

Optymalizacja półokreślona w wykrywaniu splątania kwantowego

Spis treści

1	Wprowadzenie do informatyki kwantowej	3
1.1	Formalizm algebraiczny	3
1.1.1	Przestrzeń Hilberta	3
1.1.2	Baza kanoniczna	4
1.1.3	Współczynniki wektora w bazie ortonormalnej	5
1.1.4	Iloczyn skalarny – równoważne podejście	6
1.1.5	Iloczyn tensorowy	7
1.1.6	Iloczyn Kroneckera	8
1.1.7	Przestrzeń Hilberta-Schmidta	9
1.1.8	Operatory hermitowskie	10
1.2	Rozkład spektralny operatora	11
1.3	Definicje	12
1.3.1	Ślad operatora	13
1.3.2	Macierze Pauliego	14
1.3.3	Operator von Neumanna	15
1.3.4	Bazy	16
2	Kryteria separowalności	17
3	Wprowadzenie do programowania półokreślonego	17
3.1	Definicje	17

1 Wprowadzenie do informatyki kwantowej

1.1 Formalizm algebraiczny

1.1.1 Przestrzeń Hilberta

Weźmy przestrzeń liniową wymiaru n nad \mathbb{C} i wyposażmy ją w iloczyn skalarny. Tak powstałą strukturę nazwiemy *przestrzenią Hilberta* (ogólnie, tzn. nie skonkretyzowaną w żaden sposób przestrzeń Hilberta oznaczać będziemy \mathcal{H}). Element (wektor) tej przestrzeni oznaczamy $|\psi\rangle$, natomiast iloczyn skalarny pomiędzy dwoma wektorami $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ oznaczymy $\langle\psi|\phi\rangle$ (taką konwencja określana jest mianem *notacji Diraca*). Przypomnijmy jeszcze, że na przestrzeni Hilberta indukowana jest za pomocą iloczynu skalarnego *norma* wektora, standardowo $\|\psi\| \equiv \sqrt{\langle\psi|\psi\rangle}$.

1.1.2 Baza kanoniczna

Jako $\mathcal{B} \equiv \{|i\rangle_{i \in I}\}$ oznaczmy bazę przestrzeni \mathcal{H} . Zakładamy też, że \mathcal{B} stanowi ortonormalny układ wektorów – w przestrzeniach o skończonym wymiarze jesteśmy bowiem w stanie zastosować procedurę Grama-Schmidta. Dla ustalenia uwagi przyjmijmy $I \equiv \{0, 1, \dots, n-1\}$ – przy takich oznaczeniach bazę \mathcal{B} nazywamy bazą *kanoniczną*. Przyjmuje się, że wektory bazy kanonicznej oznaczamy

$$|i\rangle \equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

gdzie nad współczynnikiem 1 znajduje się i zer.

1.1.3 Współczynniki wektora w bazie ortonormalnej

Przypomnimy obecnie wzór na współczynniki wektora w rozwinięciu w bazie \mathcal{B} , która zgodnie z założeniem stanowi układ ortonormalny, tzn.

$$\langle i|j\rangle = \delta_{ij},$$

gdzie dwuargumentowa funkcja δ_{ij} , zwana *deltą Kroneckera*:

$$\delta_{ij} \equiv \begin{cases} 1, & \text{dla } i = j \\ 0, & \text{dla } i \neq j \end{cases}$$

Niech więc dowolnie ustalony wektor bazowy $|\alpha\rangle$ zostanie przemnożony skalarnie przez wektor $|\psi\rangle$. Pamiętając o własnościach iloczynu skalarnego (liniowość w drugim składniku) napiszemy

$$\langle \alpha|\psi\rangle = \langle \alpha|\left(\sum_i \psi_i |i\rangle\right) = \sum_i \psi_i \langle \alpha|i\rangle = \sum_i \psi_i \delta_{\alpha i} = \psi_\alpha$$

tzn.

$$\psi_\alpha = \langle \alpha|\psi\rangle .$$

1.1.4 Iloczyn skalarny – równoważne podejście

Iloczyn skalarny wektorów $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ można wyznaczyć wprost z definicji funkcji $\langle\psi|\phi\rangle$, a także za pomocą sumy współczynników tych wektorów. Dla

$$|\psi\rangle = \sum_{i \in I} \psi_i |i\rangle$$

oraz

$$|\phi\rangle = \sum_{i \in I} \phi_i |i\rangle$$

mamy bowiem

$$\langle\psi|\phi\rangle = \left(\sum_{i \in I} \psi_i \langle i| \right) \left(\sum_{j \in I} \phi_j |j\rangle \right) = \sum_{i,j \in I} \psi_i^* \phi_j \langle i|j\rangle = \sum_{i \in I} \psi_i^* \phi_i$$

1.1.5 Iloczyn tensorowy

Definicja 1 (Iloczyn tensorowy wektorów) Dla danych przestrzeni Hilberta \mathcal{H}_A oraz \mathcal{H}_B działanie mnożenia tensorowego wektorów z \mathcal{H}_A z wektorami z \mathcal{H}_B definiuje się jako funkcję $\otimes : \mathcal{H}_A \times \mathcal{H}_B \rightarrow \mathcal{H}_{AB}$, mającą własność liniowości w obu swoich składnikach, tzn.

