# 数学セミナー

昭和37年4月3日 第3種郵便物認可

1
2022
vol.61_no.1_723
日本評論社

## 計算理論から量子計算理論へ



↑切り絵:Triangle／岡本健太郎（本誌コーナー「今月の表紙の切り絵」に簡単な解説があります.）

# 数学セミナー

1
2022
vol.61_no.1_723
日本評論社

目次

## 特集◎計算理論から量子計算理論へ

[京都賞業績紹介]

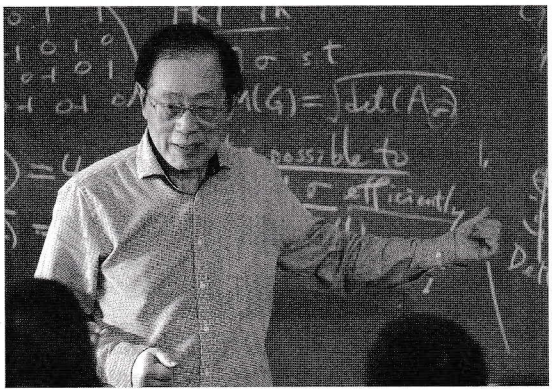
# A.C.ヤオ

## 通信計算量理論：ヤオの卓越した独創の産物

垂井 淳
◉電気通信大学大学院情報理工学研究科

## 1……Andrew Chi-Chih Yao

2021年京都賞を受賞したAndrew Chi-Chih Yao（アンドリュー・チーチー・ヤオ）について説明したい．Yaoは**理論計算機科学者**（theoretical computer scientist）で，**計算量理論**（computational complexity）を主な専門としている．卓越したproblem solverでありつつ，難問を解くプロセスにおいて，**まったく新しい分野・視点・手法を独創的に切り拓く**ということを何度が成し遂げてきた．



アンドリュー・チーチー・ヤオ［写真提供：稲盛財団］

### ◉——1.1 略歴

Yaoは，1946年上海生まれで，1972年物理のPhDをハーバード大学で取得後，1975年コンピュータサイエンスのPhDをイリノイ大学アーバナ・シャンペーン校で取得．その後，マサチューセッツ工科大学，スタンフォード大学，カリフォルニア大学バークレー校，プリンストン大学，中国・清華大学と移っている．1987年ポリヤ賞，1996年クヌース賞，2000年チューリング賞などを受賞している．

### ◉——1.2 エピソード

2021年京都賞は，新型コロナウイルスのため，授賞式などがないのは残念だ．そのかわりにYouTubeにて動画が公開されているようなので，その動画や，より昔のYaoの動画なども眺めてみてほしい．専門については，真面目に丁寧に語る一方で，インフォーマルには非常に率直に話したり，挑発的な話をすることもあって，とにかく興味深い人という印象だ．

「計算量理論の研究者は，全員，P vs NP問題に，少なくとも半年間，全身全霊で取り組むべきだ．そうすれば，何らかの進展は得られるだろう．難しいと怖気づいているのがダメなんだ．」とYaoが言ったという話もある．

プリンストン大学コンピュータサイエンス科のパーティで，各教員のデスクの写真を集めて，大学院生に「誰のデスクでしょう？クイズ」をやったとき，Yaoのデスクだけは全員Yaoのものと当てられたという．彼のデスクにはまったく何も置かれていないのだ．

筆者は共同研究者とともに，Yaoが初期にした研究をほんの少し精密化する研究をしたことがある．それについて，Yaoと話をしていると，彼は，「昔はぬるい結果でもOKだったんだよ，ガハハハハ．」みたいなことを言っていて，面白くて，優しい人だなと思ったことがある．

2010年にYaoがプリンストン大学から清華大学に移るというニュースが伝えられたときは，かなりの衝撃があったと思う．中国の理工系超エリート学

生が集結しているという清華大学生のなかでのベスト・アンド・ブライテストがYaoのもとに集結して育成されるのではないか，などの憶測とともに．

Yaoは，「困難な問題に挑戦し続けるのが好きだ」と言い続けている．有効に利用できると知られていなかった数学分野を独創的に使い始めたことは何度もある．トポロジーのベッチ数を駆使して，代数的計算量の結果を鮮やかに示したこともある．新たな理論を作り上げようというtheory builderという感じよりは，困難な問題を素晴らしく独創的に解いてみせ，「**いったい何をしたんだ？**」と他の研究者が整理していくと大発見がされていた，新理論が出来上がっていた，ということが何度かあったという印象だ．その中でも特筆すべきものを以下で説明したい．

