

題名	数学の新展開―伝統的理論と新しい応用の架け橋―
Title	A Fledgeling Subject Bridging Classical Theory and New Applications
著者名	ラースロー・ロヴァース
Author(s)	László Lovász
言語 Language	日本語・英語 Japanese, English
書名	稲盛財団：京都賞と助成金
Book title	Inamori Foundation: Kyoto Prize & Inamori Grants
受賞回	26
受賞年度	2010
出版者	公益財団法人 稲盛財団
Publisher	Inamori Foundation
発行日 Issue Date	8/20/2011
開始ページ Start page	136
終了ページ End page	171
ISBN	978-4-900663-26-3

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と同時に、今でも自分がそうした方々のお仲間に入って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。

A Fledgeling Subject Bridging Classical Theory and New Applications

László Lovász

It is great pleasure and honor for me to receive the Kyoto Prize. Indeed, when looking at the list of past laureates I feel dwarfed by these great scientist, and I cannot believe that I am included among them. I am also grateful for this opportunity to be able to speak about my way to mathematical research, and about how I see the development of the fields of mathematics that have interested me most.

1. Family

I grew up in Budapest (Fig. 1), which is a large city by Hungarian standards (population 2 million). At the time of my childhood there were still many remnants of the war: ruined buildings, shot-holes in the walls, and some of the bridges across the Danube were still in ruin. The traffic was much less than nowadays: we could go and play soccer in some streets, where a car came only every 10 minutes or so.

Budapest was on the wrong side of the iron curtain. I have some dramatic memories about the revolution in 1956 (I was 8 years old), but I cannot say that my childhood was bad. My father was a surgeon, and we lived in relative comfort. I have a brother two years younger than me, and we had a good time playing together (Fig. 2).

I met my wife Kati when we were in high school; we got married when we were university students. I feel that we have been real partners in life; she is an active mathematician, and an enthusiastic teacher. She has also made a lot of sacrifices to help my research in many possible ways, moving with me to America and back, bearing the burden of the family, proofreading my books and papers, and, above all, understanding the plans, goals, and concerns in my professional life.

We have four children (Fig. 3), and (as for now) five grandchildren, who give us a lot of pleasure. My children were all very good in math, but their interests took the three girls in other directions: our oldest daughter to literature, the other two, to economics. Our son, however, is a university student studying mathematics.

2. Meeting with mathematical research

I was introduced to mathematical research already in high school. I think my father was hoping that I would follow him in the medical profession, but when I was finishing elementary school (at the age of 14), Director Bellay of the school came to see my parents and told them about a specialized high school for mathematically

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、校長のペ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。ファゼカシュでは素晴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いましたラバイ先生は、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



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

talented children, which was just starting, and convinced them to enroll me in this school. This high school, called Fazekas (Fig. 4), was not really well known then (it is now quite famous), but eventually my parents agreed. I still feel that this was the greatest moment in my life. In this high school I had excellent teachers, and met many outstanding students (including my wife), who are still among my best friends.

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示されました。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もので、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。



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

Hungary has a long tradition of nurturing mathematical talent. The first mathematical monthly journal for high school children started in 1894 (it is still alive, and has become a very important institution in math education), and national mathematical competitions started in 1894. Our math teacher, Mr. Rábai, decided that his best students in the class should get more than school math (even though school math in our school was quite advanced), and introduced us to some of the best research mathematicians at the university and the research institute, who were happy to meet and teach talented high school children (travel restrictions behind the iron curtain may in fact have had a beneficial effect in this respect). Besides the very advanced classes in the school, I learned a lot from many excellent research mathematicians. One of them was Paul Erdős (Fig. 5 left). Probably many of you have heard of him: not only was he one of the greatest mathematicians of the 20th century, but also a very special person, and there are many legends about him. He did not want to settle down, did not want to have property (so that it does not distract him from doing mathematics), and was traveling all the time, staying in hotels, guest rooms, or with his numerous friends. He was always surrounded by a big group of people, and shared with them all his new problems, his research ideas, and new results of others he learned about during his travels. He was great in raising new research problems in mathematics, or to communicate new, unexplored research problems all over the world.

He liked very much to talk with children and young people, and he visited our school several times during the 4 years I spent there. He gave the students unsolved

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し問題」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

problems, which were elementary in the sense that even a good high school student could understand them, but this did not mean that they were easy or uninteresting. One or two of these I could solve, and so started my lifelong commitment to mathematical research.

