数学の新展開　―伝統的理論と新しい応用の架け橋―

ラースロー・ロヴァース

今回、京都賞の受賞者に選ばれましたことは、この上ない名誉であり喜びであります。科学の分野で過去に受賞された錚々たる先達のお名前を見るにつけて、私自身戸惑いの念を禁じえないのと同時に、今でも自分がそうした方々のお仲間に入れていただいたことが信じられません。また、本日は研究者として私がこれまで歩んできた道程、そしてこれまで私を魅了してやまなかった数学という学問の発展について私の考えを皆様にお話しする機会をいただき、深く感謝いたします。

１．　家族

私はブダペストで育ちました（Fig. １）。（２００万の人口を擁する）この町は、ハンガリーの中では「大都市」です。子どもの頃は、壊れた建物、弾痕の残る壁など、戦争の傷跡が街のあちこちに残っていました。ドナウ川に架けられた橋も修復されないままのものもいくつかありました。道を行き交う車などは今と比べると遙かに少なく、私たちは道でサッカーをして遊びました。何しろ車が通るのは１０分に一台ほどでしたから。

ブダペストは「鉄のカーテン」の「不幸な側」にありました。（当時８歳だった）１９５６年の革命「ハンガリー動乱」に関しても忘れえない記憶がありますが、振り返って考えると私の子ども時代はそれほど悪いものでもありませんでした。父は外科医で、我が家は、比較的恵まれた暮らしをしていました。二歳下の弟とも一緒によく遊んだことを覚えています（Fig. ２）。

妻のカティとは高校で知り合い、大学の時に学生結婚をしました。私にとって妻は本当の意味で「人生のパートナー」です。彼女も現役の数学者であり、熱心な教育者でもあります。また、彼女は多大な犠牲を払って、色々と私の研究の後押しをしてくれました。アメリカにも一緒に行ってくれましたし、家の面倒なことを引き受ける一方で、私の著書や論文の校正を手伝ってくれたりもしました。そして、何と言っても彼女は、私の研究者としての計画や目標、そしてその時々で関心を抱いていた問題を最も良く理解してくれました。

私たち夫婦は４人の子どもに恵まれました（Fig. ３）。（今では）孫も５人おり、楽しく暮らしています。私たちの子どもはみんな数学が得意でしたが、３人いる娘は、現在、一番上が文学、他の２人が経済と、別の道を歩んでいます。

唯一、息子だけが大学で数学を学んでいます。

２．　数学研究との出会い

私が研究対象としての数学と出会ったのは高校生の頃に遡ります。父は私に父と同じ医学の道を歩んで欲しいと願っていたと思うのですが、（１４歳になって）初等学校の卒業を間近に控えた頃、校長のベレー先生が私の家まで両親を訪ねて来られました。先生は、数学が得意な子どもたちを集めた専門クラスを新しく作った高校があることを説明され、私をその学校に入れてはどうかと両親に強く勧めてくださいました。「ファゼカシュ」の名前は（今でこそ大変よく知られていますが、）当時は知る人ぞ知る、という存在でした（Fig. ４）。最終的には、両親は校長先生の勧めを受け入れてくれました。今でも、これが私にとって人生最大の転機であったと思います。ファゼカシュではすばらしい先生方だけでなく、（妻を含めて、）優秀な生徒にも数多く出会いました。当時の仲間とは今でも親しく付き合っています。

ハンガリーには、数学に秀でた人材を育てる、という長い伝統があります。１８９４年には、高校生向けの月刊数学雑誌が創刊されています。（この専門誌は今も存在しており、数学の教育に大切な役割を担っています。）また、１８９４年からは、全国的な数学コンクールが開催されています。（ファゼカシュで教える数学は非常に高度でしたが、）私のクラスに数学を教えてくださっていたラバイ先生は、クラスで特に成績が良い生徒には、学校で教わる数学の他にもさらに進んだ教育を受ける機会を与えるべきだ、という考えの持ち主で、大学や研究機関で数学の研究をしている、最も優れた数学者の方々に私たちを紹介してくださいました。（当時のハンガリーでは個人の海外渡航が制限されていることもあって、）そうした諸先輩方も喜んで優秀な高校生に会って指導してくださいました。（この時ばかりは「鉄のカーテン」が味方してくれたようです。）こうして私は、学校での高度な授業に加え、数多くの優秀な数学研究者から多くを学ぶ機会に恵まれたのです。そうして出会った研究者の一人がポール・エルデシュ先生です（Fig. ５左）。皆さんの中にも名前を聞かれたことがある方は大勢いると思いますが、先生は２０世紀最高の数学者の一人であっただけでなく、一風変わった人柄でも知られており、その逸話は枚挙にいとまがありません。先生は、居を定めることを望まれず、（「研究の妨げになる」として）一切の財産も持とうとされませんでした。そして、いつも旅をしておられ、ホテルやゲストルーム、そして数多くの友人の家が先生のねぐらでした。常に大勢の人々に囲まれ、その時に自分が取り組んでいる問題や研究に関するアイデアだけでなく、旅先で仕入れてきた他の学者の研究成果などについて議論しておら

れました。先生は数学に関する新たな研究課題を提起したり、誰も研究に手を付けていない新しい課題を世界中の人々に向かって投げかけたりする術に長けていらっしゃいました。

エルデシュ先生は子どもや若い人たちと話をすることが好きで、私の４年間の在学中にも何度かファゼカシュに来てくださいました。学校では、優秀な高校生なら理解できるレベルの「基本的な」未解決問題を私たちに出されました。とは言っても、簡単でつまらない、ということでもありませんでした。私も一つか二つは解いたと記憶していますが、現在に至る数学者としての私の研究生活はここから始まったのです。

恩師と言えば、もう一人忘れてはならないのがティボル・ガライ先生です(Fig. ５右)。この先生には高校在籍時だけでなく卒業後もお世話になり、学位論文執筆の指導までしていただきました。(当時、学位論文は必ずしも学校で正式に指導教官から指導を受けないといけないということではなかったので、いわばプライベートな指導教官として貴重なアドバイスをいただきました。)人柄はエルデシュ先生とは正反対の、控え目で慎ましい方で、一対一で長時間、静かに議論をすることを好まれました。学生の頃には先生を定期的にお訪ねし、数学、特にグラフ理論とその発展していく方向性に関する先生のお考えを色々と学びました。

