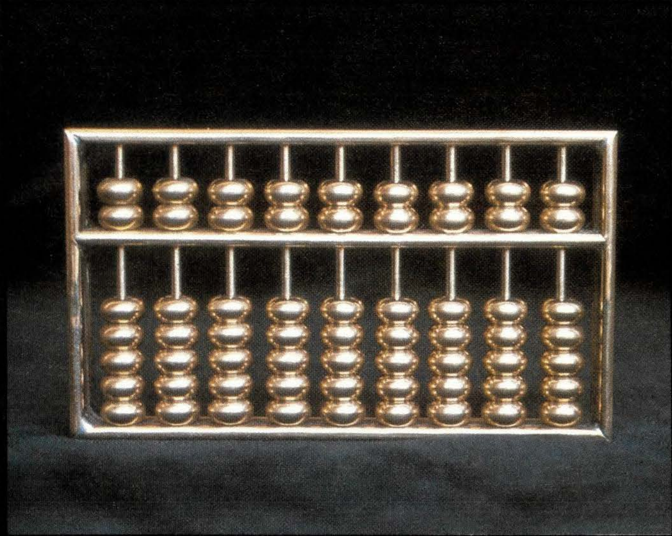
Centre for Mathematics and Computer Science Amsterdam

Centre for Mathematics and Computer Science

Kruislaan 413
1098 SJ Amsterdam
Telephone 020–592 4171/592 9333



abacus

$24+49=73$

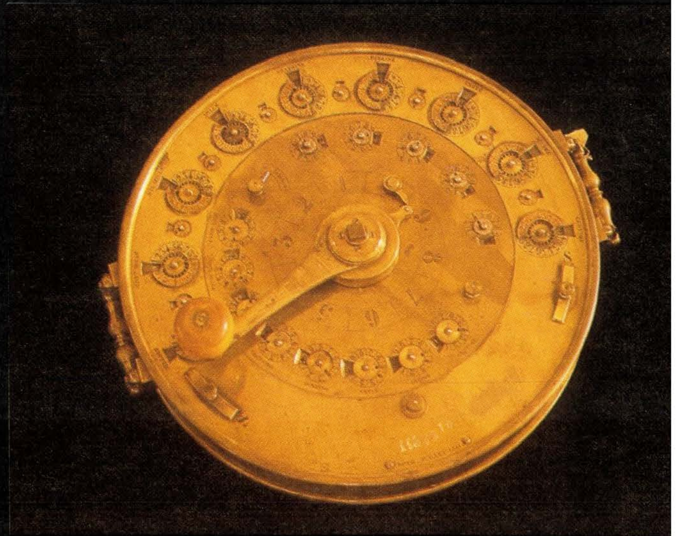
computer

$$\frac{\partial u}{\partial t}-\nu\Delta u+\Sigma u_i D u_i+\nabla(p)=f,$$

$$\operatorname{div}(u)=0,$$

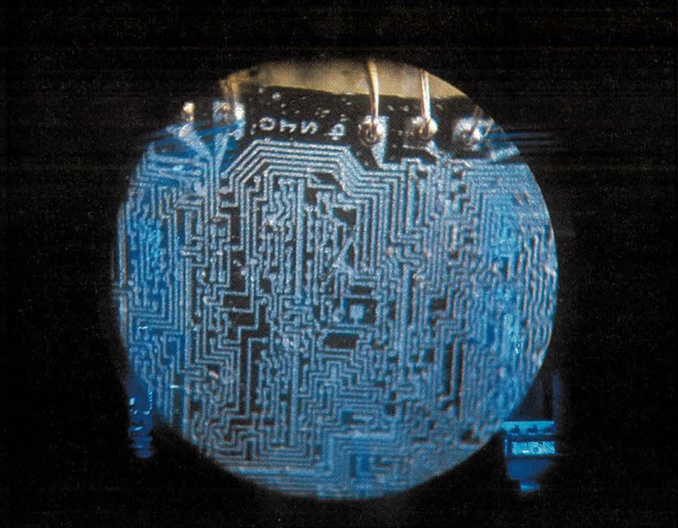
$$u=0 \text{ op } \partial\Omega\times(0,T),$$

$$u(x,0)=u_0(x)$$



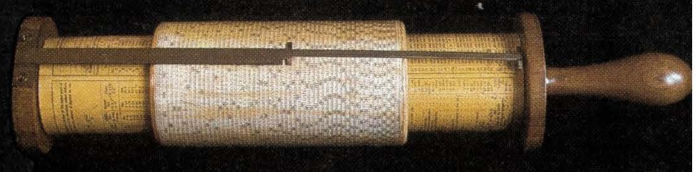
hand calculator

$\bar{x}=(x_1+\ldots+x_n)\,/\,n$



slide rule

$12{,}2\times 89{,}3\approx 1089{,}5$



Introduction

A great deal goes on in a Centre for Mathematics and Computer Science. For more than 35 years research groups, supported by technicians, programmers and other experts, have worked intensively on a wide range of problems. To some extent these problems arise from within science, but we devote a great deal of attention to problems derived from the 'real world', through a variety of commissions and consultations.

The results of our efforts seldom make the newspapers. They do appear regularly in scientific publications, but these are intended for experts. Our advice and reports to our customers are also seen by very few. We hope that this brochure gives some idea as to what we can offer that 'real world' when it comes to solving problems. Problems for which we already have the necessary knowledge and expertise, or which will challenge our experts. You now know who we are!

Prof.dr. P.C. Baayen
Scientific Director

ZWO

The CWI (Centre for Mathematics and Computer Science) is an institute of the Stichting Mathematisch Centrum. This 'stichting' is one of a family of foundations and institutes chiefly supported by the Netherlands Organization for the Advancement of Pure Research (ZWO).

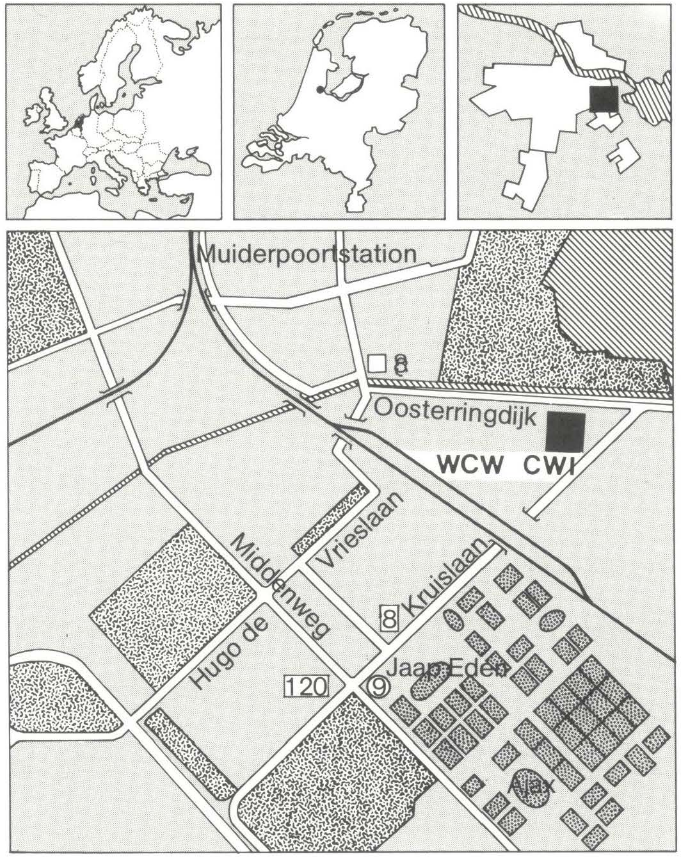
For more than thirty years this organization has played an extremely important role in fundamental research in the Netherlands. In the future, ZWO will add applied and technical research to its responsibilities; the necessary legislation is now being formulated. To handle these responsibilities in the interim, the Foundation for the Technical Sciences (STW) has been established; it will be merged with ZWO in due course. Meanwhile, the CWI has already carried out projects supported by STW.

Mathematical Centre

The Stichting Mathematisch Centrum was established shortly after World War II, more precisely, on February 11, 1946. Its purpose was, among other things, 'to foster the systematic pursuit of pure and applied mathematics in the Netherlands'. Since then, the Stichting has managed an institute that, until September 1, 1983, was called the Mathematisch Centrum (MC). At that time, the institute was renamed the Centre for Mathematics and Computer Science (CWI), to emphasize the independent roles of computer science and mathematics. CWI is housed in its own quarters at the Watergraafsmeer Scientific Centre in Amsterdam. The Stichting is financed partially by the government (chiefly via ZWO) and partially through fees for commissioned research.

Function

Nowhere else in the Netherlands are there so many mathematicians and computer scientists under one roof. It is therefore no wonder that the CWI (formerly the MC) has always played an important role in



The CWI is located on the grounds of the Watergraafsmeer Scientific Centre (WCW) in Amsterdam East, in the region bounded by the Kruislaan, Oosterringdijk, and the railroad line Amsterdam-Hilversum. It is near the Ajax Stadium and the Jaap Eden Ice Rink, about 15 minutes walk (1600 meters) from the Muiderpoort station. It can be reached from the Amstel Station by bus 8, from the Central Station by tram 9, and from the direction Abcoude/Utrecht by bus 120, Vervoersmaatschappij Centraal Nederland. In each case, the most convenient stop is the Kruislaan.