### ◉──1.3　業績

Yaoの仕事は多岐に渡る．Yaoは，計算量理論のもっとも重要な本質・未解決問題に迫ろうという意識が常にある一方で，技術革新により重要となった新分野の研究へと積極的に手を出していく．量子計算について現在に至るまで積極的に研究をし続けていて，また，最近はブロックチェーンの研究もしているようだ．量子計算に関するYaoの仕事は，本号の他の記事で説明されている．

### ◉──1.4　説明したい業績：通信計算量の理論

この記事では，**通信計算量の理論**というYaoが創始した分野に集中して説明したい．これは，1979年の論文[1]でYaoが初めて定式化し，分析・証明手法をゼロから作り上げ，重要な結果を示し，いい未解決問題を具体的に提示し，発展させるべき将来図も示したというものだ．

その後，この分野は，1冊の専門書の対象となり，また，計算量理論の本やコースでとりあげられるものとなった．40年以上経た現在でも活発な研究が続き，計算量理論における未解決問題に対する有力なアプローチとなる可能性もあると考えられている．

要するに，Yao1979論文[1]は，**独創の塊**だったといえる．京都賞や他の賞においても，業績として筆頭に挙げられるものだろうし，Yaoの独創性を示す筆頭例だと思う．

本記事では，欲張って，実際のテクニカルな説明まで踏み込みたい．ただし，おもちゃ的な例の説明が主となる．Yaoが発見した分野がどんな感じのものなのか，また，計算量理論がどんな感じのものなのか，雰囲気だけでも読者に伝えようとしてみたい．

このあと説明する設定すべては基本的に，Yaoが発見し，提示したものだ．分析手法や結果について，細かく，どの部分がどの程度Yao1979論文に既にあったのかは説明しない．こういう**アプローチ・設定・世界・手法・結果**をYaoが発見したということを伝えようとしてみたい．

## 2……通信計算量の導入と定義

### ◉──2.1　ブール関数値決定の通信計算量

AliceとBobが，それぞれ，$n$ビット列$x$と$y$をもっていて，プロトコル$P$にしたがい，1ビットずつ通信しあう．$x=y$かどうか，ふたりともが知ることができれば終わりとなる．最大で何ビット通信する必要があるか？

通信プロトコル$P$は，**完全な非同期**を前提をする．つまり，「1秒待って相手が何も言わなければ，こちらが発信する」ことなどは許されない．

**最初のビットはどちらが送信するのか**，今までの通信履歴と自分のもつ入力をふまえて，**次のビットはどちらが送信するのか**，はすべてプロトコル$P$によって決まっていなければならない．ただし，最初に送信されたビットによって次の送信者が変わるのはかまわない．すなわち，プロトコル$P$は履歴に**適応的**であってもよい．

実世界の問題例としては，離れたサーバにある巨大データとそのバックアップデータが現在同じものとなっているかの検証に必要な通信量を考えてみてもいい．

### ◉—2.2 まるごと送信プロトコル

前節の問題に対するプロトコルの1つは次のものだ．

**プロトコル $Q$** Alice が自分のもつ $n$ ビット列 $x$ をまるごと Bob に送る．受け取った Bob は，$x=y$ が成立するかどうかの答えの1ビットを Alice に送る．

プロトコル $Q$ は，全部で，$n+1$ ビットの通信をしている．Bob は，$x$ を受け取った直後に $x=y$ かどうかがわかるけれど，答えを**ふたりとも**が知る必要があるので，最後の1ビットの通信が行われている．

### ◉—2.3 もっといいプロトコルは存在するのか？

**問い** 2.1節の問題に対するプロトコルで，**通信量**，すなわち，**トータルで通信されるビット数**が $n$ ビット以下のものは存在するか？

ちなみに，このような問いは計算量理論の根本に共通するものとしてある．もっとはやいアルゴリズムは存在するのか？ 限界はどこまでなのか？ 量子計算機は古典計算機より真にはやい計算ができるのか？ 等々．これらの問いを数学的に扱うために，問題のサイズ $n$ をパラメータとし，$n$ が増大したときの計算時間の増え方が多項式的 (poly($n$))，つまり，ある定数 $c$ によって，$n^c$ で抑えられるか？ という話を展開することになる．

