Cholevův odhad

Z postulátu měření plyne, že von Neumannova entropie přesně odpovídá entropii náhodné veličiny, kterou je měření daného smíšeného stavu v bázi jeho vlastních vektorů. Jak už jsme ale řekli, „správně“ definovaná entropie by měla brát v úvahu všechna možná měření. Náhodná veličina, o které se měřením snažíme získat informaci je náhodná veličina s rozdělním definujícím soubor stavů. Přesný vztah von Neumannovy entropie k informaci dosažitelné libovolným měřením není znám. Nejdůležitější výsledek v tomto směru je tzv. Cholevův odhad (anglicky: Holevo bound).

Věta (Cholevův odhad). Nechť X je diskrétní náhodná veličina s rozdělením $\Pr[X = i] = p_i$. Nechť $\rho = \sum_{i=1}^{n} p_i \rho_i$ je smíšený stav vzniklý zakódováním hodnoty X pomocí stavů ρ_i. Nechť Y je náhodná veličina výsledků nějakého měření stavu ρ. Pak

$$I(X:Y) \leq S(\rho) - \sum_{i=1}^{n} p_i S(\rho_i)\,.$$

Cholevův odhad říká, že Von Neumannova entropie je horním odhadem pro informaci dostupnou jakýmkoli měřením o náhodné veličině X. Pokud jsou všechny stavy ρ_i čisté, pak má nerovnost tvar $I(X:Y) \leq S(\rho)$. Navíc víme, že $S(\rho) \leq H(X)$, což dává klasické $I(X:Y) \leq H(X)$.

Rovnost $S(\rho) = H(X)$ přitom nastává, právě když jsou stavy čisté a rozlišitelné. Pak se totiž jedná o klasickou náhodnou veličinu, není důležité, že její hodnoty chápeme kvantově. Pak také $I(X:Y) = H(X)$ pro měření v bázi obsahující volené stavy, kdy $Y = X$.

Pro důkaz Cholevova odhadu uvažujme kromě samotného připravovaného a měřeného systému, označme ho Q, ještě systém P, který obsahuje informaci o hodnotě náhodné veličiny X zakódovanou do bázových stavů, a systém M, obsahující naopak podobně zakódovaný výsledek Y měření, které nechť je dáno operátory (M_j). Po přípravě je matice hustoty tohoto složeného systému

$$\rho_0^{PQM} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i \otimes |0\rangle\langle 0|\,,$$

a po měření je

$$\rho_1^{PQM} = \sum_{i,j} p_i |i\rangle\langle i| \otimes M_j \rho_i M_j^\dagger \otimes |j\rangle\langle j|\,.$$

Ukazuje se, že Cholevův odhad je vlastně nerovnost

$$S(\rho_1^P : \rho_1^M) \leq S(\rho_0^P : \rho_0^Q)\,.$$

Ověřme pro pravou stranu:

$$\rho_0^P = \sum_i p_i |i\rangle\langle i| \qquad S(\rho_0^P) = H(X)$$

$$\rho_0^Q = \rho = \sum_i p_i \rho_i \qquad S(\rho_0^Q) = S(\rho)$$

$$\rho_0^{PQ} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i \qquad S(\rho_0^{PQ}) = H(X) + \sum_i p_i S(\rho_i)$$

Pro levou stranu si nejprve uvědomme, že $\mathrm{tr}(M_j \rho_i M_j)$ je pravděpodobnost, že výsledek měření bude j, za podmínky, že měřený stav je ρ_i, označme ji $p_{j|i}$. Protože

je výsledek měření na volbě X nezávislý, je $p_i p_{j|i}$ sdružená pravděpodobnost i a j, označme ji p_{ij}. Tedy:

$$\rho_1^P = \sum_{i,j} p_{ij}|i\rangle\langle i| = \sum_i p_i|i\rangle\langle i| \qquad S(\rho_1^P) = H(X)$$

$$\rho_1^M = \sum_{i,j} p_{ij}|j\rangle\langle j| = \sum_j p_j|j\rangle\langle j| \qquad S(\rho_1^M) = H(Y)$$

$$\rho_0^{PM} = \sum_{i,j} p_{ij}|i\rangle\langle i| \otimes |j\rangle\langle j| \qquad S(\rho_1^{PM}) = H(X,Y)$$

Cholevův odhad nyní plyne takto:

$$S(\rho_0^P : \rho_0^Q) = S(\rho_0^P : \rho_0^{QM}) \geq S(\rho_1^P : \rho_1^{QM}) \geq S(\rho_1^P : \rho_1^M).$$

Odvození vyplývá ze tří intuitivních (a dokazatelných) principů:

- vzájemná informace se nezmění přidáním dodatečného (nekorelovaného) systému;
- vzájemnou informaci dvou systémů nelze žádným měřením (ani žádnými unitárními operacemi) zvýšit;
- vzájemnou informaci nelze zvýšit odstraněním části jednoho ze systémů.

První princip jednoduše plyne ze vztahu entropie rozložitelných stavů $S(\sigma\otimes\rho) = S(\sigma) + S(\rho)$, který dostaneme přímo z definice.

Třetí princip plyne ze silné subaditivity. V našem případě máme

$$S(\rho_1^{PQM}) + S(\rho_1^M) \leq S(\rho_1^{PM}) + S(\rho_1^{QM}),$$

odkud dostáváme požadované

$$S(\rho_1^P) + S(\rho_1^M) - S(\rho_1^{PM}) \leq S(\rho_1^P) + S(\rho_1^{QM}) - S(\rho_1^{PQM})\,.$$

Pokud jde o druhý princip, všimněme si nejprve, že matice $U\rho U^\dagger$ jsou podobné, tedy mají stejný diagonální tvar, tedy $S(\rho) = S(U\rho U^\dagger)$. Je přirozené, že entropie se nemění volbou jiné báze. Pro měření můžeme princip redukovat na princip druhý tím, že ukážeme, že každé měření lze chápat jako unitární transformaci našeho systému spolu s nějakým vnějším, dodatečným systémem, který po měření opět odstraníme. Tato elegantní a užitečná konstrukce probíhá následujícím způsobem.

Označme měřený systém Q a uvažujme měření pomocí operátorů (M_j). Dodatečný systém M bude mít bázové prvky $|j\rangle$. Pak platí, že „indexující“ zobrazení

$$U : |\varphi\rangle \otimes |0\rangle \mapsto \sum_j M_j|\varphi\rangle \otimes |j\rangle$$

je unitární. Přesněji řečeno, toto zobrazení zachovává skalární součin (jak lze přímočaře ověřit za použití vztahu úplnosti $\sum_j M_j^\dagger M_j = E$), a můžeme ho tedy rozšířit na unitární zobrazení systému $Q \otimes M$. Výsledná matice hustoty je tedy

$$\rho^{QM} = U(|\varphi\rangle\langle\varphi| \otimes |0\rangle\langle 0|)U^\dagger = \sum_{j,j'} M_j|\varphi\rangle\langle\varphi|M_{j'}^\dagger \otimes |j\rangle\langle j'|$$

a redukovaná matice pro původní systém je

$$\rho^Q = \sum_j M_j|\varphi\rangle\langle\varphi|M_j^\dagger\,,$$

jak jsme chtěli.