I also want to say a few words about Tibor Gallai (Fig. 5 right), from whom I also learned a lot in high school and later, when he was my thesis advisor (in an unofficial way; we did not necessarily have official thesis advisors at that time). As a person he was just the opposite of Erdős, a reserved, very modest person, who preferred a long quiet conversation one-on-one. When I was a student, I visited him regularly and learned a lot about mathematics, in particular about graph theory, and about his ideas of the directions it is developing.

One event which made a great impression on me happened when I wrote up my first paper, a rather complicated graph-theoretic argument. Gallai helped me a lot; I could even say that based on my inexperienced notes, he was the one who wrote the paper. At the end, not only that did he refuse to be a co-author of the paper; he even objected to thanking him at the end of the paper. He said that as a teacher, this was his duty. I don't know if I always managed to follow his moral standards, but I have tried.

When I finished high school, it was natural to enroll as a mathematics student at the Eötvös Loránd University in Budapest. I got an excellent education there, learning both the foundations of most branches of mathematics, and also the spirit of mathematical research.

3. About graphs

The area of mathematics that inspired most of my work is graph theory. This studies structures that are mathematically very simple: they consist of a some elements called *nodes* or *vertices*, and a relation between them: some pairs of nodes are *adjacent*, or *connected by an edge*, some pairs are not. Such a structure is called a *graph* or *network*. For example, if we want to describe the acquaintanceship structure of a society, we can represent every person by a node, and connect two nodes by an edge if these two persons know each other. We usually represent the nodes by points in the plane, and the edges, by curves connecting them (not necessarily straight). This way we get a drawing like in Fig. 6. A graph is one of the simplest possible structures, and it is clear that graphs are needed for the

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性を増してきました。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つ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?」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

representation or modeling of a great variety of structures in sciences, economics, engineering, logistics, and many other areas.

Graph theory is not a new subject. The first result in graph theory, the Königsberg Bridges Problem, was solved by Euler (one of the greatest mathematicians of all times) in 1736. However, it was not until the 1960's when graph theory started to become a large and active field. Paul Erdős was especially instrumental by asking many simple but nontrivial and inspiring questions, and thereby leading the subject to more and more depth and maturity.

Graph theory is usually considered to be one branch of “discrete mathematics.” Note the spelling: we don't mean “discreet” (in the sense of respecting privacy) but rather that we consider structures which consists of well-separated objects, usually finite in number (in contrast, the real line consists of an infinite number of points, which can be arbitrarily close to each other). Graph theory and areas in which generalizations or abstractions of graphs are studied constitute a substantial part of discrete mathematics, and I will not make a distinction between them in this talk.

I was introduced to graph theory, and through it to mathematical research, quite early in my life. My high school classmate and friend Lajos Pósa had met Paul Erdős when he was quite young. Erdős gave him graphtheoretic problems to solve, and he was successful, and by the time he started high school, he wrote a joint research paper with Paul Erdős and some more papers by himself. Later when we met in high school, he told me about some further Erdős problems, and since I was able to solve one or two, he introduced me to Erdős. Erdős gave me unsolved problems, and then I thought of some of my own, and so started my lifelong commitment to graph theory.

I must add that in those days, graph theory was quite isolated from “mainstream” mathematics, and I was often advised by older mathematicians to do something more serious instead. But for me, the novelty of the subject and its potential applications were fascinating.

Things have changed since then. Graph theory has become quite important in the last decades, through many of the applications, but also through its tighter and tighter links with other parts of mathematics. I will mention some of these developments below.

マッチングに関する問題には未だに解が見つから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は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

4. Meeting with applications

4-1. Combinatorial optimization

In the last years of my studies, I got interested in the strong connection between operations research and graph theory. I wrote my thesis under the guidance of Gallai on the problem of factors of graphs (today we call them matchings). The basic question is: *Given a graph, can we pair up its nodes so that the two nodes in each pair are adjacent?* More generally, what is the maximum number of edges that are pairwise disjoint (without a common endpoint)? For bipartite graphs (graphs in which the nodes are divided into two classes, so that each edge connects two nodes in different classes) the answer was given by König in 1931: *The maximum number of pairwise disjoint edges is equal to the minimum number of nodes covering all edges.* Tutte and Berge extended the characterization to all graphs (the condition is beautiful but a bit too complicated to state here). Many other matching problems remained unsolved, however (allowing me to write a thesis by solving some), and matching theory is still an important source of difficult, but not hopelessly difficult, graph theoretic problems.

