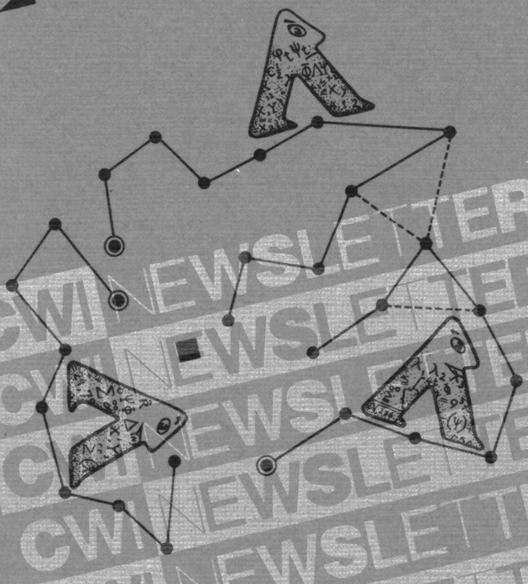
CWI NEWSLETTER

CWI
Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

Quarterly, Issue no. 7
June 1985



CWI NEWSLETTER

Number 7, June 1985

Editors

Arjeh M. Cohen Richard D. Gill Jo C. Ebergen

The CWI Newsletter is published quarterly by the Centre for Mathematics and Computer Science (Centrum voor Wiskunde en Informatica), Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. The Newsletter will report on activities being conducted at the Centre and will also contain articles of general interest in the fields of Mathematics and Computer Science, including book reviews and mathematical entertainment. The editors encourage persons outside and in the Centre to contribute to the Newsletter. Normal referee procedures will apply to all articles submitted.

The Newsletter is available free of charge to all interested persons. The Newsletter is available to libraries on an exchange basis.

All correspondence should be addressed to: *The CWI Newsletter, Centre for Mathematics and Computer Science, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands.*

ISSN 0168-826x

Contents

CWI

Centre for Mathematics and Computer Science
Centrum voor Wiskunde en Informatica

Second Order Approximations [1]

Willem Albers
University of Limburg
P.O. Box 616
6200 MD Maastricht

Before embarking on a discussion of second order approximations, it is perhaps a good idea to first say a few words about the need for such approximations. To begin with, we would of course prefer to use exact results only. However, it turns out that in statistics this is very often not feasible, which forces us to settle for some kind of approximation. Typically such an approximation is of an asymptotic nature. Consider for example the following situation: we are interested in some characteristic of a random quantity, such as the mean value of the performance of a particular medical treatment, or the variance of a new method for weighing items of a given type. To obtain the desired information, we draw a sample $X_1,...,X_n$, that is, we collect n independent measurements of the quantity under consideration. From these we evaluate an appropriate function $T_n = T_n(X_1,...,X_n)$ for our purpose, which could e.g. be testing or estimation. Then a result like:

$$T_n \text{ is } \mathrm{AN}(\mu_n, \sigma_n^2) \qquad (1)$$

where 'AN' stands for 'asymptotically normal' and μ_n and σ_n^2 are the known mean and variance of this normal distribution, will provide us with first order approximations to the quantities which are of interest for assessing the quality of the procedure we use. For an estimator this could be its variance and for a test its size and power (which stand for the probability of rejecting the null hypothesis when it is true and when it is not true, respectively). To be just slightly more precise, (1) can be stated equivalently as

1. This paper was presented at a meeting organized by the Mathematics Department of the University of Leiden on the occasion of the honorary degree in mathematics which was awarded by this University to Professor Erich L. Lehmann on February 8, 1985.

$$P(\frac{T_n - \mu_n}{\sigma_n} \leqslant x) = \Phi(x) + o(1), \tag{2}$$

where Φ stands for the standard normal distribution function. Establishing a second order approximation now entails replacing the '$o(1)$' in (2) by 'something better'. (You see that technicalities are ruthlessly estimated!) A first obvious advantage of this additional effort will be that the numerical approximations will typically improve.

The approach above is rather single-minded in the sense that one single statistic at a time is considered. Usually, we are interested not in a particular statistic, but in a particular statistical problem, for which as a rule several statistics present themselves as possibilities on which to base the solution. Moreover, quite often several of these candidates are first order equivalent. That is, the same result (2) (with the same μ_n and σ_n) holds for all of these statistics. At first sight, this looks delightful: as long as the good choices are equivalent, it does not matter much which one we pick. However, the same objection as above applies: the equivalence holds to first order only and the finite sample behaviour of the statistics may (and in fact often does) differ quite a bit.

It is to this problem that Professor LEHMANN, together with Professor HODGES, drew attention with admirable clarity in his 1970 paper in the *Annals of Mathematical Statistics* with the concise title 'Deficiency'. We shall now briefly review the main idea and some illustrative simple examples from this paper. Suppose we are given two statistical procedures A and B for a certain statistical problem. For simplicity of presentation, let us assume that it is known beforehand that A is the better of the two. For each $n = 1,2,...$, we can determine the number k of observations which is needed by the poorer procedure B to match the performance (e.g. reach the same power or the same variance) of procedure A when based on n observations. Clearly $k \geqslant n$, and since it will depend on n, we shall denote it by k_n. Typically, people have been studying the behaviour of the ratio

$$e_n = \frac{n}{k_n} , \tag{3}$$

which is called the relative efficiency of B with respect to (wrt) A. Quite often it can be shown that e_n tends to a limit e, which is called the asymptotic relative efficiency (ARE) of B wrt A. Now HODGES and LEHMANN point out that it would be more natural to study the difference $k_n - n$, rather than the ratio in (3). They call this difference, which is nothing but the additional number of observations required by the poorer procedure, the deficiency d_n of B wrt A. And in analogy to the above, its limit d, if it exists, is called the asymptotic deficiency of B wrt A.

Note that this discussion is a bit deceptive in the following sense: it may be true that a difference is more natural to study than a ratio, but it is also true that it is more difficult to handle. In fact, first order results like (2) suffice to evaluate e_n and e, but for d_n and d second order approximations are required.

Consequently, before going on, it makes sense to figure out in which cases efficiencies suffice and in which cases the additional effort involved in obtaining deficiencies is worthwhile. A situation of the first kind arises when $e < 1$. Then it is already clear which of the two procedures is superior and information on d_n is at most useful to improve the numerical approximation. If $e=1$, however, the opposite situation occurs. Then the two procedures are first order equivalent and d_n (and possibly d) are vital in finding out which of the two is best, and by how much the poorer one falls short of the better one. Hence in what follows we shall concentrate on cases where $e=1$.

A first, very simple example, is the following. Let $X_1,...,X_n$ be a sample from an unknown distribution function F with mean ξ and variance σ^2. To estimate σ^2, two obvious estimators are available:

$$M_n=\frac{1}{n}\sum_{i=1}^{n}(X_i-\xi)^2 \ , \quad M_n'=\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\overline{X})^2 \ , \tag{4}$$

where $\overline{X}=n^{-1}\sum_{i=1}^{n}X_i$. Clearly if ξ is known, we should use the first, and if ξ is unknown, we should use the second estimator. Quite often, however, we are somewhat 'in between': a value of ξ is available, but its reliability is not above all suspicion. Using M_n if the value of ξ is false can be disastrous; using M_n' if the value happens to be correct is a bit wasteful. Consequently, it is a robustness question we are facing: what is the price we may have to pay for the protection afforded by using M_n' rather than M_n?

This question can be nicely answered by using the deficiency concept. It turns out that the variances V_n and V_n' of the unbiased estimators in (4) equal

$$V_n=\sigma^4\frac{\gamma}{n} \ , \quad V_n'=\sigma^4\frac{\gamma(n-1)+2}{n(n-1)} \ , \tag{5}$$

where $\gamma=(\mu_4/\sigma^4)-1$, with μ_4 the fourth central moment of F. By elementary computations it follows from (5) that $e=1$ (hence we indeed have the interesting case of first order equivalence!) and moreover that d_n tends to a finite limit

$$d=\frac{2}{\gamma} \ . \tag{6}$$

If $F=\Phi$, we have that $\gamma=2$, and thus one additional observation is all we have to pay for the robustness in the normal case. This is not such a big surprise after all, since the estimators in (4) are in that particular case following χ_n^2- and χ_{n-1}^2-distributions, respectively. But (6) holds true in general. In practice F will quite often be slightly heavier-tailed than the normal, which results in $\gamma > 2$ and therefore in a value of d which is less than one. Incidentally, a possible interpretation of such a broken value of d can for example be provided by means of stochastic interpolation: use $n+1$ observations with probability d and n observations with probability $1-d$.

A second elegant example, also taken from the 'Deficiency' paper, is concerned with a related problem. Again $X_1,...,X_n$ is a sample from a distribution with mean ξ and variance σ^2, but here we assume the distribution to be normal. Instead of estimators we are now going to compare two test statistics. The testing problem involved is the classical $H_0 : \xi = 0$ against $H_1 : \xi > 0$. We can either use the test based on the sample mean $\overline{X}$ or Student's t-test. In the first case we reject if

$$\frac{n^{1/2}\overline{X}}{\sigma} \geqslant u_\alpha = \Phi^{-1}(1-\alpha) , \tag{7}$$

with α the size of the test. In the latter case we reject if

$$\frac{n^{1/2}\overline{X}}{(M_n')^{1/2}} \geqslant t_\alpha , \tag{8}$$

where M_n' is as in (4) and t_α is the upper α-point of the t-distribution. Note the analogy to the first example, the only difference being that the role of ξ and σ has been interchanged. Hence the issue now is whether we should rely on possible information about σ or use the t-test all the time. Again a nice answer is provided by the application of deficiencies. HODGES and LEHMANN demonstrate, using an elegant conditioning argument, that not only $e = 1$ but that the deficiency tends to the finite limit

$$d = \frac{u_\alpha^{\,2}}{2} , \tag{9}$$

with u_α as in (7). For $\alpha = 0.01$, 0.025 and 0.05 respectively, this leads to $d =$ 2.706, 1.921 and 1.353, respectively. Hence a very moderate number of additional observations suffices to achieve the desired robustness against deviations of σ. Of course these results are of an asymptotic nature, but it has also been demonstrated for this example that already for sample sizes as small as $n = 4$ and 8 a beautiful agreement with the exact values exists.

Summarizing the above, we can conclude that HODGES and LEHMANN have made a very nice point in their paper and have done so with great clarity. But this is by no means the end of the story. Even more important perhaps is the fact that their paper has stimulated a lot of further research. The authors encouraged this development by stating a number of questions at the end of their paper. Now it is well known that one fool may ask more than ten wise men can answer, but fortunately in this case two wise men have apparently succeeded in coming up with such questions that it has turned out worthwhile rather than foolish to try to answer them!

In the remainder of this paper we shall take a look at some of these questions and try to give an impression of what progress has been made in finding answers. The general background of the questions is more or less the following. As we have seen, the evaluation of deficiencies requires second order approximations. In a number of non-standard areas the derivation of such approximations presents serious technical difficulties. These have to be overcome before the often quite interesting application to deficiencies can be made.

The first question we consider is of the following nature. As we saw in (9), the asymptotic deficiency $d_{t,\overline{X}}$ of the t-test wrt the $\overline{X}$-test is finite and equals

$u_\alpha^2/2$. What happens if we do not stop at scale invariance but in addition require distribution-freeness? For example, would the asymptotic deficiency $d_{NSc,t}$ of the normal scores test, which is the best rank test for the normal case, wrt the t-test be finite? And if not, at what rate would the deficiency tend to infinity? Note that this is a 'good' question in the sense that $e_{NSc,t}$ is known to equal 1. This itself came as a bit of a surprise originally, as people at first used to think of rank tests as 'quick-and-dirty' methods, which probably sacrificed a lot of efficiency in exchange for their ease of application. Now that we know that this is not the case, at least to first order, we become eager for more and hope to show that the loss incurred is small to second order as well.

