多項式法

平成 30 年 9 月 30 日

「指数的に爆発するような組み合わせパターンの中から解を探すような問題は、古典計算の場合、全ての組み合わせをしらみつぶしにチェックする必要があるので指数時間かかる。一方で、量子計算の場合、全ての組み合わせを量子力学的重ね合わせで並列処理できるので一発で解ける。」

量子計算の一般向けの記事等で、このような説明が良くなされますが、これは間違いです。たしかに重ね合わせで並列処理はできますが、最後に測定したときに、一つの結果のでる確率は指数的に小さいので、結局指数回計算を繰り返さないといけません。また、これでは、乱数を利用した古典確率的計算と何も変わりません。

量子論では、重ね合わせだけでなく、干渉効果で異なる状態を打ち消すことも可能です。実際、量子的干渉効果をうまく利用して、不必要な状態を打ち消すことにより、古典より高速な計算が実現できる量子アルゴリズムが知られています。しかし、そのようにうまくいくのは問題が良い構造を持っておりそれをたまたまうまく利用できた場合だけであり、一般にはどうやって打ち消していいか全く分からないのが現状です。

特に、しらみつぶしに全てをやらないといけないということは、問題の構造を全く利用できないブラックボックスの状況だということですが、そのような場合、量子計算も指数時間必要であることは、量子計算のかなり初期の段階にすでに数学的に証明されています。

これは、多項式法という非常に美しい方法で証明することができます [1, 2]。多項式法は専門家の間では常識ですが、あまり一般向けには解説が無いようですので、ここでは、そのアイデアを簡単に説明します。

ある関数 $f : \{0,1\}^n \to \{0,1\}$ を考えましょう。これは、組み合わせ x が解なら $f(x) = 1$、解でないなら $f(x) = 0$ を出力します。例えば、夏休みに、東京、京都、大阪、群馬の 4 つの都市のうちいくつかに旅行に行きたいとします。しかし予算は 7 万円しかないので、7 万円以下で行ける組み合わせが解であるとします。「行く」を 1、「行かない」を 0 で表すことにすると、例えば、

- 東京に行かない、
- 京都に行く、

- 大阪に行かない、
- 群馬に行く、

という組み合わせは 0101 のように 4 ビット列で表すことができます。全ての組み合わせの総数は $2^4 = 16$ 個あります。そして、関数 f は

$$f(x) = \begin{cases} 1 & (x \text{ の費用は 7 万円以下}) \\ 0 & (x \text{ の費用は 7 万円より上}) \end{cases}$$

という関数になります。例えば上の組み合わせ、0101、の費用は 7 万円以下なので、$f(0101) = 1$ となります。

さて、「$f(x) = 1$ なる x が少なくとも一つ存在するか、あるいは全く存在しないか？」という問題を考えましょう。これは上記の例でいうと、7 万円以下の費用ですむ旅行の組み合わせが少なくとも一つ存在するか？ということになります。

今、関数 f についての構造は全く分かっておらず、単にブラックボックスとしてしか使えないとします。つまり、x を入れると $f(x)$ を吐き出すようなブラックボックスがあり、その中身がどう動作するかについては全く分からないとします。上記の例でいうと、単に、行きたい都市の組み合わせを入れたら費用を出してくれるようなアプリ（ジョ○ダンとか）を機械的に使うことしかできない、という状況を考えていることになります。日本に長く住んでいる人であれば、普通は、4 つの都市の互いの位置関係（例えば東京ー群馬は近く、京都ー大阪は近いが、両者は遠い、とか）とか、国内の電車賃の目安とかいった情報を前提知識としてもっているので、アプリを使う前に、ある程度直観的に検討して、明らかにあり得ない候補はアプリを使うことなく最初から外したり、ある候補の結果から、他の候補の結果をアプリを使うことなく推定したりすることができます。ところが、今は仮に、そういうことが全くできない、という状況を考えるのです。（例えば、日本に到着したばかりの外国人で、日本についての前提知識が全く無い、とか。）しらみつぶしに全て調べないといけない、というのはまさにこういう状況を指すわけです。

ブラックボックスを一回利用することは、

$$O|x, b\rangle = |x, b \oplus f(x)\rangle$$

というユニタリゲート O を作用させることに対応します。ただし、$x \in \{0,1\}^n$、$b \in \{0,1\}$ です。したがって、ブラックボックスを T 回利用する量子計算が最後に 1 を出力する確率は一般に

$$p = \Big\| (|1\rangle\langle 1| \otimes I^{\otimes m-1}) \Big(\prod_{j=1}^{T} (U_j O) \Big) U_0 |0^m\rangle \Big\|^2,$$

と書くことができます。ここで、U_j は任意のユニタリです。

$$O = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes (f(x)X + (1-f(x))I)$$

であることに注意すると、p は $\{f(x)\}_{x\in\{0,1\}^n}$ の、高々次数 $2T$ の多項式になっていることが分かります。

この量子計算が、高い成功確率で、問題を解いてくれるとします。つまり、もし、少なくとも一つ $f(x)=1$ なる x が存在する場合は、$p \geq \frac{2}{3}$ であり、そうでない場合は $p \leq \frac{1}{3}$ となるとします。すると、

$$|OR - p| \leq \frac{1}{3} \tag{1}$$

となります。ここで、

$$OR \equiv 1 - \prod_{x\in\{0,1\}^n} (1-f(x))$$

です。

式 (1) は、多項式 p が関数 OR を「近似している」ことを意味します。OR 関数を近似する多項式の次数は $\sqrt{\frac{2^n}{6}}$ 以上でないといけないことが知られています [3]。一方で、p は高々$2T$ 次の多項式でした。したがって、

$$2T \geq \sqrt{\frac{2^n}{6}}$$

つまり、

$$T \geq \frac{1}{2}\sqrt{\frac{2^n}{6}}$$

でないといけません。したがって、結論として、量子計算はブラックボックスを $\frac{1}{2}\sqrt{\frac{2^n}{6}}$ 回以上呼ばないといけない、ということが分かりました。仮にブラックボックスの処理は 1 ステップでできき、ブラックボックス以外の処理は全く時間がかからないと仮定しても、指数時間必要になってしまいます。

参考文献

[1] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, Quantum lower bounds by polynomials. Journal of the ACM, **48**, 4, 778-797 (2001).

[2] H. Buhrman and R. de Wolf, Complexity measures and decision tree complexity: a survey. Theoretical Computer Science **288**, 21-43 (2002).

[3] N. Nisan and M. Szegedy, On the degree of Boolean functions as real polynomials. Computat. Complex. **4**, 4, 301-313 (1994).