Shortly after I defended my thesis, I solved a problem which was called the Weak Perfect Graph Conjecture of Berge, and the method of solution turned out to have interesting consequences in integer programming and through this, to polyhedra. I have found repeatedly that this connection between graph theory, optimization, and geometry is most fruitful.

There are many other graph-theoretical optimization problems, some of which, like the Maximum Flow Problem or the Traveling Salesman Problem, are very important in practice, and broadly known. These problems (and also the perfect graph problem, which I don't describe in detail) are examples of optimization problems quite different from traditional optimization problems.

In a typical optimization problem in analysis, we want to find the minimum or maximum of a "smooth" (differentiable) function, and one learns as an important application of differential calculus how to solve this by finding the points where the derivative is 0. In discrete optimization the situation is quite different: we want to optimize functions that are defined on a finite, but large and complicated set (like the set of all matchings in a graph, where the function is the number of edges in the matching). This objective function has no derivative, and the classical methods

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・グレッツェル、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

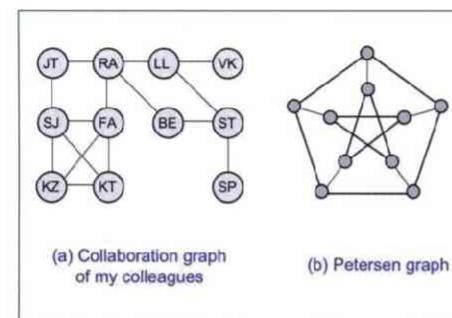


Fig. 6 (a) 私の研究仲間の協力関係を表したグラフ。論文を共著した関係にある人々を線で繋いでいる。(b) 多くの対称を含む、数学的に定義されたグラフ（ピーターセングラフ）
(a) The collaboration graph between some of my colleagues. An edge indicates a joint paper. (b) A mathematically defined graph with a lot of symmetries (called the Petersen graph)

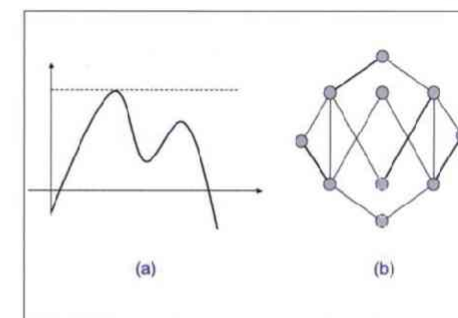


Fig. 7 最適化課題：(a) 「導関数=0」 $f'(x)=0$ となる点を求めて、関数の最大値を出す。
(b) 太線で示したマッチングは最大か？
Optimization tasks: (a) Finding the maximum of a function where the derivative is 0. (b) Is the matching shown by the heavy lines maximum?

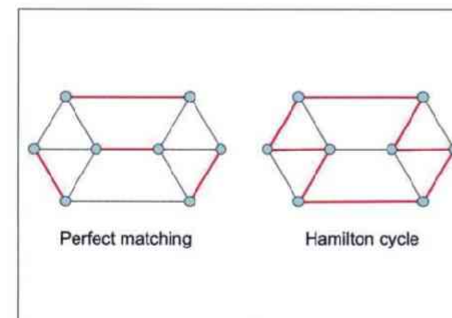


Fig. 8 完全マッチング問題とハミルトン閉路の例
Example of a Perfect matching and a Hamilton cycle

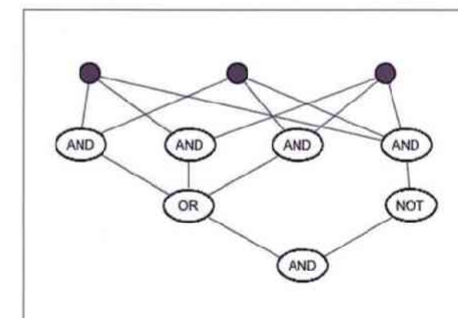


Fig. 9 インプットビットのちょうど二つがTRUEであるかどうかを計算するブール回路。中が塗りつぶされている頂点がインプットゲート、一番下の頂点がアウトプットゲートとなる。
A Boolean circuit computing whether exactly two of the input bits are TRUE. The filled nodes are the input gates, the node on the bottom is the output gate.

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かりました。(余談になりますが、それから二週間程は、私たち二人は $P \neq NP$ 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、とちょ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、 $P=NP?$ 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

of analysis are useless (Fig. 7).

