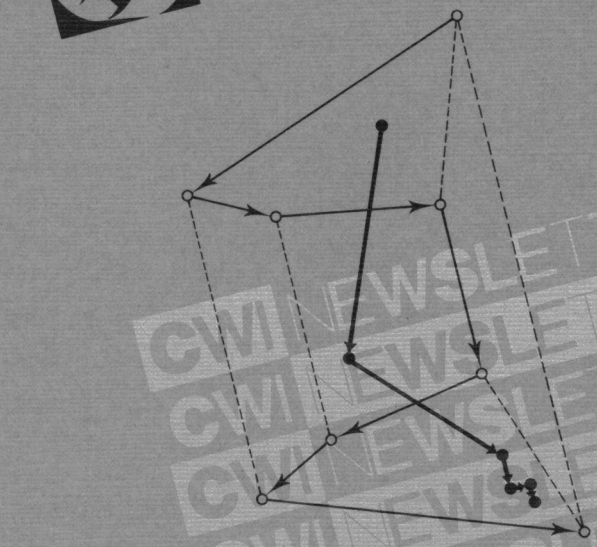
CWI NEWSLETTER



Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

Quarterly, issue no. 8
September 1985

CWI NEWSLETTER

Number 8, September 1985

Editors

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

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

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

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

ISSN 0168-826x

Contents

Centre for Mathematics and Computer Science

Centrum voor Wiskunde en Informatica

The New Linear Programming Method of Karmarkar

A. Schrijver
Department of Econometrics Tilburg University
P.O. Box 90153, 5000 LE Tilburg, The Netherlands
and
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

1. Introduction

In April 1984, at the 16th Annual ACM Symposium on Theory of Computing, Narendra Karmarkar of AT&T Bell Laboratories presented a new algorithm for linear programming. The algorithm was not only shown to be theoretically efficient (i.e., its running time is bounded by a polynomial in the input size), but was also claimed to be very fast in practice — about 50 times faster than Dantzig's classical *simplex method,* for the largest problems evaluated.

This news created much excitement among computer scientists and mathematical programmers, and subsequent reports, inter alia in *Science* magazine and on the front page of the *New York Times,* contributed to a further propagation of the sensation. Linear programming is one of the mathematical fields most applied in practice. Linear programming problems occur in such diverse areas as engineering, transportation, agriculture, distribution, scheduling, nutrition, management, and a reduction of the computer time needed would not only speed up solving linear programming problems, but also would allow one to solve larger LP-problems than before. In situations like oil processing and automatic control, quick, almost forthwith, solution of LP-problems is essential.

In 1979, L.G. Khachiyan published the first polynomial-time method for linear programming, the *ellipsoid method.* This method, though theoretically efficient, turned out to behave rather disappointingly in practice. So Karmarkar's claim that he now has found a method which is both theoretically and practically efficient, was much welcomed. Karmarkar's paper was published in the December issue of *Combinatorica* [5]. However, no computational details were given.

Next, Karmarkar was invited to give plenary lectures at two international

conferences, the ORSA/TIMS-meeting in November 1984 in Dallas, and the 12th International Symposium on Mathematical Programming in August 1985 at MIT. KARMARKAR described his method and variants, explaining some of the tricks used in practice, claiming superiority of his method over the simplex method, and giving a few comparisons, but he refused to give full disclosure of test problems, computer programs and running times. This has led to much uncertainty and discussion among mathematical programmers with respect to the practical value of the new method. It led to a report 'Founding father of just a footnote?' in the *Boston Globe* of August 9, 1985:

> 'This week in Cambridge, the 28-year-old KARMARKAR came under mounting fire from his colleagues at the 12th International Symposium on Mathematical Programming. They snorted at his scientific manners, scoffed at his claims and derided his results as being everything from 'frisky' to 'majestic'. Mostly, they said that his accounts of super-fast solutions to difficult problems couldn't be replicated. ....
> ... 'He may have some wonderful method after all, but I habitually mistrust all secret mathematics', said E.M.L. BEALE, a pioneer in the commercial applications of linear programming. ...
> ... KARMARKAR himself didn't advance his cause much in a talk before an unusual plenary session of the MIT meeting of some 800 scientists from around the world. He began by observing that while mathematicians agree on what constitutes convincing proof of a mathematical proposition, there is no corresponding consensus as to what makes a persuasive presentation of experimental results — a contention that was immediately disputed by many of his listeners.'

Indeed, there is some generally accepted standard in presenting computional results. One gives (or makes available) the computer program, the test data, the type of computer, the output, and the CPU-time. In essence, the results are replicable, possibly making due allowance for the running time. Generally, one tries to give as much information as possible within the compass of a lecture or report.

Although this consensus differs from that holding in mathematics, with its strict rules for definitions, theorems and proofs, it essentially is comparable with the praxis in other branches of sciences, such as physics and chemistry, when reporting on experiments.

Karmarkar's reservedness in presenting computational details may have respectable reasons, for instance that Bell Labs has propriety of the actual computer program, which might not yet be ready as a marketable package, but the scientific community turns out to sputter if despite that a similar reservedness in making claims is not observed.

In this account of the new method I will restrict myself to the theoretical aspects.

In Section 2 and 3 we briefly discuss the simplex method and Khachiyan's ellipsoid method. In Section 4 and 5 we describe Karmarkars method, while in Sections 6 and 7 we show that the method has polynomially bounded running time.

2. Linear programming and the simplex method

The *linear programming problem* (or *LP-problem)* is as follows:

$$\text{given } A \in \mathbb{Z}^{m \times n},\ b \in \mathbb{Z}^m,\ c \in \mathbb{Z}^n, \tag{1}$$

$$\text{find a vector } x \in \mathbb{Q}^n \text{ attaining } \max\{c^T x \mid Ax \leqslant b\}.$$

So it is asked to maximize the linear function $c^T x$ where x ranges over the polyhedron $\{x \mid Ax \leqslant b\}$. The practical relevance of this problem was revealed in the 1940s by the work of L.V. Kantorovich, Tj.C. Koopmans and G.B. Dantzig.

In 1947 Dantzig designed his famous *simplex method* for solving (1). The idea is to make a trip over the polyhedron $P := \{x \mid Ax \leqslant b\}$ from vertex to vertex along edges, on which $c^T x$ increases, until an optimum vertex is attained. The correctness of this algorithm is based on the property that if a vertex x_0 of a polytope P does *not* maximize $c^T x$ over P, then there exists a vertex x_1 *adjacent to* x_0 for wich $c^T x_1 > c^T x_0$. (Here x_1 *adjacent to* x_0 means that the segment $x_0 x_1$ forms an edge of P.)

Roots of this idea occur already in Fourier [3], describing a method for minimizing $\|Ax - b\|_\infty$ (where $\|\star\|_\infty$ denotes the maximum absolute value of the entries in $\star$):

> 'Pour atteindre promptement le point inférieur du vase, on élève en un point quelconque du plan horizontal, par exemple à l'origine des x et y, une ordonnée verticale jusqu'à la rencontre du plan le plus élevé, c'est-à-dire que parmi tous les points d'intersection que l'on trouve sur cette verticale, on choisit le plus distant du plan des x et y. Soit m_1, ce point d'intersection placé sur le plan extrême. On descend sur ce même plan depuis le point m_1 jusqu'à un point m_2 d'une arête du polyèdre, et en suivant cette arête, on descend depuis le point m_2 jusqu'au sommet m_3 commun à trois plans extrêmes. Apartir du point m_3 on continue de descendre suivant une seconde arête jusqu'à un nouveau sommet m_4, et l'on continue l'application du même procédé, en suivant toujours celle des deux arêtes qui conduit à un sommet moins élevé. On arrive ainsi très-prochainement au point le plus bas du polyèdre.'

According to Fourier, this description suffices to understand the method in

more dimensions. DE LA VALLÉE POUSSIN [9] gave a similar method.

DANTZIG [2] algebraized the method, obtaining an attractive compact scheme *(simplex tableau)* and iterative procedure *(pivoting),* which facilitates computer implementation. This simplex method turns out to be very efficient in practice and enables one to solve LP-problems in several thousands of variables.

However, it could not be proved theoretically that the simplex method is efficient. That is, no proof has been found that the running time of the simplex method is bounded by a polynomial in the size of the problem, i.e. in

$$\sum_{i,j} \log(|a_{ij}|+1) + \sum_{i} \log(|b_i|+1) + \sum_{j} \log(|c_j|+1). \tag{2}$$

In fact, KLEE and MINTY [7] showed, by giving a bad class of LP-problems, that with Dantzig's pivoting rule, the simplex method can require exponential running time. Their examples have as feasible regions a deformation of the n-dimensional cube (described by $2n$ inequalities), for which Dantzig's rule leads to a trip along all 2^n vertices. Several alternative pivot selection rules have been proposed, but none of them could be proved to yield a polynomial-time method.

On the other hand, BORGWARDT [1] recently gave a pivoting rule which he showed to yield a polynomial-time algorithm *on the average,* in a certain natural probabilistic model. His result very much agrees with practical experience, where data seem to be more 'random' than structural.

3. THE ELLIPSOID METHOD

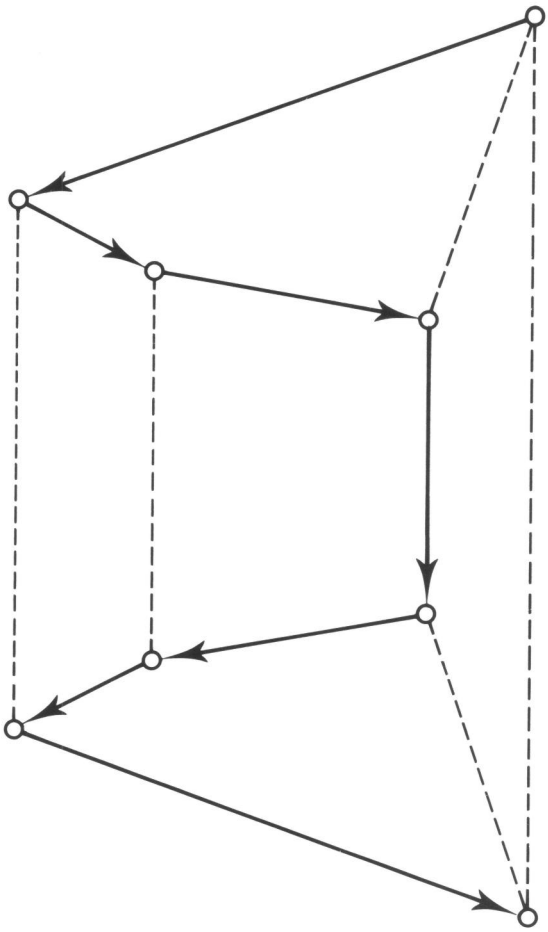
It has been an open question for a long time whether linear programming is solvable in polynomial time. Although the simplex method works well for present-day practical problems, one never knows whether the barycenter of practical problems will change, and it would then be good to have a method which can be proved to perform well always.

It was a big surprise when in 1979 the Soviet mathematician L.G. KHACHIYAN answered this question affirmatively, showing that the *ellipsoid method* for nonlinear programming has polynomially bounded running time when applied to LP-problems. Also this result was reported on the front page of the *New York Times.*

Khachiyan's method can be described by application to the following problem:
given

$$A \in \mathbb{Z}^{m\times n},\quad b \in \mathbb{Z}^m,\ \text{find } x \in \mathbb{Q}^n \text{ such that } Ax \leqslant b. \tag{3}$$

This problem is *polynomially equivalent* to problem (1), i.e., any polynomial-time algorithm for problem (1) yields a polynomial-time algorithm for problem (3), and conversely. Indeed, (3) easily reduces to (1) by taking $c \equiv 0$. Conversely, by the Duality theorem of linear programming, solving (1) is



A deformation of the n-dimensional cube, with a simplex path along 2^n *vertices* $(n=3)$

equivalent to solving the following system of linear inequalities:

$$Ax \leqslant b,\ \ y^T \geqslant 0,\ \ y^T A = c,\ \ y^T b \leqslant c^T x \tag{4}$$

(clearly, equations can be split into two opposite inequalities). This is a special case of (3).

To sketch Khachiyan's method, we assume that the polyhedron $\{x \mid Ax \leqslant b\}$ is bounded and full-dimensional (KHACHIYAN showed that we without loss of generality may restrict ourselves to this case). Let T be the maximum absolute value of the entries in A and b (w.l.o.g. $T \geqslant n \geqslant 2$). With Cramer's rule, one may show that the components of the vertices $\{x \mid Ax \leqslant b\}$ are at most $n^n T^n$ in absolute value. Hence $\{x \mid Ax \leqslant b\}$ is contained in the ball $E_0 := B(\mathbf{0}, R)$

around the origin of radius $R := n^{n+1}T^n$.

E_0 is the first ellipsoid. Next ellipsoids $E_1, E_2, \ldots$ are determined with the following rule. If E_k has been found, with center say z_k, check if $Az_k \leqslant b$ holds. If so, we have found a solution of $Ax \leqslant b$ as required. If not, we can choose an inequality, say $a_i^T x \leqslant b_i$ in $Ax \leqslant b$ violated by z_k. Let E_{k+1} be the ellipsoid such that

$$E_{k+1} \supseteq E_k \cap \{x \mid a_i^T x \leqslant a_i^T z_k\} \tag{5}$$

and such that E_{k+1} has smallest volume (there exist simple updating formulas for obtaining the parameters describing E_{k+1} from those describing E_k and from a_i). Since $\{x \mid Ax \leqslant b\} \subseteq \{x \mid a_i^T x \leqslant a_i^T z_k\}$, it follows by induction on k from (5) that

$$E_k \supseteq \{x \mid Ax \leqslant b\}. \tag{6}$$

Moreover, it can be proved that

$$\text{volume } E_{k+1} < e^{-1/4n} \cdot \text{volume } E_k. \tag{7}$$

Since one easily sees that volume $E_0 \leqslant (2R)^n < n^{2n^2} T^{n^2}$, inductively from (7) we have:

$$\text{volume } E_k < e^{-k/4n} \cdot n^{2n^2} T^{n^2}. \tag{8}$$

On the other hand, with Cramer's rule, using the boundedness and fulldimensionality of $\{x \mid Ax \leqslant b\}$, we know:

$$\text{volume } \{x \mid Ax \leqslant b\} \geqslant n^{-2n^2} T^{-n^2}. \tag{9}$$

(6), (8) and (9) imply:

$$n^{-2n^2} T^{-n^2} \leqslant e^{-k/4n} \cdot n^{2n^2} T^{n^2}, \tag{10}$$

i.e.,

$$k \leqslant 16n^3 \ln n + 8n^3 \ln T. \tag{11}$$

So after a polynomially bounded number of iterations we will have found a solution of $Ax \leqslant b$. Updating the ellipsoid parameters can be done in $\mathcal{O}(n^2)$ arithmetic operations, while all calculations have to be done with a precision of $\mathcal{O}(n^3 \log T)$ digits. Altogether this amounts to $\mathcal{O}(n^8 \log^2 T)$ bit operations (excluding data-handling, which takes $\mathcal{O}(\text{loglog } T \cdot \text{logloglog } T)$ for each bit operation).