ガライ先生に関して特によく覚えているのは、初めての論文を書き上げた時のことです。テーマはかなり複雑なグラフ理論でしたが、先生には執筆にあたって大変お世話になりました。私の未熟なメモをベースに先生が論文を書き上げてくださった、と言っても過言ではありません。そして、いよいよ脱稿という時に、先生は論文の共著者として名前を入れることを固辞されただけでなく、論文の末尾で謝辞を捧げることさえお断りになりました。「教師としてやるべきことをやったまで」、というのが先生のお言葉でした。翻って、こうした人格者としての先生の教えを自分が常に実践することができたかは分かりませんが、とにかく努力だけはしてきたつもりです。

こんな私が、高校卒業後の進路としてブダペストのエトヴェシュ・ロラーンド大学で数学を専攻することを選んだのは、至極当たり前のことでした。大学では良質な教育を受け、ほとんどの数学分野の基礎を学んだだけでなく、数学者としての心構えを教わりました。

３．　グラフについて

数学者として私が最も関心を持ったのは、グラフ理論です。この学問分野の研究対象は、「節点」あるいは「頂点」と呼ばれる要素と、その要素間の関係で

構成される、数学的には非常にシンプルな構造です。頂点同士は隣接、すなわち辺で繋がれているものもあれば、そうでないものもあります。こうした構造をグラフと呼んだりネットワークと呼んだりします。例えば、ある社会における知人関係を描きたい場合は、人物を頂点で表すことができ、二人の人物が知り合いなら二人の頂点を辺で繋ぎます。通常、グラフの頂点は平面上の点、辺は頂点を繋ぐ曲線となります。（この時、辺は曲線でも直線でも構いません。）このような作業を行えば、Fig. ６に示すような図形が得られます。グラフというものは考えうる中でも最もシンプルな構造の一つであり、科学、経済、工学、物流など、幅広い分野で用いられている様々な構造を図式化して表示することやモデリングに欠かせないことは明らかです。

グラフ理論は何も新しい学問という訳ではありません。１７３６年、「ケーニヒスベルクの橋渡り問題」に対して、（史上最も優れた数学者の一人である）オイラーが示した解き方がグラフ理論の始まりとされています。しかし、グラフ理論が数学の分野の一つとして現在のように大きくなり、活発に研究が行われるようになったのは１９６０年代のことです。その後押しをされたのが他ならぬエルデシュ先生でした。先生はシンプルでありながら自明ではなく、知的好奇心を掻き立てるような問題をいくつも提示され、この分野に深みを与え、学問的な成熟をもたらされたのです。

通常、グラフ理論は「離散数学」の一分野に分類されます。ちなみに、この「離散」という言葉、英語では「ディスクリート」と言います。綴りに注意してください。“d-i-s-c-r-e-e-t”と綴ると「プライバシーを尊重する（思慮深い）」という意味になりますが、「離散数学」の「ディスクリート」は“d-i-s-c-r-e-t-e”と綴ります。「離散数学」では、通常は有限個の離散的な対象からなる構造を研究します。（これに対して、例えば実直線は無限個の点が連続的に並んだものと考えられます。）グラフ理論並びにグラフの一般化や抽象化を研究する分野は、離散数学のかなりの部分を占めていますので、本日の話ではこの二つを区別いたしません。

私がグラフ理論に出会い、それを通じて数学者を志すようになったのはかなり若い頃でした。高校時代に仲が良かったクラスメートにラヨシュ・ポーシャという人物がいるのですが、彼は私よりも先にエルデシュ先生から指導を受けていました。先生が出題されたグラフ理論の問題を見事に解いた彼は、高校に上がるまでにエルデシュ先生と共著で研究論文一本をまとめただけでなく、単独でもいくつか論文を書いていました。彼は高校で一緒になった私にエルデシュ先生が出された問題をいくつか見せてくれました。そのうちの一つか二つを私が解いたので、先生に紹介してくれたのです。先生からまだ解かれていない問題をいくつかいただき、その後、自分でもいくつか問題を作るようになりま

した。それ以来、私は生涯をグラフ理論に捧げてきました。

ここで一つ付け加えておかなければならないことがあります。グラフ理論というのは当時の数学界の「主流」からはかけ離れた存在だったので、先輩の数学者の方々からもっと他の重要な研究をやるようにとしばしば忠告を受けました。しかし私はと言えば、この分野の目新しさと応用への可能性の大きさにすっかり魅了されていました。

当時のことを思うと隔世の感がいたします。グラフ理論は数多くの分野で応用が進んだだけでなく、他の数学分野とも結びつきを強め、この数十年間でその重要さを増してきました。ここからはその発展の道筋の一部をお話ししたいと思います。

４．　応用との出会い

４－１．　組合せ最適化

学生として大学にいた最後の数年間、私はオペレーションズ・リサーチとグラフ理論が強い結び付きを持っていることに関心を抱くようになりました。そこで私はガライ先生の指導の下、グラフの因子に関する問題について学位論文を書きました。（現在、この分野は「マッチング」と呼ばれています。）基本となる問いは、「*あるグラフにおいて、二つの頂点が隣接するようにペアを作ることができるか？*」というものです。より一般的な言い方をすれば、「（共通の端点を持たない、すなわち）二つの頂点が互いに素である辺の最大数はいくつか？」となります。二部グラフ（つまり二つに分けられた領域に頂点が置かれ、異なる領域に属する頂点同士をそれぞれの線が繋いでいるグラフ）においては、その答えはケーニッヒによって１９３１年に示されました。それは、「*互いに素である辺の最大数は、すべての辺を被覆する頂点の最小数と等しい*」というものです。また、トゥッテとベルジュは、この説明をすべてのグラフへと展開して一般化しました。その条件は大変美しいものなのですが、ここでお話しするにはいささか複雑すぎますので割愛させていただきます。しかし、この他にもマッチングに関する問題には未だに解が見つかっていないものが数多くあります。（私はいくつかを解き、博士論文を書くことができました。）現在もマッチング理論は、難しいことは難しいが、全く歯が立たないとまでは言えない難度のグラフ理論の問題の有力な供給源となっています。