The theorem of König described above characterizes the maximum matching, and it is very useful in theoretical considerations, but it does not tell how to *compute* this optimum (such an algorithm was designed much later by Kuhn in the bipartite case and by Edmonds in the general case). For other problems like the Traveling Salesman Problem, not even a good characterization similar to König's Theorem is possible. But the problems are there, arising from practice, and we have to solve them as well as we can.

There are several methods to attack such problems; perhaps the most successful one goes through linear programming, which can be thought of as the art of solving systems of linear inequalities. Solving systems of linear equations is a basic undergraduate level skill. Solving systems of linear inequalities is quite a bit more complicated, but it is also possible. It is interesting to note that this algebraic problem can be translated to geometry, by constructing a convex polyhedron (in a high dimensional space) and reducing the optimization problem to finding the highest point of this polyhedron.

Combinatorial optimization problems can be translated into linear programming, even though the systems of linear inequalities one gets can be very large and complicated, sometimes forbiddingly so (like in the case of the Traveling Salesman Problem). But quite often one gets very elegant connections between graph theory and linear programming this way. I got fascinated by these connections, and spent a lot of time trying to understand them in general. Eventually I wrote a book with Martin Grötschel and Lex Schrijver about geometric methods in combinatorial optimization; but I will come back to this later.

4-2. Computer science

Coming back to the early 1970's, when I was working on matching theory, many of us tried to obtain an analogue of Tutte's Theorem (characterizing when a graph has a perfect matching) for Hamilton cycles (Fig. 8): *given a graph, is there a cycle in it going through each node exactly once?* The problem is quite similar to the matching problem, and my advisor Tibor Gallai and many of us were wondering why is it so much more difficult. This time (around 1970) was also the time of the fast development of computer science, in particular of the theory of algorithms and their complexity. In 1972/73, I spent a year in the

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ふ、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ふ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)学問的関心を裏付け、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

US, and learned about the newly developed theory of polynomial time algorithms and NP-completeness. Polynomial time problems were considered “easy,” or at least efficiently solvable.

NP-complete problems are hard in the sense that every other problem in a rather wide class of problems can be reduced to them. It is widely expected that this is a real distinction, and NP-complete problems cannot be solved efficiently, but no mathematical proof of this assertion exists. This fundamental problem of complexity theory, usually stated as “ $P=NP?$,” was included in 2000 among the 7 most important open problems in mathematics. The theory of complexity of algorithms thrilled me because it gave an explanation of the difference between the matching problem and the Hamilton cycle problem: one of them was in P, the other was NP-complete!

When I returned to Hungary, I met a friend of mine, Péter Gács, who spent the year in Moscow. Cutting into each other's words, we began to explain the great ideas we learned about Leonid Levin's work in Moscow, and about the work of Cook and Karp in the US: as it turned out, it was independent development of the same theory. (For about two weeks we thought we had a proof for $P \neq NP$. Nowadays we would be more suspicious of our own too simple ideas for a famous problem...)

Graph theory became one of the most important areas of the mathematical foundations of computer science. We have seen that graph theoretic problems motivated the “ $P=NP?$ ” problem, and many more of the most interesting questions in the development of complexity theory.

There is also an important connection pointing the other way: to describe in mathematical terms the process of a complicated computation, one can use a graph. Steps in the computation are represented by nodes (often called “gates” in this context), and an edge indicates that the output of one step is an input of the other. We can assume that these outputs are just single bits (“TRUE” or “FALSE”), and the gates themselves can be very simple. The most natural version is to use AND gates (which output TRUE if both of their inputs are TRUE), OR gates (which output TRUE if at least one of their inputs is TRUE) and NOT gates (which have only one input bit, and they output the negation of it). All the complexity of the computation goes into the structure of this graph (called a *Boolean circuit*; Fig. 9).

I am sorry to report that we, graph theorists, have not achieved much in this direction. For example, the famous “ $P=NP?$ ” problem boils down to the following question: Let us fix a set of n nodes. Suppose that there is a network as above, which

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・グレッツェル、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、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ツ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がきました。例えば、 $\sqrt{2}=1.41421\dots$ や $\sqrt{3}=1.73205\dots$ などは $10/7=1.42857\dots$ や $12/7=1.71428\dots$ 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、 $58/41=1.41463\dots$ や $71/41=1.73170\dots$ などの分数の方が遙かに近似していると言えます。

has an input gate for every pair of nodes, and a single output gate u . Assigning “TRUE” or “FALSE” values to the input gates, we specify a graph on the given nodes (TRUE meaning that the given nodes are adjacent). We want the output to be TRUE if and only if the graph has a Hamilton cycle. Such a network can be designed, but the question is, whether its size can be bounded by some polynomial in n , say by n^{100} . To understand the complexity of computations using graph theory is a BIGGGG challenge!