Although KHACHIYAN showed the polynomial solvability of the linear programming problem, his method turned out to perform badly in practice. This is caused, among others, by the facts that the upper bound (11) of iterative steps, though polynomial in the input size, can be rather big also for moderate problems, and that the precision required to describe the successive ellipsoids is huge. (The ellipsoid method has implications in combinatorial optimization — see [4].)

Thus the question remained if there is a method for linear programming which is both practically and theoretically efficient. KARMARKAR claims that the following method is so.

4. KARMARKAR'S FORM OF THE LINEAR PROGRAMMING PROBLEM

Karmarkar's method applies to problems of the following form:

$$\text{given } A \in \mathbb{Z}^{m \times n},\ c \in \mathbb{Z}^n \text{ such that } A\mathbf{1} = \mathbf{0}, \tag{12}$$

$$\text{find } x \in \mathbb{Q}^n \text{ such that } x \geqslant 0,\ Ax = \mathbf{0},\ \mathbf{1}^T x = 1,\ c^T x \leqslant 0.$$

(Here $\mathbf{1}$ denotes an all-one column vector of appropriate dimension.) This is a problem equivalent to (1) and (3). Indeed, (12) clearly is a special case of (1), as (12) amounts to finding x attaining $\max\{-c^T x \mid x \geqslant 0, Ax = \mathbf{0}, \mathbf{1}^T x = 1\}$. Conversely, (3) can be reduced to solving a system of linear equations in non-negative variables:

$$\text{given } A \in \mathbb{Z}^{m \times n},\ b \in \mathbb{Z}^m, \tag{13}$$

$$\text{find a vector } x \in \mathbb{Q}^n \text{ such that } x \geqslant 0,\ Ax = b.$$

This follows by replacing $Ax \leqslant b$ by the system: $Ax' - Ax'' + x''' = b,\ x', x'', x''' \geqslant 0$. Now (13) can be reduced to (12) as follows. Let A, b as in (13) be given. Let T be the maximum absolute value of the entries in A and b. With Cramer's rule we can prove that if $x \geqslant 0,\ Ax = b$ has a solution, it has one satisfying $\mathbf{1}^T x \leqslant n^{n+1} T^n$. So we wish to solve:

$$x \geqslant 0,\ Ax = b,\ \mathbf{1}^T x \leqslant n^{n+1} T^n. \tag{14}$$

By adding one extra variable we may assume we must solve:

$$x \geqslant 0,\ Ax = b,\ \mathbf{1}^T x = n^{n+1} T^n. \tag{15}$$

By subtracting multiples of the last equation in (15) from the equations in $Ax = b$ and by scaling equations, this is equivalent to:

$$x \geqslant 0,\ Ax = \mathbf{0},\ \mathbf{1}^T x = 1. \tag{16}$$

If $A\mathbf{1} = \mathbf{0}$ then $n^{-1}\mathbf{1}$ is a solution. Otherwise, by elementary changes of the system we may assume $A\mathbf{1} = \mathbf{1}$. So we wish to find a solution x, λ for:

$$x \geqslant 0,\ \lambda \geqslant 0,\ Ax - \mathbf{1}\lambda = \mathbf{0},\ \mathbf{1}^T x + \lambda = 1, \text{ such that } \lambda \leqslant 0. \tag{17}$$

Since $A\mathbf{1} - \mathbf{1} \cdot 1 = 0$, this is a special case of (12) (taking $A := [A, -\mathbf{1}]$, $c := (0, \ldots, 0, 1)^T \in \mathbb{Z}^{n+1}$).

So Karmarkar's method applied to (12) solves linear programming in general.

5. KARMARKAR'S METHOD

Karmarkar's method consists of constructing a sequence of vectors $x^0, x^1, x^2, \ldots$ converging to a solution of (12) (provided (12) has a solution). The essence of the method is to replace the condition $x \geqslant 0$ by a stronger condition $x \in E$, for some ellipsoid E contained in $\mathbb{R}^n_+$. As we shall see, minimizing $c^T x$ over $\{x \mid x \in E, Ax = \mathbf{0}, \mathbf{1}^T x = 1\}$ is easy, while minimizing $c^T x$ over $\{x \mid x \in \mathbb{R}^n_+, Ax = \mathbf{0}, \mathbf{1}^T x = 1\}$ is the original problem (12).

Let A and c as in (12) be given. We may assume without loss of generality that the rows of A are linearly independent, and that $n \geqslant 2$. Throughout we use

$$r := \sqrt{\frac{n}{n-1}}. \tag{18}$$

Let

$$x^0 := \frac{1}{n} \cdot \mathbf{1}. \tag{19}$$

So $Ax^0 = 0$, $\mathbf{1}^T x^0 = 1$, $x^0 > 0$. Next a sequence of vectors $x^0, x^1, x^2, \ldots$ such that $Ax^k = 0$, $\mathbf{1}^T x^k = 1$, $x^k > 0$ is determined, with the following recursion: denote $x^k =: (x_1^{(k)}, \ldots, x_n^{(k)})^T$, and let D be the diagonal matrix:

$$D := \operatorname{diag}(x_1^{(k)}, \ldots, x_n^{(k)}). \tag{20}$$

Define z^{k+1} and x^{k+1} as :

$$\begin{aligned} &z^{k+1} \text{is the vector attaining} \\ &\min \{(c^T D)z \mid (AD)z = \mathbf{0}; \mathbf{1}^T z = n;\ z \in B(\mathbf{1}, \tfrac{1}{2}r)\}, \\ &x^{k+1} := (\mathbf{1}^T D z^{k+1})^{-1} \cdot D z^{k+1}. \end{aligned} \tag{21}$$

Note that if we replace in the minimization problem the condition $z \in B(\mathbf{1}, \frac{1}{2}r)$ by the weaker condition $z \geqslant 0$, then we would obtain a minimization problem with optimum value at most 0 if and only if $\min \{c^T x \mid Ax = \mathbf{0},\ \mathbf{1}^T x = 1,\ x \geqslant 0\} \leqslant 0$, which is our original problem (12).

As z^{k+1} minimizes $(c^T D)z$ over the intersection of a ball with an affine space, we can write down a formula for z^{k+1}:

PROPOSITION 1.

$$z^{k+1} = \mathbf{1} - \frac{1}{2}r \cdot \frac{(I - DA^T(AD^2A^T)^{-1}AD - n^{-1} \cdot \mathbf{1} \cdot \mathbf{1}^T)Dc}{\|(I - DA^T(AD^2A^T)^{-1}AD - n^{-1} \cdot \mathbf{1} \cdot \mathbf{1}^T)Dc\|}.$$

PROOF. The minimum in (21) can be determined by projecting Dc onto the space $\{z \mid (AD)z = \mathbf{0},\ \mathbf{1}^T z = 0\}$, thus obtaining the vector:

$$p := (I - DA^T(AD^2A^T)^{-1}\mathbf{1} \cdot \mathbf{1}^T)Dc. \tag{22}$$

(Indeed, $ADp = 0$, $\mathbf{1}^T p = 0$, as one easily checks (using $AD\mathbf{1} = Ax^k = 0$), and

$c^T D - p^T$ is a linear combination of rows of AD and of the row vector $\mathbf{1}^T$.)

Then z^{k+1} is the vector reached from $\mathbf{1}$ by going over a distance $\frac{1}{2}r$ in the direction $-p$, i.e.,

$$z^{k+1} = \mathbf{1} - \tfrac{1}{2}r\frac{p}{\|p\|}. \qquad \square \tag{23}$$

This method describes Karmarkar's method.

6. A LEMMA IN CALCULUS

In order to show correctness and convergence of the algorithm, we use the following lemma in elementary calculus. For $x=(x_1, \ldots, x_n)^T$, we denote:

$$\Pi x := x_1 \cdot \ldots \cdot x_n. \tag{24}$$

LEMMA. *Let* $n \in \mathbb{N}$, $H := \{x \in \mathbb{R}^n \mid \mathbf{1}^T x = n\}$. *Then:*

(i) $H \cap B(\mathbf{1},r) \subseteq H \cap \mathbb{R}^n_+ \subseteq H \cap B(\mathbf{1},(n-1)r)$;

(ii) *if* $x \in H \cap B(\mathbf{1}, \frac{1}{2}r)$, *then* $\Pi x \geqslant \frac{1}{2}(1+\frac{1/2}{n-1})^{n-1}$.

(i) Let $x=(x_1, \ldots, x_n)^T \in H \cap B(\mathbf{1},r)$. To show $x \in \mathbb{R}^n_+$, suppose without loss of generality $x_1 < 0$. Since $x \in B(\mathbf{1},r)$ we know: $(x_2-1)^2+\ldots+(x_n-1)^2 \leqslant r^2-(x_1-1)^2 < r^2-1 = 1/(n-1)$. Hence, with Cauchy-Schwarz:

$$(x_2-1)+\ldots+(x_n-1) \leqslant \sqrt{n-1}\cdot\sqrt{(x_2-1)^2+\ldots+(x_n-1)^2} < 1.$$

Therefore, $x_1+\ldots+x_n < x_2+\ldots+x_n < n$, contradicting the fact that x belongs to H.

Next let $x \in H \cap \mathbb{R}^n_+$. Then

$$\begin{aligned}(x_1-1)^2+\ldots+(x_n-1)^2 &= (x_1^2+x_n^2)-2(x_1+\ldots+x_n)+n \\ &\leqslant (x_1+\ldots+x_n)^2-2(x_1+\ldots+x_n)+n \\ &= n^2-2n+n = (n-1)^2r^2.\end{aligned}$$

(The last inequality follows from the fact that $x \geqslant 0$.) So $x \in B(\mathbf{1},(n-1)r)$.

(ii) We first show an auxiliary result:

$$\begin{aligned}&\text{let } \lambda,\mu \in \mathbb{R}; \text{ if } x^*,y^*,z^* \text{ achieve} \\ &\min\{xyz \mid x+y+z=\lambda,\ x^2+y^2+z^2=\mu\}, \text{and} \\ &x^* \leqslant y^* \leqslant z^*, \text{ then } y^*=z^*.\end{aligned} \tag{25}$$

By replacing x, y, z by $x-\frac{1}{3}\lambda$, $y-\frac{1}{3}\lambda$, $z-\frac{1}{3}\lambda$, we may assume $\lambda=0$.Then it is clear that the minimum is nonpositive, and hence

$x^* \leqslant 0 \leqslant y^* \leqslant z^*$. Therefore,

$$x^* y^* z^* \geqslant x^* \left(\frac{y^*+z^*}{2}\right)^2 = \frac{1}{4}(x^*)^3 \geqslant -\frac{\mu}{18}\sqrt{6\mu}. \tag{26}$$

The first inequality here follows from the geometric-arithmetic mean inequality (note that $x^* \leqslant 0$), and the second inequality from the fact that if $x+y+z=0$, $x^2+y^2+z^2=\mu$, then $x \geqslant -\frac{1}{3}\sqrt{6\mu}$.

On the other hand, $(x,y,z) := (-\frac{1}{3}\sqrt{6\mu}, \frac{1}{6}\sqrt{6\mu}, \frac{1}{6}\sqrt{6\mu})$ satisfies $x+y+z=0$, $x^2+y^2+z^2=\mu$, $xyz = -\frac{\mu}{18}\sqrt{6\mu}$. Hence we have equality throughout in (2.6). Therefore, $y^* = z^*$, proving (25).

We now prove (ii) of the Lemma. The case $n=2$ being easy, assume $n \geqslant 3$. Let x attain

$$\min \{\Pi x \mid x \in H \cap B(\mathbf{1}, \tfrac{1}{2}r)\}. \tag{27}$$

Without loss of generality, $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$. Then for all $1 \leqslant i < j < k \leqslant n$, the vector (x_i, x_j, x_k) attains

$$\min\{xyz \mid x+y+z = x_i+x_j+x_k,\ x^2+y^2+z^2 = x_i^2+x_j^2+x_k^2\} \tag{28}$$

(otherwise we could replace the components x_i, x_j, x_k of x by better values). Hence by (25), $x_j = x_k$. Therefore $x_2 = x_3 = \ldots = x_n$. As $x \in H \cap B(\mathbf{1}, \frac{1}{2}r)$, this implies $x_1 = \frac{1}{2}$, and $x_2 = \ldots = x_n = (1+\frac{1}{2}/(n-1))$. This shows (ii). □

7. Operativeness of the algorithm

The operativeness of the algorithm now follows from the following proposition:

Proposition 2. *If (12) has a solution then for all $k \geqslant 0$:*

$$\frac{(c^T x^{k+1})^n}{\Pi x^{k+1}} < \frac{2}{e} \cdot \frac{(c^T x^k)^n}{\Pi x^k}. \tag{29}$$

Proof. First note:

$$\frac{(c^T x^{k+1})^n}{\Pi x^{k+1}} \cdot \frac{\Pi x^k}{(c^T x^k)^n} = \frac{(c^T D z^{k+1})^n}{\Pi (D z^{k+1})} \cdot \frac{\Pi x^k}{(c^T x^k)^n} = \left[\frac{c^T D z^{k+1}}{c^T D \mathbf{1}}\right]^n \cdot \frac{1}{\Pi z^{k+1}}. \tag{30}$$

using (21) and $\Pi(Dz^{k+1}) = (\Pi x^k)(\Pi z^{k+1})$ and $x^k = D\mathbf{1}$.

