Rozróżnialność stanów kwantowych - kwantowa wersja twierdzenia Chernoffa

Stanisław Czachórski

8 czerwca 2015

Spis treści

Jabłko czy gruszka?

Informacja Shannona

- Ilość informacji o zdarzeniu x zależy tylko od jego prawdopodobieństwa p_x,
- $I(p)$ jest ciągłą funkcją p,
- $I(p_x, p_y) = I(p_x) + I(p_y))$.

$$I(x) \sim -\log(p_x)$$

Entropia Shannona

$$H(X) = -\sum_x P(X = x) \log P(X = x)$$

Względna entropia Shannona (Dywergencja Kullbacka-Leiblera)

$$D(X\|Y) = \sum_{x,y} p(X=x) \log \frac{p(X=x)}{p(Y=y)}$$
$$= -\sum_{x,y} p(X=x) \log p(Y=y) - H(X)$$

Przykład: rozkłady rzutów monetami

Pierwsza moneta: $P(X=0)=1-r$, $P(X=1)=r$
Druga moneta: $P(Y=0)=1-s$, $P(Y=1)=s$

$$D(X\|Y)=(1-r)\log\frac{1-r}{1-s}+r\log\frac{r}{s}$$

$$D(X\|Y)=(1-s)\log\frac{1-s}{1-r}+s\log\frac{s}{r}$$

Jeżeli $r=s$, wtedy: $D(X\|Y)=D(Y\|X)=0$
Jeżeli $r=\frac{1}{2}$, $s=\frac{1}{4}$, wtedy:

$$D(X\|Y)=\frac{1}{2}\log\frac{\frac{1}{2}}{\frac{3}{4}}+\frac{1}{2}\log\frac{\frac{1}{2}}{\frac{1}{4}}=1-\frac{1}{2}\log 3=0.2075\text{bit}$$

$$D(Y\|X)=\frac{3}{4}\log\frac{\frac{3}{4}}{\frac{1}{2}}+\frac{1}{4}\log\frac{\frac{1}{4}}{\frac{1}{2}}=\frac{3}{4}\log 3-1=0.1887\text{bit}$$

Testowanie hipotez

1. H_0 hipoteza zerowa - (*null hypotheses*)
   - to jest jabłko,
   - to jest rozkład X,
   - to jest stan ρ_0
2. H_1 alternatywa
   - to jest to gruszka,
   - to jest rozkład Y,
   - to jest stan ρ_1

Funkcja decyzyjna

- $g(x) = 0$ - akceptujemy H_0
- $g(x) = 1$ - akceptujemy H_1

Ponieważ przyjmuje dwie wartości wystarczy obszar A na którym przyjmuje 0 i jego dopełnienie.

$$A = \{z : P(X = z) > P(Y = z)T\}$$

Prawdodobieństwo błędu

$$\alpha = P(g(x) = 1 | H_0 \text{ prawdziwe})$$
$$\beta = P(g(x) = 0 | H_1 \text{ prawdziwe})$$

Średnie prawdopodobieństwo błedu

$$P_e := \pi_0 \alpha + \pi_1 \beta,$$

gdzie π_0 i π_1 są prawdopodobieństwami *a priori*

Asymetryczne testowanie hipotez: lemat Chernoffa-Steina i kwantowy lemat Chernofa-Steina.

(Klasyczne) Twierdzenie Chernoffa

Średnie prawdpodobieństwem błędu, po n testach hipotezy

$$P_{e,n} := \pi_0 \alpha_n + \pi_1 \beta_n,$$

zachowuje się asymptotycznie jak

$$P_{e,n} \sim e^{-n\xi_{CB}p,q},$$

gdzie

$$\xi_{CB}(p,q) := -\log\left(\inf_{0\leqslant s\leqslant 1} \sum_i p(i)^{1-s} q(i)^s\right)$$

Związek twierdzenia Chernoff i Dywergencja Kullbacka-Leiblera

Wielkość $\xi_{CB}(p_0, p_1)$ możemy wyrazić poprzez dywergencję Kullbacka-Leiblera

$$\xi_{CB}(p_0, p_1) = D(p_{s^*} \| p_0) = D(p_{s^*} \| p_1), \tag{1}$$

gdzie

$$p_s(b) = \frac{p_0^s(b) p_1^{1-s}(b)}{\sum_b p_0^s(b) p_1^{1-s}(b)}, \quad s \in [0, 1],$$

a s^* jest wartością dla której zachodzi równość w równaniu (1).