Facilities

CWI has command of a large number of facilities for internal and external use.
Among them are:

- On-line literature information
  Access to data bases all over the world.
- Library
  A large collection covering all areas of mathematics and computer science:
  29.000 books:
  39.000 reports;
  950 current journals
- Computer hardware
  VAX 780, PDP's and M68000's under UNIX;
  25 lines to the two CD-CYBER 750 mainframes at SARA;
  HARRIS 7500 photo-typesetter.
- System advising
  Evaluation, installation and acceptance of UNIX systems.
- Software development centre
  Technical/scientific

mathematics and its applications in the Netherlands. The Dutch universities and technical schools are closely involved in the management of the Stichting; there is also contact with many research departments of these institutions and those of large industrial enterprises.
Although the CWI has no educational responsibilities, it contributes to 'continuing education' by holding seminars, organizing courses, etc.

The past
In the very beginning there was heavy emphasis on numerical and applied mathematics and applied statistics. Even then, however, computer science played an important role. In the post-war years, a large number of MC staff members travelled to England and America, where the development of computers was further along. Partly as a result, a self-built relay computer (the ARRA) was put into service in 1952 - the first in the Netherlands, and one of the first in Europe. This was followed by fully electronic computers, including the X1, very fast for its time (15,000 operations per second), and later the X8. A large number of businesses and institutions placed orders for these computers. It was then decided to farm out the production, which led to the establishment of Electrologica, Inc. (later taken over by Philips). The MC continued to use computers itself (for example to carry out the numerical calculations required for the Delta Plan), and developed new methods for their efficient use. This led to a steady stream of requests to carry out calculations for others on MC equipment. It was finally decided to farm out these activities also. And thus was born the Academic Computer Centre Amsterdam (SARA), the joint computing centre of the two Amsterdam universities and the SMC, now housed in a building next door to the CWI. New applications are continually being developed by the CWI, and made available through SARA.

Present organization
The CWI employs over 150 workers spread over six scientific divisions and a separate extensive service for handling work on commission. Commissions are received either directly or through one of the scientific divisions, after which other divisions can be involved as needed.

MANAGEMENT	
services	**divisions**
commissions and support	pure mathematics
library	applied mathematics
publication service	mathematical statistics
	operations research and system theory
	numerical mathematics
	computer science

programs in FORTRAN, PASCAL, C, and ADA.
- Software packages for statistically responsible data analysis, including SPSS and BMDP, and for statistical analyses.
- Numerical analysis packages NUMAL and NUMPAS.
- Word processing
  Automatic word division;
  Text processing with the TEX and TROFF programs;
  Automatic photo-typesetting, including formulas;
  In-house press for black-and-white offset.
- Computer networks
  Communication via telephone and data lines with computers in the US and Europe.

Commissioned research

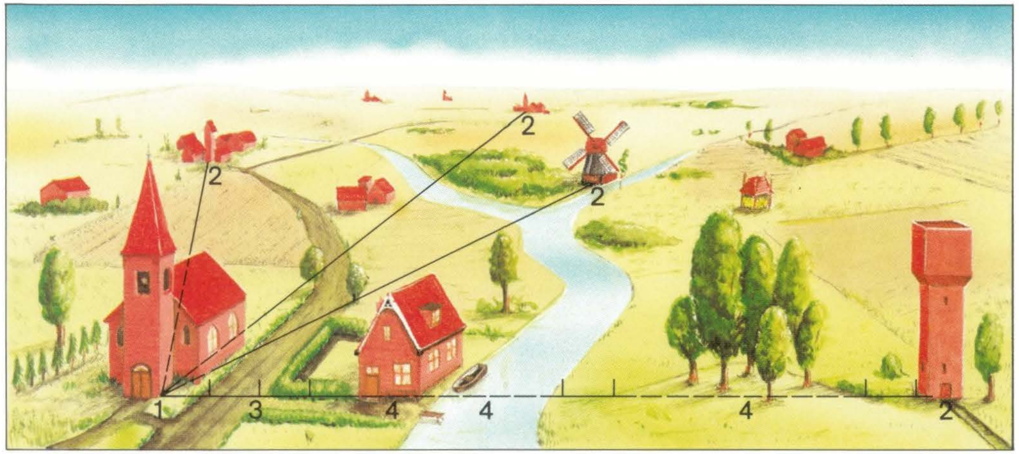
The research activities of the Centre for Mathematics and Computer Science are many and varied. A portion of its effort is devoted to pure research. However, the CWI undertakes a great deal of work at the request of others. This often involves solving practical problems for government or industry.

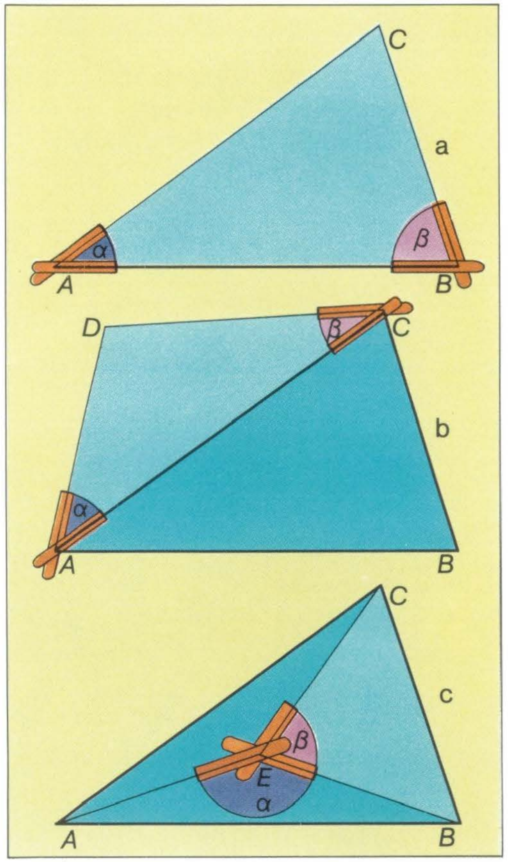
The turbulent developments in the computer world have brought with them a host of problems for both the suppliers and the users of hardware and software. Here the CWI can often help with advanced equipment and specialized programming. The application of mathematics is another matter. Here the problem must first be expressed in mathematical terms; this is called model building or mathematization. Many mathematical models require a specialized software package; on the other hand, problems in computer science often call for a mathematical approach.
Those lacking experience in mathematics and/or computing often do not have the faintest idea that their problems can be mathematized and sometimes solved by applying standard techniques. What could mathematics and computers have to do with the Delta works, or the distribution of goods?
This booklet attempts to answer such questions by describing some of the problems we have taken on over the years. We hope this will give some impression of what the CWI has to offer.

Guidelines
The CWI employs a number of guidelines when considering projects. Here are some examples of the kinds of problems we are interested in:
- the methods of solution are generally known, but the problem is so complicated and requires contributions from such varied disciplines that a solution could no be expected from an organization with fewer facilities.
- the method of solution is known only in scientific circles and has seldom or never been applied in a practical problem.
- there is no known method of solution.

Sometimes a solution can be linked to current research or existing knowledge. In other cases the attempt to find a solution may lead to an entirely new area of scientific research, resulting in a mutual enrichment of science and practice.

Mathematization
It is possible that mathematics was originally strictly practical: calculation and the determination of areas and volumes were matters of great practical import.
However, mathematics had already achieved a high level of abstraction in ancient Greece. By then there were already thinkers who used the notions and techniques of mathematics as building blocks for theories of the universe or for constructing what we now call models. From the sixteenth century on, new mathematical models were created (such as the calculus) that played an ever more important role in science and technology. In the beginning of the twentieth century mathematicians began to study functions of several variables much more intensively, bringing to light completely new phenomena. This led to a flourishing of pure mathematics, with the result that an enormous arsenal of techniques is now available, and an astounding variety of problems

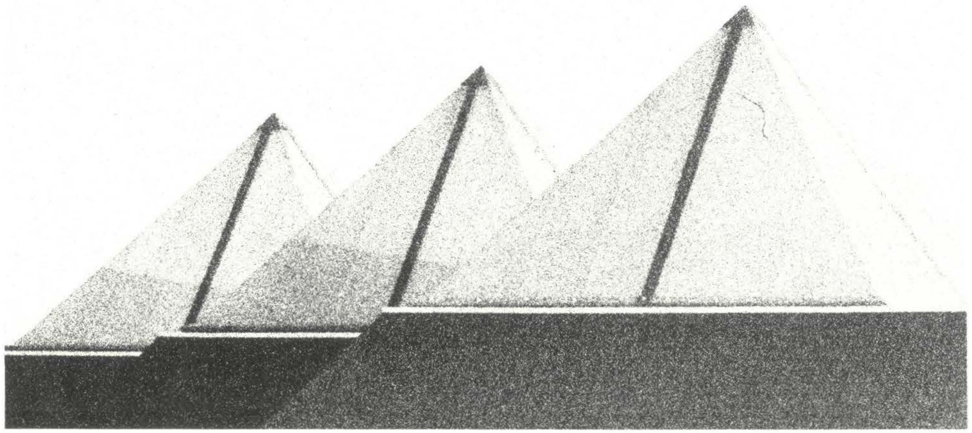




Surveying
Measuring distances over land (from 1 to 2) is difficult: an attempt to stretch a measuring tape along markers (3) may be blocked by obstacles (4).

Triangulation
(a) Mathematics comes to the rescue. The distances AC and BC can be calculated if the distance AB and the angles α and β are known. We choose a clearly visible point as C.
(b) A newly calculated distance (AC) can be used as a baseline for a succeeding triangle ACD etc.
(c) Within a known triangle, the position of a point E can be determined from the angles α and β.

now lends itself to modelling, analysis, and sometimes prediction. The time seems to have arrived to pluck the fruits of all this effort, and to restore the balance between pure and applied mathematics. There is also a need to tighten the ties with the other sciences again, and to build new relations with them. It is significant that the fastest growing areas of applied mathematics are to be found in fields like biology, economics and geology. The enormous supply of mathematical techniques tends to make the mathematician feel that there are very few areas in which a mathematical analysis could not provide deeper insight. Such an analysis must always be preceded by extensive experimentation and polling to decide precisely which quantities are critical (and therefore must be carefully determined).