The second question is of a similar spirit: can rank tests be concocted which are second order equivalent wrt their parametric competitors, i.e. which have $d=0$? Finally the third question we shall consider is about the relationship between tests and estimators. Suppose that for a problem two test statistics T_1 and T_2 are given and that each of these statistics gives rise to an estimator, say $\hat{\theta}_1$ and $\hat{\theta}_2$, respectively, for the parameter of interest. Then it is well-known that typically the efficiency results for tests and estimators coincide, i.e. that

$$e_{T_1,T_2} = e_{\hat{\theta}_1,\hat{\theta}_2} \,. \tag{10}$$

The question then is whether a result like (10) also holds for deficiencies, that is, will $d_{T_1,T_2} = d_{\hat{\theta}_1,\hat{\theta}_2}$ also be true?

As a first step towards answering the first question, we shall indicate the nature of the difficulties that arise here. For a first order approximation we saw in (1) and (2) that an asymptotic normality result is needed. In the classical case of sums of independent random variables this is provided by the central limit theorem. The extension to second order is made by using Edgeworth expansions. To rank tests, and to distributionfree tests in general, these standard results cannot be applied. As is well known, quite a lot of effort has been devoted to obtaining asymptotic normality results for these cases. Hence it will come as no surprise that considerably more obstacles still have to be eliminated before second order approximations become available in this area. Here however we shall be content with noting that such approximations have indeed become available and we shall, ignoring all technicalities involved, concentrate on the results. At first sight, the result is discouraging: it turns out that the asymptotic deficiency $d_{NSc,t} = \infty$. However, it can in addition be shown that the deficiency satisfies

$$(d_{NSc,t})_n \sim \tfrac{1}{2} \log \log n \,, \tag{11}$$

which for all practical purposes is finite (and almost constant). Hence rank tests do live up to optimistic expectations to second order as well: the amount by which their performance falls short of that of their parametric counterparts is indeed enjoyably small. Incidentally, it is also possible to have a finite asymptotic deficiency. For example in the logistic case we have Wilcoxon's signed rank test as the optimal rank test and its asymptotic deficiency with respect to the optimal parametric test for the logistic case is indeed finite.

Next we have the related question about the possibility of rank tests with $d = 0$. In this connection we make the following reexamination of the foregoing. In the normal case we started out with the $\bar{X}$-test, which is the best parametric test. From there we went to the t-test, which is the best scale invariant test for the normal case. Then we decided to buy ourselves in addition distributionfreeness, and we moved on to the normal scores test, which, as noted before, is the best rank test for the situation at hand. Note now that this last step can be judged to be larger than strictly necessary. If we want the test to be distributionfree, we should perhaps look for the best distributionfree test, and not immediately restrict ourselves to rank tests, Indeed it turns out that such an intermediate possibility exists in the form of the best permutation test. The surprising result now is that the asymptotic deficiency $d_{P,t}$ of this best permutation test wrt the t-test satisfies

$$d_{P,t} = 0. \tag{12}$$

Hence once the price $d_{t,\bar{X}} = u_\alpha^2 / 2$ for scale invariance has been paid, no additional charge is involved to obtain distributionfreeness! Of course, besides forming some kind of answer to the second question, this result is more amusing than useful. In practice, people will probably be quite willing to pay the further price given in (11) to buy themselves in addition the ease of application of a rank test.

The answer to the third question simply seems to be yes. To give it a bit more body, we shall consider an illustrative example. Let S_n be the best rank statistic based on a sample $X_1,...,X_n$ from $F(x-\xi)$. Then introduce $S_n(\theta)$ which is the same statistic but now based on the shifted sample $X_1-\theta,...,X_n-\theta$. Let $\tilde{\theta}_n$ be such that $S_n(\tilde{\theta}_n) = E_{H_0} S_n$, then this is (ignoring once more the technical details) the so-called Hodges-Lehmann estimator of ξ. (This has nothing to do with the HODGES-LEHMANN 'Deficiency' paper, but it is simply difficult to discuss a contribution of Professor LEHMANN to statistics without running into other such contributions!) The relation between $\tilde{\theta}_n$ and the rank statistic is precisely the same as between the maximum likelihood estimator $\hat{\theta}_n$ and the parametric counterpart T_n of S_n. We already know that

$$e_{\tilde{\theta}_n, \hat{\theta}_n} = e_{S_n, T_n} = 1. \tag{13}$$

It turns out to be possible to show that the deficiency of $\tilde{\theta}_n$ wrt $\hat{\theta}_n$ (when properly defined) agrees to first order with the deficiency of S_n wrt T_n evaluated at size $\alpha = ½$. Hence if the limits involved exist, we indeed have that

$$d_{\tilde{\theta}_n, \hat{\theta}_n} = d_{S_n, T_n}. \tag{14}$$

In the above we have only considered one-sample results for rank tests. Similar results have also been obtained for the two-sample case and for simple linear rank statistics. Moreover, many contributions have been made to other areas in nonparametrics as well, L-statistics for example. Nevertheless, it is hoped that the brief sketch above has been sufficient to give an idea of the impact of Professor LEHMANN's work on a lot of recent research in statistics.

Erich L. Lehmann was granted an honorary degree by the University of Leiden on 8th February 1985

W.R. van Zwet
Institute for Mathematics and Computer Science
University of Leiden
Wassenaarseweg 80
2333 AL Leiden
The Netherlands

Erich Leo Lehmann was born on 20th November 1917 in Strasbourg. He studied mathematics in Zürich and at Trinity College, Cambridge. In 1942 he switched from pure mathematics to mathematical statistics and became an assistant to Jerzy Neyman at the University of California at Berkeley. Less than a year later he was sorry! He missed the beauty of pure mathematics and was put off by the inelegant methods used by statisticians to solve what he felt to be badly formulated and unattractive problems. He was on the point of starting work with Tarski in algebra when Neyman offered him a better position which on financial grounds he simply couldn't refuse. A statistician against his better judgement, he has done everything in his powers during the last forty years to remove the grounds of his initial complaint. More than anyone else he has contributed to the mathematization of statistics.

His only just started statistical career was interrupted in 1944 when he joined the American airforce in Guam. In 1946 he obtained his Ph.D under Neyman and also became a U.S. citizen. He was assistant professor by 1947 and full professor in 1954 in Berkeley, to which institution he has always been faithful. He was on the editorial board of the Annals of Statistics for 15 years, three of which as editor-in-chief. He has been a president of the Institute of Mathematical Statistics, twice holder of both Miller and Guggenheim fellowships. He is a member of the American Academy of Arts and Sciences and of the National Academy of Sciences.

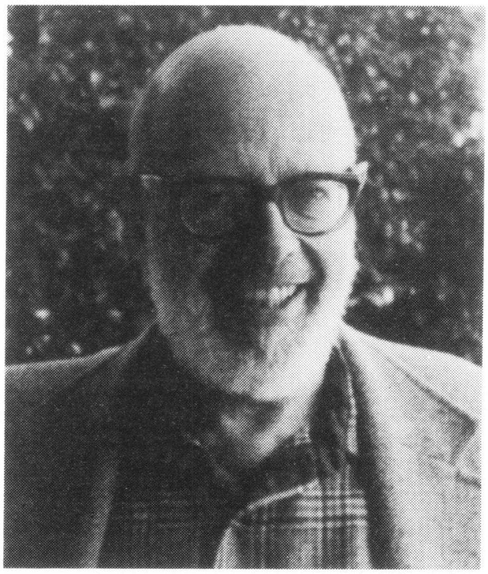
Berkeley and Lehmann were made for one another from the start. Neyman already accentuated the mathematical character of statistics in his work, so Lehmann was his natural heir. Moreover, the small group of statisticians at Berkeley was gradually built up by Neyman in those early years into the most important centre of mathematical statistics in the world. Students from many countries - among them the Netherlands - were attracted to Berkeley and many worked with Lehmann and wrote theses under his supervision. Also the constant stream of visitors from American and other universities were influenced by his work.

In 1959 his book *Testing Statistical Hypotheses* (see CWI Syllabus 3) appeared. Actually he had worked on this book since the start of his career and refined its material many times over in his lecture courses. That this book took so long to reach its final published form (actually a revised edition will appear soon!) is no exception for him: he worked for more that thirty years on the book *Theory of Point Estimation,* from 1950 to 1983.

Along with Cramér's 1945 book *Mathematical Methods of Statistics,* Lehmann's book on the testing of hypotheses has been the most influential book ever written on mathematical statistics. In this book the mathematical structure of statistics was laid bare with perfect precision, but without compromising its applied character. The book has formed a whole generation of statisticians all over the world.

Of course Lehmann was not just engaged in the general structure of the whole area of statistics. He has made key contributions in a large number of more specialized subareas, such as the theory of rank-tests, robust methods, and second order approximations. In all these areas there has been close cooperation over the years with Dutch researchers especially but by no means exclusively from Leiden. The paper by Wim Albers in this same edition of CWI Newsletter is devoted to the third mentioned topic. The research programme on second order approximations which Lehmann originally proposed has been almost completed now by workers in Berkeley, Leiden, Cologne, Amsterdam and Moscow and has led to surprising results. The technical tools which have been developed in the course of this programme are right now being successfully applied to at first sight completely unrelated problems.

Statistics does not have such a long tradition in the Netherlands as many other research areas in mathematics. That the University of Leiden has honoured one of the pioneers of the discipline, in the person of this charming and modest man, is a stimulus to statisticians in the whole country.



Set Theory and Topology [1]

Jan van Mill
Free University Amsterdam
De Boelelaan 1081
1081 HV Amsterdam

1. Introduction

Set theoretic topology is that part of topology that uses results and techniques from set theory in order to solve its problems. In this field set theory and topology walk hand in hand. Set theoretic topology has been quite vital for the last 20 years and has solved major problems. Mathematicians involved in this area are primarily set theorists who enjoy doing 'applied' set theory and general topologists who solve their problems by working in the well-known models of set theory where axioms such as $V=L$, $MA + not - CH$, CH or $\Diamond$ hold. Right now there is a growing number of general topologists however that try to construct their own models instead of making the set theorists prove the consistency results they need. The beautiful book *Set Theory: An Introduction to Independence Proofs* by KUNEN [7] is an important tool now for set theoretic topologists.

What are the problems considered in set theoretic topology? This question is unfortunately undecidable: one never knows whether one will run into a set theoretical problem and many famous mathematicians working in various parts of mathematics posed problems that looked sensible in their field but turned out to be set theoretical ones. We shall present several well-known examples of such problems.

Who is safe from set theory? Well, WHITEHEAD, ALEXANDROFF, WILDER and CHOQUET were not. Maybe you are. But then be wise, never pose a mathematical problem. Set theory is watching you and is ready to attack.

The reader of these notes should be aware of the fact that I am not an

1. These notes form a write-up of a lecture given at the *Topologiedag CWI,* Amsterdam, September 28, 1984.

expert in set theory. I am merely an interested amateur who is fascinated by some of the results in set theoretic topology. The problems I discuss are mostly well-known and only on one occasion do I take the liberty of discussing a problem I helped to solve.

2. Alexandroff's problem

Most people are only interested in metrizable spaces. However, there are also mathematically important spaces that are not always metrizable, for example manifolds, *CW*-complexes, and topological vector spaces. A *manifold* is a locally Euclidean Hausdorff space. Manifolds are certainly mathematically important and the manifolds (with or without differential or algebraic structure) being mostly studied in topology are metrizable. Let M be a manifold (not necessarily assumed to be metrizable). If $A \subseteq M$ is closed then one certainly wants to be able to extend every continuous function $f: A \to \mathbb{R}$ (the reals) to a continuous function $\bar{f}: M \to \mathbb{R}$. By the Tietze-Urysohn Theorem, see [5, 2.1.8] for details, this property of M is equivalent to the following one: every two disjoint closed subsets of M can be separated by disjoint open sets. General topologists say that M is a *normal* topological space. In the process of constructing new continuous functions from old ones it is also extremely pleasant if M has the following property: for every closed subset A of M there is a sequence $\{U_n : n \in \mathbb{N}\}$ of open subsets of M such that $A = \bigcap_{n=1}^{\infty} U_n$. General topologists say that a space with this property is *perfect.* A space which is both perfect and normal is called *perfectly normal.* If X is a perfectly normal space then X has the following important property: for every closed subset A of X there is a continuous function $f: X \to \mathbb{R}$ with $f^{-1}(0) = A$. Clearly, every metric space is perfectly normal. If one wants to generalize some of the existing theory on metrizable manifolds to nonmetrizable ones, it becomes clear quite quickly that in many instances it is inevitable to restrict oneself to perfectly normal manifolds. The question then naturally arises whether there is a perfectly normal manifold which is not metrizable, i.e. whether the extension of the theory is worth while. This question was asked by ALEXANDROFF [1] and later also by WILDER [18].