学位論文の審査が無事に終了して間もなく、私はベルジュの「弱パーフェクトグラフ定理」という問題を解くことに成功したのですが、この解き方はその後興味深い方向へと展開しました。まずは整数計画法に、そして整数計画法を

経て多面体へと繋がっていったのです。その後、このグラフ理論と最適化と幾何学とのつながりは最も実り多いものだと何度も再認識させられました。

この他にもグラフ理論が関係する最適化問題は数多く存在し、例えば「最大フロー問題」や「巡回セールスマン問題」は実用的な問題としても重要であり、また、一般にも広く知られています。これらの問題（それにここでは詳述はしませんがパーフェクトグラフ問題）は、グラフ理論と結びつく以前の最適化問題とは全く異なる最適化問題の例となります。

以前の典型的な最適化問題を分析する際には、「滑らかな（微分可能な）」関数の最小値あるいは最大値を求めます。そして、微分学の重要な応用として、導関数が「０」となる点（f’（x）＝０となる点）を求めることによって解いていくのですが、離散数学における最適化は、これとはまったく異なるアプローチを取ります。そこで扱うような有限ではあるが大きく、複雑な集合上（例えばマッチングでの辺の数が関数であるように与えられたグラフの全てのマッチングの集合のようなもの）で定義される関数の最適化を行いたい時、この目的関数では導関数を持たないため、古典的な分析手法は役に立ちません（Fig. ７）。

先程説明したケーニッヒの定理は最大マッチングの特徴付けを行うものであり、理論的考察には大変有用ですが、どうすればこの最適条件を実際に計算で求めることができるのかは教えてくれません。（ちなみに、こうしたアルゴリズムは、ずっと後になってから、二部グラフの場合にはクーンによって、一般的な場合においてはエドモンズによって設計されています。）他の問題、例えば「巡回セールスマン問題」などに関しては、ケーニッヒの定理のような巧みな特徴付けさえもできていません。しかし、問題は現場から生まれ、そこに存在する訳であり、我々はそうした問題をできる限りうまく解いていかなければなりません。

こうした問題の攻略法はいくつか存在しますが、最も有効なのは線形計画法を用いたものです。線形計画法は、線形不等式系を解く技術と考えることができます。連立一次方程式を解くことは、大学の学部生レベルの基本スキルです。線形不等式系を解くことはそれよりもかなり込み入っていますが、解くことは可能です。ここで興味深いことは、この代数の問題を幾何の問題に置き換えることができる、という点です。それには（高次元空間に）凸多面体を形成し、最適化問題をこの多面体の最高点を求める、というところまで単純化する方法を用います。

組合せ最適化問題は、線形計画法に置き換えることができます。この置き換えは、得られる線形不等式系が膨大で複雑なものであっても可能です。時には（「巡回セールスマン問題」のように）恐ろしいほど膨大で複雑なものもあるのですが。しかし、こうしたアプローチにより、グラフ理論と線形計画法の非常

にエレガントな結びつきを得られることがよくあります。私自身こうした結びつきに魅せられ、その全体像を理解すべく、多くの時間を費やしたことがあります。この問題に関しては、後にマーティン・グレッチェル、レックス・シュライバーとの共著で、組合せ最適化における幾何学的方法に関する本を書きました。この話の続きは後程お話しします。

４－２．　コンピュータサイエンス

１９７０年代初頭に話を戻します。私がマッチング理論に取り組んでいた頃、研究仲間の多くが、「*あるグラフにおいて、すべての頂点をちょうど一度だけ通る閉路は存在するか？*」というハミルトン閉路に関するトゥッテの定理に類似した命題を編み出そうとしていました（Fig. ８）。この問題はマッチングの問題と非常に似通っていますが、当時私を指導してくださっていたガライ先生を含め、私たちの多くは、なぜこの問題がそんなに難しいのか思案していました。この（１９７０年前後という）時代は、コンピュータサイエンス、特にアルゴリズムとその計算量の理論が急速な進歩を遂げていた時代でもあります。１９７２年から翌１９７３年にかけて、私はアメリカで一年を過ごし、多項式時間アルゴリズムやNP完全問題という、当時できて間もない理論を知りました。多項式時間問題は「易しい」、あるいは少なくとも効率的に解くことが可能である、と考えられていました。

一方、NP 完全問題は、かなり広いクラスの他の問題のすべてがそこに集約されるということもあって、難しいとされています。これは実に大きな相違点で、NP 完全問題を効率的に解くことはできないというのが大方の見方ですが、この数学的な証明は存在していません。通常、「P=NP？」で表わされるこの計算量理論に関する基本的な問題は、２０００年に数学の分野における七大未解決問題の一つに選ばれました。アルゴリズムの計算量理論には随分と胸躍らされました。というのも、この理論はマッチング問題とハミルトン閉路問題の違い、つまり「一方はP、他方はNP完全」という説明になっていたからです。

その後、ハンガリーに戻った私は、私がアメリカにいた一年をモスクワで過ごし帰国していた友人のペーテル・ガックスと旧交を温めました。私たちは、お互いの話に割り込み合いながら、モスクワでレオニード・レビンが行っていた研究とアメリカでのクックとカープの研究について意見交換をしました。その結果、この二つの研究は同じ理論をそれぞれ独自に発展させていたのだということが分りました。（余談になりますが、それから二週間程は、私たち二人はP≠NPの証明をものにしたような気になっていました。今なら、これほど有名な問題に対して自分たちのアイデアはシンプルすぎたかも、ともっと慎重になっ

ていたでしょうが。）

グラフ理論は、コンピュータサイエンスを数学的に支える基盤である学問分野の中でも最大のものの一つとなりました。これまでにも、「P=NP？」問題に限らず、計算量理論の発展過程において最も興味深い問題の多くがグラフ理論の問題から刺激を受けています。

