

Optymalizacja półokreślona w wykrywaniu splątania kwantowego

Wojciech Wantka
promotor: dr inż. Piotr Mironowicz

- 1 Przegląd literatury odnośnie programowania półokreślonego.
- 2 Wprowadzenie do metod informatyki kwantowej.
- 3 Implementacja mechanizmu do wykrywania splątania kwantowego podanego stanu (z wykorzystaniem programowania półokreślonego).
- 4 Sporządzenie dokumentacji.

- $[n] \equiv \{0, 1, \dots, n-1\}$
- \mathcal{H} – przestrzeń Hilberta o wymiarze n z ortonormalną bazą kanoniczną

$$\mathcal{B} = \{|i\rangle\}_{i \in [n]}$$

- $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$

Stan czysty układu pojedynczego

W przestrzeni \mathcal{H} stanem czystym nazywamy unormowany wektor

$$|\psi\rangle = \sum_{i \in [n]} \psi_i |i\rangle.$$

Stan mieszany układu pojedynczego

Jeżeli pojedynczy układ kwantowy z prawdopodobieństwem p_i znajduje się w stanie czystym $|\psi_i\rangle$, to jego stan opisuje operator liniowy na \mathcal{H} , nazywany operatorem gęstości. Jest on postaci

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i|, 0 \leq p_i \leq 1, \sum_i p_i = 1.$$

Ślad operatora

Jeżeli ρ jest operatorem liniowym w przestrzeni z bazą ortonormalną $|i\rangle$, to ślad

$$\text{Tr}[\rho] = \sum_i \langle i | \rho | i \rangle$$

Dodatnia określoność

Operator liniowy ρ jest dodatnio określony, jeśli dla każdego $|\psi\rangle$ jest

$$\langle\psi|\rho|\psi\rangle \geq 0.$$

Pisze się wtedy $\rho \geq 0$.

Charakteryzacja operatorów gęstości

Operator ρ działający na przestrzeni Hilberta \mathcal{H} jest operatorem gęstości \Leftrightarrow

- 1 $\text{Tr}[\rho] = 1$
- 2 ρ jest operatorem dodatnio określonym

W przypadku układów złożonych można definiować pojęcie *splątania* i *separowalności* stanu kwantowego.

Czysty stan układu złożonego

W przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B$ stanem czystym nazywamy unormowany wektor

$$|\psi\rangle = \sum_{i \in [n_A], j \in [n_B]} \psi_{ij} |i_A\rangle |j_B\rangle$$

Czysty stan splątany

Stan w przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B$, którego nie da się przedstawić w postaci

$$|\psi\rangle = |\psi_A\rangle |\psi_B\rangle, |\psi_A\rangle \in \mathcal{H}_A, |\psi_B\rangle \in \mathcal{H}_B,$$

nazywamy stanem splątanym.

Uwaga

Stan, który nie jest splątany, nazywamy stanem separowalnym.

Czysty stan splątany – Przykład

Przykładem stanu splątanego na $\mathbb{C}^2 \otimes \mathbb{C}^2$ jest jeden ze stanów bazy Bella:

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

Niech

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$|\psi\rangle = c|0\rangle + d|1\rangle$$

Wtedy iloczyn tensorowy

$$|\psi\rangle|\phi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

Musiąłoby być

$$\begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases}$$

Widać od razu, że warunki te są sprzeczne.

Stan mieszany układu złożonego

W przypadku stanów mieszanych stan układu złożonego definiuje się jako operator gęstości ρ^{AB} działający na przestrzeni \mathcal{H}_{AB} . Nazywa się go wtedy *łącznym* operatorem gęstości. Definiujemy go ogólnie jako

$$\rho^{AB} \equiv \sum_{i,k \in [n_A]; j,l \in [n_B]} \rho_{ij,kl}^{AB} |a_i\rangle \langle a_k| \otimes |b_j\rangle \langle b_l|,$$

gdzie

$$0 \leq \rho_{ij,kl}^{AB} \leq 1, \quad \sum_{i,k \in [n_A]; j,l \in [n_B]} \rho_{ij,kl}^{AB} = 1$$

Definicja stanu separowalnego zostaje dla stanów mieszanych rozszerzona w stosunku do przypadku stanów czystych – za taki stan uważa się nie tylko produkt dwóch stanów, ale każdą wypukłą kombinację produktów.