1. **Jednorodność w obu składnikach.** Dla każdego skalaru $z \in \mathbb{C}$ i dla każdych wektorów $A \in \mathcal{H}_A$ oraz $B \in \mathcal{H}_B$

$$z(|A\rangle \otimes |B\rangle) = (z|A\rangle) \otimes |B\rangle = |A\rangle \otimes (z|B\rangle)$$

2. **Addytywność w pierwszym składniku.** Dla każdych wektorów $|A_1\rangle, |A_2\rangle \in \mathcal{H}_A$ oraz $|B\rangle \in \mathcal{H}_B$

$$(|A_1\rangle + |A_2\rangle) \otimes |B\rangle = |A_1\rangle \otimes |B\rangle + |A_2\rangle \otimes |B\rangle$$

3. **Addytywność w drugim składniku.** Dla każdych wektorów $|A\rangle \in \mathcal{H}_A$ oraz $|B_1\rangle, |B_2\rangle \in \mathcal{H}_B$

$$|A\rangle \otimes (|B_1\rangle + |B_2\rangle) = |A\rangle \otimes |B_1\rangle + |A\rangle \otimes |B_2\rangle$$

Definicja 2 (Iloczyn tensorowy przestrzeni) Iloczynem tensorowym przestrzeni Hilberta \mathcal{H}_A (z ortonormalną bazą $|i^A\rangle$) i \mathcal{H}_B (z ortonormalną bazą $|j^B\rangle$) nazywamy przestrzeń $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$, której elementy stanowią wszystkie wektory postaci

$$|C\rangle \equiv |A\rangle \otimes |B\rangle, \text{ dla } |A\rangle \in \mathcal{H}_A, |B\rangle \in \mathcal{H}_B. \quad (1)$$

Dodatkowo, wektory tej przestrzeni stanowią z definicji wszystkie kombinacje liniowe układu wektorów $|i^A\rangle \otimes |j^B\rangle$, tzn. zbiór wektorów postaci

$$|C\rangle = \sum_{ij} c_{ij} |i^A\rangle \otimes |j^B\rangle. \quad (2)$$

Definicja 3 (Stan splątany) Stan $|\psi\rangle \in \mathcal{H}_{AB}$ nazywamy splątany wtedy, gdy nie da się go przedstawić w postaci (1). Jest on wówczas stanem o postaci (2).

1.1.6 Iloczyn Kroneckera

Definicja 4 (Iloczyn Kroneckera) Dla macierzy $A \in M_{p \times q}(\mathbb{C})$ i $B \in M_{r \times s}(\mathbb{C})$ ich iloczyn Kroneckera zdefiniowany jest jako macierz $C \in M_{pr \times qs}(\mathbb{C})$ dana wzorem

$$C \equiv A \otimes B = \begin{pmatrix} A_{00}B & A_{01}B & \dots & A_{0,q-1}B \\ A_{10}B & A_{11}B & \dots & A_{1,q-1}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{p-1,0}B & A_{p-1,1}B & \dots & A_{p-1,q-1}B \end{pmatrix}.$$

Przykład 1 (Iloczyn Kroneckera) Dla danych macierzy

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$B = \begin{pmatrix} e & f & g \\ h & i & j \end{pmatrix}$$

ich iloczyn Kroneckera przyjmuje wartość

$$C = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \begin{pmatrix} ae & af & ag & be & bf & bg \\ ah & ai & aj & bh & bi & bj \\ ce & cf & cg & de & df & dg \\ ch & ci & cj & dh & di & dj \end{pmatrix}$$

1.1.7 Przestrzeń Hilberta-Schmidta

Definicja 5 (Przestrzeń Hilberta-Schmidta) *Dla danej przestrzeni Hilberta \mathcal{H} z bazą \mathcal{B} wprowadzamy przestrzeń operatorów liniowych $A : \mathcal{H} \rightarrow \mathcal{H}$ z działaniem standardowego dodawania dwóch operatorów i działaniem mnożenia operatora przez liczbę zespoloną. Przestrzeń taka jest przestrzenią liniową. Wyposażamy ją w działanie dwuargumentowe postaci*

$$\langle A|B \rangle \equiv \text{Tr}[A^\dagger B].$$

Łatwo pokazać, że tak zdefiniowana funkcja jest iloczynem skalarnym (nazywamy ją iloczynem skalarnym Hilberta-Schmidta) – przestrzeń operatorów rozszerzyliśmy wobec tego do przestrzeni Hilberta. Nazywamy ją przestrzenią Hilberta-Schmidta sprzężoną z przestrzenią \mathcal{H} i oznaczamy \mathcal{HS} .