Alice から Bob への**一方向の通信**のみができるという設定では，Bob が $x=y$? を決定できるまでに $n$ ビットの送信が必要なのは簡単にわかる．$n$ ビット列 $x$ は全部で $2^n$ 個あり，$n-1$ ビットしか送信されなければ，ある異なるペア $v\neq w$ に対して，Alice の入力が $v$ のときと $w$ のときで，同じ $n-1$ ビット列が送信されてしまい，Bob は $x=y$? の判定が正しくできないためである．これは，より古典的な**シャノンの情報理論**のもっとも単純な例ともいえる．本節の問いでは，**双方向**の**適応的通信**ができることにより，少し非自明になっている．

### ◉—2.4 ベストプロトコルの通信量 = 通信計算量

より一般的には，$2n$ ビット入力，1ビット出力のブール関数 $f_n(x,y):\{0,1\}^n\times\{0,1\}^n\to\{0,1\}$ に対して，$f_n$ の**通信計算量**(= communication complexity)，$\mathrm{cc}(f_n)$ とは，2.1節と同じように，Alice と Bob が $x,y$ を与えられたとき，$f_n(x,y)$ の値を決定するために，入力 $x,y$ については最悪ケースを考えて，**最小限必要な通信ビット数**のこととする．つまり，最悪ケース分析のもとで，ベストプロトコルのトータル通信ビット数を考えている．前節の問いでは，次のブール関数 $\mathrm{EQ}_n(x,y)$ の通信計算量を考えていたことになる：

$$\mathrm{EQ}_n(x,y)=\begin{cases}1 & (x=y\text{ のとき})\\ 0 & (x\neq y\text{ のとき})\end{cases}$$

$n$ ビット列 $x,y$ に対して，$\mathrm{Parity}_{2n}(x,y)$ を次のように定義する：ビット列 $x$ と $y$ に含まれる1の総数が奇数のとき，$\mathrm{Parity}_{2n}(x,y)=1$；偶数のとき，$\mathrm{Parity}_{2n}(x,y)=0$.

**命題1** $\mathrm{cc}(\mathrm{Parity}_{2n})=2$.

Alice が Bob に，$x$ に含まれる1の数の偶奇を1ビット送信し，Bob が答えの1ビットを返すという2ビット通信プロトコルによって計算することができ，また，1ビットだけの通信では両方が答えを知るのは不可能であることが簡単にわかり，命題1がわかる．

$\mathrm{EQ}_n$ については，次が成立する．つまり，上記のまるごと送信プロトコル $Q$ の通信量は最小である．

**命題2** $\mathrm{cc}(\mathrm{EQ}_n)=n+1$.

## 3……通信計算量における下界，単色長方形，ログランク予想

命題2の主張のうち，$\mathrm{cc}(\mathrm{EQ}_n)\geqq n+1$ はどうや

って示せるのだろうか？ イメージしやすいように $n=3$ としよう．つまり，Alice, Bob それぞれが3ビット列 $x, y$ を与えられていて，$\mathrm{EQ}_3(x,y)$ を決めたい．

3ビット列は全部で $2^3=8$ 個ある．Alice の $x=\langle x_1, x_2, x_3\rangle$ によって，8行が000から111までにインデックスされ，Bob の $y$ によって8列が同様にインデックスされた8×8正方行列を $M$ としよう．$M(x,y)=\mathrm{EQ}_3(x,y)$ とする．$M$ の各要素は0か1であり，1は対角線にのみ現れる．つまり，$M=\mathrm{Id}_8$ である．

### ◉── 3.1 通信プロトコル＝単色長方形への分割，命題2の下界の証明スケッチ

通信プロトコルは何をしているのだろうか？ 最初の1ビットを Alice が送信する場合は，Alice 側の8行の集合 $R$ に対して，ある分割 $R=R_0\cup R_1$ $(R_0\cap R_1=\emptyset)$ が事前に決められていて，Alice は自分のもつ $x$ が $R_0, R_1$ のどちらに属するかを1ビットで伝えているとみなせる．このあと，さらに Alice が次の1ビットを送信する場合は，さらなる $R_i$ の分割に対応し，Bob が次の1ビットを送信する場合は，列集合の分割に対応する．

