CWI NEWSLETTER

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

Quarterly, Issue no.2
March 1984

在中国的三周

CWI NEWSLETTER

Number 2, March 1984

Editors

Arjeh M. Cohen Richard D. Gill Jan Heering

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

Calligraphy on the cover by H.T. Sie, Postmuseum, The Hague.

Contents

CWI

Centre for Mathematics
and Computer Science
Centrum voor Wiskunde en Informatica

Two Applications of Topological Dynamics in Combinatorial Number Theory

The shift system and the Stone-Čech compactification of the non-negative integers

by Jan de Vries

In Combinatorial Number Theory, various results say that if $\mathbb{Z}^+$ is partitioned into finitely many sets, then one of those sets is large in some sense. Theorems of this type were obtained by Hilbert, Schur, Van der Waerden, Rado and Hindman among others (see [9] and its references). For example, in Van der Waerden's result, 'large' means: containing arithmetic progressions of arbitrary finite length. In this paper, proofs of Van der Waerden's Theorem (2.6 below) and Hindman's Theorem (4.1 below) will be given using methods from Topological Dynamics.

This paper will also illustrate certain techniques from 'abstract' Topological Dynamics, i.e. Topological Dynamics in the tradition of, say, Gottschalk and Hedlund and of Robert Ellis (see [10], [7]). Roughly, Topological Dynamics can be described as the discipline in which one studies asymptotic and recurrence properties of points in a topological space under the action of a group of homeomorphisms or a semigroup of continuous mappings. A historical sketch of this field of mathematical research falls outside the scope of this paper. Let me just say that Topological Dynamics, together with Ergodic Theory, originated from the qualitative theory of differential equations; see for instance [15] or the introductions of [3] or [18] for brief historical sketches. The results that will be presented in this paper are from 'abstract' Topological Dynamics, i.e. there is no direct relationship with the theory of differential equations.

Finally, this paper may be seen as an attempt to persuade the reader to have a look in the beautiful book [8] (although there the main role is played by Ergodic Theory) or at least the paper [9]. Essentially, the present paper is based on [9]; in particular, the proof of Van der Waerden's Theorem is taken from [9]: I have included it just to show how elegantly it follows from an admittedly rather deep dynamical result. The proof of Hindman's theorem is different from the one in [9]; as far as I know, the present proof does not appear in the existing literature. I learned it from a discussion with Dr. B. Balcar (Prague).

The paper is essentially self contained (except for the proof of the Multiple Recurrence Theorem, i.e. Theorem 1.4 below). It can be read by anybody who knows some elementary topology and the basic properties of ultrafilters (summarized in Section 4).

1. Introduction

A *dynamical system* is a pair (X,T) with X a compact Hausdorff space and $T:X \to X$ a continuous mapping. A *homomorphism of dynamical systems* $\phi:(X,T) \to (X',T')$ is a continuous mapping $\phi:X \to X'$ such that $\phi \circ T = T' \circ \phi$. Most of the dynamical properties of a dynamical system are preserved by homomorphisms; the proof that this is so for the notions to be defined below (orbit, orbit-closure, recurrence, almost periodicity) will be left to the reader.

Let (X,T) be a dynamical system. The *orbit* of a point x in X is the set $O(x) := \{T^n x \colon n \in \mathbf{Z}^+\}$; here T^n is the n'th iterate of T, so $T^n := T \circ T^{n-1}$ $(n = 2,3,...)$, while $T^1 := T$ and $T^0 = id_X$. The *orbit-closure* of x is the closure $\overline{O(x)}$ of the orbit $O(x)$. A point x in X is called *recurrent* whenever it is in the orbit-closure of x. Equivalently, x is recurrent iff for every nbd(= neighbourhood) U of x there exists $n \geqslant 1$ such that $T^n x \in U$. Clearly, if x is a recurrent point, then for each nbd U of x the set of 'return times'

$$R(x,U) := \{n \in \mathbf{Z}^+ \colon n \geqslant 1 \ \& \ T^n x \in U\}$$

is infinite. It is easy to see that if the space X is metrizable, then a point x is recurrent iff there is an increasing sequence $n_1, n_2, ...$ in $\mathbf{Z}^+$ such that $x = \lim_{i \to \infty} T^{n_i} x$.

Recurrent points do exist abundantly. The easiest way to prove this is by invoking the axiom of choice. In fact more will be shown, namely, that uniformly recurrent (terminology of e.g. [2] and [8]) or, as I will call them (terminology of e.g. [7], [10] and [17]), almost periodic points exist. A point x in X is called *almost periodic* whenever for each nbd U of x the set $R(x,U)$ has bounded gaps. This is equivalent to saying that for every nbd U of x there exists $l > 0$ such that

$$\forall n \in \mathbf{Z}^+ \ \exists r \in \{0,...,l\} \colon T^{n+r} x \in U.$$

(It has been remarked that a periodic point returns to itself every hour exactly on the hour; but an almost periodic point returns to a nbd every hour within the hour.) There is a nice characterization of almost periodicity in terms of minimal subsets. A closed subset A of X is called *minimal* whenever $A \neq \varnothing$, A is invariant (that is, $TA \subseteq A$) and A has no closed invariant proper subsets. It is easy to show that a non-empty subset A of x is minimal iff $\overline{O(x)} = A$ for every $x \in A$. (Note that orbits and their closures are invariant.)

1.1. LEMMA. *Let (X,T) be a dynamical system. Every non-empty closed invariant subset of X contains a minimal subset.*

PROOF. Apply Zorn's lemma to the partially ordered (with respect to inclusion) family of all non-empty closed invariant subsets of X. This family is not empty (X belongs to it), and the intersection of a chain in it is non-empty because X is compact. □

Here is the promised characterization of almost periodicity; the result is a form of Birkhoff's Recurrence Theorem:

1.2. PROPOSITION. *Let (X,T) be a dynamical system and $x \in X$. The following statements are equivalent:*
(i) x is an almost periodic point;
(ii) $\overline{O(x)}$ is a minimal set.

PROOF. $(i) \Rightarrow (ii)$: Clearly, $\overline{O(x)}$ is non-empty, closed and invariant. It remains to prove that if $y \in \overline{O(x)}$ then $x \in \overline{O(y)}$. Let U be a nbd of x. Almost periodicity of x implies that there exists $l>0$ such that for every $i \in \mathbb{Z}$, $T^{i+r}x \in U$ for some $r \in \{0,...,l\}$; that is

$$T^i x \in \bigcup_{r=0}^{l} T^{-r}[U].$$

So $O(x) \subseteq \cup_{r=0}^{l} T^{-r}[U]$, hence $\overline{O(x)} \subseteq \cup_{r=0}^{l} T^{-r}[\overline{U}]$. Consequently, if $y \in \overline{O(x)}$, then $T^r y \in \overline{U}$ for some $r \in \{0,...,l\}$ and this means that $\overline{U} \cap O(y) \neq \emptyset$. As every nbd W of x includes the closure of some smaller nbd of x, this implies that $W \cap O(y) \neq \emptyset$ for every nbd W of x. Hence $x \in \overline{O(y)}$.

$(ii) \Rightarrow (i)$: Let U be a nbd of x. By minimality, one has for every $z \in \overline{O(x)}$ that $x \in \overline{O(z)}$, hence $U \cap O(z) \neq \emptyset$, i.e. $z \in T^{-r}[U]$ for some $r \in \mathbb{Z}^+$. This shows that $\overline{O(x)} \subseteq \cup_{r=0}^{\infty} T^{-r}[U]$, and compactness implies that $\overline{O(x)}$ can be covered by finitely many of the sets $T^{-r}[U]$, say with $r \in \{0,...,l\}$. In particular, for each $n \in \mathbb{Z}^+$ there exists $r \in \{0,...,l\}$ such that $T^n x \in T^{-r}[U]$, hence $T^{n+r}x \in U$. □

1.3. COROLLARY. *Let (X,T) be a dynamical system. Every non-empty closed invariant subset of X, in particular X itself, contains an almost periodic point.* □

Remark. Since homomorphisms of dynamical systems preserve almost periodicity (this is almost trivial), it follows from 1.2 that homomorphisms preserve minimal sets: if $\phi:(X,T) \rightarrow (X',T')$ is a homomorphism and M is a mimimal subset of X, then $\phi[M]$ is a minimal subset of X'. (Of course, this can also be proved rather easily directly!)

As every almost periodic point is recurrent, it follows from 1.3 that every dynamical system has recurrent points. Other proofs of this fact are possible, e.g. using the existence of an invariant measure (the Poincaré Recurrence Theorem). The following result is much stronger, although its validity is restricted to metrizable spaces (as long as one is not willing to use 'exceptional' axioms like Martin's Axiom). If X is a compact Hausdorff space and if for $j = 1,...,l$ $T_j : X \rightarrow X$ is a continuous mapping, then a point x in X is called *multiply recurrent* (under $T_1,...,T_l$) whenever for each nbd U of x there exists $n \geqslant 1$ such that $T_j^n x \in U$ for $j = 1,...,l$. If X is metrizable, then x is multiply recurrent under $T_1,...,T_l$ iff there exists an increasing sequence $n_1, n_2,...$ in $\mathbb{Z}^+$ such that $x = \lim_{i \rightarrow \infty} T_j^{n_i} x$ for $j = 1,...,l$.

1.4. THEOREM. *Let X be a compact metrizable space, and for $j = 1,...,l$, let $T_j : X \rightarrow X$ be mutually commuting continuous mappings. Then there exists a mutually recurrent point in X.*

PROOF. See [9], or [8] Chapter 2. □

In the next section, we describe an application of this result due to H. Furstenberg and B. Weiss (see [9]).

2. Symbolic dynamics

An important source of examples are the so-called shift systems and their subsystems. For literature on these systems, see for example [14] and its references. For applications to the investigation of Anosov diffeomorphisms, see [4], and for applications in coding theory, see [1]. We shall use the shift system mainly for illustration of the notions defined in Section 1.

2.1. Let S be a finite set, say $S = \{0,..., s-1\}$ with $s \geqslant 2$, and let $\Omega := S^{\mathbf{Z}^+}$, the space of all (one-sided) infinite sequences $(\xi(0),\xi(1),\xi(2),...)$ with $\xi(n) \in S$ for $n \geqslant 0$. With the usual product topology, Ω is a compact Hausdorff space, homeomorphic with the Cantor discontinuum. A basis for the nbd system of a point ξ in Ω is formed by the set of all so-called *cylinders*, i.e. all sets of the form

$$[\xi(0),...,\xi(k)] := \{\eta \in \Omega \vdots \eta(i) = \xi(i) \text{ for } i = 0,...,k\}$$

with $k \in \mathbf{Z}^+$.

The (one-sided) *shift* on Ω is the continuous mapping $\sigma : \Omega \rightarrow \Omega$ given by

$$(\sigma\xi)(n) := \xi(n+1) \quad \text{for } n \in \mathbf{Z}^+$$

where $\xi = (\xi(n))_{n \in \mathbf{Z}^+}$ in Ω. Thus, σ shifts sequences ξ one place to the left. Note that σ is an s-to-one mapping: the s possible values for $\xi(0)$ do not affect the value of $\sigma\xi$. (In a similar way, a two-sided shift can be defined on the space $S^{\mathbf{Z}}$, and this is a homeomorphism.) We consider the dynamical system (Ω,σ).

Observe that for $\xi,\eta \in \Omega$ and $k \in \mathbf{Z}^+$ one has $\sigma^r \eta \in [\xi(0),...,\xi(k)]$ for some $r \in \mathbf{Z}^+$ if and only if the finite sequence ('block') $\xi(0),...,\xi(k)$ occurs in η at place r, that is, if and only if $\xi(i) = \eta(r+i)$ for $i = 0,...,k$. Using this, the following observations are easy to prove:

2.2. OBSERVATIONS. (i) *A point ξ in Ω has a dense orbit iff every finite block over S occurs in ξ at some place.*
(ii) *A point ξ in Ω is recurrent iff every block which occurs in ξ occurs infinitely often in ξ.*
(iii) *A point ξ in Ω is almost periodic iff each block B which occurs in ξ occurs with bounded gaps, that is, there exists a number $l > 0$ such that every block of length l in ξ contains a copy of B.*

2.3. In view of the characterizations mentioned in 2.2, the following facts are almost trivial:
(i) *There exists a point in Ω which has a dense orbit:* let $B_1,B_2,...$ be an enumeration of all possible finite blocks. Then the point

$$\xi_0 = B_1 B_2 ...,$$

i.e. the sequence which is obtained from concatenation of all blocks B_i, has a

dense orbit by 2.2 (i).
(ii) *The point* ξ_0 *defined in* (i) *is recurrent:* let B be a block which occurs in ξ_0; then B occurs in some beginning block $B' := B_1 ... B_k$ with $k \in \mathbb{N}$. In the sequence of all blocks $B_1, B_2,...$ the block B' has a place with index $\geqslant k+1$. Hence the original block B occurs in ξ also at some place $\geqslant k+1$. Repetition of this argument shows that B occurs infinitely often in ξ_0. So by 2.2(ii) the point ξ_0 is recurrent.

Remark. If η is an arbitrary recurrent point of Ω and B is an arbitrary block from the beginning of η, then by 2.2(ii) there is a block C such that $\eta = BCB....$ Repeating this procedure, starting with the 1-element block a given by $a = \eta(0)$, we see that

$$\eta = \{(aC_1a)C_2(aC_1a)\}C_3\{(aC_1a)C_2(aC_1a)\}...$$

for certain blocks $C_1, C_2,....$ Conversely, every sequence η with this structure is recurrent.

(iii) *The set* Ω *is not minimal under the shift:* there are many non-empty closed invariant subsets, e.g. the (finite) orbits of the periodic points, i.e. all sequences which have the following form:

$$\zeta = BBB...B...$$

for some finite block B. (Note that the set of periodic points is dense in Ω: if $\xi \in \Omega$, then the cylindrical nbd $[\xi(0),...,\xi(k)]$ of ξ contains the periodic point $\zeta = BBB...$ with $B := \xi(0)...\xi(k)$.) So it follows from 1.2 that the point ξ_0 defined in (i) above is *not* almost periodic.

Remark. It follows immediately from Observation 2.2(iii) that a recurrent point of the form

$$\eta = \{(aC_1a)C_2(aC_1a)\}C_3\{(aC_1a)C_2(aC_1a)\}...$$

is almost periodic iff the blocks $C_1, C_2,...$ have bounded lengths. All kinds of methods have been invented to produce almost periodic points in Ω (i.e. minimal orbit-closures) and points whose orbit closures have other topological-dynamical or ergodic properties. For an important method - substitutions - cf. [19]. A famous almost periodic point is the so-called Morse sequence

$$\underbrace{\underbrace{\underset{B_1}{01}\qquad\underset{B_1'}{10}}_{B_2}\qquad\underset{B_2'}{1001}}_{B_3}\qquad\underset{B_3'}{10010110}\quad\cdots$$

(Here B' denotes the block which is obtained from B by replacing every 0 by a 1 and every 1 by a 0).
(iv) *Although there are many recurrent points (it can be shown that they form a residual subset, i.e. they contain a dense* G_δ*-set; cf. [10], 7.15 and 12.24(2); this*

follows also rather easily from the description given in (ii) above), there are also many non-recurrent points; e.g. the point 101001000100001··· is not recurrent.

2.4. For the proof of the next theorem, it will be convenient to use the following metric d on Ω:

$$d(\xi,\eta) := \begin{cases} (1+\ \min\{n\in\mathbf{Z}^+ : \xi(n)\neq\eta(n)\})^{-1} & \text{if } \xi\neq\eta \\ 0 & \text{if } \xi=\eta. \end{cases}$$

It is straightforward to verify that d is a metric. In addition, for every $\xi\in\Omega$ one has

$$[\xi(0),...,\xi(k)] = \{\eta\in\Omega : d(\xi,\eta)\leqslant\frac{1}{k+2}\}.$$

This implies immediately that d is compatible with the topology of Ω. The following special feature of the metric d will be needed: if $\xi,\eta\in\Omega$ and $d(\xi,\eta)<1$, then $\xi(0) = \eta(0)$.

2.5. Elements of Ω can be used to describe partitions of $\mathbf{Z}^+$ as follows. Suppose $\mathbf{Z}^+ = B_0\cup...\cup B_{q-1}$ with $B_i\cap B_j = \varnothing$ for $i\neq j$. Let $S:=\{0,...,q-1\}$ and $\Omega := S^{\mathbf{Z}^+}$, and consider the point $\xi = (\xi(n))_{n\in\mathbf{Z}^+}\in\Omega$ with

$$\xi(n) := i \quad \text{if} \quad n\in B_i \quad (i = 0,...,q-1)$$

Thus, ξ registers the 'colour' i for each $n\in\mathbf{Z}^+$. Conversely, it is clear that every point ξ in Ω defines a partition of $\mathbf{Z}^+$ into q disjoint subsets such that the given point ξ gives the 'colouring' of this partition. This correspondence is the basis of the proof of the following theorem.