As usual, $\mathfrak{c}$ denotes the cardinal number of the reals. The *Continuum Hypothesis* (abbreviated *CH*) is the statement that if X is any subset of $\mathbb{R}$ then either X is countable or the cardinality of X is $\mathfrak{c}$.

It is well-known that GÖDEL [6] proved that *CH* is consistent with the usual axioms of set theory. In addition, COHEN [2] showed that $not - CH$ is consistent too. Consequently, the Continuum Hypothesis is undecidable.

It seems unlikely that *CH* has anything to do with manifolds, let alone with Alexandroff's problem. In [13] however, RUDIN and ZENOR, assuming *CH*, constructed an example of a perfectly normal nonmetrizable manifold. Later, KOZLOWSKI and ZENOR [9] even constructed such a manifold that is analytic. These contributions to the solution of Alexandroff's problem very strongly suggested a positive answer.

Let X be a compact Hausdorff space. We say that X satisfies the *countable* *chain condition* (abbreviated *ccc*) if every pairwise disjoint family of open sets in X is at most countable. *Martin's Axiom* (abbreviated *MA*) states that no compact Hausdorff *ccc* space is the union of fewer than $\mathfrak{c}$ nowhere dense sets. So if one assumes *CH* then 'fewer than $\mathfrak{c}$' means countable and hence *MA* is true by the classical Baire Category Theorem. In [16], SOLOVAY and TENNENBAUM proved that the statement $MA + not - CH$ is consistent with the usual axioms of set theory, thereby showing that *MA* is strictly weaker than *CH*.

It seems extremely unlikely that an 'exotic' axiom such as $MA + not - CH$ has anything to do with Alexandroff's problem. However, in [12] RUDIN showed that under $MA + not - CH$ all perfectly normal manifolds are metrizable.

Consequently, Alexandroff's problem is undecidable.

3. WHITEHEAD'S PROBLEM

Let all groups be abelian and let 1_X denote the identity function on a set X. If A and B are groups then a surjective homomorphism $f: A \to B$ is said to *split* if there is a homomorphism $g: B \to A$ with $f \circ g = 1_B$. A group G is a *Whitehead group* if for every group B, every surjective homomorphism $f: B \to G$ with kernel isomorphic to $\mathbb{Z}$ (the integers) splits. It is clear that all free groups are whitehead and WHITEHEAD asked whether all Whitehead groups are free. STEIN [17] showed that all countable Whitehead groups are free.

GÖDEL defined a subclass L of the class V of all sets, the so-called *constructible sets.* The statement $V = L$ means that all sets are constructible: it was proven to be consistent in [6].

SHELAH [14], [15] showed that Whitehead's problem is undecidable by showing that under $V = L$ all Whitehead groups are free while under $MA + not - CH$ there exists a Whitehead group G which is not free. In fact, the group G can be constructed in *ZFC* alone, that is, its construction 'only' needs the usual axioms of set theory plus the *Axiom of Choice.* So if one is a friend of the Axiom of Choice, the group G 'really' exists and has the amazing property that it is free under $V = L$ but not so under $MA + not - CH$. For details, see also [4].

The reader should have noticed by now that without a warning we switched from topology to algebra. However, an application of Pontrjagin duality allows one to translate Whitehead's problem into topological language as follows: *is every compact arcwise-connected abelian topological group isomorphic to a product of circles?* Since I am a friend of the Axiom of Choice [1], Shelah's results imply that for me there 'really' exists a compact arcwise-connected abelian topological group which is nothing but a product of circles under $V = L$ but not under $MA + not - CH$. This is truly unbelievable.

The fact that Whitehead's problem can be formulated both into algebraic

1. If you want to support the work of the society 'Friends of the Axiom of Choice' (president: Dr. H.M. Mulder) please send a cheque to J. van Mill, Department of Mathematics, Free University, De Boelelaan 1081, Amsterdam, The Netherlands.

and topological language is not an exception for a problem that turns out to be dependent upon one's set theory. These problems can often successfully be translated into many mathematical languages and can therefore be attacked from several directions.

4. CHOQUET'S PROBLEM

Our last problem is not as important as the other two. However, since I took part in the solution of the problem myself, I take the liberty to mention this one too.

A *Boolean algebra* (abbreviated *BA*) will be identified with its universe. A *BA* B is called

complete/countably complete/weakly countably complete

if for any two subsets P and Q of B such that $p \wedge q = 0$ for $p \in P, q \in Q$

without further condition/with P or Q countable/ with P and Q countable

there is an $s \in B$ which separates P and Q, i.e. $p \leqslant s$ for $p \in P$ and $q \leqslant s'$ for $q \in Q$.

CHOQUET asked whether every weakly countably complete *BA* is a homomorphic image of a complete *BA*. LOUVEAU [10] proved that under *CH* the answer to Choquet's problem is in the affirmative for *BA*'s of cardinality at most $\mathfrak{c}$. The problem was shown to be undecidable by VAN DOUWEN and VAN MILL [3] who constructed under $MA + \mathfrak{c} = \kappa^+$, with κ any regular uncountable cardinal, an example of a weakly countably complete *BA* which is not a homomorphic image of any countably complete *BA*.

Again, Choquet's problem can be translated into purely topological language (by Stone duality) and in fact VAN DOUWEN and myself, being topologists, thought about it as a topological problem.

There are numerous other problems in topology that turned out to be set theoretical, for example, Souslin's problem, the normal Moore space conjecture, $\beta\mathbb{N}$-type problems, the S-space problem, covering-type problems, etc. For more information, see Rudin's monograph [4] and the recently published *Handbook of Set Theoretic Topology* (edited by K. KUNEN and J.E. VAUGHAN), [8]. Many papers on set theoretic topology appear in the journal *Topology and its Applications,* which I recommend.

REFERENCES

1. P. ALEXANDROFF (1935). On local properties of closed sets. *Ann. Math. 36,* 1-35.
2. P.J. COHEN (1963). The independence of the Continuum Hypothesis I, II. *Proc. Nat. Acad. Sci. USA 50,* 1143-1148; ibid. (1964) *51,* 105-110.
3. E.K. VAN DOUWEN, J. VAN MILL (1980). Subspaces of basically disconnected spaces or quotients of countably complete Boolean Algebras.

Trans. Am. Math. Soc. 259, 121-127.

4. P.C. EKLOF (1976). Whitehead's problem is undecidable. *Am. Math. Monthly 83,* 775-788.
5. R. ENGELKING (1977). *General Topology,* PWN, Warszawa.
6. K. GÖDEL (1940). *The Consistency of the Continuum Hypothesis,* Princeton University Press, Princeton.
7. K. KUNEN (1980). *Set Theory: An Introduction to Independence Proofs,* North-Holland, Amsterdam.
8. K. KUNEN, J.E. VAUGHAN (eds.) (1984). *Handbook of Set Theoretic Topology,* North-Holland, Amsterdam.
9. G. KOZLOWSKI, P. ZENOR (1979). A differentiable, perfectly normal, nonmetrizable manifold. *Top. Proc. 4,* 453-461.
10. A. LOUVEAU (1973). Caractérisation des sous-espaces compacts de βN. *Bull. Sci. Math. (2) 97,* 259-263.
11. M.E. RUDIN (1975). *Lectures on Set Theoretic Topology,* American Mathematic Society, Providence.
12. M.E. RUDIN (1979). The undecidability of the existence of a perfectly normal nonmetrizable manifold. *Houston J. Math. 5,* 249-252.
13. M.E. RUDIN, P. ZENOR (1976). A perfectly normal nonmetrizable manifold. *Houston J. Math. 2,* 129-134.
14. S. SHELAH (1974). Infinite abelian groups - Whitehead problem and some constructions. *Isr. J. Math. 18,* 243-256.
15. S. SHELAH (1975). A compactnes theorem for singular cardinals, free algebras, Whitehead problem and transversals. *Isr. J. Math. 21,* 319-349.
16. R.M. SOLOVAY, S. TENNENBAUM (1971). Iterated Cohen extensions and Souslin's problem. *Ann. Math. 94,* 201-245.
17. K. STEIN (1951). Analytische Funktionen mehrerer komplexer Veränderlichen zu vorgegebenen Periodizitätsmoduln und das zweite Cousinsche Problem. *Math. Ann. 123,* 201-222.
18. R.L. WILDER (1949). *Topology of Manifolds,* American Mathematical Society, Providence.

Vehicle Routing and Computer Graphics

M.W.P. Savelsbergh
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

1. Introduction

Due to the enormous increase in the cost of physical distribution and the economic depression of the last decade, there is a growing demand for decision support systems and optimization methods for distribution management. Although there is a great variety of distribution problems, the basic components are nearly always a fleet of vehicles with fixed capabilities (capacity, speed, etc.) and a set of demands for transporting certain objects (school children, consumer goods, etc.) between specified pick up or delivery points. The *Vehicle Routing Problem* is then to determine which of the demands are assigned to each vehicle and what route each vehicle will follow serving its assigned demand in order to minimize the cost of operating the vehicle fleet. (For further information on the vehicle routing problem see [1].)

Nowadays, a number of software packages is available for solving vehicle routing problems, some of which are based on sophisticated mathematical programming techniques. Reports indicate that the application of these packages results in a considerable saving of distribution costs. Almost all of the currently available packages are batch oriented, by which we mean that the user has no control over the solution process. The program functions as a black box: after specifying all input data the user is provided, on termination, with a final set of routes. In day to day use, it is often necessary to adjust the final set of routes due to practical considerations. Therefore many developers of vehicle routing packages are working on interactive extensions that support post optimization and route manipulation. Although these extensions contribute to the flexibility of the package, we claim that better results can be obtained if interaction between planner and computer starts at the beginning of the solution process. We propose to open up the black box and to combine the strengths of the human planner and the computer in order to obtain the best possible results.

The intent of this paper is twofold. First we indicate that an interactive approach is well suited for vehicle routing problems and secondly we emphasize the importance of a user interface based on colour graphics. In the next section we shall present a more formal definition of the problem. After that we shall discuss some of the advantages of an interactive approach to vehicle routing and make some remarks on the impact of such an approach on the optimization algorithms to be used. A key part of every interactive system is the user interface. Not only does a clear and user friendly interface add to the acceptance of the system, it is also for a major part responsible for the quality of the results obtained. In the last sections we present our views on a colour graphics user interface for an interactive vehicle routing package and relate some of our experiences with the *Graphical Kernel System* graphics package [6].

2. The Vehicle Routing Problem

We consider the following variant of the vehicle routing problem. A vehicle fleet delivers goods stored at a central depot to satisfy customer demands. Each vehicle has a fixed capacity, and each demand uses a fixed portion of this vehicle capacity. To provide a precise statement of this problem we introduce the following notation.

Constants

K = number of vehicles.
n = number of customers to which delivery must be made. Customers are indexed from 1 to n and index 0 denotes the central depot.
b_k = capacity (weight or volume) of vehicle k.
a_i = size of the delivery to customer i.
c_{ij} = cost of direct travel from customer i to customer j.

Variables

$$y_{ik} = \begin{cases} 1 & \text{if the demand from customer } i \text{ is delivered by vehicle } k \\ 0 & \text{otherwise} \end{cases}$$

$$x_{ijk} = \begin{cases} 1 & \text{if vehicle } k \text{ travels directly from customer } i \text{ to customer } j \\ 0 & \text{otherwise} \end{cases}$$

Formulation of the Vehicle Routing Problem

minimize

$$\sum_{ijk} c_{ij} x_{ijk} \tag{1}$$

subject to

$$\sum_i a_i y_{ik} \leqslant b_k, \qquad k = 1,...,K, \tag{2}$$

$$\sum_k y_{ik} = \begin{cases} K & i=0, \\ 1 & i=1,...,n, \end{cases} \qquad (3)$$

$$\sum_i x_{ijk} = y_{jk}, \qquad \begin{cases} j=0,...,n, \\ k=1,...,K, \end{cases} \qquad (4)$$

$$\sum_j x_{ijk} = y_{ik}, \qquad \begin{cases} i=0,...,n, \\ k=1,...,K, \end{cases} \qquad (5)$$

$$\sum_{(i,j) \in S \times S} x_{ijk} \leqslant |S|-1, \qquad \begin{cases} S \subseteq \{1,...,n\}, \\ 2 \leqslant |S| \leqslant n-1, \\ k=1,...,K. \end{cases} \qquad (6)$$

Two well known combinatorial optimization problems are embedded within this formulation. Constraints (2)-(3) are the constraints of a *generalized assignment problem* and ensure that the depot is part of each route, that every customer is served by some vehicle, and that the load assigned to a vehicle is within its capacity. If the y_{ik} are fixed to satisfy (2)-(3), then for each k, constraints (4)-(6) define a *traveling salesman problem* over the customers assigned to vehicle k.