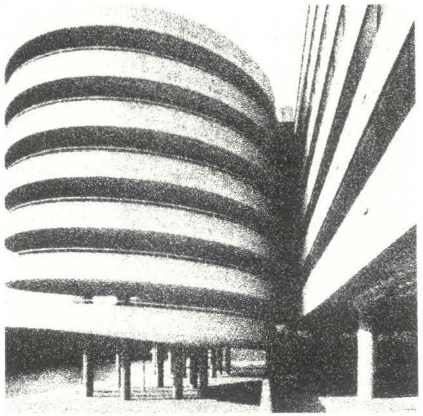


Tetrahedron

Sym (tetraëder) $= S_4 =$

$< v_1, v_2, v_3 : \; v_1^2 = v_j^3 =$

$(v_i v_j)^2 = E \;, \; 1 \leqslant i < j \leqslant 3 >$

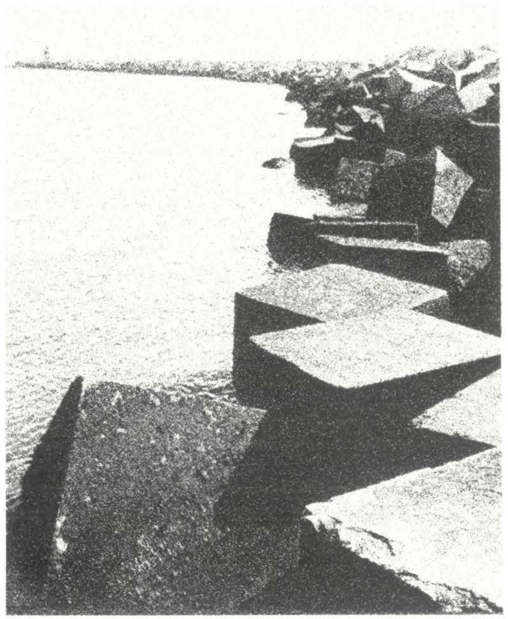


Parking garage

$\vec{z}(t) = (r \sin t, r \cos t, bt)$,

$0 \leqslant t \leqslant t_0$, min $J(r, b, t_0)$ so that

$\mathrm{Cap}(G(\vec{z})) \geqslant N$



Basalt blocks

$\rho_t = \Delta\rho + f(\rho) + g\epsilon(t)$

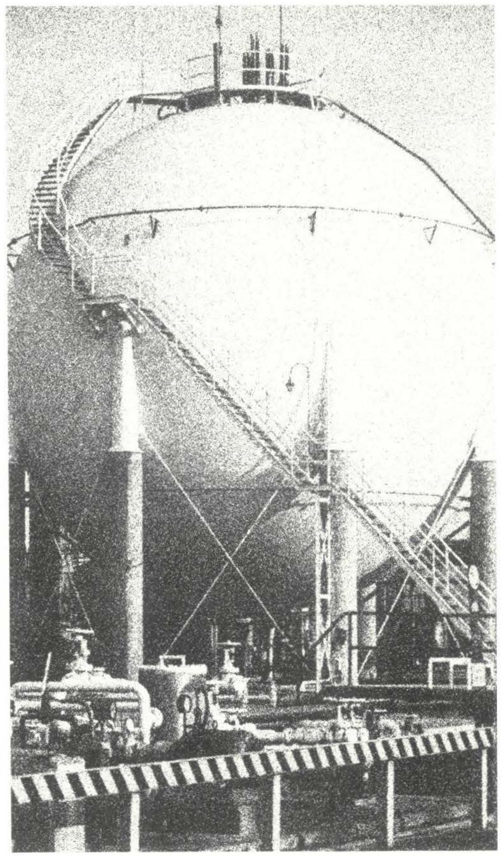
Chemicals tank

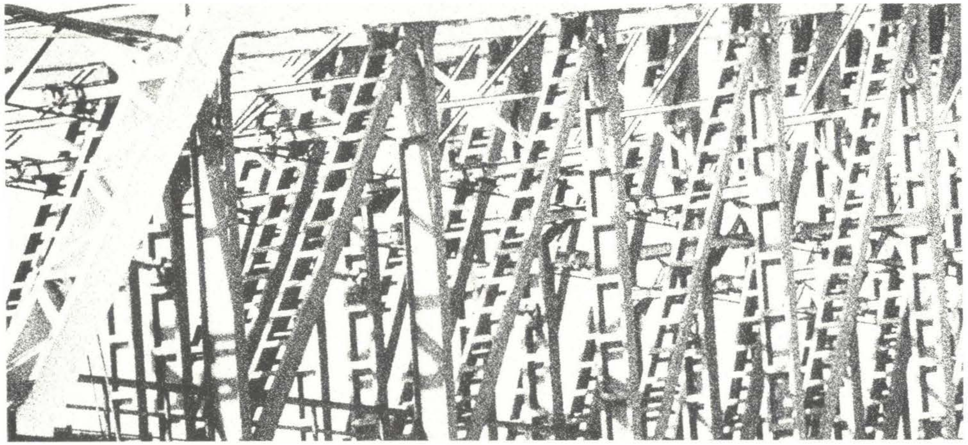
$\dot{\xi}(t) = A\xi(t) + Bu(t) + Cu(t-\tau)$

$\xi, u \in \mathbb{R}^2$

$$A = \begin{bmatrix} -\tfrac{1}{2}\theta^{-1} & 0 \\ 0 & -\theta^{-1} \end{bmatrix}, \; B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 0 \\ c_1 v_0^{-1} & c_2 v_0^{-1} \end{bmatrix}.$$

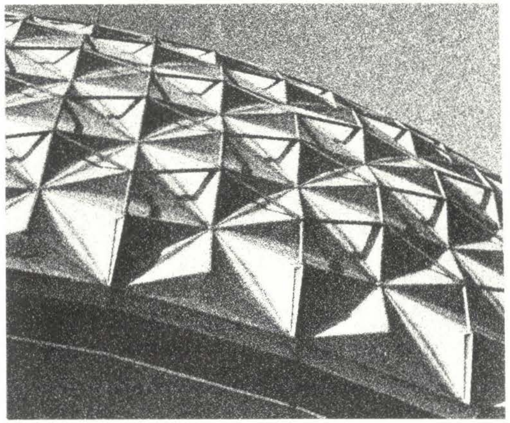


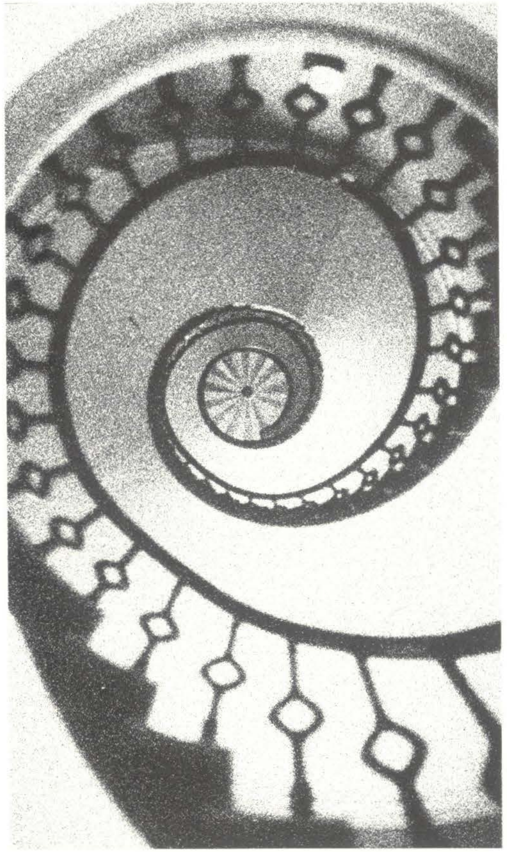


Dome

$\gamma(t)$ a geodesic on surface M

if and only if $\int_a^b <\ddot{\gamma}(t), \eta(t)> = 0$ for all η so that $<\eta(t), n\gamma(t)> = 0$

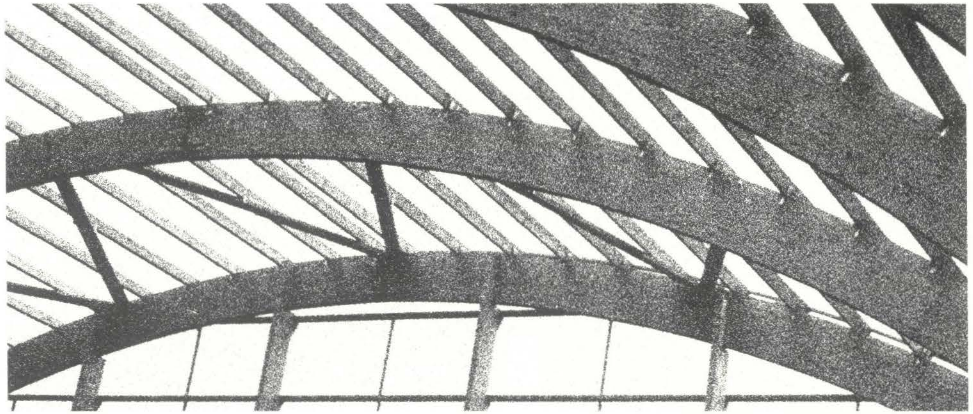




Railroadbridge

$$\max \sum_{i,j} c_{ij} x_{ij} ,$$

$$\sum_j x_{ij} = A_i , \sum_i x_{ij} = B_j$$



$$\tau = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}$$

$$a_{n+1} = a_n + a_{n-1} , a_1 = a_2 = 1$$

(Fibonacci sequence)