2.6. THEOREM (Van der Waerden). *Let $\mathbf{Z}^+ = B_0\cup...\cup B_{q-1}$ with $B_i\cap B_j = \varnothing$ for $i\neq j$. Then one of the sets B_i contains arithmetic progressions of arbitrary length.*

PROOF. ([9], [10]). It is sufficient to show that for every $l\in\mathbf{Z}^+$, $l\neq 0$, there exists an index $i(l)\in\{0,...,q-1\}$ and numbers n, $m\in\mathbf{Z}^+$ (also depending on l) such that $m+jn\in B_{i(l)}$ for $j = 0,...,l$. Indeed, since there are only q possible values for $i(l)$, there is $i_0\in\{0,...,q-1\}$ such that $i(l) = i_0$ for infinitely many values of l in $\mathbf{Z}^+$; then B_{i_0} contains arithmetical progressions of arbitrary length.

Let $\Omega := \{0,...,q-1\}^{\mathbf{Z}^+}$ and form $\xi_0\in\Omega$ corresponding to the given partition of $\mathbf{Z}^+$ as indicated in 2.5. Let $X:=\overline{O(\xi_0)}$ and let for any given integer $l>0$ and $j = 1,...,l$ the mappings $T_j:X\rightarrow X$ be defined by $T_j := (\sigma|_X)^j$. Then the continuous mappings $T_1,...,T_l$ satisfy the hypothesis of Theorem 1.4, so there exists a point $\eta\in X$ and an increasing sequence $n_1,n_2,...$ such that

$$T_j^{n_k}\eta\rightarrow\eta \quad \text{for } k\rightarrow\infty \ (j = 1,...,l).$$

Consequently, there exists $n\in\mathbf{N}$ such that the points η, $T_1^n\eta$, $T_2^n\eta$, ..., $T_l^n\eta$, that is, the points

$$\eta,\ \sigma^n\eta,\ \sigma^{2n}\eta,\ ...,\ \sigma^{ln}\eta$$

have mutual distances $<\frac{1}{2}$. By continuity of the maps σ^{jn}, $j = 0,...,l$, there exists a nbd V of η in Ω such that for each $\eta' \in V$ the points

$$\eta',\ \sigma^n \eta',\ \sigma^{2n} \eta',\ ..., \sigma^{ln} \eta'$$

also have distances $<\frac{1}{2}$. As $\eta \in X = \overline{O(\xi_0)}$, $V \cap O(\xi_0) \neq \varnothing$, hence $\sigma^m \xi_0 \in V$ for some $m \in \mathbf{Z}^+$, and the points

$$\sigma^m \xi_0,\ \sigma^{m+n} \xi_0,\ \sigma^{m+2n} \xi_0,\ ...,\ \sigma^{m+ln} \xi_0$$

have distances $<\frac{1}{2}$. By the last remark of 2.4, these points have equal zero'th coordinates, that is,

$$\xi_0(m) = \xi_0(m+n) = \xi_0(m+2n) = ... = \xi_0(m+ln).$$

If we denote this value by $i(l)$, then this shows that the set $B_{i(l)}$ contains the arithmetic progression $m, m+n, m+2n, ..., m+ln$ of length $l+1$. □

3. The semigroup $\beta\mathbf{Z}^+$

In this section the basic elements will be discussed of a machinery that is one of the corner stones of abstract topological dynamics. For a thorough discussion in a general context see [7] (or [5]). In this paper, we will develop just enough of this machinery to present a very elegant proof of Hindman's Theorem (Theorem 4.1 below). The key idea is to consider a natural semigroup structure on the Stone-Čech compactification of $\mathbf{Z}^+$ (denoted $\beta\mathbf{Z}^+$) and to relate dynamical properties of a point in a dynamical system with the algebraic structure of $\beta\mathbf{Z}^+$.

3.1. For those who do not use the concept of Stone-Čech compactification in their daily work, a few basic facts will be recalled.

The space $\beta\mathbf{Z}^+$ is a compact Hausdorff space which contains $\mathbf{Z}^+$ as a dense subspace. It is characterised by the following 'universal' property: every mapping $\psi: \mathbf{Z}^+ \to X$ with X a compact Hausdorff space has a unique continuous extension $\overline{\psi}: \beta\mathbf{Z}^+ \to X$. For a proof that a space $\beta\mathbf{Z}^+$ with these properties exists and is unique up to homeomorphism, the reader is referred to introductory topology textbooks. Concerning a useful model for $\beta\mathbf{Z}^+$ some remarks will be made in Section 4 below.

3.2. The universal property of $\beta\mathbf{Z}^+$ mentioned above implies that for every $n \in \mathbf{Z}^+$ the mapping

$$\omega^n : k \mapsto n+k : \mathbf{Z}^+ \to \mathbf{Z}^+ \subset \beta\mathbf{Z}^+$$

has a continuous extension to $\beta\mathbf{Z}^+$, which will also be denoted by ω^n. The value of $\xi \in \beta\mathbf{Z}^+$ under ω^n will be denoted by $n \oplus \xi$:

$$\omega^n : \xi \mapsto n \oplus \xi : \beta\mathbf{Z}^+ \to \beta\mathbf{Z}^+. \tag{1}$$

This implies that for every $\xi \in \beta\mathbf{Z}^+$ the mapping

$$\omega_\xi : n \mapsto n \oplus \xi : \mathbf{Z}^+ \to \beta\mathbf{Z}^+$$

is well defined. It has a continuous extension, denoted by

$$\omega_\xi\colon\ \eta\mapsto\eta\oplus\xi\colon\ \beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}. \tag{2}$$

Now a mapping $\omega\colon\beta\mathbb{Z}^{+}\times\beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$ can be defined by

$$\omega(\eta,\xi) := \omega_\xi(\eta) = \eta\oplus\xi \quad \text{for } \xi,\eta\in\beta\mathbb{Z}^{+}\cdot$$

Note that ω extends the addition in $\mathbb{Z}^{+}$ to all of $\beta\mathbb{Z}^{+}$. It can be shown that ω is not commutative on $\beta\mathbb{Z}^{+}$. Related to this is the fact that all right translations $\omega_\xi\colon\eta\mapsto\eta\oplus\xi$: $\beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$ for $\xi\in\beta\mathbb{Z}^{+}$ are continuous (cf. (2) above), but not all left translations ω^η: $\xi\mapsto\eta\oplus\xi$: $\beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$ for $\omega\in\beta\mathbb{Z}^{+}$ (notice the place of ξ and η as sub- respectively super-script). In particular, $\omega\colon\beta\mathbb{Z}^{+}\times\beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$ is not continuous. (For each $n\in\mathbb{Z}^{+}$, ω^n is continuous (cf. (1) above), and no doubt the $\beta\mathbb{Z}^{+}$-specialists have figured out characterizations for those points $\eta\in\beta\mathbb{Z}^{+}\setminus\mathbb{Z}^{+}$ for which ω^η is continuous, but until now I have found none in the literature.) The 'addition' ω in $\beta\mathbb{Z}^{+}$ is associative. The straightforward proof is as follows: for all $m,n\in\mathbb{Z}^{+}$ the continuous (!) mappings

$$\left.\begin{array}{l} \omega^{m+n}\colon\ \zeta\mapsto(m+n)\oplus\zeta \\ \omega^{m}\circ\omega^{n}\colon\ \zeta\mapsto m\oplus(n\oplus\zeta) \end{array}\right\}\colon\ \beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$$

are equal to each other on the dense subset $\mathbb{Z}^{+}$ of $\beta\mathbb{Z}^{+}$ (associativity of addition in $\mathbb{Z}^{+}$). Hence they are equal on all of $\beta\mathbb{Z}^{+}$. This means exactly that for all $m\in\mathbb{Z}^{+}$ and $\zeta\in\beta\mathbb{Z}^{+}$ the continuous (!) mappings

$$\left.\begin{array}{l} \omega_\zeta\circ\omega^{m}\colon\ \eta\mapsto(m\oplus\eta)\oplus\zeta \\ \omega^{m}\circ\omega_\zeta\colon\eta\mapsto m\oplus(\eta\oplus\zeta) \end{array}\right\}\colon\ \beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$$

are equal on $\mathbb{Z}^{+}$. Hence they coincide on all of $\beta\mathbb{Z}^{+}$. This can be rephrased by saying that the continuous mappings $\omega_\zeta\circ\omega_\eta$ and $\omega_{\eta\oplus\zeta}$ are equal on $\mathbb{Z}^{+}$. Hence they are equal on $\beta\mathbb{Z}^{+}$, which means that $(\xi\oplus\eta)\oplus\zeta = \xi\oplus(\eta\oplus\zeta)$ for all ξ,η and ζ in $\beta\mathbb{Z}^{+}$.

Conclusion: *$(\beta\mathbb{Z}^{+},\oplus)$ is an (associative) semigroup in which $\mathbb{Z}^{+}$ is a dense subsemigroup. All right translations ω_ξ with $\xi\in\beta\mathbb{Z}^{+}$ are continuous, and so are the left translations ω^n with $n\in\mathbb{Z}^{+}$.*

3.3. Let $\tilde{T}\colon\beta\mathbb{Z}^{+}\to\beta\mathbb{Z}^{+}$ be defined by $\tilde{T} := \omega^1$, that is $\tilde{T}\xi := 1\oplus\xi$ for $\xi\in\beta\mathbb{Z}^{+}$. Then $(\beta\mathbb{Z}^{+},\tilde{T})$ is a dynamical system. The following proposition gives a relationship between dynamical properties of $(\beta\mathbb{Z}^{+},\tilde{T})$ and algebraic properties of the semigroup $(\beta\mathbb{Z}^{+},\oplus)$. First we need two definitions. An *idempotent* in $\beta\mathbb{Z}^{+}$ is an element ξ such that $\xi\oplus\xi = \xi$. A *left ideal* in $\beta\mathbb{Z}^{+}$ is a non-empty subset K such that $\beta\mathbb{Z}^{+}\oplus K\subseteq K$ (if P,Q are subsets of $\beta\mathbb{Z}^{+}$, then of course $P\oplus Q := \{\xi\oplus\eta \,\vdots\, \xi\in P \;\&\; \eta\in Q\}$; similarly, $P\oplus\eta := \{\xi\oplus\eta \,\vdots\, \xi\in P\} = \omega_\eta[P]$, etc.). A *minimal left ideal* is a left ideal which does not properly contain any other left ideal. Since for every left ideal K and every element $\xi\in K$ one has $\beta\mathbb{Z}^{+}\oplus\xi = \omega_\xi[\beta\mathbb{Z}^{+}]\subseteq K$, where $\beta\mathbb{Z}^{+}\oplus\xi$ is a left ideal (trivial) which is compact, hence closed in $\beta\mathbb{Z}^{+}$ (image of $\beta\mathbb{Z}^{+}$ under the continuous right translation ω_ξ), *every minimal left ideal is closed.* Hence the minimal left ideals are the minimal elements of the partially ordered (under inclusion) set of all closed left ideals, and a traditional Zorn argument shows that every closed left ideal contains a minimal left ideal. However, the existence of minimal left ideals will also follow from 3.4(ii) below in combination with Lemma 1.1. In the proof of the proposition below, we shall use the notion of filter base. Those who are not acquainted with this notion might want to read the definition in Section 4 first.

3.4. PROPOSITION. *Let M be a non-empty closed subset of $\beta\mathbb{Z}^+$ and let $\xi\in\beta\mathbb{Z}^+$. Then the following equivalences are valid:*
(i) *M is invariant under $\tilde{T} \Leftrightarrow M$ is a left ideal;*
(ii) *M is minimal under $\tilde{T} \Leftrightarrow M$ is a minimal left ideal;*
(iii) *ξ is recurrent under $\tilde{T} \Leftrightarrow \exists \eta\in\beta\mathbb{Z}^+\setminus\mathbb{Z}^+ : \eta\oplus\xi = \xi$;*
(iv) *ξ is almost periodic under $\tilde{T} \Leftrightarrow \exists$ minimal left ideal $M : \xi\in M$.*
Moreover, the element η in (iii) can always be assumed to be an idempotent.

PROOF. (i): M is invariant under $\tilde{T}$ iff $\mathbb{Z}^+\oplus M\subseteq M$, that is, $\omega_\xi[\mathbb{Z}^+]\subseteq M$ for every $\xi\in M$. Since ω_ξ is continuous and M is closed, this is equivalent to $\omega_\xi[\beta\mathbb{Z}^+]\subseteq M$ for every $\xi\in M$, that is, $\beta\mathbb{Z}^+\oplus M\subseteq M$.
(ii): Clear from (i).
(iii): '⇒'. Let $\xi\in\Omega$ be recurrent. Then the family $\{R(\xi,U) : U \text{ a nbd of } \xi\}$ is a filter base in $\mathbb{Z}^+$, which has an adherence point $\eta\in\beta\mathbb{Z}^+$, i.e. $\eta\in\cap\{\overline{R(\xi,U)} : U \text{ a nbd of } \xi\}$ (the bar denotes closure in $\beta\mathbb{Z}^+$). We may assume that $\eta\notin\mathbb{Z}^+$. Indeed, if ξ is not periodic, then this filter base is not fixed, that is, no $n\in\mathbb{Z}^+$ belongs to all sets $R(\xi,U)$. Consequently, the point η does not belong to $\mathbb{Z}^+$. If ξ is periodic, say with period n, then the sequence $\{kn\}_{k\in\mathbb{N}}$ has an adherence point $\eta\in\beta\mathbb{Z}^+\setminus\mathbb{Z}^+$. Clearly, η is in $\overline{R(\xi,U)}$ for every nbd U of ξ, that is, η is an adherence point of the filter base. So in all cases we have an adherence point $\eta\in\beta\mathbb{Z}^+\setminus\mathbb{Z}^+$. As the mapping ω_ξ is continuous, $\omega_\xi(\eta) = \eta\oplus\xi$ is an adherence point of the filter basis $\{R(\xi,U)\oplus\xi : U \text{ a nbd of } \xi\}$. However, $R(\xi,U)\oplus\xi\subseteq U$, hence $\eta\oplus\xi\in\overline{U}$ for every nbd U of ξ. As $\beta\mathbb{Z}^+$ is a Hausdorff space, this implies that $\eta\oplus\xi = \xi$.
'⇐' Let U be a nbd of ξ. As $\omega_\xi(\eta) = \xi$, continuity of ω_ξ implies that there is a nbd V of η such that $\omega_\xi[V]\subseteq U$, that is, $V\oplus\xi\subseteq U$. As $\mathbb{Z}^+$ is dense in $\beta\mathbb{Z}^+$ and $\eta\neq 0$, V may be chosen so that $0\notin V\cap\mathbb{Z}^+\varnothing$. Hence there exists $n\in\mathbb{Z}^+$, $n\neq 0$ with $\tilde{T}^n\xi\in U$ (any $n\in V$ suffices).
(iv) Clear from (ii) and 1.2.
In the case that ξ is a recurrent point, (iii) shows that the subset $\{\eta\in\beta\mathbb{Z}^+\setminus\mathbb{Z}^+ : \eta\oplus\xi = \xi\}$ is not empty. It is easily seen that this is a subsemigroup of $\beta\mathbb{Z}^+$. Finally, since it is the intersection of the closed sets $\beta\mathbb{Z}^+\setminus\mathbb{Z}^+$ and $\omega_\xi^{-1}[\xi]$ (again, by continuity of ω_ξ), it is a non-empty, closed subsemigroup of $\beta\mathbb{Z}^+$. By Lemma 3.6 below, it contains an idempotent. □

3.5. COROLLARY. *For every idempotent $\eta\in\beta\mathbb{Z}^+\setminus\mathbb{Z}$ and every element $\xi\in\beta\mathbb{Z}^+$, $\eta\oplus\xi$ is recurrent under $\tilde{T}$, and in particular, η is recurrent under $\tilde{T}$. If η is an idempotent in $\beta\mathbb{Z}^+\setminus\mathbb{Z}^+$, then η is almost periodic iff η belongs to a* *minimal left ideal.* □

Remark. It can be shown that $\beta\mathbf{Z}^+$ contains at least 2^c different minimal left ideals ($c :=$ cardinality of $\mathbb{R}$). Note that each minimal left ideal is included in $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$. (Otherwise, its intersection with $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ would be a proper closed subideal; that $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ is a left ideal follows from the fact that ω^n maps $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ into $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ for each $n \in \mathbf{Z}^+$. Cf. [12], 6.11.)

Since every minimal left ideal is a closed subsemigroup of $\beta\mathbf{Z}^+$, the lemma below implies that every minimal left ideal contains at least one idempotent. More about the structure of minimal left ideals can be found in [20]. At this point it is instructive to observe that any minimal left ideal, as a minimal subset of the dynamical system $(\beta\mathbf{Z}^+, \tilde{T})$, is the orbit closure of each of its points: in particular, it is the orbit closure of an idempotent. Thus, the almost periodic points of $(\beta\mathbf{Z}_+, \tilde{T})$ are just all points which are in the orbit closures of idempotents $\eta \in \beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ which are situated in a minimal left ideal of $\beta\mathbf{Z}^+$. In 3.8 it will be shown that there exist idempotents in $\beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ that do not belong to any minimal left ideal.

