta nad $\mathbb{C}$**

Rozważymy teraz konstrukcję skończenie wymiarowej przestrzeni Hilberta złożonej ze skończenie wymiarowej przestrzeni wektorowej $\mathbb{V} = (\mathbb{C}^n, \mathbb{C}, +, \cdot)$, której elementy będziemy w danej bazie *ortonormalnej* $\{\phi_1, \ldots, \phi_n\}$ 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 utożsamić (poprzez iloczyn wewnętrzny) z macierzą kolumnową jego współrzędnych w danej bazie ortonormalnej. Jasne jest również czym jest funkcjonał liniowy stowarzyszony z danym wektorem

$$\langle \psi | = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}^{\dagger} = \begin{bmatrix} a_1^* & \ldots & a_n^* \end{bmatrix},$$

gdzie † oznacza *sprzężenie hermitowskie* macierzy, tj. sprzężoną macierz transponowaną. W dalszej części skupimy się głównie na skończenie 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 $\mathscr{H} = (\mathbb{V}, \langle \cdot | \cdot \rangle)$ 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 $\mathscr{H}$.

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 $\{\phi_1, \ldots, \phi_n\}$ są dane przez wartości $\mathbf{A}$ na wektorach bazowych

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

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

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

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

$$A^\dagger_{ij} = A^*_{ji} \, .$$

**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

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

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

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

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

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

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

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

**Tw 1.9.** Podstawowe własności śladu.

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

**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 samosprzężone, rzutowe i unitarne.

---

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

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

$$A_{ij} = A^*_{ji}\,.$$

W przypadku nieskończenie 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 samosprzężonymi.

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

**Tw 1.10.** Wartości własne operatora samosprzężonego są liczbami rzeczywistymi.

**Tw 1.11.** Zbiór wektorów własnych operatora samosprzężonego rozpina przestrzeń $\mathscr{H}$.

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

---

**Def 1.18.** *Operatorem rzutowym* nazywamy operator $\mathbf{P}$ taki, że $\mathbf{P} = \mathbf{P}^\dagger$ (samosprzężoność) 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 $\phi$), 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 $\alpha$, $\beta$ 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 $\mathscr{H}$, 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

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

---

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

- $\mathbf{P}(\lambda_1)\mathbf{P}(\lambda_2) = \mathbf{P}(\min(\lambda_1, \lambda_2))$
- $\forall\lambda : \lim_{\epsilon\to 0^+} \mathbf{P}(\lambda + \epsilon) = \mathbf{P}(\lambda)$
- $\lim_{\lambda\to-\infty} \mathbf{P}(\lambda) = \mathbf{0}$

- $\lim_{\lambda\to+\infty} \mathbf{P}(\lambda) = \mathbf{1}$
- $\mathbf{A} = \int\limits_{-\infty}^{+\infty} \lambda \, \mathrm{d}\mathbf{P}(\lambda)$

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

$$\int\limits_a^b f(x) \, \mathrm{d}\sigma(x) := \lim_{n\to\infty} \sum_{k=1}^{n} f(x_k) \left[\sigma(x_k) - \sigma(x_{k-1})\right] ,$$

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

$$f(\mathbf{A}) = \int\limits_{-\infty}^{+\infty} f(\lambda) \, \mathrm{d}\mathbf{P}(\lambda) .$$

W szczególnym przypadku, gdy operator samosprzężony $\mathbf{A}$ ma niezdegenerowane widmo $\{\lambda_i\}$ będące zbiorem przeliczalnym, wiemy, że zbiór unormowanych wektorów własnych $\{\phi_i\}$ jest bazą ortonormalną przestrzeni $\mathscr{H}$, czyli dla dowolnego wektora $\psi \in \mathscr{H}$ 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 $\psi$ 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 $\mathscr{H}$, przy czym utożsamiamy ze sobą wektory różniące się jedynie globalnym czynnikiem fazowym tj. $|\Psi\rangle \sim \mathrm{e}^{\mathrm{i}\alpha} |\Psi\rangle$, $\alpha \in \mathbb{R}$.

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 $\Psi$ wynosi

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

Zauważmy, że z samosprzężoności 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 samosprzężony 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 $\lambda$?

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 $\Psi$ obliczamy jako

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

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

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

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

$$\frac{\mathrm{d}\,\langle\Psi|\Psi\rangle}{\mathrm{d}t} = \left\langle\dot{\Psi}\middle|\Psi\right\rangle + \left\langle\Psi\middle|\dot{\Psi}\right\rangle = -\frac{1}{\mathrm{i}\hbar}\,\langle\mathbf{H}\Psi|\Psi\rangle + \frac{1}{\mathrm{i}\hbar}\,\langle\Psi|\mathbf{H}\Psi\rangle = 0\,,$$

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

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

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

### Zasady nieoznaczoności

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

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

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

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

Jednocześnie dla dowolnego $z = x + \mathrm{i}y \in \mathbb{C}$ mamy

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

Z powyższego mamy więc

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

skąd po prostych przekształceniach otrzymujemy

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

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

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

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

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

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

$$0 = \operatorname{Tr} \mathbf{AB} - \operatorname{Tr} \mathbf{BA} = \mathrm{i}n\hbar \neq 0 \,.$$

**Twierdzenie Ehrenfesta**

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

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

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

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

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

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

Powyższe równanie nazywamy *twierdzeniem Ehrenfesta.*

**Zasada nieoznaczoności energii–czasu**

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

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

Jednocześnie z zasady nieoznaczoności Robertsona mamy

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

Podstawiając wyrażenie na wartość oczekiwaną komutatora otrzymujemy z powyższego

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

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 $\Delta t$ o $\Delta A$ to możemy dokonać przybliżenia

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

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

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

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

### 1.4.1 Macierze Pauliego

Macierze Pauliego definiujemy jako zespolone macierze $2 \times 2$

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

Przydatne jest zdefiniowanie *wektora macierzy Pauliego* $\boldsymbol{\sigma}$

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

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

Zauważmy, że dowolny operator samosprzężony $\mathbf{A}$ w rozpatrywanej przestrzeni $\mathscr{H}$ ma postać

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

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

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

Tabela 1: Wybrane własności macierzy Pauliego

### 1.4.2 Sfera Blocha

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

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

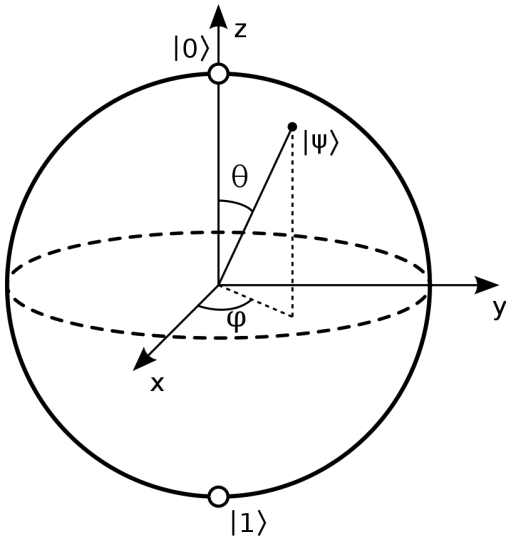
czyli 4 zmienne rzeczywiste, ale ze względu na warunek unormowania $|\alpha|^2+|\beta|^2 = 1$ mamy tylko 3 zmienne niezależne. Dodatkowo pamiętając, iż globalna faza wektora stanu nie ma znaczenia możemy wyeliminować jeszcze jedną zmienną i zapisać wektor $\Psi$ jako

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

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 $\mathsf{0}$). Zmienne $\phi$, $\theta$ 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 $|1\rangle$.