Mieszany stan splątany

Jeżeli operator gęstości ρ^{AB} działający na przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B$ da się zapisać w postaci

$$\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B, 0 \leq p_i \leq 1, \sum_i p_i = 1,$$

gdzie ρ_i^A, ρ_i^B są operatorami gęstości działającymi na przestrzeni $\mathcal{H}_A, \mathcal{H}_B$ odpowiednio, to stan mieszany ρ^{AB} nazywamy separowalnym.

Okazuje się, że dla układów dwuczęściowych sprawa rozstrzygnięcia, czy operator gęstości działający na przestrzeni \mathcal{H}_{AB} jest separowalny, jest problemem algorytmicznie NP-trudnym (zob. [3]). Dla przypadku $n_A = n_B = 2$ istnieje jednak bardzo ważne kryterium. Najpierw podamy jednak definicję tzw. *częściowej transpozycji operatora gęstości*.

Niech $\mathcal{H}_A = \mathcal{H}_B$ są przestrzeniami Hilberta wymiaru n z ortonormalnymi bazami $|i\rangle_A, |j\rangle_B$ odpowiednio. Niech ρ jest operatorem gęstości na \mathcal{H}_{AB} i niech w bazie $|i_A j_B\rangle$ jego reprezentacja macierzowa ma postać

$$\begin{pmatrix} \rho_{00} & \rho_{01} & \cdots & \rho_{0,n-1} \\ \rho_{10} & \rho_{11} & \cdots & \rho_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \rho_{n-1,0} & \rho_{n-1,1} & \cdots & \rho_{n-1,n-1} \end{pmatrix}$$

Częściowa transpozycja operatora gęstości

Częściową transpozycją operatora ρ ze względu na podukład \mathcal{H}_B nazywamy operator ρ^Γ , którego reprezentacja macierzowa w bazie $|i_A j_B\rangle$:

$$\rho^\Gamma \equiv \begin{pmatrix} \rho_{00}^T & \rho_{01}^T & \cdots & \rho_{0,n-1}^T \\ \rho_{10}^T & \rho_{11}^T & \cdots & \rho_{1,n-1}^T \\ \vdots & \vdots & \vdots & \vdots \\ \rho_{n-1,0}^T & \rho_{n-1,1}^T & \cdots & \rho_{n-1,n-1}^T \end{pmatrix}$$

Częściowa transpozycja – własności

Częściowa transpozycja ze względu na podukład B :

- 1 Zachowuje hermitowskość operatora
- 2 Zachowuje ślad operatora

Kryterium Częściowej Transpozycji (*Peres-Horodecki criterion*),
zob. [3]

Operator gęstości ρ działający w przestrzeni $\mathbb{C}^2 \otimes \mathbb{C}^2$ jest stanem separowalnym \Leftrightarrow operator ρ^Γ jest operatorem gęstości.

Dodatnia półokreśloność (positive semidefiniteness)

Macierz S nazywa się *dodatnio półokreśloną*, gdy dla każdego $v \in \mathbb{R}^n$ jest

$$v^T S v \geq 0.$$

Pisze się wtedy $S \geq 0$. Pisze się też $-S \leq 0$.

Problem programowania półokreślonego – postać pierwotna

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

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.

Problem programowania półokreślonego – postać dualna

$$\begin{cases} \min c^T x \\ \text{ze względu na:} \\ \bullet F(x) \leq 0 \\ \bullet Ax = b, \end{cases}$$

gdzie

$$F(x) = G + \sum_{i=1}^m x_i F_i$$

dla

$$x \in \mathbb{R}^m; c \in \mathbb{R}^m; G, F_1, \dots, F_m \in \mathbf{S}^n$$

- 1 SDPA – wiele interfejsów do różnych języków programowania; wersje wspierające zrównoleglanie obliczeń etc.
- 2 YASS (C++)
- 3 CSDP (C)
- 4 DSDP

- ① SeDuMi
- ② SDPT3
- ③ YALMIP
- ④ CVX

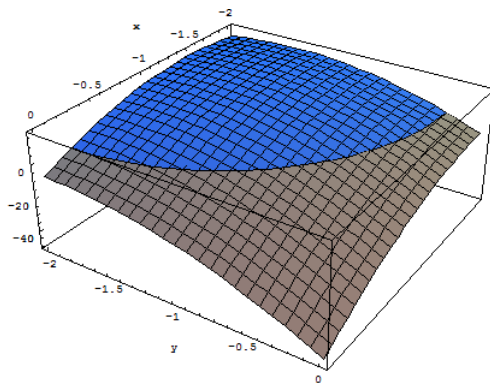
- 1 cvxopt (Python [dostępne jako pakiet w PyPI central]) – optymalizacja wypukła