Helix

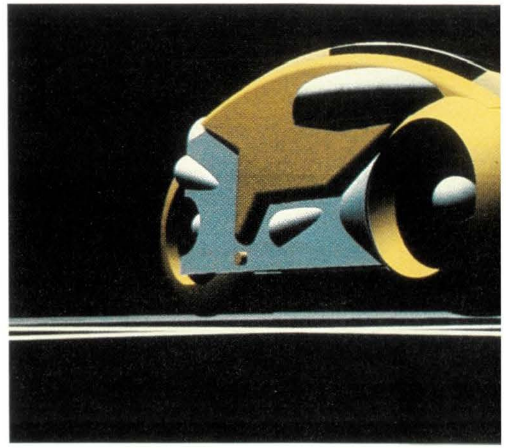
Span

$$\frac{\partial^4 w}{\partial x^4} + p(t)\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial t^2} = q(x,t) - p(t)\frac{\partial^2 w_0}{\partial x^2}$$

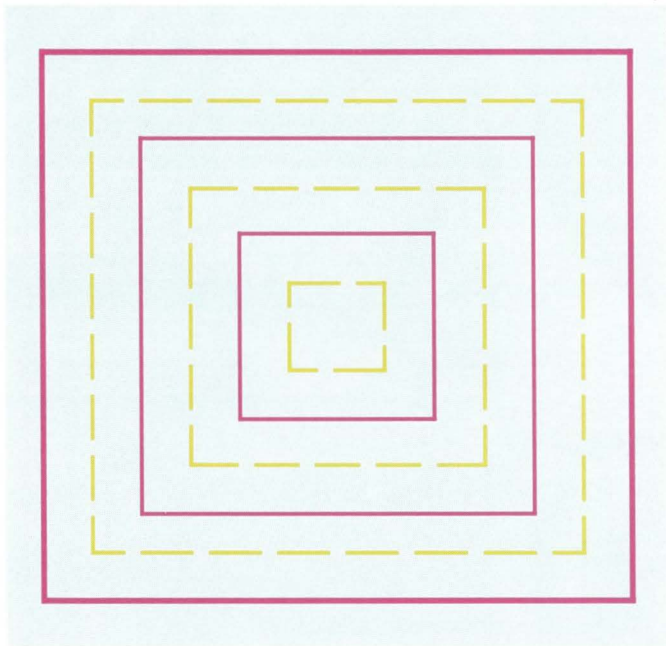
GKS
The new graphic standard GKS employs six elementary drawing commands, including TEXT, POLYLINE (draws lines), POLYMARKER (plots points), and FILLAREA (fills in a region). Their positions are specified by coordinates; the coordinate units can also be specified. For each element, colour, scale factor, size, type, etc. can be defined separately. See, for example, the illustration with the coloured squares. It is also possible to translate, rotate, or change the scale factor for elements already defined. In addition, GKS offers two commands that permit feedback from the user. The first, REQUEST LOCATOR, asks for input from the keyboard that can mark a point from which, for example, a drawing is to begin. The second is used to alter existing drawings. One first puts together a drawing consisting of separate segments, using the instruction CREATE SEGMENT. Then, using REQUEST PICK, one

Computer graphics

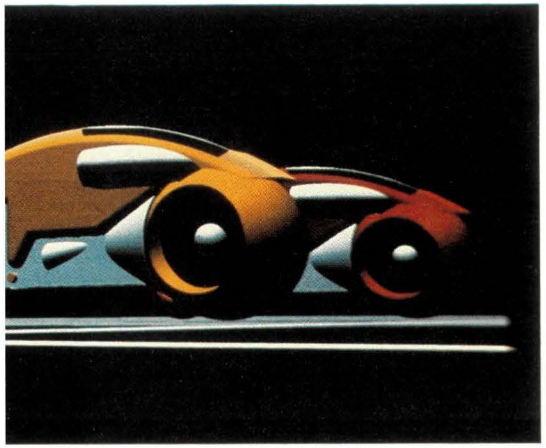
Computer graphics and computer aided design (CAD) are among the fastest growing applications of the computer. Sophisticated computer programs produce high-quality drawings on a screen, often in colour. The objective is to reproduce data, or to present views of structures or objects. Among the advantages of the computer for design work are:
- replacement of a part can be accomplished by modifying the program;
- standard parts can be stored as programs, to be used as desired;
- the drawing can be manipulated through the program. For example, it is possible to show a different perspective of a three-dimensional object by simply recomputing coordinates. Or one can study the influence of forces on a structure (bending,



The motorbikes carrying the electrons in TRON, Walt Disney's animated film that takes place inside a computer. The motorbikes and their

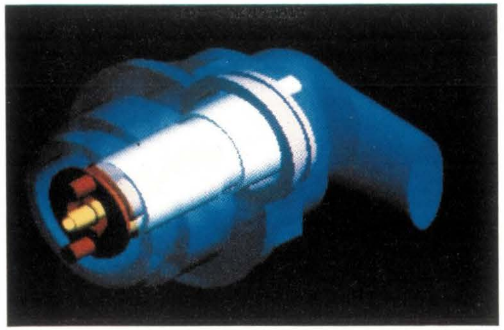


```
SET POLYLINE
REPRESENTATION
   (PLOTTER, INDEX1,
   RED,WIDTH1,
   SOLID);
SET POLYLINE
REPRESENTATION
   (PLOTTER, INDEX2,
   GREEN, WIDTH2,
   DASHED);
j = 1;
FOR i = 1 TO 6 DO
   { j = 3 – j;
      SET POLYLINE
      INDEX(j);
      POLYLINE ([ –i, –i ],
         [ i, –i ] , [ i, i ],
         [ –i, i ] , [ –i, –i ]);
   }
```



movements are simulated by a computer. This kind of simulation plays an important role in the production of science-fiction films.

Working- drawing of a pump motor in its housing.

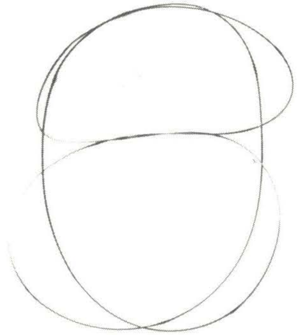


deformation) by simulating the forces through a program and depicting their effects on the structure.

Standardization

Up until now, the market for computer graphics has essentially been dominated by a few American firms. Neither their computers nor their graphics computer languages are interchangeable. This makes the user strongly dependent on the manufacturer of his system, and makes it difficult for concerns wishing to supply programs to penetrate the market. These problems can be resolved through standardization, and the CWI has strongly exerted itself to help in the development of a machine-independent graphics language. In 1977, the International Standards Organization (ISO) established a work group, chaired by a CWI staff member. In 1982, the ISO published a design standard, which is recently accepted. Meanwhile the large manufacturers have already announced their intention to adopt the standard, and CWI has acquired experience in implementing the standardized language on various machines. We plan to make our experience available to the Dutch business community.

can single out a segment to translate, rotate, cut up, cover another segment etc. Thus GKS provides a complete set of instructions for graphics manipulation. The manufacturer must arrange for implementation on his equipment. Many installations will be able to implement only a portion of the standard, for example because the extensive specifications may require too much software overhead. Also, some installations may not permit all possible combinations. For example, a plotter may have only one red pen with a fixed line thickness. GKS can take this into account automatically.

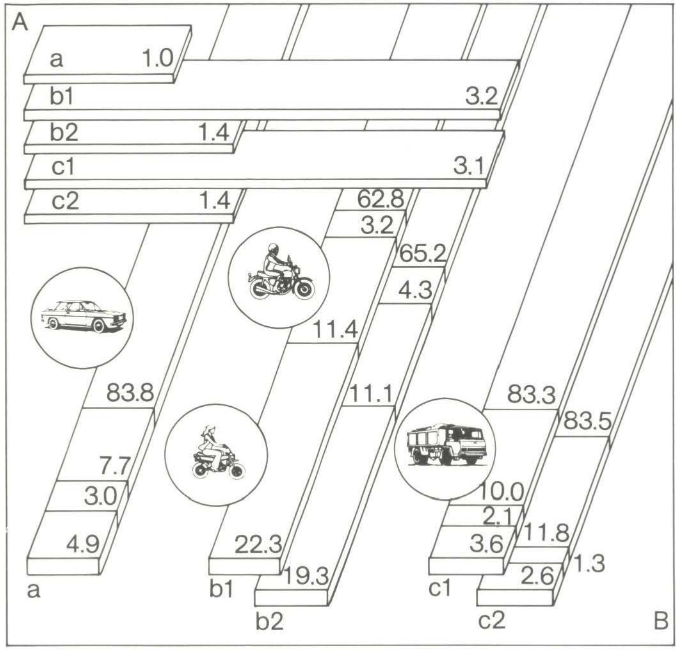


Estimation method
Not all the insurance companies participated in the 1977 survey. It consisted of two experimental samples, the first random, the second focussing on high-claim accidents involving motorbikes. However the damages paid to a number of the victims could not be determined, since the company polled was not liable. In these cases we made a reasonable estimate. This was done by dividing all the cases into groups and subgroups until a division was found that exhibited a certain homogeneity. Payments about which little or nothing was known were estimated by known payments from the appropriate group. All the companies participated in the 1980 survey. Since that was not the case in 1977, a system of 5 categories $C_1,...,C_5$ was developed using analysis of variance, so that it was possible to make good estimates using the average damages and payments from the 1980 figures. This estimate was used for both

Traffic liability

At the request of the Dutch Association of Automobile Insurance Underwriters (NVVA), the CWI conducted an investigation concerning the effects that modifications of the traffic liability law could have on the assessment of damages in personal injury cases. Two alternatives to the present system (legal liability) were proposed: traffic insurance and risk liability. Under the first proposal, every accident victim is fully compensated for damage by his or her own insurance company. The question of responsibility is not taken into consideration. Under the second proposal, victims of multiple vehicle accidents are compensated by the insurance company or companies of the other vehicles involved: the insurance premium covers the increased risk to other drivers due to one's own involvment in traffic. Since in both cases the drivers at fault are also compensated, both alternatives result in higher costs to the insurance companies. These costs can be reduced somewhat by eliminating the right of recourse of the social insurers. This

Chain collision
In multiple-vehicle accidents it is often a monumental task to sort out who was responsible for what. This must be done because the present insurance system is based on liability. Innocent victims are compensated by the insurance companies of the guilty parties; the guilty themselves receive nothing.