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

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




Rysunek 1: Sfera Blocha

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 $\Psi$ możemy reprezentować jako wektor $\mathbf{s}$ określający punkt na sferze jednostkowej w trójwymiarowej przestrzeni, a operator samosprzężony jako dowolny wektor $\mathbf{a}$ w tej przestrzeni. Przejście od rzeczywistego wektora $\mathbf{s}$ do abstrakcyjnego wektora stanu $|\Psi\rangle$ odbywa sie poprzez określenie współrzędnych sferycznych $(\theta, \phi)$ wektora $\mathbf{s}$ i zmapowanie ich zgodnie z przepisem

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

### 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

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

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

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

Z powyższego mamy więc dla $\boldsymbol{\rho} = \frac{1}{2}(\mathbf{1} + \mathbf{s}\cdot\boldsymbol{\sigma})$ 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 $\mathscr{H}$ reprezentowane przez samosprzężone operatory Pauliego $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$. Istotnie zgodnie z twierdzeniem Ehrenfesta

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

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

$$\begin{aligned} [\mathbf{H}, \mathbf{X}] &= -2\mathrm{i}H_y\mathbf{Z} + 2\mathrm{i}H_z\mathbf{Y} \\ [\mathbf{H}, \mathbf{Y}] &= -2\mathrm{i}H_z\mathbf{X} + 2\mathrm{i}H_x\mathbf{Z} \\ [\mathbf{H}, \mathbf{Z}] &= -2\mathrm{i}H_x\mathbf{Y} + 2\mathrm{i}H_y\mathbf{X} \end{aligned}\quad ,$$

skąd

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

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 $\Psi$ 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 $\varphi$ 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 $\mathsf{U}$, tj.

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

Warte zbadania wydaje się więc wyznaczenie operatora $\mathsf{U}$, który odpowiada obrotowi na sferze Blocha. Aby wyznaczyć jawny wzór na operator $\mathsf{U}$ rozważmy infinitezymalny obrót wektora $\mathbf{s}$ wokół osi $\hat{\mathbf{n}}$ o kąt $\epsilon$. 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 $\epsilon$. Wektor rzeczywisty $\mathbf{s}$ najłatwiej powiązać z abstrakcyjnym wektorem $|\Psi\rangle$ poprzez operator rzutowy $\boldsymbol{\rho} = |\Psi\rangle\langle\Psi|$ dla którego zachodzi

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

skąd

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

Otrzymujemy zatem równanie

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

Poszukajmy $\mathsf{U}$ spełniających to równanie postaci

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

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

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

Widzimy zatem, iż taki, a nie inny strzał na postać operatora $\mathsf{U}$ był podyktowany wyprowadzonymi wcześniej wzorami na komutatory operatora samosprzężonego z

operatorami Pauliego, które naśladują strukturę zwykłego trójwymiarowego iloczynu wektorowego. Z powyższego otrzymujemy zatem $\mathbf{a} = \frac{1}{2}\hat{\mathbf{n}}$, skąd

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

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

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

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

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

### 1.4.5 Przykład – magnetyczny rezonans jądrowy

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

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

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

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

Równania ewolucji na amplitudy prawdopodobieństwa mają więc postać

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

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

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

gdzie

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

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

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

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

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

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

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

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

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

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

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

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

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

Poprzez dostosowanie czasu $t$ przez jaki układ dwupoziomowy oddziałuje z wirowym polem możemy sterować stanem $\Psi$ 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* $\pi$, gdyż na sferze Blocha odpowiada mu obrót o $\pi$) 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

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

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, $\omega$ jest częstością laserową, a iloczyn $\mu B_{\mathrm{rf}}$ przechodzi na iloczyn elektrycznego momentu dipolowego atomu i amplitudy pola elektrycznego fali elektromagnetycznej $pE_0$.

## 1.5 Korelacje kwantowe

### 1.5.1 Stany dwuqubtiowe

Rozważmy dwa układy dwupoziomowe $A$, $B$, których modelem matematycznym są przestrzenie Hilberta $\mathscr{H}_A = \{|0_A\rangle, |1_A\rangle\}$, $\mathscr{H}_B = \{|0_B\rangle, |1_B\rangle\}$ (zauważmy, iż w przypadku przestrzeni skończenie wymiarowych 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 $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$. Ogólny stan układu złożonego ma zatem postać

$$\begin{aligned}|\Psi_{AB}\rangle &= \psi_{00}|0_A\rangle\otimes|0_B\rangle + \psi_{01}|0_A\rangle\otimes|1_B\rangle + \psi_{10}|1_A\rangle\otimes|0_B\rangle + \psi_{11}|1_A\rangle\otimes|1_B\rangle \\ &= \psi_{00}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \psi_{01}\begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \psi_{10}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} + \psi_{11}\begin{bmatrix}0\\0\\0\\1\end{bmatrix} \\ &= \psi_{00}|0_A0_B\rangle + \psi_{01}|0_A1_B\rangle + \psi_{10}|1_A0_B\rangle + \psi_{11}|1_A1_B\rangle\ .\end{aligned}$$

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

$$\begin{aligned}|\Psi_{AB}\rangle &= \begin{bmatrix}\psi_0^{(A)}\\ \psi_1^{(A)}\end{bmatrix}\otimes\begin{bmatrix}\psi_0^{(B)}\\ \psi_1^{(B)}\end{bmatrix} \\ &= \psi_0^{(A)}\psi_0^{(B)}|0_A0_B\rangle + \psi_0^{(A)}\psi_1^{(B)}|0_A1_B\rangle + \psi_1^{(A)}\psi_0^{(B)}|1_A0_B\rangle + \psi_1^{(A)}\psi_1^{(B)}|1_A1_B\rangle\ ,\end{aligned}$$

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 $\Psi_{AB}$, 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 $N$ qubtiów potrzebujemy $2^N$ współczynników $\psi_{q_1 q_2 \ldots q_N}$, gdyż możliwych konfiguracji, których amplitudy prawdopodobieństwa musimy określić jest właśnie $2^N$).

### 1.5.2 Układy złożone

Zajmiemy się teraz ogólnymi układami złożonymi postaci $\mathscr{H}_A \otimes \mathscr{H}_B$, gdzie modelami układów $A, B$ będą dowolne $n_A$– i $n_B$–wymiarowe zespolone przestrzenie Hilberta zadane przez bazy ortonormalne $\{|i_A\rangle\}$, $\{|i_B\rangle\}$. Bazą ortonormalną przestrzeni $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$ jest więc $|i_A j_B\rangle$ ze standardowo zdefiniowanym iloczynem wewnętrznym.

#### Operatory

W ogólności operatory liniowe w przestrzeni $\mathscr{H}_{AB}$ są zespolonymi macierzami $(\dim \mathscr{H}_A)^2 \times (\dim \mathscr{H}_B)^2$. Jednakże interesować nas będą głównie operatory liniowe postaci

$$\mathbf{M} = \mathbf{M}_A \otimes \mathbf{M}_B\,,$$

gdzie $\mathbf{M}_A$, $\mathbf{M}_B$ są operatorami liniowymi w przestrzeniach $\mathscr{H}_A, \mathscr{H}_B$. Nietrudno zauważyć, iż jeśli $\mathbf{M}_A$, $\mathbf{M}_B$ są samosprzężone to $\mathbf{M}_A \otimes \mathbf{M}_B$ również jest samosprzężony. 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 $\mathscr{H}$. 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 samosprzężony. 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 $\mathscr{H}_A$ przez $\mathbf{M}$. W przestrzeni $\mathscr{H}_{AB}$ 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 $\mathscr{H}_A$ pytanie o wartość wielkości $M$, to w przestrzeni $\mathscr{H}_{AB}$ (tj. jeśli $A$ jest częścią większego układu $AB$) pytanie to reprezentuje operator $\mathbf{P}_M(\lambda_1; \lambda_2) \otimes \mathbf{1}_B$.