さらに重要なのは、「その逆も真」である、ということです。複雑な計算過程を数学的に説明するためにグラフを用いることができるのです。具体的には、頂点が計算のステップを表します。（この場合、「頂点」は「ゲート」と言うことが多いのですが、）辺は、あるステップのアウトプットが他のステップのインプットとなっていることを示します。これらのアウトプットは単なる（「TRUE」もしくは「FALSE」という）シングルビットと想定することができ、その場合のゲート自身も非常にシンプルなものとなります。基本となるバージョンは、（二つのインプットのいずれも「TRUE」なら「TRUE」をアウトップットとする）「ANDゲート」、（二つのうちのいずれか一つでも「TRUE」なら「TRUE」をアウトプットとする）「OR ゲート」、（インプットビットを一つしか持たず、それを否定するものをアウトプットとする）「NOT ゲート」で構成されます。こうした計算量はすべて、ブール回路と呼ばれるこのグラフの構造で表されます（Fig. ９）。

残念ながらこうした方面に関しては、グラフ理論の研究は大きな進展が得られてはいません。例えば、有名な「N=NP？」問題は煎じ詰めると次のような問題になります。「n 個の頂点の集合を決めます。上のようなネットワークが存在するとします。このネットワークは、すべての頂点のペアに対してインプットゲートがあり、アウトプットゲート u を一つ持ちます。インプットゲートに「TRUE」または「FALSE」という値を入れることにより、任意の頂点上にグラフを特定します。（この時、「TRUE」は任意の頂点が隣接していることを示しています。）グラフがハミルトン閉路を持つ時かつその時に限り、アウトプットが「TRUE」であるようにします。こうしたネットワークを設計することは可能ですが、問題は、n におけるある多項式、例えば n^{100} でそのサイズを制限することができるのか、ということです。グラフ理論を用いて計算量を理解しようとするのは、この上なく大変なチャレンジなのです。

とはいえ、コンピュータサイエンスの話を悲観的なままで締めくくるわけにはいきません。何しろ、１９７０年代のコンピュータサイエンスの研究者は、悲観主義とは正反対の精神を備えていたのですから。２０世紀の最後の３０年間は、グラフ理論と理論計算機科学が二人三脚で発展を遂げるという、非常に特殊な時代でした。

しかし、数学が他の科学分野とともに成長を遂げるという事例は過去にもありました。ご存知の通り、１８世紀には力学と数理解析が発展を遂げました。

それぞれの分野から寄せられた問いや得られた知恵は交配を重ね、ニュートン、ライプニッツ、オイラーなど、数学と物理学という二つの分野で大きな功績を残した巨人が誕生しました（Fig. １０）。

私は離散数学とコンピュータサイエンス（つまりグラフ理論と計算量理論）の相互的な発展に、それに似たものを感じるのです。後者はグラフ理論に問いを投げかけ、その答えを求めるための仕組みを提供してくれましたが、それが（例えば、マッチング問題とハミルトン閉路問題の間の難易度の違いなどの）学問的閃きを裏付け、新たな成果の誕生に結びついたという事実は、興奮を禁じえない経験でした。一方、グラフ理論は計算、半導体の設計、コンピュータネットワークなどを始めとする、コンピュータサイエンスに関する数多くの問題を理解するためのツールを与えてくれました。グラフ理論の研究者にとっては、本当にエキサイティングで大いに刺激的な時代でした。

事実、コンピュータサイエンスはグラフ理論の枠を超え、数学のより古典的な分野の多くへと入り込み、それを作り変えてしまいました。例えば、素数というのは、太古の昔から数多くの優秀な数学者が取り組んできた問題であり、示唆に富んだ成果が積み重ねられてきました。（それに伴い、数多くの未解決問題も生まれました。）しかし、コンピュータの発達によって、シンプルではあるが新しい問題が提起されるようになりました。それは、「*任意の数が素数であるかをどのように判定するか？*」というものです。もちろん、素数を用いて数多くの計算を行ったガウスなど、偉大な数学者はそれぞれ独自の優れた手法を用いていましたが、こうした手計算をベースにしたやり方では、数の桁が二つか三つ程度でなければ時間的にとてもではありませんが追いつきません。コンピュータがあれば、より大きな数に関しても答えを出すことができますが、そのために新たな手法が必要とされました。コンピュータサイエンスは素数性を判定するツールを提供しただけでなく、実は素数性を判定する必要性をも作り出したのです。１９７０年代後半、非常に難しい（と予想される） 整数を素数に因数分解するという手法ではなく、素数判定の効率性に基づいて重要な暗号プロトコルの設計を行えることが判明したのです。

４－３．　最適化から暗号法へ

１９８０年頃、当時ボンにいたマーティン・グレッチェル、それにアムステルダムのレックス・シュライバーと一緒に、楕円体法のグラフ理論的応用に関する本を書き始めました。楕円体法というのは、線形プログラムを解くために（ショア、ユーディン、ネミロフスキー、カチヤンという） 旧ソ連の科学者が考え出したもので、先程私がお話ししたような組合せ最適化問題には好都合な

手法なのです。（適当な枠組みの設定に少し時間がかかりましたが、）組合せ最適化問題とも相性も良く、順調に進んでいたのですが、一つだけ困ったことがありました。「縮重」（つまり多面体に内点が存在しないと見なされるような場合） においては、楕円体法はうまくいかないのです。実際問題として、個々の場合に限定すれば、この問題を解決することは決して難しくないのですが、厄介なことに解法に「アドホック」な要素が含まれていたのです。作業セッションのうち一つを終えてグレッチェルとシュライバーがそれぞれボン、アムステルダムに帰った後、私はこの問題について考察を深め、「*任意の無理数を近似する有理数で共通の分母を持つものを求めよ*」という、基本的な数論的問題を解くことができればこの難点を取り除くことができることに気付きました。例えば、$\sqrt{2}$＝１．４１４２１…や$\sqrt{3}$＝１．７３２０５…などは１０／7＝１．４２８５７…や１２／7＝１．７１４２８…など（７という共通の分母を持つ分数） でも非常に近い数値が得られるのですが、５８／４１＝１．４１４６３…や７１／４１＝１．７３１７０…などの分数の方が遙かに近似していると言えます。

こうして私は、数ある数学の分野の中でも最も長く、輝かしい歴史を誇る整数論に足を踏み入れることになったのです。文献を紐解くと、そうした近似値の「存在」について多くの情報が見つかるのですが、実際にそれらを計算で求める方法はどこを探しても見当たりませんでした。１９世紀、ミンコフスキーの時代に考案されたスタンダードなアプローチとして、この問題を、格子の中で最も近い位置にある二つの点を求める、という問題に置き換えるというものがあります。ここでは詳しい定義は行いませんが、格子というのは、例えば結晶を形作る原子がそうであるように、空間上に点を非常に規則的に配列したものです（Fig. １１）。私が知りたかったのは、その中で最も近い位置にある二点を求める方法でした。

