DISCRETE MATHEMATICS

Kazuo Murota
University of Tokyo, Tokyo, Japan

Keywords: discrete mathematics, graph, matching, matroid, Dulmage-Mendelsohn decomposition, Latin square, Euler square, discrete convex function, algorithm, optimization

Contents

Summary

Discrete mathematics is a branch of mathematics dealing primarily with finite and combinatorial structures. It often plays a pivotal role in pure mathematics, and also in applied mathematics in the widest sense of the word, including computer science, statistics, mathematical programming, operations research, etc. Discrete mathematical considerations are also useful in engineering, e.g., electrical and chemical engineering. After a brief introduction to the fundamental issues in discrete mathematics, this chapter explains some typical aspects of discrete mathematics often with motivations from applications. The discrete mathematical objects covered here are square configurations (magic, Latin, and Euler squares), bipartite graphs, and discrete convex functions.

1. Introduction

1.1 Fundamental Issues

Discrete mathematics is a branch of mathematics that primarily studies finite and combinatorial structures. It seems to be difficult, however, to give a formal definition of discrete mathematics. Let us, instead, start with a very simple example to explain some fundamental issues in discrete mathematics.

Suppose that we are interested in possible words of length four, composed of distinct English alphabets, ‘a’ to ‘z’. For simplicity of our arguments, let us assume that we do not care whether the words have meanings or not. This means that we are, in fact, interested in possible sequences of length four, rather than legitimate English words of length four.

The first question we may ask is: Does there exist such a word? The answer is obviously ‘yes’. We can indeed justify this answer by demonstrating a word of length four, say ‘math’. We could have chosen ‘four’ or ‘fuor’ as an evidence of existence, but ‘good’ is not a valid choice because it does not consist of distinct alphabets. The problem of *existence* of an object with certain prescribed properties is most fundamental in every branch of mathematics.

Knowing the existence, we may then ask: How many? The answer is not trivial, but relatively easy. There are 26 possibilities for the first alphabet of a word, 25 for the second, 24 for the third, and 23 for the fourth. Therefore, there are $26 \times 25 \times 24 \times 23 = 358{,}800$ words of length four that are composed of distinct alphabets. This is a problem of *counting*, which asks for the number of the objects with certain prescribed properties. Some of us may want to see a list of these 358, 800 words. This is a problem of *enumeration*, which asks for an explicit list of the objects with certain prescribed properties. Here we distinguish enumeration from counting, although enumeration sometimes means counting. Listing all these 358,800 words is easy in principle, but not feasible in practice, at least on a blackboard. This is often the case in discrete mathematics: The number of these objects is finite, but just too large.

Someone else may want to select the best word from these 358,800 words---the best according to his/her criterion. This is a problem of *optimization*, which asks for an optimal choice from among the objects with certain prescribed properties. The optimal object depends, of course, on the criterion we employ. In our present problem, for example, the optimal word could be ‘math’ or ‘love’, depending on our criterion. Optimization on discrete objects is called *discrete optimization* or *combinatorial optimization.*

For enumeration or optimization, for example, we need systematic and automatic methods to handle a huge number of objects, explicitly or implicitly. *Algorithmic construction* is an important ingredient in discrete mathematics in that it gives concrete ways for constructing desired objects, and also it makes it possible to apply discrete mathematical results to real world problems. Efficiency of algorithms is crucial in applications to large-scale problems. As we have seen above, the number of possible configurations is typically huge, though finite.

Thus the questions of existence, counting, enumeration, optimization, and algorithmic construction may be identified as the fundamental issues in discrete mathematics.

As the name indicates, discrete mathematics studies discrete structures or discrete objects in general. The adjective ‘discrete’ means ‘being separate’, as opposed to ‘continuous’ or ‘smooth’. For example, the set of integers is discrete in contrast to the set of real numbers, which is continuous. A discrete set is not always finite, but even if it contains an infinite number of elements, like the set of integers, discrete mathematics usually studies the properties that are consequences of the finiteness in a certain appropriate sense. A typical discrete mathematical study on the set of integers is the residue classes modulo prime numbers. Such finite algebraic structures are typical discrete structures.