Increase in damage payments
A. Cost-increase factors for damages (for the present system, a, the factor is 1). b1 and b2 indicate the increase for traffic insurance with and without right of recourse, c1 and c2 those for risk liability.

B. Distribution of damages in per cent for various types of vehicle (from top to bottom motorbikes, motorcycles, trucks, and automobiles) for each system. Other vehicles make up the difference between the totals and 100%.

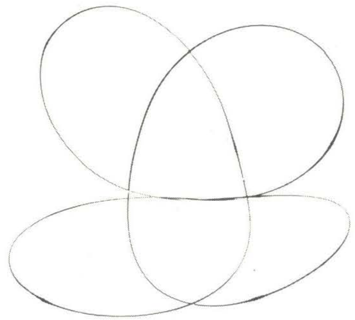
right permits medical insurers, for example, to shift the burden of paying innocent accident victims to the insurance companies of those at fault. Thus we are led to four possible schemes: traffic insurance with or without right of recourse, and risk liability with or without right or recourse.

Approach
In order to arrive at reasonable estimates, figures were gathered for 1977 and 1980 to acquire some insight into the amounts and composition of payments, and the numbers of victims. Given this information, an extensive statistical analysis provided an estimate of the cost increase factor associated with each of the four possibilities. For traffic insurance with right of recourse this came to 2.92, and without right of recourse to 1.31, for risk liability with right of recourse 2.86, and without right of recourse, 1.28. According to an enquiry conducted in several hospitals, a rather high percentage of traffic victims do not report their damages either to the police or to their insurance companies, but probably would do so under the proposed systems. The estimates were adjusted to take this into account, resulting in cost-increase factors of 3.2, 1.4, 3.1, and 1.4 respectively.
The investigation was rounded off with the publication of the GRAS-commission Report (GRAS is an acronym for 'monetary estimates of alternative systems').

parts of the 1977 survey. To accomodate the second, random, part, the accident population was divided into groups G_h, ($h = 1,...,5$). Elements selected from these did not constitute a random sample, but those from the $C_i G_h$ did. Therefore $P(G_h|C_i)$ could be estimated by Bayes' formula:

$$P(G_h|C_i) = P(C_i|G_h)\cdot P(G_h)\cdot \left[\sum_{k=1}^{5} P(C_i|C_k)\cdot P(G_k)\right]$$

(where the $P(G_h)$ are estimated with data from the companies and the other probabilities by counts from the questionaires). The mean in category C_i is now estimated as a weighted average of $C_i G_h$. Since the 1980 questionaire concerned only accidents reported to the insurers, we enlisted the help of the VOR (Accident Registration Service) which has data on all accidents reported to the police, to compile corrected records.



Prediction problems
The branch of mathematics used to solve the prediction problem described on these pages is called systems and control theory. It is devoted to the study of dynamic (time-dependent) phenomena. The most important problems considered are:
1. obtaining system representations;
2. prediction problems;
3. control problems.

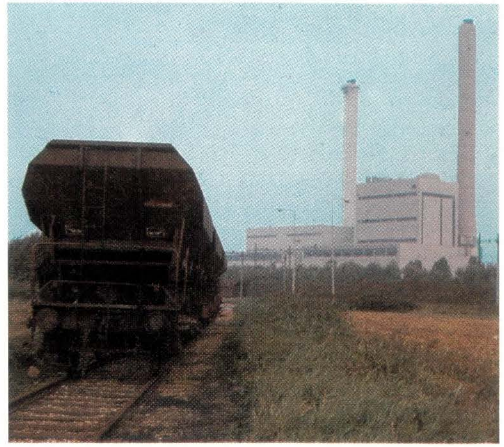
Results from systems theory find their applications in electrical engineering, mechanical engineering, aeronautic and space sciences, and econometrics.

Kalman filter
Suppose the process to be predicted can be represented as the solution of a linear Gaussian stochastic system of the form

$$x(t+1) = Ax(t)+Bv(t),\ x(0),$$
$$y(t) = Cx(t)+Dv(t).$$

The prediction problem is then: to

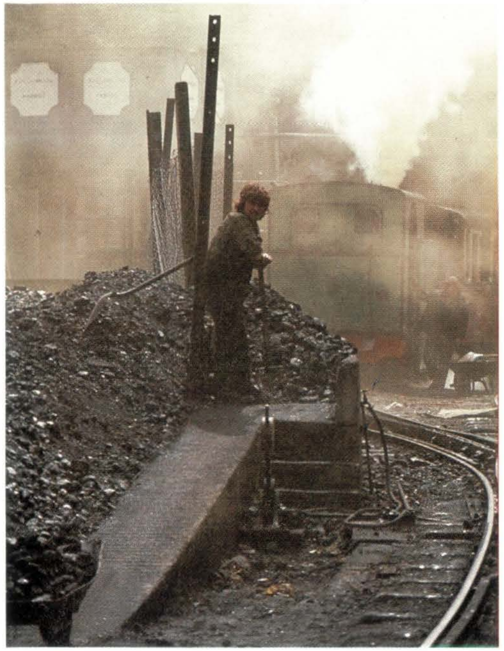
Predicting energy consumption



The Dutch Railway Corporation (NS) called on the CWI to predict the consumption of electrical energy by its substations. This constitutes a portion of a project of the Study and Research Division of the NS, charged with studying the problem of lowering energy costs.

Motivation for the research
The NS uses electricity to propel rolling stock, for light and heat, to operate safety and control systems, etc. The energy is delivered by overhead lines via equally spaced substations. The energy consumption of a substation is usually at its height during the morning and evening rush hours.
The provincial electrical companies base their rates for each substation on both total usage and peak usage. To calculate the latter, consumption is measured at short time intervals, say every ten minutes, and the maximum of the values obtained is used in the cost calculation. The NS is contemplating a plan to lower the cost of electricity. If it were possible to lower consumption during the rush hours, the cost would be less even if the total consumption remained constant. They believe this can be accomplished by storing energy in the hours preceding the rush hours, to be used during the rush hours. In order to be able to make decisions concerning the storage procedures, it is necessary to have estimates of the expected energy consumption during various time periods.

Carrying out the research
The figures for electrical consumption of a substation during 1979 exhibited a certain structure. It was possible to distinguish:
- an hourly pattern, caused by the train schedules;
- a daily pattern, with variations between days caused by, among other things, the weather;
- a weekly pattern, with differences between weekdays and Saturdays and Sundays;
- a seasonal pattern, with heavier consumption in the winter than in the summer.
The eventual model was based on the weekly-daily-hourly patterns. For these, a prediction procedure was developed. The necessary software was mounted and tested on the NS computer by the CWI. The results, after statistical evaluation, were extremely gratifying.



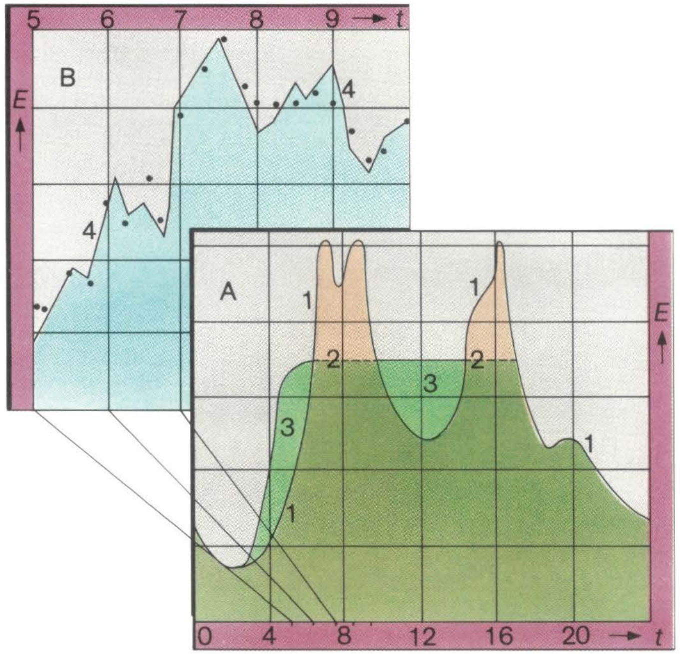
Energy delivery

In the old days, locomotives travelled to coal loading sites to take on energy (right). Today trains carry coal to electrical generating plants, and electrical energy is then delivered via overhead cable (left).

Energy consumption

A. Energy consumption by a substation on a typical day (1). Energy consumption E is measured vertically, and the time from 0 to 24 hours, horizontally. In order to level off the rush hour peaks, energy can be stored in the hours preceding (3). The consumption graph might then resemble (2). To accomplish this, one must be able to predict the times and consumption figures for the peaks.