We next show that, if (12) has a solution, then

$$\frac{(c^T D)z^{k+1}}{(c^T D)\mathbf{1}} \leqslant 1 - \frac{\frac{1}{2}}{n-1}. \tag{31}$$

Indeed, if (12) has a solution then $ADz=0$, $z\geqslant 0$, $c^T Dz\leqslant 0$ for some $z\neq 0$. We may assume $\mathbf{1}^T z=n$. Hence,

$$\begin{aligned} 0 &\geqslant \min\{(c^T D)z \mid z\in\mathbb{R}^n_+, ADz=\mathbf{0},\ \mathbf{1}^T z=n\} \\ &\geqslant \min\{(c^T D)z \mid z\in B(\mathbf{1},(n-1)r), ADz=\mathbf{0}, \mathbf{1}^T z=n\} \end{aligned} \tag{32}$$

(the last inequality follows from (i) of the Lemma).

The last minimum in (32) is attained by the vector $\mathbf{1}-(n-1)r\frac{p}{\|p\|}$, as $\mathbf{1}-\frac{1}{2}r\frac{p}{\|p\|}$ attains the minimum in (21), (cf. (22)).

Therefore, $c^T D(\mathbf{1}-(n-1)r\frac{p}{\|p\|}\leqslant 0$.

This implies

$$\begin{aligned} c^T Dz^{k+1} &= c^T D(\mathbf{1}-\tfrac{1}{2}r\frac{p}{\|p\|}) \\ &= (1-\frac{\frac{1}{2}}{n-1})c^T D\mathbf{1} + \frac{\frac{1}{2}}{n-1}c^T D(\mathbf{1}-(n-1)r\frac{p}{\|p\|}) \\ &\leqslant (1-\frac{\frac{1}{2}}{n-1})\,(c^T D)\mathbf{1}, \end{aligned} \tag{33}$$

proving (31).

Therefore, as $\Pi z^{k+1}\geqslant \frac{1}{2}(1+\frac{1}{2}/(n-1))^{n-1}$, by (ii) of the Lemma,

$$\left(\frac{c^T Dz^{k+1}}{c^T D\mathbf{1}}\right)^n \frac{1}{\Pi z^{k+1}} \leqslant (1-\frac{\frac{1}{2}}{n-1})^n \cdot \frac{1}{\frac{1}{2}(1+\frac{\frac{1}{2}}{n-1})^{n-1}} < \frac{2}{e} \tag{34}$$

(as $(1-x)/(1+x)\leqslant e^{-2x}$ for $x\geqslant 0$, since the function $e^{-2x}-(1-x)/(1+x)$ is 0 for $x=0$, and has nonnegative derivative if $x\geqslant 0$). (30) and (34) combined give (29). □

By induction on k, Proposition 2 implies, if $c^T x^0\geqslant 0, c^T x^1\geqslant 0, \ldots, c^T x^k\geqslant 0$, (using

$$(\Pi x^k)^{1/n}\leqslant \frac{1}{n}\sum_{i=1}^n x_i^k = \frac{1}{n}\leqslant 1):$$

$$c^T x^k \leqslant \frac{c^T x^k}{(\Pi x^k)^{1/n}} < \left(\frac{2}{e}\right)^{k/n}\cdot\frac{c^T x^0}{(\Pi x^0)^{1/n}}\leqslant \left(\frac{2}{e}\right)^{k/n}\cdot nT, \tag{35}$$

where T denotes the maximum absolute value of the entries in A and c (w. l.o.g. $T\geqslant n$).

This gives, if we take

$$N := \lceil \left(\frac{2}{1-ln2} \right) n^2 \ln(nT) \rceil, \tag{36}$$

the following theorem.

THEOREM. *If (12) has a solution, then* $c^T x^k < n^{-n} T^{-n}$ *for some* $k = 0, \ldots, N$.

PROOF. Suppose $c^T x^0, \ldots, c^T x^N \geqslant n^{-n} T^{-n}$. Then (35) holds for $k = N$, implying $c^T x^N < (2/e)^{N/n} \cdot nT \leqslant n^{-n} T^{-n}$. Contradiction. □

So suppose (12) has a solution. Then with Karmarkar's method we find a vector x^k satisfying $x^k \geqslant 0$, $Ax = \mathbf{0}$, $\mathbf{1}^T x = 1$, $c^T x^k < n^{-n} T^{-n}$. By elementary linear algebra, it is easy to find a *vertex* x^* of the polytope $\{x \geqslant 0 \mid Ax = \mathbf{0}, \mathbf{1}^T x = 1\}$ with $c^T x^* \leqslant c^T x^k$. Hence, $c^T x^* < n^{-n} T^{-n}$. By Cramer's rule, the entries in x^* have a common denominator at most $n^n T^n$. As c is integral, this implies $c^T x^* \leqslant 0$. So x^* is a solution of (12).

Karmarkar's method consists of $\mathcal{O}(n^2 \log T)$ iterations, each consisting of $\mathcal{O}(n^3)$ arithmetic operations (due to the updating formula given by Proposition 1). All calculations have to be made with a precision of $\mathcal{O}(n^2 \log T)$ digits. Altogether this amounts to $\mathcal{O}(n^7 \log^2 T)$ bit operations (excluding data-handling, which takes $\mathcal{O}(\text{loglog}\, T \cdot \text{logloglog} T)$ for each bit operation).

Parts of the description above are taken from the forthcoming book [8].

REFERENCES

1. K.-H. BORGWARDT (1982). The average number of pivot steps required by the simplex method is polynomial. *Zeitschrift für Operations Research 26,* 157-177.
2. G.B. DANTZIG (1951). Maximization of a linear function of variables subject to linear inequalities. TJ.C. KOOPMANS (ed.). *Activity Analysis of Production and Allocation,* John Wiley & Sons, New York, 339-347.
3. J.B.J. FOURIER (1826). Analyse des travaux de l'Académie Royale des Sciences, pendant l'année 1823, Partie mathématique. *Histoire de l'Académie Royale des Sciences de l'Institut de France 6,* xxix-xli.
4. M. GRÖTSCHEL, L. LOVÁSZ, A. SCHRIJVER (1986). *The Ellipsoid Method and Combinatorial Optimization,* Springer-Verlag, Berlin.
5. N. KARMARKAR (1984). A new polynomial-time algorithm for linear programming. *Combinatorica 4,* 373-395.
6. L.G. KHACHIYAN (1979). A polynomial algorithm in linear programming (in Russian). *Doklady Akademii Nauk SSSR 244,* 1093-1096.
7. V. KLEE, G.J. MINTY (1972). How good is the simplex algorithm? O. SHISHA (ed.). *Inequalities, III,* Academic Press, New York, 159-175.
8. A. SCHRIJVER (1986). *Theory of Linear and Integer Programming,* John

Wiley & Sons, Chichester.

9. CH. DE LA VALLÉE POUSSIN (1910). Sur la méthode de l'approximation minimum. *Annales de la Société Scientifique de Bruxelles 35 (2),* 1-16.

A Recent Algorithm for the Factorization of Polynomials

Arjen K. Lenstra
Department of Computer Science
The University of Chicago, Ryerson Hall
1100 E. 58th Street, Chicago, IL 60637, USA

1. Introduction

The last few years a lot of attention has been paid to the problem of factoring polynomials with rational coefficients. An important result was the discovery of a *polynomial-time* factoring algorithm [7]. The purpose of this note is to provide an informal description of this new algorithm.

It is well known that a polynomial in $\mathbb{Q}[X]$ can be decomposed into irreducible factors in $\mathbb{Q}[X]$ and that this factorization is unique up to units. Such a factorization is equivalent to the factorization of a *primitive* polynomial with integral coefficients, where a polynomial is called primitive if the greatest common divisor of its coefficients equals 1. Throughout this note we will therefore restrict ourselves to primitive integral polynomials.

In Van der Waerden [13] it is shown that the factorization of a polynomial in $\mathbb{Z}[X]$ is effectively computable. The method described there was invented in 1793 by the German astronomer von Schubert, and later re-invented by Kronecker; it is usually referred to as *Kronecker's method.* For practical purposes this algorithm can hardly be recommended. A better algorithm was published in 1969 by Zassenhaus [15]. It is based on a combination of Berlekamp's algorithm for the factorization of polynomials over finite fields [6, Section 4.6.2] and Hensel's lemma [6, Exercise 4.6.2.22], and is therefore called the *Berlekamp-Hensel algorithm.* Zassenhaus' method performs quite well in practice, and there is some evidence that its expected running time is a polynomial function of the degree of the polynomial to be factored [2]. It has however one important disadvantage: its worst-case running time is an exponential function of the degree. Polynomials that exhibit the exponential behaviour of the Berlekamp-Hensel algorithm can easily be constructed [5].

In 1982 an algorithm was presented whose running time, when applied to

some polynomial f in $\mathbb{Z}[X]$, is always bounded by a fixed polynomial function of the degree and the coefficient-size of f [7]. A simplified and slightly improved version of this algorithm was given in [4] and [12]. This latter version, which we will follow here, is based on the following observation. The irreducible factors in $\mathbb{Z}[X]$ of f can be regarded as the minimal polynomials (in $\mathbb{Z}[X]$) of its roots. Therefore, to find an irreducible factor of f, it suffices to determine the minimal polynomial of one of its roots. The minimal polynomial of a root α of f immediately follows from an integral linear combination of minimal degree among the powers of α. In Section 2 it is shown that the problem of finding such a relation among the powers of α can be reduced to the problem of finding a relatively short vector in a certain subset of a real vector space. Such a short vector can then be found by means of the *basis reduction algorithm* , as is explained in Section 3.

2. Reduction to finding short vectors

Let f in $\mathbb{Z}[X]$ be the polynomial to be factored and let α be one of its roots. For simplicity we assume that α is real; the general case easily follows from this. Denote by h in $\mathbb{Z}[X]$ the minimal polynomial of α. Obviously, this polynomial h is an irreducible factor of f.

Suppose the degree of h equals m, for some positive integer m. Let c be some fixed positive integer. Below we will show how this integer should be chosen. For an arbitrary polynomial $g \in \mathbb{Z}[X]$ of degree at most m we denote by $\bar{g}$ the $(m+2)$-dimensional vector having the coefficient of X^{i-1} of g as ith coordinate, for $0 < i \leqslant m+1$, and with last coordinate $c \cdot g(\alpha)$. By L_m we denote the subset of $\mathbb{R}^{m+2}$ consisting of these vectors $\bar{g}$; notice that the $(m+2)$-dimensional vector $\bar{h}$ is contained in L_m. There is a natural correspondence between the vectors $\bar{g}$ and integral linear combinations of degree at most m among the powers of α: the first $m+1$ coordinates of $\bar{g}$ correspond to the coefficients of the integral linear combination, and the last coordinate of $\bar{g}$ is the value of that particular combination, multiplied by c. In this Section we show that a relatively short non-zero vector in L_m leads to the coefficients of h, where we use the ordinary Euclidean norm in $\mathbb{R}^{m+2}$ (denoted $|\ |$).

Because h is a factor of f, there exists an upper bound on the absolute value of the coefficients of h that depends only on f [9]. Combined with $h(\alpha) = 0$, we find that there is a bound $B_f \geqslant 2$, only depending on f and not on c, such that $|\bar{h}| \leqslant B_f$. We claim that for any $C > 1$ the value for c can be chosen such that $|\bar{g}| > C \cdot B_f$ if $\gcd(h, g) = 1$. This means that we can choose c in such a way that any non-zero vector $\bar{g}$ that is not much longer than $\bar{h}$, leads to h. Namely, if $|\bar{g}| \leqslant C \cdot B_f$ then $\gcd(h, g) \neq 1$, so that g is an integral multiple of h because h is irreducible and because the degree of g is at most m. Thus h can be found if we can find a vector $\bar{g}$ that is relatively short, i.e., $|\bar{g}| \leqslant C \cdot B_f$ for some $C > 1$.

To prove our claim, let $C > 1$ be a real number, and let $g \in \mathbb{Z}[X]$ of degree

at most m be such that $\gcd(h, g) = 1$. We prove that c can be chosen such that $|\bar{g}| > C \cdot B_f$. Obviously, if the Euclidean length of the vector g (i.e., the vector consisting of the first $m+1$ coordinates of $\bar{g}$) is $> C \cdot B_f$; then also $|\bar{g}| > C \cdot B_f$. Therefore we may assume that the Euclidean length of the vector g is bounded by $C \cdot B_f$; it suffices to prove that c can be chosen such that $|c \cdot g(\alpha)| > C \cdot B_f$.

Denote by n the degree of g. Define the $(m+n) \times (m+n)$ matrix M as the matrix having ith column $X^{i-1} \cdot h$ for $1 \leqslant i \leqslant n$ and $X^{i-n-1} \cdot g$ for $n+1 \leqslant i \leqslant m+n$, where $X^{i-1} \cdot h$ and $X^{i-n-1} \cdot g$ are regarded as $(m+n)$-dimensional vectors. By R we denote the absolute value of the determinant of M, the so-called *resultant* of h and g.

We prove that this resultant R is non-zero. Suppose on the contrary that the determinant of M is zero. This would imply that a linear combination of the columns of M is zero, so that there exist polynomials $a, b \in \mathbb{Z}[X]$ with $\text{degree}(a) < n$ and $\text{degree}(b) < m$ such that $a \cdot h + b \cdot g = 0$. Because $\gcd(h, g) = 1$, we have that h divides b, so that with $\text{degree}(b) < m$, we find $b = 0$, and also $a = 0$. This proves that the columns of M are linearly independent, so that $R \neq 0$. Because the entries of M are integral we even have $R \geqslant 1$.