But I cannot end my remarks about computer science on this pessimistic note, because pessimism was very far from the spirit of computer science in the 1970's. In fact, the last 3 decades of the 1900's was a very special period of co-development of graph theory and theoretical computer science.

Such a co-development of mathematics with another science happens every now and then: one can think, for example, of the development of mechanics and mathematical analysis in the 18th century. Questions and results from both areas cross-fertilized each other, and the same great scientists (Newton, Leibniz, Euler) contributed to both the mathematical and the physical sides (Fig. 10).

I felt something similar about the co-development of discrete mathematics (graph theory) and computer science (complexity theory). The latter provided a new framework to ask questions and seek answers in graph theory, and it was most exciting to see how this confirmed some intuition (like about the difference in difficulty of the matching problem and the Hamilton cycle problem) and lead to new results. In the other direction, graph theory provided the tools of understanding computations, the design of chips, computer networks, and many other questions in computer science. It was an exciting and inspiring time for a graph theorist to live in!

In fact, computer science did not stop at the boundaries of graph theory; it has penetrated and re-shaped many other, more classical parts of mathematics. For example, prime numbers have been studied by many of the best mathematicians since ancient times (these are positive integer numbers that are not multiples of any smaller integer other than 1). A lot of deep results have been accumulated about primes (as well as open many questions). The theory of prime numbers was considered as one of the most “pure” areas, studied for its own internal interest. But the development of computers raised a very simple but novel question: *how do you decide whether a given number is a prime?* Certainly, great mathematicians like Gauss, who did a lot of computation with primes, had good individual methods, but

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。そこで私が思い出したのが、その数ヶ月前に聞いた、アムステルダムへのンドリック・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、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



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.

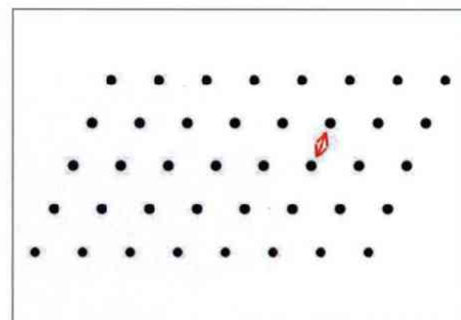


Fig. 11 格子の例
Example of a lattice

these hand calculations became too slow as soon as the numbers had more than a few digits. With computers, you could try to answer this question for much larger numbers, but for this new methods were needed. Computer science not only provided the tools to test primality, it also provided the need: as discovered in the late 1970's, one can design important cryptographic protocols based on the efficiency of primality testing, as opposed to the (likely) difficulty of factoring an integer into primes.

4-3. From optimization to cryptography

Around 1980, Martin Grötschel from Bonn, Lex Schrijver from Amsterdam and I started to write a book about graph-theoretic applications of the ellipsoid method. This method was developed by Soviet scientists (Shor, Yudin, Nemirovsky and Khachiyan) to solve linear programs, and it was particularly well suited for the kind of combinatorial optimization problems that I mentioned above. The theory fitted together very nicely (once the right framework for it has been found), but there was one annoying little gap: the method failed in a case which could be considered “degenerate” (technically, when the polyhedron had no interior point). In practice, it was easy to eliminate this difficulty in every concrete case, but the solutions had an annoying “ad hoc” element. After we ended one of our working sessions and

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。

Martin and Lex went back to Bonn and Amsterdam, I started to think about the problem, and realized that the difficulty could be eliminated if we could solve the basic number-theoretic problem: *find rational numbers with a common denominator approximating given irrational numbers*. For example, $\sqrt{2}=1.41421\dots$ and $\sqrt{3}=1.73205\dots$ are quite well approximated by the fractions $10/7=1.42857\dots$ and $12/7=1.71428\dots$ (having a common denominator of 7), and much better by $58/41=1.41463\dots$ and $71/41=1.73170\dots$

So this took me to number theory, one of the oldest and noblest branches of mathematics. There was a lot of information in the literature about the *existence* of such approximations, but I found no methods to *compute* them. One of the standard approaches to this problem, going back to Minkowski in the 19th century, was to translate the problem into finding the closest pair of points in a lattice. I will not define this exactly, but a lattice is a very regular arrangement of points in space, like the atoms of a crystal (Fig. 11), and I needed a method to find the closest pair among them.