B. The dots indicate the energy consumption as predicted a quarter earlier by the CWI. The graph (4) indicates the actual consumption.



estimate $y(t+s)$, given $y(0)$, $y(1),\ldots,y(t)$. Under certain conditions the solution is given by the Kalman filter:

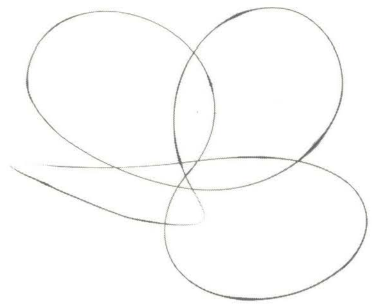
$$\hat{x}(t+1|t) = A\hat{x}(t|t-1) + K[y(t) - C\hat{x}(t|t-1)]$$

$$\hat{y}(t+s|t) = CA^{s-1}\hat{x}(t+1|t).$$

The importance of this filter lies in the fact that the prediction:

1. can be computed recursively
2. is optimal in the sense of least squares.

The prediction algorithm employs an adaptive Kalman filter and produces not only the value of the prediction, but also a reliability interval.



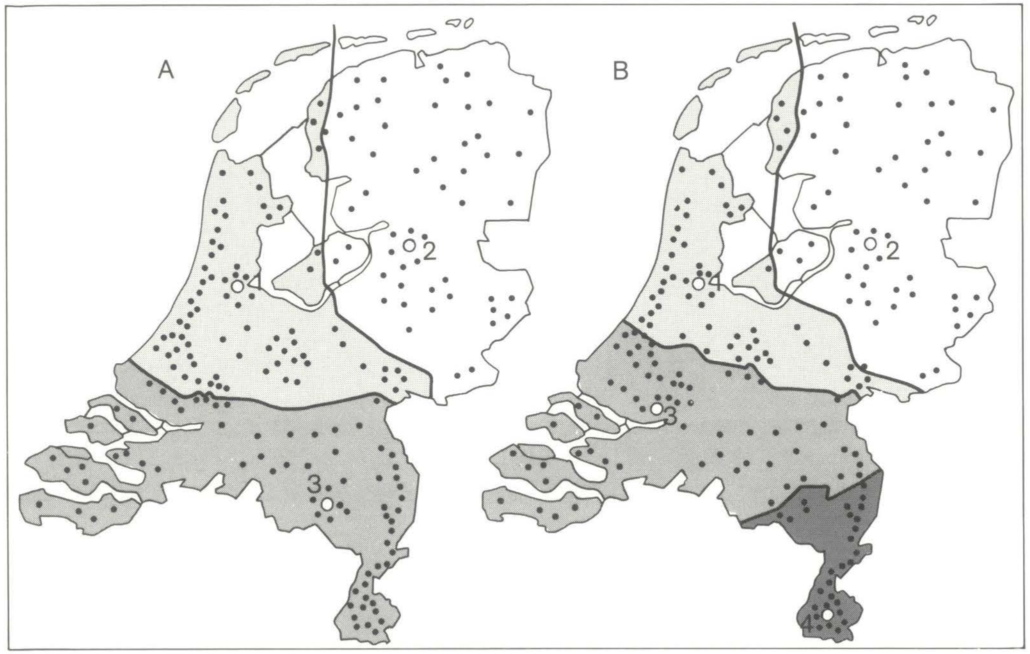
Channel-choice rule
The answer to the question as to which customers should be served directly and which indirectly should be given in the form of a channel-choice rule depending on a small number of customer characteristics. Such a rule can be applied to new customers and to current customers whose purchase pattern have changed. The rule eventually employed was based on the size of the orders of the customer and the demand from customers in his vicinity. These quantities are obviously important. It makes sense to serve a customer directly only if his order is large enough or if there is sufficient demand from customers near him. In addition these quantities are monotonic - so that a customer will be considered for direct delivery to the extent that his orders increase - and do not depend on the yet to be determined distribution network. The size of a customer's order is clearly defined. The demand in his vicinity is related to the cost of

Distribution of goods

The costs of distributing goods are often substantial. Depending on the type of industry, they can amount to 15 or 20% of volume. AGA Gas, Inc., producer of industrial gasses, consulted the CWI to find a more efficient distribution system. The existing system involved four distribution centres, from which trucks made deliveries to some hundred depots, themselves independent operators. The majority of customers (indirect customers) placed their orders at a depot. Some indirect customers picked up the goods themselves from the closest depot. Some clients (direct customers) were served directly from the distribution centres, in which case no commission had to be paid to a depot. Ordinarily the total transportation costs were higher for direct deliveries than for indirect.
Often the sizes of the orders were such that one truck could serve several depots or direct customers before returning to the distribution centre. If necessary, a truck could make several trips a day.

Toward a new structure
AGA provided a list of about 20 locations where distribution centres could possibly be established. In addition they presented a number of possible structures for the placement of depots. The number of depots varied from 45 to 200, depending on the structure. These data formed the basis for the design of a better distribution system.
In addition the trucks had to be provided with a certain built-in overcapacity, so

Truck
One of the approximately 40 trucks of the AGA fleet in the Netherlands, ready to depart from the grounds of AGA Gas, Inc., Distelweg 90, in Amsterdam North. Trucks like these make deliveries to direct customers and depots. Deliveries from depots to indirect customers are made with smaller trucks. As a consequence, total transportation costs are usually lower for indirect customers than for direct customers.



Distribution structures
Two of the combinations of distribution centres considered, with the regions that each centre, according to CWI calculations, could serve most advantageously. The dots indicate the delivery points (depots or direct customers) assigned to the distribution centres.
A System with three centres: Amsterdam (1), Zwolle (2), and Eindhoven (3).
B System with four centres: Amsterdam (1), Zwolle (2), Alblasserdam (3) and Nuth (4).

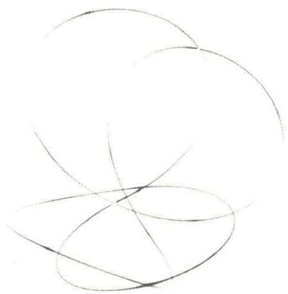
they would not have to make an extra trip if a client or depot wanted a little more on a given day, while on the other hand the trucks were not constantly running half empty.

The CWI was able to answer the following questions.

1. What is the most desirable number of distribution centres, and where should they be located?
2. What region of the Netherlands should each centre serve, and what should its capacity be?
3. Which customers should be served directly, and which indirectly?
4. How many depots should there be?
5. What routes should the trucks follow in order to serve the largest number of customers and depots in the least time?

The structure discovered by the CWI differed considerably from that currently in use, and would result in a saving of about one million guilders a year. Naturally the existing system cannot be changed suddenly, but the company will attempt to switch gradually to the structure recommended by the CWI.

delivering a full truckload to customers in his area, beginning with himself. As these costs decrease, the customer will be more favourably considered for direct delivery. The costs are computed for each customer separately by solving a **travelling salesman problem** with side conditions; this can demand a great deal of computing time. Therefore the computation was based on a relaxation of the travelling salesman problem, the **spanning tree problem,** which is easy to solve and gives a reliable estimate of the costs in the travelling salesman problem. In order to obtain a workable rule for the firm, research was restricted to rules with the following structure: customers with 'large' orders are served directly, customers with 'small' orders indirectly; the remaining cases are served directly if there is 'sufficient' demand in their vicinity. The research consisted in deciding the appropriate meanings of 'large', 'small', and 'sufficient'.



Knapsack
Someone wishing to receive messages coded according to the Knapsack method openly publishes a list of, say, 256 large numbers. Whoever wants to send a message first writes it in a binary code, using for example the ASCII code. The resulting sequence of bits, **1101...** is then split into groups of 256. To code such a group, one adds up the corresponding numbers from the published list. For **1101...**, for example, we add the first two numbers, skip the third, add in the fourth, etc. Finally, the sum is tansmitted.
To decipher the message, an interceptor must discover how the number can be written as a sum of numbers from the published list. Trying out all possibilities is clearly impractical, but even the best systematic methods known would require, on the average, millions of years of computer time. The possessor of the code, on the other hand, can decode the sum with his list. His basis list consists

Cryptography

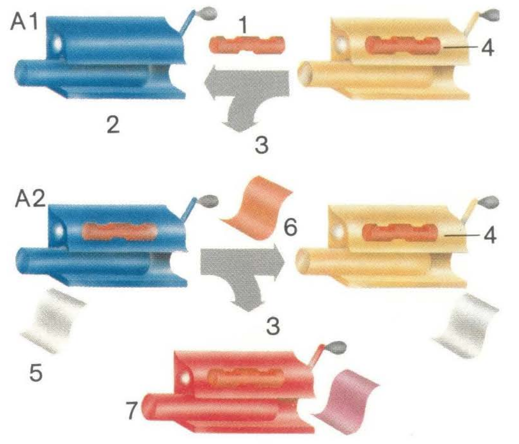
All cryptographic systems (codes) are based on a coding key and a decoding key. In the classical system these keys are so closely related that knowledge of one makes the other easy to find. In the American 'data-encryption standard' the two are in fact identical. When two principals wish to communicate in code, the key must somehow be transmitted from one to the other. In the diplomatic world this is done by courier, not a practical alternative for commercial traffic via electronic media. Recently the CWI developed a modern ('public key') system for a bank that eliminates the problem.

