Kvantová entropie

Entropie je mírou informačního obsahu náhodné veličiny. Klasická entropie, měřená v bitech a nazývaná podle svého objevitele *Shannonova*, je pro diskrétní náhodnou veličinu X s pravděpodobnostmi $\Pr[X = i] = p_i$, definovaná vzorcem

$$H(X) = -\sum_i p(i) \log p_i.$$

Tuto hodnotu lze neformálně interpretovat jako průměrný počet bitů adresy náhodného jevu, ke kterému došlo. Základní vlastnost Shannonovy entropie, která ukazuje, že skutečně vyjadřuje informační obsah, je věta o kódování zdroje, nazývaná též věta o kompresi nebo věta o kapacitě kanálu bez šumu. Ta ukazuje, že posloupnost n nezávislých kopií náhodné veličiny X lze zakódovat posloupností bitů délky $nH(X)$ s pravděpodobností chyby asymptoticky jdoucí k nule pro velká n. (Věta se dokazuje tak, že si všimneme, že převážná většina posloupností má očekávané rozložení počtu písmen, a ukážeme, že takových typických posloupností délky n je téměř přesně $2^{nH(X)}$.)

Celková informace dvojice náhodných veličin $H(X, Y)$ je nejvýše součet $H(X) + H(Y)$, může však být menší. Pokud je například Y funkcí X, pak je hodnota (X, Y) zcela určena hodnotou X a platí $H(X, Y) = H(X)$. Zbylý informační obsah Y při znalosti X je entropie podmíněné náhodné veličiny $H(Y \mid X)$. (Správně bych měli říct „průměrná entropie“, protože jde o průměr přes různé hodnoty X. Entropie $H(Y)$ sama je ostatně průměrem přes různé hodnoty Y.) Hodnota $H(Y) - H(Y \mid X)$ tedy vyjadřuje kolik informace o Y se dozvídáme, pokud známe X. Podobně je $H(X) - H(X \mid Y)$ mírou informace, kterou Y odhaluje o X. Platí očekávaný vztah $H(X, Y) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y)$. Hodnota

$$I(X : Y) := H(X) + H(Y) - H(X, Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

je tedy mírou závislosti obou veličin a je nazývaná *vzájemné informace*. Všimněme si, že tato hodnota je symetrická vzhledem k X a Y.

Informační obsah kvantového systému je dána nejistotou o výsledcích měření. Jinak řečeno, výsledek daného měření daného systému je náhodná veličina s nějakou entropií. Entropie kvantového stavu však musí brát v úvahu všechna možná měření. Je-li systém v čistém stavu, existuje měření, jehož výsledek je dán jednoznačně (je to jakékoli měření v bázi obsahující měřený stav). Entropie kvantového systému je tedy nenulová jen v případě smíšených stavů a pochází z nejistoty o připraveném stavu. Ovlivňuje ji ale také povaha souboru. Ilustrujme to na stavech, které se vyskytují v protokolu BB84. Víme-li, v jaké bázi Alice kóduje, ale nevíme jaký kóduje bit, je systém ve stavu

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}E\,.$$

Měření v kanonické bázi je ekvivalentní přijetí náhodného bitu. Skutečnost, že hodnota byla zakódována kvantově, a ne klasicky zde nehraje žádnou roli. Entropie takového stavu by tedy měla být rovna jedné. Víme-li naopak, že Alice kódovala nulu, ale nevíme v jaké bázi, dostáváme matici

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \sim \begin{pmatrix} \frac{2+\sqrt{2}}{4} & 0 \\ 0 & \frac{2-\sqrt{2}}{4} \end{pmatrix}.$$

Diagonální tvar je vůči (znormovaným) vlastním vektorům

$$|v_1\rangle = \frac{1}{\sqrt{4+2\sqrt{2}}}\begin{pmatrix}-1\\ \sqrt{2}+1\end{pmatrix}, \qquad |v_2\rangle = \frac{1}{\sqrt{4-2\sqrt{2}}}\begin{pmatrix}1\\ \sqrt{2}-1\end{pmatrix}.$$

Stejnou matici hustoty tedy dostaneme, pokud zvolíme $|v_1\rangle$ nebo $|v_2\rangle$ s pravděpodobnostmi $\frac{2+\sqrt{2}}{4}$ a $\frac{2-\sqrt{2}}{4}$. Klasická entropie takové náhodné veličiny je

$$-\frac{2+\sqrt{2}}{4}\log\frac{2+\sqrt{2}}{4} - \frac{2-\sqrt{2}}{4}\log\frac{2-\sqrt{2}}{4} \doteq 0.6\,.$$

Entropie není rovna jedné, protože zvolený bit byl zakódován do dvou stavů, které nejsou zcela rozlišitelné, čímž se část informace ztratila.

Na tomto příkladu můžeme také ilustrovat nezávislost výsledku měření na způsobu, jakým daná matice hustoty vznikla. Zkoumejme pravděpodobnost, s jakou při měření v bázi $|0\rangle$, $|1\rangle$ dostaneme výsledek odpovídající $|0\rangle$. Podle Postulátu 3' je to $\mathrm{tr}(|0\rangle\langle 0|\rho) = 3/4$. To odpovídá prosté úvaze: s pravděpodobností jedna polovina máme stav $|0\rangle$, a pak výsledek měření odpovídá $|0\rangle$ s jistotou; s pravděpodobností jedna polovina máme stav $|+\rangle$, kdy výsledek odpovídá $|0\rangle$ s pravděpodobností jedna polovina. Podobně bychom mohli ověřit, že pokud $|v_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ a $|v_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, pak

$$\frac{2+\sqrt{2}}{4}|\alpha_1|^2 + \frac{2-\sqrt{2}}{4}|\alpha_2|^2 = \frac{3}{4}\,.$$

Uvedené příklady vedou k definici *Von Neumannovy entropie* matice hustoty ρ. Je to entropie náhodné veličiny odpovídající volbě vlastních vektorů ρ, což lze úsporně zapsat jako

$$S(\rho) = -\,\mathrm{tr}(\rho\log\rho)\,.$$

Vyjmenujme některé vlastnosti kvantové entropie. Pro entropii smíšeného stavu $\rho = \sum_i p_i\rho_i$ platí

$$S(\rho) \le H(X) + \sum_i p_i S(\rho_i),$$

kde X je náhodná veličina výběru stavu ρ_i, tedy diskrétní náhodná veličina s pravděpodobností $\Pr[X=i] = p_i$. Rovnost přitom platí pravě když jsou stavy ρ_i rozlišitelné, tedy pokud jsou definované na vzájemně kolmých prostorech. Entropie stavu ρ je nejvýše entropie příslušného procesu volby ρ_i plus průměrná entropie obsažená v samotných ρ_i. Jsou-li stavy ρ_i čisté, dostáváme $S(\rho) \le H(X)$. Jsou-li čisté a rozlišitelné, máme $S(\rho) = H(X)$. Pak se totiž jedná o klasickou náhodnou veličinu, není důležité, že její hodnoty kódujeme kvantově.

Pro složené systémy platí *silná subaditivita*:

$$S(\rho^{ABC}) + S(\rho^B) \le S(\rho^{AB}) + S(\rho^{BC})\,.$$

Definujme po vzoru klasické vzájemné informace vzájemnou informaci dvou kvantových stavů jako

$$S(\rho^A : \rho^B) := S(\rho^A) + S(\rho^B) - S(\rho^{AB})\,.$$