こうして私は、さらに古く、由緒ある幾何学へと辿り着きました。ところが困ったことに、幾何学の世界では、我々が慣れ親しんだ三次元空間ではなく、より高次元の空間で問題を解かなければなりませんでした。そこで私が思い出したのが、その数ヶ月前に聞いた、アムステルダムのヘンドリック・レンストラの話でした。彼は他の組合せ最適問題のために考え出された新しいアルゴリズムについて語っていたのですが、私の取り組んでいたのと同じ幾何学上の問いのためのアルゴリズムを考え出すことによってその問題を解いた、ということでした。彼が考え出したアルゴリズムは、（高次元になるとスピードが落ちすぎるため、） 私が取り組んでいた問題に最適である、とは言えなかったのですが、方向性は間違っておらず、最終的にはこの「最短格子ベクトル問題」に対して効果的なアルゴリズムを考え出すことができました。このアルゴリズムでは近似解しか得られませんでしたが、私にはそれで十分でした。

私がレンストラに手紙を（１９８１年のことですからもちろん「メール」ではありません）書くと、しばらくして返事が来ました。それには彼の兄弟のアリエン・レンストラがこのアルゴリズムに関する、より重要な応用を見つけた、とありました。その「応用」とは、多項式の既約因子を求めるというものでした。（これは整数の素因数分解を求めるという問題と似た、アルゴリズム的問題です。当時はもっと難しいように思えたのですが、実際にやってみたら簡単に解けました。）私たち三人はこのアルゴリズムについて論文をまとめたのですが、それ以降も実用的な応用法が数多く発見されました。中でも重要なのが暗号法への応用で、このアルゴリズムを潜在暗号システムの評価ツールとして使います。

ここまで、暗号法への応用に至るまでの経緯を詳しくお話ししましたが、今日、この話をしようと思ったのはこの例が、様々な数学分野がお互い複雑に結びついていること、純粋に数学的な美しさを愛でる感性のために提起された問いが実用面でも重要な結果に結びつくことがある、ということを如実に示しているためです。

５．　古典数学から受け継いだツール

私がまだ学生だった頃、数学という学問分野は細分化の方向に向かっているように思えました。人類の科学の「核」と考えられていた分野で、抽象的なパラダイムが作り出され、（少なくとも私の眼には）そのパラダイムに合った研究だけが評価されるという状態になっていたのです。確率やグラフ理論などの比較的新しい分野もお互いに枠を作って近づこうとせず、そして古典数学の分野からも距離を置いているように思えました。また、純粋数学と応用数学の間や離散数学と連続数学の間にも境界線が引かれていました。（喜ばしいことにその後こうした傾向は逆転し、今では、より強固な基盤の上で数学の統一性が図られています。）確かに、研究者がより深い枠組みやパラダイムを求めることは大事なことであり、一見かけ離れた分野の問題や成果が、ある日突然、巧みに構築された抽象的な枠組みにぴったりとはまった時には心躍るものです。こんな時に、今まで見過ごされていた重要なポイントが見つかったり、興味深い研究課題が新たに見つかったりすることがよくあります。しかし、こうした「既成の」枠組みには当てはまらないような結果や手法の方が面白いのではないか、と私は思うのです。

これに関連して、「手法の純粋性原則」というのがしばしば議論の的になります。例えば、目の前に幾何学の問題が存在する場合、幾何学的な手法のみを用いて解くのか、あるいは代数や解析などの手法も借用すべきか、という議論で

す。いずれのアプローチにも利点はあるのですが、ここでもまた私個人としては、一見かけ離れた数学分野同士が思いもよらなかった結びつきを見せた時の喜びこそ、何ものにも代えがたいものであると思います。グラフ理論では、代数などの非常に古典的な数学を巧みに応用した試みがなされており、そうした成果を見るにつけて私は感動させられるのですが、私自身もそうした分野同士の結びつきを生み出そうと、チャレンジを続けてきました。実際に１９７０年代には、位相幾何学をグラフ理論へ応用する方法をいくつか考えつき、それを使って長い間解かれることのなかった問題を解くことに成功しました。位相幾何学は離散数学とは正反対である、連続性を研究する学問ですので、私自身もこうした成果が得られたことは意外でした。

　このようにグラフ理論に他の数学分野の手法を応用するという試みにおいて、非常に重要なステップの一つとなったのは、１９５０年代半ばのポール・エルデシュによる「確率的手法」の導入です。アイデアとしてはシンプルなものですが、実際に機能するという事実にはほとんど感動的と言ってもいいくらいです。例えば、よくあることですが、なにか複雑な特性を持った物体を構築したいと思い、いろいろと構造を考えるがどれ一つとしてうまくいかない、といった場合に、コインを投げたりサイコロを振ったりして次のステップを決めながら、ランダムにその物体の構築を進めることができます。このアイデアはいかにも常軌を逸しているとしか思えません。テレビの部品一式がカバンに入っていて、組立てようにもその方法が分からない、といった状況に置かれた場合、コイン投げで組立て方を決める、というようなことは決してしないでしょう。しかし、テレビの組立てには使えなくても、それが魔法のようにうまくいくケースが実際に存在するのです。（これに関してもう一つ例を挙げるなら、他の複雑なネットワーク、例えば人間の脳もおそらくランダムな接続を数多く内包していると考えられますが、見事に機能しています。）

　ここでのエルデシュの功績は、ラムゼーグラフと呼ばれる、非常に特殊な特性を持ったグラフの存在を証明したことです。n 個の頂点を持つグラフはすべからく、相互に隣接する log n 頂点、もしくは相互に隣接していない log n 頂点を必ず持つ、ということはかなり以前から知られていました。ラムゼーグラフは、こうした境界値に近い値を持つ、つまり相互に隣接する頂点並びに相互に隣接しない頂点の最大数がおよそ log n となるグラフです。エルデシュは、一定の数の頂点を持ったグラフをすべてカバンに入れ、よく振って混ぜ合わせ、一つのグラフを取り出すと、それがほぼ確実にラムゼーグラフである、ということを実際に証明しました。現在でもラムゼーグラフの作り方は分かっていないという事実は、エルデシュによるこの研究成果を一層驚くべきものにしています。どのようにやってみても、ラムゼーグラフとは異なるグラフの小さなか