Although the formulation given above is very compact, the number of variables and constraints involved is enormous. Furthermore the two embedded optimization problems are strongly interwoven and should be solved simultaneously in an optimization algorithm. With the currently available techniques this is impossible for problems of even moderate size. We therefore have to rely on heuristic methods.

One of the first and most used algorithms has become known as the *savings* method [3]. Initially, we suppose that every customer is served individually by one vehicle. Now suppose we link two customers i and j and serve them by one vehicle. This eliminates one vehicle and results in a saving in distance of

$$(2c_{0i} + 2c_{0j}) - (c_{0i} + c_{ij} + c_{j0}) = c_{0i} + c_{0j} - c_{ij}.$$

For every possible pair of delivery points i and j there is a corresponding saving s_{ij}. We order these savings in decreasing order and starting at the top of the list we link the points i and j unless the problem constraints are violated.

A more recent approach is due to FISHER & JAIKUMAR [4]. They separate the embedded generalized assignment problem and traveling salesman problems thus creating a *two phase* method. In the first phase, an *assignment* of customers to vehicles is obtained by solving a generalized assignment problem with an objective function that approximates the cost of the traveling salesman tours of the vehicles through the customers. In the second phase, once the assignment has been made, a *routing* of each vehicle through its set of customers is obtained by solving a traveling salesman problem.

CHRISTOFIDES, MINGOZZI & TOTH [2] developed a branch and bound method, capable of solving small instances to optimality. As is the case with all branch and bound algorithms the effectiveness is entirely dependent on the quality of the bounds used to limit the tree search. The bound they use is related to the notion of *through-q-routes*. A through-q-route is the least cost route, with total load q and without loops, starting from the depot, passing through a certain customer and finishing back at the depot.

3. INTERACTIVE OPTIMIZATION

There are two main reasons why an interactive approach to vehicle routing should be preferred over a batch oriented one. One of them is based on algorithmic considerations, the other on practical ones.

The vehicle routing problem (described above) belongs to the class of NP-hard problems [7]. This class contains problems that are very likely to be inherently intractable [5]. This indicates that it is difficult to solve even small instances of the problem to optimality with a reasonable computational effort. Furthermore, the formulation given in the previous section represents the most elementary version of the vehicle routing problem. Practical problems are often complicated by additional constraints such as maximum route length for the vehicles and time windows for the customers. As a consequence, we should not insist on finding an optimal solution, but instead we should try to find a 'good' solution within an acceptable amount of time. To accomplish this we have to resort to heuristic methods. In designing a heuristic for the vehicle routing problem, we can exploit its geometrical structure in conjunction with the spatial perception capabilities of a human planner. A human planner can guide the computer by indicating subsets that are likely to contain near-optimal solutions and discarding beforehand subsets that are very unlikely to contain near-optimal solutions. This kind of man-machine interaction can substantially decrease the practical complexity of a problem instance.

A second and certainly no less important feature of interactive systems is the flexibility. Below certain aspects of practical vehicle routing are described where flexibility and human decisions are essential:

- A serious drawback of (batch oriented) computerized vehicle routing is the difficulty of taking the flexibility of the data into account. Capacity constraints or time window constraints have a certain degree of flexibility. Take for instance the time window constraints of a delivery point; arriving fifteen minutes after the closing of the window does not necessarily lead to infeasibility of the solution. Some customers will not mind very much as long as it does not happen all the time. Such decisions are easily made by a human planner, based on his knowledge of both the customer itself and its history of the past few days. It is almost impossible though to build such considerations into the software.
- By not allowing any control over the solution process, it is very well possible that in day to day planning the routes differ very much. This might lead to a decrease in travel distance and planned travel time, but, in reality, because of drivers' unfamiliarity with certain areas it might cause an increase in actual travel time. In an interactive approach the planner can weigh which of the aspects is dominant before making a decision.
- In a batch oriented software package it is more difficult to react to certain unpredictable events (road innovations, rush orders arriving when the

planning has already started, etc.).
- Beside the obvious distance, time and capacity utilization criteria other objectives, for which it is difficult to give a precise definition, often play an important role in the planning decisions (evenly spread workload for the drivers, drivers' preferences, etc.).

An interactive planning method for vehicle routing should not only contain sophisticated mathematical tools, it should also contain points where human interaction is possible and beneficial. We have chosen for a two phase method based on the FISHER & JAIKUMAR [4] approach. Especially in the assignment phase a human planner can improve the performance of the method. The objective function that approximates delivery cost is obtained by *seed routes* and the cost of inserting customers into these seed routes. A seed route is an artificial route consisting initially of the depot and a *seed point*, where the seed point indicates an area that is expected to be visited by one vehicle. The seed points are chosen by the planner based on his knowledge and intuition. He can iteratively experiment with different seed routes and immediately see the effect on the cost and routing decisions. In the routing phase the planner can create routes according to his own specific objectives or modify the computer generated ones.

4. Colour graphics user interface

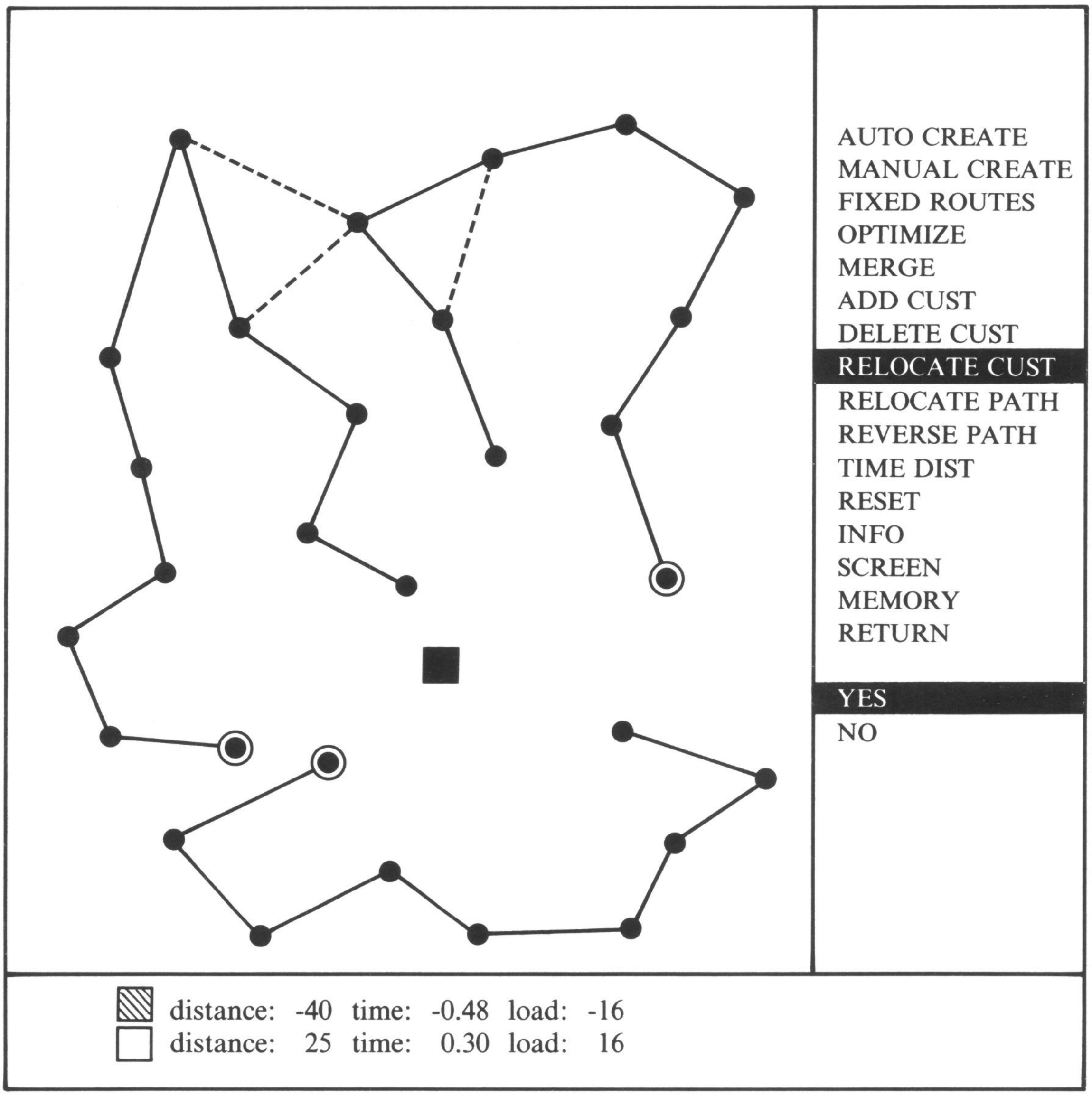
As indicated earlier an interactive approach to computerized vehicle routing is beneficial in increasing the flexibility and performance of the planning system. A very important part of such a system will be the user interface. We believe that a *graphical* user interface is a necessity. The principal argument in favour of the use of graphical displays is their effectiveness in displaying information. Data that would otherwise have to be printed out in numerical form can, with the aid of the display, be used to compose a geometrical representation of the problem which is both clear and informative.

The effect of a graphical user interface will even be stronger if *colour graphics* are used. Colour graphics provide the means to distinguish between the various routes by giving them a different colour. When dealing with only a few routes this advantage is small but when the number of routes increases it becomes more and more a necessity.

But of course a geometrical representation is just one side of the problem. The user should also have the possibility of examining part of the enormous amount of numerical data involved.

We try to keep the screen as steady as possible and therefore divide the screen into three areas:

COMMAND INFO AREA:	This area is reserved for the display of commands;
GRAPHICAL INFO AREA:	This area is reserved for the visualization of the *geometrical* representation;


AUTO CREATE
MANUAL CREATE
FIXED ROUTES
OPTIMIZE
MERGE
ADD CUST
DELETE CUST
RELOCATE CUST
RELOCATE PATH
REVERSE PATH
TIME DIST
RESET
INFO
SCREEN
MEMORY
RETURN
YES
NO
distance: -40 time: -0.48 load: -16
distance: 25 time: 0.30 load: 16

ALPHA-NUMERICAL INFO AREA: This area is reserved for all kinds of *alpha-numerical* information.

We have chosen for a menu-driven interaction mode. Menu-driven interaction has the advantage that the full range of options available to the user at any stage is plainly displayed and it prevents the user from making selections outside this range, and hence solves the problem of erroneous commands.

The commands available to the user are divided into four menus. There are two main menus, the first containing the commands applicable in the assignment phase and the other containing the commands applicable in the routing phase. In addition we have two menus for the utilities available at any stage of the program, one for the set of commands that control the display of information and one for the set of commands that define the contents of the graphical info area. The division of the commands into four subsets has enabled us to reduce the space of the screen needed to display the commands as at any stage at most two of the menus are displayed together.

A subset of the commands in the routing phase provides the planner tools for route manipulation. At any stage the planner can move customers around and adjust routes. Route manipulation takes place by applying interchange techniques [9]. The planner has two possibilities: he can either relocate or reverse the order of a string of consecutive customers. A local change consists of two steps. In the first step the planner specifies the customer(s) he wants to relocate or reverse. This results in the following:

- visualization of the proposed change in the graphical info area (the original situation also remains visible!);
- display of information concerning the change in travel time, waiting time, route length, capacity and feasibility.

It is only in the second step that the planner actually decides whether to carry out the change or not. In this way the planner is able to examine several changes before actually making one and he is protected against input mistakes.