New developments

Modern coding keys are no longer secret, they can even be openly published. Anyone who wishes to communicate with the constructor of the code can do so by using the key. But to decode a message the decoding key is necessary, and that is strictly secret, usually buried in the safe or the computer of the code constructor. So the trick is to devise a system for which the decoding key is difficult to deduce from the coding key.
Suppose we have a machine that can assume 26 different states and, depending on its input, mangles, grinds, crushes, and mixes successive incoming letters. Even if everyone is familiar with this machine, it is not at all clear how he could reconstruct its input, given its output. However, the creator of the machine has designed not only the publicly known grinder, but also a secret 'inverse' machine that can reverse the process, that is, can decode the code produced by the first machine. Several concrete realizations of such systems have been developed. One of them, the 'knapsack-system', will be described here.

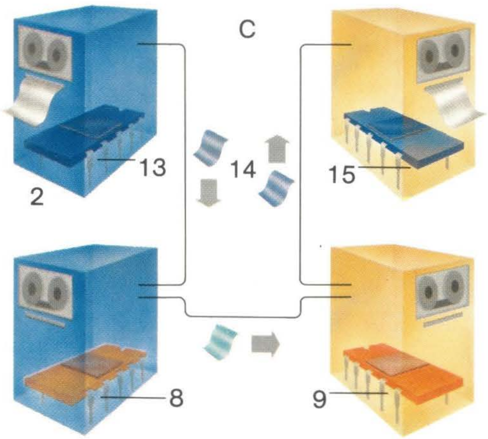
Double codes

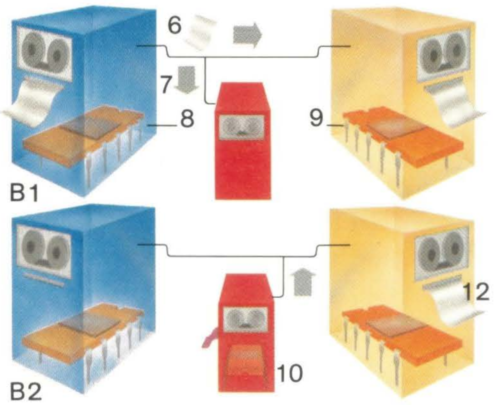
In many applications the sender of the message must be able to identify himself positively. For example, some transactions are not legally binding without a signature. Certain coding systems can be



A1. Older codes required that the coding key (1) be delivered to the coder (2). In case of interception (3) the decoding key (4) can be deduced from the coding key.
A2. A message (5) is coded to produce a coded message (6). An intercepted decoding key (7) can decode the message just as easily as the original key (4).

C. In double coding, the sender (2) first applies his own decoding key (13) to the message, producing a code (14) which he encodes with the receiver's coding key (8). To decode the message, the receiver first applies his own decoding key (9) and then the sender's coding key (15). Both (9) and (13) are strictly secret, and both are needed to transmit the message.





B1. In modern systems, the decoding key (8) cannot be deduced from the coding key (9). Hence a possible interception (7) of the coding key and message (6) is harmless.

B2. It is possible for an outsider (10), using the public coding key, to send bogus messages. These cannot be distinguished from genuine messages by the receiver (12).

used to produce an 'electronic signature'. In principle this requires a two-fold coding process, the open coding of the receiver and then once again a secret decoding by the sender. Since the sender is the only one who knows his decoding process, the message acquires a form that can be produced only by him, and hence can be unambiguously identified (see figure C).

of a sequence of rapidly increasing numbers, for example

7, 50, 338, 1001, $\cdots$.

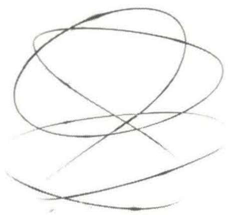
With these numbers, the code **1101** yields the sum 1058, from which the code 1101 can be immediately recovered. However, the owner does not publish this list as it stands, but first transforms it using three large numbers p, q, and m (where m is larger than the largest number in the list), satisfying the condition

$$p{\cdot}q \equiv 1 (\text{mod } m),$$

that is, $p{\cdot}q$ is $1+$a multiple of m. With $p=123$, $q=4472$, and $m=1001$, we have $p{\cdot}q = 55056 = 55 \times 10001 + 1$. The owner now replaces each number in his basis list by $p{\cdot}q$ (mod m), that is, the remainder obtained when $p{\cdot}q$ is divided by m. In our case this gives

861, 6150, 1570, 3111, $\cdots$.

The sender now codes **1101** and 10122. The owner multiples 10122 by q and divides by m, and uses the remainder, 1058, to recover the code **1011** from his original list.

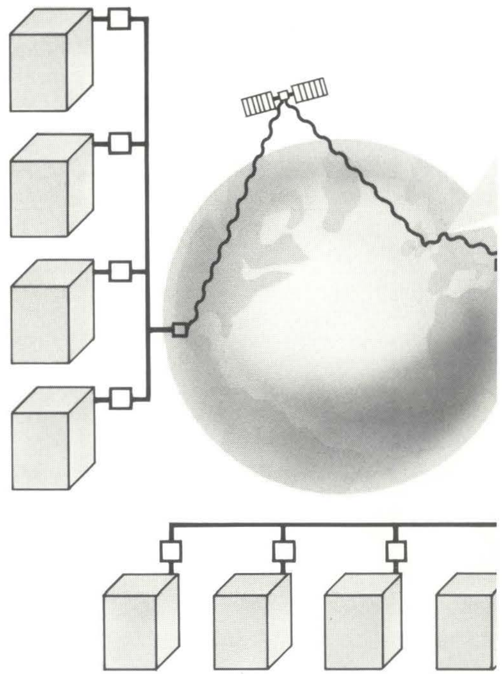


Computer networks

In the next few years, computer networks will become more and more important. The CWI is very active in this area, and is developing several different facilities.

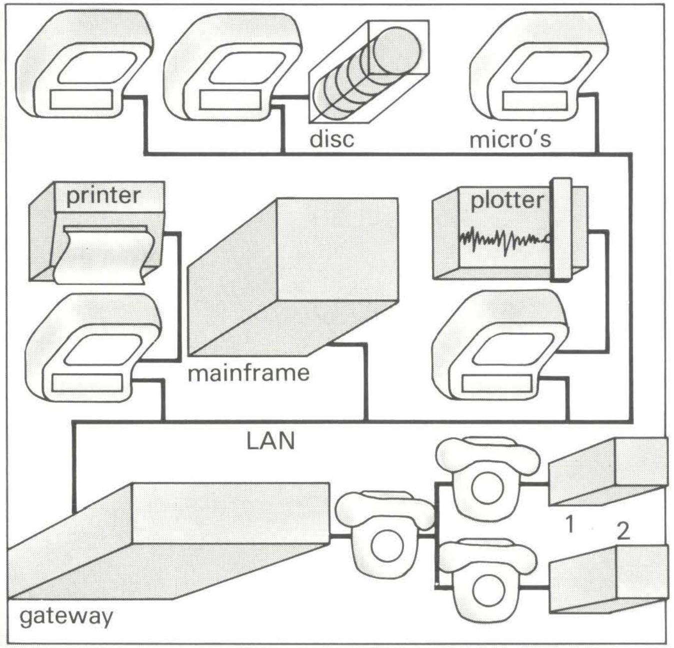
Global networks
First of all there is the Long-distance Network Service, which provides entry to computers in the US and Europe. Here the CWI acts as a 'gateway', providing access to a large number of existing networks (including Arpanet, Telenet, Tymnet, Dabas, and the public telephone network). The network can be accessed by all computers employing the UNIX operating system. Using a modem and a telephone, one first contacts the CWI, which in turn establishes communication with the desired computer. The user pays only the cost of a phone call to the CWI, plus his actual share of the long-distance costs - a small fraction of the cost of membership in one of the networks. It is possible to transmit files, have programs run elsewhere, exchange electronic mail with another user, or to send and receive electronic publications (a kind of computer news service). Messages can be tagged with a classification code, so that subscribers can specify the types of publication they wish to receive. This permits a suitable selection from the large amount of material available (currently about 1 Mbyte, or 200 pages, per day).

Local networks
The rise of the microcomputer makes it possible to provide each user or user's group with a made-to-order computer. The current system, one large general-purpose computer with many terminals, will gradually be superseded, since the micros provide a larger calculating capacity for less cost. Micros in one building or building complex can communicate with each other and make efficient use of peripheral equipment through a Local Area Network (LAN) Th central computer manages the use of peripheral equipment such as disc drives to store large amounts of data, fast printers, execution of graphics, etc. For extensive calculations exceeding the capacity of the micros, one can connect u with large computers (number crunchers). In addition, it is possible to tie into a



Collison detection
Ethernet employs a simple coaxial cable to which at most 1024 connecting stations can be coupled. Traffic is managed by CSMA/CD, Carrier Sense Multiple Access with Collision Detection. Before a message is sent, the system first checks to see if the cable is already in use (carrier detection). If it is not, the message is sent and the cable is not accessible to the other stations. However, some time elapses before the message shuts off stations further down the line. If two stations send a message at (essentially) the same time, the two messages 'collide', rendering both unusable. This situation is monitored, and as soon as the sending station senses a collison (collison detection), the station attempts to send the message again, after a randomly chosen time delay so that both stations do not repeatedly attempt to use the net simultaneously. If another collison is detected, the next time delay is doubled; after a successful

LAN
CIW's local network makes it possible for participating micros and mini's to communicate with each other and to make common use of peripheral equipment installed elsewhere, such as discs, printers, and plotters. In addition, they can be put through to a large computer, or, via gateway, with computers elsewhere. By means of the telephone and modems, others (1,2) can also make use of the gateway.



transmission, the time delay is again set at zero.

Capacity
Clearly Ethernet does not have unlimited capacity. Under heavy traffic conditions stations must wait longer before the cable is free, and the probability of collisions increases. With less than 1000 users there is almost no delay, even with heavy traffic. Starting at two or three thousand users (several users can use one station) the delays increase rapidly. A simulation with 3000 users yielded an average waiting time of 1/10 s (with an average of 13 attempts), and the net was about 70% occupied.

