題名	コンピュータ科学の世界を旅して
Title	A Journey Through Computer Science
著者名	アンドリュー・チーチー・ヤオ
Author(s)	Andrew Chi-Chih Yao
言語	日本語
行事名	第 36 回(2021)京都賞記念講演
出版者	公益財団法人 稲盛財団
発行日	2022 年 10 月 1 日
開始ページ	1 ページ
終了ページ	7 ページ
URL	https://www.kyotoprize.org/wp-content/uploads/2022/10/2021_yao_jp.pdf

英語版テキストURL：https://www.kyotoprize.org/wp-content/uploads/2022/10/2021_yao_en.pdf

第 36 回(2021)京都賞記念講演
アンドリュー・チーチー・ヤオ

コンピュータ科学の世界を旅して

皆様、この場にいることを大変嬉しく思います。

まず初めに、京都賞を受賞できたことは、私にとってこの上ない栄誉です。歴代の受賞者の方々の輝かしい業績を知るだけに、その仲間入りをするに相応しいとお考えいただいたことに、深く身が引き締まる思いです。本日この場でお話しできることは、私にとって大きな喜びであり、大変な名誉です。

私の身の上とコンピュータ科学との出会い、またその道のりについてお話しさせていただきたいと思います。具体的には、私の生い立ちから始めて、若い頃に物理学に魅了され、物理学者を最初の職業としながらも、なぜ後に分野を変えてコンピュータ科学者になったのかを、まずお話しします。その後、私の研究の概要、特に、私が考えている問題と興味を抱いている理由をお伝えしたいと思います。最後に、私の人生と仕事に大きな影響を与えてくださった方々にお礼を述べて締めくくらせていただきます。

私は1946年に中国の上海で生まれました。その後、間もなくして香港にそれから台湾へと家族で引っ越しました。愛情深い両親と、大変仲の良い二人の兄弟がいる中産階級の幸せな家庭で、私は、文化と勉学を特に大切にする伝統的な中国の価値観の下で育ちました。幸い、両親も喜んだことに、学校での成績は優秀でオールAでした。子供の頃は数学、科学、歴史が好きだったのを覚えています。例えば、並外れた勇気と知恵のある歴史上の人物に魅せられました。同様に、ガリレオやニュートンのような偉大な科学者も私にとってはヒーローでした。彼らの才能と、自分が信じるもののために立ち上がる勇気、その素晴らしさに畏敬の念を抱きました。そして、いつか私も同じような運命をたどることを夢見ていました。

1. 物理学に魅せられた若い頃

高校3年生のとき、相対性理論に関するエディントン卿が著したものを偶然見つけました。そこには相対性の単純明快な導出が示されており、論旨は次のようなものでした。私たちは、光の速度は一定であることを実験的に知っています。この事実から、巧みな説明で導き出すことができるのは、私たちが慣れている時間の概念が絶対的な普遍的概念ではないということです。誰もが長い間当然のように思っていた時間の概念が、です。私はこの説明に深い感銘を受けました。物理学は探偵小説のように読むことができ、シャーロック・ホームズのどの巧妙なエピソードよりも想像力に富んでいます。私は大いに感銘を受け、勇気づけられました。

1963年、私は大学に入り物理学を専攻しました。その後間もなく、ファインマンの物理学に関する講義録が出版されました。言い伝えによると、当時、カリフォルニア工科大学は物理学の新入生コースを根本から再構成したいと考えており、ファインマンは一度限りという条件で講師を引き受けたようです。これが伝説的な3巻構成の書物『ファインマン物理学』にまとめられたのです。

私はこの本を読み、目からうろこが落ちました。説明が難しい高度な概念が、初歩的な数学だけで説明でき、導き出せることがわかりました。物理学の奥深さと美しさを知り、深く感動しました。実際にこの時初めて、量子力学の原理を本当の意味で理解したと感じました。その30年後に、私は量子計算に取り組むことになるのですが、ファインマンの量子現象に関する説明は、今でも私にとって最も明快で役立つ説明だと思います。この一件により、私は大学卒業後に物理学を学ぼうと決心しました。

1967年に大学を卒業し、兵役を1年務めた後、ハーバード大学の大学院で物理学を学びました。そして1972年に、シェルドン・グラショー教授のもとで物理学の博士号を取得しました。これで私は本物の物理学者としてのスタートを切ったのです。