So I got to geometry, even older and nobler; the trouble was that one needed to solve the problem in a high dimensional space, not in our familiar 3-dimensional space. But I remembered that a few months earlier I heard a talk by Hendrik Lenstra from Amsterdam, in which he described a new algorithm for another combinatorial optimization problem, which solved it by developing an algorithm for the very same geometric problem. His algorithm was not quite right for me (it became too slow in high dimension), but it put me on the right track, and I was able to develop an efficient algorithm for this “shortest lattice vector problem.” The algorithm gave only an approximate solution, but this was good enough.

I wrote a letter to Lenstra (on paper: this was back in 1981), and a little later he wrote back that his brother Arjen Lenstra had found a much more important application for this algorithm, namely finding the irreducible factors of a polynomial. (This is an algorithmic problem similar to the problem of finding the prime factorization of an integer. It seemed more difficult at that time, but in the end it turned out to be easier.) The three of us wrote a joint paper about this. Since then, this algorithm has found many practical applications, in particular to cryptography, where it serves as a tool to test potential cryptosystems.

I described the history of this result in detail, because it illustrates the intricate connections between various branches of mathematics, and also how a problem raised for purely esthetic reasons may lead to practically important developments.

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は思えません。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ず、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

5. Tools from classical mathematics

When I was a student, mathematics seemed to move in the direction of fragmentation. Areas which were considered as the “core” of our science developed their abstract paradigms and (at least it seemed so to me) only appreciated research which fit into this. Relatively new branches like probability or graph theory, seemed to become separated from each other and from classical branches. Other division lines ran between pure and applied mathematics, and between discrete and continuous mathematics. (I am happy to report that this tendency seems to have turned around, and the unity of mathematics is on much firmer grounds.) To be sure, it is very important to seek a deeper framework or paradigm of research, and it is always exciting if a problem or result from some seemingly remote area, all of a sudden fits in a nice abstract framework; often this reveals important points that have been missed and suggest interesting problems to work on. However, I have felt that results and methods that do not fit in these established frameworks are perhaps even more interesting.

A related controversial point is the principle of “purity of method.” If we have a problem in geometry, should we attempt to solve it using just geometry, or should we try to bring in methods from algebra or analysis? Again, both approaches have their merits, but for me, unexpected connections between seemingly distant areas of mathematics have always been the most fascinating. There are beautiful applications of very classical mathematics such as algebra in graph theory, which I have always found very fascinating, and have tried to find such connections myself. In the 1970’s I found a couple of applications of topology to graph theory, and was able to solve a rather long-standing open problem by these methods. This was surprising, because topology is the study of continuity, the opposite of discrete mathematics.

One of the most important steps in the direction of applying other areas of mathematics in graph theory was the introduction of the “probabilistic method” by Paul Erdős in the mid-1950’s. The idea is simple, but the fact that it works is almost mind-boggling: quite often, if you want to construct some object with complicated properties, and no construction you can think of works, you can try to construct the object randomly, flipping a coin or rolling dice to determine how to make the next construction step. This sounds crazy: if you get all parts of a TV set in a bag, and you don’t know how to put it together, surely you would not try to

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に、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の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を湧きませんでした。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、ネットワークング、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

attach them to each other on the basis a coin flips. Well, this would not be the right approach to construct a TV-set, but it does work miraculously in some other cases. (To stay at this example, other complicated networks like the human brain most likely have a lot of random connections and they work well.)

What Erdős did was to prove that graphs with certain very special properties, called *Ramsey graphs*, exist. It had been long known that every graph with n nodes must have either $\log n$ nodes that are mutually adjacent, or $\log n$ nodes that are mutually nonadjacent. Ramsey graphs are graphs for which this bound is tight, that is, where the largest number of mutually adjacent nodes is about $\log n$, and so is the largest number of mutually adjacent nodes. Erdős in fact proved that if we put every graph with a given number of nodes in a bag, shake it, and pull out one graph, it will be, almost certainly, a Ramsey graph. What makes this surprising is the fact that even today, we don't know how to construct a single Ramsey graph; whatever we construct, it always ends up among the tiny fraction of graphs which are not Ramsey graphs.