1.2 Squares

Balanced square configurations represent another kind of discrete structures studied in discrete mathematics. We describe here magic squares, Latin squares, and Euler squares. A *magic square* is a square array in which integers are placed in such a way that the sums of the numbers in each row, in each column, and in each of the two diagonals are the same. If the size of the square is n, the integers placed are all distinct, ranging from 1 to n^2. The common value of the sums should be $1+2+\cdots+n^2$ divided by n, which is equal to $n(n^2+1)/2$.

Magic squares of order $n = 3,4,5$ are given respectively by

$$\begin{array}{|ccc|}\hline 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \\ \hline\end{array}\,, \quad \begin{array}{|cccc|}\hline 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \\ \hline\end{array}\,, \text{and} \quad \begin{array}{|ccccc|}\hline 17 & 24 & 1 & 8 & 15 \\ 23 & 5 & 7 & 14 & 16 \\ 4 & 6 & 13 & 20 & 22 \\ 10 & 12 & 19 & 21 & 3 \\ 11 & 18 & 25 & 2 & 9 \\ \hline\end{array}\,,$$

where these squares are not the only possibilities. For the square of order $n = 3$, for example we can verify the row sums:

$$8+1+6 = 3+5+7 = 4+9+2 = 15,$$

the column sums:

$$8+3+4 = 1+5+9 = 6+7+2 = 15,$$

and the diagonal sums:

$$8+5+2 = 4+5+6 = 15.$$

The common value of the sums is $15 = 3\times(3^2+1)/2$.

Magic squares are known to exist for $n \geq 3$, whereas the nonexistence for $n = 2$ is easy to see. Construction algorithms are also known. Magic squares have been studied for mathematical recreations, but there are a number of other types of combinatorial configurations that have serious practical applications.

Latin squares are more serious objects in discrete mathematics that have applications to the design of experiment. A *Latin square* of order n is a square array in which integers $1, 2, ..., n$ are placed in such a way that each row contains each integer exactly once and each column contains each integer exactly once. This implies that each integer appears n times, once in each row and once in each column.

Here are two examples of a Latin square of order $n = 4$:

$$\begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ \hline\end{array}. \tag{1}$$

Note that the first array, for instance, can be decomposed as the 'sum' (superposition) of the following four square arrays:

$$\begin{array}{|cccc|}\hline 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline & 2 & & \\ 2 & & & \\ & & 2 & \\ & & & 2 \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline & & 3 & \\ & & & 3 \\ & 3 & & \\ 3 & & & \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline & & & 4 \\ & & 4 & \\ 4 & & & \\ & 4 & & \\ \hline\end{array}.$$

This shows that a Latin square of order n, in general, is equivalent to a collection of n 'disjoint' permutations.
A Latin square exists for any order n. The simplest construction method is to define the entry a_{ij} at position (i, j) to be the remainder of $i + j - 1$ when divided by n, where the remainder 0 is replaced by n. For instance, this construction for $n = 4$ yields

$$\begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \\ \hline\end{array},$$

which is a Latin square indeed. This construction is algebraic in that it is based on arithmetic modulo n. More sophisticated algebraic methods, relying on the theory of finite fields, are developed for the construction of Latin squares.

A pair of Latin squares, say, (a_{ij}) and (b_{ij}) of the same order n is said to be *orthogonal* if the n^2 pairs (a_{ij}, b_{ij}) are all distinct. The two Latin squares in (1) are, in fact, orthogonal and the array of the pairs (a_{ij}, b_{ij}) looks like

$$\begin{vmatrix} (1,1) & (2,2) & (3,3) & (4,4) \\ (2,4) & (1,3) & (4,2) & (3,1) \\ (4,3) & (3,4) & (2,1) & (1,2) \\ (3,2) & (4,1) & (1,4) & (2,3) \end{vmatrix}.$$

Such a configuration formed by a pair of orthogonal Latin squares is called an *Euler square*. The order of an Euler square is defined naturally as the order of the component Latin squares.