In order to enable the planner to view only part of the graphical info area we provided two screen utilities. The first one enables the user to zoom in on a certain area and the second enables him to change the visibility of routes temporarily. Both these utilities are very useful when the planner is considering local changes.

5. GKS

For the implementation of a colour graphics interface we used the C implementation of the GKS graphics package developed at the CWI [8]. GKS is a basic graphics system for applications that produce computer generated two dimensional pictures on line graphics or raster graphics output devices. It supports man-machine interaction by supplying basic functions for graphical input and picture segmentation.

To be able to use pictures or sub-pictures again during a program's execution GKS supplies a storage mechanism called *segment*. In our application these segments are extremely useful, also for interaction. GKS has six different *logical input device* classes which allow the operator to input data to the program. One of them, the PICK logical input device, returns the name of a segment to the application program identifying the sub-picture that was indicated by the operator. The additional *pick identifier* makes it possible to identify picture parts within a segment. This level of naming is provided in GKS to reduce the segment overhead for applications where a great number of picture parts need to be distinguished for input but the need for manipulation is less important. This is exactly the situation in the application we are currently discussing. In the vehicle routing problem there is a large number of customers, who need to be distinguished for input, divided into a relatively small number of routes. Therefore the most natural thing to do is to create a segment for each route and give each of the customers that make up the route a different pick identifier. As an immediate consequence a call of the REQUEST PICK function uniquely determines both the customer and the route of which it is a member.

The *segment attributes*, which allow the application programmer to modify the appearance of a segment (visibility, detectability, highlighting, transformation), also play a significant part in this application. The detectability of a segment gives us the means to control the input and shield the user from erroneous calls of the REQUEST PICK function. In addition the two screen handling utilities are almost entirely based on the segment attributes. The visibility of a segment and thus the visibility of the corresponding route can be changed by altering the visibility attribute. The effect of zooming can be accomplished by adjusting the current segment transformation.

Our choice for a menu-driven interaction mode is supported by the GKS CHOICE logical input device. GKS permits the application programmer to select the most appropriate *prompt* type for each logical input device and one of the possible types for the CHOICE logical input device is a prompt displaying character strings, representing a menu.

GKS knows three operating modes for a logical input device: REQUEST, SAMPLE and EVENT. The current implementation only supports the synchronous REQUEST mode. This means that when the application program requests an input it suspends action until the user activates a trigger to signal that the input is completed. The two remaining modes allow asynchronous input and therefore support more complex interaction. However, the absence of asynchronous input facilities did not restrict the development of the interactive application we had in mind.

The current system is being tested on an AED512, a rather simple raster graphics device of 500 by 500 pixels. This device in no way supports modern workstation features like internal segmentation, transformations and clipping and filling algorithms. All these actions are therefor carried out on the host, a VAX 11/750. This does not mean though that interaction is slow. Because the output primitives used by the application program are not too complex (no complicated fill areas or rasters) and a fast host is used, the speed of interaction is acceptable. In the future a modern screen with GKS based firmware will speed up interaction considerably and the users feedback will take on spectacular forms.

Although the system is being developed on a large configuration, we will also implement a version that will run on a smaller (stand alone) configuration, probably an IBM PC/AT in combination with a GX-screen.

As GKS is defined device independently, no change other than the substitution of the screen type in the OPEN WORKSTATION function is necessary when the system is moved to another graphical device. This implies a good portability.

6. Conclusion

We have described a number of arguments in favour of interactive approaches to computerized vehicle routing. The arguments are based on considerations concerning algorithmic aspects, flexibility and user friendliness. We have indicated that certain optimization methods developed for the vehicle routing problem are better suited for man-machine interaction than others and described a *cluster first - route second* approach. A very important part of an interactive system is the user interface. We argued that colour graphics should form the basis of such a user interface for vehicle routing packages. A good user interface not only adds to an easy acceptance of the system, but also plays a vital part in the solution process. We also reported some of our experiences with the implementation of a colour graphics user interface with the GKS graphics package. It turned out that for the application described in this paper most of the screen handling can be done with simple basic GKS functions.

7. Acknowledgements

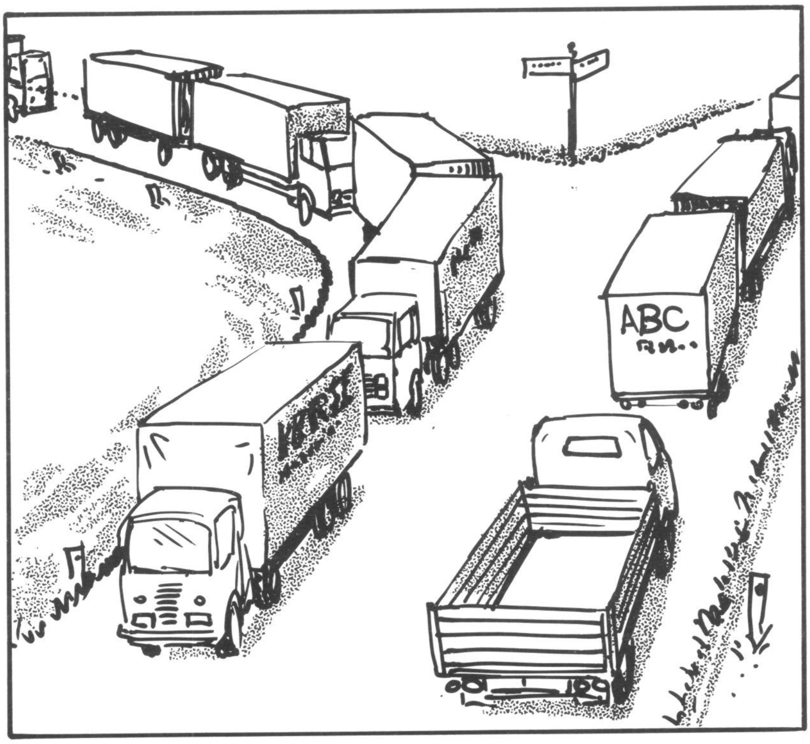
This research was supported by the Netherlands Foundation for the Technical Sciences (STW) through grant nr. CWI-22.0348.

References

1. L.D. Bodin, B.L. Golden, A. Assad, M. Ball (1983). The state of the art in routing and scheduling of vehicles and crews. *Computers and Oper. Res. 10,* 63-212.
2. N. Cristofides, A. Mingozzi, P. Toth (1980). Exact algorithms for the vehicle routing problem based on spanning tree and shortest path relaxation. *Math. Programming 19,* 255-282.
3. G. Clarke, J.W. Wright (1964). Scheduling of vehicles from a central depot to a number of delivery points. *Oper. Res. 12,* 568-581.
4. M.L. Fisher, R. Jaikumar (1981). A generalized assignment heuristic. *Networks 11,* 109-124.
5. M.R. Garey, D.S. Johnson (1979). *Computers and Intractability: A guide to the Theory of NP-Completeness,* W.H. Freeman, San Fransisco.
6. ISO (1982). *Graphical Kernel System (GKS) - Functional Description,* Standard ISO/DIS 7942.
7. J.K. Lenstra, A.H.G. Rinnooy Kan (1981). Complexity of vehicle routing and scheduling problems. *Networks 11,* 221-227.

8. D.S.H. ROSENTHAL, P.J.W. TEN HAGEN (1982). *GKS in C,* Report IW 204/82, Mathematisch Centrum, Amsterdam.

9. M.W.P. SAVELSBERGH (1984). *Local Search in Routing Problems with Time Windows,* Report OS-R8409, Centre for Mathematics and Computer Science, Amsterdam.



Book Review

Steven Pemberton
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

SAMUEL P. HARBISON, GUY L. STEEL JR. (1984). *C: A Reference Manual,* Prentice-Hall.
BRIAN W. KERNIGHAN, ROB PIKE (1984). *The Unix Programming Environment,* Prentice-Hall.

Unix has become a runaway success. Less than ten years ago, many of us were battling with our department heads or computing centres trying to persuade them to ditch the manufacturer's (supported) operating system and replace it with this upstart unsupported system, a system that if it went wrong they would have to fix themselves. Now, not only can you get supported versions of the operating system from several different sources, but computer manufacturers are even bringing out 'Unix computers'. Hand in hand with the success of Unix, C, the programming language associated with Unix, has also gained a high position, putting it amongst the ranks of the most-used languages.

And, of course, along with this success has come a welter of books on the subject: when I checked at a local bookshop they had 20 different books on Unix and another 20 on C. However, up to now, there have only been two books on the subject really worth reading, both written by people at the heart of Unix development. The first of these is *The C Programming Language* by Brian Kernighan and Dennis Ritchie, a book so central in C circles that it is usually just referred to as 'K&R', and the second is *The Unix System* by S.R. Bourne, the man responsible for writing the Bourne shell. These two new books, *C: A Reference Manual* by Samuel P. Harbison and Guy L. Steele Jr., and *The Unix Programming Environment* by Brian W. Kernighan and Rob Pike, are the first books in my opinion to be able to challenge these two classics.

Kernighan and Ritchie's book was the first book about C to be published. Ritchie himself is one of the two people mainly responsible for Unix, and since he was largely responsible for the creation and implementation of C, the book became the *de facto* standard for C: the test of a C compiler was often how closely it conformed to the book. It principally teaches the language rather than defines it (although it does contain a reference manual as an appendix) and as a consequence is not ideal as a source of help when using the language, despite its reputation as the final arbiter in questions of doubt. Another problem is that since the book was published (1978) the language has somewhat changed, making the book a bit out of date. Harbison and Steele's book on the other hand was specifically written (as the title suggests) as a reference book. The authors are part of a group (Tartan Laboratories) producing C compilers for a wide variety of machines, as well as being members of the ANSI committee working on standardising C, and their knowledge of C, especially in the area of how and where different implementations of C perform differently, is clear to see from the book.

Its structure, as is usual for descriptions of C, is 'bottom-up', starting with the lowest level elements, lexical structure, working through types, expressions, to statements and program structure. Each part of the language, even individual operators, is given its own section with cross references to related sections, and they attempt to keep each section complete, as is necessary in a reference manual. This of course leads to some repetitious passages if you read the book from start to finish, but it is easy to recognise such repetition and skim those sections. On the other hand the repetition is rather necessary for a reference book.

Despite being a reference book, it is very pleasant reading, with many example programs to illustrate points, and they do their best to emphasise good style and portability, as well as just conformance with the language. As an example, the sections on the bitwise operators all warn against confusion with the logical operators that look similar ('&' against '&&'), and include a 6 page example program implementing small sets using the operators.

The treatment of portability questions is good. Not only do they point out where different implementations may interpret the language differently (such as the bitwise operators on signed numbers), but also parts of the language that implementations typically mis-compile. This may be going too far, but it can be very useful for people who want to write programs that will run on as many machines as possible. The only thing that I missed in the book was a chapter on portability, collecting all these facts together.

In conclusion then, a good book for the serious C programmer or implementer, and while not a tutorial book, readable enough to learn the language from if you already know a similar language.

Bourne's book on Unix was long awaited. When you start to learn Unix you often get the feeling that there must be ten simpler and more elegant ways to do what you are doing, but it's just a case of discovering them, and usually the only way is to ask a guru. Before Bourne's book, the only books available were ones describing Unix and how to use it, but not really giving you a feel for how you can put different Unix tools together to create new ones, one of the strengths of Unix. Bourne's book was aimed at all users of Unix, from the novice to the expert, and starts by describing the basics of each part of Unix, and then builds useful tools from these parts as examples. As a consequence, the novice learns a lot very fast, and the expert still finds it interesting and useful, because it's full of good ideas and interesting techniques.

Kernighan and Pike's book is aimed at a slightly different audience: the programmer using Unix, and therefore, while it has much in common with Bourne, it has a somewhat different emphasis. Bourne's book tries to cover all parts of using Unix, including editors, and uses a chapter for each major topic, so that each chapter is largely self contained, and can still be used as reference material. Kernighan and Pike's book is very much more of a tutorial and less of a reference, and since it is primarily about programming, not all Unix features are treated. Many chapters have the same subject matter as Bourne's, such as the shell and document preparation, but the treatment is very much continuous, each chapter being a development of the previous ones. This is done by writing programs, each time introducing and using new facilities to write the program or improve a previous one. This is the most notable difference between Kernighan and Pike's treatment and Bourne's: Bourne introduces facilities of Unix, and then produces programs to illustrate the facilities, while Kernighan and Pike write programs, and introduce facilities to write them. This is very clear from the table of contents, where each entry in a chapter often only gives the program name and little detail about what is being handled there, while Bourne gives what topics are treated, and no information about what programs are used as examples.