Stan czysty

Niech $\mathcal{H}$ będzie skończenie wymiarową przestrzenią Hilberta. (Czyste) stany kwantowe są opiswane przez wektory tej przestrzeni

$$|\psi\rangle \in \mathcal{H} : |\langle\psi|\psi\rangle|^2 = 1.$$

Rzutowanie i prawdopodobieństwo

Prawdopodobieństwo, że stan ψ może by zmierzony w stanie ϕ wynosi $|\langle\phi|\psi\rangle|^2$.

Jednowymiarowe operatory rzutowe

Wektorom (stanom czystym) $|\psi\rangle \in \mathcal{H}$ odpowiadają jednowymiarowe operatory rzutowe

$$|\psi\rangle \langle\psi| \in \mathcal{B}(\mathcal{H}).$$

Macierz gęstości

Jeżeli stany $|\psi\rangle$ występują z prawdopodobieństami p_i możemy je opisać przy pomocy macierzy gęstości ρ

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| .$$

Macierz gęstości

1. jest hermitowska ($\rho^\dagger = \rho$)
2. ma ślad równy 1 ($\mathrm{Tr}(\rho)$=1)

Pomiar realizujemy poprzez POVMy

Positive Operator Valued Measure (POVM)

Rodzina operatorów E_b

1. dodatnio określonych: $\langle\psi|E_b|\psi\rangle \geqslant 0$ dla wszystkich b i $|\psi\rangle$,
2. zupełna:

$$\sum_b E_b = \mathbb{1}$$

.

Wierność (Fidelity) dla stanów czystych

$$F\left(|\psi\rangle, |\phi\rangle\right) = |\langle\phi|\psi\rangle|$$

Prawdopodobieństwo rozróżnienia

$$\begin{aligned} P_H &= \frac{1}{2}\left(1 + \sqrt{1 - |\langle\phi|\psi\rangle|^2}\right) \\ &= \frac{1}{2}\left(1 + \sqrt{1 - F^2}\right) \end{aligned}$$

Niech E - pomiar $(E_1 + E_2 = \mathbb{1})$

$$\begin{aligned} P_H &= \frac{1}{2}\left(\langle\psi_1|E_1|\psi_1\rangle + \langle\psi_2|E_2|\psi_2\rangle\right) \\ &= \frac{1}{2}\left(1 + \langle\psi_2|E_2|\psi_2\rangle - \langle\psi_1|E_2|\psi_1\rangle\right) \\ &= \frac{1}{2}\left(1 + \mathrm{Tr}E_2\left(|\psi_2\rangle\langle\psi_2| - |\psi_1\rangle\langle\psi_1|\right)\right) \end{aligned}$$

Wprowadźmy macierz Γ postaci

$$\Gamma = |\psi_2\rangle\langle\psi_2| - |\psi_1\rangle\langle\psi_1|.$$

Zatem

$$P_H = \frac{1}{2}\left(1 + \mathrm{Tr}(E_2\Gamma)\right)$$

Problem sprowadza się do zmaksymalizowania wielkości $\mathrm{Tr}(E_2\Gamma)$. Żeby to osiągnąć szkamy wektorów własnych macierz Γ, a nstępnie dobieramy macierz E_2, tak żeby była rzutem na wektor własny do dotaniej wartości. Γ ma diwe wartości własne $\pm\frac{1}{2}\left(1 + \sqrt{1 - |\langle\phi|\psi\rangle|^2}\right)$.

Wierność (Fidelity)

$$F(\sigma, \rho) := \mathrm{Tr}[(\rho^{1/2}\sigma\rho^{1/2})^{1/2}],$$

Norma śladowa

$$\frac{1}{2}||\rho - \sigma||_1 = \mathrm{Tr}|\sigma - \rho|,$$

gdzie wartość bezwzględna z operatora jest zdefiniowana:

$$|A| = (A^\dagger A)^{1/2}$$

„Najlepsza” strategia rozróżniania

Prawdopodbieństow błędu

Stany kwantowe ρ_0 i ρ_1 z prawdopodobieństwani *a priori* π_0 i π_1. Prawdopodobieństwo błędu definiujemy jako

$$P_e = \pi_0 \mathrm{Tr}(\rho_0 E_1) + \pi_1 \mathrm{Tr}(\rho_1 E_0).$$

Chcemy znaleźć takie POVM $(E_0^{(H)}, E_1^{(H)})$, żebe P_e było jak najmniejsze.