### 1.5.3 Operator gęstości

Jak zauważyliśmy na przykładzie układów dwuqubtiowych stan układu złożonego $\Psi_{AB}$ jest w ogólności stanem splątanym, w którym amplitudy prawdopodobieństw przy wektorach bazowych $|i_A j_B\rangle$ są dowolnymi liczbami zespolonymi $\psi_{ij}$ spełniającymi warunek unormowania. 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

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

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

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

gdzie $\boldsymbol{\rho}$ nazywamy *operatorem gęstości*. Zauważmy, iż możemy zapisać $\boldsymbol{\rho}$ również jako

$$\boldsymbol{\rho} = \mathrm{Tr}_B(|\Psi_{AB}\rangle\langle\Psi_{AB}|)\,,$$

gdzie $\mathrm{Tr}_B$ oznacza tzw. *ślad częściowy* względem układu $B$, taki że element $ij$ macierzy gęstości jest dany przez

$$\rho_{ij} = \langle i_A|\boldsymbol{\rho}|j_A\rangle = \sum_k \langle i_A k_B|\Psi_{AB}\rangle\,\langle\Psi_{AB}|j_A k_B\rangle \ .$$

Zauważmy, że operator gęstości jest operatorem samosprzężonym $\boldsymbol{\rho}^\dagger = \boldsymbol{\rho}$, nieujemnie określonym[1], o śladzie równym jedności $\mathrm{Tr}\,\boldsymbol{\rho} = 1$. Z powyższych własności

[1]Istotnie wystarczy zauważyć, że dla dowolnego $\Phi$ mamy

$$\langle\Phi|\boldsymbol{\rho}|\Phi\rangle = \sum_{i,j}\phi_i^*\phi_j\sum_k\psi_{ik}\psi_{jk}^* = \sum_k\sum_{i,j}(\phi_i^*\psi_{ik})(\phi_j\psi_{jk}^*) = \sum_k\left|\sum_i\phi_i^*\psi_{ik}\right|^2 \geq 0\,.$$

wynika, iż istnieje baza ortonormalna $\{|\nu\rangle\}$, w której macierz gęstości jest diagonalna, a elementy na przekątnej są nieujemnymi liczbami[2] sumującymi się do 1, czyli możemy zapisać

$$\boldsymbol{\rho} = \sum_{\nu} p_\nu \, |\nu\rangle\langle\nu| \, , \quad \sum_{\nu} p_\nu = 1 \, , \quad \forall \nu : p_\nu \geq 0 \, .$$

Widzimy zatem, iż $\boldsymbol{\rho}$ nie ma w ogólności postaci $|\Psi_A\rangle\langle\Psi_A|$, przy czym warunkiem wystarczającym aby tak było jest $\boldsymbol{\rho}^2 = \boldsymbol{\rho}$ (czyli aby macierz gęstości była idempotentna), co wynika wprost z powyższej postaci[3]. W ogólności więc jeśli $A$ jest podukładem układu złożonego $AB$ w stanie splątanym to informacja o nim (w sensie prawdopodobieństw wyników pomiarów wielkości fizycznych) nie jest opisywana przez wektor stanu tylko przez macierz gęstości

$$\boldsymbol{\rho} = \mathrm{Tr}_B(|\Psi_{AB}\rangle\langle\Psi_{AB}|) \, ,$$

a prawdopodobieństwa i wartości oczekiwane są dane przez ślady

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

Mówimy wtedy, iż układ $A$ jest w *stanie mieszanym*. Jeżeli z kolei układ można opisać poprzez wektor stanu (tj. macierz gęstości ma postać $|\Psi_A\rangle\langle\Psi_A|$) to mówimy, iż jest on w *stanie czystym*. Zauważmy, czym fundamentalnie różni się stan mieszany powyższej postaci od stanu czystego $|\Psi_A\rangle = \sum_\nu \sqrt{p_\nu}\,|\nu\rangle$. W przypadku stanu czystego prawdopodobieństwo odpowiedzi na $\mathbf{P}$ zawiera człony interferencyjne

$$p = \sum_{\nu,\mu} \sqrt{p_\mu p_\nu}\,\langle\mu|\mathbf{P}|\nu\rangle = \sum_{\nu} p_\nu \,\langle\nu|\mathbf{P}|\nu\rangle + \sum_{\mu\neq\nu} \sqrt{p_\mu p_\nu}\,\langle\mu|\mathbf{P}|\nu\rangle \, ,$$

natomiast w przypadku stanu mieszanego mamy

$$p = \mathrm{Tr}(\mathbf{P}\boldsymbol{\rho}) = \sum_{\nu} p_\nu \,\langle\nu|\mathbf{P}|\nu\rangle \, ,$$

czyli tak naprawdę klasyczny wzór na prawdopodobieństwo całkowite. Stan mieszany opisuje więc efektywnie niekoherentną mieszaninę stanów $|\nu\rangle$, w których każdy przygotowano z prawdopodobieństwem $p_\nu$.

---

[2]Istotnie ponieważ $\boldsymbol{\rho}$ jest nieujemnie określona, więc w szczególności dla $\Phi$ będącego wektorem własnym macierzy $\boldsymbol{\rho}$ z wartością własną $\lambda$ mamy $0 \leq \langle\Phi|\boldsymbol{\rho}|\Phi\rangle = \lambda\,\langle\Phi|\Phi\rangle$, skąd $\lambda \geq 0$.

[3]Istotnie jeśli $\boldsymbol{\rho}^2 = \boldsymbol{\rho}$ to dla wszystkich $\nu$ $p_\nu^2 = p_\nu$, co oznacza $p_\nu \in \{0,1\}$ ale z warunku unormowania wynika, iż dokładnie wszystkie poza jednym $p_\nu$ są zerowe, a jeden równy 1 i odzyskujemy postać $\boldsymbol{\rho} = |\Psi_A\rangle\langle\Psi_A|$.

**Ewolucja operatora gęstości**

Równanie ewolucji operatora gęstości (tzw. *równanie von Neumanna*) można wyprowadzić rozważając równanie ewolucji prawdopodobieństw. Istotnie zakładając, iż hamiltonian układu złożonego ma postać $\mathbf{H} \otimes \mathbf{1}_B$ mamy

$$\begin{aligned}\frac{\mathrm{d}p}{\mathrm{d}t} &= \left\langle \dot{\Psi}_{AB} \middle| \mathbf{P} \otimes \mathbf{1}_B \middle| \Psi_{AB} \right\rangle + \left\langle \Psi_{AB} \middle| \mathbf{P} \otimes \mathbf{1}_A \middle| \dot{\Psi}_{AB} \right\rangle \\ &= \frac{1}{\mathrm{i}\hbar} \langle \Psi_{AB} | [\mathbf{P}, \mathbf{H}] \otimes \mathbf{1}_B | \Psi_{AB} \rangle = \mathrm{Tr}\left( \frac{1}{\mathrm{i}\hbar} [\mathbf{P}, \mathbf{H}] \boldsymbol{\rho} \right) = \mathrm{Tr}\left( \frac{1}{\mathrm{i}\hbar} \mathbf{P} [\mathbf{H}, \boldsymbol{\rho}] \right) ,\end{aligned}$$

gdzie skorzystaliśmy z liniowości i niezmienniczości śladu względem cyklicznych przestawień. Jednocześnie z drugiej strony $\dot{p} = \mathrm{Tr}(\mathbf{P}\dot{\boldsymbol{\rho}})$, zatem

$$\mathrm{i}\hbar \frac{\partial \boldsymbol{\rho}}{\partial t} = [\mathbf{H}, \boldsymbol{\rho}] .$$