Today, such probabilistic arguments are used in graph theory in many other ways, and in fact this method is becoming a fundamental tool in many areas of mathematics. Around 1960, Paul Erdős and Alfréd Rényi developed the theory of random graphs. In their model, we start with n nodes, which we fix; then we begin to add edges, where the location of each new edge is chosen randomly from among all pairs of nodes not adjacent yet. After a certain prescribed number m of edges, we stop. Of course, if we repeat this construction, almost surely we will end up with a different graph. However, if n and m are large, the graphs constructed this way will be very similar, with a very small probability of getting an "outlier." (This is a manifestation of the Law of Large Numbers.) A related phenomenon is that watching these random graphs develop (as edges are added), we observe sudden changes in their structure. For example, if we look at the graph when it has $0.49n$ edges, almost surely it will consist of many small connected components. If we look again when the graph has $0.51n$ edges, then it will contain a single giant component (containing about 4% of all nodes), along with a few very small ones.

To determine these typical properties of random graphs is not easy, and Erdős and Rényi have worked out many of them. Less than a decade later, I learned probability theory from the lectures of Rényi, and he gave me copies of their papers on random graphs. I have to admit that I was not interested in them for a while; they contained long, detailed computations, and who likes to read such things?

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トドクのバラージュ・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。

Since then, the field has blossomed into one of the most active areas in graph theory, and became fundamental for modeling the internet, and of course I could not avoid working with random graphs, as we shall see below.

6. Very large networks

More recently, I got interested in the theory of very large networks. Between 1999 and 2006 I worked in the Theory Group of Microsoft Research, which was an excellent place, with several outstanding mathematicians and good cooperative atmosphere. We were free to do any mathematical research that we were interested in, but of course it was also worth while to listen to the problems that were raised by software development, networking, cryptography, and other areas which were important for a large software company. In the Fall of 2002, I heard three questions raised by three colleagues, which seemed quite different, but on the long run turned out to be very closely related.

Jennifer Chayes was looking at internet models that were initiated by Albert and Barabási just a few years earlier. The internet was modeled as a randomly growing network, and she asked whether one can describe a limit distribution in a fashion similar to the way the limit of the sum of more and more independent coin-flips can be described by the “Bell curve” (Gaussian distribution). I remembered that in 1979, Paul Erdős, Joel Spencer and I had written a paper where we implicitly used such a limit notion. This had not gotten much attention at that time, but now it also tied in with a question of Vera Sós about quasirandomness, and adding many new ideas, Christian Borgs, Jennifer Chayes, Vera Sós, Kati Vesztegombi and I were able to work out a theory of convergent graph sequences.

About the same time, Michael Freedman, who was working on quantum computing based on methods from topology, asked for a characterization of partition functions of statistical physical models. With Lex Schrijver, who was visiting, we managed to give a characterization of such functions. Based on both works, my postdoc Balázs Szegedy and I were able to construct limit objects for convergent graph sequences.

This suggested a general framework for the study of very large networks, and I began to look around where such networks were used besides the internet. It turned out that they were all over the place: many areas in mathematics, computer science, biology, physics and social sciences study properties of very large graphs.

「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、一人ひとりと人間の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(そしてすべからず一般の人々)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。

This gives a new twist to graph theory, and further areas of classical mathematics turn out to be needed here. I have to re-learn areas that I last met when I was a student, and I enjoy this enormously.

The internet is an obvious example. There are in fact more than one networks that we can define based on the internet. One is a “physical” network, the graph whose nodes are all the electronic devices (computers, telephones, routers, hubs, etc.), and whose edges are all the connections between them (wired or wireless). There is also the “logical” structure of the internet, often called the World Wide Web, which consists of all the documents available on the web, and whose edges are the hyperlinks pointing from one to the other.

Social networks are of course formed by people, with various definitions of connections between them, although the best known and best studied social networks are internet based (like Facebook). Some historians would like to understand history based on a network of humans. The structure of this network determines, among others, how fast news, diseases, religions, inventions spread through society, with enormous impact on the events of history.

There are many other networks related to humans. The brain is a great example of a huge network whose working is not fully understood. It is too large for its structure (all its neurons and their connections) to be encoded in our DNA; how come that it still functions and is able to solve math problems?

Biology is full of systems whose basic structure is a network. Interactions between all animals and plants living in a forest (who eats whom), interactions between proteins in our body, etc. All in all, networks are about to become a basic language for the description of structures and systems in many parts of nature; just as continuous functions, differentiation and integration became the basic language for the description of mechanics and electromagnetism.

For the mathematician, this should say that we have to provide powerful tools for biologists, historians, sociologist to describe the systems they (and all of us) are interested in. This will not be an easy task, since these systems are very diverse; modeling of traffic, information distribution or electrical networks discussed above, are only the peak of the iceberg.