Euler squares have a long history. As the name suggests, this configuration was first conceived by L. Euler, a Swiss mathematician in the 18th century, in the problem of the 36 officers. Suppose that there are 36 officers of 6 ranks from 6 regiments. Is it possible for them to form a 6-by-6 square configuration such that each row contains one officer of each rank and each column contains one officer from each regiment? As is easily seen, this problem asks about the existence of an Euler square of order 6.

Euler investigated the existence of Euler squares of a given order n in general. First, it is trivial to see that no Euler square of order $n=2$ exists. He showed how to construct Euler squares when n is odd or is a multiple of 4. But he could not see how to construct the square for $n=6$ and conjectured futher that no Euler square existed when n is of the form $n=4k+2$ with an integer $k \geq 1$. Note that $n=6$ is of this form with $k=1$. A proof of the nonexistence for $n=6$ was given by. G. Tarry only around 1900. Furthermore, around 1960, R. C. Bose, S. S. Shrikhande and E. T. Parker disproved the conjecture of Euler for $n=4k+2$ with $k \geq 2$. Thus it is known, at present, that Euler squares of order n exist unless $n=2$ or $n=6$.

Orthogonal Latin squares are closely related to block designs, to be explained in a later chapter. (see *Combinatorics*)

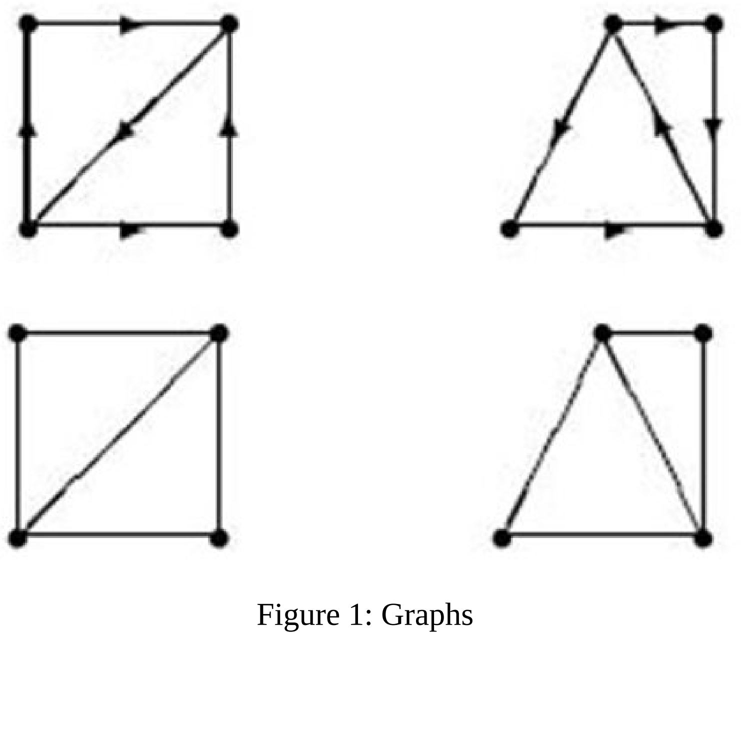

Figure 1: Graphs

1.3 Graphs

Graphs are also typical discrete structures. A graph consists of vertices (points) and arcs (lines), as illustrated in Fig.1. When the arcs are given orientations, as in the top of Fig. 1, a graph is called a directed graph, or a *digraph* for short. When the arcs have no orientations, as in the bottom of Fig. 1, it is called an undirected graph. A graph can be drawn in a plane, but in many different ways.

Usually we are not concerned how we draw pictures. For examples, the two directed graphs in the top of Fig. 1 are not distinguished from each other, but identified with each other; rotate the right picture counterclockwise by 90 degrees to see this. Similarly, the two undirected graphs in the bottom of Fig. 1 are identified with each other.