Macierz Γ Helstorma

Uogólnie macierzy $\Gamma = |\psi_2\rangle\langle\psi_2| - |\psi_1\rangle\langle\psi_1|$ na przypadek stanów mieszanych

$$\Gamma := \pi_1\rho_1 - \pi_0\rho_0.$$

$$\begin{aligned} P_e &= \pi_0 \mathrm{Tr}(\rho_0 E_1) + \pi_1 \mathrm{Tr}(\rho_1 E_0) \\ &= \pi_0 \mathrm{Tr}\left(\rho_0(\mathbb{1} - E_0)\right) + \pi_1 \mathrm{Tr}(\rho_1 E_0) \\ &= \pi_0 \mathrm{Tr}\rho_0 - \pi_0 \mathrm{Tr}(\rho_0 E_0) + \pi_1 \mathrm{Tr}(\rho_1 E_0) \\ &= \pi_0 + \mathrm{Tr}\left((\pi_1\rho_1 - \pi_0\rho_0)E_0\right) \\ &= \pi_0 + \mathrm{Tr}(\Gamma E_0) \end{aligned}$$

Niech Γ ma rozkład spektralny

$$\Gamma = \sum_j \gamma_j |j\rangle\langle j|$$

Zatem

$$\mathrm{Tr}(\Gamma E_0) = \sum_j \gamma_j \langle j|E_0|j\rangle$$

Ponieważ Γ nie jest ani ujemnie ani dodatnio określona, zatem ta wielkość jest ograniczona od dołu przez sumę ujemnnych wartości własnych

$$\mathrm{Tr}(\Gamma E_0) \geqslant \sum_j{}' \gamma_j.$$

Zatem jeżeli znajdziemy E_0 wysycające tę nierówność będzie ono optymalne.

Optymalny E_0

$$\left\langle j|E_0^{(H)}|j\right\rangle = 1 \quad \text{gdy} \quad \gamma_j < 0$$
$$\left\langle j|E_0^{(H)}|j\right\rangle = 0 \quad \text{gdy} \quad \gamma_j > 0$$

Niech $E_0^{(H)}$ ma rozkład spektralny

$$E_0^{(H)} = \sum_k e_k \left|e_k\right\rangle \left\langle e_k\right| .$$

Następnie rozważmy taki j, że $\gamma_j > 0$, wówczas

$$0 = \left\langle j\right| E_0^{(H)} \left|j\right\rangle = \sum_k e_k \left|\left\langle e_k|j\right\rangle\right|^2 .$$

Ponieważ $\left|\left\langle e_k|j\right\rangle\right|^2 \leqslant 0$, więc $\left\langle e_k|j\right\rangle = 0$, gdy $e_k \neq 0$. Zatem

$$\left\langle k\right| E_0^{(H)} \left|j\right\rangle = \sum_l e_l \left\langle k|e_l\right\rangle \left\langle e_l|j\right\rangle = 0$$

1. Zatem nie musimy definiować elementów pozadiagonalnych, są one równe zero ze względu na własności E_0
2. Mamy operator określony jednoznacznie z dokładnością do tych j, gdzie $\gamma_j = 0$
3. Analogicznym rozumowaniem możemy pokazać $\langle j|E_1|k\rangle = 0$.
4. Mamy zatem zdefiniowane operatory E_0 i E_1
5. Sa one diagonalne w bazie własnej operatora Γ

Problem

Możemy znaleźć dwie pary stanów kwantowych ρ, σ i ρ, σ

$$\|\rho - \sigma\|_1 < \|\rho' - \sigma'\|_1$$

ale równocześnie

$$\|\rho^{\otimes 2} - \sigma^{\otimes 2}\|_1 > \|\rho'^{\otimes 2} - \sigma'^{\otimes 2}\|_1$$

Weźmy macierze

$$\rho = \begin{pmatrix} 1/4 & 0 \\ 0 & 3/4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$$

$$\rho' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma' = \begin{pmatrix} b & 0 \\ 0 & 1-b \end{pmatrix}$$

wówczas jeśli parametr b przyjmie wartość z przedziału $b \in (1 - 1/\sqrt{2}, 1/2)$ to otrzymamy

$$\|\rho - \sigma\|_1 = 1 > 2b = \|\rho' - \sigma'\|_1$$

i jednocześnie

$$\|\rho^{\otimes 2} - \sigma^{\otimes 2}\|_1 = 1 < 2b(2-b) = \|\rho'^{\otimes 2} - \sigma'^{\otimes 2}\|_1.$$

Defincje

$$P_{e,n}^{(H)} := \frac{1}{2}\left(1 - \|\pi_1\rho_1^{\otimes n} - \pi_0\rho_0^{\otimes n}\|_1\right)$$

$$\xi_{QCB} := -\log(\min_{0\leqslant s\leqslant 1} \mathrm{Tr}[\rho^s\sigma^{1-s}])$$