❶ JOptimizer (Java, dostępne przez maven central)

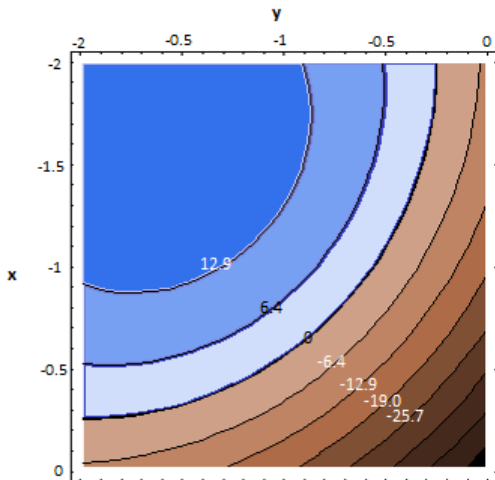
- 1 sdpt3r
- 2 Rcsdp (interfejs do CSDP)
- 3 Rdsdp (interfejs do DSPD)

$$\left\{ \begin{array}{l} \min \left(\begin{bmatrix} -\sqrt{\frac{21}{50}} & 0 \\ \frac{-\sqrt{2}}{5} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \right)^T \left(\begin{bmatrix} -\sqrt{\frac{21}{50}} & 0 \\ \frac{-\sqrt{2}}{5} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \right) \\ \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} \right)^T \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} \right) - 1.75^2 \leq 0 \end{array} \right.$$

Rysunek: Przykład 1 – obszar dopuszczalny



Rysunek: Przykład 1 – obszar dopuszczalny



$$\text{objectiveFunction}(\mathbf{x}) \equiv \mathbf{q} \cdot \mathbf{x} + r$$

```
double[] q = {<q0>, <q1>, ..., <q_n>};  
double r = <r_value>;  
LinearMultivariateRealFunction objectiveFunction =  
    new LinearMultivariateRealFunction(q, r);
```

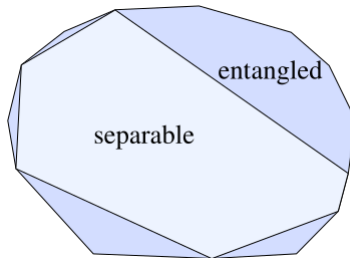
```
private static double[] optimize(  
    List<double[][]> fiMatrixList,  
    double[][] gMatrix,  
    OptimizationRequest optimizationRequest)  
    throws JOptimizerException  
{  
    BarrierFunction barrierFunction =  
        new SDPLogarithmicBarrier(fiMatrixList, gMatrix);  
    BarrierMethod barrierMethod =  
        new BarrierMethod(barrierFunction);  
    barrierMethod.setOptimizationRequest(  
        optimizationRequest);  
    barrierMethod.optimize();  
  
    return barrierMethod  
        .getOptimizationResponse()  
        .getSolution();  
}
```




Świadek splątania



Obserwabłę W nazywa się *świadkiem splątania*, gdy

- 1 $\text{Tr}[W\rho] \geq 0$ dla każdego separowalnego ρ
- 2 $\text{Tr}[W\rho] < 0$ dla przynajmniej jednego splątanego ρ

Rysunek: Stany kwantowe jako wypukłe kombinacje



-  [1] A. C. Doherty, Pablo A. Parrilo, Federico M. Spedalieri, *Distinguishing separable and entangled states* [arXiv:quant-ph/0112007].
-  [2] A. C. Doherty, Pablo A. Parrilo, Federico M. Spedalieri, *A complete family of separability criteria* [arXiv:quant-ph/0308032].
-  [3] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Quantum entanglement*, Reviews of Modern Physics **81**, 865 (2009) [arXiv:quant-ph/0702225].

-  Stephen Boyd, Lieven Vandenbergh, *Convex Optimization*
[<https://web.stanford.edu/~boyd/cvxbook/>].
-  www-user.tu-chemnitz.de/~helmberg/semidef.html.



[https://en.wikipedia.org/wiki/List_of_optimization_software.](https://en.wikipedia.org/wiki/List_of_optimization_software)



Ehsan Elhamifar, Guillermo Sapiro, Allen Yang, S. Shankar Sastry, *A Convex Optimization Framework for Active Learning.*