Many interesting problems, from pure mathematics and from engineering applications, can be formulated through graphs. For example, given a graph, we may ask whether there exists a path with certain prescribed properties. The Hamiltonian path problem asks if a given graph contains a path that goes through every vertex exactly once.

The Eulerian path problem asks if a given graph contains a path that goes through every arc exactly once. The linking problem asks if a given graph contains a set of disjoint paths that connect a specified set of entrance vertices to another specified set of exit vertices.

A graph $G=(V,A)$ with vertex set V and arc set A is said to be *bipartite* if the vertex set V can be partitioned into two disjoint subsets, say, S and T such that each arc connects a vertex in S and a vertex in T. In this case we often denote the biparitite graph as $G=(S,T;A)$. A bipartite graph is illustrated in Fig. 3, in which the vertices in S are denoted by $\bullet$ and those in T by $\odot$.

Bipartite graphs are often used in applications to represent incidence relations, or connections, between two different sets of objects. A typical example of such representation appears in the assignment problem in operations research. In the assignment problem, possible assignments of workers to jobs are represented by a bipartite graph $G=(S,T;A)$, where S and T denote the given sets of workers and jobs, and an arc between a worker and a job means that the worker is capable of the job. The assignment problem will be treated later under the name of the matching problem.

1.4 Algorithms

Discrete mathematics is used in applied mathematics in the widest sense of the word, including computer science, statistics, mathematical programming, operations research, etc. Discrete mathematical considerations are also useful in science (e.g., chemistry, physics, biology) and engineering (e.g., electrical engineering). Use of discrete mathematics in applications is reinforced when mathematical results are accompanied by efficient algorithms. Many different kinds of algorithms have been developed in discrete mathematics; algorithms for graphs and networks, for strings and texts, for algebraic operations, for geometric computations, etc.