2. 物理学からコンピュータ科学へ

しかし、それも長くは続きませんでした。1973年に、当時MITの博士課程の学生だった妻のフランシスが、私にアルゴリズムを紹介してくれました。当時、アルゴリズムという言葉は今日とは異なり、ほとんどの人にとって馴染みのないものでしたが、今では日常的に使われています。ドナルド・クヌース教授の著した『The Art of Computer Programming』(コンピュータ・プログラミング技法)第3巻はアルゴリズムに関するものでしたが、読者は限られていました。実に素晴らしい名著でした。魅力的な新しい科学を紹介する内容でした。読んでから、本の中で提起された研究課題について寝ても覚めても考えていました。

それが頭から離れず、間もなくして物理学のポスドクの仕事を辞めて、コンピュータ科学の大学院に再度入学することにしました。母には私が長年にわたる物理学の研究をあきらめたように見え、とても心配していたことを覚えています。しかし、私の妻が全面的に支援してくれたこともあり、私はイリノイ大学のコンピュータ科学の大学院生になりました。私を快く受け入れてくれたC・L・リュウ教授に感謝しています。

3. 研究概観

それでは、私の研究について少しお話ししたいと思います。最初は、最小全域木やB木など、それまで未解決のアルゴリズムの問題に取り組んでいました。しかし、卒業後しばらくしてから、コンピュータ科学の新しい枠組みと新しい理論の開発に興味をもち始めました。その後数十年にわたって、トップクラスの大学に勤める機会に恵まれ、カリフォルニア大学バークレー校とスタンフォード大学で10年間、プリンストン大学で18年間を過ごし、2004年には現在在籍している清華大学に移りました。

それぞれの時期に私は多少異なることに従事していましたが、興味深いことに、これらの時期に私が焦点をあてたテーマは時代の変化や学問としてのコンピュータ科学の発展、そして私が関わった大学の環境に大きく関係していました。

ここで、三つのテーマを取り上げます。ミニマックス複雑度(通称「ヤオの最小最大原理」)、通信複雑度、そして暗号理論およびマルチパーティ計算(Multi-Party secure Computation、MPC)です。

私が考える最も優れた研究方法は、洞察力のある、大胆な問いを見つけることです。良い問いが見つかれば必ず良い研究ができ、研究の世界に応用できる重要な結果を見つけることができます。ここで、テーマごとに私を発見に導いた複数の問いと、それらがなぜ重要であるのかを説明したいと思います。

3.1 ミニマックス複雑度

一つ目は1977年のミニマックス複雑度で、これは私にとって特別な思い入れのあるテーマです。というのも、これは私が自分で問いを立て、それに対処する良い方法を見つけた最初の重要な機会だったからです。

そして今、アルゴリズムは本質的に、料理のレシピと同じものであることがわかってきました。例えば、3オンスの塩と数グラムの肉を順次入れるといった具合です。

1970年代半ばに、乱択アルゴリズムと呼ばれる新しいスタイルのアルゴリズムが人々の注目を集めました。この新しいタイプのアルゴリズムには、確率論的な要素が組み込まれています。料理に例えると、スプーン2杯の塩を入れるという明確な手順でなく、コインを投げてスプーン2杯の塩を入れるか1カップの赤ワインを入れるかを決めて、調理を進めるというものです。従来の考え方では、これは物事を行う上で突拍子もない方法に見えますが、1970年代に人々は実際にこのようなアルゴリズムを提案し、実行することに利点があることを示し、いくつかのケースで素晴らしい結果を得ました。

しかしここで人々が分析し、理解できなかった問題は、このアルゴリズムの限界がどこにあるのかということでした。そこで私は、どちらが優れているのかを自問自答しました。つまり、提案された乱択アルゴリズムの方がよいのか、あるいは平均的なケースのときの挙動を見るような、データの分布を見てよいアルゴリズムを選ぶというような従来のアプローチの方がよいのか、自問自答したので

す。このような形で問題を捉えると、乱択アルゴリズムについての多くの洞察を与える素晴らしいつながりが見えてきます。

乱択のアプローチと従来の分布型アプローチを比較すると、これは乱択アルゴリズムとデータの間で行われるゲームと見なすことができます(Fig. 1)。一方のプレーヤーであるアルゴリズムは確率的に動く方法を選択しますが、もう片方のプレーヤーであるデータはより計算コストがかかる方法を選択します。