Równoważnie jeśli $|\Psi_{AB}(t)\rangle = \mathbf{U} \otimes \mathbf{1}_B \, |\Psi_{AB}(t_0)\rangle$ to

$$\begin{aligned}p(t) = \mathrm{Tr}(\mathbf{P}\boldsymbol{\rho}(t)) &= \langle \Psi_{AB} | (\mathbf{U}^\dagger \otimes \mathbf{1}_B)(\mathbf{P} \otimes \mathbf{1}_B)(\mathbf{U} \otimes \mathbf{1}_B) | \Psi_{AB} \rangle \\ &= \langle \Psi_{AB} | \mathbf{U}^\dagger \mathbf{P} \mathbf{U} \otimes \mathbf{1}_B | \Psi_{AB} \rangle = \mathrm{Tr}(\mathbf{U}^\dagger \mathbf{P} \mathbf{U} \boldsymbol{\rho}) = \mathrm{Tr}(\mathbf{P}\mathbf{U}\boldsymbol{\rho}\mathbf{U}^\dagger) ,\end{aligned}$$

skąd

$$\boldsymbol{\rho}(t) = \mathbf{U}\boldsymbol{\rho}(t_0)\mathbf{U}^\dagger .$$

### 1.5.4 Kula Blocha

Jak każdy operator samosprzężony w przestrzeni qubtiów również operator gęstości można rozłożyć na macierze Pauliego

$$\boldsymbol{\rho} = s_0 \mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma} = \begin{bmatrix} s_0 + s_z & s_x - \mathrm{i}s_y \\ s_x + \mathrm{i}s_y & s_0 - s_z \end{bmatrix} .$$

Ponieważ macierz gęstości ma ślad jednostkowy, więc $s_0 = 1/2$. Dodatkowo ponieważ jest nieujemnie określona, więc wartości własne muszą być nieujemne. Jednocześnie wartości te wyznaczone są jako pierwiastki wielomianu

$$\det(\boldsymbol{\rho} - \lambda \mathbf{1}) = \lambda^2 - \lambda + \frac{1}{4} - |\mathbf{s}|^2 .$$

Aby wielomian $Ax^2+Bx+C$ miał oba pierwiastki nieujemne musimy mieć $-B/A \geq 0$ i $C/A \geq 0$, skąd $|\mathbf{s}|^2 \leq \frac{1}{4}$. Operator gęstości możemy zatem zapisać jako

$$\boldsymbol{\rho} = \frac{1}{2}(\mathbf{1} + \mathbf{s} \cdot \boldsymbol{\sigma}) ,$$

gdzie $|\mathbf{s}|^2 \leq 1$. Możemy go zatem reprezentować geometrycznie jako punkt wewnątrz kuli jednostkowej w kartezjańskim układzie współrzędnych, którą nazywamy *kulą Blocha*. Zauważmy, iż jeśli $\boldsymbol{\rho}$ przedstawia stan czysty to zachodzi $s_x^2 + s_y^2 = 1 - s_z^2$, czyli stany czyste są reprezentowane przez punkty na sferze Blocha, a stany mieszane jako punkty wewnątrz kuli Blocha.

Stan mieszany, dla którego $\mathbf{s} = \mathbf{0}$ tj. $\boldsymbol{\rho} = \frac{1}{2}\mathbf{1}$ nazywamy *stanem maksymalnie splątanym* lub *stanem Bella*. Nietrudno zauważyć, iż wszystkie stany Bella mają postać

$$\frac{1}{\sqrt{2}}\left(|i_A j_B\rangle + \mathrm{e}^{\mathrm{i}\alpha}\,|(1-i)_A(1-j)_B\rangle\right) .$$

Zauważmy, iż jeśli układ złożony ewoluuje zgodnie z przekształceniem unitarnym będącym iloczynem tensorowym $\mathbf{U} \otimes \mathbf{1}_B$ to $\boldsymbol{\rho}(t) = \mathbf{U}\boldsymbol{\rho}(t_0)\mathbf{U}^\dagger$ i w przestrzeni $\mathbf{s}$ tej ewolucji odpowiada obrót dany wzorami wyprowadzonymi dla sfery Blocha (w szczególności więc długość wektora $\mathbf{s}$ nie zmienia się, choć niekoniecznie wynosi 1).

### 1.5.5 Fizyczna realizacja stanu splątanego

Rozpocznijmy od prostej obserwacji, iż jeśli początkowo układ złożony $AB$ nie jest w stanie splątanym tj. $|\Psi_{AB}(t_0)\rangle = |\Psi_A(t_0)\rangle \otimes |\Psi_B(t_0)\rangle$ i ewolucja unitarna układu złożonego ma postać iloczynu tensorowego $\mathbf{U}_A \otimes \mathbf{U}_B$ to

$$|\Psi_{AB}(t)\rangle = \mathbf{U}_A\,|\Psi_A(t_0)\rangle \otimes \mathbf{U}_B\,|\Psi_B(t_0)\rangle = |\Psi_A(t)\rangle \otimes |\Psi_B(t)\rangle ,$$

więc układ pozostaje niesplątany. W celu utworzenia stanu splątanego z początkowego stanu niesplątanego hamiltonian układu złożonego musi zawierać człony opisujące oddziaływanie między podukładami $A$ i $B$. Jako przykład rozpatrzymy magnetyczne oddziaływanie dwóch spinów 1/2 opisane hamiltonianem

$$\mathbf{H}_{AB} = \frac{\hbar\omega}{2}\boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B = \frac{\hbar\omega}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} .$$

Wartości własne $\mathbf{H}_{AB}$ wynoszą $\hbar\omega/2$ i $-3\hbar\omega/2$, a odpowiadające im wektory własne

$$a\,|00\rangle + b\,|01\rangle + b\,|10\rangle + c\,|11\rangle \ , \quad d\,|01\rangle - d\,|10\rangle$$

dla $a, b, c, d \in \mathbb{C}$. Rozwiązanie ma zatem postać

$$|\Psi_{AB}(t)\rangle = \mathrm{e}^{-\mathrm{i}\omega t/2}\left(a\,|00\rangle + b\,|01\rangle + b\,|10\rangle + c\,|11\rangle\right) + \mathrm{e}^{3\mathrm{i}\omega t/2} d\left(|01\rangle - |10\rangle\right) .$$

Dla $t = 0$ mamy

$$|\Psi_{AB}(0)\rangle = a\,|00\rangle + (b+d)\,|01\rangle + (b-d)\,|10\rangle + c\,|11\rangle\ .$$

Załóżmy, iż początkowo stan jest niesplątany i $|\Psi_{AB}(0)\rangle = |10\rangle$ tj. $a = c = 0$ i $b = -d = 1/2$, wówczas

$$\begin{aligned}|\Psi_{AB}(t)\rangle &= \frac{1}{2}\mathrm{e}^{-\mathrm{i}\omega t/2}\left(\mathrm{e}^{-\mathrm{i}\omega t}(|01\rangle + |10\rangle) - \mathrm{e}^{\mathrm{i}\omega t}(|01\rangle - |10\rangle)\right)\\ &= \mathrm{e}^{\mathrm{i}\omega t/2}\left[\cos(\omega t)\,|10\rangle - \mathrm{i}\sin(\omega t)\,|01\rangle\right]\ .\end{aligned}$$

Po czasie $t = \pi/4\omega$ otrzymujemy więc stan maksymalnie splątany

$$\frac{1}{\sqrt{2}}\left(|10\rangle - \mathrm{i}\,|01\rangle\right)\ .$$

Trudności przy fizycznej implementacji powyższego schematu wynikają z faktu, iż opisane oddziaływanie jest najczęściej oddziaływaniem wewnętrznym układu, dla którego nie możemy kontrolować czasu oddziaływania $t$ jak w przypadku MRJ.