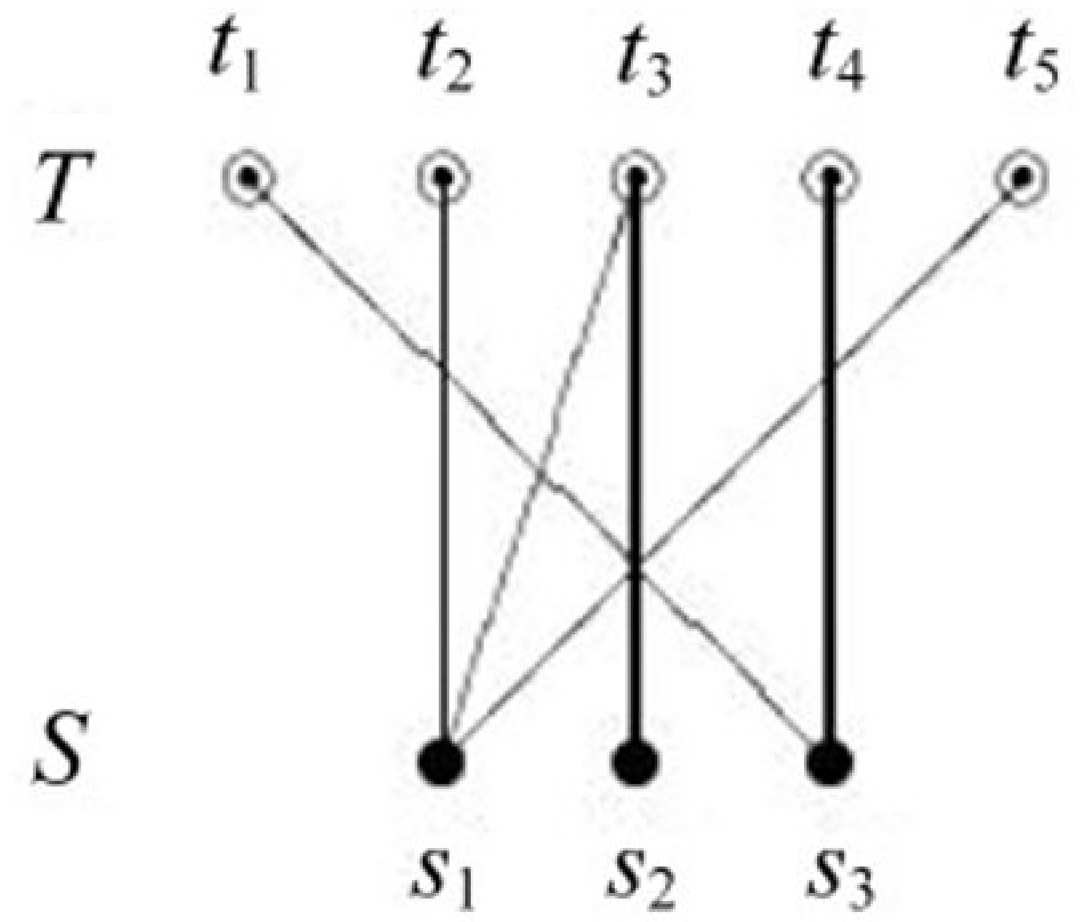

Figure 2: Bipartite graph

The theory of *computational complexity* affords a theoretical framework to investigate the efficiency of algorithms in a rigorous manner. Roughly speaking, the efficiency of a particular algorithm is measured in terms of the number of basic operations needed in the algorithm.

If the number of basic operations involved in the algorithm is bounded by a polynomial in the size of a problem instance to be solved, the algorithm is said to be a *polynomial-time* algorithm. It is widely accepted that a polynomial-time algorithm may be regarded as being efficient, in theory and in applications. What matters is not the distinction between finite and infinite, but the distinction between polynomial and nonpolynomial.

Some typical aspects of discrete mathematics are explained in the following subsections for matchings on bipartite graphs and discrete convex functions. The following sections present more systematic descriptions on graph theory (see *Graph Theory*), combinatorics (see *Combinatorics*), computational complexity (see *Computational Complexity*), algorithms (see *Algorithms*), and optimization (see *Optimization*).

2. Bipartite Matchings

In this section we consider matchings in bipartite graphs to explain some typical results in discrete mathematics. Emphasis is placed on min-max duality phenomena and decomposition into subgraphs with reference to matchings. A possible application of this result to large-scale numerical computation is also explained.

-
-
-

Bibliography

[1] Biggs N (1989) *Discrete Mathematics* (revised ed.) 480 pp, Caleredon Press, Oxford. [A highly reputed introductory textbook on discrete mathematics.]

[2] Bollobas B.(1990) *Graph Theory, An Introductory Course*(3rd ed.), Graduate Text in Mathematics 63, 180 pp, Springer-Verlag. [A textbook on graph theory containing both fundamental and advanced topics in combinatorics on graph theory. Suitable for students in mathematics and theoretical computer science.]

[3] Brualdi R. A. (1992) *Introductory Combinatorics* (2nd ed.), 618 pp, North-Holland. [An enjoyable introductory textbook on combinatorics.]

[4] Conway J.H. and Sloane N.J.A.(1988) *Sphere Packings, Lattices, and Groups*, 663 pp , Springer Verlag. [A book containing advanced combinatorial theory related to groups.]

[5] Cormen T.H., Leiserson C.E., Rivest R.L. and Stein C. (2001) *Introduction to Algorithms* (2nd ed.), 1180 pp MIT Press. [A comprehensive exposition on algorithms.]

[6] Diestel R. (1996) *Graph Theory*, Graduate Texts in Mathematics 173, 289 pp, Springer-Verlag. [A standard textbook on graph theory.]

[7] Graham R.L., Grötschel M. and Lovász, L. (ed.) (1995) *Handbook of Combinatorics*, two volumes, 2198 pp, MIT Press. [Complete handbook of combinatorics, including theory and applications.]