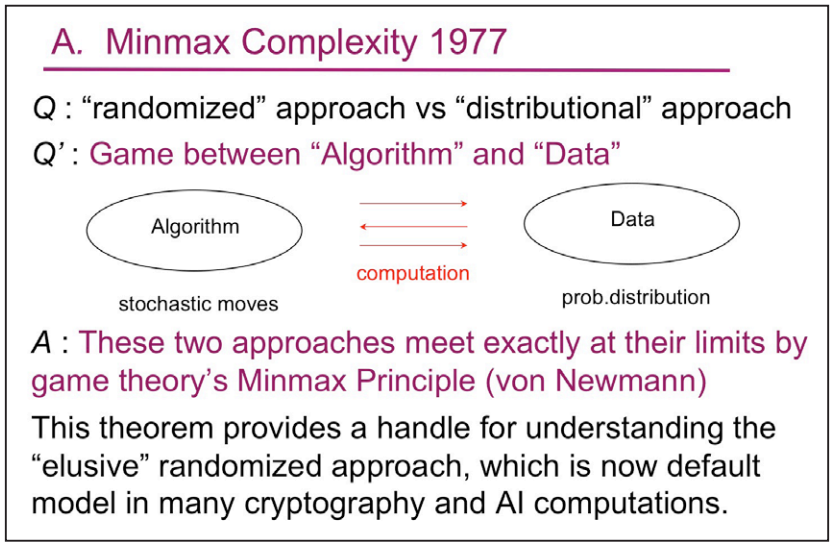

Fig. 1

これら二つのアプローチは、フォン・ノイマンのゲーム理論におけるミニマックス定理により、その限界で正確に一致します。したがってこの結びつきは、私たちが証明したい定理、すなわち、これら二つのアプローチが同じであるという定理を与え、さらに乱択のアプローチをさらに理解する手段を提供することになります。

重要なことは、当時のこれらの新しいタイプのアルゴリズムは、現在多くの暗号化およびAIアルゴリズムの標準的なモデルになり、乱択アルゴリズムの限界を理解したいと人々は望んでいるということです。そのため40年以上もの間、現在も、私が見つけたアルゴリズムは多くの研究者によって問題解決のためにたびたび使用されています。

3.2 通信複雑度

二つ目のテーマは、私が1979年に提起した通信複雑度です。まず、数学的な問いを立てることから始めましょう。アリスとボブの二人は別々の場所にいます。彼らはそれぞれxとyのデータをもっています。それらはnビットの整数です。

そして、解決したい問題を、二人である量Fを計算することだと仮定します(Fig. 2)。彼らの間で何ビットを通信する必要があるでしょうか。この問題は現在、この関数についての通信複雑度と呼ばれています。

これはもちろん、計算する関数に依存します。たとえば、二つの整数の合計が奇数か偶数かを計算するには、2ビットの通信のみで十分であることは明らかです。つまり、彼らがお互いに偶数か奇数かを伝えるだけで、答えを決定できます。一方、xがyより大きいかどうかを計算したい場合は、問題を解決するために、基本的に一方から他方にそのストリーム全体を送信する自然なアルゴリズムを利用し、確認することになります。

さらに深く立ち入ると、この問題の解決のためには、このような単純な方法で行うよりも良い方法はないということに気づき、証明する必要があります。一般的に、これは非常に難しい問題です。特定の計算Fを与えると、その計算には通常、深い数学的分析が必要になります。

ここで、この問題を検討する理由は、1970年代後半に、それ以前は誰もが慣れ親しんでいた大型汎用コンピュータからコンピューティングのパラダイムが変化し、徐々に私たちが現在目にするネットワークコンピューティングに移行していることが明らかになったためです。つまり、人々は分散システムで問題を解決することに興味があり、多くの人々が共同で問題を解決したいと望んでいるからです。つまり、このことは、それまでコンピューティングに関して使用していたモデルを、ネットワークモデルによるコンピューティングに調整する必要があることを意味します。

この新しい世界では、通信コストがしばしば高くなります。データの通信が必ず伴い、それが最もコストがかかる部分です。したがって、先ほど説明した通信複雑度の概念は、このパラダイムの変化をモデル化して、新たなパラダイムに反映させたものなのです。このモデルが提案、研究されて以来、通信複雑度は、チップの設計からデータストリーミングに至るまでの幅広い用途が見つかっています。