### Operator SWAP

Zauważmy, iż dla operatora $\boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B$ zachodzi

$$\boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B\left[(\alpha+\beta)\,|01\rangle + (\alpha-\beta)\,|10\rangle\right] = (\alpha - 3\beta)\,|01\rangle + (\alpha+3\beta)\,|10\rangle\ ,$$

skąd w szczególności dla $\alpha = \beta = 1$

$$2\boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B\,|01\rangle = -2\,|01\rangle + 4\,|10\rangle$$

a dla $\alpha = -\beta = 1$

$$2\boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B\,|10\rangle = 4\,|01\rangle - 2\,|10\rangle\ .$$

Z powyższego możemy zdefiniować tzw. operator SWAP postaci

$$\mathbf{U}_{\mathrm{SWAP}} = \frac{1}{2}\left(\mathbf{1} + \boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B\right) = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

dla którego $\mathbf{U}_{\mathrm{SWAP}}\,|i_A j_B\rangle = |j_A i_B\rangle$. Operator ten permutuje qubtiy $A$ i $B$. Nietrudno dodatkowo zauważyć, iż $\mathbf{U}_{\mathrm{SWAP}}$ jest operatorem samosprzężonym i unitarnym.

### 1.5.6 No-cloning theorem

Uniwersalnym procesem klonującym stan kwantowy $|\chi\rangle \in \mathscr{H}$ na stan $|\Phi\rangle \in \mathscr{H}$ nazwiemy proces, dla którego istnieje operator unitarny $\mathbf{U}$ działający w przestrzeni $\mathscr{H} \otimes \mathscr{H}$ taki, że

$$\mathbf{U}(|\chi\rangle \otimes |\Phi\rangle) = |\chi\rangle \otimes |\chi\rangle$$

dla dowolnego stanu $|\chi\rangle$. Udowodnimy, iż taki proces nie istnieje. Istotnie załóżmy nie wprost, iż taki proces istnieje. Wówczas dla dowolnych wektorów $|\chi_1\rangle, |\chi_2\rangle$ mamy

$$\mathbf{U}(|\chi_1\rangle \otimes |\Phi\rangle) = |\chi_1\rangle \otimes |\chi_1\rangle \ , \quad \mathbf{U}(|\chi_2\rangle \otimes |\Phi\rangle) = |\chi_2\rangle \otimes |\chi_2\rangle \ ,$$

ale zauważmy, że

$$\langle\chi_1|\chi_2\rangle^2 = \langle\chi_1\chi_1|\chi_2\chi_2\rangle = \langle\chi_1\Phi|\mathbf{U}^\dagger\mathbf{U}|\chi_2\Phi\rangle = \langle\chi_1\Phi|\chi_2\Phi\rangle = \langle\chi_1|\chi_2\rangle \ ,$$

skąd $\langle\chi_1|\chi_2\rangle$ jest równy 0 lub 1, czyli $\chi_1, \chi_2$ nie mogą być dowolne, a zatem otrzymaliśmy sprzeczność.

### 1.5.7 Dekoherencja

Dekoherencją nazywamy zjawisko polegające na nieodwracalnej utracie zależności fazowych przez układ kwantowy na skutek oddziaływania z otoczeniem. Innymi słowy jest to proces, podczas którego tłumione są człony pozadiagonalne macierzy gęstości podukładu, co skutkuje odzyskaniem klasycznych wzorów na dodawanie prawdopodobieństw.

Rozważymy prosty model sprzężenia układu z otoczeniem, w którym występuje zjawisko dekoherencji. W modelu tym mamy układ dwupoziomowy $A$ (qubit) i foton $F$, który jest na nim rozpraszany. Zakładamy, iż rozproszony foton może być modelowany układem trójpoziomowym $\{|0\rangle, |1\rangle, |2\rangle\}$, a oddziaływanie między układami jest opisane operatorem unitarnym[4]

$$\mathbf{U}\,|00\rangle = \sqrt{1-p}\,|00\rangle + \sqrt{p}\,|01\rangle \ , \quad \mathbf{U}\,|10\rangle = \sqrt{1-p}\,|10\rangle + \sqrt{p}\,|12\rangle \ ,$$

[4]Jest tutaj jedna subtelna kwestia; zauważmy, iż działanie operatora $\mathbf{U}$ zdefiniowaliśmy jedynie na podprzestrzeni rozpiętej przez $\{|00\rangle, |10\rangle\}$, a nie na całej przestrzeni $\mathscr{H}_{AF}$. Skąd możemy mieć pewność, iż istnieje odwzorowanie unitarne działające na całej przestrzeni takie, że jego działanie na podprzestrzeni jest takie jak zdefiniowane? Zauważmy najpierw, iż zdefiniowany $\mathbf{U}$ jest izometrią w podprzestrzeni tj. dla dowolnych wektorów $\Psi, \Phi$ należących do niej zachodzi $\langle\mathbf{U}\Psi|\mathbf{U}\Phi\rangle = \langle\Psi|\Phi\rangle$ ($\mathbf{U}$ nie jest unitarny w tej podprzestrzeni, zauważmy bowiem iż jest reprezentowany przez macierz prostokątną $4 \times 2$). Można jednak pokazać, iż dowolna izometria w podprzestrzeni $\mathscr{V} \subset \mathscr{H}$ $\mathbf{V} : \mathscr{V} \mapsto \mathscr{H}$ posiada unitarne rozszerzenie $\mathbf{U} : \mathscr{H} \mapsto \mathscr{H}$ tj. istnieje operator unitarny $\mathbf{U}$ zdefiniowany na całej przestrzeni $\mathscr{H}$ taki, że $\forall\Phi \in \mathscr{V} : \mathbf{U}\Phi = \mathbf{V}\Phi$.
Istotnie niech $\{|v\rangle\} \cup \{|u\rangle\}$ będzie bazą ortonormalną $\mathscr{H}$, gdzie $\{|v\rangle\}$ jest bazą ortonormalną podprzestrzeni $\mathscr{V}$ i zakładamy $\dim\mathscr{V}, \dim\mathscr{H} < \infty$. Ponieważ $\mathbf{V}$ jest izometrią, więc obrazem bazy ortonormalnej podprzestrzeni $\mathscr{V}$ będzie pewien zbiór ortonormalny $\{|v'\rangle\}$ o liczności $\dim\mathscr{V} < \infty$.

gdzie zakładamy, iż amplitudy prawdopodobieństwa rozproszenia fotonu są niezależne od stanu układu $A$, ale końcowy stan fotonu zależy od stanu qubitu. Możemy sobie wyobrazić, iż qubitem jest kwantowe lusterko, które może być pod kątem $+\pi/4$ lub $-\pi/4$ w stosunku do toru fotonu, który może nie trafić w lusterko (tj. pozostać w stanie podstawowym $|0\rangle$), odbić się w górę ($|1\rangle$) lub w dół ($|2\rangle$), przy czym amplituda prawdopodobieństwa trafienia lub nie w lusterko jest niezależna od jego ustawienia. Załóżmy, iż początkowo qubit jest w stanie czystym

$$|\Psi_{AF}\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle\ .$$

Początkowo macierz gęstości układu $A$ ma zatem postać

$$\boldsymbol{\rho} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} = \begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix}.$$