[8] Graham R.L., Knuth D. E. and Patashnik O. (1994) *Concrete Mathematics* (2nd ed.), 657 pp, Addison-Wesley. [Elementary introduction to combinatorial results for computer science.]

[9] Grimaldi R.P. (1998) *Discrete and Combinatorial Mathematics: An Applied Introduction* (4th ed.), 791 pp, Addison-Wesley. [Complete textbook on combinatorics with many nice exercises and historical notes.]

[10] Hoffman P. (1998) *The Man Who Loved Only Numbers*, 299 pp Hyperion Books. [A biography of P. Erdős, a unique Hungarian discrete mathematician.]

[11] Knuth D. E. (1997) *The Art of Computer Programming* Vol.1 (3rd ed.), 650 pp Addison-Wesley. [Theory of fundamental computing, including many combinatorial ideas for efficient computation in computer science/engineering.]

[12] Knuth D. E. (1998) *The Art of Computer Programming* Vol. 2 (3rd ed.), 762 pp, Addison-Wesley. [Theory of seminumerical algorithms, including many combinatorial ideas for efficient computation in computer science/engineering.]

[13] Knuth D. E. (1998) *The Art of Computer Programming* Vol. 3 (2nd ed.), 780 pp, Addison-Wesley. [Theory of sorting and searching, including many combinatorial ideas for efficient computation in computer science/engineering.]

[14] Lovász, L., Pelikán, J. and Vesztergombi, K. (2003) *Discrete Mathematics*, 290 pp, Springer-Verlag. [An undergraduate textbook covering wide range of discrete mathematics.]

[15] Lovász, L. and M. Plummer, M. (1986) *Matching Theory,* North-Holland, 544 pp. [A standard reference for matching theory with emphasis on structures rather than algorithms.]

[16] Matoušek J. and Nešetřil J. (1998) *Invitation to Discrete Mathematics,* 410 pp, Oxford University Press. [A recommendable textbook on discrete mathematics, especially for students in computer science and engineering.]

[17] Murota K. (2003) *Discrete Convex Analysis,* 480 pp Society for industrial and Applied Mathematics, Philadelphia. [A recent monograph on discrete convex functions.]

[18] Roberts F. S. (1984) *Applied Combinatorics*, 606 pp, Prentice Hall. [Applications of combinatorics to operations research are explained thoroughly.]

[19] A. Schrijver (2003) *Combinatorial Optimization –Polyhedra and Efficiency,* 1881 pp in three volumes, Springer-Verlag, Heidelberg. [Comprehensive expositions on theoretical aspects of combinatorial optimization]

[20] Stanley R. P. (1997) *Enumerative Combinatorics I,* 306 pp, Cambridge University Press. [The first volume of a complete book series on enumerative combinatorics. Basic theory on posets and applications to algebra.]

[21] Stanley R. P. (1999) *Enumerative Combinatorics II*, 581 pp, Cambridge University Press. [The second volume of a complete book series on enumerative combinatorics. Advanced theory on generating functions.]

[22] van Lint J. H. and Wilson R. M.(2001) *A Course in Combinatorics* (2nd ed.), 602pp, Cambridge University press. [A standard textbook on combinatorics.]

[23] Welsh D. J. A. (1976) *Matroid Theory,* 433 pp, Academic Press. [A classic on matroid.]

Biographical Sketch

Kazuo Murota was born in April 1955. He received BS, MS and PhD degrees in 1978, 1980 and 1983 respectively , all from the University of Tokyo. He also received an additional PhD degree in 2002 from the University of Kyoto.
He was an Instructor at The University of Tokyo during 1980-83, Lecturer at The University of Tsukuba during 1983-86, Associate professor at The University of Tokyo during 1986-1992, Associate professor at The University of Kyoto during 1992-1994 before becoming a Professor at the latter place in April 1994. Since 2002 he is with the University of Tokyo as a Professor.