3.6. LEMMA. *Let S be a compact Hausdorff space which has a (multiplicatively written) semigroup structure such that all right translations $p \mapsto pq : S \to S$ with $q \in S$ are continuous. Then S contains an idempotent.*

PROOF ([7], [20]): By Zorn's lemma, S contains a minimal closed nonempty subsemigroup E. Let $q \in E$. Then Eq is a closed (continuous image of E under right translation) subsemigroup of E, so by minimality, $Eq = E$. In particular, $q \in Eq$, so $W := \{p \in E : pq = q\} \neq \varnothing$. Clearly, W is a subsemigroup of E and, again by continuity of right translation over q, W is closed. Now minimality of E implies $W = E$. In particular, $q \in W$, that is, $qq = q$. □

Next, consider an arbitrary dynamical system (X,T). For every $x \in X$, the mapping $\delta_x : n \mapsto T^n x : \mathbf{Z}^+ \to X$ has a continuous extension $\overline{\delta}^x : \beta\mathbf{Z}^+ \to X$. Put $T^\xi x := \overline{\delta}_x(\xi)$ for $\xi \in \beta\mathbf{Z}^+$. This can be done for every $x \in X$, so we obtain a mapping $T^\xi : X \to X$ for every $\xi \in \beta\mathbf{Z}^+$. (It can be shown that T^ξ need not be continuous for every $\xi \in \beta\mathbf{Z}^+$.) By an argument very similar to the proof that the operation $\oplus$ in $\beta\mathbf{Z}^+$ is associative (see 3.2 above), it can be shown that $T^{\eta \oplus \xi} x = T^\eta(T^\xi x)$ for all $x \in X$ and $\xi, \eta \in \beta\mathbf{Z}^+$. Thus,

$$\forall \xi, \eta \in \beta\mathbf{Z}^+ : T^{\eta \oplus \xi} = T^\eta \circ T^\xi.$$

This can be restated as follows: the given action of $\mathbf{Z}^+$ on X (by means of $(n,x) \mapsto T^n x$) can be extended to an action of the semigroup $\beta\mathbf{Z}^+$ on X. In this situation, there are also relations between algebraic properties of the semigroup $(\beta\mathbf{Z}^+, \oplus)$ and the dynamical properties of (X,T).

3.7. PROPOSITION. *Let (X,T) be a dynamical system and let $x \in X$. The following equivalences are valid:*

(i) *x is recurrent* $\Leftrightarrow \exists \eta \in \beta\mathbf{Z}^+ \setminus \mathbf{Z}^+ : T^\eta x = x;$

(ii) *x is almost periodic $\Leftrightarrow\forall$ minimal left ideal M in $\beta\mathbf{Z}^+$ there is an idempotent $\eta\in M$ with $T^\eta x = x$;*

(iii) *x is almost periodic $\Leftrightarrow\exists$ minimal left ideal M in $\beta\mathbf{Z}^+$ such that $T^\eta x = x$ for some $\eta\in M$;*

Also, in (i) *the element η may be assumed to be an idempotent.*

PROOF. (i): Completely similar to 3.4(i).
(ii) Assume that x is almost periodic, i.e. that $\overline{O(x)}$ is minimal. Let M be an arbitrary minimal left ideal in $\beta\mathbf{Z}^+$ i.e. a minimal subset of the dynamical system $(\beta\mathbf{Z}^+,\tilde{T})$ (cf. 3.4). It is easy to check that the continuous function $\overline{\delta}_x:\beta\mathbf{Z}^+\rightarrow X$ defined above satisfies $\overline{\delta}_x\circ\tilde{T} = T\circ\overline{\delta}_x$. So $\overline{\delta}_x$ is a homomorphism of dynamical systems from $(\beta\mathbf{Z}^+,\tilde{T})$ into (X,T). It follows that $\overline{\delta}_x[M]$ is a closed invariant subset of X. However,

$$\overline{\delta}_x[M]\subseteq\overline{\delta}_x[\beta\mathbf{Z}^+] = \overline{\delta}_x[\overline{\mathbf{Z}^+}]\subseteq\overline{\delta_x[\mathbf{Z}^+]} = \overline{O(x)},$$

and by minimality of $\overline{O(x)}$, $\overline{\delta}_x[M] = \overline{O(x)}$. In particular, $x\in\overline{\delta}_x[M]$. Stated differently, the set $\{\eta\in M: T^\eta x = x\}$ is not empty. Obviously, it is a subsemigroup of M, and as $\overline{\delta}_k\,|_M:\eta\mapsto T^\eta x$ is continuous, it is closed. So by 3.6 above it contains an idempotent. This proves one implication. The other implication will follow from the proof of (iii).
(iii) If x is almost periodic, existence of M as wanted follows from the implication proved in (ii). Conversely, assume that $T^\eta x = x$ for some element η of some minimal left ideal. Then $x\in\overline{\delta}_x[M]$. Since M is a minimal subset of $(\beta\mathbf{Z}^+,\tilde{T})$ and $\overline{\delta}_x:(\beta\mathbf{Z}^+,\tilde{T})\rightarrow(X,T)$ is a homomorphism, the remark following 1.3 implies that $\overline{\delta}_x[M]$ is a minimal subset of X. Since $x\in\overline{\delta}_x[M]$, 1.2 implies that x is almost periodic. □

3.8. Remark. In the shift system (Ω,σ) we have observed the existence of a point which is recurrent but not almost periodic. It follows immediately from 3.7 that this implies the existence of an idempotent in $\beta\mathbf{Z}^+\setminus\mathbf{Z}^+$ which is not contained in any minimal left ideal. Consequently, the dynamical system $(\beta\mathbf{Z}^+,\tilde{T})$ also has a point which is recurrent but not almost periodic (cf. 3.5).

4. A characterization of idempotents in $\beta\mathbf{Z}^+\setminus\mathbf{Z}^+$

In this section, we study a particular model of $\beta\mathbf{Z}^+$ in more detail. This will enable us to give a nice description of idempotents in $\beta\mathbf{Z}^+$. Using this, a very short proof of Hindman's theorem is possible. Our proof is different from those in [8] and [9]. Although in [11] a proof is also given using the Stone-Čech compactification, that proof is different too. The theorem is as follows:

4.1. THEOREM (Hindman). Let $\mathbf{Z}^+ = A_1\cup...\cup A_q$ *with* $A_i\cap A_j = \varnothing$ *for* $i\neq j$. *Then one of the sets* A_i *is an IP-set.*

A set $A\subseteq\mathbf{Z}^+$ is called an *IP-set* whenever there exists a sequence $x_0\leqslant x_1\leqslant x_2\leqslant...$ in A such that $x_{n_1}+...+x_{n_k}\in A$ for every finite subset $\{n_1,..., n_k\}$ of different elements of $\mathbf{Z}^+$. So an IP-set consists (at least) of a non-decreasing sequence in $\mathbf{Z}^+$ together with all sums of finitely many elements of the sequence (no repetitions allowed).

The following model of $\beta\mathbf{Z}^+$ will be useful (for details, see e.g [12]). First, recall that a *filter* in a set S is a family $\mathcal{F}$ of subsets of S such that
(i) $\varnothing \notin \mathcal{F}$;
(ii) if $A, B \in \mathcal{F}$, then $A \cap B \in \mathcal{F}$;
(iii) if $A \in \mathcal{F}$ and B is a subset of S such that $A \subseteq B$, then $B \in \mathcal{F}$.
A family B of subsets such that $\varnothing \notin \mathcal{B}$ and for all $A, B \in \mathcal{B}$ there exists $C \in \mathcal{B}$ with $C \subseteq A \cap B$ is called a *filter base*. Note that if $\mathcal{B}$ is a filter base, then $\{A \subseteq S \vdots \exists B \in \mathcal{B}$ with $A \supseteq B\}$ is a filter. An *ultrafilter* in S is a filter which is not properly contained in any other filter. The following characterization of ultrafilters is rather easy to prove: if $\mathcal{F}$ is a filter in S, then $\mathcal{F}$ is an ultrafilter iff for every subset A of S either $A \in \mathcal{F}$ or $S \setminus A \in \mathcal{F}$. Although we shall not need it explicitly, it is essential for the proofs of the statements about $\beta\mathbf{Z}^+$ below that ultrafilters do exist: by Zorn's lemma, every filter can be extended to an ultrafilter. Examples of ultrafilters are e.g. the fixed ultrafilters, i.e. the filters of the form $\{A \subseteq S \vdots s \in A\}$, where $s \in S$.
Points of $\beta\mathbf{Z}^+$*:* ultrafilters in $\mathbf{Z}^+$. The points of $\mathbf{Z}^+$ will be identified with the fixed ultrafilters; to be precise, the point $n \in \mathbf{Z}^+$ is identified with the ultrafilter

$$h(n) := \{B \subseteq \mathbf{Z}^+ \vdots n \in B\}.$$

Topology of $\beta\mathbf{Z}^+$: a basis for the topology is given by the family of all subsets of $\beta\mathbf{Z}^+$ of the form

$$h(A) := \{\xi \in \beta\mathbf{Z}^+ \vdots A \in \xi\}$$

with A a subset of $\mathbf{Z}^+$. It can be shown that the sets $h(A)$ for $A \subseteq \mathbf{Z}^+$ are both open and closed in $\beta\mathbf{Z}^+$.
It follows from the definitions of $h(A)$ for $A \subseteq \mathbf{Z}^+$ and $h(n)$ for $n \in \mathbf{Z}^+$ that $h(A) \cap \mathbf{Z}^+$ is the set of all fixed ultrafilters $h(n)$ with $A \in h(n)$, i.e. $n \in A$. Thus, if we identify n with $h(n)$, then $h(A) \cap \mathbf{Z}^+ = A$.

If $\xi \in \beta\mathbf{Z}^+$, then a nbd base of ξ is given by the set of all open sets $h(A)$ with $A \subseteq \mathbf{Z}^+$ such that $\xi \in h(A)$, i.e. the set

$$\mathcal{B}_\xi := \{h(A) \vdots A \subseteq \mathbf{Z}^+ \& \ A \in \xi\} \tag{1}$$

The trace $\mathcal{B}_\xi \cap \mathbf{Z}^+$ of $\mathcal{B}_\xi$ in $\mathbf{Z}^+$ (i.e. the set of all intersections $h(A) \cap \mathbf{Z}^+$ with $h(A) \in \mathcal{B}_\xi$) apparently consists of all sets A with $A \in \xi$. This means that

$$\mathcal{B}_\xi \cap \mathbf{Z}^+ = \xi. \tag{2}$$

Next, consider a mapping $\psi: \mathbf{Z}^+ \to X$, X a compact Hausdorff space. Let $\bar{\psi}: \beta\mathbf{Z}^+ \to X$ be its continuous extension. Consider $\xi \in \beta\mathbf{Z}^+$ and put $x := \bar{\psi}(\xi)$. For every open nbd U of x, $\bar{\psi}^{-1}[U]$ includes an element of $\mathcal{B}_\xi$, hence $\bar{\psi}^{-1}[U] \cap \mathbf{Z}^+$ includes an element of ξ. As ξ is a filter, $\bar{\psi}^{-1}[U] \cap \mathbf{Z}^+$ itself belongs to ξ. This shows that

$$\forall U: U \text{ a nbd of } \bar{\psi}(\xi) \text{ in } X \Rightarrow \{m \in \mathbf{Z}^+ \vdots \psi(m) \in U\} \in \xi \tag{3}$$

Using this, the operation $\oplus$ in $\beta\mathbf{Z}^+$ can be described as follows.

If $n \in \mathbf{Z}^+$ and $\xi \in \beta\mathbf{Z}^+$, then application of (3) to the mapping $\omega^n: m \mapsto n+m: \mathbf{Z}^+ \to \mathbf{Z}^+ \subset \beta\mathbf{Z}^+$ gives, in view of (1) and (2):

$$\forall A \in n \oplus \xi : \{m \in \mathbf{Z}^+ \vdots\, n+m \in A\} \in \xi.$$

For convenience, write $A \dot{-} n := \{m \in \mathbf{Z}^+ \vdots\, n+m \in A\} = (A-n) \cap \mathbf{Z}^+$. Then the above can be rewritten as: for all $A \subseteq \mathbf{Z}^+$:

$$A \in n \oplus \xi \Rightarrow A \dot{-} n \in \xi \tag{4}$$

(The converse can also be proved, but this will not be needed in the sequel.) Next, apply (3) to the mapping ω_η: $m \mapsto m \oplus \eta$: $\mathbf{Z}^+ \to \beta\mathbf{Z}^+$, with $\eta \in \beta\mathbf{Z}^+$, and find that for every nbd U of the image $\xi \oplus \eta$ of $\xi \in \beta\mathbf{Z}^+$ under the extended mapping, the set $\{m \in \mathbf{Z}^+ \vdots\, m \oplus \eta \in U\}$ belongs to ξ. So by (1) and (2), if $A \subseteq \mathbf{Z}^+$, then

$$A \in \xi \oplus \eta \Rightarrow \{m \in \mathbf{Z}^+ \vdots\, A \in m \oplus \eta\} \in \xi. \tag{5}$$

Using (4), it follows that

$$\{m \in \mathbf{Z}^+ \vdots\, A \in m \oplus \eta\} \subseteq \{m \in \mathbf{Z}^+ \vdots\, A \dot{-} m \in \eta\}.$$

As ξ is a filter, it follows from (5) that

$$\forall A \subseteq \mathbf{Z}^+ : A \in \xi \oplus \eta \Rightarrow \{m \in \mathbf{Z}^+ \vdots\, A \dot{-} m \in \eta\} \in \xi. \tag{6}$$

Finally, we need one more (trivial) observation: if $\xi \in \beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ and $A \in \xi$, then A must be an infinite subset of $\mathbf{Z}^+$. Indeed, as ξ is not a fixed ultrafilter, for every $n \in \mathbf{Z}^+$ there is $B_n \in \xi$ such that $n \notin B_n$. In particular, $A \cap (\bigcap_{n \in A} B_n) = \varnothing$. If A were finite, this would contradict the filter property of ξ.

4.2. LEMMA. *Let $\eta \in \beta\mathbf{Z}^+ \setminus \mathbf{Z}^+$ be an idempotent. Then every $A \in \eta$ is an IP-set.*

PROOF. By (6) with $\xi = \eta$ and therefore $\xi \oplus \eta = \eta \oplus \eta = \eta$:

$$\forall B \subseteq \mathbf{Z}^+ : B \in \eta \Rightarrow \{m \in \mathbf{Z}^+ \vdots\, B \dot{-} m \in \eta\} \in \eta.$$

So in particular, as η is a filter:

$$\forall B \in \eta : B \cap \{m \in \mathbf{Z}^+ \vdots\, B \dot{-} m \in \eta\} \in \eta.$$

In view of the remark just before the lemma, this implies that for every $B \in \eta$ there are infinitely many elements $m \in \mathbf{Z}^+$ such that $m \in B$ and $B \dot{-} m \in \eta$. Using this, one easily defines by induction for a given element $A \in \eta$ a sequence $x_0, x_1, x_2, \ldots$ in A and elements $A_n \in \eta$ ($n \in \mathbf{Z}^+$) such that

(i) $A_0 := A$;

(ii) $x_n \in A_n$, $A_n \dot{-} x_n \in \eta$ and $x_n > x_{n-1}$;

(iii) $A_{n+1} := A_n \cap (A_n \dot{-} x_n)$.

Note that by the filter property of η, if $A_n \in \eta$ and x_n satisfies (ii), then $A_{n+1} \in \eta$. Also, as $x_n \in A_n$ and the sequence $\{A_n\}_{n \in \mathbf{Z}^+}$ is decreasing, $x_n \in A_0 = A$ for all $n \in \mathbf{Z}^+$.