Po rozproszeniu fotonu natomiast stan układu złożonego ewoluuje do

$$\mathbf{U}\,|\Psi_{AF}\rangle = \alpha\sqrt{1-p}\,|00\rangle + \alpha\sqrt{p}\,|01\rangle + \beta\sqrt{1-p}\,|10\rangle + \beta\sqrt{p}\,|12\rangle\ ,$$

skąd macierz gęstości ma postać

$$\boldsymbol{\rho}' = \begin{bmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{bmatrix}.$$

Jeśli $p = 1 - \epsilon$ to macierz jest prawie diagonalna. Zauważmy jednak, iż w tym modelu dekoherencja jest jedynie pozorna gdyż stan pełnego układu $AF$ jest oczywiście stanem czystym i jeśli tylko potrafimy mierzyć wielkości związane z rozproszonym fotonem to mamy pełną informację o układzie. W realistycznym przypadku otoczenie ma tak wiele stopni swobody, iż jest nie możliwe abyśmy mieli nad nimi pełną kontrolę i efektywnie wielkości związane z otoczeniem są nieobserwowalne. Możemy ulepszyć nasz model jeśli założymy, iż nasz qubit rozprasza nie pojedynczy foton a wiele ($N$) fotonów jeden po drugim. W stanie początkowym wszystkie fotony są w stanie podstawowym tj.

$$|\Psi_{AE}\rangle = (\alpha\,|0_A\rangle + \beta\,|1_A\rangle) \otimes |\underbrace{0\ldots0}_{N}\rangle\ .$$

---

Zbiór ten możemy rozszerzyć do bazy przestrzeni $\mathscr{H}$ dodając do niego pewne wektory $|u'\rangle$. Jeśli teraz zdefiniujemy odwzorowanie $\mathbf{U} : \mathscr{H} \mapsto \mathscr{H}$ jako $\mathbf{U}\,|v\rangle = \mathbf{V}\,|v\rangle = |v'\rangle\,, \mathbf{U}\,|u\rangle = |u'\rangle$ to skonstruowaliśmy izometrię w przestrzeni $\mathscr{H}$, ale każda izometria reprezentowana przez macierz kwadratową jest unitarna (gdyż jeśli dla macierzy kwadratowej $\mathbf{A}$ istnieje macierz $\mathbf{B}$ taka, że $\mathbf{BA} = \mathbf{1}$ to $\mathbf{A}$ jest odwracalna). W przykładzie nie interesują nas wartości tego odwzorowania dla pozostałych wektorów bazowych (poza wektorami bazowymi podprzestrzeni) gdyż stany te w tym modelu są nierealizowalne fizycznie.

Aby odtworzyć ewolucję dla przypadku pojedynczego fotonu zdefiniujmy ciąg operatorów unitarnych $\mathbf{U}_n = \mathbf{V}_n \otimes \mathbf{1}_{N-n}$, gdzie

$$\mathbf{V}_n \left|0_A i_1 \dots i_{n-1} 0\right\rangle = \sqrt{1-p}\left|0_A i_1 \dots i_{n-1} 0\right\rangle + \sqrt{p}\left|0_A i_1 \dots i_{n-1} 1\right\rangle$$
$$\mathbf{V}_n \left|1_A j_1 \dots j_{n-1} 0\right\rangle = \sqrt{1-p}\left|1_A j_1 \dots j_{n-1} 0\right\rangle + \sqrt{p}\left|1_A j_1 \dots j_{n-1} 2\right\rangle$$

dla $n \geq 1$ i dowolnych $i_1, \dots, i_{n-1} \in \{0,1\}$, $j_1, \dots, j_{n-1} \in \{0,2\}$. Ponownie operator izometryczny $\mathbf{V}_n$ zdefiniowaliśmy jedynie na $2^n$–wymiarowej podprzestrzeni ale posiada on unitarne rozszerzenie do przestrzeni $2 \cdot 3^n$–wymiarowej. Operator $\mathbf{V}_n$ jest operatorem opisującym rozproszenie $n$–tego w kolejności fotonu na qubicie. Niech

$$\left|\Psi_n\right\rangle = \mathbf{U}_n \dots \mathbf{U}_1 \left|\Psi_{AE}\right\rangle \ .$$

Niech $\{0,1\}^n, \{0,2\}^n$ oznaczają zbiory wszystkich słów binarnych długości $n$ nad alfabetem odpowiednio $\{0,1\}$ oraz $\{0,2\}$. Dla słowa $\mathfrak{a} \in \{0,1\}^n$ ($\mathfrak{b} \in \{0,2\}^n$) przez $\kappa(\mathfrak{a})$ oznaczmy liczbę niezerowych miejsc w tym słowie. Wówczas

$$\left|\Psi_n\right\rangle = \Bigg[\alpha \sum_{\mathfrak{a}\in\{0,1\}^n} \left(\sqrt{1-p}\right)^{n-\kappa(\mathfrak{a})} \left(\sqrt{p}\right)^{\kappa(\mathfrak{a})} \left|0_A \mathfrak{a}\right\rangle$$
$$+ \beta \sum_{\mathfrak{b}\in\{0,2\}^n} \left(\sqrt{1-p}\right)^{n-\kappa(\mathfrak{b})} \left(\sqrt{p}\right)^{\kappa(\mathfrak{b})} \left|1_A \mathfrak{b}\right\rangle \Bigg] \otimes \left|\underbrace{0 \dots 0}_{N-n}\right\rangle \ .$$

Istotnie dowodząc indukcyjnie; dla $n = 1$ mamy

$$\left|\Psi_1\right\rangle = \left[\alpha\sqrt{1-p}\left|0_A 0\right\rangle + \alpha\sqrt{p}\left|0_A 1\right\rangle + \beta\sqrt{1-p}\left|1_A 0\right\rangle + \beta\sqrt{p}\left|1_A 2\right\rangle\right] \otimes \left|\underbrace{0 \dots 0}_{N-1}\right\rangle$$

co jest oczywiście równe $\mathbf{U}_1 \left|\Psi_{AE}\right\rangle$, następnie zakładając, że wzór jest słuszny dla $\left|\Psi_n\right\rangle$ mamy

$$\left|\Psi_{n+1}\right\rangle = \mathbf{U}_{n+1}\left|\Psi_n\right\rangle = \Bigg[\alpha \sum_{\mathfrak{a}\in\{0,1\}^n} \left(\sqrt{1-p}\right)^{n-\kappa(\mathfrak{a})} \left(\sqrt{p}\right)^{\kappa(\mathfrak{a})} \mathbf{U}_{n+1} \left|0_A \mathfrak{a} 0\right\rangle$$
$$+ \beta \sum_{\mathfrak{b}\in\{0,2\}^n} \left(\sqrt{1-p}\right)^{n-\kappa(\mathfrak{b})} \left(\sqrt{p}\right)^{\kappa(\mathfrak{b})} \mathbf{U}_{n+1} \left|1_A \mathfrak{b} 0\right\rangle \Bigg] \otimes \left|\underbrace{0 \dots 0}_{N-(n+1)}\right\rangle \ ,$$

skąd współczynnik przy $\alpha$ ma postać (dla uproszczenia zapisu oznaczymy $r = \sqrt{1-p}, s = \sqrt{p}$)

$$\sum_{\mathfrak{a}\in\{0,1\}^n} r^{n+1-\kappa(\mathfrak{a})} s^{\kappa(\mathfrak{a})} \left|0_A \mathfrak{a} 0\right\rangle + \sum_{\mathfrak{a}\in\{0,1\}^n} r^{n-\kappa(\mathfrak{a})} s^{\kappa(\mathfrak{a})+1} \left|0_A \mathfrak{a} 1\right\rangle \ ,$$

a przy $\beta$

$$\sum_{\mathfrak{b}\in\{0,2\}^n} r^{n+1-\kappa(\mathfrak{b})}s^{\kappa(\mathfrak{b})}\,|1_A\mathfrak{b}0\rangle + \sum_{\mathfrak{b}\in\{0,2\}^n} r^{n-\kappa(\mathfrak{b})}s^{\kappa(\mathfrak{b})+1}\,|1_A\mathfrak{b}2\rangle\ .$$