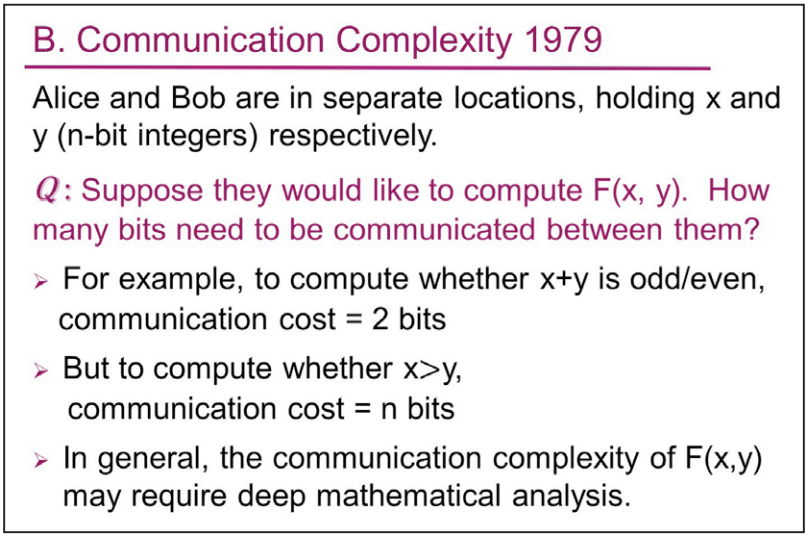

Fig. 2

3.3 MPCおよびミリオネア問題

さて、最後に詳細に説明するテーマは、暗号理論とMPCについてです。1982年に私は三つの論文を執筆し、これが現代の暗号理論に大きく貢献しています。この三つの論文は、ドレフ-ヤオのセキュリティモデル、疑似乱数の生成、および安全なMPCに関するものです。ここでは、最後のMPCについて説明します。

MPCは、暗号化されたデータを計算できる暗号の概念です。MPCを使用すれば、複数のデータベースで自身のデータを開示せずに協調計算できます。つまり、基本的にデータを見なくてもデータを共有できるのです。

とっておきの例を説明させていただければ、わかりやすくなると思います。論文でも取り上げたよく知られたミリオネア問題(Millionaires' Problem)を例として使います。二人の富豪アリスとボブは、自分たちの数値情報を明らかにすることなく、どちらがよりお金持ちであるかを把握したいと思いました(Fig. 3)。つまり、アリスにはx百万ドル、ボブにはy百万ドルがあり、数学的な問題は、xがyより小さいかを判断するために互いに話し合いたいというものです。要は、最終的にアリスとボブは二人ともどちらがお金持ちであるかの答えを得ますが、互いの情報は知らずに会話ができるか否かという問題です。

単純かつ直感的に、それは不可能だと思うのではないでしょうか。どちらの当事者も情報を明かさずに、どちらがよりお金持ちであるかを知るにはどうすればよいでしょうか。少し考えると、1982年の標準的なセキュリティの定義、つまりシャノンの情報理論を使用すると、それが不可能であることがわかります。

しかし、必要は発明の母です。必要に駆られた時、人は方法を考え出すものです。既成概念に囚われない考え方をすると、実際にそれが可能になります。つまり、ここで言う既成概念に囚われない考え方とは、シャノンの構築した理論に基づく非常に厳格で強固な考え方を捨てるべきだということです。そしてここに、アラン・チューリングを登場させます。これについてはあまり多くは述べませんが、基本的には、セキュリティの定義を緩和しても実用的に非常に優れた定義であれば実現可能であることがわかりました。

特に現在、秘匿回路(garbled circuit)と呼ばれているものでは、これが実現でき、使用できることが示されました。そして約40年の間でハードウェアとアルゴリズムが進歩し、現在ではほぼ実現可能になっています。この点に関しては多くの研究が行われており、金融工学、データ流通、および共同創薬での分野で準備が整いつつあります。