We add, for $2 \leqslant i \leqslant m+n$, the ith row of M times T^{i-1} to the first row of M, for some indeterminate T. The first row of M then becomes $(h(T), T \cdot h(T), \ldots, T^{n-1} \cdot h(T), g(T), T \cdot g(T), \ldots, T^{m-1} \cdot g(T))$. Expanding the determinant of M with respect to the first row, we find that

$$R = |h(T) \cdot (a_0 + a_1 \cdot T + \ldots + a_{n-1} \cdot T^{n-1}) + g(T) \cdot (b_0 + b_1 \cdot T + \ldots + b_{m-1} \cdot T^{m-1})|,$$

where the a_i and b_j are determinants of $(m+n-1) \times (m+n-1)$ submatrices of M. Evaluating the above identity for $T = \alpha$ yields

$$R = |g(\alpha)| \cdot |b_0 + b_1 \cdot \alpha + \ldots + b_{m-1} \cdot \alpha^{m-1}|,$$

because $h(\alpha) = 0$. From $|\bar{h}| \leqslant B_f$, $|g| \leqslant C \cdot B_f$, and Hadamard's inequality it follows that $|b_j| \leqslant (C \cdot B_f)^{m+n-1}$. Because B_f is also an upper bound for the roots of f we get

$$R \leqslant |g(\alpha)| \cdot (C \cdot B_f)^{2m+n-1},$$

so that, with $R \geqslant 1$, we find

$$|g(\alpha)| \geqslant (C \cdot B_f)^{-2m-n+1}.$$

Therefore, in order to get $|c \cdot g(\alpha)| > C \cdot B_f$, it suffices to take $c > (C \cdot B_f)^{3m}$. This proves our claim.

Of course, the degree m of h is not known beforehand. The way in which we apply the above to determine h is as follows.

For some $C > 1$, to be specified in the next section, we take c minimal such that $c > (C \cdot B_f)^{3 \cdot \text{degree}(f)}$. Next for $m = 1, 2, \ldots, \text{degree}(f) - 1$ in succession we

do the following. Consider the set L_m of $(m+2)$-dimensional vectors $\bar{g}$ as defined above. Because $(C \cdot B_f)^{3 \cdot \text{degree}(f)} \geqslant (C \cdot B_f)^{3 \cdot \text{degree}(h)}$, a non-zero vector $\bar{g}$ in L_m satisfying $|\bar{g}| \leqslant C \cdot B_f$ leads to a polynomial g that has a non-trivial greatest common divisor with h. Therefore, for values of m smaller than the degree of h all non-zero vectors in L_m must have length $> C \cdot B_f$, and there can only be non-zero vectors $\bar{g}$ in L_m satisfying $|\bar{g}| \leqslant C \cdot B_f$ if m is at least equal to the degree of h, i.e., if $\bar{h}$ is also contained in L_m. And, as reasoned above, if m equals the degree of h, then a reasonably short non-zero vector $\bar{g}$ leads to a polynomial g that is a non-trivial multiple of h. This implies that for $m = \text{degree}(h)$ vector $\bar{h}$ is a shortest non-zero vector in the set L_m, and that $\bar{h}$ can be determined if we can find a non-zero vector in L_m that is longer than $\bar{h}$ by at most a factor C. In the next section we will see that, for some value of $C > 1$, we can always find a non-zero vector in L_m that is at most a factor C longer than a shortest non-zero vector in L_m. Thus the algorithm can be terminated as soon as we succeed in finding a non-zero vector $\bar{g}$ of length at most $C \cdot B_f$. If no such vector is found, then all values for m are smaller than degree(h), so that $h = f$.

REMARK. If α is irrational, then in practice it is impossible to work with an exact representation of α. However, it is not difficult to see that the same arguments as above apply if we use a sufficiently close approximation $\tilde{\alpha}$ to α. It appears that it suffices to have $|\alpha - \tilde{\alpha}| < 2^{-s}$, where s is bounded by a polynomial function of the degree of f and of $\log|f|$. Such an approximation of a root of f can be found in polynomial time, as is shown in [11].

If α is a non-real complex number, then we modify the definition of $\bar{g}$ as follows: for arbitrary $g \in \mathbb{Z}[X]$ of degree at most m we denote by $\bar{g}$ the $(m+3)$-dimensional vector having the coefficient of X^{i-1} of g as ith coordinate, for $0 < i \leqslant m+1$, and with last two coordinates $c \cdot \text{Re}(g(\alpha))$ and $c \cdot \text{Im}(g(\alpha))$.

3. How to find the shortest vector

In the previous section we have reduced the problem of factoring polynomials with rational coefficients to the problem of finding a relatively short vector in a certain subset L_m of $\mathbb{R}^{m+2}$. Such a subset of a real vector space is usually called a *lattice*. In this section we will discuss the problem of finding short non-zero vectors in a lattice, and we will see that the shortest vector problem from Section 2 can be solved by means of L. Lovász' *basis reduction algorithm.*

Let n and k be positive integers, and let $b_1, b_2, \ldots, b_k$ be linearly independent vectors in $\mathbb{R}^n$. The *lattice of dimension* k generated by $b_1, b_2, \ldots, b_k$ is defined as the set

$$\{ \sum_{i=1}^{n} r_i b_i : r_i \in \mathbb{Z} \}.$$

The lattice is denoted $L = L(b_1, b_2, \ldots, b_k)$ and $b_1, b_2, \ldots, b_k$ is said to be a

basis for the lattice. Clearly, the set L_m from Section 2 is an $(m+1)$-dimensional lattice generated by $\overline{g}_0, \overline{g}_1, ..., \overline{g}_m$ where $g = X^i$, for $i = 0, 1, ..., m$.

The shortest vector problem for a lattice $L = L(b_1, b_2, ..., b_k)$ is the problem of finding a shortest non-zero vector in L. Of course this problem depends on our choice of norm in $\mathbb{R}^n$. It is known that for the L_∞-norm (the max-norm) the shortest vector problem is **NP**-hard (see for instance [14]), which makes it quite unlikely that there is an efficient algorithm to find a shortest vector with respect to that norm. In Section 2 we are interested in the L_2-norm (the ordinary Euclidean norm). For the L_2-norm the shortest vector problem is still open, i.e., it is unknown whether the problem is **NP**-hard or allows a polynomial-time solution (see [3] for an algorithm that runs in polynomial time if the dimension of the lattice is fixed).

In Section 2 we have a weaker version of the shortest vector problem: it suffices to find a non-zero vector that is longer than a shortest vector by at most a factor C, for some $C > 1$. This problem can be solved as follows. Let $L = L(b_1, b_2, ..., b_k)$ be as above a lattice of dimension k in $\mathbb{R}^n$. In 1981 L. LOVÁSZ invented an algorithm, the basis reduction algorithm (see [7, Section 1]), that transforms the basis $b_1, b_2, ..., b_k$ for L into a *reduced* basis $\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_k$ for L. Roughly speaking, a reduced basis is a basis that is *nearly orthogonal* ; for a precise definition of this concept, and for a description of the basis reduction algorithm, we refer to [7, Section 1].

It is intuitively clear that a basis that is nearly orthogonal contains a vector that is not much longer than a shortest vector in the lattice. For a reduced basis $\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_k$ for L the following can be proved:

$$|\tilde{b}_1|^2 \leqslant 2^{k-1} \cdot |x|^2$$

for every non-zero x in L. This implies that the first vector $\tilde{b}_1$ in the reduced basis is longer than a shortest non-zero vector in L by at most a factor $2^{(k-1)/2}$. In Section 2 it is therefore sufficient to take $C = 2^{m/2}$.

In [7] it is shown that the running time of the basis reduction algorithm, when applied to a basis $b_1, b_2, ..., b_k$ in $\mathbb{Z}^n$, is bounded by a polynomial function of k, n, and $\max_i(\log|b_i|)$. Combined with a precise analysis of the results from Section 2 it follows that a primitive polynomial f in $\mathbb{Z}[X]$ of degree n can be factored in time polynomial in n and $\log|f|$.

Except for a polynomial-time algorithm for factoring polynomials, there exist many more applications of L. Lovász' basis reduction algorithm. To mention a few: simultaneous diophantine approximation [7], breaking knapsack based cryptosystems [1, 8], and the disproof of the Mertens conjecture [10].

REFERENCES

1. E. BRICKELL. Breaking iterated knapsacks. *Proceedings Crypto 84.*
2. G.E. COLLINS. Factoring univariate polynomials in polynomial average time. *Proceedings Eurosam 79,* 317-329.
3. R. KANNAN (1983). Improved algorithms for integer programming and

related problems. *Proceedings 15th STOC.*

4. R. KANNAN, A.K. LENSTRA, L. LOVÁSZ (1984). Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Proceedings 16th STOC.*
5. E. KALTOFEN, D.R. MUSSER, B.D. SAUNDERS (1981). A generalized class of polynomials that are hard to factor. *Proceedings ACM Symposium on Symbolic and Algebraic Computation,* 188-194.
6. D.E. KNUTH (1981). *The Art of Computer Programming, Vol. 2, Second Edition, Seminumerical Algorithms,* Reading, Addison-Wesley.
7. A.K. LENSTRA, H.W. LENSTRA, Jr., L. LOVÁSZ (1982). Factoring polynomials with rational coefficients. *Math. Ann. 261,* 515-534.
8. J.C. LAGARIAS, A.M. ODLYZKO (1983). Solving low-density subset sum problems. *Proceedings 24th FOCS.*
9. M. MIGNOTTE (1974). An inequality about factors of polynomials. *Math. Comp. 28,* 1153-1157.
10. A.M. ODLYZKO, H. TE RIELE (1985). Disproof of the Mertens conjecture. *J. reine und angew. Math. 357.*
11. A. SCHÖNHAGE (1982). *The Fundamental Theorem of Algebra in Terms of Computational Complexity,* Preliminary Report, Math. Inst. Univ. Tübingen.
12. A. SCHÖNHAGE (1984). Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. *Proceedings 11th ICALP, LNCS* 172, 436-447.
13. B.L. VAN DER WAERDEN (1931). *Moderne Algebra,* Springer, Berlin.
14. P. VAN EMDE BOAS (1981). *Another* **NP***-complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice,* Report, Univ. Amsterdam.
15. H. ZASSENHAUS (1969). On Hensel factorization, I. *J. of Number Theory 1,* 291-311.

The Home of the Big Whopper*

Paul M.B. Vitányi
Centre for Mathematics and Computer Science
P.O. Box 4079,
1009 AB Amsterdam,
The Netherlands

Wherein visits to: Computer Science Department, University of Chicago, Chicago, IL; Complexity Workshop (same address); 17th ACM Symposium on Theory of Computing, Providence, RI; Laboratory for Computer Science, MIT, Cambridge, MA; Computer Science Department, University of Rochester, Rochester, NY; Chapel Hill VLSI Conference, Chapel Hill, N.C.; Computer Science Department, University of California, Berkeley, CA; Computer Science Department, Stanford University, Palo Alto, CA; Digital Equipment Co., System Research Center, Palo Alto, CA; IBM San Jose Research Laboratory, San Jose, CA; Computer Science Department, University of California, San Diego, CA.

1. Plains

On April 29 I flew from Amsterdam to Chicago. The purpose of the visit to the Windy City was the newly established Computer Science Department of the University of Chicago (1100 East 58 St) where I gave a talk next day. The strong position of the US $ was advertised by giant billboards along the highway leading into town stating "Europe is on sale! Book a $469 round trip now!"

The Chicago Symphony Orchestra and the Lyric Opera of Chicago are famous. The Art Institute of Chicago has the best collection of impressionists this side of Paris (e.g., Seurat's 'Grande Jatte'), is strong in contemporary art (most appropriately Hopper's 'Nighthawks' is here) and has a distinguished

* This is a modified and gentlified version of the original internal accounting for the described trip. All resemblance to existing people and institutes is unintentional and accidental. All opinions expressed are my own. All errors as well. Free after John Bunyan's "Apology for this Book (Pilgrim's Progress)": *"Some said 'Paul, print it'; others said 'not so'. Some said 'It might be good'; others said 'no'."*

oriental collection. Innovative architecture has long been a Chicago theme: Frank Lloyd Wright and Mies Van Der Rohe worked here. Now downtown Chicago proudly boasts the most expensive skyscraper (the Standard Oil Building covered with Carrara marble), the tallest skyscraper 'Sears Tower' and, with the new state building of Illinois, the skyscraper with most empty space inside. Here we find a gigantic open air mosaic of Chagall - tender and lovely - opposite the Burger King 'Home of the Big Whopper'. On Wabash and Randolph the Underground stands on 10 yard stilts between an admiring crowd of high rise developments. It shudders and sheds flakes of rust whenever a screeching train ventures to pass.

Open air mosaic of Chagall

The University of Chicago is situated in the Hyde Park area of Chicago (East 50th St - East 60th St), and consists for a large part of attractive gargoyle studded neo-gothic buildings. This area forms a pleasant enclave in threatening surroundings. Going on foot below the 50s or above the 60s is ill advised; going too far away from the lake front is dangerous as well. In fact, without tin cover on wheels you can only swim out. The Computer Science Department is presently situated on the ground floor of the Physical Sciences building in Ryerson Hall. The CS department has been recently reestablished under the chairmanship of Robert I. Soare. His philosophy is to attract initially a large number of very strong researchers in algebraical and combinatorial aspects of the theory of computing, and slowly build up a group in Theory and later in Systems. Among the impressive group he has collected are: Laszlo Babai, Laszlo Lovasz, Arjen Lenstra, Janos Simon, Endre Szemeredi. AT&T has supported the department by instituting two AT&T fellowships, of which Babai and Lenstra are the first recipients. In the context of building up the name of the department, the (pre-ACM Symposium on Theory of Computing) Workshop on Computational Complexity in Chicago was held from May 2 — May 4. The main feature of this workshop was a cycle of 4 lectures giving the state of the art in the "NC-class and P-RAM" type of parallel complexity theory, by Richard M. Karp of the Computer Science Division, University of California, Berkeley. NC stands for "Nick's Class": Turing Award winner and originator of the NP-completeness concept Stephen Cook has named this parallel complexity class after one of the original investigators Nicholas Pippenger, Maria Klawe's husband. (At the time unknown, this highest distinction in Computer Science, the Turing Award, has now been conferred to Dick Karp for 1985.) New results were presented by Tom Leighton, Laboratory for Computer Science, MIT, and by Lovasz and Szemeredi, but the big news was the talk by Andrew Chi-Chih Yao of the Computer Science Department, Stanford University, where progress related to the famous P versus NP question was announced. (No solution, but an oracle set which separates the polynomial hierarchy uniformly. Officially presented at 26th IEEE-FOCS in Portland, OR, October 1985.) The Workshop drew over 70 invited participants from the US, together with a couple from Europe. Most participants stayed in the conveniently located Hyde Park Hilton. A late night excursion to Buddy Guy's Checkerboard Lounge in the desolation of 423 E. 43rd Street (five specially dressed excursionists in a ramshackle car) gave that authentic Chicago feeling. "Bluesman Buddy Guy [has] one of the establishments which have made Chicago's blues scene one of the best. The Checkerboard is not in a great area, so don't wander about; rent a car and don't depend on public transportation."