一般的に，プロトコルが進行していった任意の時点で，Alice と Bob は，ふたりのもつ $(x,y)$ が行列 $M$ の**どの部分長方形 $S$ 内のペアなのか**がわかっている．ここで，長方形 $S$ とは，幾何的なものではなく，行集合 $R$ のある部分集合 $R'$ と列集合 $C$ のある部分集合 $C'$ について，$S=R'\times C'$ と表せる**組合せ論的長方形**のことである．

プロトコルは，この組合せ論的長方形が**単色**になったとき，すなわち，**内部のすべての要素が0または1となった**ときに，終了となる．そうなれば，相手の行，相手の列がスバリ特定できなくても，決めたいブール関数値は0/1と決められる．

つまり，任意のブール関数 $f(x,y)$ について，**$\mathrm{cc}(f)$ は，$f$ に対応する $2^n\times 2^n$ の0/1正方行列 $M_f$ について，行と列を，すべての部分が単色になるまで分割していくのに最小限必要な分割回数に等しい．**

行列 $M$ について，$\mathrm{rank}(M)$ は，線形独立な行の最大個数であり，同時に，線形独立な列の最大個数でもある．したがって，行または列を分割して，行列 $M$ を2つの $M_1, M_2$ にカットしたとき，少なくとも一方の $M_i$ について，$\mathrm{rank}(M_i)\geqq \mathrm{rank}(M)/2$ となり，ランクは半分以上となる．一方で，要素すべてが1/0の行列のランクは，それぞれ1と0である．

$\mathrm{EQ}_n$ に対応する $2^n\times 2^n$ 行列は，ランク $2^n$ で，それをたかだか半分にまで減らし続けて，単色部分へとカットするには $n+1$ 回のカットが必要なので，命題2の下界がわかる．（最後のカットにより，オール0とオール1に分かれるので，最後のカット直前でランク1まで落ちている必要があるため，$n+1$ 回必要である．）

### ◉── 3.2 ログランク下界，ログランク予想

以上の議論は，任意のブール関数 $f(x,y)$ とその $f$ に対応する正方行列 $M_f$ に関して，そのまま成立する：

**命題3** $\mathrm{cc}(f)\geqq \log_2 \mathrm{rank}(M_f)$.

この話だけだと飛躍しすぎと感じられるかもしれないが，命題3の右辺の「ログランク」による下界は，任意の $f$ に対して，$\mathrm{cc}(f)$ を多項式的に決定する**上界でもある**という**ログランク予想**があり，現在未解決である．

**ログランク予想** $\mathrm{cc}(f)\leqq \mathrm{poly}(\log \mathrm{rank}(M_f))$.

## 4……回路の最小深さ＝並列時間計算量

$n$ ビットブール関数 $f(x_1,\cdots,x_n):\{0,1\}^n\to\{0,1\}$ に対して，計算モデルとして論理回路を考えよう．論理回路は，2ビット入力，1ビット出力の AND ゲートと OR ゲートからなるものとする．

回路のいちばん「上」のゲートの1ビット出力が回路全体の出力で，回路の入力は，いちばん「下」

に，$x_1, \overline{x_1}, x_2, \overline{x_2}, \cdots, x_n, \overline{x_n}$ という**リテラル**としてあるとする．ここで，$\overline{x_i}$ は，ビット $x_i$ の論理的否定(NOT)である($x_i = 0$ のとき $\overline{x_i} = 1$ で，$x_i = 1$ のとき $\overline{x_i} = 0$)．回路において，**否定はリテラルとしてのみ出現できる**とする．回路の**深さ**とは，**出力ゲートから入力リテラルまでのパスの長さの最大値**のことである．ブール関数 $f$ を計算する回路の深さをどこまで浅くできるかを考えたい．すなわち，次のように定義される $\mathrm{depth}(f)$ を考えたい．

$\mathrm{depth}(f)$ = $f$ を計算する回路の深さの最小値

回路において，同一の深さにあるゲートの値を並列に計算できるとした場合に，$\mathrm{depth}(f)$ は，出力値を決定するステップ数に対応するので，ブール関数 $f$ の**並列時間計算量**である．出力値が $n$ ビットすべてに依存するブール関数 $f$ を計算するためには，回路において，出力ゲートから $n$ 個の入力すべてへのパスがないといけないので，$\mathrm{depth}(f) \geqq \log_2 n$ となる．