Now consider $n_1 < n_2 < ... < n_k$ in $\mathbf{Z}^+$. Then $n_{i+1} \geqslant n_i + 1$ for $i = 1,...,k-1$ hence

$$A_{n_{i+1}} \subseteq A_{n_i+1} \subseteq A_{n_i} \dot{-} x_{n_i}$$

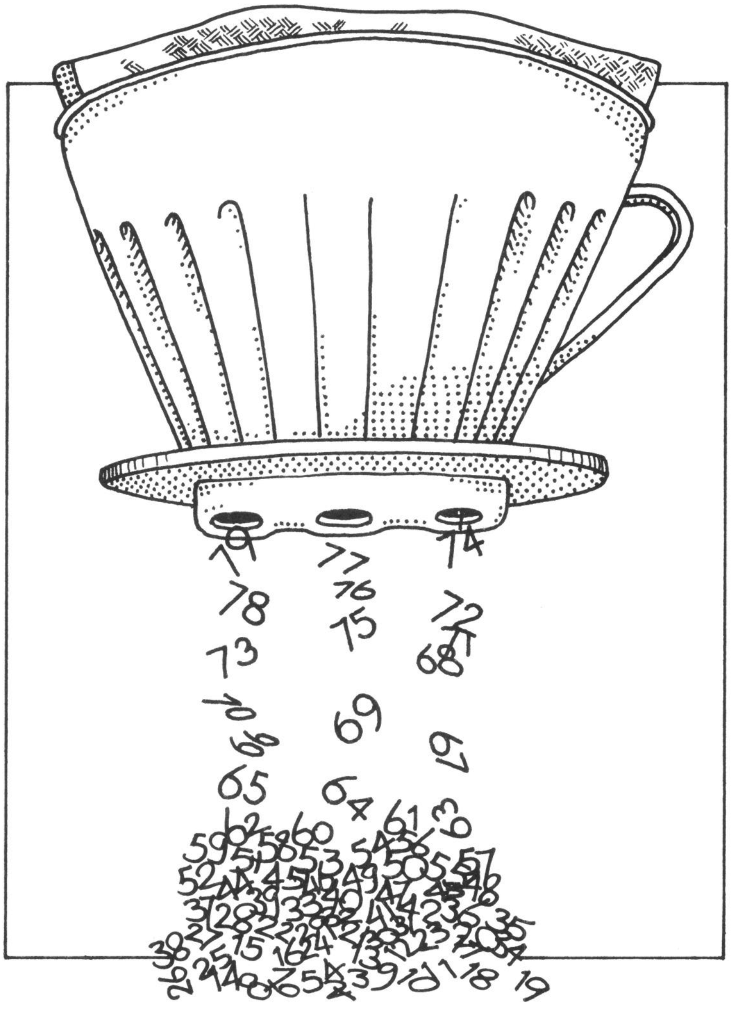
by (iii). This implies that

$$x_{n_i} + A_{n_{i+1}} \subseteq A_{n_i}.$$

By induction it follows that

$$x_{n_1} + ... + x_{n_{k-1}} + x_{n_k} \subseteq A_{n_1} \subseteq A_0 = A.$$

So the sequence $\{x_n\}_{n \in \mathbf{Z}^+}$ in A has the required property with respect to A. □



4.3. PROOF OF THEOREM 4.1. By 3.6, there exists an idempotent η in the closed semigroup $\beta\mathbb{Z}^+ \setminus \mathbb{Z}^+$ of $\beta\mathbb{Z}^+$. Since η is an *ultra*filter in $\mathbb{Z}^+$, there is $i \in \{1,...,q\}$ such that $B_i \in \eta$ (this follows with induction from the property that for every subset B of $\mathbb{Z}^+$, either $B \in \eta$ or $\mathbb{Z}^+ \setminus B \in \eta$). Now apply 4.2. □

4.4. COROLLARY ([9]). *If (X,T) is a dynamical system and $x \in X$ is a recurrent point, then for every nbd U of x the set $R(x,U)$ is an IP-set.*

PROOF. In 3.7 we have observed that there exists an idempotent η in $\beta\mathbb{Z}^+ \setminus \mathbb{Z}^+$ such that $T^\eta x = x$. Since $T^\eta x = \overline{\delta}_x(\eta)$, where $\overline{\delta}_x$ is the continuous extension to $\beta\mathbb{Z}^+$ of the evaluation mapping $\delta_x: n \mapsto T_n x : \mathbb{Z}^+ \to X$, it follows from formula (3) above that for every nbd U of x in X:

$$\{n \in \mathbb{Z}^+ : \delta_x(n) \in U\} \in \eta.$$

This means exactly that $R(x,U) \in \eta$. Now apply 4.2. □

4.5. Remark. As an application of 4.4. one sees that if ξ is a recurrent point in a shift dynamical system (Ω,σ), then for any block B which occurs in ξ the set of numbers $k \in \mathbb{Z}^+$ such that B occurs in ξ at place k is an IP-set.

5. Epilogue

The results and methods described above form only a minor part of 'Abstract Topological Dynamics', by which I mean the part of the theory that was initiated by Gottschalk and Hedlund (cf. [10]). More of this theory can be found in [6], [7], [8] and [5]. In [17] and the final chapters of [5] relations between the abstract theory and differential equations are still visible. The theory in books like [2], [3], [13], [16] and [18] is in much closer contact with the classical qualitative theory of differential equations.

References

[1] R.L. Adler, D. Coppersmith & M. Hassner, *Algorithms for sliding block codes,* IEEE Trans. Inform. Theory **IT-29** (1983), 5-22.

[2] G.D. Birkhoff, *Dynamical systems,* Amer. Math. Soc. Colloquium Publications, Vol. 9, New York, 1927.

[3] N.P. Bhatia & G.P. Szegö, *Stability theory of dynamical systems,* Springer-Verlag, 1970.

[4] R. Bowen, *Equilibrium states and the ergodic theory of Anosov diffeomorphisms,* LNM 470, Springer-Verlag, 1975.

[5] I.U. Bronstein, *Extensions of minimal transformation groups,* Sijthoff & Noordhoff, 1979. (Russian original: 1975.)

[6] M. Denker, C. Grillenberger & K. Sigmund, *Ergodic theory on compact spaces,* LNM 527, Springer-Verlag, 1976.

[7] R. Ellis, *Lectures on topological dynamics,* W.A. Benjamin, New York, 1969.

[8] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory,* University Press, Princeton, 1981.

[9] H. Furstenberg & B. Weiss, *Topological dynamics and combinatorial number theory,* J. d' Analyse Math. **34** (1978), 61-85.

[10] W.H. Gottschalk & G.A. Hedlund, *Topological dynamics,* Amer. Math. Soc. Colloquium Publications, Vol. 36, 1955.

[11] S. Glasner, *Divisible properties and the Stone-Čech compactification,* Can. J. Math. **22** (1980), 993-1007.

[12] L. Gillman & M. Jerison, *Rings of continuous functions,* D. Van Nostrand, 1960.

[13] O. Hadjek, *Dynamical systems in the plane,* Academic Press, 1968.

[14] G.A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system,* Math. Systems Theory **3** (1969), 320-375.

[15] S. Lefschetz, *Geometric differential equations: recent past and proximate future, in: Differential equations and dynamical systems* (Proc. Internat. Symposium, Puerto Rico, 1965), 1967, pp. 1-14.

[16] V.V. Nemytiskii & V.V. Stepanov, *Qualitative theory of differential equations,* Princeton University Press, 1960. (Russian original: 1947.)

[17] G.R. Sell *Topological dynamics and ordinary differential equations,* Van Nostrand Reinhold, 1971.

[18] K.S. Sibirsky, *Introduction to topological dynamics,* Noordhoff, 1975.

[19] F.M. Dekking, *Combinatorial and statistical properties of sequences generated by subsitutions,* Thesis, Katholieke Universiteit Nijmegen, 1980.

[20] J.F. Berglund et al., *Compact right topological semigroups and generalizations of almost periodicity,* LNM 663, Springer-Verlag, 1978.

Software development: Science or Patchwork?

by Robert L. Baber

Abstract
In the past, software development has been variously described as a science, art, craft, trade, racket, etc. Even today opinions vary considerably about how software should be developed and what qualifications are most appropriate for software developers.

In this paper a series of case examples illustrates the problematic state of affairs in the field of software development today. Many of these examples also illustrate the often overlooked potential and practical value of a mathematically oriented approach to solving software developmental problems.

The spectrum of possible software worlds of the future is characterized by its three extremes: an audacious (reckless), a backward (reactionary) and a celestial (radical) software future. The paths leading to each of these extremes and the prerequisites for achieving a significantly better future are discussed.

In this paper it is argued that the detailed specification, design and development of computer software is by nature an engineering field with mathematics as an important theoretical foundation. In practice, however, software development is too often treated today as patchwork. It is too often conducted by underqualified personnel instead of by professionally educated engineers. These are the major causes of the many problems and disappointments that we have been and still are experiencing in applying computer systems.

1. Prologue: the land of Moc

Imagine that you are living in an ancient country in the cradle of civilization. The time is about 2500 B.C. In the course of the years an active foreign trade has developed and several cities have been founded. A construction industry has been established in which professionally trained architects and civil engineers play an important role.

Suddenly and unexpectedly, a group of teachers of civil engineering develop a new technique for designing buildings. Using the new method, buildings can be designed and built which are much larger than those previously possible. Perhaps even more importantly, the new method reduces construction costs to about a tenth of their former levels.

As a consequence, the demand for buildings of all types increases very rapidly. The construction industry grows correspondingly. But new architects and civil engineers cannot be educated so quickly. Nor can the capacity of the civil engineering colleges be expanded sufficiently rapidly. Nevertheless, a solution is found: New construction planners are trained in special short courses conducted by the suppliers of building materials. In this way the quantitative gap between supply and demand is bridged.

The application of this advanced technology is not without its dark side, however. Because the new 'three week wonders' (as the professionally trained designers contemptuously label their minimally trained colleagues) only superficially understand the theory underlying their designs, minor catastrophes are common. All too often the three week wonders rely on 'trial and error' (instead of theoretically based calculations) in order to determine if a proposed design will collapse or not.

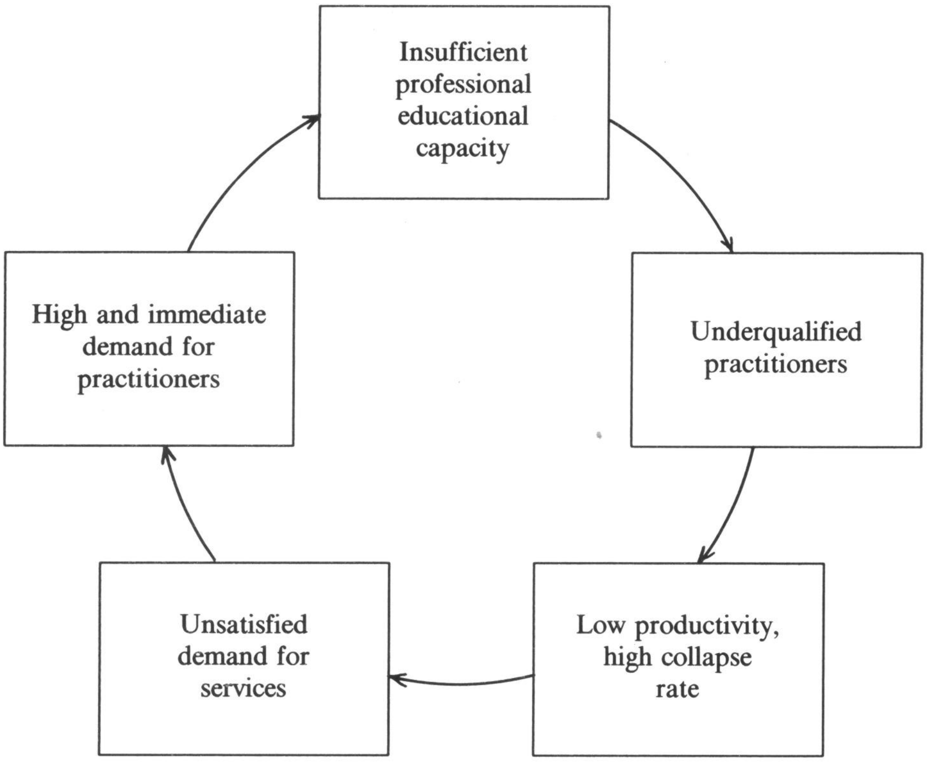

Insufficient professional educational capacity
Underqualified practitioners
Low productivity, high collapse rate
Unsatisfied demand for services
High and immediate demand for practitioners

Fig. 1. The Mocsian vicious circle

The result of this 'trial and error' approach is not really surprising: about 30% of all newly designed buildings collapse during construction. As an eloquent professional once put it as he arrived at the scene of a particularly spectacular collapse, 'rubbish in, rubble out'. The rubbish was the design prepared by a three week wonder; the rubble, an incredible quantity of debris which shortly before had been a wondrous building under construction.

To combat the problem of collapses during construction, elaborate testing schemes have been worked out. These do not solve the problems, of course, but they do tend to limit the negative consequences of the frequent collapses. The test procedures are expensive — causing as much as half of the total construction costs. Nevertheless, there is clearly a net economic benefit for the Mocsian society of using the new design technique.

Although the shortcomings of current design practice are widely recognized, this modus operandi appears to be firmly established. Prospective new designers prefer a short, cursory, practical training instead of a professional course of study lasting several years because they can thereby begin earning good money earlier. And most of the professionally trained architects and engineers, from whose ranks teachers could come, prefer a more lucrative professional practice over a career in teaching.

As a result, the fraction of professionals among the building designers in the land of Moc is declining. This is, in turn, causing a corresponding decline in the quality of Moc's building planners, a decline in productivity, a still larger gap between supply and demand and a demand for more building designers, even underqualified ones. Thus, as shown in fig. 1, the vicious circle is closed.

2. Moc Today

The story of the land of Moc is obviously pure fiction. Such a ridiculous story could never be true. Or could it? It is my thesis that the story of the land of Moc is true. The time is not 4500 years ago, but the present. The true story does not concern an ancient construction industry in the cradle of civilization, but our modern computer software industry in the most 'advanced' countries in the world.

Software development today is plagued by many — too many — unnecessary collapses. From time to time we read about some of these collapses. But many more go generally unnoticed because they occur so frequently that they cannot be considered unusual. Design by 'trial and error' (following the Mocsian motto 'try building it and see if it collapses') has become commonplace. In order to limit to some extent the effect of our failures we conduct an incredible amount of 'testing' (a euphemism for finding and correcting mistakes). Typically, 'testing' accounts for half of the effort expended in a software development project.

What has caused this situation? Advances in the computer area have been made so rapidly that we still have difficulty absorbing them — although computer systems are, after several decades, nothing new. Especially our educational programs have not kept pace with developments on the computer scene. Our concentration on short term problems and solutions has prevented us from building a solid, optimum base for the long term.

Why has this state of affairs become so accepted? The computer is a fundamentally new tool so useful that even when sloppily applied by beginners and amateurs, the net benefit — after due consideration of the collapses — is still very great. We believe that the benefits realized are due to our own good efforts. In reality, we have, more or less by accident, stumbled onto a good thing. We could and should endeavor to make much more of this good thing in the future than we are now doing.

In my opinion software development is by nature an engineering discipline. The more successful developers of challenging software systems apply mathematical and scientific knowledge when specifying, designing and implementing their systems. They proceed in a systematic manner, whereby creative aspects of their work an be recognized — just as in already recognized engineering fields.

Unfortunately, an engineering approach is not characteristic of typical software developments today. The following examples illustrate the consequences of this deficiency. They also show some of the advantages of a mathematically and scientifically founded approach to software development. The examples are in chronological order.

- In the mid 1950's a course in computer programming was offered to advanced students at a particular engineering school. A sophomore applied to enroll in the course. After initial hesitation, the professor granted his request.
- Two years later, a course in computing was offered to freshmen. As many as 10% of the freshmen were expected to enroll. At least twice as many actually applied. The number of instructors available was hopelessly insufficient to meet the demand. It was assumed, of course, that this large gap between supply and demand for the education of software specialists was only a temporary phenomenon. Little did they know.
- In the early 1960's in one country's defense establishment, a series of programs printed a long classified report. Because of logical flaws in the programs' printing routines, a few pages would, from time to time, be printed which included the security legend at the top or bottom but no data. They could not be deleted from the report without introducing a discrepancy in the page count. It was necessary, therefore, to register and retain the 'TOP SECRET' blank pages.
- A major computer manufacturer installed several very large, fast computers. When it was discovered that the systems operated unreliably, many customers withheld their monthly rental payments. The manufacturer soon solved the hardware problems, but despite many corrections and revisions the operating system remained unreliable. The manufacturer's liquidity became very strained; some observers of the industry expected the company to become insolvent. Finally, large

infusions of loan capital enabled the supplier to remain in business while the errors in the system were being corrected.

- In a large information system, data relating to individual persons was indexed by the person's name. A method was required for locating data on a particular person even when the name was misspelled. This was to be accomplished by transforming the name into an abbreviation in such a way that typical misspellings transformed to the same abbreviation. Several rules for forming the abbreviations were to be investigated. A logically complex program was written to test the first rule. Whenever the programmer corrected one error, another appeared in its stead. After several months, the project manager asked a consultant for assistance.

  The consultant noticed that a transformation of names was homomorphic to (and could therefore be represented by) a finite automaton with a small number of states. He suggested expressing each abbreviation rule in the form of a transition table and writing a single table driven program to simulate the automaton defined by the table for each rule. In the attempt to construct the table for the rule already programmed, a logical inconsistency in the rule was discovered. After the rule was corrected, this approach led quickly to success.