Kwantowa wersja twierdzenia Chernoffa

Niech $\mathcal{H}$ będzie skończenie wymiarową przestrzenią Hilberta, σ, ρ stanami kwantowymi na $\mathcal{H}$ o prawdopodobieństwach *a priori* π_0 i π_1, wówczas przy powyższych definicjach zachodzi

$$\xi_{QCB} = \lim_{n\to\infty}\left(-\frac{1}{n}\log P_{e,n}^{(H)}\right).$$

$\xi_{QCB} \leqslant \liminf_{n\to\infty}\left(-\frac{1}{n}\log P_{e,n}^{(H)}\right)$

Twierdzenie

Niech A i B będą operatorami dodatnimi. Wtedy dla wszystkich $0 \leqslant s \leqslant 1$ zachodzi:

$$\mathrm{Tr}[A^s B^{1-s}] \geqslant \mathrm{Tr}[A+B-|A-B|]/2$$

.

Niech $A = \pi_1\rho_1^{\otimes n}$ i $B = \pi_0\rho_0^{\otimes n}$, wtedy:

$$\mathrm{Tr}[A+B-|A-B|]/2 = \frac{1}{2}\left(1 - \|\pi_1\rho_1^{\otimes n} - \pi_0\rho_0^{\otimes n}\|_1\right) = P_{e,n}^{(H)},$$

oraz

$$\log(\mathrm{Tr}[A^s B^{1-s}]) = \log(\pi_0^s\pi_1^{1-s}) + n\log(\mathrm{Tr}[\rho_0^s\rho_1^{1-s}]).$$

$\xi_{QCB} \geqslant \liminf_{n\to\infty} \left(-\frac{1}{n}\log P_{e,n}^{(H)}\right)$

Weźmy rozkład spektralny stanów ρ i σ

$$\rho = \sum_{i=1}^{d} \lambda_i |x_i\rangle \langle x_i| , \sigma = \sum_{j=1}^{d} \mu_i |y_i\rangle \langle y_i|$$

a następnie z wartości i wektorów własnych ρ i σ tworzymy macierze:

$$p_{i,j} = \lambda_i |\langle x_i|y_j\rangle|^2 , q_{i,j} = \mu_j |\langle x_i|y_j\rangle|^2$$

Lemat

$$\mathrm{Tr}[\rho^{1-s}\sigma^s] = \sum_{i,j} p_{i,j}^{1-s} q_{i,j}^s$$

Własności wielkości Q

Non-logarythmic Variety Quantum Chernoff Bound

$$Q(\rho,\sigma) := \min_{0\leqslant s\leqslant 1} \mathrm{Tr}[\rho^s \sigma^{1-s}]$$

Związek z wiernością o odległością śladową

Przy definicjach

$$F(\sigma,\rho) := \mathrm{Tr}[(\rho^{1/2}\sigma\rho^{1/2})^{1/2}],$$

$$T(\sigma,\rho) := \frac{1}{2}||\rho-\sigma||_1,$$

zachodzi:

$$1-\sqrt{1-F^2} \leqslant 1-T \leqslant Q \leqslant F \leqslant \sqrt{1-T^2}.$$

Ciągłość

Funkacja $Q(\rho, \sigma)$ jest ciągła.

Wypukłaość

Funkcja $s \to Q_s = \mathrm{Tr}[\rho^{1-s}\sigma^s]$ jest wypukła jako względem s.

Monotoniczność względem odwzorowań CPTP

Jeżeli Ψ jest odwzorowaniem CPTP, wówczas

$$Q(\Psi(\rho), \Psi(\sigma)) \geqslant Q(\rho, \sigma).$$

W szczególności, Q jest niezmiennicze względem podobieństw unitarnych

$$Q(U\rho U^\dagger, U\sigma U^\dagger) = Q(\rho, \sigma).$$

Bibliografia

1. T. M. Cover, J. A. Cover *Elements of Inforamtion Theory* Wiley, 2006
2. V. Vedral *Introduction to Quantum Information Science* Oxford Univ. Press, 2006
3. C. W. Helstrom *Quantum Detection and Estimation Theory* Elsevier, Academic Press, 1976
4. K. M. R. Audenaert, J. Calsamiglia, R. Munoz-Tapia, E. Began, L. Masanes, A. Acin, F. Verstraete *Discriminating States: Quantum Chernoff Bound* PRL **98**, 160501 (2007),
5. K. M. R. Audenaert, M. Nussbaum, A. Szkoła, F. Verstreate *Asymptotic Error Rates in Quantum Hypothesis Testing* Comm. Math. Phys. 279, 251-283 (2008)
6. C. F. Fuchs *Distinguishability and Accessible Information in Quantum Theory*