2. New England

On May 5 I flew from Chicago to Providence, Rhode Island, to attend the 17th ACM Symposium on the Theory of Computing. This conference is one of the two yearly preeminent (if you have a hang for theory) computer science conferences in the US (the other one is the IEEE Conference on Fundamentals of Computer Science). The symposium took place in the Biltmore Plaza Hotel, Kennedy Plaza, Providence, and was mainly devoted to issues in the theory of computation. Several interesting new results in the area of distributed computing were presented. Narendra Karmarkar of AT&T Bell Labs presented an impromptu lecture in which he gave a comparison in number of iterations and cpu time between his applauded new method for solving linear programming problems and the standard Simplex method. The practical performance of the new method has this last year been the subject of much debate in the Operations Research community. This issue is so important because of the huge economic investment in linear programming problems. Karmarkar has compared 4 types of problems, ranging in number of parameters and size of problem instances, and prepared by independent outside experts as benchmarks. According to Karmarkar, the results showed a 10 to 300 fold speedup by using the new method, the latter for the very large problem instances.

Rhode Island, smallest state in the Union, is first in corruption. This time Providence hit the news with the Von Bulow trial. The long drawn out case about the Honourable Von Bulow's supposed murder attempt on his rich wife (in coma for the last five years) led first to a life imprisonment sentence; now Von Bulow was acquitted and had a happy reunion in front of the networks with his (long time) girlfriend. During the trial (and the STOC) the famous man stayed in the Biltmore besieged by the national press. This too is the city of which the mayor, offering to host the STOC last year, had to resign half an hour after signing the invitation letter on being charged in a corruption case. The city also contains Ivy League's Brown University. Nearby Newport is the home of the very rich. Their mansions border the ocean along 'Cliff Walk'. In Rosecliff Manor a champagne reception on the grass lawn with view over the ocean took place on the filmic location of 'the Great Gatsby' followed by a lobster dinner in the ballroom.

From May 8 - May 11 I visited the Laboratory for Computer Science, Massachusetts Institute of Technology. In the aftermath of the nearby STOC conference, some more attendees descended on MIT to give talks. Main purpose of my visit here was the Distributed Computing group centered around Nancy Lynch, and to reconnoitre the Boston-Cambridge area for a more protracted visit in the near future. Invited to the weekly faculty luncheon, I had the good fortune to hear director M.L. Dertouzos of the Laboratory for Computer Science expound the newly proposed guidelines for proprietary rights for products like books or software developed at LCS-MIT. As Dertouzos stated: "the proposed guidelines are the most liberal possible. Everybody, from

faculty to students, will be the legal owner of their own work, shared among the participants according to contribution, without MIT having any title to it. This holds insofar as the work has been produced using ordinary (computer) resources. For extraordinary resources like the Athena Project, the ownership will have to be shared with MIT. Similar exceptions have to be made for contract work. The policy will put the LCS at odds with the general MIT policy. This is a responsibility I will take, and the outlined new policy will be the department policy from the immediate future onwards." In the discussion it became clear that the new LCS-MIT policy aimed at trying to keep good faculty and students who are able to write profitable books and software. The previous policy, that MIT has the title to such work produced during employment by MIT (as is common elsewhere), is perceived to encourage the very best people to look for more grazy pastures. This is a general issue among all top US Universities, and, true to its reputation for excellence, LCS-MIT seems the first to change its policy by, in effect, opting to attract and keep the very best experts and waiving short-term (and doubtful because of law suits) monetary gain.

MIT (founded in 1861 in Boston and moved to Cambridge in 1916) is the hub of the high-tech developments along US Route 128 'America's Technology Highway'. MIT has 9,500 students and 123 buildings. (Compare Harvard/Radcliffe with 23,000 students, 274 buildings.) It occupies a sprawling elongated terrain bordering the Charles river in Cambridge opposite from the Back Bay area in Boston. The site is interspersed with sturdy looking turn-of-the-century buildings (viz., the mascot MIT dome), new *avant garde* architecture like the Auditorium by Saarinen, ramshackle barracks which are shedding loose planking, decrepit smoking factory buildings which are left-overs from the last century, factory railroads crossing the area, high-tech companies in modern buildings, and, on Technology Square 545, the Laboratory for Computer Science. Excavations are going on, roads are being paved, buildings are being erected. The institute is appropriately -and perhaps fondly- nicknamed "the factory". One of the newer looking buildings is the CS building, which does not prevent it from being renovated bottom up. Therefore, the Theory part on the third floor is handsomely designed, whereas the Distributed Systems group on the fifth floor is housed somewhat oldfashionedly. Office and other space is pretty tight. Although the regular professors have a 10 times 10 ft cubicle to themselves, with another such cubicle for their private secretary, the graduate students and more ordinary faculty members share rooms, sometimes three to a small room of 12 times 12 ft. This was a pattern I saw repeated also at Stanford University, contrasting with the very spacious accommodations at Chicago University, and the in-between accommodations at Berkeley. Although UNIX is available, the most commonly used operating system seems to be DEC's TOPS 20, and the usual editor Emacs. Finally, MIT proudly boasts an enormously long corridor: crossing the Mathematics

wing is the second longest* corridor in the world (two miles).

To the European eye, Boston-Cambridge makes a pleasing view, with as highlights the Back Bay, Beacon Hill and Harvard Square. In between lies the Charles River lined with frantic joggers and supporting innumerable sailing boats. The Boston area has nearly a hundred Universities, some of them far larger than Harvard or MIT. Beacon Hill is a curious part of the New World in that it looks largely 18th century. Here we find the graves of Paul Revere and Benjamin Franklin bordering a several miles long red stripe in the pavement: the Freedom Trail. This is where it all began.

On May 12 - May 13 I visited the Computer Science Department, University of Rochester, Ray P. Hylan Building, Rochester, NY. On Rochester Airport visitors are gladdened by a large 'Welcome to the Home of Eastman-Kodak' and 'Rochester, first in film'. Without scorning Kodak, or Xerox for that matter 'Xerox, a Rochester Employer', the main reason for my visit was cooperation with former chairman Joel Seiferas on a subject in automata-complexity. The Computer Science Department in Rochester has 36 graduate students and no undergraduates. It has three specialisations: Theory of Computing, Systems and Artificial Intelligence. The department has a wealth of hardware, which is partly connected to the fact that Rochester is the home of the above mentioned industrial giants. Among the equipment of the faculty are: several VAXs 780 and 750, 12 Xerox Altos intelligent work stations (where the MacIntosh technology comes from), 10 SUNs, 6 new Xerox Dandelion Intelligent work stations (descendants of the Altos), part of a BBN Butterfly, and the first Butterfly to be delivered on order. The Bolt Beranek & Newman Butterfly is a multiprocessor machine consisting of 128 Motorola 68010 microprocessors, each with its own few M memory, in a fast permutation topology (viz., in the "butterfly" or Fast Fourier Transform circuit).

3. Old South

May 14 I left Rochester for 'Gone with the Wind' country to visit the Chapel Hill VLSI Conference, held at Chapel Hill, N.C., May 15 - May 17. Attendance to this conference was by invitation only. This is a ruse to keep out hordes of nontechnicians which may flock to conferences graced by the golden acronym. The conference was held on the campus of the University of North Carolina in Chapel Hill, the oldest (1795) *state* university in the US. (Harvard (1636) is the oldest university.) Chapel Hill has about 15,000 regular inhabitants and 23,000 transient students. The latter amuse themselves on Franklin (the main drag) before 12.00 pm in "He Is Not Here" drinking beer and after 00.00 am at "Cat's Cradle" swinging it out. Alumnus Thomas Wolfe once described it as a place that "beats every other town all hollow." The

* Where is the longest?

conference was unusual among scientific conferences because of a sizeable group of reporters attending, and rushing off their findings in the evening. Chapel Hill is one corner of the famous 'Research Triangle': University of North Carolina at Chapel Hill, North Carolina State University at Raleigh and Duke University in Durham, in the center of which is Research Triangle Park. This area is reputed to have the most Ph.D.s per head of population in the US. On Thursday 16th the conferencees visited the new Microelectronics Center of North Carolina (MCNC) located in the Triangle Research Park. MCNC is a not-for-profit corporation founded by five universities: Duke University, North Carolina A&T State University, University of North Carolina at Chapel Hill, University of North Carolina at Charlotte, and Triangle Research Institute. The headquarters is a $20M building with extensive Integrated Circuit design and fabrication facilities. A total of about $100M has by now been invested in this venture. No actual chips had as yet been produced. The color graphics design facilities were demonstrated, and the super cleanness of the building spoke for itself. Another day we were shown the advanced facilities at the University itself. Among the interesting talks at the conference was the idea of "Hot Clocks" by Ch. Seitz from Caltech. Formerly the pope of the idea of delay-insensitive VLSI circuits, this paper presented a 180 degree *volte-face* by propagating chips which are the epitome of synchronization by using the clock itself to power the circuits. Substantial area savings appeared to result. Remarkable was the presented Chapel Hill research on building a VLSI-based graphic system "Pixel-Planes", by conference organizer H. Fuchs et. al., which would also be presented at the July SIGGRAPH conference in San Francisco. This was one of several papers of using VLSI in computer graphics. N.L. Lincoln, of ETA Systems, gave a talk on very large scale computation (VLSC) in which he described feasible approaches of building supercomputers. One approach which recently seemed to become viable was putting a hundred mainframes (in the form of chips) on a sub-pc board, and stacking such boards in a cabinet. The quest for speed with Gallium-Arsenide substrates instead of silicon continues. Optical computing was a scientist dreaming, or, in any event, way out in the future. Another talk was about legal protection for VLSI from patent laws through the 1978 and 1980 revisions of the US Copyright Act to the 1984 Chip Protection Act. Nearly all of the projects presented used the general chip-bakery: the MOSIS project, where those institutes with access to the Arpanet could get a turn-around time, between sending the design and receiving the packaged chips, of about 6 weeks. (Volume about 1300 design projects per year.) One feature of the conference was that nearly all talks concluded with a slide with the magnified picture of 'the final chip': formerly a sign that something had been *actually fabricated*, now somewhat boring because everybody does so and one design looks very much like another. (Except to the proud parents.) Here I could not miss but meeting a 7 ft expatriate Dutchman, Adriaan Ligtenberg, presently at AT&T Bell Labs, Holmdell,

N.J., engaged in the development of VLSI design tools. At his work site his facilities included having a private microVAX under his desk. Another meeting, at the conference dinner in the historic building of Morehead Planetarium (used by U.S. astronauts in preparing for space flights), was with new Computer Science Department (UNC Chapel Hill) Chairman J. Nievergelt who will leave his present position at Informatik, ETH Zurich, Switzerland. At the end of the conference the United Airlines pilots went on strike, which was inconvenient for holders of a United Airlines Airpass, like myself. Having to fly to San Francisco that same day, May 17, I succeeded in cajoling the airlines to first transport me by Delta to Dallas/Fort Worth, and continuing with Braniff to San Francisco.

4. California

Arriving 15 minutes early in San Francisco, was compensated for by having to wait a long time for my checked luggage. The good fortune in arriving early was further offset by the removal from the bag of a small satchel containing half a pound of Dutch coin and *all* receipts so far accumulated. Here I visited Leslie Lamport, lately of SRI-International at Menlo Park, now at DEC-SRC in Palo Alto. On May 20 I spent the day at the Computer Science Department, University of California, Berkeley. My host was Associate Chairman for Computer Science Dominico Ferrari, of the EECS Department. Here I nearly overdid it by giving a CS seminar in the morning and one in the afternoon as well. Luckily, there was coffee on the premisses and goodsized audiences in the room. The group of Ferrari is responsible for the Berkeley Unix releases. In between seminars I had luncheon with the faculty and staff, where the relative responsibilities and the resulting frictions between those two echelons were discussed. One problem is that secretaries have to learn the Unix system, and when they are highly qualified users do not earn more for that. Thus, they tend to go elsewhere to where the appreciation is expressed by an appropriate salary. This results in an extraordinarily high turnover of the supporting administrative staff. Another issue at the meeting was that the staff should screen the faculty from administrative duties and random visitors. (A well known faculty like the one at UC Berkeley attracts so many people who want to talk to them that if they are not shielded no time for significant research is left. Eventually then the faculty looses prominence and the visitors stop coming: a prospect which had little appeal to faculty and staff alike.) UC Berkeley is doing well, and somebody told me that soon the big three in Computer Science will be the big four.

On May 21 I proceeded to nearby Palo Alto, Cal., focal point of Silicon Valley, to visit the Computer Science Department, Stanford University, housed in Margaret Jacks Hall. Stanford University owes its existence to one Leland Stanford Jr., in whose memory his doting mother erected a garishly mosaic studded chapel in - what is described as - "Spanish brown sandstone style".

The chapel wall bears the unforgettable legend 'for the glory of God and <doubling of point size> the memory of Leland Stanford Jr', as well as exhortations to lead a moral and religious life. The Stanfords were railroad barons and owned the huge tract of land on which the university now stands scattered among waving palm trees and approved by a one yard across copper embossed 'Seal of the President of the United States' in the pavement. Shortly after junior changed this earthly existence for a more eternal one, around the turn of the century, senior did so too. The bereaved mother and wife subsequently added a museum (second largest collection of Rodin sculptures) and a mausoleum (for the Stanford family) to the grounds. Just as UC Berkeley has its twice life size copy of the San Marco Campanilla of Venice as focal point on campus, also Stanford has its rallying tower. As far as I know, this may be one of a kind.