However, Kernighan and Pike's book is very good, but has to be read from start to finish: you can't use individual chapters as reference. And just like Bourne's book, it is full of interesting ideas and techniques, which makes it a treasure house for the regular Unix user. It is less suitable for complete beginners than Bourne, for instance it has no introductory chapter on C programming, but with a little introductory reading (e.g. Bourne's book itself) it is eminently readable, and a must for all serious Unix users.

REFERENCES

S.R. BOURNE (1982). *The Unix System,* Addison-Wesley.

BRIAN W. KERNIGHAN, DENNIS M. RITCHIE (1978). *The C Programming Language,* Prentice-Hall.

Abstracts

of Recent CWI Publications

When ordering any of the publications listed below please use the order form at the back of this issue.

CWI Tract 16. R.P.J. Groothuizen. *Mixed Elliptic-Hyperbolic Partial Differential Operators: A Case Study in Fourier Integral Operators.*
AMS 35A08, 35C05, 35M05, 42B20; 145 pp.

Abstract: In this tract the utility of Fourier Integral Operators (FIOs) is tested for the study of two types of partial differential operators of mixed elliptic-hyperbolic type, viz. the Tricomi operator $\partial^2 / \partial t^2 + t\Delta_x$ and the operator $t\partial^2 / \partial t^2 + \Delta_x + \alpha(\partial / \partial t)$, called the Pseudo Tricomi operator. The Tricomi operator is of real principal type, the Pseudo Tricomi operator is not. So for the Tricomi operator parametrices can be constructed using FIOs. Here fundamental solutions for the Tricomi operator in $\mathbb{R}^{n+1}$ are constructed using adapted FIO-techniques. The same is done for the Pseudo Tricomi operator. Moreover boundary value problems for the Tricomi operator with distributional data are discussed. Since a rather extensive summary of the theory of FIOs is included, the results thus obtained can be used to illustrate the use of FIO-techniques in concrete problems. Also these results show that these techniques can lead not only to parametrices but also to the exact solutions in explicit form.

CWI Tract 17. H.M.M. ten Eikelder. *Symmetries for Dynamical and Hamiltonian Systems.*
AMS 35L65, 35Q20, 58F05, 58F07, 58F35, 58G35, 70H99; 191 pp.

Abstract: Symmetries and adjoint symmetries of a dynamical system $\dot{u} = X(u)$ on a manifold are introduced as possibly ($t-$) parametrized vector fields or one-forms which are invariant for the flow corresponding to the vector field X. The symmetries of a dynamical system form a Lie algebra. Tensor fields of total order two, which are invariant under the flow corresponding to X, can be used as operators which transform (adjoint) symmetries into (adjoint) symmetries. For a Hamiltonian system every constant of the motion gives rise to a symmetry; this type of symmetry will be called a canonical symmetry. Every non-canonical symmetry (in fact every non-semi-canonical) symmetry Z gives rise to a recursion operator for symmetries. By repeated application of this

recursion operator to X and Z we obtain two series X_k and Z_k of symmetries. Under certain conditions the series X_k consists of canonical symmetries and corresponds to a series of constants of the motion in involution, while the series Z_k consists of non (semi-) canonical symmetries. We also describe the corresponding Lie algebra. Moreover, we show how to use differential geometrical methods for certain infinite-dimensional systems and give function spaces in which some infinite-dimensional systems can be considered. Finally a number of examples is given.

CWI Tract 18. A.D.M. Kester. *Some Large Deviation Results in Statistics.*
AMS 62F10, 62F12, 62F03, 62F05, 60F10, 60F05; 135 pp.

Abstract: This treatise concerns two main subjects involving 'large deviations' in statistics. The first main subject of this tract is parameter estimation. Instead of the usual expected squared error, we take the probability of missing the parameter by a fixed amount, the probability of a large deviation, as a criterion for the quality of estimators. The standardized leading term of this usually exponentially small probability is called the inaccuracy rate. In convex exponential families we prove that the maximum likelihood estimator has optimal inaccuracy rate. Properties (in terms of their inaccuracy rates) of estimators are furthermore studied in curved exponential families and in shift families on the real line. The second main subject is the Bahadur efficiency of classical two-sample conditional tests for testing the equality of the parameters two in one-parameter exponential families. It is proved that the uniformly most powerful unbiased test is not only fully efficient with respect to most powerful tests, but also that its Bahadur deficiency is finite. Some numerical results supplement the theory.

CWI Syllabus 2. E.M. de Jager & H.G.J. Pijls (eds.). *Proceedings Seminar 1981-1982 Mathematical Structures in Field Theories.*
AMS 81EXX, 81E10, 53BXX, 55RXX; 217 pp.

Abstract: During the last decades a revival of mutual interest and scientific cooperation between mathematicians and physicists has become manifest. On the one hand very sophisticated theories from many branches of mathematics are needed nowadays in theoretical physics, and on the other hand the overwhelming results in mathematical physics, substantiated by experiments, are a source of inspiration and motivation for many mathematicians. Reflecting this growing mutual interest between mathematicians and physicists, a national seminar 'Mathematical Structures in Field Theories' started in 1981 at the University of Amsterdam. The reader finds in this book the contents of the lectures given during the seminar of the academic year 1981-1982. The programme of this first year seminar was mainly directed to differential geometry and gauge field theory; in order to give participants a better understanding of theories in which they are not fully conversant, some of the lectures are of an introductory character. This text will be followed at least by the proceedings of the seminars 1982-1983 and 1983-1984.

CS-R8502. J.C.M. Baeten, J.A. Bergstra & J.W. Klop. *Conditional axioms and α / β calculus in process algebra.*
AMS 68B10, 68C01, 68D25, 68F20; CR F.1.1, F.1.2, F.3.2, F.4.3; 26 pp.; **key words:** concurrency, process algebra, alphabet, conditional axiom.

Abstract: We define the alphabet of finite and infinite terms in ACP_τ, the algebra of communicating processes with silent steps, and also give approximations of it (the α / β calculus). Using the alphabet, we formulate some conditional axioms. The usefulness of these axioms is demonstrated in several examples.

CS-R8503. J.C.M. Baeten, J.A. Bergstra & J.W. Klop. *Syntax and defining equations for an interrupt mechanism in process algebra.*
AMS 68B10, 68C01, 68D25, 68F20; CR F.1.1, F.1.2, F.3.2, F.4.3; 45 pp.; **key words:** concurrency, process algebra, interrupts, priorities.

Abstract: A mechanism is introduced to describe priorities in ACP, the algebra of communicating

processes, whereby some actions have priority over others in a non-deterministic choice (or sum). This mechanism can be used to model the working of interrupts in a distributed system. This is illustrated in an extensive example.

CS-R8504. J.A. Bergstra, J. Heering & P. Klint. *Algebraic definition of a simple programming language.*
AMS 68BXX; CR D.2.1, D.3.1, F.3.1, F.3.2; 99 pp.; **key words:** software engineering, algebraic specifications, formal definition of programming languages, programming environments, modularization techniques, specification languages, executable specifications, prototyping.
Abstract: What are the potentials and limitations of algebraic specifications for defining programming languages and their processors? This paper tries to answer this question by developing a specification for the toy programming language PICO. This specification describes in detail all necessary steps from entering a PICO program in its textual form to computing its value. A major part of this specification is devoted to general techniques for defining programming languages and does not depend on specific properties of PICO. The size of this specification (more than 350 axioms) makes it mandatory to use modularization techniques. In the specification formalism used we have experimented with polymorphism, infix operators, conditional equations, rules for import and export and with parameterization. The results of this experiment and their implications for further research are discussed.

CS-R8505. H. Cohen & A.K. Lenstra. *Implementation of a new primality test.*
AMS 10-04, 10A25; CR F.2.1; 29 pp.; **key words:** primality testing.
Abstract: An implementation of the Cohen-Lenstra version of the Adleman-Pomerance-Rumely primality test is presented. Primality of prime numbers of up to 213 decimal digits can now be routinely proved within approximately ten minutes.

CS-R8506. J.W. de Bakker, J.-J.Ch. Meyer & E.-R. Olderog. *Transition systems, infinitary languages and the semantics of uniform concurrency.*
AMS 68B10, 68C01; CR D.3.1, F.3.2, F.3.3; 11 pp.; **key words:** concurrency, operational semantics, denotational semantics, transition systems, uniform languages, infinitary languages, shuffle, synchronization, local nondeterminacy, global nondeterminacy, linear time, branching time, specification-oriented semantics, ready set.
Abstract: Transition systems as proposed by Hennessy & Plotkin are defined for a series of three languages featuring concurrency. The first has shuffle and local nondeterminacy, the second synchronization merge and local nondeterminacy, and the third synchronization merge and global nondeterminacy. The languages are all uniform in the sense that the elementary actions are uninterpreted. Throughout, infinite behaviour is taken into account and modelled with infinitary languages in the sense of Nivat. A comparison with denotational semantics is provided. For the first two languages, a linear time model suffices; for the third language a branching time model with processes in the sense of De Bakker & Zucker is described. In the comparison an important role is played by an intermediate semantics in the style of Hoare & Olderog's specification oriented semantics. A variant on the notion of ready set is employed here. Precise statements are given relating the various semantics in terms of a number of abstraction operators.

CS-R8507. S.J. Mullender & A.S. Tanenbaum. *A distributed file service based on optimistic concurrency control.*
AMS 68A05, 68B20, 68H05; CR D.4.3, H.2.2, H.2.4, H.3.2; 20 pp.; **key words:** file server, data base server, distributed control, optimistic concurrency control, atomic update, serialisability, differential files.

Abstract: Principles are presented for a distributed file and database system that leaves a large degree of freedom to the users of the system. It can be used as an efficient storage medium for files, but also as a basis for a distributed data base system. An optimistic concurrency control mechanism, based on the simultaneous existence of several versions of a file or data base is used. Each version provides to the client who owns it, a consistent view of the contents of the file at the time of the version's creation. We show how this mechanism works, how it can be implemented and how serialisability of concurrent access is enforced. A garbage collector that runs independently of, and in parallel with, the operation of the system is also presented.

CS-R8508. J.W. de Bakker, J.-J.Ch. Meyer & E.-R. Olderog. *Infinite streams and finite observations in the semantics of uniform concurrency* (preliminary version).
AMS 68B10, 68C01; CR D.3.1, F.3.2, F.3.3; 12 pp.; **key words:** concurrency, denotational semantics, streams, uniform languages, observations, Smyth ordering, parallel composition, topological closedness.

Abstract: Two ways of assigning meaning to a language with uniform concurrency are presented and compared. The language has uninterpreted elementary actions from which statements are composed using sequential composition, nondeterministic choice, parallel composition with communication, and recursion. The first semantics uses infinite streams in a sense which is a refinement of the linear time semantics of de Bakker et al. The second semantics uses the finite observations of Hoare et al., situated 'in between' the divergence and readiness semantics of Olderog & Hoare. It is shown that the two models are isomorphic and that this isomorphism induces an equivalence result between the two semantics.

CS-R8509. J. Heering & P. Klint. *The efficiency of the Equation interpreter compared with the UNH Prolog interpreter.*
AMS 68B99; CR D.2.1, F.4.1, D.3.4; 13 pp.; **key words:** performance evaluation, Prolog, Equation interpreter, prototyping algebraic specification.

Abstract: There are several alternatives for transforming algebraic specifications into executable prototypes. In this note the Equation interpreter (a rewrite rule interpreter) and the University of New Hampshire Prolog interpreter are viewed as target systems for executing prototypes. The efficiencies of these systems are compared with each other.

CS-R8510. P.M.B. Vitányi. *Time-driven algorithms for distributed control.*
AMS 68C05, 68C25, 68A05, 68B20, 94C99; CR C.2, D.4, F.2.2, G.2.2; 28 pp.; **key words:** distributed clock synchronization, distributed spanning tree, distributed elections, algorithms using time, time-independent correctness and termination, robustness, accelerated efficiency by improved synchronicity, distributed control, computer networks, network topology.