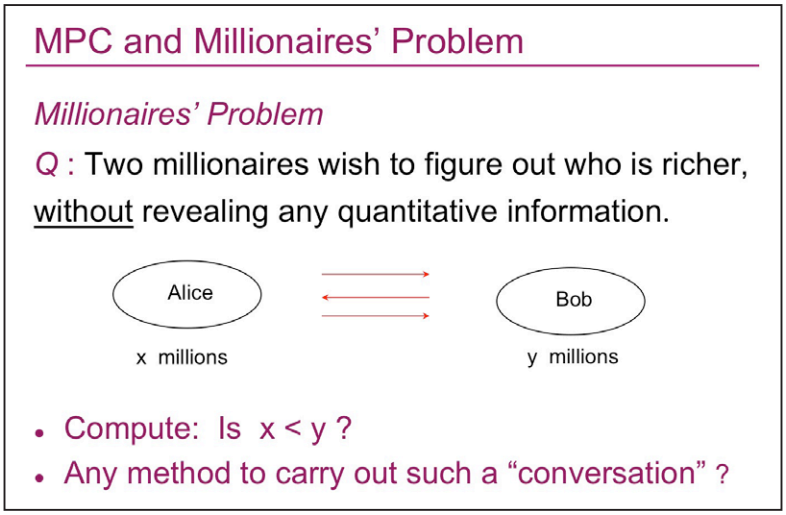

Fig. 3

3.4 その他の研究テーマとまとめ

私は現在、他のテーマにも取り組んでいます。詳細には説明しませんが、ここで列挙しておきます。量子計算は、有望な指数関数的な高速化を含む革新的なアプローチです。オークション理論は、ゲーム理論のフレームワークにおいて、とらえどころのない経済的問題を取り扱います。人工知能は、AlphaGoのような機械学習アルゴリズムによって成し遂げられた驚くべき偉業を目の当たりにしますが、その成功の理由はまだ謎に包まれています。すべて非常に興味深い新しい分野ですが、まだ発展途上です。

ご覧のとおり、私は多くの、そしてさまざまなテーマに取り組んできました。そして、これらの多様で多彩なテーマは、実際には私自身の個人的な好みを反映しているだけでなく、半世紀かけて花開いた情報科学の成果と今日目にする学際的な繋がりの発展を反映しているのです。

4. インスピレーションを与えてくれた二人のメンター

最後に、私が出会った人々について少し触れたいと思います。コンピュータ科学者として長年活動する中で、並外れた才能を持つ多くの人々と出会う幸運に恵まれました。インスピレーションを与えてくれる二人のメンターがいたことは、特に幸運でした。グラショー教授とクヌース教授です。

グラショー教授は、私のハーバード大学での物理学博士課程の指導教員でした(Fig. 4)。彼は、チャームクォークと呼ばれる新しい粒子が存在することを最初に予測した人々の内の一人であり、一番熱心な提唱者でもありました。

私はグラショー教授から、科学には大胆さが必要であり、自分の信じるものを貫かなければならないということを学びました。そして、彼から学んだもう一つのことは、数学は物理学とは異なるということです。

物理学者は、数学的議論の正確性に固執するのではなく、物理的な実状に基づいて正解を見つけることが最も重要です。この実践的な精神は、その後の私の研究に大いに役立ったと思います。

グラショー教授からは、他にも重要な事を学びました。人生を楽しむということです。1971年の春、若い学生だった私は、教授がフランスのマルセイユにあるCNRS（フランス国立科学研究センター)に短期滞在した折に同行しました。マルセイユは素晴らしく魅力的な街でした。また、それが私にとってはじめてのヨーロッパでした。そして夏の終わりに、彼は私をイタリアのシチリア島でのサマースクールにも連れて行ってくれました。これも素晴らしい経験でした。グラショー教授が私に指し示した非常に重要な教えは、人生の楽しみと知的探求は密接に関係しているということです。