Zauważmy jednak, iż $\kappa(\mathfrak{a}) = \kappa(\mathfrak{a}0) = \kappa(\mathfrak{a}1) - 1$, zatem możemy zapisać

$$\begin{aligned}
&\sum_{\mathfrak{a}\in\{0,1\}^n} r^{n+1-\kappa(\mathfrak{a})}s^{\kappa(\mathfrak{a})}\,|0_A\mathfrak{a}0\rangle + \sum_{\mathfrak{a}\in\{0,1\}^n} r^{n-\kappa(\mathfrak{a})}s^{\kappa(\mathfrak{a})+1}\,|0_A\mathfrak{a}1\rangle\\
&= \sum_{\mathfrak{a}0\in\{0,1\}^{n+1}} r^{n+1-\kappa(\mathfrak{a}0)}s^{\kappa(\mathfrak{a}0)}\,|0_A\mathfrak{a}0\rangle + \sum_{\mathfrak{a}1\in\{0,1\}^{n+1}} r^{n+1-\kappa(\mathfrak{a}1)}s^{\kappa(\mathfrak{a}1)}\,|0_A\mathfrak{a}1\rangle\\
&= \sum_{\mathfrak{a}\in\{0,1\}^{n+1}} r^{n+1-\kappa(\mathfrak{a})}s^{\kappa(\mathfrak{a})}\,|0_A\mathfrak{a}\rangle
\end{aligned}$$

i analogicznie dla współczynnika przy $\beta$, zatem

$$\begin{aligned}
|\Psi_{n+1}\rangle = \Bigg[&\alpha \sum_{\mathfrak{a}\in\{0,1\}^{n+1}} \left(\sqrt{1-p}\right)^{n+1-\kappa(\mathfrak{a})} (\sqrt{p})^{\kappa(\mathfrak{a})}\,|0_A\mathfrak{a}\rangle\\
&+ \beta \sum_{\mathfrak{b}\in\{0,2\}^{n+1}} \left(\sqrt{1-p}\right)^{n+1-\kappa(\mathfrak{b})} (\sqrt{p})^{\kappa(\mathfrak{b})}\,|1_A\mathfrak{b}\rangle\Bigg] \otimes |\underbrace{0\ldots0}_{N-(n+1)}\rangle\ ,
\end{aligned}$$

więc z zasady indukcji matematycznej zaproponowany wzór jest poprawny dla dowolnych $n \geq 1$. Możemy więc nareszcie obliczyć macierz gęstości układu $A$ po rozproszeniu $N$ fotonów. Mamy

$$\begin{aligned}
\rho'_{00} &= \sum_{\mathfrak{c}\in\{0,1,2\}^N} |\,\langle 0_A\mathfrak{c}|\Psi_N\rangle\,|^2 = |\alpha|^2 \sum_{\mathfrak{a}\in\{0,1\}^N} (1-p)^{N-\kappa(\mathfrak{a})}p^{\kappa(\mathfrak{a})}\\
&= |\alpha|^2 \sum_{k=0}^{N} \binom{N}{k}(1-p)^{N-k}p^k = |\alpha|^2(1-p+p)^N = |\alpha|^2 = \rho_{00}
\end{aligned}$$

analogicznie $\rho'_{11} = \rho_{11}$, natomiast dla elementów pozadiagonalnych mamy

$$\begin{aligned}
\rho'_{01} = \rho'^{*}_{10} &= \sum_{\mathfrak{c}\in\{0,1,2\}^N} \langle 0_A\mathfrak{c}|\Psi_N\rangle\,\langle\Psi_N|1_A\mathfrak{c}\rangle\\
&= \langle 0_A\underbrace{0\ldots0}_{N}|\Psi_N\rangle\ \langle\Psi_N|1_A\underbrace{0\ldots0}_{N}\rangle = \alpha\beta^*(1-p)^N = \rho_{01}(1-p)^N\,,
\end{aligned}$$

czyli

$$\boldsymbol{\rho}' = \begin{bmatrix} \rho_{00} & \rho_{01}(1-p)^N \\ \rho_{10}(1-p)^N & \rho_{11} \end{bmatrix}.$$

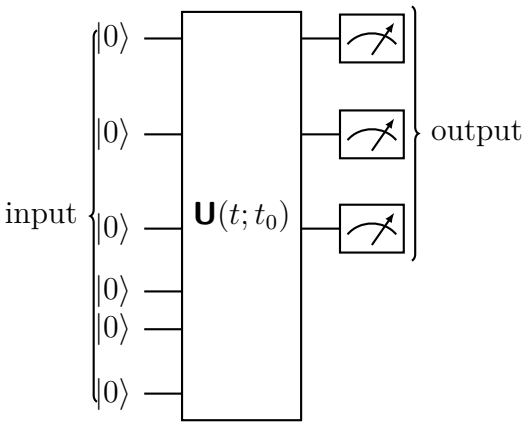
Widzimy zatem, iż nawet jeśli $p$ nie jest bliskie 1 to dla bardzo dużej liczby $N$, na przykład rzędu $10^{23}$, elementy pozadiagonalne się praktycznie zerują i nie mamy jak odzyskać tej informacji, gdyż jest rozłożona na $\sim 10^{23}$ stopni swobody. Zakładając, że liczba rozproszonych fotonów na jednostkę czasu wynosi $\Gamma$ możemy oszacować czas dekoherencji tj. czas po którym $(1-p)^{\Gamma t} \leq \epsilon$

$$\tau = \frac{1}{\Gamma} \frac{\log \epsilon}{\log(1-p)} \sim \frac{1}{\Gamma}.$$

# 2 Obliczenia kwantowe

Niech $\mathscr{H} = \{|0\rangle, |1\rangle\}$ będzie przestrzenią Hilberta opisującą pojedynczy qubit. Podstawowym obiektem zainteresowania w kontekście obliczeń kwantowych jest przestrzeń Hilberta $\mathscr{H}^{\otimes n} = \underbrace{\mathscr{H} \otimes \ldots \otimes \mathscr{H}}_{n}$, której baza ortonormalna ma postać $\{|\mathfrak{a}\rangle \mid \mathfrak{a} \in \{0,1\}^n\}$. Oczywiście każde słowo binarne długości $n$ możemy utożsamić z liczbą naturalną z przedziału $k \in \{0, 1, \ldots, 2^n - 1\}$, więc bazę ortonormalną przestrzeni $\mathscr{H}^{\otimes n}$ będziemy zapisywać również jako $\{|k\rangle \mid k \in \{0, 1, \ldots, 2^n - 1\}\}$. Bazę tą nazywamy *bazą obliczeniową*.

Na Rysunku 2 przedstawiono ogólny schemat obliczeń kwantowych. Najpierw w chwili $t_0$ inicjalizujemy $n$ qubitów (np. poprzez pomiar powodujący kolaps), następnie qubity ewoluują zgodnie z pewnym odwzorowaniem unitarnym $\mathbf{U}(t; t_0)$, a następnie aby odczytać wynik dokonujemy pomiaru na (pod)układzie qubitów. Zauważmy, iż ponieważ wymagamy aby ewolucja była unitarna, więc obliczenia kwantowe są z konieczności obliczeniami odwracalnymi tj. z uzyskanego wyniku (stanu końcowego $|\Psi(t)\rangle$) możemy odtworzyć dane (stan początkowy $|\Psi(t_0)\rangle$) poprzez zastosowanie operatora unitarnego $\mathbf{U}^{-1}$.