We often use the finite to approximate the infinite; numerical solution of physics equations (say, for the purposes of weather prediction) usually go through restricting the whole space and time to a finite number of points, and computing step-by-step (approximately) how temperature, pressure etc. develops at these

ここで大きな金属片を具体的な例として、この考え方を説明します。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えます。(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。

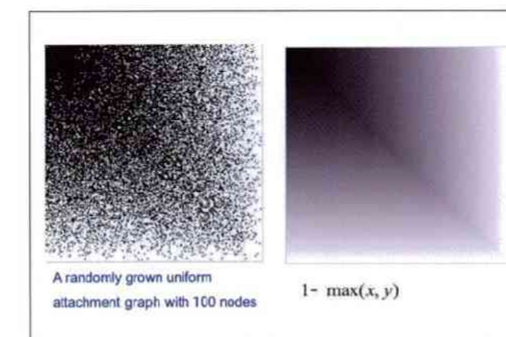


Fig.12 ランダムに成長した均一接続のグラフ(頂点数100)(左)とそれに近似する連続関数 $1-\max(x, y)$ (右)
A randomly grown uniform attachment graph with 100 nodes, and the continuous function $1-\max(x, y)$ approximating it.

points. It is a more subtle thought that the infinite is often a good approximation of the large finite. Continuous structures are often cleaner, more symmetric, and richer than their discrete counterparts. Graph limits are good examples for this method.

To illustrate the idea on a physical example, look at a large piece of metal. This is a crystal, that is a really large graph consisting of atoms and bonds between them (arranged in a periodic and therefore rather boring way). But for an engineer, who uses this metal to build a bridge, it is more useful to consider it as a continuum with a few important parameters (density, elasticity, temperature) as functions on this continuum. Our engineer can then use differential equations to compute the stability of the bridge. Can we consider a more general very large graph as some kind of a continuum?

In some cases this is possible, and Fig. 12 illustrates the idea. We start with a random graph which is just a little more complicated than the random graphs introduced by Erdős and Rényi. It is constructed by growing it randomly according to the following rule: at each step, either a new node or a new edge is born. If the number of nodes is n , then the probability that a new node is born is $1/n$, and the probability that a new edge is born is $(n-1)/n$. A new edge connects a randomly chosen pair of nodes.

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、数学者はすべからず教育、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>

The picture on the left represents the graph after 100 steps in the following way: the pixel in the intersection of the i -th row and the j -th column is black, if there is an edge connecting the i -th node and the j -th column, and white, if there is no such edge. So the area in the upper left is darker, because a pixel there represents a pair of nodes that have been around for a longer time and have had more chance to get connected.

While this graph depends on chance, the pixel picture on the left is, from a distance, quite similar to the continuous function $1 - \max(x, y)$, which is depicted on the right. If instead of a hundred steps we took 1000, the similarity would be even more striking. One can prove that the rather simple function on the right encodes all the information one needs to know about the graph on the left, except for random fluctuations, which become smaller and smaller as the number of nodes grows.

Large graphs, with thousands of nodes, and huge graphs, with billions, represent quite new kind of challenges for the graph theorist. It is a special beauty of mathematics that to meet some of these challenges, we have to discover and use more and more connections with other, more classical parts of mathematics.

7. Beyond research

The life of a mathematician is not all research. In varying proportions, we all have to take our shares of teaching, administration, and popularization of science. I personally have always felt that teaching is a very rewarding activity. Of course, teaching advanced material to very good students is more fun, but even very basic classes can have their interesting, challenging moments.

I have written several books, both research monographs and textbooks, and found that to find the best definitions, the best organization of the material, the right examples, and many other details can be fascinating. I have had my successes and failures in administration, but this is not the right place to talk about them.

One activity I am interested in is exploiting the possibilities offered by computers and the internet in teaching and popularization of science, in particular mathematics. I made an attempt to develop an expository “paper” making use of the possibilities of interaction and animations offered by computers; see <http://www.cs.elte.hu/~lovasz/tuttedemo.html>

稲盛財団 2010——第26回京都賞と助成金

発行 2011年8月20日

制作 公益財団法人 稲盛財団

〒600-8411 京都市下京区烏丸通四条下ル水銀屋町620番地

Phone: 075-353-7272 Fax: 075-353-7270

E-mail admin@inamori-f.or.jp URL <http://www.inamori-f.or.jp/>

ISBN4-900663-26-3 C0000

*2011年4月1日付にて、公益財団法人としての認定を受け、名称を公益財団法人稲盛財団に変更いたしました。