Interactive proof of quantumness: 暗号を使った対話型量子性証明

2020 年 3 月 9 日

ある箱があるとします。ここに入力を入れると何かしらの出力をだしてくれるとします。この箱は量子計算機である、あるいは少なくとも量子的なマシンであるということをどうやったら確認できるでしょうか？

一つの方法はその箱に素因数分解をさせることです。整数を入れて、毎回正しい素因数を返して来たら、素因数分解が正しくできていると考えられます。そして、素因数分解は量子計算機では高速にできるが古典計算機では高速にやる方法は知られていないので、たしかにこの箱は量子的であると確認できます。しかしながら、ショアーのアルゴリズムを実現するのはとても大変であることが知られていますのですぐにはできないでしょう。

もう一つの方法はこの箱にビット列をある確率分布にしたがって吐き出させることです。古典計算量理論で信じられている仮定（多項式階層は崩壊しない）を認めるならば、ある確率分布にしたがってビット列を吐き出すことは量子計算機では高速にできるが、古典計算機では不可能であることが知られています。したがって、その箱がそういう確率分布にしたがってビット列を吐き出していればたしかにその箱は量子的であると保証できます。このようにして量子優位性を示すアプローチはサンプリングと呼ばれています。しかしながら、問題点は、その箱が実際にその正しい確率分布でビット列を吐き出しているのかどうかをチェックする方法が知られていないという点です。さきほどの素因数分解の場合はたまたまチェックが簡単（かければよい）な問題だったので、箱の出力が正しい解かチェックすることができましたが、このサンプリングの場合は正しいサンプリングができているのかどうかをチェックする方法はまだ知られていません。

最近、interactive proof of quantumness というとても面白いアプローチが研究されています [arXiv:1804.00640]。それを理解するために、次のような量子的タスクをする箱を考えてみましょう。まず、箱に関数 f を入力します。f は（古典計算機で）簡単に計算できる 2-to-1 関数とします。さらに、f は trap-door claw-free であるとします。これはどういうものかというと、$f(x_0) = f(x_1) = y$ なる (y, x_0, x_1) を見つけるのはとても難しいけど、ある秘密の鍵を使うと y から $f(x_0) = f(x_1) = y$ なる (x_0, x_1) が簡単に求まる、と

いうものです。さらに、f は adaptive hardcore bit property という性質ももつとします。これはどういうものかというと、$f(x_b) = f(x_{b\oplus 1}) = y$ なる x_b $(b \in \{0,1\})$ と $d \cdot (x_b \oplus x_{b\oplus 1}) = 0$ なる d を同時に求めるのは難しい、というものです。このような関数（厳密にはこれに似た性質をもつもの）は LWE 仮定から作ることができます。

箱は、

$$\sum_x |x\rangle \otimes |f(x)\rangle$$

という量子状態を作ります。そして第二レジスターを測定します。y という値がでたとしましょう。すると、測定後の状態は

$$(|x_0\rangle + |x_1\rangle) \otimes |y\rangle$$

となります。ただし、x_0, x_1 は $f(x_0) = f(x_1) = y$ を満たします。箱は y を吐き出します。次に、$c \in \{0,1\}$ をランダムに選んで箱に入力します。もし $c = 0$ のときは、箱はさらに第一レジスターを測定し、測定値 τ を出力します。もし $f(\tau) = y$ なる τ がちゃんと箱から出力されたら、この箱は量子であると認めます。もし $c = 1$ のときは、箱はアダマールゲートをかけて

$$\sum_d ((-1)^{d\cdot x_0} + (-1)^{d\cdot x_1})|d\rangle$$

を作ります。そして、状態を測定して結果 τ を出力します。もしその出力 τ が $\tau \cdot (x_0 \oplus x_1) = 0$ を満たしていれば、この箱は量子であると認めます。（箱の外の人は秘密鍵を使って、(x_0, x_1) を求めることができるので、チェックは簡単にできます。）

さて、実はこのタスクは古典ではできません。なぜなら、もし、古典でこれができたということは、この箱はまず自ら $c = 0$ を入力して $f(x_b) = y$ なる x_b $(b \in \{0,1\})$ を求めた後に、計算を戻してこんどは $c = 1$ を自ら入力して、$\tau \cdot (x_0 \oplus x_1) = 0$ なる τ を求める、ということができます。しかしこれは adaptive hardcore bit property に反します。（このような巻き戻し操作は rewinding といい、ゼロ知識証明でもでてきます。量子でやる場合、測定で状態が壊れてしまうのでこのような「巻き戻し」はできませんが、古典計算の場合、状態は壊れないので巻き戻しが可能なのです。）以上まとめると、もし箱が量子なら、箱の外の人は箱が量子であることを必ず認めるし、古典的な箱は箱の外の人に量子であることを認めさせることはできません（LWE 仮定が正しい限り）。

実験的に見た時に、この interactive proof of quantumness は実現するのはサンプリングよりは難しいけど、ショアーよりは簡単そうだと言われています。（現在さらにシンプルにする研究が進行中です。）さらに、サンプリングと違って、量子性の検証も可能です。ですから、サンプリングの後、ショアーの前、に実現が目指されるようなものになる可能性はあります。

理論的にも、逆に古典で出来たらもっと強力なことができてしまうので古典ではできない、というロジックで量子優位性を示すこのアイデアはとても面白いです。ちなみに、シャローサーキットの研究においても最近このアイデアが使われています [arxiv:1911.02555]。また、Mahadev の結果はこれをさらに拡張して、量子性の検証だけでなく、任意の量子計算の検証を可能にしたものです。