  In this example the method of 'trial and error' could never have led to a successful result, because the programmer had been trying to program an unprogrammable (logically inconsistent) task. In addition, the conventional programming approach, even if successful, would have been very inefficient, involving several complicated programs instead of one smaller, simple one and a few tables, each one page long.
- One company in the new world decided in the mid-1960's to implement a truly integrated information system. About 5 years later, around the turn of the decade, shortly before the planned implementation of the system, the project was abandoned. Only a few small parts of the system could be salvaged and used productively. Several higher level managers left the company, some willing, some not. The loss was estimated to be about $ 10 million. In the following years, the electronic data processing pendulum swung to the other, conservative extreme in this company. Many economically justifiable electronic data processing applications were overlooked or intentionally rejected. The opportunity cost of these potential applications was never estimated but was certainly substantial.
- In the early 1970's the old world was generally considered to be some years behind the new in matters concerning electronic data processing. Unfortunately, this was not the case when it came to creating spectacular collapses. Shortly after the collapse outlined above became known, almost the same occurred in a European country. In both cases unsatisfactory communication and lack of mutual understanding between the developers, users and management as well as exaggerated optimism were important reasons for the expensive failures.

- In another firm a software system for sales forecasting was designed and implemented. Several programs, which were obtained from the computer's manufacturer, had allegedly been successfully used earlier in other companies. During implementation, errors were discovered in several of these programs. One of the errors represented a fundamental oversight in the mathematical analysis of the statistical forecasting model upon which the program was based.

  Earlier, the occurrence of such errors was assumed to represent a transitory phenomenon. Slowly one began to recognize that this was not the case. The fact that a program had been used successfully by others could no longer be interpreted as evidence of its correctness.
- An inventory control system was developed to satisfy the needs of a particular company. For this system, a set of formulae was developed which could be solved only by iterative approximation. Although preliminary tests gave no indication of potential problems, one member of the team was concerned that the iterative method might not always converge or that it might sometimes converge to an undesired solution. A lengthy mathematical analysis showed that no such problems would arise in the case at hand, but that a particular kind of non-linear interpolation in a table was required in one part of the computation.

  Another member of the development team was concerned about the possible consequences of the unavoidable delays in the man-machine communication in this batch system. The desired behavior of the system was formulated as a specification of an automaton. (See Baber [2], pp. 166-167, for further details.) During the necessary discussions between the system's designers and future users, a number of possible sequences of events came to light which no one had considered before and which forced the users to think through in detail what they really wanted from the system. The resulting specification was implemented successfully and employed for many years.
- A data base system was planned as the basis for an order processing system. After detailed investigations were conducted, the software system and the data organization were selected. From the outset, some members of the project team were concerned about the system's response time, but initial analysis indicated that this would probably not be a significant problem.

  During *implementation* of the system another — insoluble — problem arose: As the data base was built up, it was noticed that the time required to load additional data increased very rapidly. It became clear that just loading the complete data base would require a *year* or so of computer time. The response time also became problematic, although it was less serious. The project was abandoned in the implementation phase, *after* design and programming were complete, and the history of software development was enriched with another collapse.

  This failure could have been avoided. Without undue difficulty, one could have determined the time complexity of the required functions using the selected data organization — before expending any significant developmental effort. Probably, no member of the development team even knew about the concept of computational complexity. A bent for quantitative analysis was apparently also lacking, for even without knowledge of complexity theory one could have estimated the time characteristics of the data base system.

- While designing a relatively straightforward application system, a system analyst was forced by arbitrary limits in the system software to make use of linked list techniques in organizing a data file. During the programming phase difficulties arose because the programmers, among them a graduate of computing science, had no experience with linked lists.

  This example shows the value of a theoretical background: without knowledge of linked lists, the analyst would have been unable to solve the problem at hand using the given computer system. This example also illustrates that today's computing science education leaves much to be desired, for the graduate was unfamiliar with a method of data organization which is basic, well known in professional literature and often used in system software.
- An experienced free lance programmer contracted to write a particular program for a software house. The program was to run on a machine with which the programmer had no prior experience. After reading the manual, he still had some questions regarding commonly used input-output functions. He turned to a specialist for that machine for clarification. The specialist could not answer his questions. The programmer asked the specialist how he resolved such problems. The specialist replied, 'I just keep trying until something works.' The programmer was not satisfied with his advice. He used only those commands which were unambiguously described in the manual. His program was perhaps not so elegant as it might have been, but it worked reliably. The same could not be said for the specialist's programs.

  Although the 'trial and error' method often leads to unsatisfactory results (or even to no results at all), it is still used again and again.
- The manager of a production planning department asked an electronic data processing specialist with a mathematical inclination to investigate the feasibility of optimizing a regularly recurring task of his department. The goal was to schedule the production of a particular product so that the amount of scrap generated would be minimized. The specialist investigated several mathematical methods such as integer programming. He concluded that all of these methods were infeasible in the given situation due to their computational complexity. During his investigation, however, he discovered a heuristic algorithm which usually gave optimum results. He programmed this algorithm on a small microcomputer which was purchased solely for this application. His system was used successfully for a long time.

Again, a combination of theoretical knowledge and a sense of what is needed in practice seems to be associated with success.

- In the early 1980's a world wide transportation company contracted with an important computer manufacturer for the development of customized software for an integrated fleet operations and accounting system. Two years later, shortly before key elements of the system were to be installed, the supplier announced that it had discontinued the project and would not deliver the application software.
  After the collapses in the old and new worlds, this was bound to happen sooner or later.
- An error in a computerized defense control system resulted in a false report of an enemy attack. Interceptors were launched. Fortunately, the error was discovered in time.
  After many years we are still building errors into our computer systems. But with time the potential consequences of these errors are becoming more serious and irreversible. They are not so comical as the 'TOP SECRET' blank pages of years before.
- An experienced software system designer developed a software system for a management game for a client. The structure of the game required that decisions be made by each team of players (representing competing companies) for successive time periods. To fit into the environment within which the game was to be played, it was necessary that the computer program could be interrupted at several points within each time period and restarted later at that or an earlier point in the game. In order to enable this mode of operation, the players' decisions were stored in separate files by team and by time period; data specifying the state of the game were stored in a 'run control file'.
  The designer, convinced that the logic of the interactive control program would be fairly simple, began to write it without planning its structure in detail. After several false starts and several hours wasted, he decided to start all over and do the job properly. He began by specifying the assertions (logical conditions) which the values of the various variables defining the state of the game would have to satisfy at all times. Supported by these eight assertions (program invariants) and knowing the intended 'variant' action — advancing to the next time period as soon as the prerequisites (implied by the invariants) were established — he was able to write the control program in a straightforward manner. As he originally expected, the program turned out to be logically simple. His successful approach took less time than he had already wasted on the false starts.
  If a mathematically oriented approach can yield such benefits even in the case of small, logically simple programs, how can one afford *not* to take such an approach when developing complex software systems?

- Computer courses are being introduced into secondary schools in many countries. The better prepared teachers of these classes took one or two courses in computing subjects in college; many have had no formal training in computing. Teachers of other subjects are required to have completed a much more extensive training in their fields (cf. mathematics, languages, history, sciences, etc.). Why is informatics treated in this very different — even irresponsible — way?
- A seminar on advanced topics in programming methodology for software developers and research scientists was arranged. The number of applications greatly exceeded the expectations of the organizers and, of course, the planned capacity. Many qualified applicants had to be rejected. After a quarter century a very considerable gap between supply and demand for computing science education still exists (cf. the course offered to freshmen at the engineering school above).
- Because of an error in software an unmanned space ship was lost in deep space.
- In the field of informatics at universities in the Federal Republic of Germany the ratio of students to faculty has grown to 100:1 [12]. Potential students are interested in studying this subject and companies are very interested in employing all graduates. Still this great — probably unprecedented — discrepancy between supply and demand for informatics education prevails. While the Federal Republic of Germany may be an extreme example in this regard, this problem is by no means a uniquely German one. Neither is this a new problem which has suddenly appeared. One could and should have seen it coming. Many *have* seen it coming for many years.

What is wrong with the current situation?

Because the net benefits resulting from applications of computer systems are so great, one might ask: 'What is really so bad about the current state of affairs? We are producing large quantities of software which is of considerable value to its users. As long as this situation prevails, we do not really have a problem.' There are, however, a number of serious negative consequences of our current approach to software development:

- The consequences of errors in software are becoming more costly, more dangerous and more irreversible.
- Major and unnecessary failures, mishaps and attendant losses occur too frequently.
- The total cost of our software systems (including the costs associated with failures and their consequences) are unnecessarily high.
- We are obtaining much less benefit from computer technology than is potentially possible.
- A large gap exists between supply and demand in the software market. This gap represents an economic loss (opportunity cost).

- Negative consequences and losses caused by errors in software are often shifted unfairly onto persons who are not responsible for those errors, who have no control over the situation and who cannot protect themselves from the consequences of such errors.
- Software products are often characterized by disappointing quality. Errors in software are often of a rather simple nature.
- Productivity in software development leaves much to be desired.
- Scarce resources are wasted in unsuccessful projects.
- Unreliable systems frustrate and confuse laymen and shake their confidence in applications of computer technology.

Why do we have these problems?

There are several different but related causes of the problems outlined above:

- The transfer of knowledge and experience from one generation of software practitioners to the next is not functioning satisfactorily. This applies to both practical and theoretical knowledge. In other words, our educational system is not achieving its objectives.
- Only a small fraction of software developers has a command of the scientific knowledge of computing science as well as of the application area for which they develop software. Educational programs were and are quantitatively and qualitatively insufficient.
- A great communication gap exists between the practical and theoretical worlds of informatics. This statement applies to a certain extent to all areas of applied science, but it is particularly true of software development today. Many practitioners do not understand the basic language of the theoretician (= mathematics) and many theoreticians exhibit little or no interest in the problems and work of the practitioner.
- 'Trial and error' appears to be a widely accepted method for designing and developing software.
- Software developers rely much too heavily upon 'testing' instead of getting their designs correct in the first place. Especially in this regard does a mathematically oriented approach and way of thinking offer considerable promise for improvement.
- The frequency and consequences of errors in software systems suggest a lack of sense of responsibility on the part of the developers (and sometimes of the users). Perhaps the developers are mentally fully occupied with the technical details of their designs. Perhaps this is due, in turn, to an inadequate understanding and command of those technicalities.
- The proper place of informatics in the academic world is still unclear. Particularly when one compares the position of informatics in universities in different countries does the full variety of organizational forms become apparent: as part of mathematics, electrical engineering, business or economics or as an independent department in a faculty of natural science, engineering or economics, with or without smaller branches in the various departments representing the fields of application of computer systems.

- Economic forces induce potential professors of informatics to become practitioners instead. Potential students are induced to become poorly prepared 'system analysts' and coding technicians today instead of good software engineers tomorrow. Income and success in the short term are overemphasized; potentially greater income and success in the longer term future are largely neglected.

Our software situation today is, it seems, very much like that of the Mocsian construction industry. The most unsettling aspect is that — just as in Moc — a stable vicious circle has arisen (fig. 2).

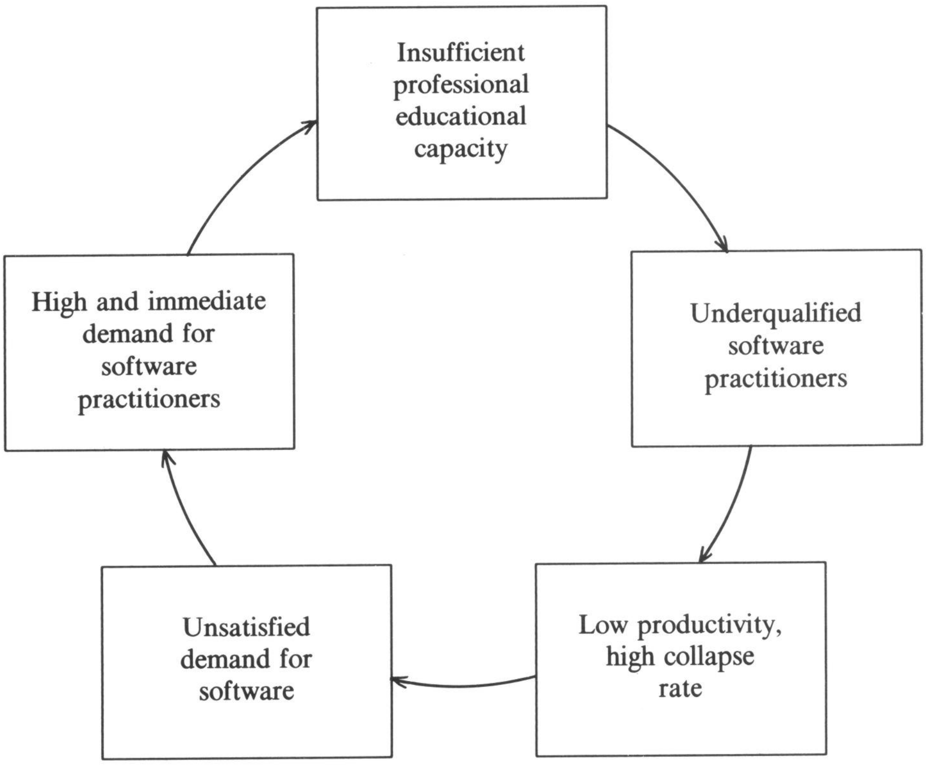

Insufficient professional educational capacity
Underqualified software practitioners
Low productivity, high collapse rate
Unsatisfied demand for software
High and immediate demand for software practitioners

Fig. 2. Our contemporary vicious circle

3. Software development tomorrow?

The nature of the software world of the future will be determined by many factors, the most important of which are our own choices and decisions regarding what sort of a future we desire. I will not, therefore, attempt to forecast the characteristics of our software future. Instead, I will outline the alternatives among which we can — and, explicitly or implicitly, will — choose.

The set of possible software worlds of the future form a continuum characterized by its three extreme points. Each possible software future can be thought of as a convex combination of these three extremes, called Future A, B and C below. The point representing our software future will be determined by the average level of professional competence achieved by software practitioners and by the complexity of the applications attempted (fig. 3).

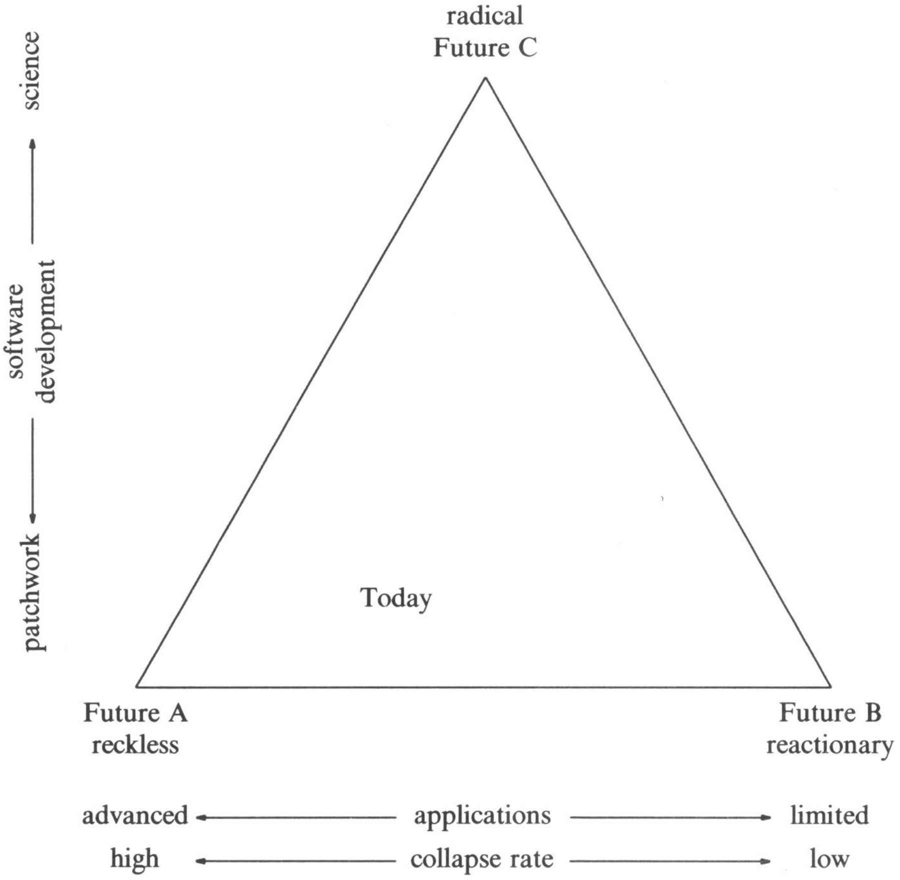


Fig. 3. Possible software futures

In the audacious Future A, much is attempted, capabilities are limited and major failures are frequent. In the backward Future B, strong pressures are present to restrict computer applications to those within the limited capabilities of the software practitioners and their customers. These systems are usually successfully realized, but of course much is left undone. In the celestial Future C, the competence of the average software practitioner has been developed to such a high level that even very complex applications are normally implemented without major difficulty or problems of a fundamental nature. The extreme Future A can be simply described as a reckless future; Future B, reactionary; and Future C, radical.