Abstract: Distributed algorithms are investigated for clock synchronization, spanning tree construction and leader-finding in large store-and-forward networks of processors communicating by message passing. In the synchronization algorithm the clocks are allowed to drift in both value and speed; the message delivery delay is unknown and may change with time. The algorithm for distributed elections and distributed spanning tree construction uses time, yet is logically time independent. Using time, we obtain better performance in terms of message-passes and passed bits than is possible otherwise, and better performance than by any other known algorithm. The algorithm works correctly for any network topology, under any asynchronicity in the network, and assumes no global knowledge about the network.

CS-R8511. J.C.M. Baeten, J.A. Bergstra & J.W. Klop. *On the consistency of Koomen's fair abstraction rule.*

AMS 68B10, 68C01, 68D25, 68F20; CR F.1.1, F.1.2, F.3.2, F.4.3; 39 pp.; **key words:** process algebra, concurrency, Koomen's fair abstraction rule, recursion.

Abstract: We construct a graph model for ACP_τ, the algebra of communicating processes with silent steps, in which Koomen's Fair Abstraction Rule (KFAR) holds, and also versions of the Approximation Induction Principle (AIP) and the Recursive Definition & Specification Principles (RDP & RSP). We use this model to prove that in ACP_τ, (but not in ACP !) each computably recursively definable process is finitely recursively definable.

CS-N8504. L.G. Bouma, J. Bruijning & J.C. van Vliet. *Document processing.* (In Dutch.)

AMS 68K05; CR H.4.1; 20 pp.; **key words:** word processing.

Abstract: The processing of documents is increasingly done using VDU's and computers. Such systems vary from simple programs for creating letters and memo's to advanced systems for the production of books with a complex contents. This article presents an overview of the main developments in this area. We also touch upon the office of the future, in which advanced workstations allow for the interactive manipulation and processing of documents including formulas, tables, pictures, and the like.

OS-R8501. G.A.P. Kindervater & J.K. Lenstra. *An introduction to parallelism in combinatorial optimization.*

AMS 90CXX, 68A05, 68C25, 68EXX; 16 pp.; **key words:** parallel computer, computational complexity, polylog parallel algorithm, sorting, scheduling, log space completeness for $\mathcal{P}$, linear programming, dynamic programming, knapsack, branch and bound, traveling salesman.

Abstract: This is a tutorial introduction to the literature on parallel computers and algorithms that is relevant for combinatorial optimization. We briefly discuss theoretical as well as realistic machine models and the complexity theory for parallel computations. Some examples of polylog parallel algorithms and log space completeness results for $\mathcal{P}$ are given, and the use of parallelism in enumerative methods is reviewed.

OS-R8502. J.M. Schumacher. *A geometric approach to the singular filtering problem.*

AMS 93E11, 93B20; 16 pp.; **key words:** singular filtering, noise-free observations, system inversion, least-squares estimation, colored noise.

Abstract: We consider the least-squares filtering problem for a stationary Gaussian process when the observation is not fully corrupted by white noise, the so-called 'singular' case. An optimal estimator is constructed consisting of an integrating part, which is, as in the regular case, computed from a spectral factorization or an equivalent matrix problem, and a differentiating part whose parameters are computed from a single matrix equation. This improves on older results which either work under restrictive assumptions, or describe the solution only as the result of some nested algorithm.

OS-R8503. B.J. Lageweg, J.K. Lenstra, A.H.G. Rinnooy Kan & L. Stougie. *Stochastic integer programming by dynamic programming.*

AMS 90C10, 90C15, 90C39; 12 pp.; **key words:** stochastic integer programming, distribution model, two-stage decision model, scheduling, bin packing, multiknapsack, dynamic programming.

Abstract: Stochastic integer programming is a suitable tool for modeling hierarchical decision situations with combinatorial features. In continuation of our work on the design and analysis of heuristics for such problems, we now try to find optimal solutions. Dynamic programming techniques can be used to exploit the structure of two-stage scheduling, bin packing and

multiknapsack problems. Numerical results for small instances of these problems are presented.

OS-R8504. J.B. Orlin. *Genuinely polynomial simplex and non-simplex algorithms for the minimum cost flow problem.*
AMS 90C08, 90C35; 39 pp.; **key words:** network flow, scaling, simplex algorithm, polynomial algorithm.
Abstract: We consider the minimum cost network flow problem min $(cx : Ax = b,\ x \geqslant 0)$ on a graph $G=(V,E)$. First we give a minor modification of the Edmonds-Karp scaling technique, and we show that it solves the minimum cost flow problem in $\mathcal{O}((|V|^2 \log |V|)(|E| + |V| \log |V|))$ steps. We also provide two dual simplex algorithms that solve the minimum cost flow problem in $\mathcal{O}(|V|^4 \log |V|)$ pivots and $\mathcal{O}(|V|^3 \log |V|)$ pivots respectively. Moreover, this latter dual simplex algorithm may be implemented so that the running time is proportional to that of the Edmonds-Karp scaling technique.

OS-R8505. J.B. Orlin. *The complexity of dynamic/periodic languages and optimization problems.*
AMS 68C25, 90CXX; 19 pp.; **key words:** PSPACE, periodic scheduling, periodic graphs.
Abstract: We provide a characterization of the class PSPACE as those languages L for which each element x of L has a 'periodic certificate'. This characterization leads to proofs that a large number of NP-complete problems have dynamic/periodic counterparts that are PSPACE-complete. This characterization is also useful in analysing periodic scheduling problems that arise in workforce planning, transportation planning, and operations management.

NM-R8502. H. Arndt, P.J. van der Houwen & B.P. Sommeijer. *Numerical integration of retarded differential equations with periodic solutions.*
AMS 65Q05, 65L05; 11 pp.; **key words:** numerical analysis, retarded differential equations, delay equations, periodic solutions.
Abstract: It is the purpose of this paper to show that the minimax versions of linear multistep methods, originally derived for *ordinary* differential equations with a periodic solution, are also suitable for the integration of *retarded* differential equations possessing a periodic solution. Especially for this type of equations it is extremely useful to have methods yielding highly accurate results for relatively large time steps h. We consider several examples of first-order and second-order equations with constant and state-dependent delay and compare the numerical results with those of the conventional methods.

NM-R8503. H.J.J. te Riele. *Computation of all the amicable pairs below* 10^{10}.
AMS 10A40, 10-04; 41 pp.; **key words:** amicable pair.
Abstract: An efficient exhaustive numerical search method for amicable pairs is described. With the aid of this method all 1427 amicable pairs with smaller member below 10^{10} have been computed, more than 800 pairs being new. This extends previous exhaustive work below 10^8 by H. Cohen. Various statistics are given, including an ordered list of all the gcd's of the 1427 amicable pairs below 10^{10} (which may be useful in further amicable pair research). Suggested by the numerical results, a theorem of Borho and Hoffmann for constructing APs has been extended.

NM-R8504. P.J. van der Houwen & B.P. Sommeijer. *Explicit Runge-Kutta (-Nyström) methods with reduced phase errors for computing oscillating solutions.*
AMS 65L05; CR G.1.7, G.1.8; 17 pp.; **key words:** numerical analysis, ordinary differential equations, periodic solutions, Runge-Kutta methods.
Abstract: We construct explicit Runge-Kutta (-Nyström) methods for the integration of first (and second) order differential equations having an oscillatory solution. Special attention is paid to the

phase errors (or *dispersion)* of the dominant components in the numerical oscillations when these methods are applied to a linear, homogeneous test model. RK(N) methods are constructed which are dispersive of orders up to 10, whereas the (algebraic) order of accuracy is only 2 or 3. Application of these methods to semi-discretized hyperbolic equations and to equations describing free and weakly forced oscillations, reveals that the phase errors can be significantly reduced.

NM-R8505. P.W. Hemker & S.P. Spekreijse. *Multigrid solution of the steady Euler equations.*
AMS 65N05, 65N30, 76G15; 11 pp.; **key words:** multigrid method, steady Euler equations, Osher's approximate Riemann-solver.
Abstract: A multigrid (MG) method for the approximation of steady solutions to the full 2-D Euler equations is described. The space discretization is obtained by the finite volume technique and Osher's approximate Riemann-solver. Symmetric Gauss-Seidel relaxation is applied to solve the nonlinear discrete system of equations. A multigrid method, the full approximation scheme, accelerates this iterative process. In a few two-dimensional testproblems (subsonic, transsonic and supersonic), the multigrid iteration is applied to an initial estimate that was obtained by means of the FMG-technique (nested iteration). For the discretization on the different levels, a fully consistent sequence of nested discretizations is used. The prolongations and restrictions selected are in agreement with this consistency. It turns out that the total amount of work required to obtain a solution that is accurate up to truncation error, corresponds to a small number of nonlinear Gauss-Seidel iterations. In the case of transsonic flow the rate of convergence of the MG-iteration appears independent of N, the number of cells in the discretization.

NM-R8506. J.G. Verwer. *Convergence and order reduction of diagonally implicit Runge-Kutta schemes in the method of lines.*
AMS 65X02, 65M10, 65M20; 15 pp.; **key words:** numerical analysis, initial boundary value problems in partial differential equations, method of lines, Runge-Kutta schemes, convergence analysis, order reduction.
Abstract: We examine four known diagonally implicit Runge-Kutta discretizations of initial-boundary value problems in partial differential equations. Our main interest lies in the derivation of bounds for the full discretization error under the assumption that the grid distances in space and time are independent parameters. We follow the method of lines approach which enables us to exploit ideas and results from the B-convergence theory for Runge-Kutta schemes applied to stiff problems. Emphasis is laid upon order reduction phenomena. Various numerical examples are presented which illustrate and confirm the theoretical results. It is shown that in the field of partial differential equations order reduction severely reduces the performances of higher order schemes.

MS-R8501. R.D. Gill. *The total time on test plot and the cumulative total time on test statistic for a counting process.*
AMS 62M99, 62N05, 62P10; 5 pp.; **key words:** total time on test plot, cumulative total time on test statistic, testing exponentiality, random time change, counting process.
Abstract: Results on the total time on test plot are usually obtained on the assumption that the number of events to be observed is fixed in advance. Here it is shown that the same large sample results hold when the number of events is random if a simple condition is satisfied.

MS-R8502. R.D. Gill. *On estimating transition intensities of a Markov process with aggregate data of a certain type: Occurences but no exposures.*
AMS 62M05, 62PXX; 23 pp.; **key words:** Markov process, aggregate data, multidimensional mathematical demography, multistate life-table, occurrence-exposure rate, fixed-point theorem, degree theory.

This report is a revised version of MS-R8411 (see Newsletter no. 5, December 1984).

MS-N8501. R.D. Gill. *Statistical investigation of weather conditions in the German Bight near Sylt, June-July 1984.*
AMS 62P99, 60F12; 40 pp.; **key words:** extrapolation.

Abstract: The company Van Oord B.V. was engaged in beach-replenishment on the island of Sylt, Summer 1984. Their material suffered some damage during heavy storms in June 1984 which also delayed the work. Continuing bad weather in July 1984 prevented essential repair work and led to further damage and delay. The questions we address here are: could weather conditions of such severity reasonably have been foreseen? Were the weather conditions indeed of exceptional severity? We especially wish to quantify the answers to these questions. The questions are answered using elementary statistical methods.

AM-R8501. H.E. de Swart. *Construction and analysis of a low order spectral model of the barotropic potential vorticity equation in a beta channel.*
AMS 35A35, 58F25; 13 pp.; **key words:** barotropic potential vorticity equation, spectral model, flows, bifurcations.

Abstract: A low order spectral model is derived from the barotropic potential vorticity equation in a beta channel. Distinction is made between the conservative - and dissipative case. Both systems are analyzed by mathematical methods. The dissipative model is similar to that of Egger (1981); however, a different value for the β parameter and a constant width of the channel are taken, giving rise to new quantitative aspects.

AM-R8506. N.M. Temme & J.T.F. Zimmerman. *On the theory of topographic vorticity production by tidal currents.*
AMS 76C05, 33A40, 35C10, 42B10; 20 pp.; **key words:** quasi linear vorticity equation, primitive perturbation series, harmonic truncation, Fourier transformed solution, asymptotic regimes.

