「量子スピードアップ」にはエンタングルメントもマクロ量子コヒーレンスも必要ない

平成 29 年 5 月 25 日

量子計算が古典計算よりも「速い」ためにはエンタングルメントやマクロ量子コヒーレンスが必要だ、とたまに言われますが、それは間違いです。（例えば、エンタングルメントについては [Van den Nest, PRL 110, 060504 (2013)] でそれが証明されています。）

今、エンタングルメントや、マクロ量子コヒーレンス等のある種の「量子性」を計る量を C としましょう。つまり、ある状態 ρ がもっている「量子性」の値は $C(\rho)$ というある実数値です。

まず、C は「明らかに量子性の無い」状態 ξ については最小値 C_{min} をとるべきです。つまり $C(\xi)=C_{min}$ です。例えば、$\frac{I^{\otimes n}}{2^n}$ や $|0^n\rangle$ などはエンタングルメントもマクロ量子コヒーレンスもありません。逆に、ρ が「ものすごく量子性のある」状態の場合、C は最大値 C_{max} をとるべきです。つまり $C(\rho)=C_{max}$ となります。例えば、猫状態 $|0^n\rangle+|1^n\rangle$ はマクロ量子コヒーレンスがある状態といってよいでしょう。また、二つの状態 ρ と σ を確率 p と $1-p$ で古典混合しても、「量子性」は増えないはずなので、

$$C(p\rho+(1-p)\sigma)\le pC(\rho)+(1-p)C(\sigma)$$

が成り立つべきです。さらに、状態 ρ に $|0\rangle\langle 0|$ をくっつけても「量子性」は増えないはずなので、

$$C(\rho\otimes|0\rangle\langle 0|)\le C(\rho)$$

が成り立つべきです。実際、これまで提案されている多くのエンタングルメントやマクロ量子コヒーレンスの尺度についてはこれらが満たされています。（むしろ、満たされていないものは不適切な尺度ということです。）

さて、BQP に入っているある言語 L を考えましょう。L を解く回路は $U=V_TV_{T-1}...V_1$ とし、$\rho_t=V_t...V_1|0^n\rangle\langle 0^n|V_1^\dagger...V_t^\dagger$ とします。つまり、計算における t ステップ目の状態は ρ_t です。この時、まず、

$$|0^n\rangle\langle 0^n|\otimes\Big[\frac{1}{poly}|0\rangle\langle 0|+\Big(1-\frac{1}{poly}\Big)|1\rangle\langle 1|\Big]$$

を用意し、ステップ i で、controlled-V_i を作用させるような量子計算を考えると、計算における t ステップ目の状態は

$$\sigma_t = \frac{1}{poly}\rho_t \otimes |0\rangle\langle 0| + \Big(1 - \frac{1}{poly}\Big)|0^n\rangle\langle 0^n| \otimes |1\rangle\langle 1|$$

となります。ところが、

$$\begin{aligned} C(\sigma_t) &\leq \frac{1}{poly}C(\rho_t \otimes |0\rangle\langle 0|) + \Big(1 - \frac{1}{poly}\Big)C(|0^n\rangle\langle 0^n| \otimes |1\rangle\langle 1|) \\ &\leq \frac{C_{max}}{poly} + \Big(1 - \frac{1}{poly}\Big)C_{min} \\ &= C_{min} + O\Big(\frac{1}{poly}\Big) \end{aligned}$$

ですので、σ_t の「量子性」は「小さい」ということになります。つまり、この量子計算においては「量子性」の「大きい」状態は現れません。

しかし、σ_T の一番目と一番最後のキュービットを計算基底で測定し、それらの結果が 00 のときにのみ受理、ということにすると、受理確率は、$x \in L$ の時は $\geq \frac{2}{3\times poly}$、$x \notin L$ の時は $\leq \frac{1}{3\times poly}$ となります。$\frac{2}{3\times poly} - \frac{1}{3\times poly} \geq \frac{1}{poly}$ なので、このような回路でも L が判定できます。