けらしか得られないのです。

こうした確率的な議論は、今日、他の多くの方法でグラフ理論にも使用され、実際、この手法は、数学の数多くの分野において基本的なツールとなりつつあります。

１９６０年前後、エルデシュとアルフレッド・レーニイは、ランダムグラフ理論を提唱しました。彼らが採用したモデルでは、固定した n 個の頂点からスタートし、辺を加えていきます。この時、まだ繋がれていない二点の組み合わせの中からランダムに選んだ二点を、新しく加える辺で結びます。規定数 m の辺を加え終わったら作業を終了します。もちろん、こうした手順を何度も繰り返せば、ほとんど確実に、違ったグラフができ上がります。しかし、n と m の値が大きい場合、こうして得られるグラフは非常に似通ったものとなり、「外れ値」が出る確率はかなり低くなります。（これは大数の法則を具現化したものと言えます。）これに関連した現象として、（辺を加えていきながら）ランダムなグラフができ上がっていく様を観察していると、突然その構造が変化するのが見られます。例えば、０．４９n の辺を持つグラフは、ほとんど間違いなく、数多くの小さな連結成分で構成されていることでしょう。次に、辺が０．５１n になった時にもう一度見てみると、（すべての頂点の４%を含む、）一つの巨大な成分と小さな成分がわずか、という構成になっているはずです。

ランダムグラフのこうした典型的な特性を決定することは簡単ではないのですが、エルデシュとレーニイはその多くを決定付けました。それから１０年もしないうちに、私はレーニイの講演で確率論を知り、ランダムグラフに関する彼らの論文を一部いただきました。正直なところ、しばらくはこの論文に興味が湧きませんでした。というのもその中身は計算過程を事細かに延々と記述したもので、誰がこんなものを好んで読むのだろうか、というような内容でした。その後、この分野はグラフ理論の中でも最も活発な分野の一つとして花開いただけでなく、インターネットのモデリングの基礎となりました。これからお話ししますが、かく言う私もランダムグラフの研究を余儀なくされるようになったのです。

６．　巨大なネットワーク

最近になって、私は巨大ネットワーク理論に関心を抱くようになりました。１９９９年から２００６年にかけて、私はマイクロソフトリサーチの理論グループにいたのですが、名立たる数学者たちが力を合わせて研究を進めるという、大変すばらしい職場でした。我々は興味の赴くままに数学の研究を行うことが認められていたのですが、ソフト開発、ネットワーキング、あるいは暗号理論

など、マイクロソフトという一大ソフト会社が重視するような分野に関して提示される課題に耳を傾けるだけでも十分に価値のあることでした。２００２年の秋、私は３人の同僚が３つの問題を提起したことを知りました。当時は全く違うものに思えたこれらの問題は、その後、密接に関連していることが判明しました。

その３人のうちの一人、ジェニファー・チェイズは、数年前にアルバートとバラバシが始めたインターネットモデルに関心を寄せていました。インターネットはランダムに成長するネットワークとしてモデル化されているのですが、彼女はますます多くの独立したコイン投げの和の極限が「ベル曲線（ガウス分布)」で表されるのと同じような感じで極限分布を表すことができないものか、と自問自答していました。１９７９年、ポール・エルデシュ、ジョエル・スペンサー、そして私の３人でそうした極限概念をそれとなく下敷きにした論文を書き上げました。この論文は、発表当時はあまり注目を集めなかったのですが、現在は準乱数性に関するヴェラ・ショーシュの問題と結び付いています。私は、クリスチャン・ボルグス、ジェニファー・チェイズ、ヴェラ・ショーシュ、カティ・ヴェステルゴンビらとともに、新たに多くのアイデアを加味し、収束グラフ列理論を確立することができました。

時をほぼ同じくして、位相幾何学から借用した手法を用いて量子計算の研究を行っていたマイケル・フリードマンが、統計物理モデルの分配関数の特徴付けを模索していました。ちょうど研究所を訪ねてきていたレックス・シュライバーと共同で、どうにかそうした関数の特徴付けを行うことができました。この二つの成果をベースに、私は私の研究室のポスドクのバラージュ・セゲディとともに収束グラフ列の極限オブジェクトを構築することができました。

これは巨大なネットワークの研究に対する普遍的な枠組みを提示するもので、インターネット以外にもそうしたネットワークが利用されていないかと、あたりを見渡してみたところ、ありとあらゆるところに存在することが分かりました。数学、コンピュータサイエンス、生物学、物理学、社会科学の数多くの分野で、巨大グラフの特性の研究が行われていたのです。これによりグラフ理論に新たな「視点」が加わり、古典数学に分類される他の分野もこの研究には必要であることが分かりました。そのお陰で私も学生時代以来お目にかかったことのない分野を再び勉強する羽目になったのですが、この「復習」はとても楽しいものです。

インターネットは分かりやすい例ですが、実際にインターネットをベースにして定義することのできるネットワークは複数存在します。その一つが「物理的な」ネットワークで、それをグラフと考えると（コンピュータ、電話、ルータ、ハブなどの）すべての電子機器が頂点であり、電子機器間の（有線または

無線による）接続のすべてが辺にあたります。インターネットには、“World Wide Web”と呼ばれる「論理的」構造もありますが、こちらはウェブ上にあるすべての文書によって構成され、また一方をクリックすると他方へ繋がるハイパーリンクが辺となります。

「社会的ネットワーク」は言うまでもなく実際の人で構成されていますが、一人ひとりとの人間関係の定義は異なるものとなります。ここでも、最も良く知られ、最も研究されている「社会的ネットワーク」は、（フェイスブックなど）インターネットをベースとしたものです。歴史学者には、人と人とのネットワークが通底する歴史の理解に取り組まれている方もいらっしゃいます。こうしたネットワークの構造は、例えば、ニュース、疾病、宗教、発明が歴史上の出来事に大きな影響を与えながら、どのようなスピードで社会に広がっていくか、といったことなどを決定します。