Today we are between Future A and Future B, somewhat closer to Future A (see the case examples in section 2 above). Many trends and developments in data processing, especially the advent of the microcomputer, will result in considerable pressure to apply computer technology much more extensively throughout society in the next decades [5,10]. This will push us even closer to the point representing Future A. If we decide to develop our professional software capability much more extensively in the future, we can deflect our path away from Future A and toward Future C. If we do not decide to do so, the catastrophic collapses characteristic of Future A can be expected to give rise to a wave of public reaction leading us to Future B.

Let us look at each of the futures A, B and C in more detail:

The reckless, audacious Future A

A software corollary to Parkinson's Law and the Peter Principle characterizes Future A particularly well: Software developers will conceive and try to build ever more complicated systems until the limit of their ability to cope with complexity is exceeded.

Despite our software problems such as those outlined in section 2 above, there is today among broad segments of society considerable optimism and confidence in our computer based future. Futurologists predict wonderful things (see e.g. Evans [5]). There is, however, a great danger that this 'wonderful' future will not turn out as hoped, but instead as follows:

- Because of an error in software in an air traffic control system, four jumbo jets collided over Paris one cloudy morning. All 1631 passengers and crew members as well as 1000 people on the ground were killed. The ensuing traffic jam blocked the area for two days.
- After an extended period of financial difficulty, one of the largest companies in a medium sized European country went into bankruptcy. The detailed reasons were not determined. Only one thing was really clear: the company's information and communication systems were in such a state that the company had become unmanageable.
- A thirty story building collapsed during construction. The design was reexamined in detail. Mistakes in the calculations of stresses in critical structural elements were discovered. These calculations had originally been done by computers whose programs contained errors.

- At the turn of the millennium 1999-2000, business in the computerized economies of the world all but collapsed. For bills rendered in 1999 but due in 2000, overdue notices were issued already in 1999, charging interest for some 99 years. After January 1, 2000, many systems failed to issue overdue notices for amounts due in 1999 but not yet paid. The cause: computer software and data bases which provided only 2 digits for the year.

When such incidents occur sufficiently often, a public reaction can be expected. Depending upon whether the reaction is directed against computer applications as such or against the inadequate capabilities of the software developers, pressure will arise which will push us in the direction of Future B or Future C.

The reactionary, backward Future B

If Future B comes to be, software related situations something like the following may become typical:

- A law was passed which placed very severe restrictions on computerized air traffic control systems. Particularly onerous were requirements for high levels of public liability insurance coverage. Shortly after passage of the new law, a governmental agency announced that a newly completed system would not be implemented. The costs of fulfilling the new legal requirements were so high that the system could no longer be economically justified.
- Members of the interest group 'Ban the Computer' discovered that applied research was being conducted on a computerized vehicle guidance and control system for automobile highways. They organized a massive two day 'sit in and lie in' strike on all major roads within 50 km of the headquarters of a company which was funding the project. Threats of violence were directed at the project's chief scientists and engineers.

The radical, celestial Future C

In comparison to Futures A and B a description of Future C seems a bit dull, because everything functions well, as planned:

- A computerized, fully automated air traffic control system which had operated uneventfully and error free since its installation several years earlier suddenly discovered that two aircraft were on a collision course, only 45 seconds flying time apart. The emergency subsystem automatically took control and guided them safely apart. Shortly thereafter, the system informed the (human) flight monitors on the ground and on board the aircraft involved about the incident. The cause was identified as a traffic volume which exceeded the system's design specifications by 34%.
- A computerized control system for a nuclear reactor discovered an operator's error and issued an appropriate warning. Two successive actions recommended by the system were overridden by the human operator. The system was finally compelled to take over control and shut

down the reactor. In the ensuing investigation, the operator stated that the chain of events took place so fast that a human was incapable of making rational, considered decisions effectively. All concerned agreed that safety regulations should be revised to require fully automatic control over such potentially dangerous processes.

- A study of the software industry showed that the 'debugging' and test phase of typical larger software development projects accounted for approximately 10% of the total effort, compared with some 50% twenty years earlier. Of 2500 projects included in the study, 3 were unsuccessful. The report also stated that 'practicing software developers are now more highly educated than ever before. The average coding technician has completed a three year technical training program; the typical semi-professional software designer, a four year university course; and every software engineer, at least a five year university course.' The study also found that all software engineers *regularly* read professional articles available through the various on-line professional literature services. These services were used regularly by 83% of the semi-professionals and by 31% of the coding technicians.

4. The path from today to tomorrow

Who must do what to achieve a better software future? Everyone directly concerned with designing and developing software as well as everyone involved in their education and training must take active steps to break the vicious circle at several points simultaneously. An attack at one point only would have no lasting effect; the positive feedback in the vicious circle would counteract any such perturbation and would serve to maintain the status quo.

It should be apparent that academic institutions must play a key role in bringing about a significant improvement. Especially in the early stages must academic institutions play a leading role in building a sufficiently widespread and qualitatively adequate base upon which software engineering can be founded. Success here is a necessary (but not sufficient) condition for a major and lasting improvement in the practice of software development.

Already in the 1940's Norbert Wiener described computer programming (he used the term 'taping') as 'a highly skilled task for a professional man of of a very specialized type' [14]. Edsger Dijkstra said much later 'Programming is one of the most difficult branches of applied mathematics' ([4], p. 129). There is no path leading to a mastery of this field in practice which does not pass through a good tertiary education in general and mathematics in particular.

We have not yet chosen our path to our software future. Do we want to proceed first toward Future A and then to be deflected to Future B? Or do we want to take the perhaps more difficult but certainly more promising path to Future C?

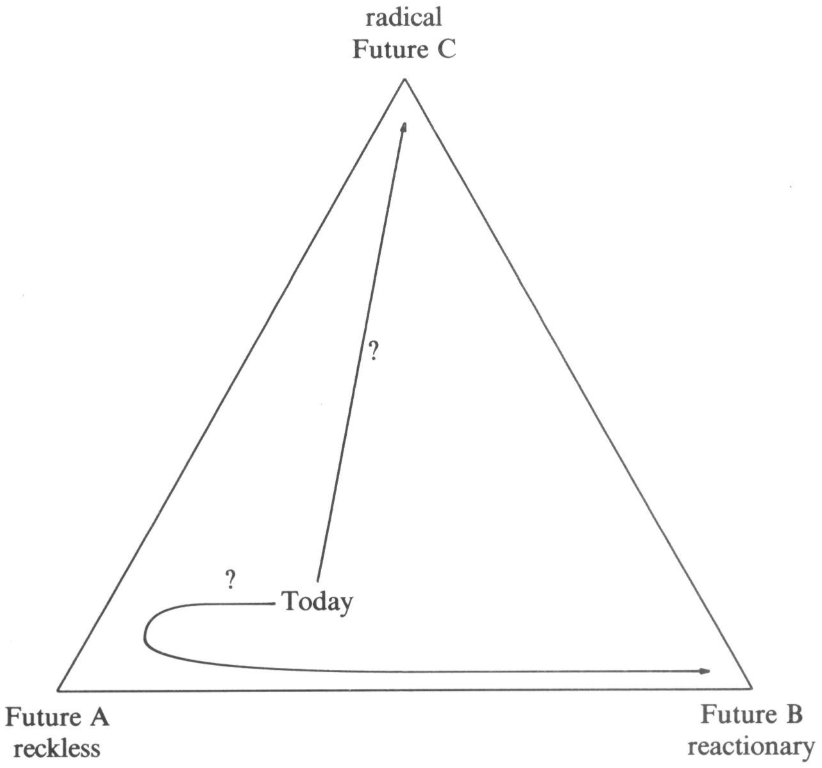


Fig. 4. Possible paths to the future

Literature

[1] Baber, R.L., "Informatikausbildung in der Bundesrepublik Deutschland: Der zukünftige Preis des gegenwärtigen Nichthandelns", *Informatik-Spektrum*, **6**(1983), 1, p. 36.

[2] Baber, R.L., *Software Reflected: The Socially Responsible Programming of Our Computers*, North-Holland Publishing Co., 1982.

[3] Buxton, J.N. & Randell, B. (eds.), *Software Engineering Techniques*, Report on a conference sponsored by the NATO Science Committee, Rome, Italy, 27th to 31st October 1969, NATO Science Committee, Brussels, 1970.

[4] Dijkstra, E.W., *Selected Writings on Computing: A Personal Perspective*, Springer-Verlag, 1982.

[5] Evans, C., *The Micro Millennium*, Washington Square Press Pocket Books, New York, 1981.

[6] Fairly, R.E., *Software Engineering Education: Status and Prospects*, Proceedings of the Twelfth Hawaii International Conference on System Sciences, Pt. I, Western Periodicals Ltd., North Hollywood, California, U.S.A., 1979, pp. 140-146.

[7] Fleckenstein, W.O., "Challenges in Software Development", *Computer*, **16**(1983), 3, pp. 60-64.

[8] Ganzhorn, K.E., "Informatik im Uebergang", *Informatik-Spektrum*, **6**(1983), 1, pp. 1-6.

[9] Gesellschaft für Informatik e. V., "Numerus Clausus in der Informatik — hochwertige Arbeitsplätze von morgen durch unzureichende Lehr- und Forschungskapazitäten von heute gefährdet?", Press Notice, *Informatik-Spektrum*, **5**(1982), 2, p. 126.

[10] Haefner, K., *Der 'Grosse Bruder'*, Econ Verlag, 1980.

[11] Haefner, K., *Die neue Bildungskrise*, Birkhäuser Verlag, 1982.

[12] Krüger, G., "Zur Situation der Informatikausbildung an den Universitäten der Bundesrepublik Deutschland", *Informatik-Spektrum*, **5**(1982), 2, pp. 71-73.

[13] Naur, P. & Randell, B. (eds.), *Software Engineering*, Report on a conference sponsored by the NATO Science Committee, Garmisch, Germany, 7-11 October 1968, NATO Scientific Affairs Division, Brussels, 1969.

[14] Wiener, N., *The Human Use of Human Beings: Cybernetics and Society*, Doubleday, 1954.

Address of the author:
Landgrav Gustav Ring 5
D-6380 Bad Homburg v.d.H.
Federal Republic of Germany

Recent Progress on the Numerical Verification of the Riemann Hypothesis

by J. van de Lune & H.J.J. te Riele

It has now been shown that the first 400,000,000 non-trivial zeros of Riemann's zeta function are all simple and lie on the so-called critical line $\sigma=\frac{1}{2}$. This extends previous results described in [1], [2] and [6].

Riemann's zeta function is the meromorphic function $\zeta:\mathbb{C}\setminus\{1\}\rightarrow\mathbb{C}$, which, for $\mathrm{Re}(s)>1$, may be represented explicitly by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad (s = \sigma+it).$$

It is well known (cf. [3], [9]) that

$$\xi(s) := \tfrac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

is an entire function of order 1, satisfying the functional equation

$$\xi(s) = \xi(1-s)$$

so that

$$\Xi(z) := \xi(\tfrac{1}{2}+iz), \quad (z\in\mathbb{C})$$

being an even entire function of order 1, has an infinity of zeros. The Riemann Hypothesis (cf. [3], [7]) is the statement that all zeros of $\Xi(z)$ are real, or, equivalently, that all non-trivial zeros of $\zeta(s)$ lie on the critical line $\sigma = \frac{1}{2}$. Since $\zeta(\bar{s}) = \overline{\zeta(s)}$, we may restrict ourselves to the halfplane $t>0$. To this day, Riemann's Hypothesis has neither been proved nor disproved. Numerical investigations related to this unsolved problem were initiated by Riemann himself (cf. [3]) and later on continued more systematically by the writers listed below (including their progress).

Investigator	Year	The first n complex zeros of $\zeta(s)$ are simple and lie on $\sigma = \frac{1}{2}$
GRAM	1903	$n = 15$
BACKLUND	1914	$n = 79$
HUTCHINSON	1925	$n = 138$
TITCHMARSH	1935/6	$n = 1{,}041$

Those listed above utilized the Euler-Maclaurin summation formula and performed their computations by hand or desk calculator whereas those listed below applied the so-called Riemann-Siegel formula (cf. [3]) in conjunction with electronic computing devices.

LEHMER	1956	$n = 25{,}000$
MELLER	1958	$n = 35{,}337$
LEHMAN	1966	$n = 250{,}000$
ROSSER, YOHE & SCHOENFELD	1968	$n = 3{,}500{,}000$
BRENT	1979	$n = 81{,}000{,}001$
BRENT, van de LUNE, te RIELE & WINTER	1982	$n = 200{,}000{,}001$
van de LUNE & te RIELE	1983	$n = 300{,}000{,}001$

An excellent explanatory account of most of the essentials of these computations may be found in [3].

In practice, the numerical verification of the Riemann Hypothesis in a given range consists of *separating* the zeros of the well-known real function $Z(t)$ (see [3]), or, equivalently, of finding sufficiently many sign changes of $Z(t)$. Our program (aiming at a fast separation of these zeros) is based, essentially, on the modification of Lehmer's [4] method introduced by Rosser et al. [8]. However, we have developed a more efficient strategy of searching for sign changes of $Z(t)$. Brent's average number of Z-evaluations, needed to separate a zero from its predecessor, amounts to about 1.41 (cf. [1]) whereas we have brought this figure down to about 1.19 (cf. [5]). This average number of Z-evaluations could not have been reduced below 1.135 by any program evaluating $Z(t)$ at all Gram points. A complete listing of our FORTRAN/COMPASS program is given in [5]. We note that 98 percent of the running time was spent on Z-evaluations. The program was executed on a CDC CYBER 175-750 and ran about 10 times as fast as the UNIVAC 1100/42 program of Brent. This is roughly what could be expected, given the relative speeds of the different machines. We intend to continue our computions in the near future on a still faster computer.

In order to give an impression of the erratic behaviour of $Z(t)$ we present its graph near the Gram block $B_{61,331,766}$. For more graphs and details see [6].

References

[1] Brent, R.P., *On the zeros of the Riemann zeta function in the critical strip,* Math. Comp., **33** (1979) 1361-1372.

[2] Brent, R.P., J. van de Lune, H.J.J. te Riele & D.T. Winter, *On the zeros of the Riemann zeta function in the critical strip,* II, Math. Comp., **39** (1982) 681-688.

[3] Edwards, H.M., *Riemann's zeta function,* Academic Press, New York, 1974.

[4] Lehmer, D.H., *On the roots of the Riemann zeta function,* Acta Math., **95** (1956) 291-298.

[5] Lune, J. van de & H.J.J. te Riele, *Rigorous high speed separation of zeros of*

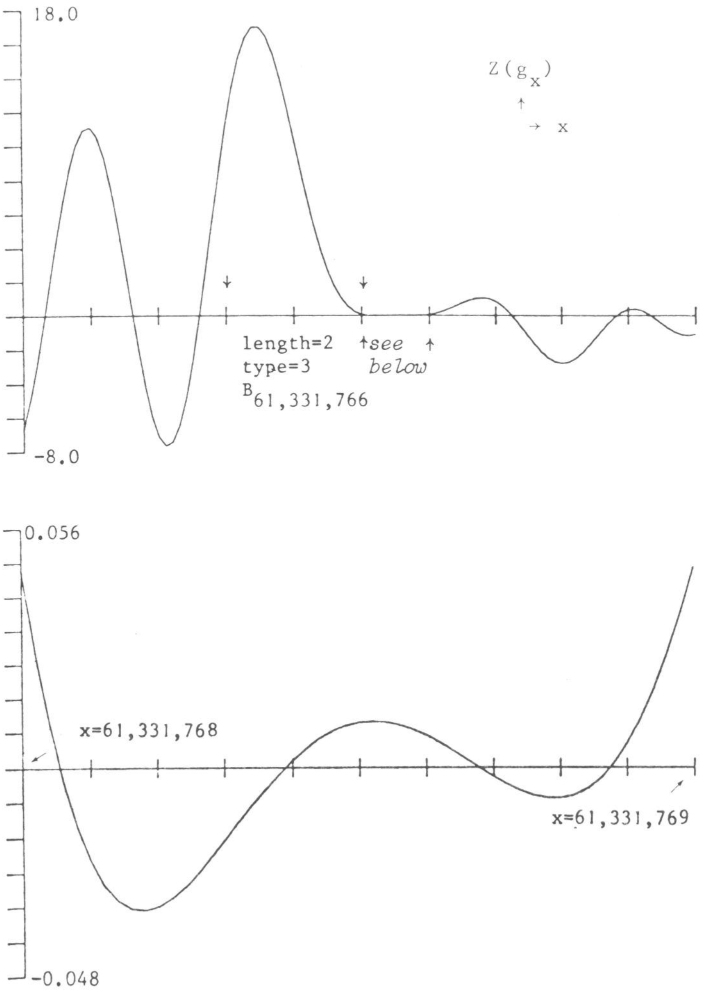
Riemann's zeta function, II, Report NN 26, Mathematical Centre, Amsterdam, 1982.