Being a speaker in the Stanford Computer Science Colloquium, I was invited to attend the weekly (?) faculty luncheon. Like MIT's, this faculty consists of a host of well-known names. In this case, with a slant towards the theoretical side. I was cheerfully welcomed by acting chairman Nils Nillson, introduced to all entering faculty, "is that Hungarian?", and invited to join the discussion. The topic here was whether the graduate students should be forced to do significant research already in their first year "slave labor for their teacher", or whether only - as is practice now - in their second year. Well-known scientist: "if I would have to have done all these things in my first year at Caltech I would have flunked". Conclusion: continue the present state of events, with perhaps some pressure added. The Stanford faculty scene seems like a firmament studded with bright solitary stars fixed in place with little communication yet fierce competition.

Stanford's CS department has 60 graduate students, computer generated mosaics (resembling pen drawings by Lucebert*) on some outdoor walls, and occupies the basement and 2nd and 3rd floors of the sandstone building. There are some mainframes which seem to be down a lot of the time, about 40 SUN intelligent work stations, Xerox Altos sprinkled here and there, Dandelions etc. Work in Stanford is theoretically oriented, systems and AI.

Giving a CS Colloquium at Stanford is a somewhat unsettling experience. The occasion takes place in a large auditorium, where each seat is supplied with a microphone connected to the sound system. In the back of the auditorium is a smoked glass division, behind which is the recording crew. Each such lecture is transmitted live on television to both remote locations on campus and off campus (for instance, to corporations in Silicon Valley). All listeners can - by direct connection - interrupt the lecture and ask questions which

* Lucebert, pseudonym of Lubertus J. Swaanswijk (1924 -) contemporary Dutch poet-painter of the COBRA group.

rudely bellow from the walls. The video recorded talks are stored in the libraries for future reference. Speakers are presented with a set of instructions on what to wear and how to behave, which follow below.

TELEVISED SEMINARS: A GUIDE FOR GUEST SPEAKERS

I. LET ME KNOW YOUR A/V NEEDS

We can provide 35mm slide projection, 16mm film projection, 3/4″ and VHS videotape playbacks, and computer hook-ups into our video system for certain computers. Please notify me if you are using any visual aids other than one overhead projector.

II. PLEASE DON'T WEAR WHITE!

Clothing with too great a contrast (white shirt with dark slacks) can interfere with the camera's operation. If possible, wear shirts in pastel blues, yellows, and greys.

III. BE AWARE OF THE LIMITATIONS OF TELEVISION

Try not to pace. Do not simultaneously refer to specific points on two separate blackboards.

Our overhead cameras can show material that you place down on your desk, for both off campus and in-studio students. Be aware that televised graphics resolve best when they conform to a ratio of 3 x 4. Material that is typed on 8 1/2 by 11 paper, and small print from books will not be clear. Use fairly large print, ideally 24 point font size. We can provide entire pads of lined paper that we have specially designed for studio use.

If you have a series of visuals that you will be placing on the desk for pickup by the overhead camera, place each page down in the same spot. Do not move your visuals hastily.

Arthur Keller
Coordinator, Stanford CS Colloquia

Dinner in Palo Alto, true to the way it ought to be, was with high-powered thirtyish Silicon Valley people like Leo Guibas (Stanford/DEC-SRC/Technical U. Athens), Pat Cole (Project Leader Personal Computers HP), Co-Chair of the upcoming SIGGRAPH Conference in San Francisco, and Susan Brennan

(Senior Researcher HP) and member of the same conference committee. Conversation turned to problems attending running a conference with 35,000 attendees, personal career planning, and problems in computer graphics. Contrary to the deplorable situation in the Low Countries, big responsibilities are often shouldered by the very young in Silicon Valley.

On May 22 I paid a short visit to the newly established DEC Systems Research Center (SRC), situated just on the edge of the Stanford Campus and Palo Alto proper. This is a new group, which aims at producing long-term work. DEC thinks it needs its own scientific research center to match those of IBM and AT&T Bell.

> SRC's role is to design, build, and use new digital systems five to ten years before they become commonplace. The purpose is to advance both the state of the knowledge and the state of the art. SRC will create and use real systems in order to investigate their properties. Interesting systems are too complex to be evaluated purely in the abstract. Our strategy is to build prototypes, use them as daily tools, and feed the experience back into the design of better tools and more relevant theories. Most of the major advances in information systems have come through this strategy, including time-sharing, the Arpanet, and distributed personal computing. Among the areas SRC will build prototypes during the next several years are applications of high-performance personal computing, distributed computing, communications, databases, programming environments, system-building tools, design automation. specification technology, and tightly coupled multiprocessors. SRC will also do work of a more formal and mathematical flavor: some members will be constructing theories, developing algorithms, and proving theorems as well as designing systems and writing programs. Some of SRC's work will be in established fields of theoretical computer science, such as the analysis of algorithms, computational geometry and logics of programming. In other cases, new ground motivated by problems arising in systems research will be explored. DEC has a commitment to open research. The improved understanding that comes with widespread exposure seems more valuable than any transient competitive advantage. SRC will freely report results at conferences and in professional journals. We will encourage visits by university researchers and conduct collaborative research. We will actively seek users for our prototype systems. To facilitate interchange, we will develop systems that run on hardware available to universities and work out ways of making our software available for academic use.

The new SRC is largely staffed by the former researchers from Xerox Palo Alto Research, the people who invented the technology of the Xerox Alto, bit map display and the like. Owing to failure of Xerox to properly market these machines, and eventual sale of the technology to Apple Co. - in search of a new product and thereby able to develop the Lisa and the MacIntosh - the innovative work of this group is not commonly realised. Work is going on in designing a new personal work station. This Firefly will probably be a follow-up of the Xerox Dandelion (itself a follow-up of the Altos), contain five micro-VAXs with a large common memory. SRC has chosen Modula-2 as its primary programming language for the next few years. The SRC has produced as yet

three technical reports. DEC-SRC is distinct from the older DEC Western Research Laboratory a couple of blocks down the road. Late in the evening I saw the Apple Co. headquarters in Cupertino (from the outside).

On May 23 I talked at IBM Research Laboratory in San Jose, geographical heart of Silicon Valley. Peter and Ghica van Emde Boas, Dutchmen for 9 months at IBM, regaled me on stories of the different life in this part of the new world. I, in turn, could tell them about the things transpiring back home. It was a pleasure to settle last year's bet which I lost in the form of a bottle of vintage Veuve Cliquot. The innominate winner, in a surprise switch from theory to practice, now runs a project to build a multiprocessor system. It is rumored that this computer consists of 1024 processors, of very special and secret design, each processor on chip and as powerful as an IBM 3081 mainframe. These processors get their input (and deliver their output) from another one of these processors over a pipelined channel with a peak of 6 Mfl. The processors communicate with each other over a fast permutation network like an FFT network. The machine seems essentially made for special purpose application in scientific computations such as the numeric solution of second order partial differential equations and the like.

IBM San Jose employes about 7,000 people, of which but a relatively small number do fundamental computer-based research. Prominently on display in the main hall of the part of the complex I visited were models and photographs of the posh group of buildings IBM is building in the nearby mountains as an attractive new site for fundamental research in Computer Science and associated branches of Mathematics. It seems that most major corporations in the field are rapidly expanding their activities in fundamental research. In the late afternoon Peter and Ghica brought me to the San Jose airport to take an American Airlines flight to San Diego (thus avoiding the UA strike).

From May 24 - May 26 I visited the Computer Science Department of the University of California, San Diego. Here my host was Walter Savitch. San Diego is appointed as the center of an interuniversity network in the southern part of California, to give universities in the area rapid access to supercomputers. Soon, supercomputer users at Stanford will compute on the supercomputers in San Diego Super Computer Center. This is the result of a nation wide campaign in US Congress, and a feasibility study at SRI-International, to give the major universities on-line access to supercomputers. The campus of UC San Diego is picturesquely situated among a million eucalyptus trees near the beach of subcity La Jolla "La Hojja". The architecture of the buildings is modern but very pleasant, and, since a few years, the statue of "The Sun God" (also called "the Chicken") in Karel Appel* like colors benevolently glowers over the campus. It emanates golden rays from its high pedestal while the sun

* Karel Appel (1921 -) contemporary Dutch painter-sculptor. Member of the COBRA group.

The Sun God

sets in the west in the Pacific. Scenic San Diego's airport is perhaps the only one in the world situated right in the center of a major city. Startled first time arrivals gaze at skyscrapers towering left and right above them just before touch-down, and wonder whether the pilot knows what he is doing. Among the attractions of the area are one of the best zoo's in the world and a major wildlife park. On the 26th I tried to figure out how to get by United to Chicago to catch the connecting KLM flight next day. But now not only were the pilots on strike, but also the computer was down "I cannot do anything for

you sir, I am looking at a blank screen". Spending Sunday in Mexico (another nearby attraction) I tried again next evening. Now the one flight which was flying was full, but I could try on stand-by basis. This was no good to me, so after some insistence and the discovery of a magical "M" status on the ticket, I was told that maybe American Airlines would endorse the ticket. And they did, most friendly and efficiently. So, on the 27th home again in a KLM plane from Chicago. The movie was 'All of me', and seated next to me in the row where you can stretch your legs in a 747 was a friendly citizen of Lincoln's birthplace (Springfield, Ill.). He had been shot down in a fighter plane above Midwoud (N-H) during the war, and was now en route to visit old friends in the Netherlands, as he did every seventh year.

Abstracts

of Recent CWI Publications

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

CWI Syllabus 6. P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls & J.W. de Roever. *Proceedings Seminar 1982-1983 Mathematical Structures in Field Theories.*
AMS 81EXX, 81E10, 53BXX, 55RXX, 55N30; 250 pp.
Abstract: Starting from 1982/1983, the University of Amsterdam played host to a series of seminars on the mathematics of field theories. This volume contains the lecture series of the first year which were concerned with the basics of quantum field theory and with Yang-Mills gauge theories. The volume contains several in depth lecture series covering on the whole known material in a form suitable on the one hand to mathematicians who desire to know more about physics and physical intuition underlying this field, and suitable to theoretical physicists who need to know more about the mathematical techniques involved. This reflected the composition of the group of participants. Further volumes covering the material presented in 1983/1984 and 1984/1985 are in preparation. Topics covered: Feynman path integral and perturbation quantum field theory, topological solutions and Derricks theorem, fields and Lagrangians, the Ward Ansatz for Y.-M. potentials, massless field equations, sheaf cohomology, Penrox tranform.

CS-R8513. S.J. Mullender & P.M.B. Vitányi. *Distributed match-making for processes in computer networks.*
AMS 68C05, 68C25; CR C.2.1, F.2.2, G.2.2; 22 pp.; **key words:** locating objects, locating services, computer networks, network topology.
Abstract: In the very large multiprocessor systems and, on a grander scale, computer networks now emerging, processes are not tied to fixed processors but run on processors taken from a pool of processors. Processors are released when a process dies, migrates or when the process crashes. In

distributed operating systems using the service concept, processes can be clients asking for a service, servers giving a service or both. Establishing communication between a process asking for a service and a process giving that service, without centralized control in a distributed environment with mobile processes, constitutes the problem of distributed match-making. Logically, such a match-making phase precedes routing in store-and-forward computer networks of this type. Algorithms for distributed match-making are developed and their complexity is investigated in terms of message passes and in terms of storage needed. The theoretical limitations of distributed match-making are established, and the techniques are applied to several network topologies.

CS-R8514. P.M.B. Vitányi. *Area penalty for sublinear signal propagation delay on chip* (preliminary version).
AMS 68C25, 94C99; CR B.7.0, F.2.3; 22 pp.; **key words:** very large scale integrated circuits (VLSI), wafer scale integration, sublinear signal propagation delay, electronic principles, driving long wires, wire aspect ratio, circuit topology, complete binary tree circuits, H-tree layout, layout area, time, computational complexity and efficiency, actual wire length distributions, Rent's Rule.
Abstract: Sublinear signal propagation delay in VLSI circuits carries a far greater penalty in wire area than is commonly realized. Therefore, the global complexity of VLSI circuits is more layout dependent than previously thought. This effect will be truly pronounced in the emerging wafer scale integration technology. We establish lower bounds on the trade-off between sublinear signalling speed and layout area for the implementation of a complete binary tree in VLSI. In particular, sublinear delay can only be realized at the cost of superlinear area. Designs with equal length wires can either not be laid out at all, viz. for logarithmic delay, or require such long wires in the case of radical delay (i.e., rth root of the wire length) that the aimed for gain in speed is cancelled. Also for wire length distributions commonly occurring on chip it appears that the requirements for sublinear signal propagation delay tend to cancel the gain.

CS-R8515. P. America, J.W. de Bakker, J.N. Kok & J. Rutten. *Operational semantics of a parallel object-oriented language.*
AMS 68B10, 68C01; CR D.1.3, D.2.1, D.3.1, F.3.2; 19 pp.; **key words:** object-oriented programming, parallelism, transition systems, language design, implementation, fairness, operational semantics, maximal parallelism.
Abstract: In this paper the semantics of the programming language POOL is described. It is a language that integrates the object-oriented structure of languages like Smalltalk-80 with facilities for concurrency and communication like the ones in Ada. The semantics is described in an operational way: it is based on transition systems. By using a way of representing parallel processes that is different from the traditional one, it is possible to overcome some difficulties pertaining to the latter. The resulting semantics shows a close resemblance to the informal language description and at the same time there are good prospects that it can serve as a secure guide for the implementation of the language.

CS-N8506. G.J. Hofman & J.C. van Vliet. *On certification and document processing.*
CR K.7.3, I.7.2; 12 pp.; **key words:** certification, testing, text processing.
Abstract: How can functional aspects of document processing systems be certified? It turns out that most existing techniques for testing cannot be applied to this problem. In this article an alternative technique is sketched and applied. This case study suggests that, in order to certify a given type of software, a considerable investment and a considerable knowledge of the problem domain in question are needed.

NM-R8507. P.W. Hemker & S.P. Spekreijse. *Multiple grid and Osher's scheme for the efficient solution of the steady Euler equations.*
AMS 65N05, 65N30, 76G15, 76H05; 22 pp.; **key words:** steady Euler equations, multigrid methods.
Abstract: An iterative method is developed for the solution of steady Euler equations for inviscid flow. The system of hyperbolic conservation laws is discretized by a finite volume Osher-discretization. The iterative method is a multiple grid (FAS) iteration with symmetric Gauss-Seidel (SGS) as a relaxation method. Initial estimates are obtained by full multigrid (FMG). In the point-wise relaxation the equations are kept in block-coupled form and local linearization of the equations and the boundary conditions are considered. The efficient formulation of Osher's discretization of the 2-D non-isentropic steady Euler equations and its linearization is presented. The efficiency of FAS-SGS iteration is shown for a transsonic model problem. It appears that the rate of convergence is independent of the gridsize and that for all meshsizes the discrete system is solved up to truncation error accuracy in only a few (2 or 3) iteration cycles.