**本質的に逐次的な計算が必要**で，$O(\log n)$ 深さの回路では**計算不可能**なブール関数が存在すると強く予想されているのにも関わらず，明示的関数に対して，この予想は現在未解決である．予想はいくつかのバージョンがあるが(すべて未解決)，たとえば，次のものがある．次は，多項式時間で計算可能な問題すべてが，並列計算で $O(\log n)$ 時間で計算できることはない，という当然と思われることを言っている．

**$\mathbf{P \neq NC^1}$ 予想**　$P \neq NC^1$.

並列計算で $O(\log n)$ 時間で計算できるならば，記憶容量として $O(\log n)$ ビットだけで計算できるので，多項式時間計算可能な問題のなかに，非常に小さな記憶容量では計算できないものがある，というこれまた当然と思われる予想より，$P \neq NC^1$ 予想は弱いものである．現在の計算量理論では，まだこんなことも未解決という例ともいえる．この深さに対する非自明な，$\omega(\log n)$ 下界を示すことは，$P \neq NP$ 予想などの大未解決問題にくらべると困難さが少ないようにも思われるのに，現在手がかりもない状態である．

## 5……Karchmer-Wigdersonゲームの通信計算量

### ◉── 5.1　Karchmer-Wigderson ゲーム

$f : \{0,1\}^n \to \{0,1\}$ を任意のブール関数とし，$x, y \in \{0,1\}^n$ を $f(x) = 0$，$f(y) = 1$ を満たす任意のビット列とする．$f$ の値が異なるので，$x, y$ は異なる $n$ ビット列であり，$x_i \neq y_i$ を満たす $i \in \{1, \cdots, n\}$ が存在する．

Alice, Bob それぞれが $x, y$ を与えられ，ビットの通信によって，そのような $i$ を見つけるという通信問題を考える．そのような $i$ が複数ある場合は，どれか1つだけ見つければ良いが，ふたりは同じ $i$ を共通認識しなければいけない．このような問題は，Karchmer-Wigderson ゲームと呼ばれ，Alice が Bob に $x$ をまるごと送り，Bob が $x_i \neq y_i$ を満たす $i$ のビット表現を送るという $n + \log_2 n$ ビットプロトコルで解くこともできる．しかし，$f$ の値が異なるという条件を用いて，より少ない通信量で解ける可能性がある．

### ◉── 5.2　Karchmer-Wigderson ゲームの通信情報量と回路最小深さの関係

ブール関数 $f$ に対して，以上の問題を解くのに最小限必要な通信ビット数を KW-cc($f$) とする．つまり，KW-cc($f$) =「$f$ に関する上記の通信問題の通信計算量」とすると，4節の回路最小深さについて，次の等式が成立する．証明は難しくない．

**定理**(Karchmer-Wigderson[2])

$\mathrm{depth}(f) = \text{KW-cc}(f)$.

この定理による $\mathrm{depth}(f)$ の特徴づけをふまえると，KW-cc($f$) に対しての下界が証明できれば，$\mathrm{depth}(f)$ に対する下界も得られることになる．回

路の最小深さを分析することとプロトコルの最小通信量を分析することは，一般には，どちらも難しく未解決ではあるのだが，切り口が異なる．プロトコル通信量の分析は，回路を出力側から入力側へと「トップダウン」で分析しようという方向となる．

実際に，Karchmer と Wigderson は，回路が**単調**な場合，すなわち，**否定ゲートを含まない**場合について，プロトコル分析により，上述の $\mathrm{P} \neq \mathrm{NC}^1$ 予想の**単調な場合バージョン**の証明に成功した[2]．

彼らのこの結果により，単調とは限らない一般の場合に対する上述の $\mathrm{P} \neq \mathrm{NC}^1$ 予想が通信計算量理論の展開により解決できるのではないかという希望的観測が盛り上がり，非常に活発に研究された．しかし，彼らの結果がでて 30 年以上経過したが，$\mathrm{P} \neq \mathrm{NC}^1$ 予想は未解決のままである．

**参考文献**


[1] Andrew Chi-Chih Yao: Some Complexity Questions Related to Distributive Computing, In: *Proceedings of ACM Symposium on Theory of Computing*, 209-213, 1979.

[2] M. Karchmer and A. Wigderson: Monotone Circuits for Connectivity Require Super-Logarithmic Depth, *SIAM Journal on Discrete Mathematics*, **3**(2), 255-265, 1990.


［たるい じゅん］