[6] Lune, J. van de & H.J.J. te Riele, *On the zeros of the Riemann zeta function in the critical strip,* III, Math. Comp., **41** (1983) 759-767.

[7] Riemann, B., *Gesammelte Werke,* Teubner, 1892, 148.

[8] Rosser, J.B., J.M. Yohe & L. Schoenfeld, *Rigorous computation and the zeros of the Riemann zeta function,* Proc. IFIP Congress, Edinburgh, 1968.

[9] Titchmarsch, E.C., *The theory of the Riemann zeta function,* Clarendon Press, Oxford, 1951.



The behaviour of $Z(t)$ near the Gram block $B_{61,331,766}$.

在中国的三周

The Day Before Tomorrow

Three Weeks in the People's Republic of China

by Jan Karel Lenstra

On September 2, 1983, Henk Tijms of the Free University and I left Amsterdam for a three week visit to China. We stayed for two weeks at the Institute of Applied Mathematics of the Academia Sinica in Beijing (Peking in former days, but Beijing sounds much better). We paid brief visits to the Institute of System Science and the Computing Center, both of the Academia Sinica, and to the Department of Mathematics of Beijing University. After leaving Beijing, we stayed at the Technical University of Xi'an and at the University of Hangzhou for three days each, spent a few days in Shanghai and Hongkong, and returned to Amsterdam on September 25. Our trip was financed through the cultural agreement between the Netherlands and China. The following is a brief account of our experiences and impressions.

Research

How rewarding is it, from a professional point of view, to spend three weeks in China? If you are a calligrapher, a cook, or a magician, then it must be extremely satisfying. If you are working in the mathematics of operations research, then it will be interesting to observe what is going on but you should not expect to encounter the latest developments in the field.

The investigations in which Chinese operations researchers are engaged extend the theory of the early sixties. Due to the 'cultural revolution' (the use of quotes here is a recent Chinese tradition), they have not been able to maintain their contacts and to follow new developments. This implies for the area of *mathematical programming* that the classical variants of nonlinear programming receive most attention and that combinatorial optimization, which grew into a discipline of its own during the seventies, is practically virgin territory. Also in *stochastic optimization* the traditional subjects are emphasized.

It goes without saying that our Chinese colleagues are very much aware of this situation. Through all kinds of bilateral agreements Western scientists are lecturing in China and Chinese students are educated abroad. We were particularly impressed by the efforts of Feng Kang, director of the Computing Center in Beijing, in formulating and pursuing an active research policy. Chinese mathematics and computer science have a considerable potential - but *tomorrow* may be five or ten years away.

An unexpected side benefit of our trip was the opportunity to meet a number of Western mathematicians. After all, September is the best time to visit China and foreign scientists are put in the same hotel.

Development and applications

Hua Loo-Keng will be well known to many readers for his fundamental work in pure mathematics. He is omnipresent as a researcher, as director of three institutes of the Academia Sinica, as editor-in-chief of several journals, and as chairman of a number of societies.

In the mid-sixties, he became involved in popularizing mathematical methodology. He and his assistants 'visited twenty-two provinces, hundreds of cities, and thousands of factories, meeting millions of people' [3]. The purpose of their mission was to promote techniques that are effective enough to yield results and simple enough to be understandable and applicable by non-specialists in a small-scale environment. Reference [2] lists 147 actual applications. Reference [3] provides information on the mathematical methods that were popularized. Among these are the *optimum seeking method* (one-dimensional Fibonacci search) and the *overall planning method* (the critical path method and a scheduling rule in disguise). My stay at the Institute of Applied Mathematics was a welcome opportunity to learn more about the amazing scope of this campaign, the underlying mathematical ideas, and the practical results.

I did not succeed in finding out much about the use of advanced mathematical programming techniques in large-scale decision situations. An exception is the successful work [1] of Gui Xiangyun (my hostess in Beijing) on the distribution of crude oil to refineries and of the resulting products to the customers. Her approach is based on Benders decomposition and as such nicely matches the Chinese-Dutch cultural cooperation.

Non-scientific aspects

When you are visiting China, you will soon discover that lecturing to and talking with your colleagues leaves ample time for other activities. I have already alluded to Chinese banquets and magic shows. They are very much worth attending. As to sightseeing, I recommend that, after having seen the Great Wall, you shouldn't miss the Lama Temple in Beijing, the Qin excavations near Xi'an, and the West Lake at Hangzhou. One of your hosts is always ready to join you, and the academy's guide acts as organizer in the background.

Communication

Communicating with the Chinese people is a chapter in itself. In giving a lecture, it is absolutely necessary to have an interpreter. He or she, being a volunteer from the audience rather than a professional interpreter, is faced with the heavy task of comprehending a lot of new material and translating it simultaneously. I am indebted to five colleagues (Gui, Liu, Wang, Ge, and Chang) for their heroic and, as far as I can judge, successful achievements in this respect.

Due to cultural differences, life can be difficult. For instance, you should *never* ask a yes/no question (as one of our neighbors did who went to the counter in the Temple of Heaven, asking 'Sprechen Sie Deutsch?'). The answer will invariably be affirmative. Except on Thursdays. 'I see you last Saturday?' *Next* Saturday, I hope? 'Uh... *the day before tomorrow*.'

References

[1] X. Gui, *Distribution system planning for crude oil and petroleum products in China by mathematical programming,* Institute of Applied Mathematics, Academia Sinica, Beijing, 1983.

[2] H. Halberstam (ed.), *Loo-Keng Hua Selected Papers,* Springer, Berlin, 1983, 877-881.

[3] L.K. Hua, H. Tong, *Some personal experiences in popularizing mathematical methods in the People's Republic of China,* Internat. J. Math. Ed. Sci. Tech., **13** (1982) 371-386.

Abstracts

of Recent CWI Publications

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

MC Tract 163. H. Schippers. *Multiple grid methods for equations of the second kind with applications in fluid mechanics.*
AMS 31A25; 130 pp;

Abstract: Multiple grid methods are studied for solving algebraic systems of equations that occur in numerical methods for Fredholm integral equations of the second kind. In general, the algebraic systems are non-sparse and in practice the dimensions are large, so that iterative schemes non-sparse are needed. Multiple grid methods are iterative schemes that work with a sequence of computational grids of increasing refinement. Theoretical and numerical investigations show that the rates of convergence of the presented multiple grid methods increase as the dimension of the finest grid increases. The method that appears to be the most robust is implemented in an Algol 68 program for the automatic numerical solution of Fredholm integral equations of the second kind. The fast convergence of multiple grid methods is established for the following problems from fluid mechanics: (1) calculation of potential flow around aerofoils and (2) calculation of oscillating disk flow.

IW239/83. P.M.B. Vitányi & L.G.L.T. Meertens. *Big omega versus the wild functions.*
AMS 26A12; 7 pp.; **key words:** computational complexity, running time of algorithms, order of infinity, monotone functions, Order-of-Magnitude symbols, definitions.

Abstract: The question of the desirable properties and proper definitions of the Order-of-Magnitude symbols, in particular Ω and Θ, is addressed once more. The definitions proposed are chosen for complementary mathematical properties rather than for similarity of form.

IW240/83. P. Klint. *A survey of three language-independent programming environments.*
AMS 68B20; 32 pp.; **key words:** software engineering, language-independent programming environments, syntax-directed editing, semantics-directed evaluation.

Abstract: The creation and maintenance of software is becoming increasingly expensive. To improve upon this situation several *software tools* and *language-specific programming environments* have come into existence. The substantial design and implementation effort to build a programming environment for each specific language can, however, be reduced by developing *language-independent* programming evironments, which can be tailored towards a particular language by supplying them with the corresponding language definition. This paper surveys three existing, but still experimental, language-independent programming environments: Mentor, the Synthesizer Generator and CEYX. The similarities between the three systems and their individual goals and characterics are outlined. Using each system a programming environment for a toy language has been constructed in order to establish some basis for comparison. The results of this experiment are discussed.

IW241/83. J.A. Bergstra & J. Tiuryn. *Process algebra semantics for queues.*
AMS 68B10; 25 pp.; **key words:** process algebra, queue, fixed point equations, bisimulation.

Abstract: An unbounded queue over a finite set of data values is modeled as a state transition system. After behavioural abstraction its behaviour is a process Q in A^{∞} where A is the collection of the input and output actions for the queue. A specification of Q by means of recursion equations is provided, using a new auxiliary operator on processes. It is shown that this operator is necessary in the sense that it is not possible to specify Q using recursion equations built from sequential, alternative and parallel composition only. Sequential composition of two queues is shown to realise another queue.

IW242/82. A.K. Lenstra. *Polynomial factorization by root approximation.*
AMS 12A20; 7 pp.; **key words:** polynomial algorithm, polynomial factorization, basis reduction algorithm, fundamental theorem of algebra.

Abstract: We show that a constructive version of the fundamental theorem of algebra combined with the basis reduction algorithm of A.K. Lenstra, H.W. Lenstra, Jr. & L. Lovász, yields a polynomial-time algorithm for factoring polynomials in one variable with rational coefficients.

IW243/83. P.M.B. Vitányi. *Distributed elections in an Archimedean ring of processors.*
AMS 68A05; 6 pp.; **key words:** decentralized algorithms, distributed systems, local area network rings, operating systems, communications management message sending.

Abstract: The use of clocks by the individual processors in elections in a ring of asynchronous processors without central control allows a deterministic solution which requires but a linear number of message passes. To obtain the result, it has to be assumed that the clocks measure finitely proportional absolute time-spans for their time units, that is, the magnitudes of elapsed time in the ring network satisfy the axiom of Archimedes. As a result, some basic subtilities associated with distributed computations are highlighted. For instance, the known nonlinear lower bound on the required number of message passes is cracked. For the synchronous case, in which the necessary assumptions hold a fortiori, the method is -asymptotically- the most efficient one yet, and of optimal order of magnitude. The deterministic algorithm is of -asymptotically- optimal bitcomplexity, and, in the synchronous case, also yields an optimal method for determining the ring size. All of these results improve the known ones.

IW244/83. P.M.B. Vitányi. *The simple roots of real-time computation hierarchies.*
AMS 68C40; 4 pp.; **key words:** multitape Turing machines, real-time computation, real-time hierarchies, multipushdown store machines, limited random access Turing machines, queues, double-ended queues, concatenable dequeues.

Abstract: If the computation power of an assemblage, consisting of a number of copies of a memory device BLAH, communicating through a single finite control, eventually increases by adding more BLAH's, and each such assemblage can be simulated in real-time by a multitape Turing machine, then an assemblage with $k+1$ BLAH copies is more powerful in real-time than one with k BLAH copies, for each k. Thus the hierarchies within the real-time definable computations are *smooth,* that is adding a device *always* increases power. It also turns out that all real-time hierarchy results in this vein are simple corollaries of a single root: the real-time hierarchy of multipushdown store machines. As examples of new results we mention that in real-time, $k+1$ tape-units with a fast rewind square are more powerful than k such units; that $(k+1)$-head tape-units with fast rewind squares are more powerful than k-head tape-units with fast rewind squares; that $(k+1)$-dequeue machines are more powerful than k-dequeue machines; and that $(k+1)$-

concatenable-dequeue machines are more powerful than k-concatenable-dequeue machines.

IW245/83. P.M.B. Vitányi. *An $N^{1.618}$ lower bound on the time to simulate one queue or two pushdown stores by one tape.*
AMS 68C40; 5 pp.; **key words:** multitape Turing machines, pushdown stores, queues, time complexity, lower bounds, on-line simulation by single-head tape units, Kolmogorov complexity.
Abstract: To simulate two pushdown stores, or one queue, on-line by a one-head tape unit requires $\Omega\ n^{1.618}$ time. (This improves the known $\Omega\ (n \log^{1/2} n)$ lower bound for the on-line simulation of two-tape Turing machines by one-tape Turing machines.)

IW246/83. P.M.B. Vitányi. *On two-tape real-time computation and queues.*
AMS 68C40; **key words:** multitape Turing machine, multihead Turing machine, real-time computation, two heads versus two tapes, storage retrieval, queue, incompressible string, Kolmogorov complexity.
Abstract: A Turing machine with two storage tapes cannot simulate a queue both in real-time and with at least one storage tape head always within $o(n)$ squares from the start square. This fact may be useful for showing that a two-head tape unit is more powerful in real-time than two one-head tape units, as is commonly conjectured.

IW247/83. J.N. Akkerhuis. *Typesetting and Troff.*
AMS 68K05; 26 pp.; **key words:** typesetting, textprocessing.
Abstract: This report gives a short introduction to typesetting in general and will discuss the UNIX typesetting tools and its recent changes.

IW248/83. A. Nienhuis, *On the design of an editor for the B programming language.*
AMS 68B99; 16pp.; **key words:** programming environments, syntax-directed editors, B.
Abstract: Language-dedicated editors use language-specific knowledge about syntax and (static) semantics of programming languages. They form a much more powerful tool for creating and modifying programs than conventional text editors. This report describes such an editor, specially designed for editing programs written in the language B.

BW190/83. E.A. van Doorn. *A note on Delbrouck's approximate solution to the heterogeneous blocking problem.*
AMS 60K30; 8 pp.; **key words:** teletraffic theory, blocking probability, heterogeneous blocking problem.
Abstract: Delbrouck's recent estimates for the call blocking probabilities experienced by heterogeneous traffic streams on a common trunk group are brought to light in a new and simple manner. A link with earlier estimates by Delbrouck is established by means of a Manfield and Downs-type approximation.

BW191/83. J.H. van Schuppen. *The weak stochastic realization problem for discrete-time counting processes.*
AMS 93E03; 11 pp.; **key words** stochastic realization problem, stochastic system, discrete-time counting process.
Abstract: The weak stochastic realization problem is considered for discrete-time stationary counting processes. Such processes take values in the countably infinite set $N = \{0,1,2,...\}$. A stochastic realization is sought in the class of stochastic systems specified by a conditional distribution for

the output given the state of Poisson type, and by a finite valued state process. In the paper a necessary and sufficient condition is derived for the existence of a stochastic realization in the above specified class.

BW192/83. J.P.C. Blanc. *The relaxation time of two queueing systems in series.*
AMS 90B22; 13 pp.; **key words:** tandem queueing system, relaxation time, asymptotic expansion, Riemann-Hilbert boundary value problem, conformal mapping.

Abstract: This paper deals with the time-dependent behaviour of two queueing systems in series, the simplest example of a Jackson network. The Laplace transform of the probability $p_0(t)$ that the tandem system is empty at time t is obtained by reducing the functional equation for the generating function of the joint queue length distribution to a Riemann-Hilbert boundary value problem. From this Laplace transform the relaxation time of $p_0(t)$ is determined for all cases, and the first term of the asymptotic expansion of $p_0(t)-p_0(\infty)$ as $t\rightarrow\infty$ is found in the ergodic and in the null recurrent cases.

BW193/83. C. van Putten & J.H. van Schuppen. *Invariance properties of the conditional independence relation.*
AMS 60A10; 15 pp.; **key words:** conditional independence relation, invariance properties, projection operator, σ-algebraic realization problem, stochastic realization problem.

Abstract: The conditional independence relation for a triple of σ-algebras is investigated. For certain operations on this relation necessary and sufficient conditions are derived such that these operations leave the relation invariant. Examples of such operations are the enlargement or reduction of the σ-algebras, and an absolutely continuous change of measure. A projection operator for algebras is defined and some of its properties are stated. The σ-algebraic realization problem is briefly discussed.

BW194/83. A. Bensoussan & J.H. van Schuppen. *Optimal control of partially observable stochastic systems with an exponential-of-integral performance index.*
AMS 93E20; 23 pp.; **key words:** stochastic control, linear systems, exponential-of-integral cost functional, linear-exponential-Gaussian problem.

Abstract: The stochastic control problem with linear stochastic differential equations driven by Brownian motion processes and as cost functional the exponential of a quadratic form is considered. The solution consists of a linear control law and a linear stochastic differential equation. The latter has the same structure as a linear control law and a linear stochastic differential equation which has the same structure as the Kalman filter but depends explicitly on the cost functional. The separation property does not hold in general for the solution to this problem.

NW162/83. P.W. Hemker. *Mixed defect correction iteration for the solution of a singular perturbation problem.*
AMS 65N10; 30 pp.; **key words:** defect correction, singular perturbations, convection diffusion equation.

Abstract: We describe a discretization method (mixed defect correction) for solving a two-dimensional elliptic singular perturbation problem. The method is an iterative process in which two basic discretization schemes are used: one with and one without artificial diffusion. The resulting method is stable and yields a second order accurate approximation in the smooth parts of the solution without using any special directional bias in the discretization. The method works well also for problems with interior or boundary layers.

NN31/83. G.T. Symm, B.A. Wichmann, J. Kok & D.T. Winter. *Guidelines for*

the design of large modular scientific libraries in Ada. Second interim report.
90 pp.; **key words:** Ada programming language, scientific software.