1.1.8 Operatory hermitowskie

Definicja 6 (Operator hermitowski) *Operator liniowy A nazywamy hermitowskim (samosprężonym), gdy*

$$A = A^\dagger$$

Twierdzenie 1 *Wartości własne operatora hermitowskiego są rzeczywiste.*

1.2 Rozkład spektralny operatora

Definicja 7 (Operator normalny) *Operator liniowy A nazywamy normalnym gdy*

$$A^\dagger A = AA^\dagger$$

Twierdzenie 2 (Twierdzenie Spektralne) *Operator liniowy ma rozkład spektralny \Leftrightarrow jest normalny.*

1.3 Definicje

Definicja 8 (Komutator) Dla operatorów liniowych A, B ich komutator definiuje się jako operator

$$[A, B] \equiv AB - BA.$$

Ponadto, jeżeli $[A, B]$ jest operatorem zerowym to mówimy, że operatory A i B komutują.

Definicja 9 (Elementy macierzowe operatora) Elementem macierzowym w bazie \mathcal{B} operatora liniowego A nazywamy liczbę

$$A_{ij} \equiv \langle i | A | j \rangle,$$

gdzie $|i\rangle, |j\rangle \in \mathcal{B}$. Ponadto, elementy macierzowe postaci A_{ii} nazywamy elementami diagonalnymi operatora A .

Operator A można zapisać w następujący sposób:

$$A = \sum_{i,j \in I} A_{ij} |i\rangle \langle j|.$$

1.3.1 Ślad operatora

Definicja 10 (Ślad operatora) *Śladem operatora liniowego A nazywamy sumę jego elementów diagonalnych:*

$$\mathbf{Tr}[A] \equiv \sum_{i \in I} A_{ii}.$$

Twierdzenie 3 (Ślad operatora jest cykliczny) *Zachodzi*

$$\mathbf{Tr}[AB] = \mathbf{Tr}[BA]$$

1.3.2 Macierze Pauliego

Definicja 11 (Macierze Pauliego)

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

1.3.3 Operator von Neumanna

Definicja 12 (Operator binarny) Operator liniowy A nazywamy binarnym, gdy A jest hermitowski i $A^2 = I$.

Definicja 13 (Operator von Neumanna) Jeżeli $\hat{v} \in \mathbb{R}^3$ jest wektorem jednostkowym, to operatorem von Neumanna (operatorem pomiaru spinu wzdłuż osi \hat{v}) nazywamy operator działający na przestrzeni $V^2(\mathbb{C})$ dany wzorem

$$\hat{v} \cdot \vec{\sigma} \equiv \sum_{i=1}^3 v_i \sigma_i = \begin{pmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{pmatrix}.$$

Twierdzenie 4 Jeżeli $\hat{a} \cdot \vec{\sigma}, \hat{b} \cdot \vec{\sigma}$ są operatorami von Neumanna, to

$$(\hat{a} \cdot \vec{\sigma})(\hat{b} \cdot \vec{\sigma}) = (\hat{a} \cdot \hat{b}) I + i (\hat{a} \times \hat{b}) \cdot \vec{\sigma}.$$

Twierdzenie 5 Operator von Neumanna $\hat{v} \cdot \vec{\sigma}$ jest operatorem hermitowskim. Ponadto łatwo sprawdzić, że $(\hat{v} \cdot \vec{\sigma})^2 = I$. Wobec tego, $\hat{v} \cdot \vec{\sigma}$ jest operatorem binarnym.

Twierdzenie 6 Spektrum operatora von Neumanna $\hat{v} \cdot \vec{\sigma}$ to zbiór $\{+1, -1\}$. Ponadto

$$\hat{v} \cdot \vec{\sigma} = \Pi_+ - \Pi_-,$$

gdzie $\Pi_{\pm} = \frac{1}{2}(I \pm \hat{v} \cdot \vec{\sigma})$ jest projektorem rzutującym na odpowiednią podprzestrzeń własną.

1.3.4 Bazy

Definicja 14 (Baza Hadamarda)

$$|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Definicja 15 (Baza Bella)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

2 Kryteria separowalności

3 Wprowadzenie do programowania półokreślonego

3.1 Definicje

Definicja 16 (Operator dodatnio określony) *Operator liniowy A nazywamy dodatnio określonym, gdy*

$$\forall_{|\psi\rangle \in \mathcal{H}} \langle \psi | A | \psi \rangle \geq 0.$$

Piszemy wtedy $A \geq 0$.

Definicja 17 (Programowanie półokreślone) *Ogólne zagadnienie programowania półokreślonego w postaci pierwotnej definiuje się jako*

$$\begin{cases} \max \mathbf{Tr}[CX] \\ \text{ze względu na:} \\ \bullet \mathbf{Tr}[A_i X] = b_i, i = 1, \dots, p \\ \bullet X \geq 0 \end{cases}$$

gdzie

- $X \in M_{n \times n}(\mathbb{R})$ jest macierzą symetryczną traktowaną jako zmienna
- $C, A_i \in M_{n \times n}(\mathbb{R}), i = 1, \dots, p$ są danymi macierzami symetrycznymi
- $b_i \in \mathbb{R}, i = 1, \dots, p$ są danymi liczbami