Rysunek 2: Ogólny schemat obliczeń kwantowych

Odwracalność obliczeń kwantowych jest zasadniczo różna od klasycznych obwodów logicznych, które w ogólności nie są odwracalne. Wiemy chociażby, iż bramki NAND wystarczą do konstrukcji dowolnych obwodów logicznych tj. funkcji $f : \{0,1\}^n \mapsto \{0,1\}^m$, ale bramka NAND jest jawnie nieodwracalna, gdyż mamy

$$\mathrm{NAND}(x,y) = 1 \oplus xy\,,$$

gdzie $\oplus$ oznacza dodawania modulo 2, więc np. $\mathrm{NAND}(0,0) = \mathrm{NAND}(0,1) = 1$, zatem z wyniku działania tej bramki nie możemy odtworzyć danych wejściowych. Istnieją jednak klasyczne odwracalne bramki logiczne postaci odwzorowań $\{0,1\}^n \mapsto \{0,1\}^n$. Przedstawimy dwie z nich, gdyż znajdują one zastosowanie również w obwodach kwantowych. Bramka cNOT (z ang. *controlled NOT*) działa w następujący sposób

$$\mathrm{cNOT}(x,y) = (x, x \oplus y)\,,$$

bit $x$ jest zatem *bitem kontrolnym*; jeśli $x = 0$ to kopiujemy $y$, natomiast jeśli $x = 1$ to $y \mapsto \mathrm{NOT}(y)$. Drugą bramką jest bramka Toffoli działająca w następujący sposób

$$\mathrm{Toff}(x,y,z) = (x,y,z \oplus xy)\,.$$

Zauważmy, iż jeśli $z = 1$ to bramka ta w sposób odwracalny realizuje operację NAND. Z tego względu bramka Toffoli jest uniwersalna i można za jej pomocą zrealizować dowolną funkcję boolowską (zakładając oczywiście odpowiednią liczbę bitów pomocniczych – takich jak $z$).

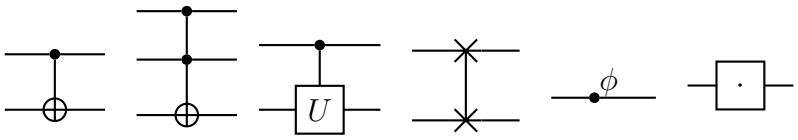
## 2.1 Kwantowe bramki logiczne

Kwantową bramką logiczną działającą na $n$ qubitach nazywamy dowolny operator unitarny $\mathbf{U}$ działający w przestrzeni $\mathscr{H}^{\otimes n}$ reprezentowany przez macierz wymiaru $2^n \times 2^n$. Będą nas interesować jednak głównie bramki jedno– i dwuqubitowe ze względu na następujące twierdzenie.

**Tw 2.1.** Każde przekształcenie unitarne w $\mathscr{H}^{\otimes n}$ może być zapisane jako złożenie przekształceń jednoqubitowych i bramek cNOT. Dodatkowo każde przekształcenie jednoqubitowe jest złożeniem bramek obrotów wokół X, Y, Z i bramki przesunięcia fazowego. Zbiór bramek $\{\mathrm{cNOT}, \mathrm{R}_x, \mathrm{R}_y, \mathrm{R}_z, \mathrm{P}\}$ jest więc uniwersalny.

Poniżej podajemy listę najczęstszych bramek jedno– i dwuqubitowych (bramki będziemy oznaczać czcionką prostą, niewytłuszczoną choć są to oczywiście operatory). Niektóre z nich pojawiły się wcześniej jako operatory. Diagramy bramek zamieszczono na Rysunku 2.1.

Łatwo sprawdzić, iż wszystkie zdefiniowane bramki są przekształceniami unitarnymi. W szczególności zauważmy, iż bramki cNOT i Toff permutują wektory




Rysunek 3: Diagramy odpowiednio bramek cNOT, Toff, cU, SWAP, P($\phi$) i pozostałych

bazy ortonormalnej i działają dokładnie w taki sposób jak klasyczne odpowiedniki tj.

$$\text{cNOT}\,|xy\rangle = |x(x \oplus y)\rangle\ , \quad \text{Toff}\,|xyz\rangle = |xy(z \oplus xy)\rangle\ .$$

Ponieważ wszystkie funkcje boolowskie można wyrazić przez klasyczne bramki Toffoli, więc dowolną taką funkcję możemy obliczyć w modelu obliczeń kwantowych zasadniczo za pomocą takiej samej liczby bramek. Zauważmy jednak, iż w przypadku modelu obliczeń kwantowych wejściem bramki może być dowolna superpozycja wektorów z bazy obliczeniowej; na wyjściu otrzymamy zatem superpozycję wszystkich wartości funkcji. Oczywiście dokonując na końcu pomiaru otrzymamy tylko jedną z wartości, więc w taki sposób nie uzyskamy oczywistej przewagi nad modelem klasycznym. Okazuje się jednak iż ów *paralelizm kwantowy* można wykorzystać w sposób dający nawet wykładniczą przewagę nad algorytmami klasycznymi.

## 2.2 Algorytmy kwantowe

TODO

### 2.2.1 Kwantowa Transformata Fouriera

TODO

### 2.2.2 Algorytm Shora

TODO

#### 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 $\phi$ to funkcja Eulera (liczbę $c$ nazywamy *kluczem publicznym*). Następnie oblicza odwrotność liczby $c$ modulo $\phi(N)$, tj. liczbę $d$

| **Pauli X** |
| --- |
| $\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |

| **Rotation X** |
| --- |
| $\mathrm{R}_x(\theta) = \begin{bmatrix} \cos(\theta/2) & -\mathrm{i}\sin(\theta/2) \\ -\mathrm{i}\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$ |

| **Pauli Y** |
| --- |
| $\mathrm{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ +\mathrm{i} & 0 \end{bmatrix}$ |

| **Rotation Y** |
| --- |
| $\mathrm{R}_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ +\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$ |

| **Pauli Z** |
| --- |
| $\mathrm{Z} = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}$ |

| **Rotation Z** |
| --- |
| $\mathrm{R}_z(\theta) = \begin{bmatrix} \exp(-\mathrm{i}\theta/2) & 0 \\ 0 & \exp(+\mathrm{i}\theta/2) \end{bmatrix}$ |

| **Hadamard** |
| --- |
| $\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |

| **Phase shift** |
| --- |
| $\mathrm{P}(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{bmatrix}$ |

| **cNOT** |
| --- |
| $\mathrm{cNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ |

| **cZ** |
| --- |
| $\mathrm{cZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ |

| **cU** |
| --- |
| $\mathrm{cU} = \begin{bmatrix} \mathbf{1} & 0 \\ 0 & \mathbf{U} \end{bmatrix}$ |

| **SWAP** |
| --- |
| $\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |

| **Toffoli** |
| --- |
| $\mathrm{Toff} = \begin{bmatrix} \mathbf{1}_6 & \mathbf{0} \\ \mathbf{0}^\top & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}$ |

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 $N$.

Załóżmy, że Alicja chce wysłać do Boba zaszyfrowaną wiadomość reprezento-

waną 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 równość 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 $\mathscr{H}$. Bazy te nazwiemy *dopełniającymi* iff

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

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

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

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

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

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

Załóżmy, że mamy zespół układów kwantowych przygotowanych w stanie $|\theta_k\rangle$, gdzie $\theta_k$ 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.

## 3.2 Entropia Shannona i von Neumanna

TODO