Global network
An operational global network makes it possible to hook up with computers in a large part of the world, at low cost and with almost no capital investment. The network utilizes existing telecommunication facilities, including satellites.

Long-distance Network, as previously described.
CWI plans, in the near future, to replace some of its minicomputers with a large number of micros connected by the Ethernet network. As soon as the Centre has acquired sufficient experience with this innovative system, it will place its knowledge of the relevant hardware and software at the disposal of others who may be considering similar large scale office automation.

Differential equations
The hydrodynamic problem of determining the influence of the wind on the water levels in the North Sea can be described mathematically in the following simplified but realistic form. Represent the sea by a region in the (x,y) plane, part of whose boundary represents the coastline. The velocity (u,v) of the water and its height ζ, as functions of the three variables x,y and t satisfy a system of three partial differential equations whose linearized and normed version is

$$\left(\frac{\partial}{\partial t}+\lambda\right)u - \Omega v + \frac{\partial \zeta}{\partial x} = U$$

$$\left(\frac{\partial}{\partial t}+\lambda\right)v + \Omega u + \frac{\partial \zeta}{\partial y} = V$$

with the continuity equation

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial \zeta}{\partial t} = 0$$

where (U,V) is the shearing caused by the wind, λ a coefficient of friction, and Ω the Coriolis coefficient, $\Omega = 2\omega \sin\phi$, where ω is the speed of rotation of the earth

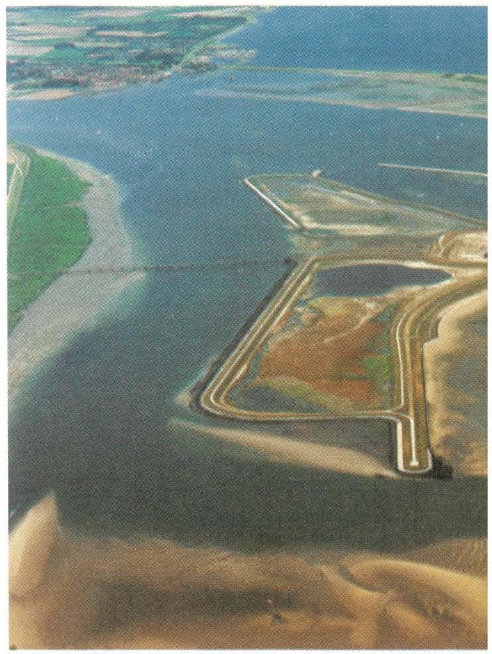
The North Sea project

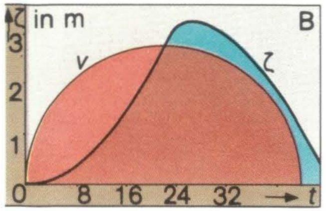
Following disastrous floods on February 1, 1953, the Dutch government created the Delta Commission. Its charge was to propose measures to prevent a repetition of the disaster. The Commission called on various scientific institutes for advice, among them the CWI. In its final report, the Commission proposed that four of the six sea arms in the province of Zeeland be closed off, and the dikes be raised on the remaining two, which provide access to the harbours of Rotterdam and Antwerp. The contribution of the CWI can be divided into three parts:

1. Organizing the statistical data on the distribution of water levels.
2. Determining the height of the dikes to be strengthened and constructed.
3. Determining the influence of wind and tide on the water levels in the North Sea.

Shallow water model
A highly simplified model of the North Sea was developed to study the effects of a storm on the water level. The North Sea was represented by a rectangular reservoir of constant depth, bounded on three sides by impermeable coastline and on the fourth by an infinitely deep ocean. Oversimplified as such a model may appear, it led to new insights (sometimes completely unexpected), though largely qualitative in nature. As computers became available, it was possible to refine the model. A computer program was developed that served to predict water levels. In recent years this investigation, undertaken in the sixties, is again attracting attention. This is partly because of off-shore oil exploration, but the CWI has also had requests from Italy for help in calculating the rise in water level in the Adriatic (the Venice problem) and from India concerning the harbour works in Calcutta. The original programs are now being revised and adjusted to take advantage of the latest calculating techniques.

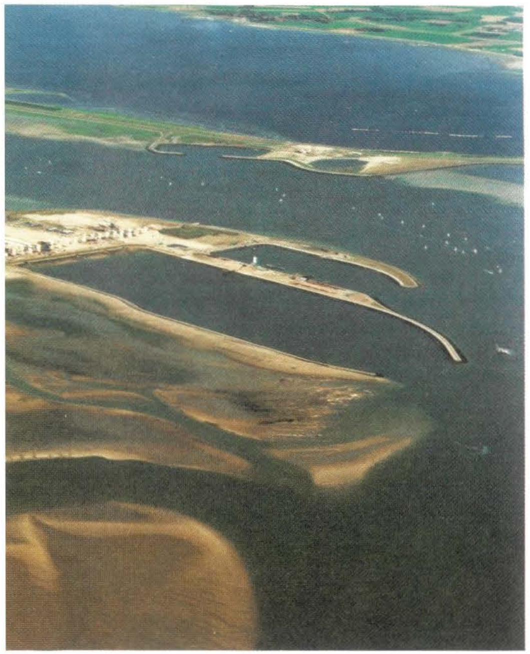
The work island 'de Krammer', and in the background the Grevelingen dam between Goeree Overflakkee and Schouwen Duiveland. Work islands are set up on existing sand banks to prepare components of dams and bridges. Some work islands serve as a jumping-off place for damming deep channels.

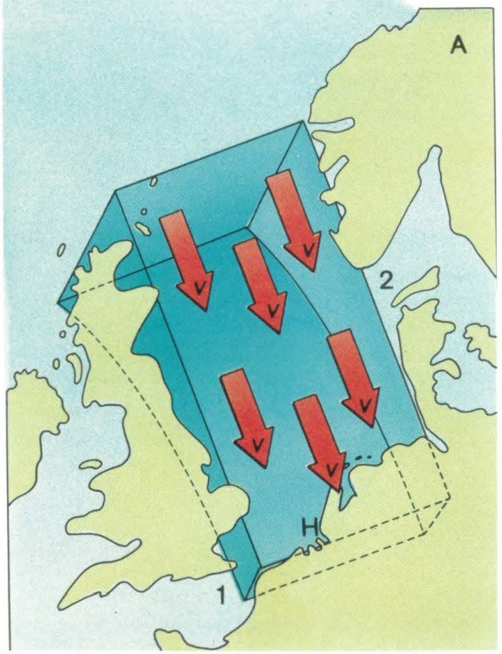




B. Results of a calculation taking into account the Coriolis force, among others. It was assumed that the wind velocity (v) increased gradually (uniformly over the whole reservoir) to 30 m/s, and then decreased again. The line ζ shows the water level at Hook of Holland (H). A few hours after the maximum wind velocity the water had risen to 3.20 meters.

A. In the simplest model, the North Sea was represented as a rectangular reservoir about 400 km wide, 800 km long, and 65 m deep. Irregularities in the coastline were ignored, as were the influence of the English Channel (1), the Kattegat (2) and the river mouths. The Coriolis force was not taken into account, and the frictional forces were replaced by linear approximations. At a later stage, we were able to take account of the Channel, the Kattegat, the Coriolis force, variable depth (as pictured) and the variability of the wind velocity.





and ϕ the latitude. To analyse this system further, one must apply a Laplace transform with respect to t; thus

$$\bar{\zeta}(x,y,p) = \int_0^\infty e^{-pt}\zeta(x,y,t)dt$$

and analogously for u,v, and U,V. One then finds an equation for $\bar{\zeta}$ to which a great deal of attention is given in the research:

$$(\Delta-\kappa^2)\bar{\zeta} = \bar{F}$$

$$\kappa^2 = p(p+\lambda)+p\Omega^2/(p+\lambda),$$

an inhomogeneous Helmholtz equation, in which $\bar{F}$ depends on the wind field. The facts that the water level of the ocean remains constant and that the normal component of the water velocity along the coast is zero are represented by boundary conditions.

Credits

The Mathematical Knot

The second-simplest knot from an infinite sequence of knots that spontaneously assume a three dimensional configuration with minimal energy. Discovered and produced by Joel Langer (J. Langer, Thesis, University of California at Santa Cruz).

The topological invariant:

$$\pi_1(\mathbb{R}^3 - K) = < x,y,z : y^{-1}xyx^{-1}y = x^{-1}zx^{-1}zxz^{-1}x, x^{-1}zxz^{-1}x = y^{-1}zyz^{-1}y >$$

Cover

Illustration	:	Birth of a bottle with no inside (Klein bottle). From a computer simulation by Steven Feiner, David Salesin, and Thomas Banchoff. See 'IEEE Transactions on Computer Graphics and Applications', September 1982.
Slide	:	ACM SIGGRAPH
Design	:	Toine Post

Drawings : MATRIX; pages 18/19 and 20/21 Hans van Leeuwen; others Armand Haye

Slides and photos

p. 10, top	:	Walt Disney via ACM SIGGRAPH
p. 11, bottom	:	P. Atherton via ACM SIGGRAPH
p. 12	:	Anefo
p. 16	:	AGA BV
p. 22	:	Bart Hofmeester/Aerocamera
others	:	MATRIX

Text, design, layout and production : MATRIX, Amsterdam

Typesetting : Phototypesetting staff CWI, especially Mrs. Nada Mitrović

Printing : Mart Spruyt BV

Research

Modelling

Simulation

Software

Implementation

Courses

Consultation

Documentation