NM-R8508. B.P. Sommeijer. *On the economization of explicit Runge-Kutta methods.*
AMS 65L05; CR G.1.7; 17 pp.; **key words:** initial value problems, Runge-Kutta methods.
Abstract: A modification of explicit Runge-Kutta (RK) methods is proposed. Schemes are constructed which require less derivative-evaluations to achieve a certain order than do classical RK methods. As an example, we give a second-order method requiring one evaluation, two third-order methods using one and two evaluations respectively, and finally a fourth-order method which requires two evaluations. Numerical examples illustrate the behaviour of these schemes.

NM-R8509. P.J. van der Houwen & B.P. Sommeijer. *Predictor-corrector methods for periodic second-order initial value problems.*
AMS 65L05; CR G.1.7; 17 pp.; **key words:** numerical analysis, ordinary differential equations, periodic solutions, predictor-corrector methods.
Abstract: Predictor-corrector methods are constructed for the accurate representation of the eigenmodes in the solution of second-order differential equations without first derivatives. These methods have (algebraic) order 4 and 6, and phase errors of orders up to 10. For linear and weakly nonlinear problems where homogeneous solution components dominate, the methods proposed in this paper are considerably more accurate than conventional methods.

NM-R8510. P.J. van der Houwen. *Discretization of hyperbolic differential equations with periodic solutions.*
(see NM-R8514).

NM-R8511. F.W. Wubs. *Performance evaluation of explicit shallow-water equations solvers on the CYBER 205.*
AMS 65M10, 76D99; 12 pp.; **key words:** stabilization, hyperbolic equations, method of lines, residual averaging, shallow-water equations.
Abstract: The performance of an explicit method and an ADI method for shallow-water equations is compared on a CYBER 205. Furthermore, a stabilization technique is discussed, which stabilizes the explicit method in such a way that any desired time step is possible without the development

of instabilities. Comparing the codes for two test models, we found that the explicit methods are attractive on the CYBER 205. Finally, some proposals are made for the handling of irregular geometries.

NM-R8512. J. Kok. *Two Ada mathematical functions packages for use in real time.*
AMS 69D49, 65-04; 9 pp.; **key words:** Ada, high level language, basic mathematical functions, scientific libraries, portability, real-time processing.
Abstract: Two portable Ada packages are proposed for the provision of basic mathematical functions in a form suitable for real-time processing. These packages satisfy the requirements given in the 'Guidelines for the design of large modular scientific libraries in Ada' with regard to services requested by real-time processes.

NM-R8513. J.H.M. ten Thije Boonkkamp & J.G. Verwer. *On the odd-even hopscotch scheme for the numerical integration of time-dependent partial differential equations.*
AMS 65M10; CR 5.17; 15 pp.; **key words:** partial differential equations, convection-diffusion equations, numerical time stepping, odd-even hopscotch method.
Abstract: This paper is devoted to the odd-even hopscotch scheme for the numerical integration of time-dependent partial differential equations. Attention is focussed on two aspects. Firstly, via the equivalence to the combined leapfrog-Du Fort-Frankel method we derive the explicit expression of the critical time step for Neumann stability for a class of multi-dimensional convection-diffusion equations. This expression can be derived directly by applying a useful stability theorem due to Hindmarsh, Gresho & Griffiths. The interesting thing about the critical time step is that it is independent of the diffusion parameter and yet smaller than the critical time step for zero diffusion, but only in the multi-dimensional case. This curious phenomenon does not occur for the one-dimensional problem. Secondly, we consider the drawback of the Du Fort-Frankel accuracy deficiency of the hopscotch scheme. To overcome this deficiency we discuss global Richardson extrapolation in time. This simple device can always be used without reducing feasibility. Numerical examples are given to illustrate the results of extrapolation.

NM-R8514. P.J. van der Houwen. *Spatial discretization of hyperbolic equations with periodic solutions.*
AMS 65M20, 76B15; 15 pp.; **key words:** numerical analysis, hyperbolic equations, periodic solutions.
Abstract: We investigate the Cauchy problem for hyperbolic equations for which the frequencies of the main Fourier components in the solution are located in a given frequency interval. Difference formulas for the spatial derivatives are constructed that are tuned to the given intervals of frequencies. Numerical examples illustrating these special discretizations are given both for linear and nonlinear problems.

NM-R8515. J. van de Lune, H.J.J. te Riele & D.T. Winter. *On the zeros of the Riemann zeta function in the critical strip; IV.*
AMS 10H05, 10-04, 65E05, 30-04; CR G.1.0; 18 pp.; **key words:** Riemann hypothesis, Riemann zeta function, Gram blocks, Rosser's rule.
Abstract: Very extensive computations are reported which extend and, partly, check previous computations concerning the location of the complex zeros of the Riemann zeta function. The results imply the truth of the Riemann hypothesis for the first 1,500,000,001 zeros of the form $\sigma + it$ in

the critical strip with $0 < t < 545{,}439{,}823.215$, i.e., all these zeros have real part $\sigma = \frac{1}{2}$. Moreover, all these zeros are simple. Various tables are given with statistical data concerning the numbers and first occurences of Gram blocks of various types, the numbers of Gram intervals containing m zeros, for $m = 0,1,2,3$ and 4, and the numbers of exceptions to 'Rosser's rule' of various types (including some formerly unobserved types). Graphs of the function $Z(t)$ are given near five rarely occurring exceptions to Rosser's rule, near the first Gram block of length 9, near the closest observed pair of zeros of the Riemann zeta function, and near the largest (positive and negative) found values of $Z(t)$ at Gram points. Finally, reference is given to various number-theoretical implications.

NM-R8516. W.H. Hundsdorfer. *Stability and B-convergence of linearly implicit Runge-Kutta methods.*
AMS 65L05, 65L20; 16 pp.; **key words:** numerical analysis, stiff initial value problems, linearly implicit Runge-Kutta methods, B-convergence.
Abstract: In this paper we study stability and convergence properties of linear implicit Runge-Kutta methods applied to stiff semi-linear systems of differential equations. The stability analysis includes stability with respect to internal perturbations. All results presented in this paper are independent of the stiffness of the system.

NM-R8517. K. Burrage, W.H. Hundsdorfer & J.G. Verwer. *A study of B-convergence of Runge-Kutta methods.*
AMS 65L05; CR 5.17; 15 pp.; **key words:** numerical analysis, implicit Runge-Kutta methods, stiff problems, B-convergence.
Abstract: This paper deals with the convergence analysis of implicit Runge-Kutta methods as applied to stiff, semi-linear systems of the form $\dot{U}(t) = QU(t)+g(t,U(t))$. A criterion is developed which determines whether the order of optimal B-convergence is at least equal to the stage order or one order higher. This criterion is studied for a number of interesting classes of methods.

NM-R8518. W.M. Lioen. *NUMVEC FORTRAN library manual. Chapter: Elliptic PDEs, Routine: MGZEB.*
AMS 65V05, 65N20, 65F10; CR 5.17; 17 pp.; **key words:** elliptic PDEs, Galerkin approximation, multigrid methods, software, sparse linear systems, zebra relaxation.
Abstract: The NUMVEC FORTRAN library routine MGZEB is described. MGZEB solves 7-diagonal linear systems, that arise from 7-point discretizations of elliptic PDEs on a rectangle, using a multigrid technique with zebra relaxation as smoothing process.

MS-R8504. R. Gill & M. Schumacher. *A simple test of the proportional hazards assumption.*
AMS 62P10, 62G05; 34 pp.; **key words:** censored data rank tests, proportional hazards.
Abstract: When comparing two samples of possibly censored survival times it is very often important to assess the proportionality of the underlying hazard functions. In order to check the assumption of proportional hazards graphical methods and several test procedures have been proposed so far. Nearly all of these tests, however, are based on an arbitrarily chosen partition of the time axis and/or are difficult to compute. The key idea behind the new test procedures proposed in this paper is the observation that in nonproportional hazards situations different two-sample tests, e.g. the logrank and a generalized Wilcoxon test, might come up with very different answers. Our test procedures use this discrepancy as a check of the proportional hazards assumption and

are based on the relationship between generalized linear rank tests and estimates of the proportionality constant. This implies that the test statistics can be interpreted in a very natural way and almost all computation effort has to be done anyway. In additional, a related graphical method is presented which was originally proposed by Lee & Pirie for comparing trends in series of events.

MS-R8505. K.O. Dzhaparidze. *On asymptotic inference about intensity parameters of a counting process.*
AMS 62F12, 62G05, 62M99; 14 pp.; **key words:** Cox's regression model, multivariate counting process, compensator, parameter estimation.
Abstract: The Cox regression model may be viewed as a special case of the general model described in this paper via the pair $(\bar{A}_t, \Psi_t)$ of predictable characteristics of an r-variate counting process $\mathbb{N}_t = (N_t^1,...,N_t^r)$, associated with its compensator $\mathbf{A}_t = (A_t^1,...,A_t^r)$ as follows: $\bar{A}_t = A_t^1 + ... + A_t^r$ and $\Psi_t = d\mathbf{A}/d\bar{A}_t$. It is supposed that the latter characteristic involves the real valued parameter β, i.e. $\Psi_t = \Psi_t(\beta)$, to be estimated by means of a given sample path of $\{\mathbb{N}_t, 0 \leqslant t \leqslant 1\}$. Treating this problem in its asymptotic setting, we consider our experiment as n-th in a sequence of experiments, and let $\bar{A}_t$ satisfy Condition I of asymptotic stability. Under this and certain additional conditions introduced on demand, we study asymptotic properties of the estimator $\hat{\beta}$ for β, which is in fact the Cox estimator extended to our situation. In particular, we characterize the consistency and asymptotic normality of $\hat{\beta}$ by estimating the probability of large deviations, and then showing the convergence in all moments of the distribution of $\hat{\beta}$ to a normal law. Finally, it is shown that $\hat{\beta}$ is the best within a class of (regular) estimators in the sense that none of them can have an asymptotic distribution that is less spread out than that of $\hat{\beta}$.

MS-R8507. P. Haccou, E. Meelis & S. van de Geer. *On the likelihood ratio test for a change point in a sequence of independent exponentially distributed random variables.*
AMS 62E20, 62F05, 62F03, 62E25, 62F04, 62P10; 31 pp.; **key words:** Bahadur efficiency, change point problem, exponential distribution, likelihood ratio test, normed uniform quantile process.
Abstract: Let $x_1,...,x_{n+1}$ be independent exponentially distributed random variables, and let x_i have intensity λ_1 for $i \leqslant \tau$ and intensity λ_2 for $i > \tau$, where τ is an unknown instant and λ_1 and λ_2 are also unknown. In this paper we prove that the asymptotic null-distribution of the likelihood ratio statistic for testing $\lambda_1 = \lambda_2$ (or, equivalently, $\tau = 0$ or $n + 1$) is an extreme value distribution, by application of theorems concerning the normed uniform quantile process. The rate of convergence is studied with Monte Carlo methods. Since it appears very low, simulated 5% critical values are given. Furthermore, it is shown that the test is optimal in the sense of Bahadur. Simulation results indicate a good power for values of n that are relevant for most applications. The likelihood ratio test is compared with another test which has the same asymptotic null-distribution. It is proved that this test has Bahadur efficiency zero. The simulation results confirm that the likelihood ratio test is superior to the latter test.

MS-R8508. A.J. Koning. *On roads with no overtaking.*
AMS 60K30, 60G35; 42 pp.; **key words:** traffic flow, stochastic processes.
Abstract: A road which narrows at a bottleneck from an ∞-lane road to a one-lane road is studied with the aid of two independent stochastic processes. Special attention is given to headways. At the bottleneck an equilibrium headway can be viewed as the maximum of a shifted exponential random variable and a minimum headway. After the bottleneck the situation becomes far more complicated. However, at a sufficiently large distance from the bottleneck an equilibrium headway may be approximated by the maximum of a shifted exponential random variable and a minimum headway, with the parameters of the shifted exponential random variable depending on the desired

speed by the car. The distance from the bottleneck only affects the location, not the scale. Results are checked by Monte Carlo experiments.

AM-R8510. F. van den Bosch & O. Diekmann. *Egg-eating predator-prey interactions: the effect of the functional response and of age-structure.*
AMS 92A15; 19 pp.; **key words:** age structured population dynamics, egg-eating predators, functional response, stability, Hopf bifurcation.
Abstract: In this paper we analyse an age-structured predator-prey model in which predators eat only very young prey. The model can be formulated as a system of three Volterra integral equations with an implicitly defined non-linearity. An interpretation of the implicit relation is given. The linearized stability of the steady-states is investigated. It turns out that concentration of the predator on very young individuals is a stabilizing mechanism. Furthermore, it is seen that a compound parameter which is a measure for the efficiency of the predator has a major influence on the stability of the steady-states. If the efficiency of the predator decreases the steady-state can become unstable and oscillations will arise. Furthermore, it is seen from the model that the destabilizing effect of a juvenile period is stronger when it concerns the predator than when it concerns the prey species.

AM-R8511. H.R. Thieme. *A differential-integral equation modelling the dynamics of populations with a rank structure.*
AMS 92A15; 21 pp.; **key words:** rank structure, population dynamics, territorial or hierarchical organization of populations, quasimonotone differential equations, uniqueness of non-trivial equilibrium states, global asymptotic stability, threshold condition, spectral properties of compact strongly positive linear operators on Banach lattices, Krasnosel'skii's sublinearity (concavity) method.
Abstract: In order to illustrate the stabilizing potential of rank structures for the development of populations we propose a differential-integral equation (differentiation in time, integration over rank) modelling the dynamics of rank-structured (e.g. territorially or hierarchically organized) populations. After establishing existence and uniqueness of solutions we prove that, under biologically interpretable conditions, the population either dies out or tends towards a uniquely determined non-zero equilibrium state. Which of these alternatives actually occurs depends on the reproductive potential of the population and the permeability of the rank structure.