Abstract: Starting from the shallow water equations of a homogeneous rotating fluid we derive the equation describing the evolution of vorticity induced by a fluctuating bottom topography. By a twofold expansion in a small parameter, it is shown that nonlinear vorticity advection can be reduced to a quasi-linear form in the limit of small amplitude topography and when the topographic horizontal length scale is much smaller than the length of a tidal gravity wave. Topographic vorticity is then produced by two mechanisms, viz. planetary vortex stretching and differential bottom friction. For both mechanisms, the vorticity response functions at the basic forcing frequency and all of its higher harmonics, as well as the residual components, are shown to be given by sums of products of Bessel functions. We discuss the asymptotic behaviour of these response functions and compare them with other approximate methods of solving the vorticity equation, particularly the method of harmonic truncation. These results are used in deriving the exact shape of the residual velocity field for a one-dimensional step-like bottom topography. We show that in the absence of vorticity diffusion the residual velocity vanishes exactly outside a region of twice the tidal excursion length scale, in contrast to the result derived by the method of harmonic truncation. Inside that region the residual velocity profile can be expressed in Legendre functions, or equivalently as a hypergeometric function, and in an integral over Legendre functions. This result is finally used to calculate the shape of the residual velocity profile numerically.

AM-R8507. N.M. Temme *A double integral containing the modified Bessel function: asymptotics and a device for computation.*
AMS 33A40, 41A60, 65D20; 7 pp.; **key words:** Bessel function integral, uniform asymptotic expansion, incomplete gamma functions.

Abstract: A two-dimensional integral containing $exp(-\xi-\eta)I_0(2\sqrt{\xi\eta})$ is considered. $I_0(z)$ is the modified Bessel function and the integral is taken over the rectangle $0 \leqslant \xi \leqslant x$, $0 \leqslant \eta \leqslant y$. The integral is difficult to compute when x and y are large, especially when x and y are almost equal. Computer programs based on existing series expansions are inefficient in this case. A representation in terms of the error function (normal distribution function) is given, from which more efficient and reliable algorithms can be constructed.

AM-R8508. M. Gyllenberg & H.J.A.M. Heijmans. *An abstract delay-differential equation modelling size dependent cell growth and division.*
AMS 34K30, 92A15, 35R10; 15 pp.; **key words:** structured populations, cell cycle, first order partial differential equation with delay and transformed argument, delay-differential equation in a Banach space, strongly continuous semigroup, generation expansion, positive operator, Riesz operator, spectral theory, stable size distribution.

Abstract: A two-phase model for the growth of a single cell population structured by size is formulated and analysed. The model takes the form of a delay-differential equation in a Banach space. Using positivity arguments we describe the spectrum of the infinitesimal generator of the semigroup associated with solutions. Under a certain condition on the growth rate of individual cells the semigroup is compact after finite time. This enables us to determine the ultimate behaviour of solutions and prove the existence of a stable size distribution.

AM-R8509. M. Gyllenberg. *The size and scar distributions of the yeast Saccharomyces cerevisiae*
AMS 92A15, 60K05; 18 pp.; **key words:** budding yeast, unequal division, first order partial differential equation with delay and transformed argument, renewal equation, stable size distribution.

Abstract: A model for the growth of populations of *Saccharomyces cerevisiae* is formulated and analysed. The probability of bud emergence is assumed to depend on the size of the cell. Under certain conditions on birth size the model can be reduced to a single renewal equation. Using Laplace transform techniques and renewal theory we establish the existence of a stable scar and size distribution under certain conditions on the growth rate of individual cells. The steady state values for the relative frequencies of unbudded and budded cells in the various scar classes are given.

CWI Activities

Summer 1985

With each activity we mention its frequency and (between parentheses) a contact person at CWI. Sometimes some additional information is supplied, such as the location if the activity will not take place at CWI.

Study group on Analysis on Lie groups. Joint with University of Leiden. Biweekly. (E.P. van den Ban)

Seminar on Algebra and Geometry. Coxeter Groups and Combinatorics. Biweekly. (A.E. Brouwer)

Study group on Cryptography. Biweekly. (J.H. Evertse)

Colloquium 'STZ' on System Theory, Applied and Pure Mathematics. Twice a month. (J. de Vries)

Study group 'Biomathematics'. Lectures by visitors or members of the group. Joint with University of Leiden. (J. Grasman)

Study group on Nonlinear Analysis. Lectures by visitors or members of the group. Joint with University of Leiden. (O. Diekmann)

Progress meetings of the Applied Mathematics Department. New results and open problems in biomathematics, mathematical physics and analysis. Weekly. (N.M. Temme)

National Study Group on Statistical Mechanics. Joint with Technological University of Delft, Universities of Leiden and Groningen. Monthly. University of Amsterdam. (H. Berbee)

Progress meetings on Combinatorial Optimization. Biweekly. (J.K. Lenstra)

System Theory Days. Irregular. (J.H. van Schuppen)

Study group on System Theory. Biweekly. (J.H. van Schuppen)

National colloquium on Optimization. Irregular. (J.K. Lenstra)

Study group on Differential and Integral Equations. Lectures by visitors or group members. Irregular. (H.J.J. te Riele)

Study group on Numerical Flow Dynamics. Lectures by group members. Every Wednesday. (J.G. Verwer)

Progress meetings on Numerical Mathematics. Weekly. (H.J.J. te Riele)

International Colloquium on Numerical Aspects of Vector- and Parallel Processors. Monthly, every last Friday. (H.J.J. te Riele)

Study group on Numerical Software for Vector Computers. Monthly. (H.J.J. te Riele)

Conference on Numerical Mathematics. 30 September - 2 October 1985 at Zeist. Invited speakers:
W. Fichtner (AT & T Bell. Labs., Murray Hill, USA), P. Markowich, (TU-Vienna, Austria), G. de Mey (University of Ghent, Belgium), B.N. Parlett (University of California, Berkeley, USA), S. Polak (Philips, Eindhoven, The Netherlands), Ph. Toint (University of Namur, Belgium). (J.G. Verwer)

Study group on Graphics Standards. Monthly. (M. Bakker)

Study group on Dialogue Programming. (P.J.W. ten Hagen)

Distributed Systems Day. 26 July. Invited speakers:
O. Berry (University of Southern California, Los Angeles, USA), U. Manber (University of Wisconsin, Madison, USA). (S.J. Mullender, P.M.B. Vitányi).

Visitors to CWI from Abroad

A. Baddeley (University of Bath, UK) 24-28 June. L. de Branges (Purdue University, West Lafayette, USA) 3 June. F.M. Callier (University of Namen, Belgium) 18-19 April. M.H.A. Davis (Imperial College, London) 17 May. Y. Desmedt (Cath. University of Leuven, Belgium) 11-14 June. M. Duflo (University of Paris VII, France) 18-20 April. R.L. Griess Jr. (University of Michigan, Ann Arbor, USA) 20-23 April. P.H. Hochschild (Stanford University, USA) 10-12 April. E. Horozov (Sofia University, Bulgaria) 12-21 June. M. Husvek (Karel University, Prague, Czechoslovakia) 17-28 June. M. Husková (Karel University, Prague, Czechoslovakia) 22 May. J. Jacod (University Pierre and Marie Curie, Paris VI, France) 15-17 May. W. Jäger (SFB 123, Heidelberg, West Germany) 13-15 May. T.A. Louis (Harvard School of Public Health, Boston, USA) 16-20 June. A. Mazurkiewicz (Polish Academy of Science, Poland) 24 May. J.B. Orlin (M.I.T., Cambridge, USA) May. A. Pfitzmann (University of Karlsruhe, West Germany) 30-31 May. Sue-Ken Yap (University of Rochester, USA) June, July, and August. A.N. Shiryayev (Steklov Institute, Moscow, USSR) 21 April-20 May. D.B. Shmoys (Harvard University, Cambridge, USA) 11-28 April. K. Strehmel (Martin-Luther University, Halle, DDR) 22-26 April. Y. Sunahara (Kyoto University, Japan) 27 June. E. Tardos (University of Budapest, Hungary) 6 May. B. Taylor (University of Sherbrooke, USA) 14 April-10 May. L.E. Trotter, Jr. (Cornell University, Ithaca, USA) 1-2 May. C. Vercellis (University of Milan, Italy) 30-31 May. J. Waldvogel (ETH, Zürich, Switzerland) 3 June. T. de Wet (University of Simonstown, South Africa) 29-30 May. J. Winkin (University of Namen, Belgium) 18-19 April.

Order Form for CWI Publications

Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

☐ Please send the publications marked below on an exchange basis
☐ Please send the publications marked below with an invoice

	Publication code	Price per copy	Number of copies wanted
☐	CWI Tract 16 *)	Dfl. 21.40	....
☐	CWI Tract 17 *)	27.40	....
☐	CWI Tract 18 *)	19.10	....
☐	CWI Syllabus 2 *)	31.--	....
☐	CS-R8502	3.70	....
☐	CS-R8503	3.70	....
☐	CS-R8504	14.30	....
☐	CS-R8505	4.80	....
☐	CS-R8506	3.70	....
☐	CS-R8507	3.70	....
☐	CS-R8508	3.70	....
☐	CS-R8509	3.70	....
☐	CS-R8510	4.80	....
☐	CS-R8511	6.--	....

*) not available on exchange

	Publication code	Price per copy	Number of copies wanted
☐	CS-N8504	3.70	....
☐	OS-R8501	3.70	....
☐	OS-R8502	3.70	....
☐	OS-R8503	3,70	....
☐	OS-R8504	6.--	....
☐	OS-R8505	3.70	....
☐	NM-R8502	3.70	....
☐	NM-R8503	6.--	....
☐	NM-R8504	3.70	....
☐	NM-R8505	3.70	....
☐	NM-R8506	3.70	....
☐	MS-R8501	3.70	....
☐	MS-R8502	3.70	....
☐	MS-N8501	6.--	....
☐	AM-R8501	3.70	....
☐	AM-R8506	3.70	....
☐	AM-R8507	3.70	....
☐	AM-R8508	3.70	....
☐	AM-R8509	3.70	....

If you wish to order any of the above publications please tick the appropriate boxes and return the completed form to our Sales Department.
Don't forget to add your name and address!
Prices are given in Dutch guilders and are subject to change without notice. Foreign payments are subject to a surcharge per remittance to cover bank, postal and handling charges.

Name ....

Street ....

City ....

Country ....

Cryptography

An in depth course October 14-25 1985 at the Centre for Mathematics and Computer Science, Amsterdam, with support of the Commission of European Communities CREST-ITG subcommittee.

Taught by leading experts making theoretical advances and those developing leading edge applications; designed to give a good theoretical and practical background for doing research and/or development.

Lecturers

D. Chaum, course director

E. Brickell	S.T. Kent
A.E. Brouwer	A.K. Lenstra
Y. Desmedt	J.H. van Lint
J-H. Evertse	P.G. Maclaine Pont
S. Goldwasser	H. van der Meer
J. Gordon	S. Micali
A. Grissonnanche	G.I. Parkin
L. Guillou	W.L. Price
W. Haemers	R.L. Rivest
C. Holloway	I. Schaumuller-Bichl
I. Ingemarsson	A.S. Tanenbaum
C.J.A. Jansen	J. Vandewalle

Topic Areas

Theory *(week 1)* classical systems; fundamentals; information theory; coding theory; shift registers; block ciphers; authentication; data encryption standard (des); knapsacks; factoring integers and polynomials; discrete log problem; public key systems; complexity theory and security; pseudorandom generators; secure signatures; and crypto protocols.

Applications *(week 2)* untraceable transactions; open shops for information services (OSIS); smart cards; key distribution; security in connection based networks; security in the open systems interconnection model (OSI); security in transaction networks; eft; public key implementation; access control; software protection; secure office automation; and standards.

SPONSORSHIP

Jointly sponsored by the Commission of European Communities CREST-ITG subcommitee and the Centre for Mathematics and Computer Science (formerly called Mathematisch Centrum), Amsterdam.

INFORMATION:

Crypto Course
Kruislaan 413
1098 SJ Amsterdam
The Netherlands
Telex 12579 mctr nl
Telephone +31 (020) 5924171

NEWSLETTER CWI NEWSLETTER CWI NEW

Contents