この他にも人間と関係のあるネットワークは数多く存在します。人間の脳は巨大なネットワークの格好の例で、その働きがまだ完全には理解されていません。このネットワークは、あまりにも巨大であるため、（ニューロン（神経細胞）とその繋がりからなる）脳の構造を我々の DNA の中へと暗号に置き換えて記すことは不可能です。ではなぜ脳は正常に機能し、数学の問題を解くことができるのでしょうか？

生物学には、そもそも基本構造がネットワークとなっているシステムが山ほど存在します。例えば、森に住むすべての動物と植物の相互作用である食物連鎖や、我々の体内に存在するタンパク質の相互作用などもネットワークです。概して言うなら、ネットワークは、自然界のあちこちに存在する構造やシステムの説明に使われる基本言語となりつつあります。ちょうど連続関数や微積分が、力学や電磁気学を説明する基本言語となったように。

このことは数学者にとって、生物学者、歴史学者、社会学者に対して、彼ら（そしてすべからく一般の人々）が関心を抱いたシステムを説明することができる強力なツールを提供していかなくてはならない、ということを意味します。こうしたシステムは非常に多岐に亘るため、この作業は決して簡単なものではありません。交通のモデリングや情報流通、あるいは先にお話しした電気ネットワークなどは氷山の一角に過ぎません。

我々は無限を近似するためにしばしば有限を用います。（例えば天気を予報するための）物理の方程式の数値解法は、全時空を有限の点として捉え、そうした点において温度や気圧などがどのように変化していくかに関して、段階的に（近似的）計算を行うという手順を通常は踏みます。少し難しくなりますが、無限とは、しばしば大きな有限の近似になります。連続構造は、離散構造に比べてすっきりとしており、より多くの対称性が存在し、内容が豊饒です。グラ

フの極限はこうした手法の好例であると言えます。

ここで大きな金属片を具体的な例として、この考え方をご説明します。これは結晶ですが、原子とその結合からなる非常に大きなグラフであると言うことができます。(ただし、原子とその結合は周期的に配列されているため、いささか退屈なグラフとなります。) しかし、この金属を使って橋を作る技術者にとっては、この金属を（密度、弾性、温度など、) いくつかの重要なパラメータを関数とする連続体として捉えた方が使い勝手が良いのです。そう考えれば微分方程式を使って橋の安定性を計算することができます。ところで、もっと一般的で非常に大きなグラフを一種の連続体として考えることは可能でしょうか？

一部のケースに限定すれば、それは可能です。Fig. １２に考え方を示しています。まずはエルデシュとレーニイが使用したものよりも少しだけ複雑なランダムグラフから始めます。このグラフは、「ステップ毎に新しい頂点または辺が生まれる」というルールに則ってランダムに成長を促すことによって構築していきます。頂点の数が n ならば、新しい頂点が生まれる確率は１/n、新しい辺が生まれる確率は（n-１）/n となります。新しい辺はランダムに選ばれた頂点のペアを結びます。

左の図は、以下のルールで１００ステップを行って得たグラフとなります。i 番目の列および j 番目の段が交差するピクセルは、i 番目の頂点と j 番目の頂点を結ぶ辺が存在する場合は黒とし、そのような辺が存在しない場合は白とします。そのルールに従うと左上の部分の色が濃くなります。これは作られてから時間が経ったために、結んでもらえるチャンスが多くなった頂点のペアを表すピクセルが左上に多いからです。

このグラフは偶然に任せて作られたものですが、左のピクセルの図を遠くから見ると右に示した連続関数１-max（x, y）に似通ったものになっています。これを１００ステップではなく１，０００ステップ行ってグラフを作った場合、類似性はさらに顕著になります。頂点の数が増えるにつれてだんだん小さくなっていくランダムな変動は除き、左のグラフの特徴が、右図のかなりシンプルな関数に含まれていると言えます。

数千の頂点を持つ大きなグラフや数十億の頂点を持つ巨大なグラフは、グラフ理論の研究者にまったく新しい種類の難問を投げかけています。こうした課題のいくつかに対応していくためには、他の古典的な数学分野との結びつきをさらに多く発見し、活用していかなければならないのですが、ある意味、これは数学だけに許された「趣」であるとも言えます。

７．　研究の向こう側にあるもの

数学者の人生はなにも研究がすべて、と言う訳ではありません。程度の違いはあるにせよ、数学者はすべからく教育、管理の仕事、そして科学の普及に対して責任を負っています。

私自身は、人を教えるということは大変やりがいのある仕事であると常々感じています。もちろん、優秀な学生に高度な内容を教えることの方が楽しいのは事実ですが、基礎のクラスを教えていても、楽しいことや逆にこちらが試されるような時があります。私はリサーチモノグラフ、教科書のいずれも書いたことがありますが、最適な定義を考えだしたり、与えられたマテリアルの構成を考えたり、適切な例を選んだり、といったこまごまとした作業はとても楽しいものです。

管理の仕事に関しては成功もあれば失敗もありましたが、本日お話しするような内容ではないと思いますのでここでは割愛させていただきます。

最後に、現在、私が関心を抱いていることの一つに、コンピュータやインターネットが生み出す可能性を利用して、数学を始めとする科学の教育及び普及を行うことがあります。コンピュータがもたらす双方向コミュニケーションやアニメーションの可能性を活用した解説「論文」を作ってみましたので、ご覧になりたい方は下記にアクセスをお願いします。

http://www.cs.elte.hu/~lovasz/tuttedemo.html

Fig.1　ハンガリー ブダペストの街並み
Budapest, Hungary

Fig.2　両親と弟とともに(1953年)
With parents and a younger brother, 1953.

Fig.3　４人の子どもたちとともに(1991年)
With 4 children, 1991.