Abstract: The new programming language Ada has been designed primarily for programming embedded systems. It is generally expected, however, that it will also be widely used in large-scale scientific computation. Several features of the language require careful consideration if large, portable, modular, scientific algorithms libraries are to be implemented successfully. Accordingly, this report is concerned with identifying the problems associated with the overall design and implementation of such libraries in Ada and with making recommendations for their solution. The problem areas treated are: precision, basic mathematical functions, composite data types, information passing, error handling, working-space organization and real-time environment. Discussions and exemplary solutions using new language features are offered, which should help numerical analysts who wish to develop large libraries in Ada to do this in such a way that compatible library components are produced.

NN32/83. J. Kok. *Ada compared with Pascal.* (In Dutch.)
AMS 69D49; 28 pp.; **key words:** Ada, Pascal, programming language.

Abstract: Several concepts of the programming language Ada are easily mastered if one is familiar with the programming language Pascal. The structure of programs and a number of programming elements, such as statements, declarations, data-types and subprogram-declarations, are compared with those of Pascal.

SW97/83. H. Berbee. *Periodicity and absolute regularity.*
AMS 60F10; 19 pp.;

Abstract: For a stationary ergodic process it is proved that the dependence coefficient associated with absolute regularity has a limit connected with a periodicity concept. Similar results can then be obtained for stronger dependence coefficients. The periodicity concept is studied separately and it is seen that the double tail σ-field can be trivial while the period is 2. The total variation metric is used.

SN12/83. R.D. Gill. *The sieve method as an alternative to dollar-unit sampling: the mathematical background.*
AMS 62D05; 22 pp.; **key words:** sieve sampling, cell sampling, Hoeffding inequalities.

Abstract: This note describes the mathematical background to sieve sampling, a new method for audit sampling developed by C. Rietveld. The method uses a probability-proportional-to-size sampling scheme, while the statistical evaluation of the sample is based on the Poisson distribution appropriate to simple random sampling. The proof of the correctness of this method, using some inequalities of Hoeffding, also shows the validity of cell sampling.

TW247/83. J.V. Lankelma. *Stochastic dynamical systems with a cyclic structure.*
AMS 35A40; 28 pp.; **key words:** random perturbations, Fokker-Planck equation, exit problems, WKB approximation, hypercycle.

Abstract: This paper deals with a stochastic version of the 'hypercycle' introduced by Eigen and Schuster. The 'cycle' is a dynamical system with a simple cyclic structure. After conversion to a set of stochastic differential equations, Kolmogorov's exit problem is asymptotically solved with the WKB-method.

TW248/83. S.A. van Gils. *Linear Volterra convolution equations: semigroups, small solutions and convergence of projection operators.*
AMS 45D05; 35 pp.; **key words:** Volterra integral equation, semigroup, adjoint semigroup, structural operator, decomposition according to the spectrum of the

infinitesimal generator, convergence of projection operators, small solution.

Abstract: In this paper we consider the initial function semigroup and the forcing function semigroup generated by linear Volterra integral equations of convolution type. We prove that the two semigroups are adjoints of one another in the sense that the adjoint of the initial function semigroup is identical to the forcing function semigroup corresponding to the equation with transposed kernel. Moreover these semigroups are equivalent. We prove that the absence of small solutions is equivalent to the injectivity of a structural operator which maps initial functions into forcing functions. We show the convergence of the spectral projection operators corresponding to the (pure) point spectrum of the infinitesimal generators on a dense subset of the state space for a special class of equations.

TW249/83. S.A. van Gils. *Hopf bifurcation and symmetry: travelling and standing waves on the circle.*
AMS 34C25; 41 pp.; **key words:** Hopf bifurcation, symmetry, secondary bifurcation, travelling waves, standing waves, stability.

Abstract: In this paper we consider Hopf bifurcation in the presence of 0(2) symmetry. The reaction diffusion equation $u_t = Du_{xx} + f(\mu,u)$ provided with periodic boundary conditions may serve as a model problem. We prove the bifurcation of a torus of standing waves and two circles of traveling waves and we compute the stability (with asymptotic phase) of these periodic solutions, giving explicit formulas. Finally we demonstrate how a small perturbation that breaks part of the symmetry leads to secondary bifurcation.

ZW196/83. A.E. Brouwer. *On the uniqueness of a regular thin near octagon on 288 vertices (or the semibiplane belonging to the Mathieu group M_{12}).*
AMS 05C25; 12 pp.;

Abstract: We show that the regular thin near octagon with parameter (s,t_2,t_3,t_4) = (1,1,4,11) and 288 vertices is unique. Its group of automorphisms is $M_{12}.2$ which has two orbits of size 144. It follows that there are exactly two nonisormorphic partial 2-geometries with blocks of size 12 and nexus 5, duals of each other. (These are the semibiplanes found by Leonard.) The same methods applied to the parameter set s,t_2,t_3,t_4 = (1,1,4,9) shows that no graph with these parameters exists.

ZW201/83. J. van de Lune. *Some observations concerning the zero-curves of the real and imaginary parts of Riemann's zeta function.*
AMS 10H05; 25 pp.; **key words:** zero-curves, Riemann's zeta function, Riemann hypothesis, Lehmer's phenomenon, exceptions to Gram's law and/or Rosser's rule.

Abstract: It is shown here that the supremum σ_0 of the set $\{\sigma \in \mathbf{R} \mid Re\,\zeta(\sigma+it)<0$ for some $t \in \mathbf{R}$ is given by the (unique) solution of the equation

$$\sum_p a\sin(p^{-\sigma}) = \frac{\pi}{2},\ (\sigma>1)$$

when p runs through the primes.
For $\sigma = \sigma_0$ we have $Re\,\zeta(\sigma+it)>0$ for all $t \in \mathbf{R}$.

Using all primes $<10^9$, we found (numerically) that $\sigma_0>1.192$. Moreover, a method is presented for the numerical determination of t-values such that $Re\,\zeta(1+it)<0$. As a result we have for example: $Re\,\zeta(1+i.682\ 112.92)=-.003$. The paper concludes with an informal discussion of how to find values of t such that the 'signed modulus' $Z(t)$ behaves quite 'unusual'.
As an example we mention the result $Z(t)<-453.9$ for t = 725, 177, 880, 629, 981. 914, 597. Finally, some values of t are listed in the vicinity of which Gram's law and/or Rosser's rule are violated.

ZW202/83. A.E. Brouwer. *An infinite series of symmetric designs.*
AMS 05B05; 5 pp.; **key words:** symmetric balanced incomplete block design.

Abstract: We construct symmetric $2-(v,k,\lambda)$ designs where

$$v = 2(q^h + q^{h-1} + \cdots + q) + 1,$$
$$k = q^h$$

and

$$\lambda = \frac{1}{2} q^{h-1}(q-1)$$

whenever q is an odd primepower and $h \geqslant 1$.

ZW203/83. G.F. Helminck. *Uniqueness of Whittaker-models for irreducible objects in Alg(Mp(k)).*
AMS 22E50; 6 pp.; **key words:** metaplectic group, algebraic respresentations, Whittaker-models.

Abstract: We discuss several methods for proving the uniqueness of Whittaker-models for the metaplectic group and relate them to work of S. Gelbart and I. Pyateckii-Shapiro.

CWI Activities

Spring 1984

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.

Introductory colloquium for teachers. On Lie groups and Lie algebras. Weekly. (J. de Vries)

Study group on Analysis on Lie groups. Semisimple pseudo-Riemannian symmetric spaces. Joint with University of Leiden. Biweekly. (T.H. Koornwinder)

Lecture series 'The Spherical Fourier Transform for Semisimple Lie groups'. Biweekly. (T.H. Koornwinder)

Seminar on Theta functions. The Lepowsky-Wilson proof of the Rogers-Ramanujan identities, representation-theoretic approach to the generalized hard-hexagon model of lattice statistical mechanics; Liouville integrable systems. Biweekly. (G.F. Helminck)

Seminar on Algebra and Geometry. The Leech lattice. Biweekly. (A.M. Cohen)

Study group on Cryptography. Biweekly. (A.E. Brouwer)

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)

Bifurcations and Nonlinear Oscillations. The lectures will be based on J. Guckenheimer & Ph. Holmes (1983), *Nonlinear Oscillations, Dynamical Systems, and Bifurcation of Vector Fields* (Springer, Berlin). One-week course, June 18-23. (J. Grasman)

Study group '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 and analysis. Biweekly. (J.V. Lankelma)

Study group 'Semiparametric estimation theory'. The group studies J.M. Begun, W.J. Hall, W.-M. Huang & J.A. Wellner (1983), *Information and asymptotic efficiency in parametric-nonparametric models* (Ann. Statist. **11,** 432-452) and related papers. Biweekly. (R.D. Gill)

Study group 'Stochastic processes and their applications'. The group studies S.R.S. Varadhan (1980), *Lectures on diffusion problems and partial differential equations* (Springer, Berlin). Joint with Technological University Delft. (P. Groeneboom)

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 of the Mathematical Statistics Department. New results in research and consultation projects. Monthly. (R.D. Gill)

National colloquium on Optimization. February, 23rd. Rotterdam. (J.K. Lenstra)

Colloquium on Queuing Theory. Triweekly. (E.A. van Doorn)

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

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

Study group on System Theory. Topics are stochastic filtering and stochastic control. Biweekly. (J.H. van Schuppen)

Colloquium 'Numerical Mathematics in Practice'. Biweekly. (J.G. Verwer)

Study group on Differential and Integral Equations. Biweekly. (H.J.J. te Riele)

Post-academic course (PAO) on Design of Interactive Graphical Systems. April 25-27 and May 9-11. (P.J.W. ten Hagen)

Post-academic course (PAO) on Modern Techniques on Software Engineering. March 8-9 and 22-23. (J.A. Bergstra)

Study groups on Graphic Standards. Monthly. (P.J.W. ten Hagen)

Study group 'Dialogue programming'. (P.J.W. ten Hagen)

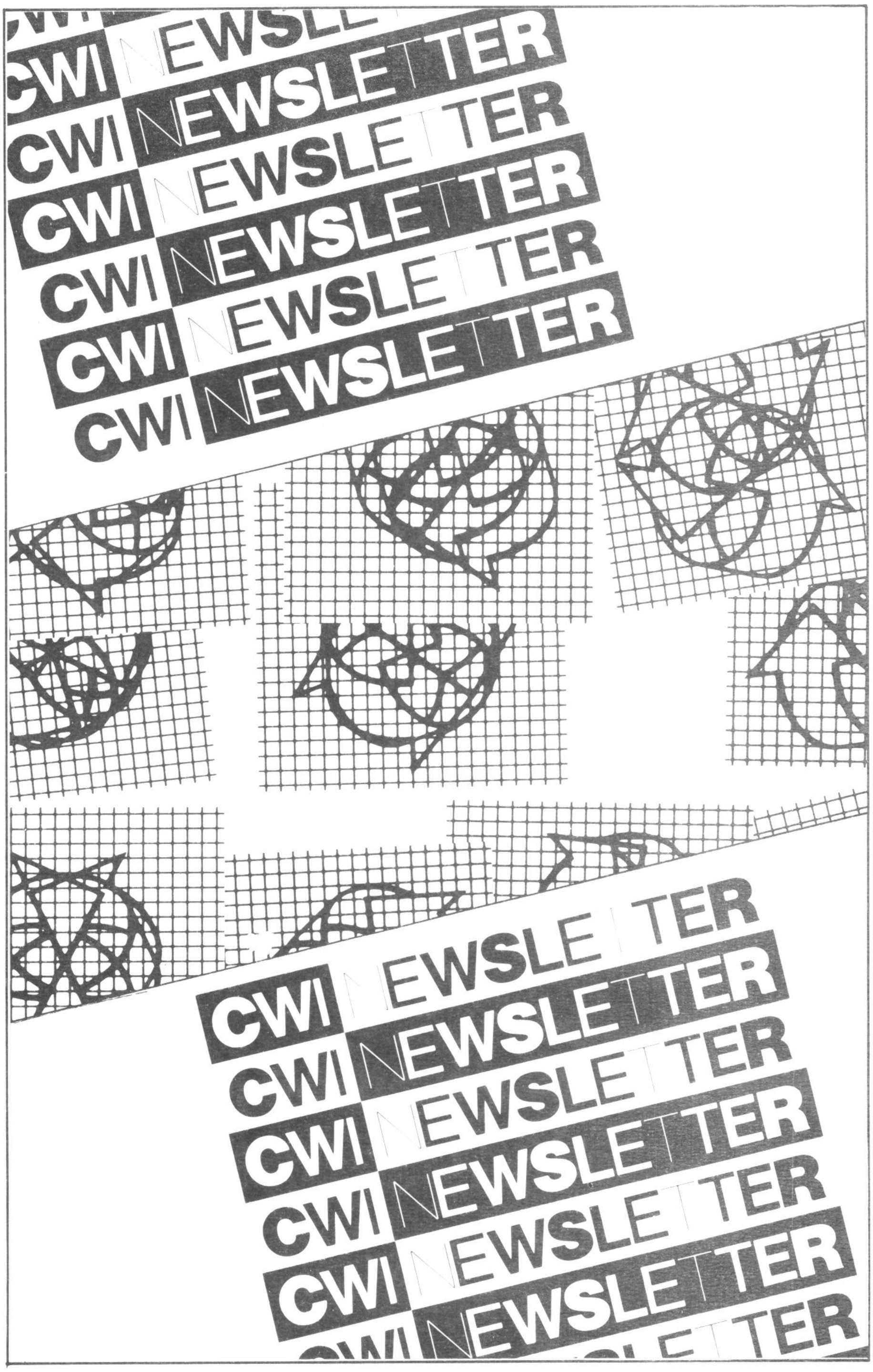
Data Flow Club. Irregular. (A.H. Veen)

Seminar National Concurrency Project. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. March 16 and May 18. (J.W. de Bakker)

National Study Group 'Concurrency'. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. February 24, March 30, April 27, May 25. University of Utrecht. (J.W. de Bakker)

Visitors to CWI from abroad

J. Cuzick (Imperial Cancer Research Fund Laboratories, London, UK) 19-20 March 1984. **L. Devroye** (McGill University, Montreal, Canada) 9-12 December 1983. **C.F. Dunkl** (University of Virginia, Charlottesville, USA) 1 January - 1 July 1984. **F. Guerra** (University of Rome, Italy) 19 December 1983. **Guo Ben-yu** (University of Shanghai) 26-28 January 1984. **O.B. Hijab** (Ohio State University, Columbus, USA) 11 March - 4 April 1984. **E. Hairer** (University of Heidelberg, West Germany) 26-30 March 1984. **T. Ikeda** (Kyoto University, Japan) 7-9 December 1983. **A. del Junco** (Ohio State University, Columbus, USA) 19 December 1983, February - May 1984. **J. Jurecková** (Charles University, Prague, Czechoslovakia) 26 January 1984. **S-O. Londen** (University of Technology, Helsinki, Finland) 21 January 1984. **M.C. Mackey** (McGill University, Montreal, Canada) 1 March 1984. **D.M. Mason** (University of Wisconsin, Madison, USA) 18-24 March 1984. **G.L. Nemhauser** (Cornell, Ithaca, USA) 2 days in March 1984. **M.F. Neuts** (University of Delaware, Newark, USA) 2-4 January 1984. **P. Révész** (Hungarian Academy of Sciences, Budapest) 19 March 1984. **P. Rousseeuw** (Brussels, Belgium) 21 December 1983. **B. Schmitt** (University of Strassbourg, France) 19-21 March 1984. **C. Smith** (University of Maryland, USA) 11-13 January 1984. **A. Tesei** (Instituto 'Mauro Picone', Rome, Italy) 20 January 1984. **C. Vercellis** (University of Milan, Italy) 23-24 January 1984. **J.A. Wellner** (University of Washington, Seattle, USA) 19 December 1983.


CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER
CWI NEWSLETTER

Order form for CWI Publications

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

□ Please send the reports marked below on an exchange basis
□ Please send the reports marked below with an invoice

Publication code	Price per copy	Number of copies wanted
MC Tract 163	Dfl. 19.10	
IW 239/83	3.70	
IW 240/83	3.70	
IW 241/83	3.70	
IW 242/83	3.70	
IW 243/83	3.70	
IW 244/83	3.70	
IW 245/83	3.70	
IW 246/83	3.70	
IW 247/83	3.70	
IW 248/83	3.70	
BW 190/83	3.70	
BW 191/83	3.70	
BW 192/83	3.70	
BW 193/83	3.70	
BW 194/83	3.70	
NW 162/83	4.80	
NN 31/83	11.65	
NN 32/83	4.80	
SW 97/83	3.70	
SN 12/83	3.70	
TW 247/83	4.80	
TW 248/83	6.--	
TW 249/83	6.--	
ZW 196/83	3.70	
ZW 201/83	3.70	
ZW 202/83	3.70	
ZW 203/83	3.70	

Contents