AM-N8501. H.E. de Swart. *Definitions and concepts in the theory of stochastic differential equations.*
AMS 34F05, 60J25; 19 pp.; **key words:** white noise, Markov process, Fokker Planck equation, stochastic differential equations.
Abstract: In this technical note we summarize some definitions and concepts of stochastic processes, which are of importance in the theory of randomly perturbed dynamical systems. The following topics are reviewed: white noise, Chapman-Kolmogorov equation, Fokker-Planck equation, Wiener process, stochastic integrals, stochastic differential equations, and coloured noise.

PM-R8503. A.E. Brouwer. *Uniqueness and nonexistence of some graphs related to M_{22}.*
AMS 05B25, 05C50; 8 pp.; **key words:** distance regular graphs.
Abstract: There is a unique distance regular graph with intersection array i (7,6, 4,4; 1,1,1,6); it has 330 vertices, and its automorphism group $M_{22}.2$ acts distance transitively. It does not have an antipodal 2-cover, but it has a unique antipodal 3-cover, and this latter graph has automorphism

group $3.M_{22}.2$ acting distance transitively. As a side result we show uniqueness of the strongly regular graph with parameters $(v,k,\lambda,\mu) = (231,30,9,3)$ under the assumption that it is a gamma space with lines of size 3.

PM-R8504. T.H. Koornwinder. *A group theoretic interpretation of Wilson polynomials.*
AMS 33A75, 33A65, 22E30, 43A80, 44A20; 20 pp.; **key words:** Askey scheme of hypergeometric orthogonal polynomials, Racah polynomials, Wilson polynomials, Racah coefficients, spherical harmonics, harmonics on a hyperboloid, Jacobi functions, Jacobi polynomials.

Abstract: Racah and Wilson polynomials figure at the top level of Askey's scheme of hypergeometric orthogonal polynomials. The first family of polynomials has a group theoretic interpretation as Racah coefficients, but for Wilson polynomials such an interpretation was not known. The paper presents a new group theoretic interpretation of Racah polynomials in connection with $O(p)\times O(q)\times O(r)$-invariant spherical harmonics on $S^{p+q+r-1}$ and next, by analytic continuation, a group theoretic interpretation of Wilson polynomials in connection with $O(p)\times O(q)\times O(r)$-invariant harmonics on the hyperboloid $O(p+q,r)/O(p+q,r-1)$. This is a preliminary report not containing full proofs.

PM-R8505. M. Hazewinkel. *Three lectures on formal groups.*
AMS 14L05; 20 pp; **key words:** formal groups, universal formal groups, functional equation lemma, BP cohomology, Witt vectors.

Abstract: This paper is the written version of a series of three lectures given in Windsor at the occasion of the Canadian Mathematical Society's summer school in Lie algebras and related topics in July 1984. They were intended as an introduction to the subject for an algebraically oriented audience with special emphasis on the kind of phenomena that appear when dealing with commutative formal groups over rings (rather than fields). These written notes follow the original lectures in structure but contain rather more. The contents are: 0) Introduction; 1) Two classes of examples of formal groups from other parts of mathematics; 2) Generalities and bialgebras; 3) The Lie algebra of a formal group. Characteristic zero formal Lie theory; 4) The commutativity theorem; 5) Logarithms; 6) The functional equation lemma. Examples of formal groups; 7) Universal formal groups. Generalities; 8) p-typical formal groups; 9) A universal p-typical formal group and a formal group universal over $\mathbf{Z}_{(p)}$-algebras; 10) Construction of a universal formal group; 11) Application to algebraic topology; 12) Atkin-Swinnerton Dyer congruences for elliptic curves; 13) Witt vectors; 14) Curves, Frobenius and Verschiebung; 15) Cart(A); 16) Cartier-Dieudonné classification theory; 17) p-typification; 18) Other classification results; 19) Universality of the formal group of the Witt vectors; 20) $U(\hat{W})$; 21) Remarks on noncommutative formal group theory.

PM-R8506. T.H. Koornwinder. *A group theoretic interpretation of the last part of de Branges' proof of the Bieberbach conjecture.*
AMS 33A75, 30C50, 33A45, 43A35, 43A90; 9 pp.; **key words:** Bieberbach conjecture, Milin conjecture, de Branges' system of differential equations, Gegenbauer polynomials, spherical functions on spheres, positive definite functions on spheres.

Abstract: A more conceptual and less computational proof is given for the last part of de Branges' proof of the Bieberbach conjecture, i.e. where the special functions enter and the Askey-Gasper inequality is applied. General solutions of de Branges' system of differential equations are brought in 1-1 correspondence first with Fourier-sine series and next with spherical function expansions on the sphere S^3. Restriction of spherical functions on S^5 to S^3 and positive definiteness then finish the proof.

CWI Activities

Autumn 1985

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

Study group on Analysis on Lie groups. Joint with University of Leiden. Biweekly. (T.H. Koornwinder)

Seminar on Algebra and Geometry. Monthly. (A.M. Cohen)

Cryptography working group. Biweekly. (J.H. Evertse)

Crypto Course. Jointly sponsored by the Commission of European Communities and the Centre for Mathematics and Computer Science. 14-25 October. (J.H. Evertse)

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

ESMI (European Symposium on Mathematics in Industry). 29 October-1 November. (M. Hazewinkel)

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

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

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

Lunteren meeting on Stochastics. 11,12,13 November 1984 at 'De Blije Werelt', Lunteren. Invited speakers:
L. Birgé (Paris, France), S. Csörgö (Szeged, Hungary), M. Jacobsen (Copenhagen, Denmark), J.T. Kent (Leeds, UK), R. Pyke (Seattle, USA), S.I. Resnick (Fort Collins, USA). (R. Helmers)

Study group on Statistical Image Analysis. Biweekly. (R.D. Gill)
Progress meetings on Combinatorial Optimization. Biweekly. (J.K. Lenstra)
National Colloquium on Optimization. Irregular. (J.K. Lenstra)
System Theory Days. Irregular. (J.H. van Schuppen)
Study group on System Theory. Biweekly. (J.H. van Schuppen)
Study group on Numerical Flow Dynamics. Lectures by group members. Every Wednesday. (J.G. Verwer)
Progress meetings on Numerical Mathematics. Weekly. (H.J.J. te Riele)
International Colloquium on Numerical Aspects of Vector- and Parallel Processors. Monthly, every last Friday. (H.J.J. te Riele)
Study group on Numerical Software for Vector Computers. Monthly. (H.J.J. te Riele)
Study group on Differential and Integral Equations. Lectures by visitors or group members. Irregular. (H.J.J. te Riele)
Study group on Graphics Standards. Monthly. (M. Bakker)
Study group on Dialogue Programming. (P.J.W. ten Hagen)
Colloquium Computer Graphics. Joint with University of Amsterdam. Monthly. (E. Dooyes)
Post-academic course on Modern Techniques in Software Engineering. 10,11,24,25 October. (J.C. van Vliet)
Seminar National Concurrency Project. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. 11 October, 8 November and 6 December. (J.W. de Bakker)
National Study Group on Concurrency. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. 27 September, 25 October and 22 November. (J.W. de Bakker)

Visitors to CWI from Abroad

D. & O. Berry (University of Southern California, Los Angeles, USA) 26 July. Chen Wende (Academia Sinica, Beijing, PRC) 11-13 September. D.M. Chibisov (Steklov Institute, Moscow, USSR) 17 September. C. Crepeau (University of Montreal, Canada) 8-11 September. J.M. Cushing (University of Arizona, Tucson, USA) 1-2 July. M.I. Dessouki (University of Illinois at Urbana-Champaign, USA) 23 August. M.E. Gurtin (Carnegie-Mellon University, USA) 26 September. P. Jagers (University of Göteborg, Sweden) 21 August. T. Kawazoe (Keio University, Yokohama, Japan) 4-5 July. R. Kühne (AEG research institute, Ulm, West Germany) 3-6 September. E.L. Lawler (University of California, Berkeley, USA) 1-31 July. T. Ledwina (Polytechnic, Wroclaw, Poland) 9-11 July. U. Manber (University of Wisconsin, Madison, USA) 24-26 July. P. Mandl (Charles University, Prague, Czechoslovakia) 11-22 August. S. Martello (University of Bologna, Italy) 17-20 September. A.J. Martin (Caltech, USA) 18 September. K. Mehlhorn (University of Saarland, Saarbrücken, West Germany) 30 September. B. Meister (IBM, Zürich, Switzerland) 12-16 August. O. Nerman (University of Göteborg, Sweden) 21 August. A. Neumaier (University of Freiburg, West Germany) 26 August - 7 September. T. Tomiyama (University of Tokyo, Japan) August 1985 - August 1987. P. Toth (University of Bologna, Italy) 17-20 September. J.A. Wellner (University of Washington, Seattle, USA) 2-9 September. M. Witten (University of Louisville, USA) 8-9 August. Zheng Yu Fan (East China Normal University, Shanghai) 1-3 July.

Order Form for CWI Publications

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

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

	Publication code	Price per copy	Number of copies wanted
☐	CWI Syllabus 6 *)	Dfl. 35.70	.....
☐	CS-R8513	3.70	.....
☐	CS-R8514	3.70	.....
☐	CS-R8515	3.70	.....
☐	CS-N8506	3.70	.....
☐	NM-R8507	3.70	.....
☐	NM-R8508	3.70	.....
☐	NM-R8509	3.70	.....
☐	NM-R8510	3.70	.....
☐	NM-R8511	3.70	.....
☐	NM-R8512	3.70	.....
☐	NM-R8513	3.70	.....
☐	NM-R8514	3.70	.....
☐	NM-R8515	3.70	.....

*) not available on exchange

	Publication code	Price per copy	Number of copies wanted
☐	NM-R8516	3.70	.....
☐	NM-R8517	3.70	.....
☐	NM-R8518	3.70	.....
☐	MS-R8504	4.80	.....
☐	MS-R8505	3.70	.....
☐	MS-R8507	4.80	.....
☐	MS-R8508	6.--	.....
☐	AM-R8510	3.70	.....
☐	AM-R8511	3.70	.....
☐	AM-N8501	3.70	.....
☐	PM-R8503	3.70	.....
☐	PM-R8504	3.70	.....
☐	PM-R8505	3.70	.....
☐	PM-R8506	3.70	.....

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

Name .....

Street .....

City .....

Country .....

ESMI

European Symposium on Mathematics in Industry
29 Oct. - 1 Nov. 1985
(Organized by: Wiskundige Dienstverlening (WD),
Univ. of Nijmegen and CWI, Amsterdam)

Very many practical problems in industry and commerce nowadays can be attacked by a combination of mathematical modelling and analysis if necessary supported by simulation. There are many active groups in Europe in this general field, all with different experiences and areas of expertise.

Goal of this symposium is to compare experiences, to assess what is possible and what should be possible, and to discuss ways and means for further (university) research lab-industry relations both at the level of problem solving and - intertwined therewith - continuing education programmes.

There will be two panel sessions to discuss these and related themes such as the possible creation of a who-does-what-where database.

Opening session

Tuesday afternoon, 13.45-18.00, at the Royal Institute of the Tropics. Speakers are: E. VAN SPIEGEL (Wetenschapsbeleid) C. SILVER BRITE programme, EEG) H. PLATE (Volkswagenstiftung) W.A. KOUMANS (TNO) H. BOSMA (Philips Nat. Lab.)

Lectures during the following three days
29 October - 1 November 1985, at CWI

J. ANDREWS (CEGB, MEL, Southampton, UK) & A.B. TAYLER (Univ. of Oxford, UK) (Integrated set of lectures), *Mathematics applied to welding problems;* M. ANILE (Univ. of Catania, Italy), *Mathematical modeling of the atmosphere and industrial agriculture;* CL. BARDOS (Ec.Norm.Sup., Paris, France), *About practical applications of the mathematical theory of kinetic equations;* A. BENSOUSSAN (INRIA, Le Chesnay, France), *Applications of stochastic control in*

electricity production: description of a cooperation with Electricité de France; G. BORNARD (Lab. d'automatique de Grenoble, France), *Control design of destillation columns;* Y. CHERRUAULT, A. RICHARD (Medimat, Paris, France) & J.F. PROST (Servier Labs, France) (Integrated set of lectures), *Mathematical models in pharmacokinetics and medicine;* E. CUMBERBATCH (Claremont College, Calif., USA), *Mathematical problems brought to the Claremont Mathematical Clinic: the American experience in university-industry relations;* M. HEILIO (Lappeenranta Techn. Univ., Finland), *Survey of the university-industry cooperation in Finland;* J.K. LENSTRA (CWI, Amsterdam, The Netherlands), *Interactive planning methods;* S. MCKEE (UCINA, Oxford, UK), *Academic-industrial collaboration in numerical analysis;* J. MOLENAAR (Univ. of Nijmegen, The Netherlands), *The optimal form of diamond heat sinks;* H. NEUNZERT (Univ. of Kaiserslautern, BRD) & J. PEDERSEN (Audi, Ingolstadt, BRD) (Integrated set of lectures), *Mathematical problems in car production reliability;* D. NORMAND-CYROT (SUPELEC, Gif sur Yvette, France), *Identification of nonlinear systems. Applications to electrical power plants;* J. OPPELSTRUP (FEMPROG, Stockholm, Sweden), *How to meet the growing demand for mathematics software in industry;* M. PRIMECERIO (Univ. of Florence, Italy), *Free boundary problems: ground freezing, swelling solvents and intumescent paints;* W. SCHEMPP (Univ. of Siegen, BRD), *Radar signal design, digital signal processing, laser beam optics and the Heisenberg group;* D. SUNDSTROM (ITM, Stockholm, Sweden), *The Swedisch industry supports research in applied mathematics and sets priorities;* P. TEN HAGEN (CWI, Amsterdam, The Netherlands) & T. TOMIYAMA (Univ. of Tokyo, Japan), *Methods bases for mathematicians;* C.B. VREUGDENHIL (TH Delft, The Netherlands), *ISNAS: a software system for flow simulation;* H.-J. WACKER (Univ. of Linz, Austria), *Mathematical research and consulting in Linz: power plants, reaction columns and kilns.*

Contents