Fig.4　ファゼカシュ高校
Fazekas High School

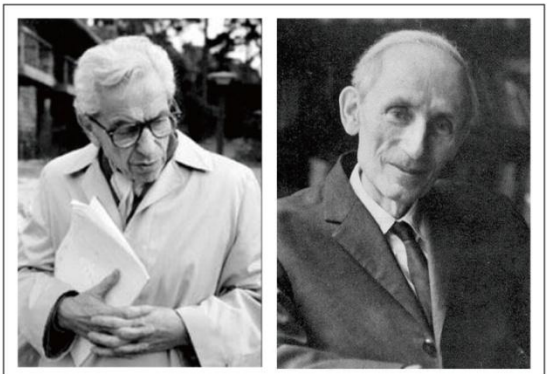

Fig.5　ポール・エルデシュ先生とティボル・ガライ先生
Paul Erdős and Tibor Gallai

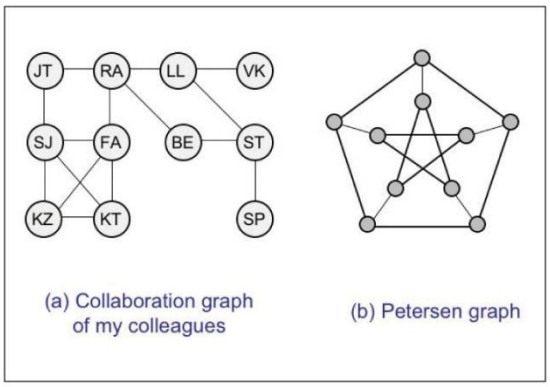

Fig.6 (a) 私の研究仲間の協力関係を表したグラフ。論文を共著した関係にある人々を線で繋いでいる。(b) 多くの対称を含む、数学的に定義されたグラフ（ピーターセングラフ）
(a) The collaboration graph between some of my colleagues. An edge indicates a joint paper. b) A mathematically defined graph with a lot of symmetries (called the Petersen graph)

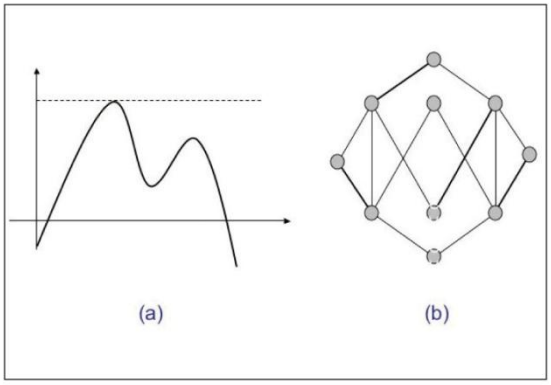

Fig.7 最適化課題：(a)「導関数=０」f’(x) =０となる点を求めて、関数の最大値を出す。(b) 太線で示したマッチングは最大か？
Optimization tasks: (a) Finding the maximum of a function where the derivative is 0. (b) Is the matching shown by the heavy lines maximum?

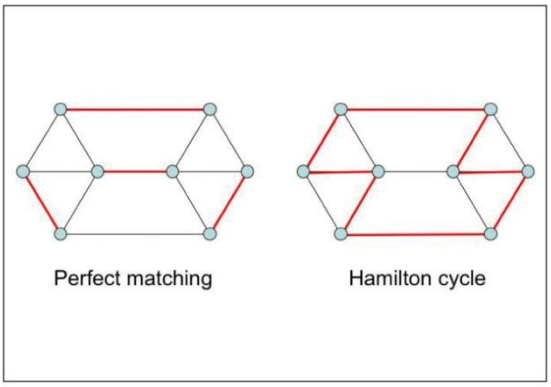

Fig.8 完全マッチング問題とハミルトン閉路の例
Example of a Perfect matching and a Hamilton cycle

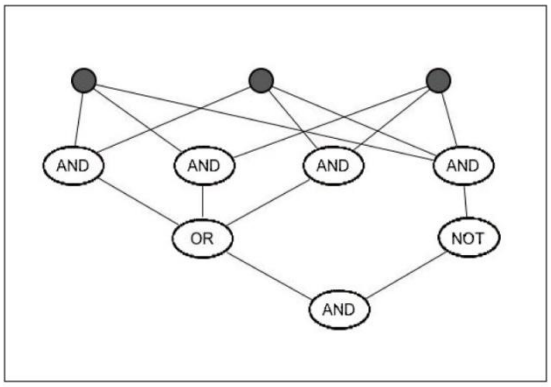

Fig.9 インプットビットのちょうど二つがTRUEであるかどうかを計算するブール回路。中が塗りつぶされている頂点がインプットゲート、一番下の頂点がアウトプットゲートとなる。)
A Boolean circuit computing whether exactly two of the input bits are TRUE. The filled nodes are the input gates, the node on the bottom is the output gate.

Fig.10 数学と物理学の二つの分野で大きな功績を残した巨人たち
Great scientists who contributed to both the mathematical and the physical sides.

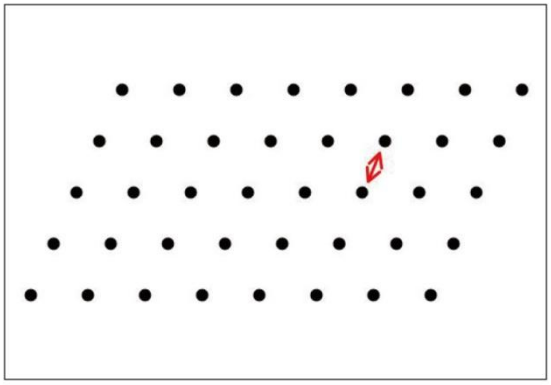

Fig.11 格子の例
Example of a lattice

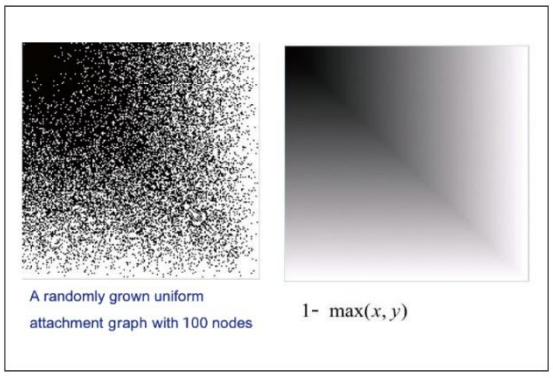

Fig.12 ランダムに成長した均一接続のグラフ（頂点数１００）（左）とそれに近似する連続関数１−max（x, y）（右）
A randomly grown uniform attachment graph with 100 nodes, and the continuous function 1-max(x, y) approximating it.