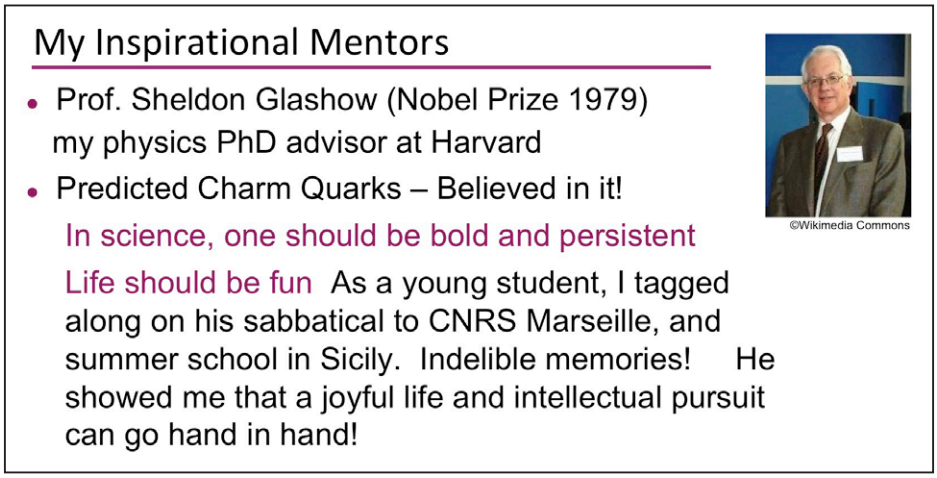

Fig. 4

次に、クヌース教授についてお話ししたいと思います(Fig. 5)。先に述べたように、彼の著書『The Art of Computer Programming』(コンピュータ・プログラミング技法)を読んだとき、私の人生は大きく変わりました。

この名著で、クヌース教授は文字通り新しい研究分野を創生し、何世代にも渡る新たなコンピュータ科学者に影響を与えました。例えば、私は彼の本を読んだことでコンピュータ科学のキャリアをスタートさせ、彼が巧妙に定式化した問題をいくつか解きました。

後にスタンフォード大学で彼の同僚になれたことは幸運でした。クヌース教授は、数学やコンピュータ科学以外にも多彩な才能の持ち主として知られています。彼は熟練のパイプオルガン奏者であり、作曲家、小説家でもあり、他にもまだまだあります。このように彼は非常に多才ですが、それでいて誠実で寛大であり、常に人の長所に目を向けています。

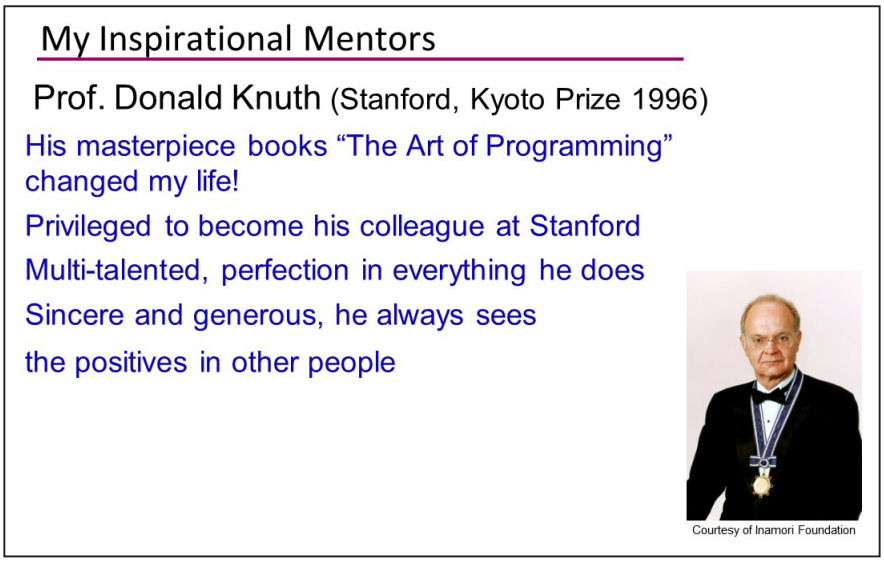

Fig. 5

5. 最後に

結果として、私は紆余曲折を経ながらも、コンピュータ科学の分野で素晴らしい旅をしてきました。

そして、違った分野から出発することも、不利に働くとは限らないことを見出したのです。実際に、物理学の初期に培った事は、少なくとも二つの点で役に立ちました。一つ目は、優れた理論がどのようなものなのかを学んだことです。物理学には、相対性理論や量子力学など、優れた理論のパラダイムが多く存在します。これは、コンピュータ科学の理論を構築するとき、私の助けになりました。そして、私が物理学から受けた恩恵の二つ目は、その実利的な精神です。重要なのは、目の前にある特定の問題を解決したいという信念です。方法は問題ではありません。最終的に問題が解決できるなら、どんなものでも利用するなり、習得するなり、新たに生み出すなりすべきなのです。

科学においてパラダイムとは、真実を探求することです。その過程で、人の精神を高めることができるパターンや美しさを発見することがあります。それは人の心を豊かにし、人類が将来の課題に備えるイノベーションにもつながります。私は、科学と人間性が協調して人類の進歩に貢献するという稲盛財団のビジョンに、大いに賛同します。

繰り返しになりますが、京都賞を受賞することができ、この講演で私の経験をみなさまと共有できたことは大変光栄です。

どうもありがとうございました。